Technological University Dublin
ARROW@TU Dublin

Doctoral

Engineering

2015

Enhanced Quality of Experience Based on Enriched Network Centric and Access Control Mechanisms

Andreas Roos
Technological University Dublin

Follow this and additional works at: https://arrow.tudublin.ie/engdoc

 Part of the Electrical and Electronics Commons

Recommended Citation

Roos, A. (2015). *Enhanced Quality of Experience Based on Enriched Network Centric and Access Control Mechanisms*. Doctoral Thesis. Technological University Dublin. doi:10.21427/D70608

This Theses, Ph.D is brought to you for free and open access by the Engineering at ARROW@TU Dublin. It has been accepted for inclusion in Doctoral by an authorized administrator of ARROW@TU Dublin. For more information, please contact arrow.admin@tudublin.ie, aisling.coyne@tudublin.ie, gerard.connolly@tudublin.ie, vera.kilshaw@tudublin.ie.

Enhanced Quality of Experience based on enriched Network Centric and Access Control Mechanisms

Andreas Roos



A Thesis Presented to the Dublin Institute of Technology

for the Degree of Doctor of Philosophy

April 2015

Supervisors:

Dr. Andreas Th. Schwarzbacher

Prof. Dr.-Ing. Sabine Wieland

School of Electrical and Electronic Engineering,

Dublin Institute of Technology,

Ireland.

Dedicated to my grandfather

Declaration

I certify that this thesis which I now submit for examination for the award of Doctor of Philosophy (PhD), is entirely my own work and has not been taken from the work of others, save and to the extent that such work has been cited and acknowledged within the text of my work.

This thesis was prepared according to the regulations for postgraduate study by research of the Dublin Institute of Technology and has not been submitted in whole or in part for another award in any other third level institution

The work reported on in this thesis conforms to the principles and requirements of the DIT's guidelines for ethics in research.

DIT has permission to keep, lend or copy this thesis in whole or in part, on condition that any such use of the material of the thesis be duly acknowledged.

Signature: _____ Date: 23th of April 2015

Andreas Roos

Abstract

In the digital world service provisioning in user satisfying quality has become the goal of any content or network provider. Besides having satisfied and therefore, loyal users, the creation of sustainable revenue streams is the most important issue for network operators [1], [2], [3]. The motivation of this work is to enhance the quality of experience of users when they connect to the Internet, request application services as well as to maintain full service when these users are on the move in WLAN based access networks. In this context, the aspect of additional revenue creation for network operators is considered as well. The enhancements presented in this work are based on enriched network centric and access control mechanisms which will be achieved in three different areas of networks capabilities, namely the network performance, the network access and the network features themselves.

In the area of network performance a novel authentication and authorisation method is introduced which overcomes the drawback of long authentication time in the handover procedure as required by the generic IEEE 802.1X process using the EAP-TLS method. The novel sequential authentication solution reduces the communication interruption time in a WLAN handover process of currently several hundred milliseconds to some milliseconds by combining the WPA2 PSK and the WPA2 EAP-TLS. In the area of usability a new user-friendly hotspot registration and login mechanisms is presented which significantly simplifies how users obtain WLAN hotspot login credentials and logon to a hotspot. This novel barcode initiated hotspot auto-login solution obtains user credentials through a simple SMS and performs an auto-login process that avoids the need to enter user name and password on the login page manually. In the area of network features a new system is proposed which overcomes the drawback that users are not aware of the quality in which a service can be provided prior to starting the service. This novel graceful denial of service solution informs the user about the expected application service quality before the application service is started.

Acknowledgements

Firstly, I would like to express my sincere appreciation and would like to thank my supervisor Dr. Andreas Schwarzbacher from the Dublin Institute of Technology for his support and abundance of patience. I would like to thank my co-supervisor Prof. Dr.-Ing. Sabine Wieland from the University of Applied Sciences Leipzig for her support and stimulating discussions throughout the thesis period.

I would like to thank my colleagues Dr. Nico Bayer and Dr. Dmitry Sivchenko for their fruitful discussions and motivations during this thesis. It is a real honour for me to work with both of them over the past years.

I am grateful for all the supports I have gotten from my colleagues from the T-Labs especially team Seamless Network Control and team Wireless Technology Networks. Furthermore, I would like to thank my colleagues in the University of Applied Sciences Leipzig for their assistance and all of those who directly or indirectly have contributed to the success of this thesis.

Last but not least, I would like to give a special thank to my wife for her patience, understanding and moral support during the time of the thesis. I also would like to thank my family for their love, support and faith with me.

Abbreviations List

AAA	Authentication, Authorisation and Accounting
ACF	Access Control Function
ADF	Access Decision Function
AP	Access Point
ARPU	Average Revenue Per User
ASQ	Assured Service Quality
AW	Authentication Window
A-RACF	Access Resource and Admission Control Function
BE	Best Effort
BER	Bit Error Rate
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
Carmen	CARrier grade MEsh Networks
CCMP	Counter-mode/CBC-MAC Protocol
CDN	Content Delivery Network
CN	Core Network
CPF	Connectivity Profile Function
CSCF	Call Session Control Functions
DHCP	Dynamic Host Control Protocol
DSL	Digital Subscriber Line
EAAA	External AAA
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data Rates for GSM Evolution
EIA	Electronic Industries Alliance
EIRP	Equivalent Isotropic Radiated Power
ETSI	European Telecommunications Standards Institute
E2E	End-to-End
FPIP	First Possible Interruption Point
FTP	File Transfer Protocol

FUPS	Flexible, User-friendly and Personalized Services
G	Generation
GDoS	Graceful Denial of Service
GPRS	General Packet Radio Service
GSM	System for Mobile Communications
GTK	Group Transient Key
HC	Hotspot Controller
HLP	Hotspot Login Page
HOKEY	Handover Keying
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IAPP	Inter Access Point Protocol
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
InfSP	Information Service Provider
IP	Internet Protocol
IPTV	IP television
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITU	International Telecommunication
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
KEK	Key Encryption Key
LTE	Long Term Evolution
LAAA	Local AAA
LAN	Local Area Network
LI	Length of Interruption
LPIP	Last Possible Interruption Point
MAC	Media Access Control
MIC	Message Integrity Check
MN	Mobile Node
MOS	Mean Opinion Score
MPI	Multiple Point of Interruption

NAC	Network Access Control
NACF	Network Access Configuration Function
NASS	Network Attachment Subsystem
NG	Neighbour Graph
NGS	Next Generation Service
NSP	Network Service Provider
NFV	Network Function Virtualisation
P-CSCF	Proxy Call State Control Function
PAP	Password Authentication Protocol
PESQ	Perceptual Evaluation of Speech Quality
PMK	Pairwise Master Key
PoA	Point of Attachment
PSK	Pre Shared Key
PSTN	Public Switched Telephone Network
PTK	Pairwise Transient Key
QoE	Quality of Experience
QoS	Quality of Service
QR	Quick Response
RACS	Resource and Admission Control Subsystem
RADIUS	Remote Authentication Dial-In User Service
RCEF	Resource Control Enforcement Function
RSN	Robust Secure Network
RSNA	RSN Association
RSSI	Received Signal Strength Indication
RTP	Real-Time Transport Protocol
ScaleNet	Scalable and converged multi-access operator’s network
SEF	Service Enhancement Function
SEFA	Service Enhancement Functional Area
SIP	Session Initiation Protocol
SLA	Service Level Agreements
SMS	Short Message Service
SPF	Service Profile Function
SPI	Single Point of Interruption

TBI	Time Between Interruption
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TLS	Transport Layer Security
TK	Temporal Key
TP	Termination Point
UDP	User Datagram Protocol
UE	User Equipment
VoIP	Voice over IP
WEP	Wired Equivalent Privacy
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WPA	Wi-Fi Protected Access
WS	Web Server

Table of Contents

DECLARATION ..... **III**

ABSTRACT ..... **IV**

ACKNOWLEDGEMENTS ..... **V**

ABBREVIATIONS LIST ..... **VI**

TABLE OF CONTENTS ..... **X**

LIST OF FIGURES ..... **XIII**

LIST OF TABLES ..... **XV**

1 INTRODUCTION **1**

1.1 MOTIVATION 7
1.1.1 Improved Network Performance to Enhance QoE 8
1.1.2 Improved Network Access to Enhance QoE 11
1.1.3 Improved Network Features to Enhance QoE 13
1.2 RELATED WORK 14
1.2.1 Improvements of Handover Process in WLAN 14
1.2.2 Network Access in WLAN Hotspots 17
1.2.3 Network Features which Improve Application Service Delivery 19
1.3 THESIS OVERVIEW 21

2 GENERAL BACKGROUND **22**

2.1 NEXT GENERATION NETWORKS 23
2.2 COMMUNICATION ECOSYSTEM 25
2.2.1 Quality of Service 28
2.2.2 Quality of Experience 32
2.3 AUTHENTICATION, AUTHORISATION AND ACCOUNTING 33
2.4 USABILITY 36
2.5 CREATION OF REVENUE FOR NETWORK OPERATORS 38
2.6 SUMMARY 41

3 CHALLENGES IN REAL-TIME COMMUNICATION AND USER SATISFIED SERVICE PROVISIONING **44**

3.1 MOBILITY AND HANDOVER TYPES 46
3.2 SPEECH QUALITY INVESTIGATION BASED ON HANDOVER SIMULATION 47
3.2.1 Speech Quality Simulation Setup 50
3.2.2 Single Interruption within Audio Streams 51
3.2.3 Multiple Interruptions within Audio Streams 53
3.3 SPEECH QUALITY INVESTIGATION BASED ON HANDOVER EMULATION 56
3.3.1 Handover Emulation Measurement Setup 57
3.3.2 Measurement Results of Handover Emulation 60
3.4 HANDOVER TIME BEHAVIOUR IN SECURED WIRELESS LANS 63
3.4.1 Handover Measurement Setup in IEEE 802.11 66
3.4.2 Measurement Preparations 68
3.4.3 Investigation of Handover Time Behaviour 69
3.4.4 WEP Investigations of Handover Time Behaviour 70
3.4.5 WPA2 Investigations of Handover Time Behaviour 71
3.4.6 Summary of Handover Time Behaviour Investigations 75

3.4.7 IEEE 802.1X using EAP-TLS Method 77
3.4.8 Drawbacks of IEEE 802.1X EAP-TLS Authentication Time Behaviour 81
3.5 MOBILITY IN DEPLOYED NETWORK ARCHITECTURES 83
3.6 WLAN-BASED HOTSPOT 90
3.7 SERVICE PROVISIONING TO USERS SUPPORTED BY ADDED VALUE SERVICES 93
3.8 SUMMARY OF CHALLENGES IN USER SATISFYING SERVICE QUALITY DELIVERY 99
3.8.1 Investigated Topics 99
3.8.2 Network Capabilities Influencing Aspects 102
3.8.3 Outlook to Improved Network Capabilities 104

4 ENHANCED QUALITY OF EXPERIENCE BASED ON IMPROVED NETWORK CAPABILITIES 106

4.1 SEQUENTIAL AUTHENTICATION SOLUTION 108
4.1.1 Objectives 109
4.1.2 Requirements 109
4.1.3 Technical Solution 111
4.2 BARCODE INITIATED HOTSPOT AUTO-LOGIN 118
4.2.1 Objectives 118
4.2.2 Requirements 120
4.2.3 Technical Solution 121
4.3 GRACEFUL DENIAL OF SERVICE FOR IP-BASED APPLICATION SERVICES 128
4.3.1 Service Enhancement Functional Area 129
4.3.2 Objectives 137
4.3.3 Requirements 138
4.3.4 Technical Solution 139
4.4 SUMMARY 145

5 IMPLEMENTATION 147

5.1 SEQUENTIAL AUTHENTICATION SOLUTION 147
5.2 BARCODE INITIATED HOTSPOT AUTO-LOGIN 159
5.3 GRACEFUL DENIAL OF SERVICE FOR IP-BASED APPLICATION SERVICES 173
5.4 SUMMARY 184

6 RESULTS 186

6.1 VERIFICATION 186
6.1.1 Sequential Authentication Solution 186
6.1.2 Barcode Initiated Hotspot Auto-login 190
6.1.3 Graceful Denial of Service for IP-based Application Services 194
6.2 BENCHMARKING 198
6.2.1 Sequential Authentication Solution 198
6.2.2 Barcode Initiated Hotspot Auto-login 200
6.2.3 Graceful Denial of Service for IP-based Application Services 203
6.3 SUMMARY 205

7 CONCLUSIONS 207

7.1 SPECIFIC CONCLUSIONS 207
7.1.1 Sequential Authentication Solution 207
7.1.2 Barcode Initiated Hotspot Auto-login 208
7.1.3 Graceful Denial of Service for IP-based Application Services 209
7.2 GENERAL CONCLUSIONS 209
7.2.1 Sequential Authentication Solution 209
7.2.2 Barcode Initiated Hotspot Auto-login 210
7.2.3 Graceful Denial of Service for IP-based Application Services 210
7.3 FUTURE WORK 211

REFERENCES 214

AUTHORS PUBLICATIONS 232

APPENDIX 236

A.1 BARCODE 236
A.2 ACCESS POINT CONFIGURATION 237
A.3 MEASUREMENT PREPARATIONS 239
A.4 WEP INVESTIGATIONS OF HANDOVER TIME BEHAVIOUR 240
A.5 WPA2 INVESTIGATIONS OF HANDOVER TIME BEHAVIOUR 243
A.6 WI-FI ALLIANCE - WPA2 STATEMENT 247
A.7 GRACEFUL DENIAL OF SERVICE MEASUREMENT 247

List of Figures

FIGURE 1.1: QUALITY OF EXPERIENCES – AREAS OF IMPROVEMENTS. 8
FIGURE 2.1: ITU-T NGN ARCHITECTURE OVERVIEW (SOURCE: [91]). 24
FIGURE 2.2: TERMINOLOGY OF A COMMUNICATION ECOSYSTEM (SOURCE: [92]). 26
FIGURE 2.3: ITU-T E.800 FRAMEWORK [IBID]. 30
FIGURE 2.4: MAPPING OF USER CENTRIC QOS REQUIREMENTS AND MODEL FOR USER CENTRIC QOS CATEGORIES BASED ON ITU-T REC. G.1010 [99]. 31
FIGURE 2.5: AUTHENTICATION, AUTHORISATION AND ACCOUNTING ARCHITECTURE. 35
FIGURE 2.6: STANDARDIZED VIEW ON USABILITY AND USER EXPERIENCE. 37
FIGURE 3.1: OVERVIEW OF SEAMLESS REAL-TIME SERVICE PROVISIONING INVESTIGATIONS. 45
FIGURE 3.2: BLOCK DIAGRAM OF PESQ VALUE DETERMINATION. 50
FIGURE 3.3: PESQ SIMULATION; A) SINGLE AND B) MULTIPLE INTERRUPTIONS WITHIN AUDIO STREAM. 52
FIGURE 3.4: POINT OF INTERRUPTION IN AUDIO STREAM INFLUENCES PESQ VALUE AND THUS THE SPEECH QUALITY; LI = 250 MS. 53
FIGURE 3.5: PESQ VALUE IN CASE OF FIVE AUDIO STREAM INTERRUPTIONS, TBI = 11.7 S. 55
FIGURE 3.6: HANDOVER EMULATION MEASUREMENT SETUP. 57
FIGURE 3.7: STRUCTURE OF VOIP PACKET. 58
FIGURE 3.8: INFLUENCE OF COMMUNICATION INTERRUPTION INTERVAL OF 5 S ON SPEECH QUALITY. 60
FIGURE 3.9: INFLUENCE OF COMMUNICATION INTERRUPTION INTERVAL OF 10 S ON SPEECH QUALITY. 61
FIGURE 3.10: INFLUENCE OF COMMUNICATION INTERRUPTION INTERVAL OF 15 S ON SPEECH QUALITY. 61
FIGURE 3.11: INFLUENCE OF COMMUNICATION INTERRUPTION INTERVAL OF 20 S ON SPEECH QUALITY. 62
FIGURE 3.12: HANDOVER MEASUREMENT SETUP WITH WEP AND WPA2-PSK ENCRYPTION. 67
FIGURE 3.13: HANDOVER MEASUREMENT SETUP WITH WPA2 EAP-TLS AUTHENTICATION – LOCAL AAA SERVER. 67
FIGURE 3.14: HANDOVER MEASUREMENT SETUP WITH WPA2 EAP-TLS AUTHENTICATION – EXTERNAL AAA SERVER. 68
FIGURE 3.15: HANDOVER TIME BEHAVIOUR MEASUREMENT RESULTS. 75
FIGURE 3.16: SEQUENCE DIAGRAM OF IEEE 802.1X USING EAP-TLS AUTHENTICATION WITH RADIUS SERVER 78
FIGURE 3.17: EAP-TLS COMMUNICATION; LOCAL AAA SERVER. 82
FIGURE 3.18: PING COMMUNICATION; LOCAL AAA SERVER. 82
FIGURE 3.19: MOBILITY SCENARIOS OF CUSTOMERS IN WLAN. 83
FIGURE 3.20: PATH LOSS IN DEPENDENCY OF DISTANCE BETWEEN TRANSMITTER AND RECEIVER [IBID]. 88
FIGURE 3.21: GENERIC HOTSPOT NETWORK ARCHITECTURE. 90
FIGURE 3.22: SERVICE, NETWORK AND USER / DEVICE ARE NOT AWARE OF EACH OTHER. 95
FIGURE 3.23: INFLUENCING ASPECTS ON NETWORK CAPABILITIES AND ITS RELATIONSHIP WITH THE USER PERCEPTIONS. 103
FIGURE 4.1: RELATION AMONG FOCUSED NETWORK CAPABILITIES AND USE CASES. 106
FIGURE 4.2: INTERRUPTION OF DATA COMMUNICATION WHILE HANDOVER PROCESS. 112
FIGURE 4.3: INTERRUPTION OF DATA COMMUNICATION DUE TO TRADITIONAL NETWORK ACCESS CONTROL MECHANISMS. 113
FIGURE 4.4: INTERRUPTION OF DATA COMMUNICATION IN SAS. 115
FIGURE 4.5: USE CASE DIAGRAM OF BARCODE INITIATED HOTSPOT AUTO-LOGIN APPROACH. 121
FIGURE 4.6: BARCODE INITIATED HOTSPOT AUTO-LOGIN ARCHITECTURE. 122
FIGURE 4.7: SEQUENCE DIAGRAM OF BIHA SOLUTION. 125
FIGURE 4.8: FUPS AS KEY FACTORS OF NEXT GENERATION SERVICE PROVISIONING. 129
FIGURE 4.9: SERVICE ENHANCEMENT FUNCTIONAL AREA IN RELATION TO APPLICATION AND NETWORK PLANE. 130
FIGURE 4.10: EXAMPLE: SEVERAL SERVICE ENHANCEMENT FUNCTIONS TO REALISE A CERTAIN USE CASE. . 131
FIGURE 4.11: MUTUAL AWARENESS OF SERVICE, NETWORK AND CUSTOMER BASED ON SEF. 132
FIGURE 4.12: SEF AS INTERMEDIATE ENTITY AMONG STANDARDISED FRAMEWORKS, SUCH AS NASS, RACS AND IMS. 133
FIGURE 4.13: ETSI TISPAN NGN ARCHITECTURE OVERVIEW. 135
FIGURE 4.14: HIGH-LEVEL VIEW ON GRACEFUL DENIAL OF SERVICE ARCHITECTURE. 140

FIGURE 4.15: SEQUENCE DIAGRAM OF GRACEFUL DENIAL OF SERVICE SOLUTION. 142
FIGURE 5.1: TEMPORAL ACTIVATED PORT IN AUTHENTICATOR OF SEQUENTIAL AUTHENTICATION SOLUTION. 149
FIGURE 5.2: DEACTIVATED TEMPORAL PORT IN AUTHENTICATOR AFTER SUCCESSFUL AUTHENTICATION AND AUTHORISATION. 150
FIGURE 5.3: OPENED TEMPORAL PORT AFTER EXPIRED TIMEOUT. 151
FIGURE 5.4: FLOW DIAGRAM OF SEQUENTIAL AUTHENTICATION SOLUTION. 153
FIGURE 5.5: FLOW CHART OF SEQUENTIAL AUTHENTICATION CONCEPT USING WPA-PSK AND 802.1X WITH EAP-TLS AND RADIUS SERVER. 154
FIGURE 5.6: STATE MACHINE OF IEEE 802.11I PSK METHOD. 155
FIGURE 5.7: STATE MACHINE OF IEEE 802.11I PMK METHOD. 156
FIGURE 5.8: NEW STATE MACHINE OF SEQUENTIAL AUTHENTICATION SOLUTION. 158
FIGURE 5.9: FLOW CHART OF SEQUENTIAL AUTHENTICATION SOLUTION USING PSK AND PMK 4-WAY HANDSHAKE WITHOUT SPECIFIED EAP METHOD. 159
FIGURE 5.10: COMPONENT DIAGRAM OF BARCODE INITIATED HOTSPOT AUTO-LOGIN SOLUTION. 160
FIGURE 5.11: ACTIVITY DIAGRAM OF BARCODE INITIATED HOTSPOT AUTO-LOGIN SOLUTION. 166
FIGURE 5.12: GDOS SYSTEM ARCHITECTURE. 174
FIGURE 6.1: SEQUENCE DIAGRAM OF SEQUENTIAL AUTHENTICATION SOLUTION. 188
FIGURE 6.2: GRAPHICAL USER INTERFACE: HOTSPOT LOGIN PAGE WITH OPTION TO SELECT BARCODE INITIATED HOTSPOT AUTO-LOGIN SOLUTION FOR HOTSPOT LOGIN. 190
FIGURE 6.3: GRAPHICAL USER INTERFACE: BARCODE INITIATED HOTSPOT AUTO-LOGIN FRONT-END TO THE USER ON THE HOTSPOT LOGIN PAGE. 191
FIGURE 6.4: GRAPHICAL USER INTERFACE: HOTSPOT LOGIN PAGE WITH INFORMATION OF SUCCESSFUL PERFORMED HOTSPOT LOGON. 191
FIGURE 6.5: GRAPHICAL USER INTERFACE: START PAGE OF EXEMPLARY VIDEO PORTAL. 195
FIGURE 6.6: GRAPHICAL USER INTERFACE: STARTED VIDEO IN THE CASE OF SUFFICIENT AVAILABLE NETWORK RESOURCES IN THE NETWORK. 196
FIGURE 6.7: GRAPHICAL USER INTERFACE: NON-STARTED VIDEO IN THE CASE OF NON-SUFFICIENT AVAILABLE NETWORK RESOURCES IN THE NETWORK. 197
FIGURE 6.8: EAP AND PING COMMUNICATION IN SEQUENTIAL AUTHENTICATION CONCEPT. 199
FIGURE 6.9: GDOS RUN TIME - MEASURED FORM SEF INITIATION REQUEST (STEP 2) TO SEF INITIATION REPLY (STEP 15). 204
FIGURE A.1: 2D BARCODES: QR CODE (LEFT) AND DATA MATRIX / SEMACODE (RIGHT); BARCODE CONTENT: "WWW.MOBILFUNKTAGUNG.DE". 237
FIGURE A.2: WEP CONFIGURATION OF ACCESS POINT 1. 238
FIGURE A.3: WEP CONFIGURATION OF ACCESS POINT 2. 238
FIGURE A.4: WPA2 (EAP-TLS) CONFIGURATION OF ACCESS POINT 1 AND 2. 239
FIGURE A.5: PING TRACE OF HANDOVER; IWCONFIG (WEP). 241
FIGURE A.6: FRAME NO. 12 OF PING TRACE USING IWCONFIG (WEP). 241
FIGURE A.7: FRAME NO. 13 OF PING TRACE USING IWCONFIG (WEP). 241
FIGURE A.8: PING TRACE OF HANDOVER; WPA_SUPPLICANT (WEP). 242
FIGURE A.9: FRAME NO. 6 OF PING TRACE USING WPA_SUPPLICANT (WEP). 243
FIGURE A.10: FRAME NO. 7 OF PING TRACE USING WPA_SUPPLICANT (WEP). 243
FIGURE A.11: EAP-TLS COMMUNICATION; INTERNAL AAA SERVER SCENARIO. 243
FIGURE A.12: PING COMMUNICATION; INTERNAL AAA SERVER SCENARIO. 244
FIGURE A.13: EAP-TLS COMMUNICATION; EXTERNAL AAA SERVER SCENARIO. 245
FIGURE A.14: PING COMMUNICATION; EXTERNAL AAA SERVER SCENARIO. 246
FIGURE A.15: WPA2 RE-KEYING PROCESS USING EAP-TLS; NO AP REBOOT. 246
FIGURE A.16: WPA2 PSK RE-KEYING PROCESS. 247
FIGURE A.17: GDOS RUN TIME - MEASURED FORM SEF INITIATION REQUEST (STEP 2) TO SEF INITIATION REPLY (STEP 15). 248
FIGURE A.17: GDOS RUN TIME - MEASURED FORM SEF INITIATION REQUEST (STEP 2) TO SEF INITIATION REPLY (STEP 15). 248
FIGURE A.17: GDOS RUN TIME - MEASURED FORM SEF INITIATION REQUEST (STEP 2) TO SEF INITIATION REPLY (STEP 15). 249

List of Tables

TABLE 3.1: RELATION OF MOS, R AND PESQ VALUE. 50
TABLE 3.2: LISTING OF SIMULATED LENGTH OF INTERRUPTION. 50
TABLE 3.3: LISTING OF SIMULATED INTERRUPTION TYPES (LIS) AS WELL AS MINIMUM AND MAXIMUM OF DETERMINED APPROPRIATE PESQ VALUES. 52
TABLE 3.4: MULTIPLE INTERRUPTIONS AND DIFFERENT LENGTH OF INTERRUPTIONS IN AUDIO STREAM – SIMULATION RESULTS WITH PESQ VALUE LESS THAN FOUR ARE MARKED WITH '-'. 54
TABLE 3.5: DURATION AMONG INTERRUPTIONS DEPENDING ON THE AMOUNT OF INTERRUPTIONS IN AUDIO STREAM. 54
TABLE 3.6: INTERVAL OF COMMUNICATION INTERRUPTION. 59
TABLE 3.7: LENGTH OF INTERRUPTION IN COMMUNICATION. 59
TABLE 3.8: SPEECH QUALITY DEPENDING ON DIFFERENT LENGTH AND INTERVAL OF INTERRUPTIONS IN IP COMMUNICATION – RESULTS WITH PESQ VALUE LESS THAN FOUR ARE MARKED WITH '-'. 63
TABLE 3.9: OVERVIEW OF EXISTING WLAN SECURITY AND NETWORK ACCESS CONTROL MECHANISMS. 65
TABLE 3.10: COMMUNICATION INTERRUPTION DEPENDING ON TOOL IWCONFIG AND WPA_SUPPLICANT – WEP ENCRYPTION. 70
TABLE 3.11: HANDOVER CONFIGURATION AND AUTHENTICATION TIME USING WPA2 WITH EAP-TLS – LOCAL AAA SERVER. 72
TABLE 3.12: HANDOVER CONFIGURATION AND AUTHENTICATION TIME USING WPA2 WITH EAP-TLS – EXTERNAL AAA SERVER. 73
TABLE 3.13: HANDOVER CONFIGURATION AND AUTHENTICATION TIME USING WPA2 EAP-TLS WITHOUT AUTHENTICATION PROCESS; NO AP REBOOT. 74
TABLE 3.14: HANDOVER CONFIGURATION AND AUTHENTICATION TIME USING WPA2 PSK. 75
TABLE 3.15: EXPONENT OF PATH LOSS FOR DIFFERENT SURROUNDINGS. 85
TABLE 3.16: DISTANCES BETWEEN TRANSMITTER AND RECEIVER DEPENDING ON EXPONENT n 87
TABLE 3.17: MINIMAL RETENTION TIME IN WLAN CELL WITH A CELL RADIUS OF 60 M. 88
TABLE 3.18: MAXIMAL RETENTION TIME IN WLAN CELL WITH A CELL RADIUS OF 200 M. 89
TABLE 3.19: TODAY'S APPLICATION SERVICE AND NETWORK ACCESS PROVISIONING BEHAVIOUR AS WELL AS THE CUSTOMER CHARACTERISTICS. 94
TABLE 4.1: DETAILS ABOUT USE CASES, RELATED NETWORK CAPABILITIES AND OBJECTIVES. 107
TABLE 4.2: OBJECTIVE OF SEQUENTIAL AUTHENTICATION SOLUTION FROM USER PERSPECTIVE. 109
TABLE 4.3: OBJECTIVES OF SEQUENTIAL AUTHENTICATION SOLUTION FROM NETWORK OPERATOR PERSPECTIVE. 109
TABLE 4.4: GENERAL REQUIREMENTS ON SEQUENTIAL AUTHENTICATION SOLUTION. 110
TABLE 4.5: TECHNICAL REQUIREMENTS ON SEQUENTIAL AUTHENTICATION SOLUTION. 110
TABLE 4.6: OBJECTIVE OF BARCODE INITIATED HOTSPOT AUTO-LOGIN SOLUTION FROM USER PERSPECTIVE. 118
TABLE 4.7: OBJECTIVES OF BARCODE INITIATED HOTSPOT AUTO-LOGIN SOLUTION FROM NETWORK OPERATOR PERSPECTIVE. 119
TABLE 4.8: GENERAL REQUIREMENTS ON BARCODE INITIATED HOTSPOT AUTO-LOGIN SOLUTION. 120
TABLE 4.9: TECHNICAL REQUIREMENTS ON BARCODE INITIATED HOTSPOT AUTO-LOGIN SOLUTION. 120
TABLE 4.10: OBJECTIVE OF GRACEFUL DENIAL OF SERVICE SOLUTION FROM USER PERSPECTIVE. 137
TABLE 4.11: OBJECTIVES GRACEFUL DENIAL OF SERVICE SOLUTION FROM NETWORK OPERATOR PERSPECTIVE. 137
TABLE 4.12: GENERAL REQUIREMENTS ON GRACEFUL DENIAL OF SERVICE SOLUTION. 138
TABLE 4.13: TECHNICAL REQUIREMENTS ON GRACEFUL DENIAL OF SERVICE SOLUTION. 139
TABLE 5.1: TABLE RADCHECK OF MYSQL DATABASE. 163
TABLE 6.1: COMPARISON OF BARCODE INITIATED HOTSPOT AUTO-LOGIN SOLUTION WITH TRADITIONAL HOTSPOT VOUCHER SOLUTIONS. 192
TABLE 6.2: BENCHMARKING FROM USER POINT OF VIEW: TIME TO GET LOGGED IN TO THE HOTSPOT. 200
TABLE 6.3: COMMUNICATION BETWEEN USER DEVICE AND HOTSPOT CONTROLLER. 202
TABLE 6.4: COMMUNICATION BETWEEN HOTSPOT CONTROLLER AND HOTSPOT CORE ENTITY. 203
TABLE 6.5: BANDWIDTH DEMAND OF GDOS INTERFACES. 205

1 Introduction

In recent years the Internet became one of the most important environments for trading, the economy and a major social environment for many people all over the world. There are millions of services available on the Internet [4] and the number of these services increases constantly [5]. Besides well-known applications, such as the World Wide Web (www) or Internet messengers, new services that are traditionally not associated with the Internet protocol (IP) [6] networks have been adapted to be delivered via the Internet. For example, traditional telephony and television have become IP-based services called voice over IP (VoIP) [7] and IP television (IPTV) [8], [9]. VoIP and IPTV are interesting services for commercial telecommunication service and network providers to extend their service portfolio. The development of new services requires detailed market research to determine customers' desire for a new service. However, even if a new service meets the desired functionalities a successful penetration of the market cannot be guaranteed. The successful market penetration depends mostly on the customers' acceptance of the new service [10], [11]. A factor that affects the acceptance is the service quality provided. A precondition of acceptance, beside the usage costs, is service provisioning in customer satisfying quality. Customer satisfying quality is a subjective rating of the individual customer, but generally speaking a new service has to provide quality that is comparable with traditional services out of the same genre. This means, e.g. speech communication using technology VoIP has to provide comparable quality as traditional speech communication via a public switched telephone network (PSTN). As outlined in [12] the development of technical solutions for VoIP have allowed VoIP to become a serious alternative to traditional voice communications.

Similarly to the rise of new IP-based services, the technologies that enable network access and thus, Internet access to the services increase statically as well, e.g. long term evolution (LTE) [13], wireless local area network (WLAN) based on Institute of Electrical and Electronics Engineers (IEEE) 802.11n [14] and worldwide interoperability for microwave access (WiMAX) [15] based on IEEE 802.16-2009 [16]. A main objective of LTE, WLAN and WiMAX is to provide mobile and

wireless Internet access with broadband connectivity. In addition, WLAN and WiMAX are used to setup wireless mesh networks (WMNs) [17], [18].

Many network operators, such as Deutsche Telekom [19] and Vodafone [20] have been involved in developments and investigations of new technologies, such as LTE [21], to achieve significantly higher spectral efficiency for future mobile communication systems through the use of innovative methods and algorithms. Moreover, academia and industry work jointly on the scalable and converged multi-access operator's network (ScaleNet) [22], focusing on enabling both service and network convergence. The multi-play of services embraces voice and video telephony, mobile TV, massively multiplayer online gaming and Internet access. Network convergence is seen as the migration of heterogeneous physical and logical network elements of fixed and mobile networks into one single IP-based infrastructure. Another project focuses on broadband wireless Internet access in public transport [23] to enable vehicular-land connectivity, mobility, transport protocols, land infrastructure as well as authentication, authorisation and accounting (AAA) and security. The aim of the projects [21], [22] and [23] is to provide Internet access everywhere and thus, service connectivity even if users are on the move.

Besides providing Internet access everywhere by means of proprietary or standalone solutions, projects [21], [22] and [23] aim to develop carrier grade network architectures and carrier grade access networks. The bases of the investigations are the requirements on carrier grade networks that have to be fulfilled. These requirements are security functionalities that ensure customers' privacy, integrity, authenticity, non-repudiation of data as well as confidentiality of customer data. Network access control is required to carry out customer authentication, authorisation and accounting (AAA). Standardisation conformable network architectures that enable the integration into existing provider network architectures are required. Moreover, this will allow a future-proof design of network architectures and thus, the adaptability for future deployment scenarios. In this context network efficiency and applicability of the mechanisms used for customers and network architecture entities have to be discussed as well. Mobility support that enables broadband wireless Internet access while users are on the move as well as provisioning of services in moving vehicles and trains [24]. Support of triple play services in access networks to fulfil the quality of experience (QoE) of customers is

required as well. Triple play services are voice, video and data services. Customers' QoE can be fulfilled when new access network technologies, such as mobile, wireless or mesh networks are able to deliver triple play services in comparable quality to existing access networks. Moreover, quality of service (QoS) has to enable resource and admission control of network capacity to enable service provisioning in customer satisfying quality.

Over the past few years the consumer behaviour has changed significantly. In the past most customers got Internet access at home or at the office while today more and more customers aim for Internet access en route. As a result, wireless and mobile access networks became very important in providing Internet access. "The number of mobile-only Internet users will grow 25-fold between 2010 and 2015, reaching 788 million mobile-only Internet users" was stated in Cisco forecast [25]. A continuing trend is forecasted in [26]. The still continuing evolution of mobile networks, such as LTE [21], enables Internet access of customers en route as well as while customers are on the move. Especially, wireless local area networks have reached the mass market. Users choose WLANs at home, business or en route to obtain a comfortable Internet connectivity. Today nearly every notebook is equipped with a WLAN interface. Moreover, the number of mobile phones that are supplied with WLAN technology is growing rapidly as well. Furthermore, enterprises, cities and social businesses, such as restaurants or cafes have started to deploy WLAN areas to provide flexible Internet access. These public WLAN based access networks, so called hotspots, enable Internet access en route as well. The amount of public hotspots is still increasing as does their popularity because hotspots enable broadband Internet access when compared to mobile networks. Furthermore, hotspots are interesting for network operators as they are able to generate additional revenue and customers' loyalty. For instance Deutsche Telekom [27] and Kabel Deutschland [28] have hotspots within their product portfolio and offer thousands of hotspot locations [27] all over Germany.

In the context of broadband wireless Internet access the WLAN based WMNs become more and more popular. Examples for large deployed WMNs are MITs Roofnet [29] or the Freifunk in Berlin [30] that have grown to a size of up to 200 access points and are still continuing to increase. The benefit of WMNs is that it is able to cover a large area with WLAN connectivity while requiring only a single

gateway to the Internet. This means WMNs are a cost efficient solution to setup up a large wireless covered access network. The large coverage is achieved due to multi-hop communication among the mesh nodes involved in the WMN that enable data forwarding to the Internet gateway. The cost efficiency and the ability to extend the coverage of a WLAN based access networks makes these WMNs also interesting for network operators. British Telecommunications and Deutsche Telekom for instance are involved within the European Commission project CARrier grade MEsh Networks (Carmen) [17]. However, WMNs have to fulfil the requirements of carrier grade access networks [31] before network operators will integrate WMNs into their network infrastructures. If in future WMNs are able to deliver services in customers satisfying quality, then WMNs can provide the advantage of ubiquitous network access and services for customers. This will in turn provide new revenue opportunities for operators, e.g. voice over WLAN services at home or at enterprise locations. Moreover, cost efficient hotspot extensions based on WMNs are also possible.

Beside broadband Internet access everywhere service provisioning in customer satisfying quality is an important issue for current and future network operators. In general the number of calls supported and the quality of the calls via an access network is important for network operators. Bad voice quality of VoIP will not satisfy customers' expectancy as users are used to a traditional voice service, such as telephony in integrated services digital network (ISDN) [32] or PSTN. This means, the QoE compared to traditional telephony would not be achieved by a VoIP service. As a result, the acceptance of VoIP services by the customers decreases. For this reason network operators aim for VoIP quality that is comparable with traditional telephony.

The investigation of QoE has gained a lot of attention in recent time [33]. The understanding what influences the QoE and which parameters are important for application and network service providers when developing new services as well as novel network architectures is increasingly investigated. For instance in [34] the impact of different network settings on the end users QoE while web surfing or file downloads is investigated. The QoE based on varying network parameters and user behaviour is assessed in [35]. Investigation of acceptability and QoE of mobile broadband data services are performed in [36]. Different topics towards improving

QoE for network services are discussed in [37]. Furthermore, QoE issues on media delivery are presented in [38]. While, the ITU-T study group 12 [39] investigates QoS and QoE.

Each service area requires specific network performance to provide the service in customer satisfying quality and thus, to fulfil the customers' QoE for the requested service. For instance, real-time services, such as VoIP require network performance with low delay, jitter and packet-loss in data communication. However, the integration of state-of-the-art network access control or security mechanisms to setup carrier grade WLAN access networks influences the network performance. Especially, when customers are on the move and handovers occur in the WLAN access network the applied access control and security mechanisms influence the handover and thus, the network performance. During a handover process the user equipment (UE) exchanges the point of attachment (PoA). This means the network connectivity is interrupted, as is the data communication. Access control and security mechanisms have a direct influence on the duration of the connectivity interruption. As a result, the deployed access control and security mechanisms influence the network performance and thus, the provided service quality as well. New access networks have to provide traditional services, such as telephony, in customer satisfying quality as existing network infrastructures. This means the performance of access networks is measurable by means of the capability to deliver carrier grade services that is affected by access control and security mechanisms.

Beside the ambition of network operators to provide broadband Internet access as well as services in QoE fulfilling performance to customers the cost aspect for the deployment and operation is very important for network operators. With the aim to develop efficient and competitive network architectures network operators spend a lot of effort in the area of fixed mobile convergence (FMC) in recent time [22]. The vision of convergence is to decouple the network infrastructure from the applications. In [40] "the term "convergence" represents the shift from the traditional "vertical silos" architecture, i.e. a situation in which different services were provided through separate networks (mobile, fixed, CATV, IP), to a situation in which communication services will be accessed and used seamlessly across different networks and provided over multiple platforms, in an interactive way". FMC can be seen as an evolutional process towards the next generation network (NGN)

framework defined by the ITU-T [41]. The term NGN is defined in [ibid] as "A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users". In [42] the ITU-T state that "for NGN it is considered that IP may be the preferred protocol used to provide NGN services as well as supporting legacy services". The expected result from the network evolution towards NGN is a common infrastructure with a common network management and control platform. Consequently, the 'vertical silo' application areas, e.g. the plain old telephone service (POTS) and circuit switched telephony will be migrated to a packet based and layer based network infrastructure. A widespread discussed control framework for the common infrastructure by network operators is the IP multimedia subsystem (IMS) [43], [44]. In [45] the benefit of IMS for operators is described, such as IMS "provides the basis for a horizontal architecture, thereby taking the concept of layered architecture a step forward. This enables reuse of service enablers and common functions for offering multiple applications". In [46] IMS is described as an enabler for "eliminating the costly and complex traditional network structure of overlapping functionality for charging, presence, group and list management, routing and provisioning. Network operators expects from the envisioned NGN common infrastructure". Beside the aspect of cost reduction network operators aim to deliver network services and application services in an efficient and flexible manner to customers. Moreover, network operators aspire to integrate new services in a fast and efficient way. As stated in [47] "the migration from separate network infrastructures to next generation core networks is a logical evolution, allowing operators to open up the development of new offers of innovative content and interactive, integrated services, with the objective to retain the user base, attract new users, and increase average revenue per user (ARPU)". The potential of NGN for operators is confirmed by [40] with the statements, such as NGN promises "the simplicity and flexibility to add/maintain/remove service, application, content and information" and "the easy creation of advanced service/application/content/information". As a result, the process towards NGN and

FMC respectively should provide the base for operators “to be more than bit pipes” [48].

In the following the enhancement of the QoE for customers is focused on from the network provider point of view. The enhancements are analysed in three different areas, such as network performance in WLAN, network access in WLAN and network features. The first area of enhancement focuses on customer satisfying VoIP service provisioning while customers are on the move in WLAN or WLAN based WMNs. The introduced network access control concept enables carrier grade real-time service provisioning even when customers are on the move. The access control concept improves the existing limitations in the authentication and confidentiality establishment process that is responsible for increased handover latency. By means of this concept service provisioning in user satisfying quality is achieved even in the case of frequently performed handovers. Moreover, the concept considers state-of-the-art security mechanisms to fulfil the requirements on carrier grade access networks. The second area of enhancement focuses on the usability to easily obtain the users credentials, such as user name and password for public WLAN access networks and to perform automated hotspot login. For that purpose a barcode initiated voucher and auto-login solution is introduced that provides hotspot login in a user-friendly way. The third area of enhancement focuses on improved QoE while service provisioning. The developed mechanism provides feedback to the customer that informs him whether the selected service is providable in the customer requested quality. This mechanism can be used to provide an engaged signal for IP-based services. Moreover, the mechanism can be applied as a service quality indicator.

1.1 Motivation

The motivation of this work is to enhance the quality of experience of customer when they connect to the Internet, request application services in the Internet as well as when customers are on the move while service use. The enhancements are based on enriched network centric and access control mechanisms and are achieved in three different areas, namely the network performance in WLAN, the network access in WLAN and improved network features. In Figure 1.1 these areas of improvement are shown. The improvements are carried out from the network operator’s point of view and show how network operators can enhance the QoE of their customers.

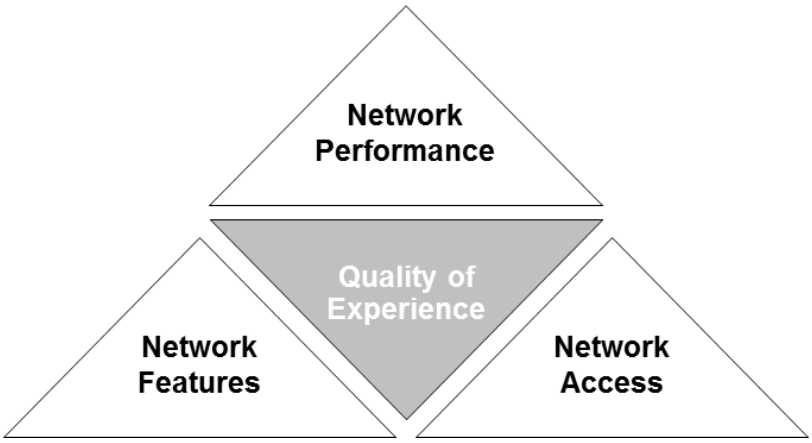


Figure 1.1: Quality of experiences – areas of improvements.

In more detail the area of network performance focuses on improvements of the authentication and authorisation process in WLAN handovers. The area network features introduces a value added functionality that informs customers about the expectable service quality provided. A user-friendly process obtaining hotspot login credentials and performing hotspot auto-login is presented in the area of network access. In the following the three different areas are introduced.

1.1.1 Improved Network Performance to Enhance QoE

The first area addressed in this work is to enhance the QoE based on improved network performance to provide real-time services even when users are one the move within WLANs. In the early stages of WLAN deployment the user movement pattern was nomadic. Users stayed at a single location to get wireless Internet access without changing the access point (AP). The users most often changed their location after they have disconnected from the Internet. This means throughout the whole Internet session the user equipment was connected to a single access point only. However, this behaviour changed within recent time. Today's trend is to provide Internet access and thus, service provisioning while users are on the move [49], [50]. This means the UE has to change the access point several times during an established Internet and service session. Due to the mobility aspect a variety of factors, such as handover and velocity arise that effects the performance of data connection.

From the business point of view service provisioning in a user mobility scenario enables new business scenarios, such as VoIP over WLAN. In general VoIP has gained significant attention from telecommunication network and service providers. The goal of the providers is to offer the voice service in a more cost efficient and

controllable way based on the IP. VoIP is used in a variety of markets. Large companies use VoIP for company internal communications and private persons use VoIP services, such as Skype [51], for free worldwide telephony. Now the combination of VoIP and WLAN initiates new business possibilities for mobile phone vendors, e.g. Apple iPhone [52] and service providers, e.g. Google hangouts [53]. By means of VoIP over WLAN it is possible to provide mobile phone like service to customers at the cost of a VoIP call. However, before VoIP over WLAN will reach the mass market the speech quality has to fulfil the QoE of a traditional voice service. A technical challenge to reach this goal is to reduce the service interruptions arising from e.g. the WLAN handover process of the user device when users are on the move.

In general real-time services suffer from network performance influences, e.g. delay, jitter and packet-loss. The VoIP service quality mainly depends on the parameters delay, jitter and packet-loss of VoIP packets as well. The general relation of the delay chain in a speech communication path and its influence on data loss are described in [54]. The network capability and their parameters delay, jitter and packet-loss are influenced by different network access conditions. In the case of fixed network access, such as digital subscriber line (DSL), delay, jitter or packet-loss arises mainly from network overload. In the case of wireless networks, such as WLAN, additional delay, jitter or packet-loss occurs moreover due to the use of a shared medium that is influenced by factors such as interference, propagation and shadowing. An additional factor that influences the network performance is the handover process when customers are on the move and the device changes the WLAN AP. A large covered wireless access network consists of multiple WLAN APs. Due to the fact that the coverage of a single AP is limited the device handovers among surrounded APs to keep IP connectivity to the network. The influence on the handover time performance depends on the wireless cards used, as is presented in [55]. In addition to the handover time caused by different wireless cards [56] shows the influence on handover time performance when the same wireless card communicates with access points made by different vendors.

Mobility in wireless networks induces changes of PoAs. The handover process that carries out the exchange from one PoA to another PoA consists of different phases according to the IEEE 802.11 standard. First, the search phase looks for

surrounding PoAs. Secondly, the configuration phase that reconfigures the WLAN card to connect to a new PoA. Thirdly, the authentication phase carries out network access control. These three phases lead to data communication interruption. This means no IP connectivity to the Internet and to the services is established during the handover process. In other words, the service is interrupted and thus, the service quality is affected.

The three phases within the handover process consists of the sending of probe messages, to scan for new APs, authentication and re-association messages that lead to data transmission delay and packet-loss, as investigated in [57]. The authors of [56] examine in detail the influence of the handover process components, such as probe delay, authentication delay and re-association delay, concluding that the probe delay is the significant part of the handover delay with up to several hundred milliseconds. However, the reduction of the probe delay is possible by means of handover triggers controlled by e.g. location based information. Consequently, the scanning process can be avoided but the authentication and re-association delay still remains. Furthermore, [ibid] observes only the two authentication types: open system and shared key specified in the IEEE 802.11 [58] standard. Investigations in [55] show that the open system authentication impacts on the handover time in a lowly dimension of 1 ms. However, there are more complex authentication mechanisms, e.g. IEEE 802.1X [59] uses the extensible authentication protocol (EAP) [60] – transport layer security (TLS) [61], that require the authentication and authorisation data exchange with external authentication, authorisation and accounting (AAA) servers. The authors of [62] describe that the integration of security mechanisms within network architectures causes time and resource consumption, which poses a problem if delay critical applications, such as VoIP, are to be provided to a user satisfying quality.

A technical challenge is to reduce the service interruption which arises from the handover process comprising of a time consuming network access control and the networks security mechanisms. The ITU-T describes in [63] that most applications, both speech and non-speech, will not be significantly affected by delays below 150 ms. However, this work will exhibit that the handover delay can exceed the recommended 150 ms. This finding is confirmed in studies [56] and [55]. Beside the authentication and authorisation time in a single handover process the frequency at

which a handover process occurs while customers are on the move influences the parameters delay, jitter and packet-loss. Due to the limited WLAN coverage of an access point the end device handovers several times during a voice session. The effect on voice quality is described in this work as well. The frequency of handovers depends on user's velocity and the size of WLAN cell area. Investigations in [64] show that voice communication interruptions greater than 40 ms in conjunction with interruption intervals less than 11,7 s leads to voice quality that is not sufficient to provide carrier grade voice quality. Investigations in [64] are based on the specification of the perceptual evaluation of speech quality (PESQ) value as defined by ITU-T G P.862 [65]. Therefore, a novel network access control mechanisms providing reduced data connectivity interruptions in handover processes of secured WLANs is needed.

In the area of improved network performance, this work introduces a novel network access control mechanism that reduces the authentication phase in the WLAN handover process significantly while applying EAP-TLS. As a result, the handover time is reduced and thus, the time of communication interruption as well. Based on this mechanism real-time services can be provided in customer satisfying quality even when customers are on the move. From the network access point of view the mechanism supports carrier grade real-time services provisioning via WLANs and WLAN based wireless mesh networks [66], [67]. The performance of the improved handover process is measured on the ability of carrier grade VoIP service provisioning.

1.1.2 Improved Network Access to Enhance QoE

The second area addressed in this work to enhance the QoE is based on improved network access in hotspots to attract hotspot use for customers. Public wireless local area network zones called hotspots offer paid Internet access in restaurants, cafés, stations, airports, hotels, campsites or within public transportations, such as high speed trains. There are two types of payment possible in hotspots, such as post-paid and prepaid. In the post-paid solution the customer pays the hotspot use according to the consumed login time. While, in the prepaid solution the customer pays the duration of hotspot use in advance. Hotels often use post-paid hotspot solutions. In post-paid solutions the billing of the Internet access is added to the overall hotel bill

or is cleared by means of Internet service providers, e.g. Telekom [27] or Kabel Deutschland [28] that provide the WLAN infrastructure. Another possibility to carry out billing of hotspots use e.g. in restaurants, cafés or campsites is by means of the prepaid solution. As confirmation of the advance payment the customer receives voucher containing the information about duration of hotspot use as well as the login name and login password.

In the prepaid hotspot solution the customer buys a certain duration of time to get access to the hotspot. There are two methods of accounting in the prepaid solution, such as used-time and passed-time. In the used-time method the consumed hotspot login time is accounted. The difference between the bought duration of time and the consumed time remains for further hotspot use. The point of time of further hotspot use is arbitrary for the customer. In the passed-time method the hotspot login marks the starting point of hotspot use. The final point of hotspot use is the starting point plus the bought time of hotspot use. Within the range of starting and final point the customer is able to logout and login to the hotspot but further use is not possible beyond that final point.

The initial step to obtain access to a hotspot is the receipt of the login information, such as user name and user password. Some prepaid and post-paid solutions provide the login information after payment by means of a credit card. But not each hotspot is trustworthy to carry out a credit card payment. Some other post-paid solutions in hotels offer the login information on the TV screen after confirming the charging the hotspot use to the overall hotel bill [68]. In most prepaid solutions as well as most post-paid solutions it is necessary to contact hotspot personal to obtain the login information. For instance the customer buys in the prepaid solution a voucher at the reception desk, of campsites, hotels or from the waiter in cafés or restaurants. This means the customer always has to plan the hotspot use in advance. Moreover, the customer has to leave his accommodation facility, such as hotel room or mobile home, to obtain the hotspot login information from the hotspot personal. Consequently, no spontaneous hotspot use is possible unless a hotspot flat rate has been booked at a high fee. Furthermore, this is not comfortable for the customer and due to this the customer might decide not to use the hotspot. The residence time staying in the hotspot has to be scheduled in advance. This effort to think about the time of hotspot use and the duration of hotspot use in advance is another issue that

influences the acceptance of hotspot usage in general. In the case when users are able to decide about the point of time and duration of hotspot use on demand a user would more often decide to use the hotspot to get Internet access. This effect would be intensified when the user gets the login data in a user-friendly and comfortable way as well as being logged in to the hotspot automatically. At this point the utilisation of a barcode will help to enable a user-friendly and comfortable way to obtain the hotspot login data. Moreover, the login process is automated without the need of the user to enter a user name and password.

The novel introduced barcode initiated voucher and auto-login concept is in the area of network access focusing on user-friendly hotspot access. The barcode initiated voucher and auto-login will be shown to be beneficial for hotspots due to the fact that the user-friendly use will decrease the inhibition threshold to use it. This means the attractiveness of hotspots is enhanced. As a result, the business aspects of hotspot provision can also be improved.

1.1.3 Improved Network Features to Enhance QoE

The third novel enhancement of the QoE will be in the area of improved network features. The results will support network operators “to be more than bit pipes” [48]. The state-of-the-art of today’s service provisioning is that the user requests an IP-based service, e.g. video service from a content provider such as YouTube [69]. The hosted video server of the content provider starts video streaming without any knowledge whether the network capabilities are sufficient to deliver the service in user satisfying quality. At this point the user is in pleasant anticipation to receive the video in good quality. However, in certain cases, such as during peak usage hours the application servers or the network might be overloaded. Overload in networks might occur on the content provider or the customer network access side due to limited network resources. As a result, the overload situation leads to degraded service quality [70], [71], [72]. For instance, the video starts playing, however, due to limited available network resources the video might stop several time for data buffering. Moreover, it is also possible that artefacts appear in the video due to lost data packets.

A mechanism that provides a feedback to the user whether the service is providable in the requested service quality would be very beneficial for the user. For

instance, a feedback mechanism is used in traditional telephony by means of the engaged tone. The engaged tone is given to the caller if the telephone line is already in use by another caller of the same telephone line or if the callee is already in a call. Such a mechanism for the IP world would overcome the circumstance that the user is no longer left in the dark about the requested and delivered service quality.

In the area of improved network features the new feedback method will show how a network provider can improve and enhance the customer experience during the service request phase using network centric added value services. The introduced feedback mechanism informs customers whether the requested service is providable in the requested quality. For instance, this mechanism can be used to provide an engaged signal for IP services comparable to the traditional telephone service. The added value service is based on network performance information provided by the access network operator, the application service requirements provided by the content provider and on the user profile information.

1.2 Related Work

This section gives an overview about related work to improve network performance in WLANs, network access in WLAN as well as network features. Network performance enhancements are presented in Subsection 1.2.1 focusing on handover process improvements in WLAN. In Subsection 1.2.2 enhancements of network access in public WLANs, such as hotspots are discussed. In Subsection 1.2.3 network feature improvements are described.

1.2.1 Improvements of Handover Process in WLAN

Several approaches have been suggested to enhance the handover performance in secured WLANs. This section gives an overview of related work focusing on the authentication time reduction or authentication mechanism improvements in handover processes. The overview consists of mechanisms specified by standardisation bodies as well as approaches to enhance existing standardized or proprietary mechanisms.

In [73] a reduction of handover time of 90% is presented. The approach consists of a neighbour graph (NG) concept that describes the nearby access points of a mobile node (MN). If the received signal strength indication (RSSI) level falls below a defined threshold the MN notifies the AP to carry out data buffering based on the

presented frame forwarding-and-buffering mechanism. Moreover, the MN carries out a selective scan of APs based on the information of the surrounded APs. Due to known APs the probe delay can be reduced. After the scan process the MN enters the active mode and initializes the inter access point protocol (IAPP) to execute authentication and transfer of credentials to the candidate AP before the handover is performed. Due to the proposed pre-registration mechanism for IAPP the IAPP delay can be avoided. If now the RSSI level falls below the handover level the handover process will be carried out without execution of the whole IAPP. Due to the frame forwarding-and-buffering mechanism the MN data of the old AP will be forwarded to the new AP. Thus, the packet loss problem during the handover is solved and seamless service provision can be provided.

The approach presented in [ibid] leads to reduced handover time. However, the concept requires additional software elements, such as the NG client and the NG server to exchange neighbour information among MN and NG server. Due to this an easy integration into existing network architectures is laborious. The IAPP data exchange evoke additional network load, especially if a lot of MNs carry out handovers in a network due to customers mobility. When the RSSI handover trigger level is reached before the pre-registration of IAPP is finished the traditional IAPP registration delay appears again and increases the overall handover delay. With regard to high appearance of MN mobility the buffered data forwarding from the old AP to the new AP increases the network load as well. Furthermore, the concept is not able to reduce the influence of IEEE 802.1X authentication time when using EAP TLS.

The IEEE 802.11i standard [74] published in 2004 describes a concept that separates the user authentication process from the data protection process. The goal of IEEE 802.11i is to build a robust secure network (RSN). The security framework ensures a strong protection of wireless communication within a RSN association (RSNA). Two protocols are described for data confidentiality, the temporal key integrity protocol (TKIP) and the counter-mode/CBC-MAC protocol (CCMP) [75]. The RSNA establishment procedure includes the 802.1X [59] authentication method and key management protocols. IEEE 802.1X provides port-based access control on layer 2 for RSN-enabled network entities. Moreover, IEEE 802.1X allows the integration of several authentication protocols, such as EAP-TLS [61] or Kerberos.

EAP-TLS enables mutual authentication of device and authentication server. The German Federal Office for Information Security (BSI) advises in [76] to employ IEEE 802.11i/WPA2 in WLANs to achieve a secure wireless network.
The authors in [62] provide measurement and analysis of handover latencies in IEEE 802.11i secured networks. It is shown that the use of IEEE 802.1x with EAP-TLS takes up to several hundred milliseconds to carry out mutual authentication, which poses a problem if delay critical applications, such as VoIP, should be provided in user satisfying quality. Moreover, the high device and implementation dependent authentication latency is shown.

Beside the design of a robust secure network IEEE 802.11i [74] provides a pre-authentication method based on IEEE 802.1X with a key caching solution. On the one hand the derived key is cached within the authenticator on the access point to provide fast re-authentication in the case of device reconnection to old access point. On the other hand the derived key is distributed among the access points. The distributed key enables the station to handover to a new access point that has not been visited before and re-uses the key established with the previous access point. This lets the station quickly handover to never authenticated APs, without the necessity to perform an authentication. In [62], [77] the benefit of the pre-authentication method is presented. Due to the pre-authentication method the delay of several hundred milliseconds during the mutual authentication phase can be avoided.
The pre-authentication method is beneficial when all points of attachments are located in the same administrated domain [78], but IEEE 802.11i cannot provide layer 2 pre-authentication during inter-domain mobility. This behaviour can lead to impairments on applicability of the mechanism in inter-provider scenarios due to the required link layer connectivity. Moreover, the network load increases due to the pre-authentication process even in the case that no handover will be performed.

The IEEE 802.11 standard does not specify the communications between access points to support users roaming from one access point to another. To overcome this drawback and thus, to reduce the re-association delay in a handover process the inter access point protocol (IAPP) is specified as IEEE 802.11f [79]. IAPP describes messages and data to be exchanged between the APs to enable enhanced re-association. Based on IAPP the new AP has to verify that the station was connected

to the previous AP. The interaction between the AP is carried via the wired backbone network. The transmission control protocol (TCP) is used for AP communication and the user datagram protocol (UDP) for remote authentication dial-in user service (RADIUS) [80].

The IAPP specifies six new packets needed to carry out the credential exchange among the old access point and the candidate access point. In general the IAPP enables a reduced handover delay. However, the additional handshakes to exchange the credentials lead to increased network load within the backbone, especially in the case of high device mobility in the access network. In the following the drawback of the above presented research work is summarised:

- Improvement of handover mechanisms and protocols leads to a reduction of authentication and re-association time. However, some handover time remains that still influences the network performance and thus, the service quality.
- Authentication and re-association time depends on used security mechanism. Handover time could be improved due to the integration of lower security level within the network architecture.
- Non state-of-the-art protocols are proposed that are incompatible with today's network architectures and are thus, not applicable in real scenarios, such as carrier grade access networks.
- Handover concept should be compatible with today hardware and state-of-the-art mechanisms.

The research idea presented in this work supports seamless real-time services provisioning when users are on the move in WLANs. Thus, the functionality contributes to enable triple play service support in WLAN based carrier grade access networks. The novel authentication concept is a generic mechanism and in general applicable for other access technologies as well enabling network access authentication and authorisation for time-critical applications.

1.2.2 Network Access in WLAN Hotspots

Today a lot of commercial and open source solution for WLAN-based hotspots exist. Some solutions are deployed and managed by operators, such as [27] and [28]. Other solutions are offered by IT equipment vendors, such as Cisco [81] or Mikrotik [82]. Moreover, there are hotspot solutions offered by hotspot providers, such as XCony

[83]. Furthermore, open source solutions exist to setup hotspots, such as Chillispot [84] and its successor CoovaChilli [85].

The benefit of centralised customer data management is that it enables customers to use hotspots at different locations with a single user account. As a result the account management effort for customers is reduced. This motivates customers to use hotspot based Internet access at different locations without the need to obtain new login data for another hotspot managed by another owner. However, centralised solutions, such as [27] and [28] are not as widely deployed to provide Internet access via an area-wide covered WLAN hotspot. This means a mix of different hotspot solutions still exists and will most likely increase in the future. A challenge will be to motivate customers to use hotspots, even if the hotspots are managed by different owners and thus, the user has no user credentials to log in to the hotspot. One aspect is the reduction of hotspot fees. Another aspect that enhances the attractiveness of hotspots can be achieved by user-friendliness.

The above mentioned hotspot solutions provide functionalities to enable public or private WLAN based Internet access. However, the following aspects can be improved when focusing on usability and user-friendliness of hotspots:

- None of the approaches provide the login information, such as user name and user password without communicating with the hotspot personal or without an indirect way, e.g. via a TV screen interface or a web-portal.
- Some solutions require the user to enter credit card credentials.
- The user identification is not realised by means of the users' mobile phone number.
- No auto-login mechanism is available which avoids entering of user name and password on the hotspot landing page.

The novel research idea in the area of network access is to introduce a barcode initiated voucher and auto-login solution for WLAN hotspots which provide hotspot user credentials and perform hotspot login in a user-friendly way. It is assumed that the barcode initiated voucher and auto-login is beneficial for hotspots because the user-friendly use will decrease the inhibition threshold of choosing hotspots. This means the attractiveness of hotspots is enhanced.

1.2.3 Network Features which Improve Application Service Delivery

Application service delivery is provided from the content provider to the user via the Internet. However, there are several issues that affect the quality of application service delivery. For instance during peak hours the application servers or the networks might be overloaded. Overload in networks can occur also on content provider or customer network access side due to consumed network resources. As a result, the overload situation leads to degraded application service quality [70], [71], [72].

A solution to avoid network capacity bottlenecks at the content provider side or at network provider peering points is the deployment of content delivery networks (CDN) [86]. A CDN is a network consisting of locally distributed and via the Internet connected servers. The CDN servers can be located in different provider backbones. The aim of CDNs is to deliver content requested by the user in an economical way. Especially large media or software files are distributed by CDNs. CDNs cache the data to distribute the content fast as possible or with little bandwidth. CDN providers are for example Akamai Technologies [87] and Edgecast [88].

Other approaches aim to avoid network congestion and to improve network capabilities based on e.g. route selection, load balancing or packet shaping. For instance, in [89] a mechanism for dynamic channel bundling in 802.11a based media-transport mesh networks is described as “The proposed multi-layer approach combines dynamic channel distribution with additional dynamic interface bundling for multi-interface mesh networks used for media transport. This novel distributed channel utilization scheme aims for a better support of QoS-related traffic as well as traffic on prioritized (gateway) routes in such networks”. A traffic shaping algorithm based on neural networks is described in [70] to avoid network congestion for improved streaming video quality at clients. “The purpose of this intelligent shaper being to eradicate all traffic congestion and improve the end-user’s video quality. It possesses the capability to predict, to a very high level of accuracy, a state of congestion based upon the training data collected about the network’s behaviour” [ibid].

A non-network mechanism related possibility to improve delivered service quality is the ability to adjust the multimedia session by means of the multimedia player software [90]. If the provided video quality is affected by artefacts or freezing effects due to less network resources the user is able to change the video configuration in the player software. For instance, the video codec or the video resolution can be adjusted. The selection of another video codec or resolution can reduce the required bandwidth demand of the video in a way that the network capability is sufficient enough to deliver the video without artefacts or freezing effects to the user.

This research work is well defined and suitable to enhance network performance and efficiency which in turn leads to improved service quality delivered. However, the following drawbacks of the above presented research work and solutions exist when focusing on information about expected and delivered application service quality:

- None of the approaches provide feedback to the customer whether the application service is providable in the requested service quality or not.
- The CDNs are not aware of the access or home network capabilities of the user.
- The network mechanisms are not aware of application service requirements, e.g. needed bandwidth of a video stream.
- Media players are not aware of the network capabilities of, e.g. the content provider access network, the transport network, the user access network as well as the user home network.
- The end to end service delivery aspect involving multiple and interconnected network providers or operator domains in the service delivery chain is not considered.

The research idea in the area of network features is a mechanism that provides feedback to the user whether the application service is providable in the requested service quality. Therefore, the in this thesis presented feedback solution will offer several choices to the user on how to consume the requested services. As a result, this mechanism would overcome the circumstance in the IP world that the user is no longer left in the dark about the awaited and delivered service quality.

1.3 Thesis Overview

The remainder of this thesis describes a network centric mechanism to enhance the quality of experience of customers. The enhancements are achieved in three different areas, the network access control, the service provisioning and the usability to obtain network access in WLAN based hotspots. Chapter 2 gives an introduction into the general background of next generation networks, quality of experience, authentication and authorisation architecture, usability as well as creation of revenue by network operators. The challenges in real-time communication and user satisfied service provisioning are described in Chapter 3. In Chapter 4 three new solutions to enhance the area network access control, usability and service provisioning is presented. First, the proposed sequential authentication solution to reduce the data communication interruption time in WLAN handovers is presented. Second, the barcode initiated hotspot auto-login solution to enable the request of hotspot user credentials on demand and to perform an automated hotspot login process is given. Third, the graceful denial of service solution to offer an engaged signal for IP-based application services is derived. In Chapter 5 the proof of concept implementations of the proposed solutions of Chapter 4 are described. The results of this work are presented in Chapter 6 while Chapter 7 presents the conclusions of this work.

2 General Background

Most of today's customers expect broadband Internet connectivity and Internet access everywhere as well as service provisioning in good quality. These customer demands build high pressure on service and network providers to fulfil the expectations of their customers. Beside the demand to deliver services in user satisfying quality network providers have to survive in the market. In the following fundamental issues from a technical, a network providers and a users point of view are presented.

The development of the next generation network architecture is foreseen by network operators to overcome the challenges of today's service provisioning and thus, to fulfil the customers demand on the expected service quality. Moreover, the next generation network architecture will be used to build the base for future service creation. Section 2.1 presents the next generation network architecture and its interfaces to applications, service providers, end users and other networks described by the ITU-T.

The application service quality depends on the human sensation. The dimension how the network performance influences the service quality and how this influence affects the perceived service quality have to be determined for each service separately. In Section 2.2 the relation between quality of service (QoS) and quality of experience (QoE) in a communication ecosystem is described. The base for further network access control considerations is provided by introducing the terms authentication, authorisation and accounting in Section 2.3. Moreover, a basic authentication, authorisation and accounting architecture is described.

Beside the pure functionality of a mechanism or a product, the applicability for users has to be kept in mind. For this reason the usability aspect as an important issue for today's and future service acceptance and is introduced in Section 2.4. In addition to the usability aspect, the revenue aspect for the network provider is important and is therefore, addressed in Section 2.5.

The improvements of this work will be in the fundamental areas of next generation network architecture, QoS and QoE in a communication ecosystem,

authentication, authorisation and accounting. Further areas of improvements are usability and creation of revenue. The limitations and existing challenges in a service provision chain are discussed later on in the context of network access control and network centric functionalities. The assumption is that a novel network access control concept can overcome the existing drawbacks in a handover process. Network centric functionalities could be used to generate added value services and thus, to create revenue for network providers. The information available only to network providers, such as information about network resources and location can be used to generate those added value services. In addition the usability of services and products can be improved to increase the attractiveness or to enhance the user-friendliness.

2.1 Next Generation Networks

The ITU-T provides in ITU-T recommendation Y.2001 [41] the general overview of NGN and describes in ITU-T recommendation Y.2012 [91] the functional requirements and architecture of next generation networks. The functional requirements and architecture description is a reference guideline for network providers to develop their network architectures. It is assumed that network and application services can be realised in an easier and efficient way if network architectures are implemented based on these recommendations [40]. Moreover, it is assumed that network inter-connections of different network operators are realisable in an efficient manner based on the NGN recommendations rather than if each network operator uses its own proprietary implementations. Figure 2.1 presents the NGN architecture overview.

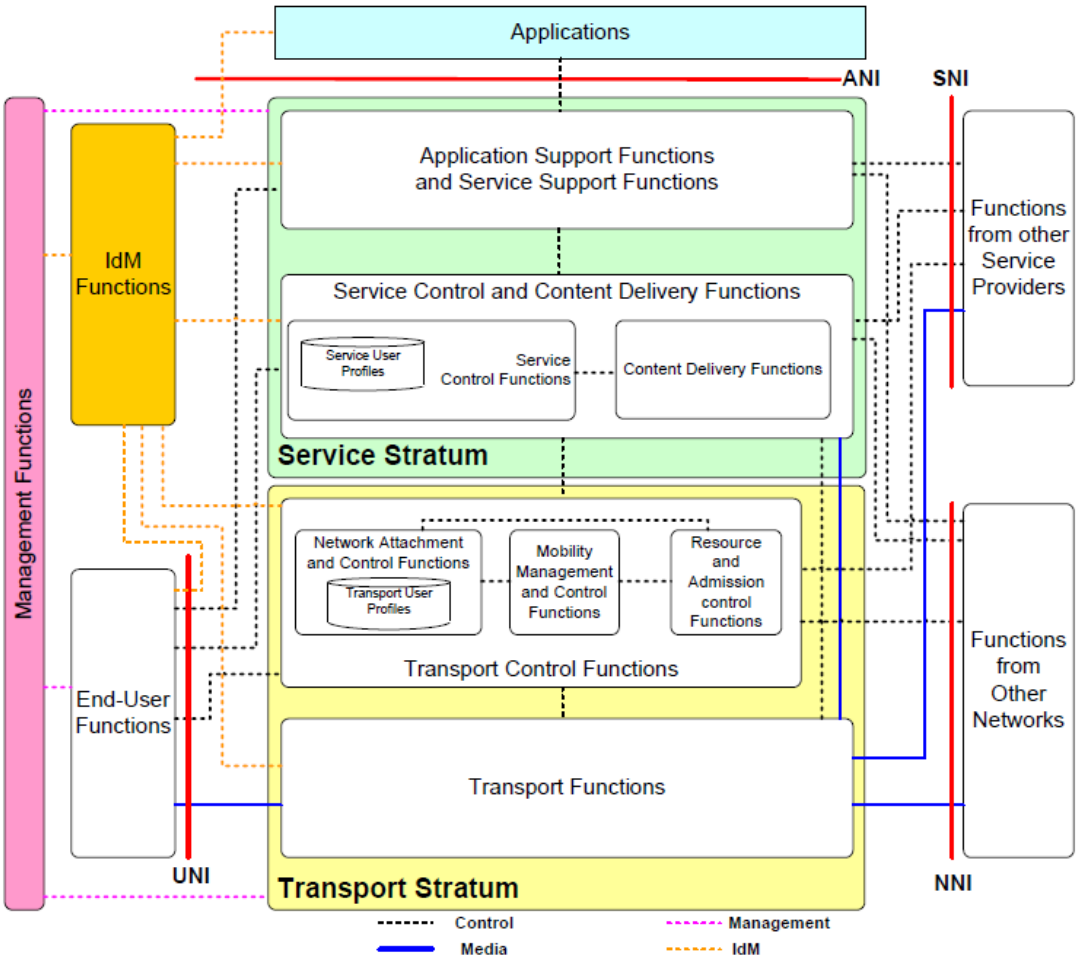


Figure 2.1: ITU-T NGN architecture overview (source: [91]).

According to ITU-T Y.2011 the NGN functions are divided into service stratum functions and transport stratum functions. As illustrated in Figure 2.1 several functions in both the service stratum and the transport stratum are needed. The delivery of services and applications to the end-user is provided by utilizing the application support functions and service support functions as well as the related control functions within the service stratum. The transport stratum provides the IP connectivity services to the NGN users under the control of transport control functions, including the network attachment control functions (NACF), the resource and admission control functions (RACF) and mobility management and control functions (MMCF).

As shown in Figure 2.1 the NGN functional architecture supports several reference points to provide connectivity to the NGN. ITU-T Y.2012 describes a reference point as “A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing

between these functional entities." and notes "A reference point may correspond to one or more physical interfaces between pieces of equipment". The user-network interface (UNI) is used to establish connectivity to the terminal equipment, user networks and corporate networks. The network-network interface (NNI) provides connectivity to other NGNs, other IP-based networks and PSTN/ISDN. Interactions and exchanges between a NGN and applications are enabled by the application network interface (ANI). ITU-T Y.2012 describes "The ANI offers capabilities and resources needed for realization of applications. The ANI supports only a control plane level type of interaction without involving media level (or data plane) interaction. The ANI is used to provide connectivity to other service providers, and their applications". The service network interface (SNI) is an interface to interact and exchange information between a NGN and other service providers, e.g. a content provider. The SNI supports both a control plane level type of interaction and a media level (or data plane) type of interaction. A control plane level type of interaction and a media level (or data plane) type of interaction is supported by the SNI.

To achieve the envisioned capabilities of the NGN framework network operators have to develop strategies to implement functionalities that enable a NGN conforming network infrastructure. A challenge for a network provider will be to which degree their network architecture is NGN conforming. A focus must be on the reference points SNI, NNI and UNI. Even if network internal functionalities are implemented in a proprietary way the standardised reference points will be beneficial for network and application service creation in the future. Beside the reference points, the network attachment and control functions in the transport stratum as well as the service control and content delivery functions in the service stratum are promising for network operators to create additional services.

2.2 Communication Ecosystem

Service provisioning in user satisfying quality is the goal of each content and network provider. It is important to analyse all issues that are involved in the service provision chain to improve the delivered service quality. The understanding of the relations between the different issues is necessary and is described by means of a communication ecosystem by Kilkki [92] as shown in Figure 2.2. The ecosystem has several issues, such as technical, business models and human behaviour. Each of

these issues uses its own languages to describe the issue internal relations. While the technical community talks about network performance and quality of service, the business community speaks about average revenue per user and the human behaviour community talks about happiness and experiences of customers. The identification of dependencies and relationships in the ecosystem enable to highlight existing drawbacks in the service provisioning chain. As a result these drawbacks can be selected and improved.

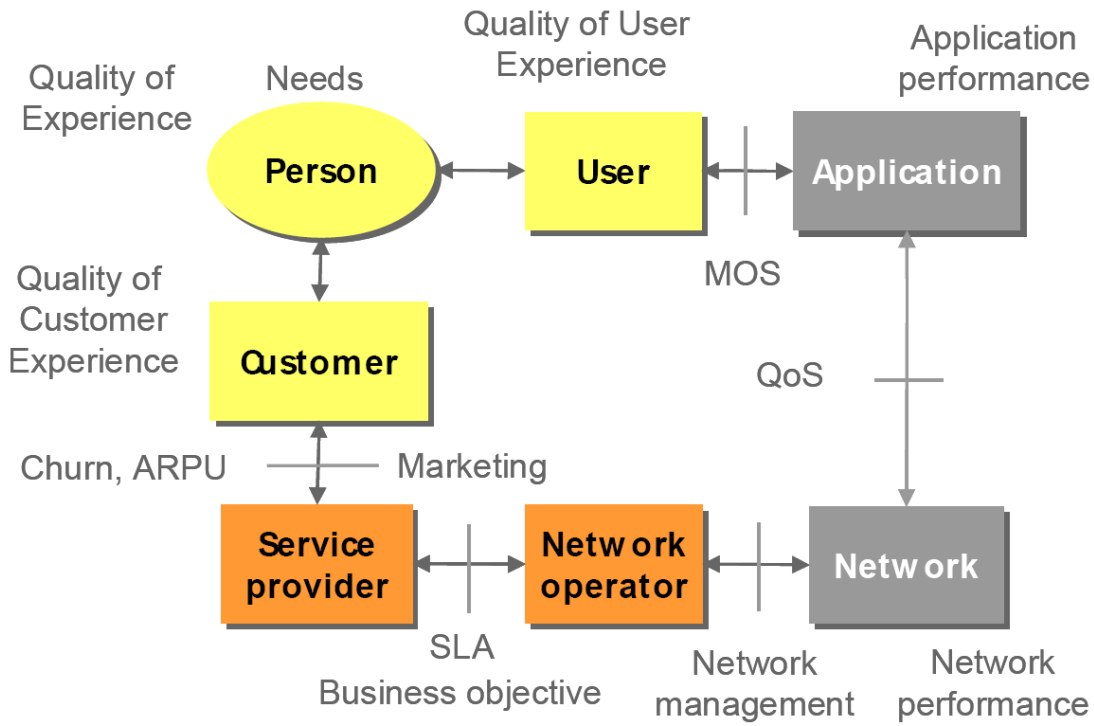


Figure 2.2: Terminology of a communication ecosystem (source: [92]).

The service provision chain attaches importance to the network. In general the success of a network and service provider depends on the satisfaction of the customers. On one hand the price of the product Internet access can lead to customer satisfaction and on the other hand the quality of the service provided by the access network as well. The framework for analysing the communication ecosystems, shown in Figure 2.2, consists of seven modules, such as the user, the application, the network, the network operator, the service provider, the customer and the person. The seventh module person is used to describe the complete ecosystem and thus, to close the gap between the user and the customer. In this framework the module person represents a human with its both sides of sensation, such as user regarding service provisioning and as a customer regarding Internet access agreements. The user represents the receiver of a provided service from an application server and the

customer represents the contractual partner of a network and service provider. This person plays an important role within the framework. A purchasing decision of the customer often depends on the quality of experience obtained from service provisioning in the past of the user. Thus, the person defines the needs and the quality level of provided services that satisfy the personal sensation.

Beside these modules the framework in Figure 2.2 also presents the relationships and interfaces between the different modules. The interface between the user and the application is the mean opinion score (MOS) that is used to describe the level of quality of user experience with the provided service. Moreover, the interface between user and application is the relationship between the areas of human behaviour and technology or usability. The quality of service (QoS) is the interface between application and network and represents the providable performance of a network. This means the service transmission from application server to the user depends on the level of QoS in the network. Thus, QoS has a direct impact on the provided service quality. The interface between the network and the network provider is similar to the relationship between the area of business and technology that can be described by the network management. The service provider describes the business objectives by means of service level agreements (SLA) that are used as an interface between the network operator and the service provider. The interface between the service provider and the customer is described by the average revenue per user (ARPU) and churn representing the marketing relationship between business and human behaviour.

The interpretation of Figure 2.2 leads to the assumption that improvements of the service provisioning chain needs to investigate the network performance and the required application performance. In this context it is necessary to investigate the influence of the network performance, such as QoS, on the provided service quality evaluated by means of the QoE. QoS and QoE are the basic issues that are focused on in the investigations in Chapter 3 to show the challenges in real-time service provisioning. The following subsections introduce in Subsection 2.2.1 QoS and in Subsection 2.2.2 QoE in more detail.

2.2.1 Quality of Service

The term quality of service (QoS) is often used with different meanings, such as user perception [93] and network performance parameters [94]. Sometimes QoS is used as a quality measure that refers to the level of quality of a provided service, i.e. the guaranteed or achieved service quality. In the area of computer networking and other packet switched telecommunication networks, the traffic engineering term QoS is related to resource reservation control mechanisms instead of the achieved service quality. In this context, QoS is the ability to provide different priority to applications, users or data flows. Moreover, QoS is the ability to guarantee a certain level of network performance to a data flow, such as a required bit rate, delay, jitter, packet loss or bit error rate.

In 1999 Kalevi Kilkki describes the definition of quality of service (QoS) in [95] as follows: "QoS is a set of attributes that can be used to define the network's capability to meet the requirements of users and applications". Then 2008 Kilkki is inclined to remove in [92] users from its definition of QoS as previously defined in [95]. In [96] QoS is described as follows: "QoS is defined as the ability of the network to provide a service at an assured service level. QoS encompasses all functions, mechanisms and procedures in the cellular network and terminal that ensure the provision of the negotiated service quality between the user equipment (UE) and the core network (CN)". Moreover, it is stated that QoS is a technical concept that is measured, expressed and understood in terms of networks and network elements.

Since there is no universal definition of quality of service, several interpretations and descriptions have been developed that are not always compatible with each other. Thus, several standardisation bodies, such as ITU, IETF, ATM Forum and OSI, have developed different definitions of QoS. The international organization for standardization (ISO) describes in ISO 8402 a definition of general quality. The international telecommunication union – telecommunication standardization sector (ITU-T) describes QoS in ITU-T Rec. E.800 "Terms and definitions related to quality of service and network performance including dependability" [94] as follows: "The collective effect of service performance which determines the degree of satisfaction of a user of the service". The terminology comprises of the following

issues to describe the term quality of service: Service support, Service operability, Serveability and Service security. The ITU-T Rec. E.800 [ibid] provides two notes regarding the term QoS:

1. Cite "The quality of service is characterized by the combined aspects of service support performance, service operability performance, serveability performance, service security performance and other factors specific to each service."
2. Cite "The term "quality of service" is not used to express a degree of excellence in a comparative sense nor is it used in a quantitative sense for technical evaluations. In these cases a qualifying adjective (modifier) should be used."

ITU-T Rec. E.800 states that service support, service operability, serveability, service security dependent on the network characteristics. The definition of the term network performance is described as follows: "The ability of a network or network portion to provide the functions related to communications between users." The terminology comprises of the following issues to describe the term network performance: Trafficability, Dependability, Transmission and Charging. Regarding the term network performance the ITU-T Rec. E.800 [ibid] provides four notes:

1. Cite "Network performance applies to the Network Provider's planning, development, operations and maintenance and is the detailed technical part of QOS, excluding service support performance and human factors."
2. Cite "Network performance is the main influence on serveability performance."
3. Cite "Network performance measures are meaningful to network providers and are quantifiable at the part of the network to which they apply. Quality of service measures are only quantifiable at a service access point."
4. Cite "It is up to the Network Provider to combine the Network Performance parameters in such a way that the economic requirements of the Network Provider, as well as the satisfaction of the User, are both fulfilled."

As stated the serveability performance is most generally affected by the network performance. A closer look into the aspect serveability performance shows three themes: the Service accessibility performance, Service retainability performance and Service integrity performance. An overview of the ITU-T E.800 framework is given in Figure 2.3.

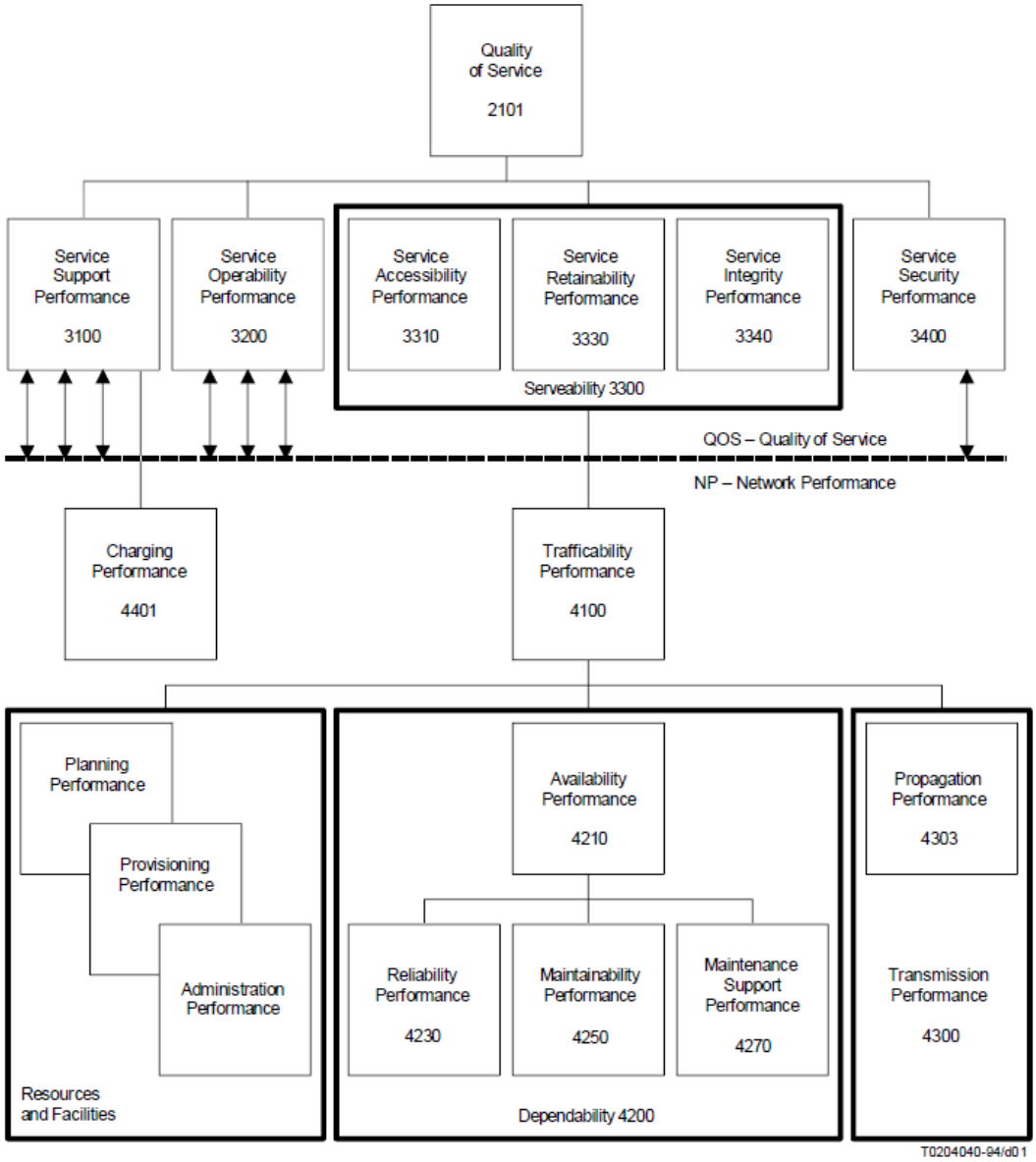


Figure 2.3: ITU-T E.800 framework [94].

The ITU-T describes in Rec. E.800 a QoS definition while ITU-T Rec. I.350 and Y.1540 focuses on network performance descriptions. To provide a relation between quality and QoS the European telecommunications standards institute (ETSI) has debriefed customers with the goal to describe QoS criteria and to derive a uniform QoS matrix, that is described in ETSI ETR 003 [97]. This QoS matrix is presented in ITU-T G.1000 [98] and can be used to determine the required QoS criteria of a telecommunication service. However, this matrix does not classify QoS requirements for service types. In ITU-T Rec. G.1010 [99] a model for multimedia QoS categories from an end user point of view and service requirements is defined. The classification subdivides services into two types of service, information loss (packet

loss) dependent and delay dependent services. The information loss dependent services are subdivided in two types of services, error tolerant and error intolerant services. The delay dependent services are subdivided in four classes interactive, responsive, timely and non-critical. Figure 2.4 combines the information of two diagrams in ITU-T Rec. G.1010 [ibid], such as mapping of user-centric QoS requirements and model for user-centric QoS categories. The two information loss dependent services and four delay dependent services results in eight QoS categories as shown in Figure 2.4.

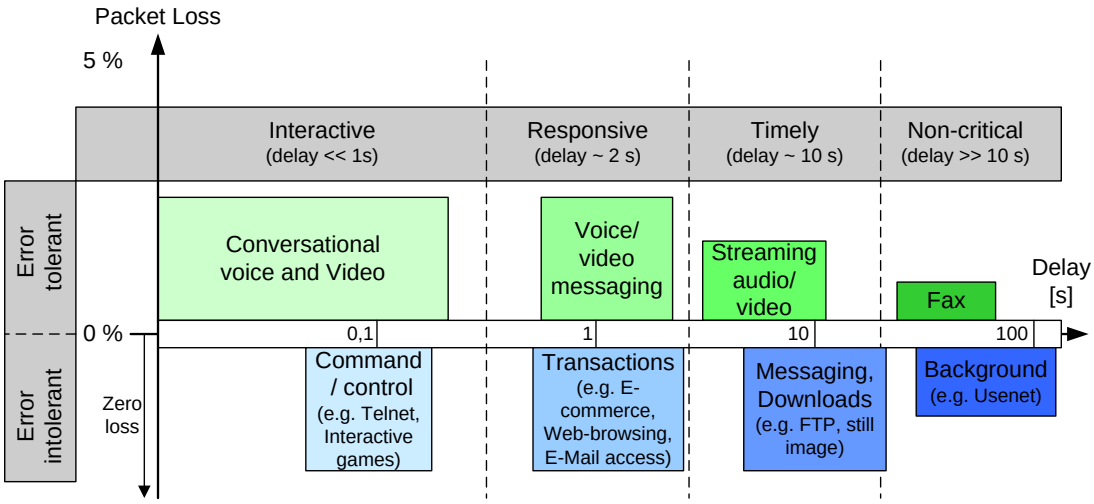


Figure 2.4: Mapping of user centric QoS requirements and model for user centric QoS categories based on ITU-T Rec. G.1010 [99].

Service acceptance of customers depends on the provided service quality. The service quality can be influenced, e.g. by network delay, jitter and packet loss. However, the degree of impact depends on the type of service. Especially for real-time streaming applications, such as VoIP, online games and IPTV quality of service guarantees are important if the network capacity is limited. Real-time streaming applications often require a fixed bit rate and are delay sensitive. In networks where the capacity is limited, for example in cellular networks it is challenging to provide the network performance to fulfil all of the service requirements. Figure 2.4 shows that conversational voice and video requires the highest network performance with regard to delay. The demand of a smaller delay is challenging when customers are on the move and handover processes have to be performed.

In recent years QoS mechanisms have been developed to manage the network performance to fulfil the network requirements of a service. Particularly, prioritising of conversational voice and video data is focused on, as described in [100]. A humans'

ear recognises the finest audio faults and delay in data communication caused for instance by network congestion or communication interruptions. In the context of network congestion prioritisation mechanisms in the network architecture help to overcome audio faults and delay. However, neither communication interruptions caused by a handover among multiple PoA nor extended handover times caused by authentication and authorisation processes within the handover process are solved by prioritisation mechanisms.

As a general summary, QoS are technical concepts, parameters, methods and mechanisms to describe and setup network performance. As a result, the QoS in the network has a direct impact on the service quality, because the delivered data via the network are influenced by the available network performance. This means, QoS mechanisms are important if the network capacity is insufficient but required for a certain type of service, especially real-time multimedia applications. By means of the integration of QoS mechanisms into the network architecture the required network performance, such as higher bit rate, less delay or packet loss, can be achieved.

2.2.2 Quality of Experience

Various definitions for QoE are presented in the literature. For instance, the International Telecommunication Union (ITU) in [101] describes QoE as the overall acceptability of an application or service, as perceived subjectively by the end-user. Muhammed *et al.* describe in [96] the difference between QoE and QoS as follows. The aim of the network and services should be to achieve the maximum user rating (QoE), while network quality (QoS) is the main issue for reaching that goal effectively.

The following definitions provide by the Collins dictionary [102]; “Experience is direct personal participation or observation; actual knowledge or contact. Quality is the basic character or nature of something. The combination of both definitions experience and quality can lead to the definition of QoE as follows. QoE is a basic character or nature of a direct personal participation or observation.”

Even if QoE is a personal impression or indicator that is created in a humans’ mind to evaluate the characteristic of an object, such as a service, it is necessary to classify the quality in general behaviour. Classification requires the definition of parameters. Even if parameters are quantitative rather than qualitative as described in

[103] the terminus should still be QoE instead of quantity of experience. A definition that describes the relationship between user and application is the mean opinion score (MOS).

In [96] QoE is described as follows: "QoE is how a user perceives the usability of a service when in use – how satisfied he or she is with a service in terms of, for example, usability, accessibility, retainability and integrity of the service. Service integrity concerns throughput, delay, delay variation (or jitter) and data loss during user data transmission; service accessibility relates to unavailability, security (authentication, authorisation and accounting), activation, access, coverage, blocking, and setup time of the related bearer service; service retainability, in general, characterises connection losses." Moreover, in [ibid] it is stated that the term QoE refers to the perception of the user about the quality of a particular service or network. The perception of the user is expressed in human feelings, such as good, excellent or poor.

A general assumption is that a higher QoS in the network will in many cases result in better QoE. However, even if all traffic QoS parameters are fulfilled a satisfied user can still not be guaranteed. This means the achievement of high QoE depends on the understanding of all factors contributing to the user's perception of the target services. As a result, the knowledge about all perception influencing factors has to be used to define the operating requirements. The mean opinion score can be used to express the QoE in a voice over IP communication. The MOS describes the relationship between user perception and provided application quality. In Section 3.2 the MOS value is used to investigate the speech quality depending on interruptions in a speech communication induced by handover processes in WLAN architectures.

2.3 Authentication, Authorisation and Accounting

Network access control (NAC), such as user authentication and authorisation as well as accounting (AAA), is a basic requirement for operator access networks. A network access control architecture is applied to avoid network access for unauthorised users. The NAC infrastructure has to fit into the operator's network architecture. Moreover, the NAC concept has to be state-of-the-art regarding security issues to provide most

suitable user privacy and data protection. This section introduces the term AAA and presents a generic AAA architecture.

Authentication is the process to verify and audit an entity's identity. Typically, the authentication is carried out by providing evidence from an entity. The evidence can be a digital identity consisting of e.g. an identifier and the corresponding credentials, such as a password or digital certificates.

Authorisation is the process that determines whether an entity is authorised to get access to a service or network architecture. Authorisation is typically carried out after the authentication process when logging on to a service or a network. Most often authorisation is performed with regard to the entity's policies, such as restrictions to services, physical location restrictions or restrictions to get multiple accesses by the same entity or user. Additional methods in the context of the network access authorisation process are for example IP address filtering, address assignment, route assignment, type of quality of service, bandwidth capabilities or type of encryption.

Accounting is the process that carries out tracking of the consumed network resources by users, events, such as login and logout of users or occurred authentications and authorisation failures. Besides the security aspect the accounting information are used e.g. for billing, management and planning. Typical stored information in the accounting process is the identity of the user or entity, the type of service delivered as well as the point in time a service starts and ends.

The general components of such an AAA architecture are the AAA database, the access decision function (ADF) and the access control function (ACF), as shown in Figure 2.5.

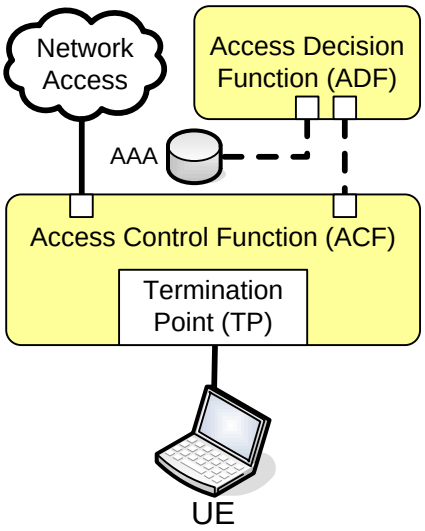


Figure 2.5: Authentication, authorisation and accounting architecture.

User profiles, together with their policies, are stored within the AAA database. The termination point (TP) terminates all access requests initiated by a UE. Depending on the used authentication mechanism, such as web-based login, wireless link encryption or tunnel connection, the ACF translates the access request into ADF compliant format. For that purpose the RADIUS [80] or Diameter [104] protocol is used. Furthermore, the ACF is responsible for gathering accounting data. The ADF carries out user authentication and authorisation considering user profiles within the AAA database and informs the ACF about the user authorisation status. Depending on this authorisation status the ACF controls network access. In the case of successful user authentication and authorisation the ACF allows network access.

A network access control framework for NGNs is described in ITU-T Y.2012 [91] by means of the network attachment control functions (NACF), such as "The network attachment control functions (NACF) provide registration at the access level and initialization of end-user functions for accessing NGN services. These functions provide transport stratum level [identification/authentication], manage the IP address space of the access network, and authenticate access sessions. They also announce the contact point of NGN functions in the service stratum to the end user." The NACF provides the following functionalities:

- Dynamic provisioning of IP addresses and other user equipment configuration parameters.
- By the endorsement of user, auto-discovery of user equipment capabilities and other parameters.

- Authentication of end user and network at the IP layer (and possibly other layers). Regarding the authentication, mutual authentication between the end user and the network attachment is performed.
- Authorization of network access, based on user profiles.
- Access network configuration, based on user profiles.
- Location management at the IP layer.

The NACF includes the transport user profile which takes the form of a functional database representing the combination of a user's information and other control data into a single "user profile" function in the transport stratum. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN." A detailed description of NACF is specified in ITU-T Y.2014 [105].

With regard to service quality improvements for real-time services, such as VoIP, the network performance and thus, the QoS of the network could be improved through enhanced network access control concepts. A novel NAC concept can provide reduced handover process times that lead to reduced communication interruptions. This would have an important effect on the VoIP quality in the case when customers are one the move and handover processes occurs many times while using the VoIP service.

2.4 Usability

Beside service provisioning in user satisfying quality the usability of services is important to achieve acceptance by the customers. For example the research project usability-in-Germany [106] states that the use of powerful application software has gained a lot of importance, especially for small and medium enterprises. The main reasons for this are business goals such, as improving productivity, quality and customer satisfaction and the fulfilment of industry-specific standards for documentation and transparency of corporate activities. Moreover, the demands of end users regarding the usability of software applications have increased. The pure availability of functions is not enough, rather aspects of usability, design and user experience are increasingly in focus. This trend of user stance on usability and user experience is characterized by the experience with which information technology used in daily life. For example, web applications such as www.amazon.com,

www.facebook.com or smart mobile phones, continuously change the way people communicate and interact with new web applications and smart phones.

The term usability is specified in International Organisation for Standardization (ISO) 9241-11 [107] as "Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." For a long time the term user experience was not defined by the ISO. However, this has been changed with the ISO 9241- 210 [108] that specify user experience as "A person's perception and responses that result from the use and/or anticipated use of a product, system or service". According to this definition user experience is an evaluative feeling that comes through the fulfilment or frustration in the interaction. Thus, usability and user experience is separated from each other. Figure 2.6 [109] presents the relation between usability and user experience.

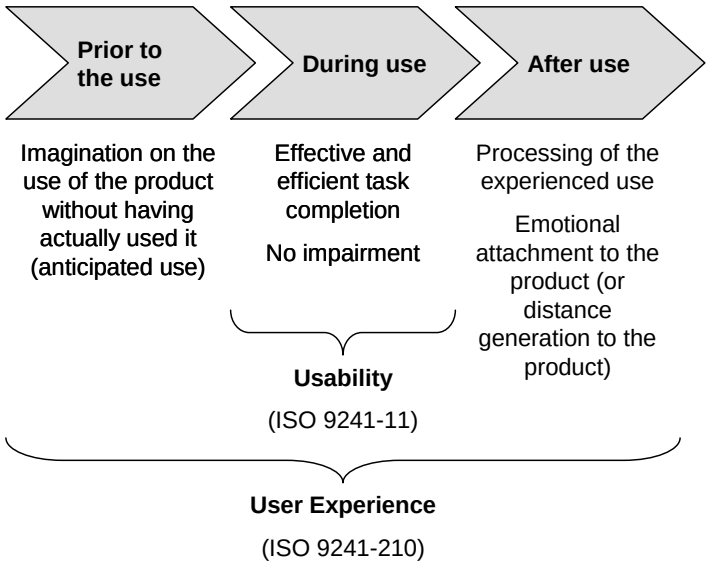


Figure 2.6: Standardized view on usability and user experience.

As shown in Figure 2.6 the user experience includes all effects on users prior to the use and after use of a product. Without having actually used the product the user imaginates the use (anticipated use). The experienced use is processed after the use leading to an emotional attachment or to a distance to the product. On the contrary the usability focuses on the actual situation of use, such as effectiveness and efficiency. Even if the project usability-in-Germany [106] focuses on applications in the context of usability it is assumed that this user behaviour is conferrable to the consumption of Internet application services and Internet access as well. Due to this, usability is a big issue for network service providers or application service providers.

The service providers are permanently striving to improve the usability of offered services. For example application service providers focuses on a ‘cool’ look and feel of the software while network service providers focuses on easy network access concepts. Therefore, the hotspots’ login process might be improved to enable a more user-friendly login.

2.5 Creation of Revenue for Network Operators

The creation of revenue is the most important issue for network operators [1], [2], [3]. There are several aspects that have to be balanced. On the one hand network operators have capital expenditure (CAPEX) to extend the network architecture and operational expose (OPEX) to run the existing or extended network architecture. On the other hand network operators have to motivate users to consume their products to generate revenue streams. However, the use of the products depends on the balance between the cost of the product and the benefit to the user. A possible benefit could be, e.g. fast Internet access or large bandwidth connectivity.

“In the struggle to manage churn, the use of flat rate tariffs has been deployed extensively, most recently in the mobile arena, leading to an explosion in mobile broadband use” as stated in [110]. The reasons why network operators have introduced flat rates is described in [111] as “Mobile carriers introduced flat-rate data plans to encourage consumers to try third-generation (3G) services like mobile email and web surfing, after spending billions of dollars on building 3G networks and buying licences in the early 2000s”. “But the unexpected success of the Apple iPhone and other smartphones in stimulating demand is leading to overcrowded networks, at a time when operators are cutting back on capital expenditure rather than expanding network capacity” [ibid]. As a result, on one hand network operators are under pressure to extend the network capacity to be able to satisfy the bandwidth demand. However, the expansion of the network capacity does not guarantee increased income. It is actually quite the contrary as the price battle between network operators is still in progress and squeezes not only the revenues as well as the margins of the network access products. Rather the increased demand of bandwidth due to web video portals, such as as Android TV [112], Maxdome [113] or LoveTV [114] pressures network operators to upgrade their network architectures to fulfil the required QoS in the network.

Cisco describes in its forecast [115] that the global IP traffic has increased more than fivefold in the past 5 years, and will increase threefold over the next 5 years until 2018. In [116] a 18-fold increase of mobile data traffic between 2000 and 2013 is disclosed. Mobile video traffic has exceeded 50% for the first time [ibid] in 2012. Global mobile data traffic will increase nearly 11-fold between 2013 and 2018 as forecasted in [116]. Even if this forecast is not correct the bandwidth demand will increase in the near future. This means that network architectures have to be extended. However, network architecture upgrades are very expensive. In this context the question occurs who cover this cost. Normally the network operators have to pay for the network architecture extension. However, another question at this point arises. Who is the largest beneficiary of this network upgrade? The additionally generated network resources are mostly used by content providers to deliver more services and large amounts of data to the customers. But from today's point of view content providers do not participate in the network architecture upgrade costs. Moreover, it is unlikely that customers spend more money for their network access, because the network access has not been changed from their point of view. As a result, both content provider and customer have little willingness to pay for a network upgrade. This is the reason why network operators in the age of flat rates search for new strategies to obtain additional revenues from content providers as well as customers.

One strategy focuses on the abolishment of flat rates and foresee usage based pricing which "will ease current capacity issues by capping demand, contain capital expenditure requirements and potentially increase revenue", as stated in [111]. Moreover, Reuters mentions in [ibid] that "The mobile telecoms industry is leaning towards ending flat-rate data plans, which have fuelled an explosion in network traffic while bringing in little extra revenue". However, the flat rate paradigm change is challenging, because it is not clear if customers will easily accept changes to the data tariffs.

Another strategy envisions the integration of QoS mechanisms in the network architecture to allow companies to delay a plain capacity extension at least for a short period of time. In most of today's service provisioning cases the best effort network traffic performance is good enough to deliver services at good quality to the users. However, in peak hours network segments, e.g. access networks on the user or

content provide side get congested which leads to reduced service quality delivered to the users. QoS supported traffic allows the transport of application services in better quality [117] compared to the provided service via best effort traffic in the Internet. The integration of QoS mechanisms can be used to transport several traffic classes separated from each other with different network performance characteristics. The network performance characteristics can be adjusted depending on the required delay, jitter or packet-loss. As a result, QoS mechanisms can be used to achieve network performance that is needed to deliver services in user satisfying quality. However, the deployment of QoS mechanisms in network architectures is expensive and needs management efforts. Moreover, from today's point of view users are not aware what improved network performance based on QoS support means and which benefits they might have. As a result, the willingness to pay for QoS supported network traffic is not given at the moment.

These days QoS provisioning in the network is envisioned by network operators to be a tool to increase revenues for the delivery of QoS supported traffic. Beside QoS support in single network operator domains [22] the provisioning of end-to-end QoS supported traffic across multiple network operator domains is the focus in the European Commission project Economics and Technologies for Inter-Carrier Services (ETICS) [118]. Moreover, new concepts and functionalities that enable added value services or new ways of revenue creation for network providers are very welcome in the context of next generation network service and application service delivery [22], [118].

For network operators the creation of added value services derived from their own or joint operations is able to generate more revenue than just for plain data transport [119], [111]. Nokia Siemens Networks describe in [119] "Surviving the global recession is crucial, but taking steps to secure future growth opportunities is essential – the grow-or-go dynamics are an unforgiving environment. Communications service providers that invest in new growth opportunities will be in pole position when business recovers. In saturated mobile markets, optimizing, leveraging and monetizing your connectivity assets are pragmatic steps towards new growth opportunities". In [111] Reuters states that "Mobile providers are remodelling their pricing strategies to sweat their assets whilst tentatively looking at new product offerings". As a result, the creation of added value services is very important for

network operators future business to attract users for new business models as well as to stimulate the willingness to pay for new products, e.g. for QoS support in the network.

In [1] over the top (OTT) services and applications and their accessibility on mobile devices is described as one of three major trends that "are driving the need for service excellence and making it more important than ever before to deliver a high-quality user experience". Furthermore, [ibid] mentioned that "OTT applications do not exclude operators from the loop. At the very least, operators need to ensure that applications are delivered correctly over their networks. In many cases, they will also be involved in the charging process". Those statements underpin the necessity of network operators to develop added value functionalities that can be offered to OTTs as additional services. The added value functionality can e.g. used by the OTT to improve its service delivery to the user. It can be assumed that OTTs will pay for such added value functionalities which are beneficial to their products. As a result, added value functionalities can contribute to create additional revenue for network operators.

2.6 Summary

In the following the above introduced fundamental issues such as next generation network architecture, QoS and QoE in a communication ecosystem, usability, authentication, authorisation and accounting, as well as creation of revenue for network operators were summarised. Moreover, the relations between network performance and application performance will be highlighted to show how improvements of one issue benefits also the other issue.

The relation of network performance on application performance in a communication ecosystem was described in Section 2.2. In this context the network performance was represented by means of the parameter QoS and the application quality perceived by a user by means of the parameter QoE. This relation shows that improved network performance is able to improve the delivery of application service quality. This fact shows the motivation of network operators to improve the network performance. The improved network performance is doubly beneficial. On the one hand it can enrich the satisfaction of customers based on the improved application service quality, while on the other hand it can be a network capability feature that

motivates content or third party providers to select this specific network provider for the application data transport. As a result, it is assumed that improved network performance can contribute to increased revenue for network providers. As described in Section 2.5 the increase of revenue is one challenging issue for network providers.

Another aspect to enrich the satisfaction of a user is to improve the usability of application services or communication products. As presented in Section 2.4 usability contributes significantly to the user experience. The user experience includes all effects of a user prior to and after the use of a product. The experienced use of a product is subconsciously evaluated by the user which leads to an emotional attachment or to distance to the product. As a result, it must be expected that improved usability which provides a good user experience is able to enrich the user satisfaction of a product. This means, from a network operators point of view improved usability contributes to increase the revenue.

The challenge for network operators is to create revenue as described in Section 2.5. Moreover, network operators want to be more than the ‘just a bit pipe’ between content providers and users. The introduced ITU-T NGN framework in Section 2.1 describes functional requirements and architecture for next generation networks. The NGN functions described in ITU-T Y.2011 are divided into service stratum functions and transport stratum functions. The service stratum functions are support and control mechanisms related to the delivery of services and applications to the end-user. The mechanisms in the transport stratum provide the IP connectivity services to the NGN users. Transport control functions perform network attachment control, resource and admission control as well as mobility management and control. Network operators assume that network and application services can be realised and managed in an easier and efficient by means of NGN conform and converged network architecture than in today’s silo network architecture [48]. A benefit of a NGN conform architecture could be that network operators use their network assets in a more efficient way.

A possibility for network operators to create revenue is the use of their existing assets in the network architecture. These assets, such as user related information can be used to develop added value services. For that purpose it is important to have a well deployed network architecture that provides information which can be used to derive added value services. For instance, a suitably implemented network access

control architecture performing authentication, authorisation and accounting by means of the described network attachment control functions as was shown in Section 2.3. As a result, the user related information can be used to setup individual added value services.

The NGN framework ITU-T Y.2011 presented in Section 2.1 describes, besides functional requirements, a reference point and interfaces which are candidates for building common interfaces. The interfaces are user-network interface (UNI), network-network interface (NNI), application network interface (ANI) and service network interface (SNI). The user-network interface (UNI) is used to establish connectivity to the terminal equipment, user networks and corporate networks. The network-network interface (NNI) provides connectivity to other NGNs, other IP-based networks and PSTN/ISDN. Interactions and exchanges between a NGN and applications are enabled by the application network interface (ANI). The service network interface (SNI) is an interface to interact and exchange information between a NGN and other service providers, e.g. a content provider. The clear separation of these interfaces among different line of actions seems to be a solid base for the design of added value services for network operators.

3 Challenges in Real-Time Communication and User Satisfied Service Provisioning

Service provisioning in customer satisfying quality is the ultimate goal for network operators as well as content providers. However, the provided service quality to customers depends on the human perception. The dimension of how the network performance influences the service quality and how this influence affects the perceived service quality of customers has to be determined. Beside the network performance which influences the delivered application service quality, the usability has to be examined. In addition to that a network architecture design which allows using the operator existing infrastructure to enrich user satisfaction is beneficial for network operators. In the following technical drawbacks are discussed which have to be addressed to enhance the quality of experience of users. The potentials to improve the user satisfaction are domiciled in the areas network capability, usability and service delivery, as shown in Figure 1.1. All these areas are network architecture related issues. This means network operators are able to improve these areas to enhance the satisfaction of users.

N. Kano describes in [120] a method for structuring customer requirements and to determine their influence on customer satisfaction. The Kano model describes three categories basic, performance and excitement. A direct relationship between improved performance and customer satisfaction is shown. Based on this background it can be explained that a service or content provider permanently improve their services and aim to provide services in the best possible quality to their customers. Each service has its own requirements, e.g. on the network performance, to be delivered at the best quality to the customer. As a result, network operators have to provide the network performance that fulfils the service requirements. Especially, real-time services, such as telephony or video conferencing over IP suffer from network performance influences, such as delay, jitter and packet-loss. Future success of access networks, for instance WLAN or WLAN based mesh networks will depend on the capability to provide real-time services in customer satisfying quality. Moreover, application services have to be delivered in user satisfying quality even

when customers are on the move. However, the aspect of mobility with its handover processes introduce an additional factor that influence the network performance in a significant manner as is demonstrated in this chapter.

The humans' ear is sensitive to sound deviation and speech interruptions and recognises finest audio faults and jitter in data communication caused for instance by network congestion or communication interruptions [109]. In the context of network congestion prioritisation mechanisms in the network architecture helps to overcome audio faults and delay, as described in [100] and [121]. However, neither communication interruptions caused by a handover among multiple PoA nor extended handover times caused by authentication and authorisation processes within the handover are solved by these prioritisation mechanisms.

The following sections determine the impact of packet loss and communication interruptions on speech quality in voice communication. Several points of view, such as voice quality, handover and mobility aspects are investigated in the context of seamless real-time service provisioning in carrier grade quality. These investigations show the existing challenges in seamless service provisioning especially when customers are on the move. Figure 3.1 presents the different topics of seamless real-time service provisioning investigation.

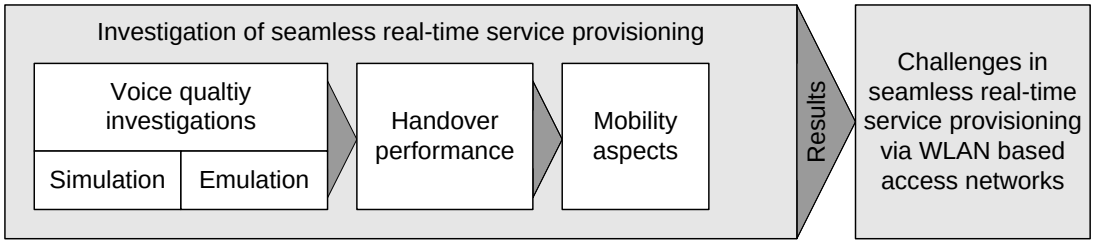


Figure 3.1: Overview of seamless real-time service provisioning investigations.

The challenges of WLAN based access networks belong to the area of improved network capability. In the area of improved service delivery the state-of-the-art of Internet based service provisioning to users is presented. In this context the potential of network operators is shown to improve service provisioning based on their exsisting network infrastructure. Moreover, the challenge to use these assets in a common way to setup added value services is presented. In the area of improved usability the challenge to motivate users to choose hotspots more often than they do today is discussed.

The remainder of this chapter is structured as follows. The term mobility and handover is presented in Section 3.1 in detail. The voice communication is simulated and the behaviour of voice quality influenced by communication interruptions is investigated in Section 3.2. In this examination the network performance is simulated. In Section 3.3 the simulated network performance is described by data interruptions that represent VoIP communication interruptions that occurred due to handover processes in real network architectures. The handover time behaviour in Section 3.4 investigates the network access authentication and authorisation process. In Section 3.5 the handover frequency of a customer with respect to the WLAN coverage size is discussed. The potential and real challenges of existing standardised frameworks in the context of improved service provisioning to customers based on added value services is shown in Section 3.7. Section 3.6 describes the behaviour of today's WLAN based hotspot use highlighting the drawbacks of usability. This section will be concluded describing the challenges in seamless real-time service provisioning concerning handover performance and network access control. Moreover, the challenges of application service and network access service provisioning in customer satisfying quality from a network operators point of view is described.

3.1 Mobility and Handover Types

The kinesics behaviour of users in a wireless access network differs from the way of being connected to the different PoAs. The first kinesics behaviour of the user can be stationary. The device is connected to the wireless network and is always served by the same PoA. This means the user is able to move around in a limited area or is located in the same position. Performing of handovers is not necessary. The second kinesics behaviour can be nomadic. The device connects to different PoAs. However, the device gets served by a single PoA during an active Internet session. The user varies the location only after the device is disconnected from the PoA. For instance, the user is connected to the business WLAN. After that the user disconnects from the PoA and connects later to another PoA in the home WLAN. As in the stationary behaviour in the nomadic behaviour no handover has to be performed. Finally, the third kinesics behaviour can be mobile. The user moves around in the WLAN access network. The WLAN consists of multiple PoAs. Due to the mobility of the user the

device changes the PoAs even while an active Internet or service session. This means the device has to handover from one PoA to another PoA. This type of mobility is called terminal mobility.

Beside terminal mobility there are other types of mobility, such as user, session and service mobility. User mobility allows a user to be contactable on different devices. Session mobility allows continuing an active service session when changing the device. Service mobility allows a user to get access to a service independent of the used device or access network.

In a handover process a device changes the PoAs. A device performs a handover when it leaves the coverage of one PoA and enters the coverage of another PoA. In the case of both PoAs using the same technology a horizontal handover is performed while in the case of both PoAs using different technologies a vertical handover is performed.

In this work the terminal mobility focuses on homogenous wireless access networks, such as WLANs. Terminal mobility enables devices to change the PoA. The challenge is to keep the Internet session active and to provide services uninterrupted even in the case of performed handover processes.

3.2 Speech Quality Investigation Based on Handover Simulation

This section evaluates the speech quality behaviour with respect to users mobility and carrier grade VoIP requirements. In a mobility scenario a wireless client changes the PoAs. This change and the handover process leads to communication interruptions. Consequently, the mobility influence can be abstracted by a communication interruption that emulates the handover process among different PoAs. The speech quality is represented by the perceptual evaluation of the speech quality (PESQ) value [65] calculated by two different types of PESQ simulations. The first simulation series focuses on a single handover process in a voice communication that is simulated by means of a single interruption within an audio stream. The second simulation series focuses on multiple handover processes in a voice communication that is simulated by means of multiple interruptions in an audio stream. In addition, different silence lengths are taken into consideration. The single and multiple interruption investigation show the effect on speech quality, such as VoIP quality in the context of user mobility.

The voice over IP service is a challenging IP based communication service [100], [121] and is therefore focused upon in the further investigation. The quality of VoIP itself mainly depends on the parameters delay, jitter and packet-loss of a VoIP packet. The challenge of VoIP data transport is that VoIP data cannot be buffered for large periods of time. Moreover, VoIP data cannot be retransmitted. This means the network performance has a direct influence on the voice quality. From the network providers' point of view the number of supported calls via an access network is important but also the quality of the calls. In the case of bad voice quality customers will not be satisfied with the service. The capability of access networks, such as WMNs is measurable by means of the amount and the quality of provided time-critical services, such as VoIP.

Delay can arise from limited network resources as well as from a difficult channel environment. Furthermore, delay is introduced by the handover process, as investigated in [57]. The handover process in WLAN comprises of sending probe messages, to scan for new PoAs as well as of sending authentication and re-association messages. [56] examines in detail the influence of the handover process components, such as probe delay, authentication delay and re-association delay. The conclusion of [ibid] is that the probe delay is the most significant part of the handover delay lasting up to several hundreds of milliseconds. However, the reduction of the probe delay is possible through handover triggers controlled by e.g. location based information. Consequently, the scanning process can be avoided but the authentication and re-association delay still remains. Due to this, the enhancement of the authentication and re-association delay is the focus of this work. There are two authentication types in the IEEE 802.11 standard for authentication, the open system and shared key system. Investigations in [55] describe, that the open system authentication process impacts on the handover time behaviour with 1 ms. The impact of 1 ms is negligible regarding the handover performance. However, there are more complicated authentication approaches that require the data exchange with external authentication servers, e.g. pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1x mode described within [122], [123]. [62] describe that the integration of security mechanisms within network architecture evoke time and resource consumption, which poses a problem if delay critical applications, such as VoIP, should be provided in user satisfying quality.

Furthermore, handover performance depending on implementations and used devices is presented in [ibid]. As shown in [ibid] the authentication delay varies between 19 ms up to 330 ms. The impact of packet-loss caused during the authentication message exchange is another important factor, described within [57].

The International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) specifies in [63] a one-way delay of 400 ms regardless of the application. However, highly interactive tasks, such as VoIP, demand less than 150 ms delay[124]. Regarding the E-model [125] for speech applications a mouth-to-ear delay of 150 ms has a transmission rating, *R*, above 90. The translation of the value $R = 90$ to the level of user acceptance by means of the speech categories of ITU-T Rec. G.109 [124] shows that users are very satisfied with a mouth-to-ear delay of up to 150 ms. The E-model [125] provides a prediction of the expected voice quality, as perceived by a typical telephone user, for a complete end-to-end, i.e. mouth-to-ear telephone connection under conversational conditions. In [54] the general relation of a delay chain in a speech communication path and the influence of data loss are described.

The ITU specified in ITU-T Rec. P.800 [126] is a standard for subjective speech quality rating. The indicator of this rating is the mean opinion score. To obtain a MOS value users determine the speech quality. Five levels are used to describe the speech quality. From level 5 which is equivalent to excellent quality down to level 1 which is equivalent to poor quality, as shown in Table 3.1. Another method for speech quality rating is specified in ITU-T G.107 [125] by means of the E-model for objective speech quality rating. The speech quality in the E-model is expressed by the factor *R*. The E-model considers the signal-to-noise ratio, the impairments that occur with the voice signal as well as the impairments caused by the delay and the low bit-rate codecs. The factor *R* is convertible into the MOS scale, as shown in Table 3.1. Another objective speech quality rating method that has been specified in ITU-T G P.862 [65] is the PESQ value. The PESQ method simulates the human speech quality rating by comparing an original speech signal with a transmitted speech signal. The PESQ value correlates with the factor 0,935 to the MOS value. The PESQ value is mapped to a MOS-like value between -0,5 and 4,5, as shown in Table 3.1.

Description of speech quality	MOS	E-model; R	PESQ
Excellent; user very satisfied	5	90-100	4.5
Good; user satisfied	4	80-90	4
Fair; some users dissatisfied	3	70-80	3
Poor; many users dissatisfied	2	60-70	2
Bad; nearly all users dissatisfied	1	50-60	-0.5 – 1

Table 3.1: Relation of MOS, R and PESQ value.

3.2.1 Speech Quality Simulation Setup

This section investigates the speech quality depending on an interrupted audio stream. The speech quality is represented by the determined PESQ value. Figure 3.2 shows the block diagram to determine the PESQ value.

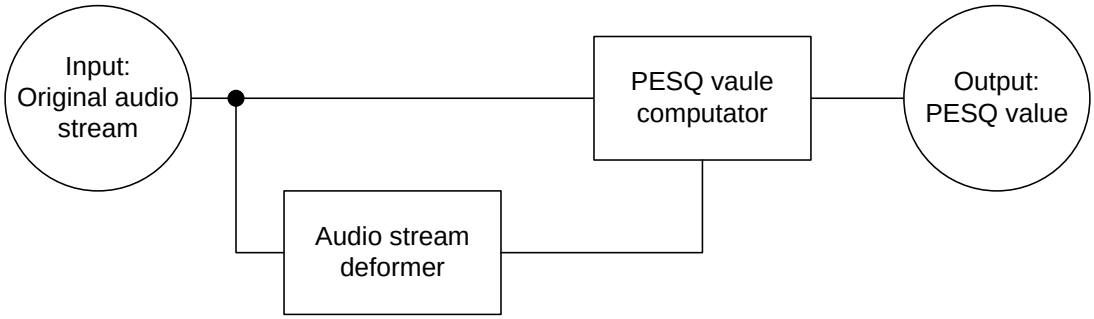


Figure 3.2: Block diagram of PESQ value determination.

The speech quality investigation focuses on two different types of PESQ value simulations series. The first simulation series investigates deformed audio streams with a single interruption within the stream while the second simulation series investigates deformed audio streams with multiple interruptions. The audio stream deformer in Figure 3.2 inserts the interruptions within the original audio stream that leads to the deformed VoIP stream. The audio stream deformer is realised in Matlab. Table 3.2 lists the interruption length in the audio stream represented by the length of interruption (LI). The distances between the LIs simulate a wireless network rollout with nearly equal distributed PoAs. Finally, the PESQ value is determined by the PESQ value computator that compares and evaluates the original VoIP stream with the deformed VoIP stream.

Length of interruption [ms]	5	10	20	40	60	80	100	125	250	500	1000	2000

Table 3.2: Listing of simulated length of interruption.

The aim of providers is to deliver VoIP services to customers in traditional telephony quality. Traditional telephony is PSTN or ISDN. However, the speech quality of ISDN is better in comparison to PSTN. Hence, it is necessary to investigate carrier grade VoIP quality in comparison to ISDN quality. Thus, a VoIP codec providing a comparable quality to ISDN is needed. The G.711 codec is used in ISDN [127] with an audio signal sampling rate of 8000 samples per second [128]. Figure 3.3 shows the method of deforming the original audio stream. The precondition of stream deforming is to read the original audio stream which is sampled about 8000 times a second and is 51 s long. Within the audio stream a range of silence insertion is defined, as shown in Figure 3.3. The range of silence insertion represents the area wherein the different lengths of interruption are positioned. The length of interruption emulates the interruption in a speech communication. Simulation failures due to the wrong locations of the interruptions or the length of interruptions are avoided by means of security distances at the beginning and at the end of the stream. In more detail near the start and end of the audio stream the range of interruption inserting starts at the defined first possible interruption point (FPIP) and ends at the last possible interruption point (LPIP). FPIP and LPIP are 2 s away from audio start and end meaning the VoIP stream is first deformed 16000 samples away from start and last deformed 16000 samples away from end of stream. The VoIP stream deformation is carried out by manipulating the audio stream samples. At the location of interruption and in the length of interruption the samples are set on the value 0. The simulation series differs from the amount of single and multiple interruptions within the deformed audio stream. Details of this difference are described within the next subsections.

3.2.2 Single Interruption within Audio Streams

The single interruption simulation series investigates the influence of a single interruption within an audio stream on the speech quality. Figure 3.3 a) shows the insertion of a single point of interruption (SPI) into the original audio stream.

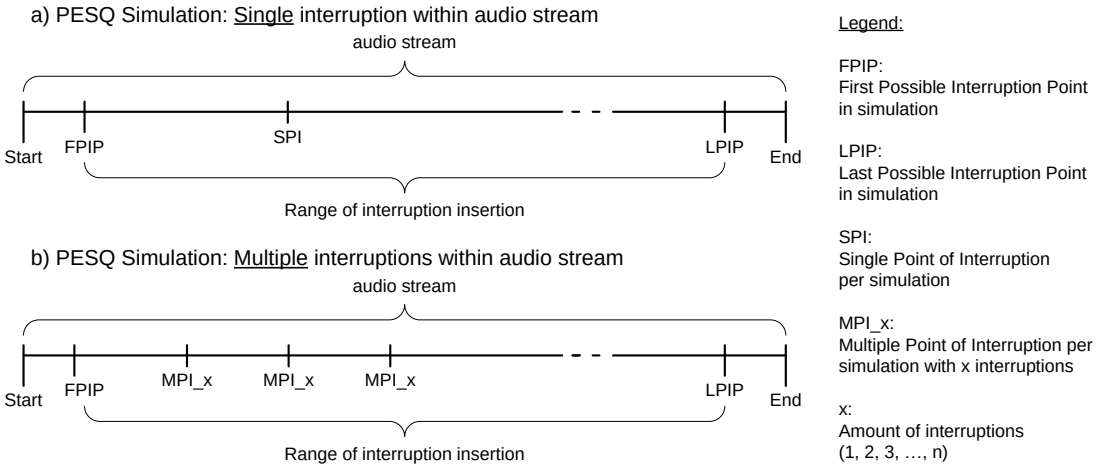


Figure 3.3: PESQ simulation; a) single and b) multiple interruptions within audio stream.

To investigate the speech quality and PESQ value depending on the SPI location multiple SPS locations have to be considered within the audio stream. The audio stream deformer distributes the SPI equally between FPIP and LPIP while FPIP and LPIP are the first and the last SPI of simulation. Nine locations of SPS are defined. The simulation is carried out per each SPI location and each time with the equal length of interruption. The lengths of interruptions are shown in Table 3.3.

Length of interruption [ms]	Min. PESQ value	Max. PESQ value
5	4.36	4.5
10	4.35	4.49
20	4.25	4.48
40	4.17	4.39
60	4.13	4.36
80	4.07	4.34
100	4.08	4.34
125	4.06	4.35
250	3.98	4.30
500	3.94	4.10
1000	3.78	4.01
2000	3.45	4.04

Table 3.3: Listing of simulated interruption types (LIs) as well as minimum and maximum of determined appropriate PESQ values.

The single interruption results are presented in Table 3.3. The determined speech quality is expressed by the PESQ value. Minimum and maximum PESQ values are listed relating to the length of simulated interruption. Keeping in mind that a provider aims to provide VoIP in a comparable quality as in traditional telephony, such as ISDN, the PESQ value should be larger than four. In general, the simulation shows

that a single interruption with up to 250 ms does not influence the speech quality in a significant manner. Furthermore, the results show that the decreased speech quality depends on the location of interruption in the audio streams, as shown in Figure 3.4. The influence of the location can be ascribed to the content in the audio stream getting lost by the interruption. Interruptions with less than 250 ms lead to a PESQ value larger than four. However, a single audio stream interruption of 250 ms can lead to a decreased speech quality with a PESQ value smaller than four, as shown in Figure 3.4. The result of a simulation with an interruption length of 250 ms is presented because it shows the underrun of the PESQ value four.

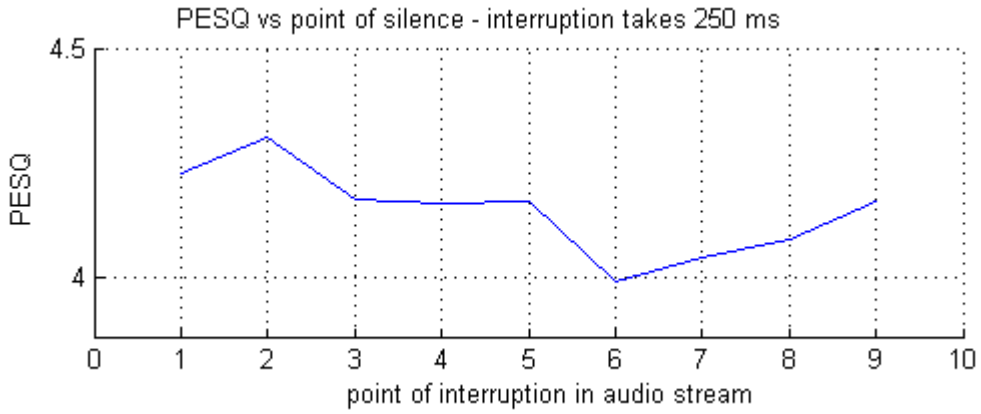


Figure 3.4: Point of interruption in audio stream influences PESQ value and thus the speech quality; LI = 250 ms.

The interpretation of the results in the context of a real handover scenario in WLAN leads to the assumption that a single interruption and a single handover respectively does not influence the overall speech quality in a significant manner. It is possible that the interruption is noticeable but the experience of the user will not be affected in a meaningful manner.

3.2.3 Multiple Interruptions within Audio Streams

This simulation series investigates the influence of multiple interruptions within an audio stream on the speech quality. This behaviour of affecting an audio stream is comparable with a WLAN mobility scenario in which a mobile node handovers among multiple PoAs in a WLAN covered area. In Figure 3.3 b) the insertion of multiple point of interruption (MPI) in the original audio stream is presented. To investigate the speech quality and PESQ value more than one MPI location has to be determined within the audio stream. The amount of MPIs within the stream is

defined by *x*. Each simulation series is carried out for the amount of $x = 2, 3, \ldots, 9$ interruptions. The audio stream deformer distributes the MPI equally between FPIP and LPIP while FPIP and LPIP are the first and the last MPI of the simulation. In case of $x = 3$ MPI_1 is equal to FPIP, MPI_3 is equal to LPIP and MPI_2 is located at the centre of the range of interruption insertion, as shown in Figure 3.3 b). Each simulation series is carried out sequentially with a specific amount of MPIs in the audio stream depending on *x*. Moreover, each simulation series is performed with different length of interruptions, as shown in Table 3.4.

x MPIs / LI [ms]	2	3	4	5	6	7
5	+	+	+	+	+	+
10	+	+	+	+	+	+
20	+	+	+	+	+	+
40	+	+	+	-	-	-
60	+	+	-	-	-	-
80	+	-	-	-	-	-
100	+	+	-	-	-	-
125	+	-	-	-	-	-
250	+	-	-	-	-	-
500	-	-	-	-	-	-
1000	-	-	-	-	-	-
2000	-	-	-	-	-	-

Table 3.4: Multiple interruptions and different length of interruptions in audio stream – simulation results with PESQ value less than four are marked with '-'.

Table 3.4 presents the PESQ simulation results depending on the length of interruption and the amount of multiple interruptions within the audio stream with a PESQ value of less than four. The corresponding fields with a PESQ value less than four are marked with '-' whereas PESQ values greater than four are marked with '+' in Table 3.4. In general, this simulation series shows that the speech quality is affected by multiple interruptions within an audio stream depending on the length of the interruption.

Table 3.5 shows the relationship between the number of interruptions in the audio stream and the time until another interruption occurs. The duration between multiple MPIs is called time between interruption (TBI) and is depicted in Table 3.5.

x of MPI	2	3	4	5	6	7
TBI [s]	47	23.5	15.6	11.7	9.4	7.8

Table 3.5: Duration among interruptions depending on the amount of interruptions in audio stream.

On the one hand Table 3.4 shows that interruptions of less than 40 ms do not lead to a speech quality with PESQ of less than four even if the amount of interruptions is greater than five. The amount of five interruptions within the audio stream corresponds to a time between interruptions of 11.7 s, as shown in Table 3.5. On the other hand it is shown that interruptions greater than 40 ms can lead to a speech quality with PESQ greater than four if the interval of interruption is greater than 11,7 s.

Concerning the carrier grade speech quality Figure 3.5 depicts the speech quality behaviour depending on the length of interruption expressed in PESQ. The time between interruptions is 11.7 s. The speech quality goes below the PESQ value of four if the length of interruption is greater than 40 ms.

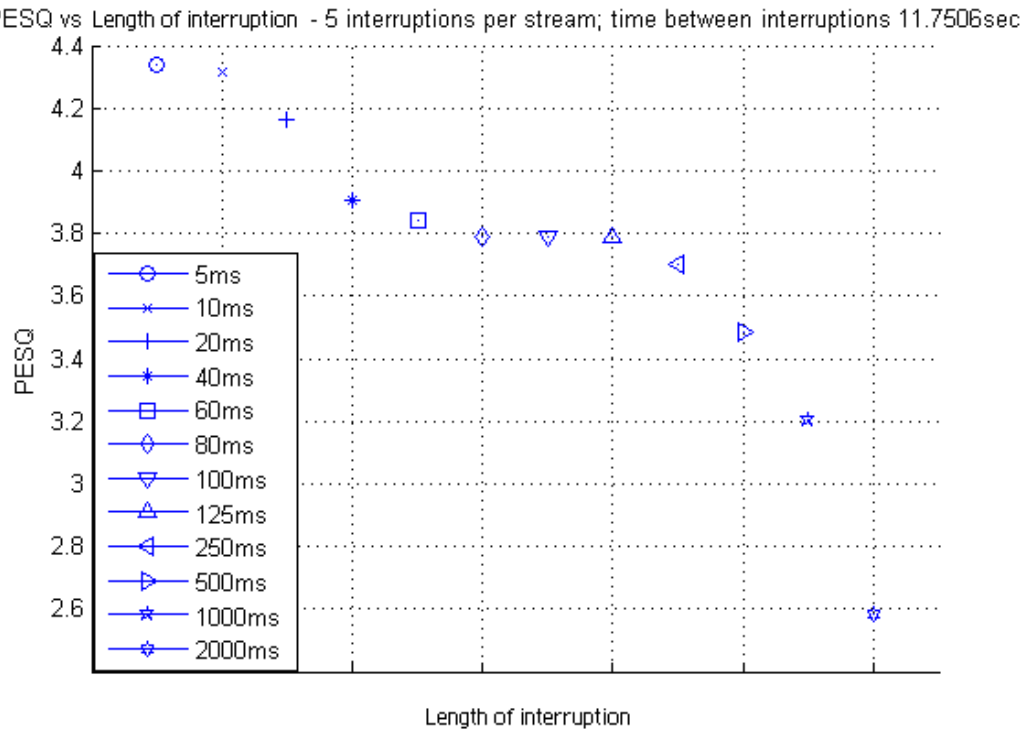


Figure 3.5: PESQ value in case of five audio stream interruptions, TBI = 11.7 s.

Comparing the results of PESQ simulation with single and multiple interruptions within an audio stream leads to a general statement that multiple interruptions influence the PESQ value and therefore the speech quality more that single interruptions of the same length.

A conclusion of Table 3.4 is that interruptions of less than 40 ms do not influence the speech quality in a significant manner. In this case, the PESQ value is greater than four, which means that carrier grade speech quality is given. With regard to a

handover scenario in WLAN this leads to the assumption that handover interruptions of less than 40 ms will not affect the speech quality even in the case of a high frequency of handovers.

Another conclusion is that interruptions of up to 250 ms do not influence the speech quality in a significant manner if the interval of interruptions is greater than 47 s. In other words, the expected speech quality depends on the combination of the length of interruption and the amount of interruption in the audio stream. This fact is important regarding the handover scenario. In a mobility scenario a WLAN device handovers many times among multiple PoAs and thus, many interruptions occur. As a result, the velocity of the user affects the frequency of handover. A WLAN cell will be passed through in a shorter time in the case of higher velocity than in the case of lower velocity. Due to this the user velocity has a direct influence on the speech quality. This behaviour affects the WLAN architecture design as well as on the handover process. One possibility could be to deploy large WLAN cells to reduce the frequency of exchange between them. Another possibility is to improve the handover process to reduce the time of interruption. A benefit of an improved handover process would be that the frequency of handovers would no longer have such a negative effect on the network performance. In the case of handover intervals with less than 11.7 s the length of interruption should be less than 40 ms to provide a speech service of carrier grade quality.

3.3 Speech Quality Investigation based on Handover Emulation

Section 3.2 investigated the speech quality based on PESQ simulations. However, no real handover process among two PoAs was carried out; instead an audio stream was manipulated by Matlab. This section evaluates the speech quality based on PESQ as well. However, in this case an interrupted IP-based voice communication is investigated. The interrupted voice communication emulates the influence of a real handover process on the speech quality. The aim of this evaluation is to show that both investigations, the simulation and the emulation, lead to comparable speech quality and PESQ results respectively. As a result, measurements of handover time behaviour in real network environment, as described in Section 3.4, can be interpreted and compared with the simulation and emulation results.

3.3.1 Handover Emulation Measurement Setup

In the following the measurement setup to carry out handover emulation is described. The handover emulation is realised based on packet-loss integration in the IP-based communication. The measurement setup, presented in Figure 3.6, consists of three main elements the VoIP client, the traffic deformer and the VoIP server. The VoIP communication takes place between the VoIP client and the VoIP server connected by the traffic deformer. All elements are connected via cross over twisted pair cables. The packet-loss of the VoIP communication is carried out by the traffic deformer. The traffic deformer manipulates the IP-based communication and thus, the VoIP communication as well. The interruption characteristic, such as length of interruption and interruption interval, is adjusted by the traffic deformer configuration. With this setup an interrupted IP communication can be emulated that is comparable with an IP communication affected by a handover process.

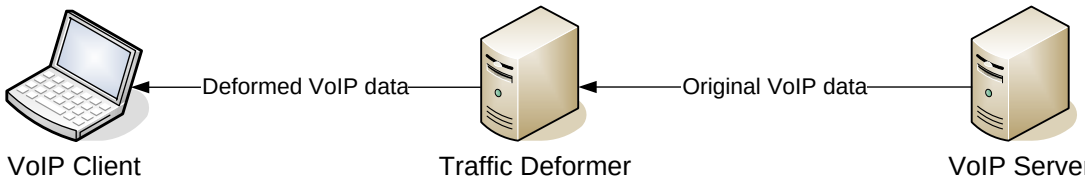


Figure 3.6: Handover emulation measurement setup.

The VoIP client is based on a notebook with Debian Linux Etch as its operation system [129] and SJPhone version 1.60.299 as VoIP software [130]. The measurements are controlled by a script. At the beginning of the script the sound card is configured to ensure a non over amplified recording. After that the script controls the softphone to setup a VoIP communication between softphone and the VoIP server while simultaneously the recording of VoIP communication is started for a defined time. The VoIP server transmits a test sequence of a reference speech conversation and the VoIP client records the VoIP communication in a WAV file. The VoIP communication as well as the recording is terminated after the defined time.

Figure 3.7 shows the structure of a VoIP packet. The VoIP packet consists of the IP header H_{IP} with 20 bytes, the user datagram protocol (UDP) header H_{UDP} with 8 bytes, the real-time transport protocol (RTP) header H_{RTP} with 12 bytes and the

voice payload PL with *n* bytes. The voice payload *n* depends on the codec. In the measurement the VoIP codec G.711 with *n* = 160 bytes is used.

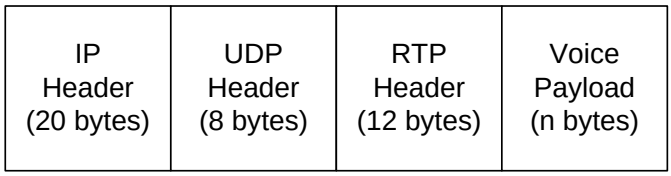


Figure 3.7: Structure of VoIP packet.

The VoIP packet size PS_{VoIP} is calculated as described by equation (3-1).

$$PS_{VoIP} = H_{IP} + H_{UDP} + H_{RTP} + PL \tag{3-1}$$

The application of codec G.711 with a bit rate of 64 Kbps has a PL of 160 bytes. Hence, with a given a PL of 160 bytes a PS_{VoIP} results as follows:

$$PS_{VoIP} = (20 + 8 + 12 + 160)bytes = 200bytes$$

To evaluate the emulated handover influence by means of the traffic deformer on the IP communication performance it is necessary to emulate a VoIP communication. The characteristic of VoIP communication is emulated using a PING series that is send to the VoIP Server. An emulated PING series that is comparable with a VoIP communication needs a PING interval of 20 ms and a PING packet size of 200 bytes. The measurement was carried out ten times with the same parameters and configuration to increase the accuracy of the results.

A PC with Debian Linux Etch and the software package Asterisk [131] establishes the VoIP server. The VoIP server is configured to accept an incoming call automatically and to return a test sequence of a reference speech conversation located in a WAV file. The measurement results of this testbed are comparable with each other result obtained.

The VoIP client and VoIP server are connected by the traffic deformer. This means the traffic deformer forwards the IP packets send from the VoIP server to the VoIP client. The task of the traffic deformers is to discard packets of the IP communication. To realise the IP forwarding capability the traffic deformer is equipped with two network interfaces. Between both network interfaces a bridge is configured. This means, that all IP packets received at one interface are forwarded via the Linux kernel to the other interface. Through the software iproute [132] it is now possible to investigate and to manipulate the IP packets. The Linux software

iproute provides many facilities to influence an IP communication. For instance, the parameters jitter, delay, bandwidth and packet-loss can be configured to affect the IP communication. This feature is used by the traffic deformer to manipulate the IP communication. The traffic deformer is also used to simulate packet-loss. This enables it to emulate IP communication interruptions. The length of interruptions as well as the interval of interruption is configurable. As a result, a VoIP communication that is affected by a WLAN handover process is emulated based on the inserted packet-loss by means of the traffic deformer. Thus, the influence of interruptions on speech quality can be investigated even without the need to carry out a real WLAN handover process in the measurement setup. The emulated handover interruptions in the IP communication are based on the parameters shown in Table 3.6 and Table 3.7. The emulated time between interruptions (TBI) is listed in Table 3.6. The handover emulation series with TBI, e.g. 5 s is performed with different length of interruptions per emulation cycle.

TBI [s]	5	10	15	20

Table 3.6: Interval of communication interruption.

The different investigated length of interruptions are presented in Table 3.7.

LI [ms]	5	10	20	40	60	80	100	125	250	500	1000	2000

Table 3.7: Length of interruption in communication.

Different length and intervals of IP communication interruptions have influence on VoIP quality. The simulated interruptions in IP communication in this measurement are comparable with the influence of a handover process in WLAN on the VoIP quality. In comparison to Section 3.2 this investigation considers real IP network transmission behaviours. In Section 3.2 the determined speech quality is based on a manipulated audio stream with silence sequences inserted. In contrast to this these investigations, this section now considers real IP-based network communication that transmits the speech service. This means that the influence of IP packet transmission on speech quality is included as well. The results of this measurement provide the base to interpret the influence of a real WLAN handover process on speech quality. For that purpose real WLAN handover performance measurements regarding IP connectivity interruption are investigated in the context of the results of these measurements. As in Section 3.2 the PESQ method is used to

determine the speech quality. The transmitted and manipulated VoIP communication is recorded by the VoIP client. Afterwards, the PESQ method is applied to obtain the speech quality.

3.3.2 Measurement Results of Handover Emulation

The measurement results of handover emulation based on manipulated IP communication is presented in this subsection. The determination of the speech quality and expressed as PESQ value is performed as described in Section 3.2.1. The PESQ value is derived by comparing the original VoIP sequence with the transmitted and manipulated VoIP sequence. Figure 3.8, Figure 3.9, Figure 3.10 and Figure 3.11 show the determined PESQ values depending on the different LIs and the interval of interruptions. Figure 3.8 shows the graph of speech quality depending on the different length of interruptions, as listed in Table 3.7, and an interval of interruption of 5 s.

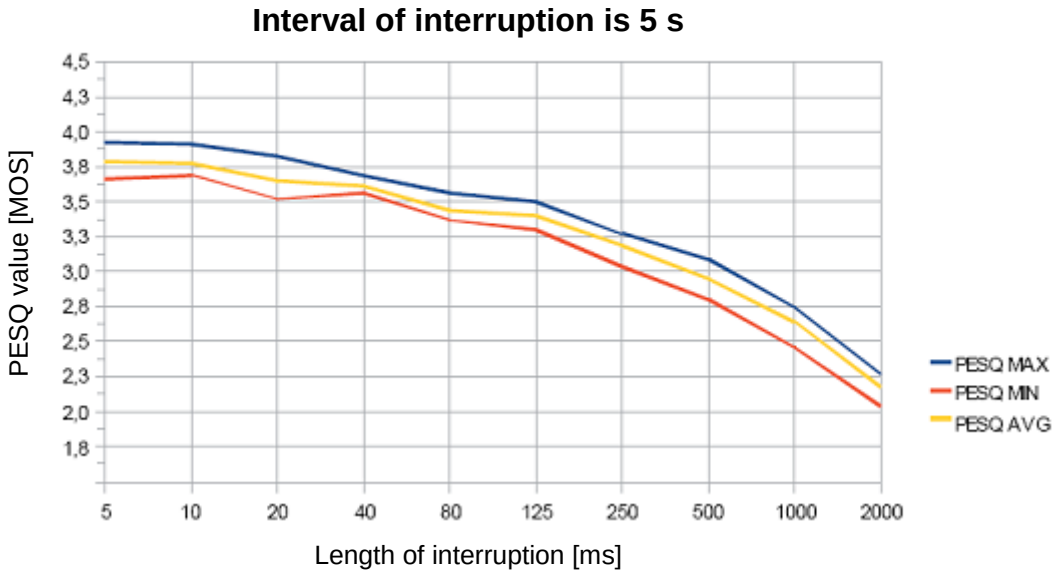


Figure 3.8: Influence of communication interruption interval of 5 s on speech quality.

Figure 3.9 shows the graph of speech quality depending on different length of interruptions, as listed in Table 3.7, and an interval of interruption of 10 s.

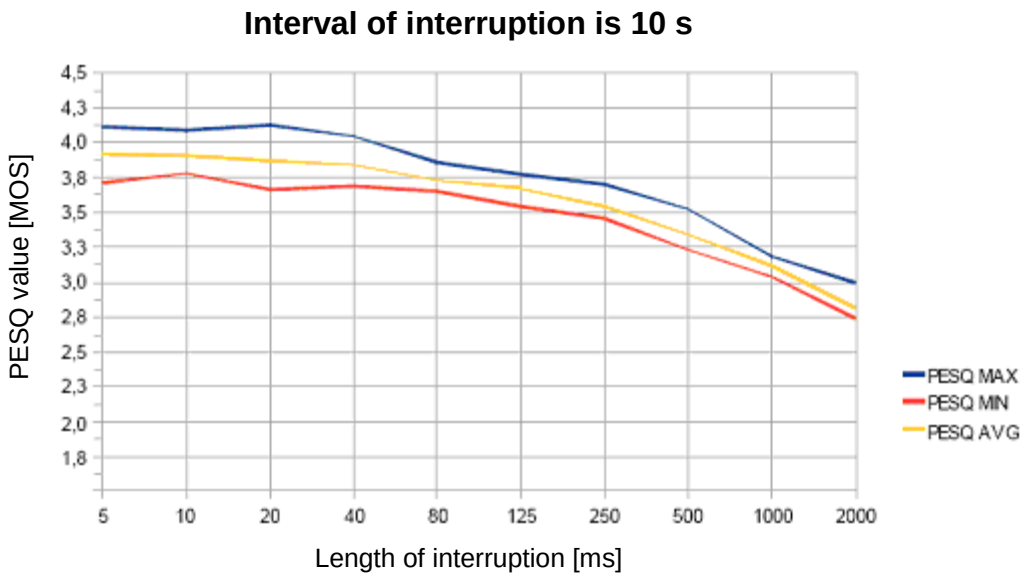


Figure 3.9: Influence of communication interruption interval of 10 s on speech quality.

Figure 3.10 shows the graph of speech quality depending on different length of interruptions, as listed in Table 3.7, and an interval of interruption of 15 s.

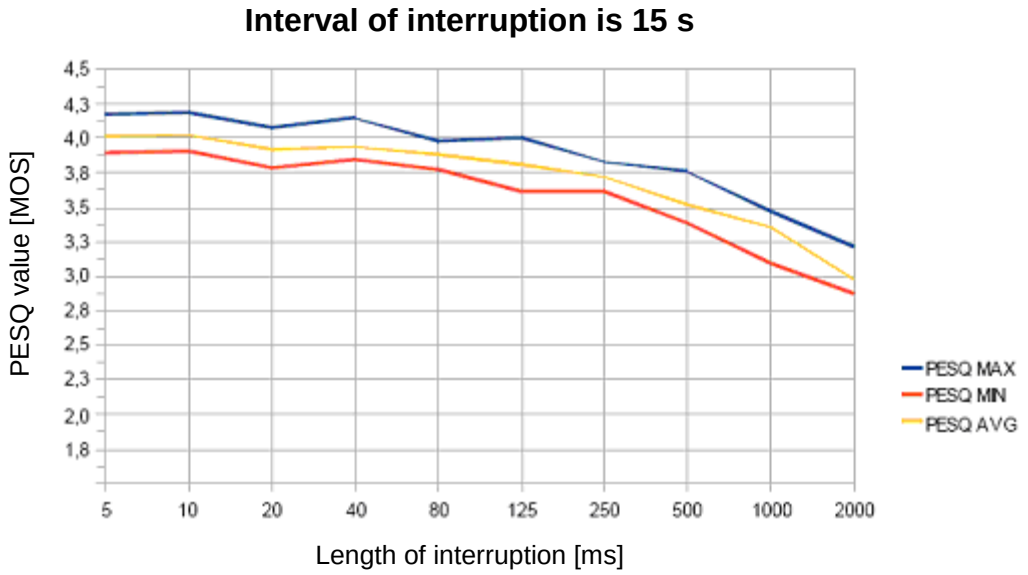


Figure 3.10: Influence of communication interruption interval of 15 s on speech quality.

Figure 3.11 shows the graph of speech quality depending on different length of interruptions, as listed in Table 3.7, and an interval of interruption of 20 s.

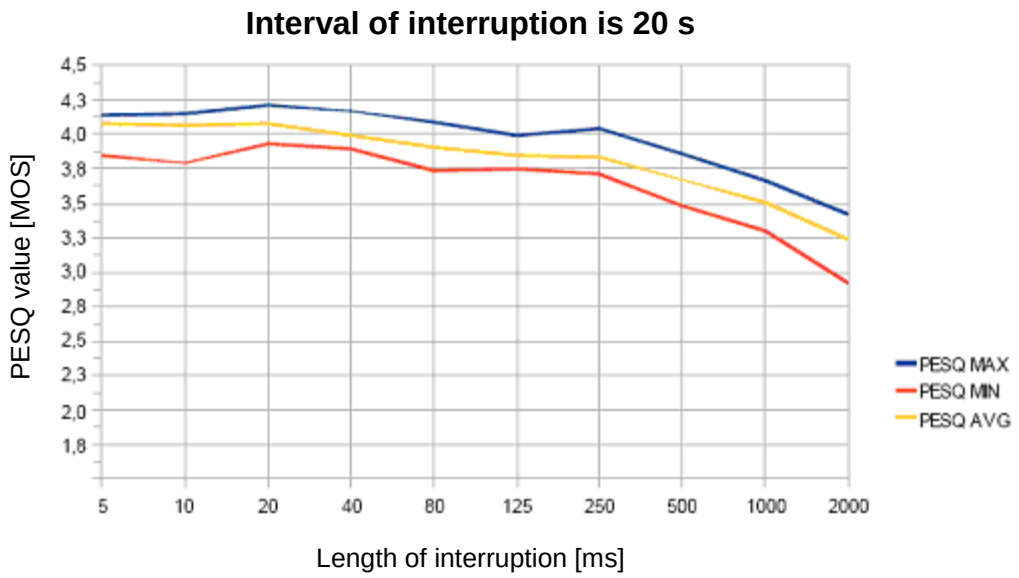


Figure 3.11: Influence of communication interruption interval of 20 s on speech quality.

The results presented in Figure 3.8, Figure 3.9, Figure 3.10 and Figure 3.11 are comparable with the PESQ simulations results of Section 3.1 and show a similar speech quality depending on the length and the interval of interruption. As expected the speech quality is less influenced by larger intervals of interruption. However, in contrast of the results of Section 3.1 interruptions of up to 40 ms have a more significant influence on the speech quality. Investigations in Section 3.1 showed PESQ values above 4.3 with a length of interruptions of 5 ms. In contrast to the results of Section 3.1 the Figure 3.8, Figure 3.9, Figure 3.10 and Figure 3.11 show that the speech quality level with a PESQ value of 4.3 is not reached. The maximum PESQ value achieved is 4.2 with a length of interruption of 20 ms and interval of interruption of 20 s, as shown in Figure 3.11. The average PESQ value is near 4.1 by length of interruption 5 ms, 10 ms and 20 ms. Moreover, Figure 3.8 and Figure 3.9 show that the speech quality of carrier grade quality, with PESQ values larger than four, are not reached in the case of interruption intervals of 5 s and 10 s. Figure 3.8, Figure 3.9, Figure 3.10 and Figure 3.11 show that length of interruptions smaller than 80 ms have a low impact on the speech quality. However, length of interruptions greater than 125 ms have an significant influence on the speech quality.

Table 3.8 shows the speech quality results depending on the length and the interval of interruption that fulfils the requirements of carrier grade speech quality. Achieved carrier grade speech quality is represented by ‘+’. This means, the

corresponding fields with an average PESQ value greater than four are marked with '+', whereas average PESQ values less than four are marked with '-', as shown in Table 3.8. Moreover, Table 3.8 shows that carrier grade speech quality is reached with interruption intervals greater than 15 s and the length of interruption less than 10 ms.

TBI [s] / LI [ms]	20	15	10	5
5	+	+	-	-
10	+	+	-	-
20	+	-	-	-
40	-	-	-	-
60	-	-	-	-
80	-	-	-	-
100	-	-	-	-
125	-	-	-	-
250	-	-	-	-
500	-	-	-	-
1000	-	-	-	-
2000	-	-	-	-

Table 3.8: Speech quality depending on different length and interval of interruptions in IP communication – results with PESQ value less than four are marked with '-'.

The grey fields in Table 3.8 represent the simulation results with PESQ values greater than four of Section 3.1. Compared to the PESQ simulation results of Section 3.1 the PESQ results of this section are worse. This highlights that that interruptions of IP based communication affects the speech quality more than in the simulated interruption as described in Section 3.1. However, the results of both investigations are comparable to each other. The speech quality behaves in the same manner depending of the length of interruption and the interval of interruption. Only the speech quality of the real IP based communication is more affected than the speech quality of the interrupted audio stream of the simulation in Section 3.1. However, this awareness is important when real handover processes in WLANs are evaluated. It is important to keep in mind that a comparable interval of interruption and equal length of interruption in IP based communication leads to a stronger degradation of the speech quality than the simulation results of Section 3.1.

3.4 Handover Time Behaviour in Secured Wireless LANs

The integration of security mechanisms in wireless communication introduces data overhead and increased data transmission delay [133]. Furthermore, security

mechanisms influence VoIP quality as described in [134] derived from PESQ investigation of voice communication. In this section the influence of network security mechanisms on the WLAN handover time behaviour in a real network environment is investigated. Beside enterprise security mechanisms security mechanisms often used in private environments are evaluated in this context. Derived from the results, the influence of handover time on voice quality is concluded.

In wired networks access is restricted to specific network socket outlets. This behaviour is different in wireless networks. The wireless medium can be accessed by each wireless node independent of the wireless node type, such as wireless station or wireless client. Hence, the interception of transmitted data by a malicious node is possible. A requirement of carrier grade access networks is the ability to control network access and to provide confidentiality of the transferred data. To avoid interception and mutation of wireless transferred data several security mechanisms have been developed. The first security mechanism is wired equivalent privacy (WEP) as part of the IEEE 802.11 standard [58]. Weak spots of WEP have been overcome by the WEP successor IEEE 802.11i standard [74]. As a fetch-ahead and subset of 802.11i the Wi-Fi Alliance has been defined Wi-Fi protected access (WPA) to overcome WEP weak spots at early stage of 802.11i standardisation [135]. WPA2 provides government grade security [136] based on the ratified IEEE 802.11i standard. The original Wi-Fi Alliance statement concerning government grade security is available in Appendix A.6.

Today's most securing mechanisms for WLAN architectures are specified by the IEEE 802.11i standard. A subset of IEEE 802.11i specifications are comprised in the Wi-Fi Alliance specification WPA2. The Federal Office for Information Security (BSI) of Germany advises in [76] the employment of WPA2 in WLANs to achieve a secure wireless network. From today's point of view WPA2 utilises the strongest algorithms to carry out encryption and to provide data integrity. Weaker mechanisms than WPA2 should not be used in wireless networks any longer [ibid]. A 104-bit key used with the mechanism WEP for WLAN encryption can be hacked in less than one minute as described in [137]. The hack on WEP can be carried out by means of the 802.11 WEP and WPA-PSK key cracking program Aircrack [138] extended by the method described by [139] of Technische Universität Darmstadt.

Even if WEP encryption should no longer be used to setup a secure WLAN connection the carried out measurement series with WEP encryption provides an important reference value of WLAN card configuration time in the case of a handover process. This reference value of WLAN card configuration time is important for the further investigation and comparison of WLAN card handover behaviour when using other security mechanisms, such as WPA2. Table 3.9 presents an overview of currently existing WLAN security mechanisms as well as the applied authentication and key management mechanisms. The following security mechanisms have been investigated: WEP, WPA2 PSK and WPA2 EAP-TLS.

Mechanism	Authentication	Key management
WEP	Shared key	None
WPA	IEEE 802.1X	IEEE 802.1X
WPA2/IEEE 802.11i	IEEE 802.1X	IEEE 802.1X

Table 3.9: Overview of existing WLAN security and network access control mechanisms.

A WLAN card in the device is needed to connect to the WLAN. However, before getting connected to the WLAN the wireless LAN card has to be configured. The tools used to configure the WLAN card on the operation system Linux are iwconfig [140] and wpa_supplicant [141]. Iwconfig and wpa_supplicant can be applied to configure a WEP secured WLAN link. However, the setup of a WPA or WPA2 secured WLAN link is only possible by means of the tool wpa_supplicant. The reason that iwconfig can only be applied for WEP is that WLAN encryption mechanisms unequal to the WEP method require additional authentication mechanisms. Due to this the tool wpa_supplicant is used for WPA2 PSK and WPA2 EAP-TLS encryption and authentication as well.

The tool iwconfing passes in the WLAN card configuration process the WEP key and the SSID directly to the driver. Unlike iwconfig the configuration tool wpa_supplicant configures the WLAN card driver indirectly. The main focus of wpa_supplicant is to provide the role of the supplicant in the IEEE 802.1X authentication process. To configure the WLAN card wpa_supplicant uses an extra interface to the driver. In this measurement iwconfig and wpa_supplicant are used to investigate the influence of different software implementations on the wireless card configuration time and thus, on the IP communication interruption time in a handover process. The comparison of both tools is carried out with a WEP based

WLAN link encryption. This allows a direct comparison of WLAN card configuration time behaviour in a WEP based handover process. Furthermore, the influence on the IP communication interruption time depending on the used tool can be pointed out.

3.4.1 Handover Measurement Setup in IEEE 802.11

The investigation consists of three different measurement setups. Each measurement setup consists of two APs to connect the user equipment to the network. The used APs are LINKSYS [142] WRT54G applying the DD-WRT [143] firmware in version 23. Furthermore, a communication server (CS) is integrated within the measurement setup that represents the communication partner of the UE to carry out VoIP or ping communication. A hub connects the APs and the servers in the measurement setup. Moreover, a wireless analyser AirPcap [144] is used consisting of a WLAN dongle and Laptop.

AirPcap works in promiscuous mode that enables it to capture all wireless 802.11 link data. In collaboration with the network analyser WIRESHARK [145] the WLAN adapter AirPcap provides a detailed view of the 802.11 traffic, such as the control frames (ACK, RTS, CTS), the management frames (beacon, probe requests and responses, association and disassociation, authentication and de-authentication) as well as the data frames. The captured frames include the 802.11 frame check sequence (FCS). To identify remote wireless stations with a weak signal it is possible to capture frames with an invalid FCS as well.

Figure 3.12 presents the measurement setup to investigate the security mechanisms WEP and WPA2-PSK. In this setup the network access is controlled by the AP and depends on the pre-shared key (PSK) that is configured in the AP and the UE. Network access is granted only for UEs with valid configured PSKs. In the PSK scenario no additional authentication and authorisation server is required to perform user authentication or authorisation. The PSK method is often used in private WLAN environments.

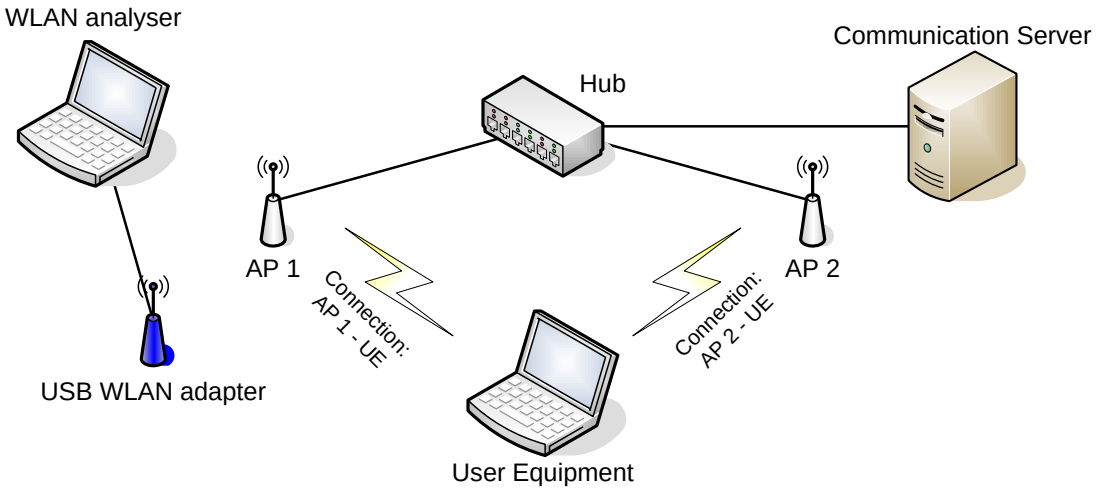


Figure 3.12: Handover measurement setup with WEP and WPA2-PSK encryption.

The measurement setup shown in Figure 3.13 is based on the setup as presented in Figure 3.12, however, with an additional AAA server to carry out UE authentication and authorisation. This AAA server is necessary when applying the security mechanism WPA2 EAP-TLS with certificates. WPA2 EAP-TLS is currently the most secure mechanism to setup a secured WLAN environment and is recommended by the Federal Office for Information Security (BSI) of Germany in [76]. WPA2 EAP-TLS is most often used in WLAN enterprise solutions to provide a secure and flexible management WLAN infrastructure. In this measurement setup the local AAA (LAAA) server is located within the local WLAN environment.

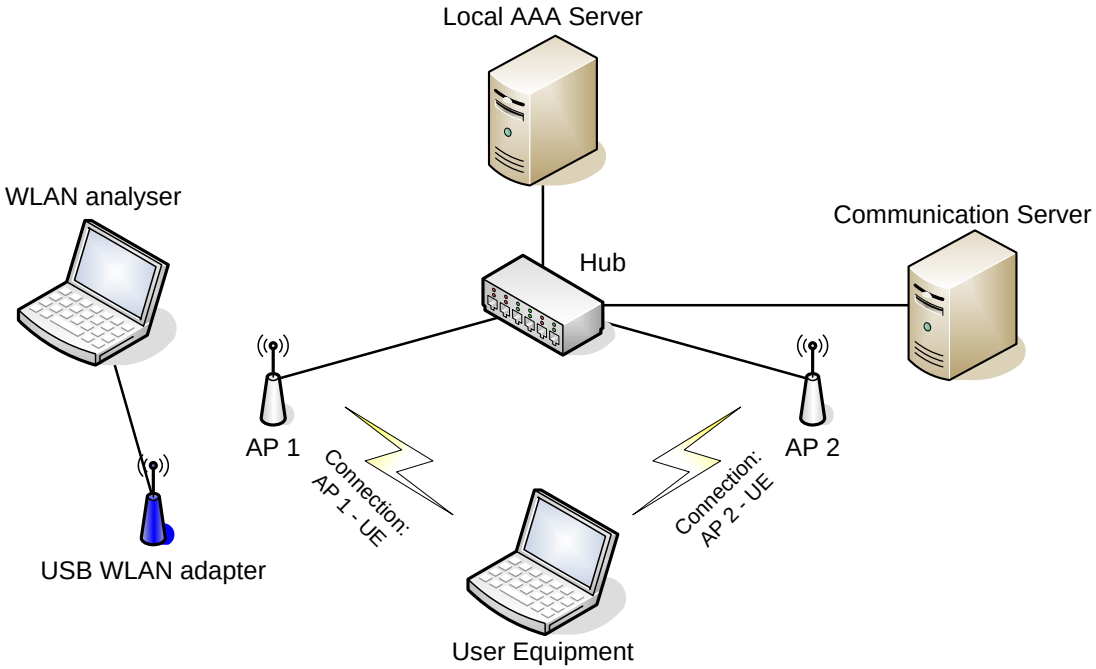


Figure 3.13: Handover measurement setup with WPA2 EAP-TLS authentication – local AAA server.

The difference between the measurement setup in Figure 3.13 and Figure 3.14 is the location of the AAA server. The external AAA (EAAA) server as shown in Figure 3.14 is located within a remote network. This scenario is more realistic in comparison to the scenario presented in Figure 3.13. In enterprise network architectures often different geographical location independent network segments are connected via the Internet. This behaviour is emulated with the measurement setup in Figure 3.14. By means of the measurement setup presented in Figure 3.13 and Figure 3.14 different authentication and authorisation scenarios with different locations of the AAA entity are emulated. The LAAA is used to carry out UE authentication and authorisation within the local network, while the EAAA is used to carry out UE authentication and authorisation within a remote network. Both locations of AAA servers are important to investigate the influence of different AAA entity locations on the authentication time behaviour when using the security mechanism WPA2 EAP-TLS. Details about the AP configuration utilizing WEP and WPA2 (EAP-TLS) method is described in Appendix A.2.

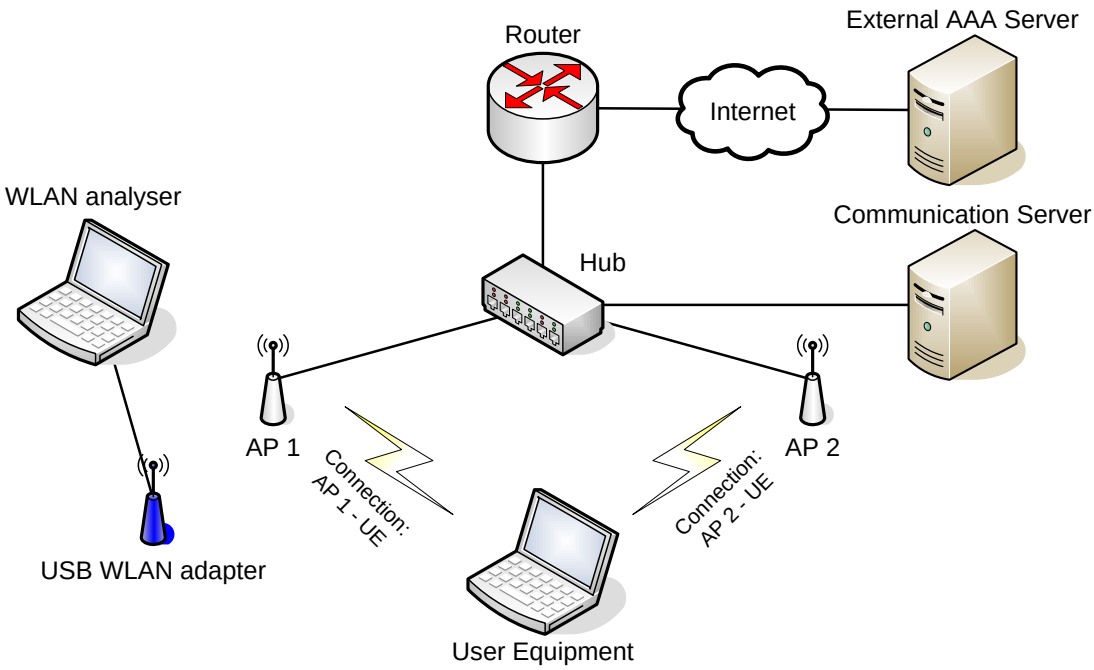


Figure 3.14: Handover measurement setup with WPA2 EAP-TLS authentication – external AAA server.

3.4.2 Measurement Preparations

The UE in the IEEE 802.11 standard sends probe messages to scan actively for surrounding APs. However, this scanning process introduces additional interruption

time in the handover process [57]. This work will focus on the authentication time improvement when using the authentication mechanism WPA2 EAP-TLS. To investigate the handover process without the influence of the scanning process the scanning process of the WLAN card has to be avoided. By means of a patch [146] the Madwifi driver v0.9.4 [147] was changed to prevent starting of UE scanning process in all WLAN channels to search for surrounding APs during connection interruptions. The previously used channel is kept for further connections. Thus, the scan process can be avoided within the handover process. Further wireless card configuration information is described in Appendix A.3.

The handover measurement is controlled by a script on the UE. Before a handover is initiated the script starts a traffic trace by means of TCPDUMP that captures all network communications sent and received by the UE. After that, the script starts a ping series. The ping is carried out in the interval of 10 ms for a duration of 1 s. Ping intervals of less than 10 ms do not lead to more detailed results. Each series of handover measurements has been carried out 100 times.

The handover interval is configured in the script as well. The script controls the handover by re-configuration of the UE wireless interface to connect to the AP 1 and AP 2 respectively. Through this the service set identifier (SSID), the wireless channel, the key (in the case of WEP method) as well as the extended service set identifier (ESSID) is configured. Furthermore, the background scanning functionality of the wireless interface is disabled. Based on this configuration the UE carries out a handover from one AP to the other AP. Only a single connection between UE and APs is established, meaning that no connection to AP 1 and AP 2 is established at the same time. The evaluation of the communication is carried out by means of WIRESHARK as presented in the following sections.

3.4.3 Investigation of Handover Time Behaviour

In the following the communication interruption time is used synonymously for handover time. The fundamental equation to describe the handover time is represented by two parameters shown in (3.1).

$$T_{handover} = T_{configuration} + T_{authentication} \tag{3.1}$$

The handover time $T_{handover}$ is described by the configuration time $T_{configuration}$ and the authentication time $T_{authentication}$. The time needed to re-establish the IP connectivity after the handover is called the configuration time of the wireless card. The time needed to carry out UE authentication with additional AAA entities to get network access is the authentication time. A detailed investigation of communication interruption leading to the interruption time is carried out using the network analyser WIRESHARK analysing the TCPDUMP communication trace of the different measurement series. The handover time measurements consisting of the configuration time and the authentication time are presented in Figure 3.15.

3.4.4 WEP Investigations of Handover Time Behaviour

The first handover measurement series focuses on WEP encryption and investigates the influence of the wireless card configuration tools iwconfig and wpa_supplicant on handover performance. Table 3.10 shows the handover performance results depending on whether iwconfig or wpa_supplicant was used. The interruption time is determined by the time difference between the last received ping reply before the handover has taken place and the first successfully answered ping request after the handover.

	iwconfig	wpa_supplicant
min	45 ms	254 ms
avg	90 ms	300 ms
max	130 ms	352 ms

Table 3.10: Communication interruption depending on tool iwconfig and wpa_supplicant – WEP encryption.

Table 3.10 presents the minimum, average and maximum communication interruption times using WEP encryption. It is shown that the use of different wireless configuration tools influences the handover time behaviour. Comparing the maximum interruption time of both wireless card configuration tools the wpa_supplicant requires up to 222 ms longer to re-establish the IP data connectivity before a communication between UE and CS is possible. This behaviour is founded in the different implementations and functionalities of the tools. Iwconfig interacts via the application programming interface wireless extension with the driver to configure the wireless parameters. This behaviour is different in the wpa_supplicant. The wpa_supplicant is a daemon program that runs in the background and controls

the whole wireless connection. The wpa_supplicant is the supplicant component of IEEE 802.1X / WPA within the client station. The supplicant performs the key negotiation with a WPA authenticator and it can optionally control roaming and IEEE 802.11 authentication/association of the WLAN driver [148]. During the controlling process different state machines, such as the WPA/WPA2 state machine, the EAPoL state machine and the EAP state machine have to be passed depending on the applied security and network access control method in the WLAN. These control processes have an effect on the computation time and thus, on the additional interruption time. A determination of communication interruption times are described in Appendix A.4.

WEP uses no authentication process that requires the interaction of the AP with an authentication server. This means that the handover time consist of the configuration time only. Due to this the (3.1) is reduced to

$$T_{handover} = T_{configuration} \tag{3.2}$$

3.4.5 WPA2 Investigations of Handover Time Behaviour

In most mobility scenarios a customer covers a distance and moves from location A to location B. In other words, the UE handover from the AP at location A each time to new APs while moving from location A into the direction of location B. This means, the UE has not been connected to one of these APs before. This movement characteristic is important for the handover time investigation and has to be considered in the measurement setup. In short the IEEE 802.1X EAP-TLS mechanism derives key material to encrypt the communication. The derivation of the key material evokes handshakes between UE and authentication server. The running periods of these handshakes are a major factor that influences the handover time. In the case of the re-connection to an AP that knows the UE's valid key due to a previous authentication process, no new key derivation is needed. As a result, no new authentication process is initiated by the AP and no handshakes between the UE and the authentication server occurs. For this reason it is important to prepare the measurement setup that a full authentication process with key derivation is carried out for each handover process. This behaviour has been emulated by rebooting the APs. For that purpose the old AP will be rebooted after the handover from the old

AP to the new AP. Due to this all previously derived encryption keys in the old AP are deleted. The next handover of the UE to this rebooted AP requires a full authentication process with key derivation. Thus, the handover time influencing a mobility scenario has been emulated.

The next measurements investigate the handover time behaviour when using WPA2 with EAP-TLS or WPA2 with EAP-PSK. WPA2 with EAP-TLS defines IEEE 802.1X to carry out authentication. The handover time will consist of the configuration time and the authentication time as described in (3.1). Four authentication scenarios have been investigated in this context. The first scenario in a) focuses on the RADIUS authentication server within the local network as shown in Figure 3.13 and the second scenario in b) focuses on the RADIUS authentication server within an external network as presented in Figure 3.14. The third scenario in c) focuses on an EAP-TLS re-keying without full EAP-TLS authentication process, while the fourth scenario in d) focuses on an EAP-PSK authentication process.

a) WPA2 encryption and EAP-TLS authentication with local AAA server

This measurement investigates the handover time behaviour when using WPA2 with EAP-TLS in the authentication scenario with a local AAA server as depicted in Figure 3.13. Table 3.11 presents the minimum, average and the maximum of WPA2 EAP-TLS handover time in the local authentication scenario. In contrast to the WEP based handover time the WPA2 EAP-TLS based handover time consists of configuration and authentication time. The comparison of wpa_supplicant configuration time in Table 3.10 and Table 3.11 provides similar results. This means that the encryption mechanism used does not influence the configuration time of the wireless card. However, in Table 3.11 it is shown that the use of WPA2 with EAP-TLS evokes additional authentication time with up to 129 ms. This additional authentication time is based on the authentication process that consists of the handshakes between AP and local AAA server. Details about the determination of communication interruptions times are described in Appendix A.5.

	Configuration time	Authentication time
Min	248 ms	87 ms
Avg	290 ms	95 ms
Max	338 ms	129 ms

Table 3.11: Handover configuration and authentication time using WPA2 with EAP-TLS – local AAA server.

WPA2 EAP-TLS comprises of an authentication process that requires the interaction among UE and AAA server as well as among PoA and AAA server. As a result, the handover time consist of the configuration time and the authentication time as described in (3.1) and shown in Table 3.11.

b) WPA2 encryption and EAP-TLS authentication with external AAA server

The next measurement investigates the handover time behaviour when using WPA2 with EAP-TLS in the authentication scenario with an external AAA server as depicted in Figure 3.14. In comparison to the authentication scenario a) with a local AAA server the external authentication scenario represents a more common authentication scenario from a network providers point of view, because the user authentication data are stored centralised within the network provider's AAA server. In this scenario the access network and thus, the PoA is connected via the Internet with the network providers management platform and the AAA entity as well.

Table 3.12 presents the minimum, average and maximum of WPA2 EAP-TLS handover time in the external authentication scenario. The comparison of the authentication time in Table 3.11 and the authentication time in Table 3.12 shows the strong influence of the running period of authentication messages through the Internet on the authentication time behaviour. The authentication time is up to 538 ms. Details showing the determination of communication interruptions times are described in Appendix A.5.

	Configuration time	Authentication time
Min	246 ms	449 ms
Avg	278 ms	494 ms
Max	336 ms	538 ms

Table 3.12: Handover configuration and authentication time using WPA2 with EAP-TLS – external AAA server.

The resulting handover time consisting of the configuration time and the authentication time as described in (3.1).

c) WPA2 encryption without full EAP-TLS authentication process

The following measurement investigates the handover process in the case of a UE reconnect to an AP that knows the valid key based on a previous authentication process. As the key is known no full EAP-TLS authentication is necessary; merely a rekeying has to be performed. To replicate the rekeying process the APs are not rebooted after the handover to keep the previously derived key.

In comparison to the authentication time in the local and external EAP-TLS authentication scenario, shown in Table 3.11 and Table 3.12, the authentication time in Table 3.13 occurs due to the re-key process only. In this measurement scenario no certificate exchange among UE and AAA server takes place, only the four-way handshake among UE and PoA is needed. Unlike the full authentication process the re-keying process leads to a reduced authentication time of up to 18 ms, as shown in Table 3.13. This means the packet loss without a full EAP-TLS authentication process is comparable with the packet loss in a WEP based link encryption using wpa_supplicant. Details about the determination of communication interruptions times are described in Appendix A.5. Independent of the reduced authentication time the handover time consists of the configuration time and the authentication time as described in (3.1).

	Configuration time	Authentication time
Min	245 ms	11 ms
Avg	286 ms	17 ms
Max	335 ms	18 ms

Table 3.13: Handover configuration and authentication time using WPA2 EAP-TLS without authentication process; no AP reboot

d) WPA2 encryption with EAP-PSK authentication

Unlike the authentication and key derivation process of WPA2 with EAP-TLS the mechanism WPA2 PSK requires no interaction between the UE and AAA server and between the PoA and AAA server respectively. The key derivation process in WPA2 with EAP-TLS is based on the TLS handshake [149] in conjunction with client and server certificates and the key distribution made by the AAA server. In comparison to this process the key derivation process in WPA2 PSK uses a pre-shared key configured in the configuration file of PoA and UE. To confirm the investigations of WPA2 with EAP-TLS in a local and an external authentication scenario the mechanism WPA2 PSK is investigated as well. Comparable handover time behaviour as in the WPA2 with EAP-TLS scenario without full EAP-TLS authentication is expected because only a re-keying process is performed. Details about the determination of communication interruptions times are described in Appendix A.5.

The measurement results are presented in Table 3.14. As expected the authentication time is in the range of the WPA2 with EAP-TLS scenario without

performing the full EAP-TLS authentication process. The maximum authentication time is 30 ms whereas the average authentication is 18 ms. Again the handover time consists of the configuration time and the authentication time as described in (3.1).

	Configuration time	Authentication time
Min	243 ms	10 ms
Avg	282 ms	18 ms
Max	334 ms	30 ms

Table 3.14: Handover configuration and authentication time using WPA2 PSK.

3.4.6 Summary of Handover Time Behaviour Investigations

Figure 3.15 summarises all handover measurement results of the investigated encryption and authentication mechanisms. The dark marked part of the bar presents the configuration time needed to configure the wireless card depending on the used configuration tool iwconfig or wpa_supplicant. The bright marked part of the bar presents the authentication time required to carry out UE authentication, authorisation and key derivation to get network access.

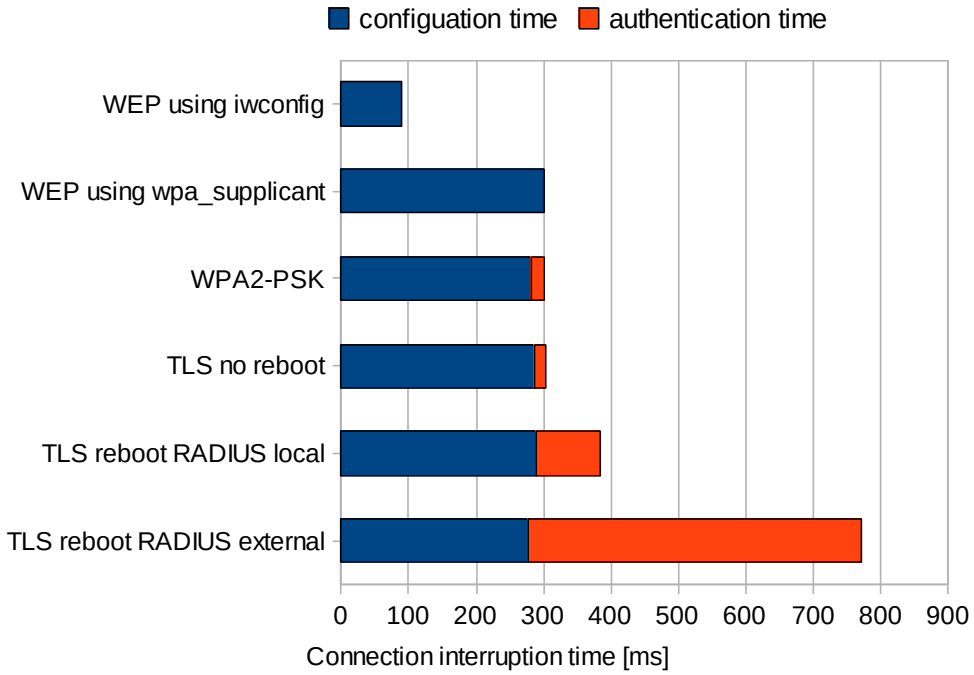


Figure 3.15: Handover time behaviour measurement results.

Figure 3.15 shows the influence of different wireless configuration tools, such as iwconfig and wpa_supplicant on the handover performance in the case of WEP encryption. Iwconfig consumes in average 90 ms to configure the wireless card. The wpa_supplicant requires up to 222 ms longer to re-establish the IP connectivity

before any communication between the UE and communication server is possible. Moreover, in Figure 3.15 it is shown that the WEP based handover process comprises of no authentication time, it solely uses the configuration time of the wireless card. This means that the WEP mechanism requires no interaction of the AP with an authentication server.

The WPA2 PSK mechanism uses the pre-shared key which is stored in the UE and the AP to perform network access control. This means that no interaction between AP and AAA Server to exchange authentication information is needed. The average authentication time of WPA2 PSK is 18 ms. The authentication time results only from the four way handshake needed between UE and AP to exchange the encryption keys.

The authentication time of WPA2 EAP-TLS, but no AP reboot, is comparable to the authentication time of WPA2 PSK, as shown in Figure 3.15. This behaviour is based on the fact that the AP stores information and keys of previously connected UE. In the case of a UE handover from the current AP to the old AP, the old AP has information about the previous connection. As a result, only a four way handshake between UE and AP is carried out to provide re-keying instead of a full authentication process.

The most connection interruption time intensive authentication and authorisation mechanism is WPA2 using EAP-TLS in conjunction with an external AAA server, as shown in Figure 3.15. The average time of authentication, authorisation and key derivation is 494 ms. This time is caused by the runtime of the required handshakes between the AP and the remote located EAAA server. A clearly shorter authentication time arises in the case of WPA2 using EAP-TLS and a local AAA server. This behaviour is due to the fact that the runtime between the AP and LAAA server is much shorter when compared to the EAAA server. In general Figure 3.15 shows the influence of authentication time on the handover time in the case of local and external EAP-TLS authentication scenarios. The external EAP-TLS authentication scenario has an average authentication time of 494 ms that leads to significant IP communication interruptions. Investigations in [56] and [150] confirm that the influence of the authentication method used on the authentication time. The authentication time varies between some milliseconds [56] and several hundred milliseconds [150]. Moreover, Figure 3.15 shows no influence of the encryption

mechanism on the configuration time. The average configuration time is 280 ms in the case of wpa_supplicant use.

3.4.7 IEEE 802.1X using EAP-TLS Method

This subsection describes the IEEE 802.1X using EAP-TLS method in detail. For that purpose the authentication process is described by means of the IEEE 802.1X using EAP-TLS sequence diagram. Figure 3.16 shows the sequence diagram of the IEEE 802.1X using EAP-TLS authentication process. The column labelled supplicant represents the client in the IEEE 802.1X scenario which is located in the user equipment. The authenticator is implemented within the access point and acts as mediator among the supplicant and AAA server. In this case the AAA server is a RADIUS server carrying out user authentication and authorisation. The communication among supplicant and authenticator is transmitted via the air while the communication among authenticator and RADIUS server is carried out by means of a wired connection. As UEs point of attachment the AP is located in the access network, while depending on the infrastructure of the network architecture the RADIUS server can be located within a remote network interconnected via the Internet. The column named access indicates the state of network access. The part ‘denied’ in the column access represents the state of non-granted network access during the authentication process. As long as the authentication process continues only the IEEE 802.1X communication among UE and AP is allowed. Full network access is granted after the successful authentication process. This state is represented by means of the part ‘allowed’ in the column access.

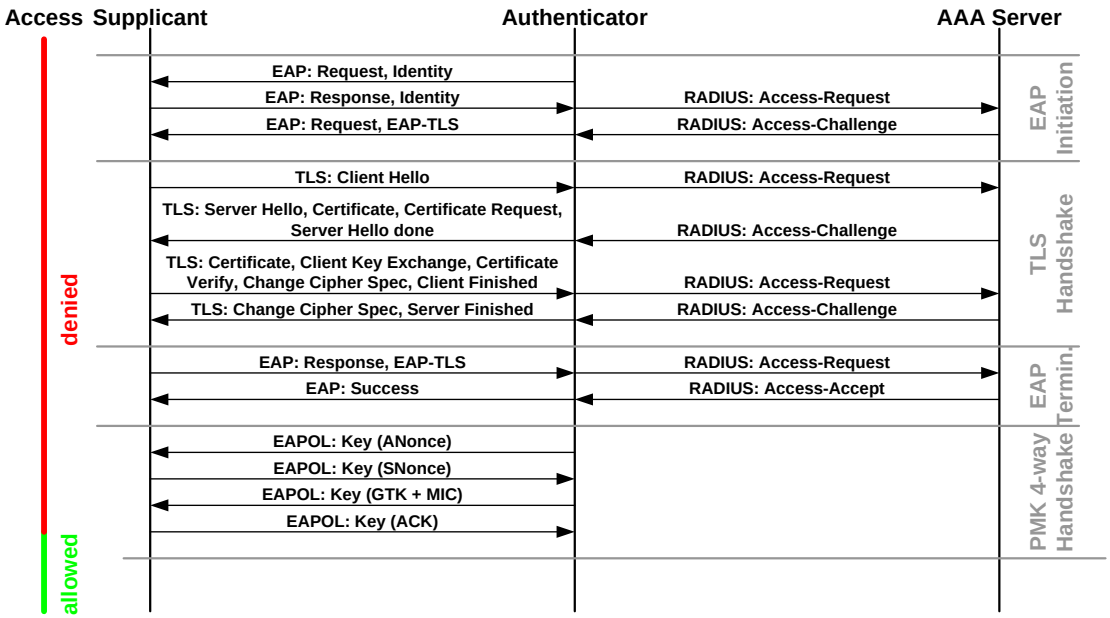


Figure 3.16: Sequence diagram of IEEE 802.1X using EAP-TLS authentication with RADIUS server

The used protocols in the authentication process shown in Figure 3.16 are: EAP, EAPoL, TLS and RADIUS.

The authentication method IEEE 802.1X with EAP-TLS consists of four sequences to carry out UE authentication and to establish a secure encrypted wireless link. The different sequences, such as EAP initiation, TLS handshake, EAP termination and PMK four-way handshake are presented in Figure 3.16 and are described as follows.

EAP initiation

The first sequence EAP initiation starts with the request of the user identity. This request is initiated by the authenticator by means of the EAP request identity packet sent to the supplicant. The answer of the supplicant is sent by means of the EAP response identity packet. This packet contains the user identity information. To carry out the authentication and authorisation process the user identity information has to be forwarded to the RADIUS server. For that purpose the authenticator wraps the user information into a RADIUS packet. This packet represents a request to the RADIUS server. Due to this reason the RADIUS packet is from the type Access-Request. Depending on the transmitted user identity the RADIUS server selects the required authentication method to initiate the authentication process. In this case the authentication method is TLS. For this reason the RADIUS server sends an Access-Challenge packet to the authenticator. The access-challenge information is forwarded by the authenticator to the supplicant by means of an EAP Request (TLS) requesting

the preferred authentication method. In this case the supplicant is configured for EAP-TLS authentication. For this reason the supplicant accepts the EAP request and initiates the TLS authentication.

TLS handshake

The second sequence starts with a TLS handshake [149] initiated by the supplicant by means of a TLS packet from the type Client Hello. This packet contains the information about the supported wireless link encryption methods as well as a random value build by the supplicant. The random value will be used to generate the premaster secret later on in the authentication process. The TLS packet from the type Client Hello as well as the following packet required to carry out TLS communication among supplicant and RADIUS server are wrapped by the authenticator into the RADIUS packet Access-Request. Vice versa the authenticator wraps the RADIUS packets Access-Challenge sent from the RADIUS server into the necessary protocol to forward the data to the supplicant. The response of the RADIUS server to the Clients Hello message consists of the following three information, Server Hello, Certificate and Certificate Request. The Server Hello information consists of the selected encryption method as well as the server random value required to generate the premaster secret. The certificate information is the server certificate. By means of the certificate the supplicant is able to verify the authenticity of the RADIUS server needed to carry out mutual authentication. To verify the authenticity of the supplicant as well the RADIUS server requests the supplicant certificate by means of the Certificate Request. The server Hello Done information indicates the end of the RADIUS server message. Consequently, the supplicant is informed that the RADIUS server has finished its information transition and is awaiting the response of the supplicant.

The supplicant answers to the previous RADIUS message with the certificate information containing the client certificate. Moreover, the premaster secret is transmitted to the RADIUS server by means of the client key exchange information. The premaster secret was previously computed by the random values of the supplicant and the RADIUS server. Furthermore, the premaster secret is encrypted by the public key of the RADIUS server certificate. The RADIUS server decrypts the encrypted premaster secret by means of its private key. By means of the premaster key and the random values of the supplicant and RADIUS server the RADIUS server

computes the session key. The session key is named master key. The certificate verify information uses the RADIUS server to verify the supplicant. The certificate verify information contains a hash value based on the previous sent information encrypted by the private key of the client. To verify the authenticity of the hash value the RADIUS server uses the public key of the transmitted client certificate. This verification process provides clarity about using the authentic private key of the client in the encryption process. The RADIUS server will be able to decrypt the hash value successfully with the public client key of the client certificate if the authentic private client key is used to encrypt the hash value. The change cipher spec information indicates that the supplicant will in future encrypt all data with the previous computed master secret. At the end a hash value based on the whole communication will be computed and transmitted by the client finish information. The client finish information is the first encrypted information. Furthermore, this information indicates that the supplicant has finished the TLS process. The end of the TLS handshake is initiated by the change cipher spec of the RADIUS server. By means of this information the RADIUS server indicates that in future all information will be encrypted by the previously computed master secret. The server finished information transmits a hash value based on the whole communication taken place and is encrypted by the master secret. If the supplicant is able to decrypt and verify the server finished information it is ascertained that the used secrets from the supplicant and RADIUS server are equal. In the case of successful verification the TLS handshake is finished as well. From now on the supplicant knows the master key also named as AAA key. The AAA key is used by the supplicant to derive the pairwise master key (PMK) required for the four way handshake. The PMK consists of the first 256 bits of the AAA key.

EAP termination

The supplicant confirms in the third sequence the successfully performed TLS authentication process by means of the EAP Response inside of the EAP-TLS packet. This packet is wrapped by the authenticator in the RADIUS access-challenge packet and is forwarded to the RADIUS server. The RADIUS server answers to the access-challenge with the RADIUS access-accept packet containing the information about the successful authentication of the supplicant and the AAA key. The authenticator receives the AAA key and sends the EAP success information to the

supplicant. By means of the AAA key the authenticator derives the PMK. Henceforward, the PMK is known by the supplicant as well as by the authenticator. Thus, the execution of the four way handshake can be initiated.

Four-way handshake

Finally, the four way handshake [74] is carried out. The first information of the four way handshake is the EAPOL key frame sent from the authenticator to the supplicant. This packet contains a random value called ANonce generated by the authenticator. The supplicant also generates a random value called SNonce. Based on the SNonce, the ANonce as well as the previously derived PMK the supplicant generates the pairwise transient key (PTK). Among others the PTK is used to derive the temporal key (TK) and the key encryption key (KEK). The PTK is necessary for data encryption. The KEK is required to distribute the group transient key (GTK). Consequently the supplicant sends an EAPOL key frame consisting of the SNonce as well as a message integrity check (MIC). From now on the authenticator knows the SNonce, the ANonce as well as the PMK and generates out of it the PTK. By means of the received MIC the authenticator verifies the validity of the last received information send by the supplicant. The authenticator answers with the GTK, the key to encrypt in future the multicast and broadcast messages as well as a demand to the supplicant to install the PTK and the GTK. Furthermore, a MIC is contained within the frame to verify the validness of this frame. In the last step of the four way handshake the supplicant confirms the installation of the GTK and PTK. Thus, the authentication and authorisation process is finished and the authenticator grants full network access of the user equipment. The state of grated network access is indicated in the part termed allowed in the column access, shown in Figure 3.16.

3.4.8 Drawbacks of IEEE 802.1X EAP-TLS Authentication Time Behaviour

This subsection analyses the authentication time behaviour of IEEE 802.1X using the EAP-TLS method. The drawback of fast authentication and authorisation using the EAP-TLS method is discussed to determine the reason of communication interruptions occurring during a handover process. For that purpose the authentication process using a local RADIUS server is investigated. A transparent overview about the authentication communication and the ping communication is depicted separately in Figure 3.17 and Figure 3.18.

No.	Time	Time Delta	Source	Destination	Protocol	Info
7	0.313	0.313	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAP	Request, Identity [RFC3748]
8	0.313	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAP	Response, Identity [RFC3748]
10	0.323	0.009	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAP	Request, EAP-TLS [RFC2716]
11	0.324	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	TLSv1	Client Hello
13	0.335	0.011	Cisco-Li_a9:1c:ff	3com_37:f7:32	TLSv1	Server Hello, Certificate,
14	0.348	0.012	3com_37:f7:32	Cisco-Li_a9:1c:ff	TLSv1	Certificate, Client Key Exc
18	0.384	0.035	Cisco-Li_a9:1c:ff	3com_37:f7:32	TLSv1	Change Cipher Spec, Encrypt
19	0.385	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAP	Response, EAP-TLS [RFC2716]
20	0.394	0.009	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAP	Success
21	0.395	0.000	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAPOL	Key
22	0.400	0.005	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAPOL	Key
24	0.404	0.003	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAPOL	Key
25	0.404	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAPOL	Key

Figure 3.17: EAP-TLS communication; local AAA server.

Figure 3.17 shows the authentication communication due to IEEE 802.1X using EAP-TLS among the UE, AP and LAAA server respectively, while Figure 3.18 presents the ping communication among the UE and CS. The dark (red) marked frame number six in Figure 3.18 shows the last successfully sent ping packet before the handover process is started. In Figure 3.17 the dark (red) marked frame number seven presents the first successfully transmitted packet after the carried out handover. The time difference between frame number six, in Figure 3.18, and frame number seven, in Figure 3.17, is 313 ms. This time difference of 313 ms corresponds to the wireless card configuration time needed to establish IP connectivity. However, there is no communication with the network possible even after the wireless card configuration. As a result, an established application communication before the handover process occurs, such as VoIP or IPTV, is not able to communicate any longer with the corresponding partner. Thus, the service provided is interrupted. Frame number 9, 12, 15, 16, 17 and 23 in Figure 3.18 presents the communication interruption by means of a ping communication.

No.	Time	Time Delta	Source	Destination	Protocol	Info
5	0.018	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
6	0.018	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
9	*REF*	*REF*	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
12	0.016	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
15	0.032	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
16	0.048	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
17	0.063	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
23	0.082	0.018	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
26	0.096	0.013	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
27	0.096	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply

Figure 3.18: Ping communication; local AAA server.

The ping requests are sent to the network by the UE but no ping reply from the CS occurs. This depends on the IEEE 802.1X mechanism that only allows interaction of authentication messages between the UE and AP, as shown in Figure 3.17. However, full network access is granted after successful UE authentication as described above by means of Figure 3.16. The light (green) marked frame number 26 in Figure 3.18 shows the first successfully transmitted ping request packet to the CS after full

granted network access by the authenticator. The time difference between frame number 9 and frame number 26 is 96 ms and corresponds to the required authentication time of IEEE 802.1X using EAP-TLS and a LAAA server.

The sequences one to three presented in Figure 3.16 require the communication between authenticator and RADIUS server. In the case of a remotly located RADIUS server interconnected via the Internet the runtime between authenticator and RADIUS server increases, as shown in Figure 3.15. This behaviour leads to the assumption that the avoidance of sequence one to three of the IEEE 802.1X using EAP-TLS method decreases the total authentication and authorisation time resulting in a reduced communication interruption time.

3.5 Mobility in Deployed Network Architectures

In this section WLAN coverage will be discussed in the context of a customers mobility. There are multiple scenarios in which a customer moves within a WLAN covered access network, as presented in Figure 3.19. For instance, the customer moves with low velocity by foot within a city, with medium velocity by car on a road or with high velocity using a high speed train. Another scenario is the nomadic mobility as described in Section 3.1. The frequency of WLAN handovers depends on the velocity of the customer en route as well as on the WLAN coverage of each single AP. However, the coverage is influenced by wave propagation.

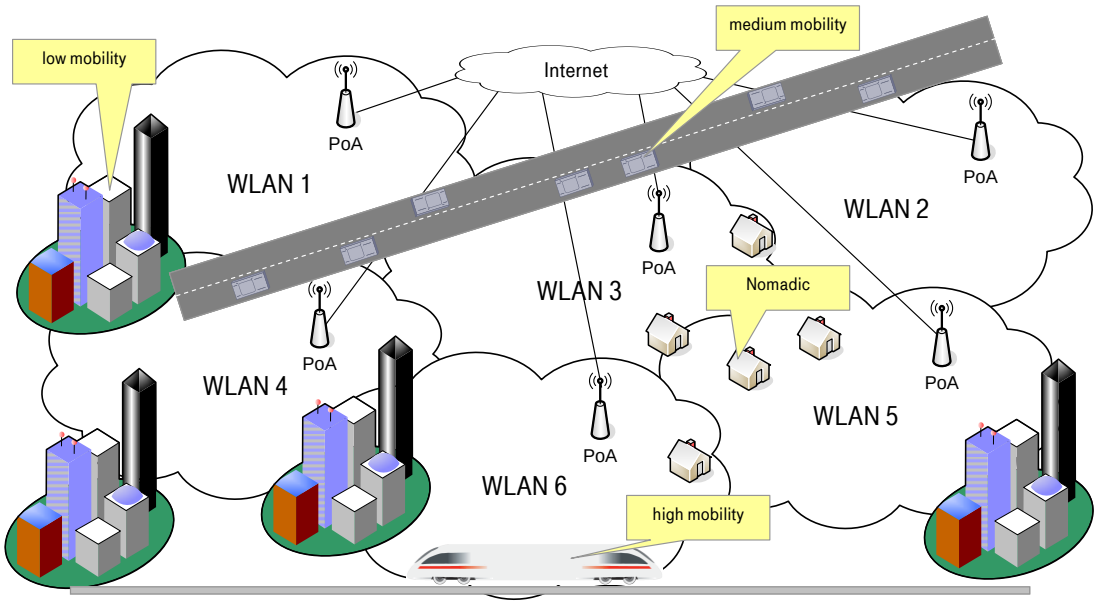


Figure 3.19: Mobility scenarios of customers in WLAN.

Depending on the range of WLAN coverage the mobility characteristic can be derived, such as low mobility, medium mobility or high mobility, as presented in Figure 3.19. To investigate the influence of velocity on the frequency of WLAN handovers it is necessary to examine the electromagnetic wave propagation of WLANs. The tolerable bit error rate (BER) of an 11 Mbit/s WLAN system is 10^{-5} as described in [151]. This means the receiver sensitivity is $-80dBm$ [151]. The receiver sensitivity of a 54 Mbit/s WLAN system is $-65dBm$. Due to the reason that the receiver is equipped with a dipole that bundles the received power, the receiver sensitivity can be additionally less $2{,}15dBi$. This means the level of

$$-80dBm - 2{,}15dBi = -82{,}15dBm$$

has to be available at the receiver antenna of an 11 Mbit/s WLAN system. In the case of a 54 Mbit/s WLAN system the level of

$$-65dBm - 2{,}15dBi = -67{,}15dBm$$

has to be available at the receiver antenna. The transmitter power of $11dBm$ and the transmitter gain of $9dBi$ that leads to an all over transmitted power of $20dBm$ the pathloss between transmitter and receiver can be

$$20dBm - (-82{,}15dBm) = 102{,}15dB$$

in the case of a 11 Mbit/s WLAN system. The pathloss of a 54 Mbit/s WLAN system can be

$$20dBm - (-67{,}15dBm) = 87{,}15dB\,.$$

By means of the freespace model of Harald T. Friss [152] the theoretical possible distance d_{km} between transmitter and receiver can be determined by (3.4) derived from (3.3) described in [151].

$$L_{PdB} = 32{,}4 + 20\log f_{MHz} + 20\log d_{km} \tag{3.3}$$

To derive (3.4) the carrier frequency f_{MHz} of the system used has to be known. The carrier frequency in an IEEE 802.11 b/g system is 2400 MHz. According to that $20\log(2400MHz) = 67{,}6dB$.

$$d_{km} = 10^{\frac{102{,}15-32{,}4-67{,}6}{20}} = 1{,}28km \tag{3.4}$$

This means the distance between transmitter and receiver in a 11 Mbit/s WLAN hotspot can reach $1{,}28km$. The distance between transmitter and receiver in a 54 Mbit/s WLAN hotspot is determined by (3.5)

$$d_{km} = 10^{\frac{87{,}15-32{,}4-67{,}6}{20}} = 0{,}277km \tag{3.5}$$

and is $277m$. However, the freespace model as a physical model is based on optimal electromagnetic wave propagation and does not consider path loss due to obstacles or surrounding area. However, it is necessary to consider these impacts to achieve propagation results that represent real environmental conditions. Typical obstacles of electromagnetic wave propagation are, e.g. trees, buildings and road canyons. There are other physical models, e.g. the two-path model to describe the wave propagation without considering obstacles in the propagation area. In general physical models underlie complex and partly temporally conditions to describe the wave propagation. Alternatively to physical models, empirical models exist. Empirical models are based on many measurements in typical propagation environments. By means of mathematical functions these measurements are then approximated. To reduce failure of these mathematical functions parameters are specified to describe specific environments, frequency dependencies of the measurements as well as the altitude of transmitter and receiver. The parameter that describes the path loss for different surroundings is the exponent n. The surrounding scenarios and its exponents are presented in Table 3.15.

Surrounding scenarios	**Exponent** n
Free space	2,0
Flat area	4,0
Urban area	2,7 – 3,5
City with shadowing	3,0 – 5,0
Within buildings with line of sight	1,6 – 1,8
Within buildings without line of sight	4,0 – 6,0

Table 3.15: Exponent of path loss for different surroundings.

As described in [153] the empirical model assumes that the received power depends on the distance d between transmitter and receiver. The received power P_R is proportional to the distance of the n^{th} potency, as presented in (3.6). In the freespace model $n = 2$.

$$P_R \propto \frac{1}{d^n} \tag{3.6}$$

Based on (3.7) described in [153] the path loss L_P can be determined. In (3.7) the reference power P_0 has to be determined in the distant field. For radio systems working within the high MHz and GHz range, the reference distance $d_0 = 1m$ can be considered as the distant field. Consequently, (3.8) results from (3.7).

$$L_P = P_0 - P_R = 10n\log d - 10n\log d_0 \tag{3.7}$$

$$L_P = 10n\log d \tag{3.8}$$

In (3.10) the reference power P_{0dB} of the WLAN system IEEE 802.11 b/g is determined. The reference power is determined for the reference distance $1m$ by means of the freespace model (3.9) described in [151] and the parameters equivalent isotropic radiated power (EIRP) = 20dBm and $f = 2{,}4GHz$.

$$L_{PdB} = 32{,}4 + 20\log f_{MHz} + 20\log d_{km} \tag{3.9}$$

$$P_{0dB} = EIRP - 32{,}4 - 20\log f_{MHz} - 20\log(1*10^{-3}km) = 20dBm \tag{3.10}$$

Keeping the minimal receiver power in mind the maximal path loss $L_{P\max}$ can be determined. The minimal required receiver power of a 11 Mbit/s WLAN system is -82,15dBm. In a 54 Mbit/s WLAN system the minimal required receiver power is -67,15dBm. The distance d between transmitter and receiver can be determined by means of (3.11) derived from (3.8). Distance d depends on the maximal path loss of the WLAN system as well as on the exponent n. The maximal path loss of a 11 Mbit/s WLAN system is

$$L_{P\max} = P_{0dB} - P_{RdB} = -20dBm - (-82{,}15dBm) = 62{,}15dB$$

The maximal path loss of a 54 Mbit/s WLAN system is

$$L_{P\max} = P_{0dB} - P_{RdB} = -20dBm - (-67{,}15dBm) = 47{,}15dB$$

$$d = 10^{\frac{L_{P\max}}{n.10}} \tag{3.11}$$

The resulting distances between transmitter and receiver depending on the exponent n and the used WLAN system, such as 11 Mbit/s or 54 Mbit/s are presented in Table 3.16.

Surrounding scenarios	Exponent n	11 Mbit/s	54 Mbit/s
Freespace	2,0	1281 m	228 m
Flat area	4,0	36 m	15 m
Urban area	2,7 – 3,5	200 – 60 m	56 – 22 m
City with shadowing	3,0 – 5,0	118 – 17 m	37 – 9 m
Within buildings with line of sight	1,6 – 1,8	2836 - 7663 m	885 – 416 m
Within buildings without line of sight	4,0 – 6,0	36 – 11m	15 – 6 m

Table 3.16: Distances between transmitter and receiver depending on exponent n.

The radio propagation for the following surrounding scenarios, such as freespace, flat area, urban area, city with shadowing, within buildings with line of sight and within buildings without line of sight are given in Table 3.16. The results of Table 3.16 are confirmed by Figure 3.20 of [153]. The most relevant results for WLAN coverage regarding the customers mobility is shown in the row urban area and city with shadowing in Table 3.16. The maximal range of coverage in urban areas for WLAN 11 Mbits/s systems is 200 m. As a result, this maximal WLAN range and the velocity of a customer impact the residence time in the WLAN cell. The shorter the retention time in a WLAN cell the more frequently a handover has to be performed to the next WLAN cell.

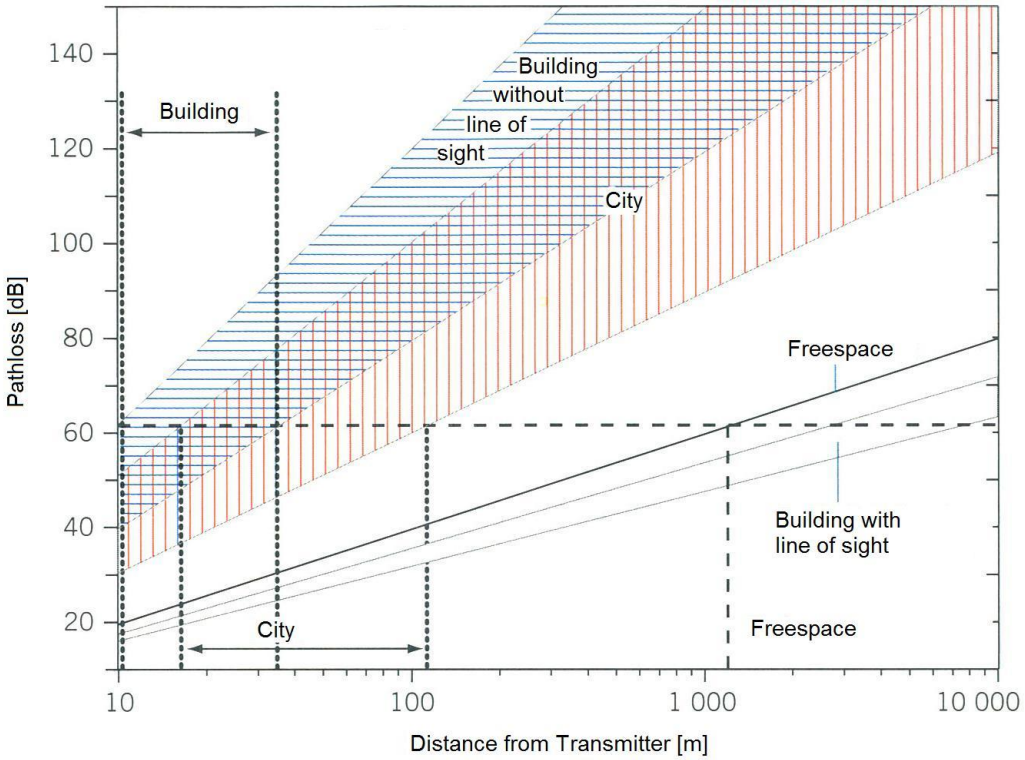


Figure 3.20: Path loss in dependency of distance between transmitter and receiver [153].

Table 3.17 and Table 3.18 show the minimal retention time t_{ret_min} and maximal retention time t_{ret_max} of a device in a WLAN cell depending on the customer velocity v. Both investigations keep the results of the realistic scenario for user mobility of Table 3.16 in mind, the urban area. The velocity v is described in 3.12 where d is the distance covered and t the time needed to cover this distance.

$$v = \frac{d}{t} \tag{3.12}$$

d is two times the radius r of a WLAN cell as shown in 3.13.

$$v = \frac{2 * r}{t} \tag{3.13}$$

v [km/h]	v [m/s]	t_{ret_min} [s]
3	0,83	144
30	8,3	14,4
40	11,1	12,96
50	13,8	8,64
100	27,7	4,32
150	41,66	3,46
200	55,5	2,16

Table 3.17: Minimal retention time in WLAN cell with a cell radius of 60 m.

The results of maximal and minimal wave propagation in urban areas, shown in Table 3.16, are used to determine the retention time in a WLAN cell. Table 3.17 presents the minimal retention time in a WLAN cell with a cell radius of 60 m. Table 3.18 presents the maximum retention time in a WLAN cell with a cell radius of 200 m. In general the WLAN propagation range can be increased, up to a defined quantity, by means of directed antennas. Moreover, the deployment scenario limits the propagation as well, e.g. site density along a street in conjunction with the path of the street.

v **[km/h]**	v **[m/s]**	t_{ret_max} **[s]**
3	0,83	480
30	8,3	48
40	11,1	43,2
50	13,8	28,8
100	27,7	14,4
150	41,66	11,52
200	55,5	7,2

Table 3.18: Maximal retention time in WLAN cell with a cell radius of 200 m.

The electromagnetic wave propagation in the urban areas scenario is typically better when compared to a city with shadowing scenario. However, the urban area scenario is selected for the investigations in Table 3.17 and Table 3.18 because the propagation range in Table 3.16 is larger in contrast to the results of the city with shadowing scenario. This means the determination of retention times for the urban area scenario will result in higher retention times compared to the city with shadowing scenario. Accordingly, the frequency of handovers in the city with shadowing scenario will increase. However, even a mobility scenario that is based on the results of the urban area scenario leads to quality degradation of a voice communication when keeping the results of Section 3.1 in mind. In the case of a cell radius of 60 m the customer velocity that impacts the voice quality is reached between 40 km/h and 50 km/h. In the case of a cell radius of 200 m the customer velocity that impacts the voice quality is reached at 150 km/h. Moreover, it has to be considered that the retention times in Table 3.17 and Table 3.18 are based on the assumption that the device moves through a radial WLAN cell where the secant crosses the centre of the WLAN cell. However, the retention times will decrease when the device moves through a WLAN cell where the secant crosses not the centre of the WLAN cell. As a result, the frequency of handover processes increases as

well. In addition, the radio propagation range of WLAN systems with 54 Mbit/s is smaller as half the range of WLAN systems with 11 Mbits/s. As a result, the residence time in such a WLAN cell decreases and the frequency of handover increases.

3.6 WLAN-Based Hotspot

Facets of WLAN-based access networks are WLAN-based hotspots which enable broadband Internet connectivity. Several network operators, e.g. Deutsche Telekom [27] and Kabel Deutschland [28] have deployed a significant number of WLAN-based hotspots. Even large city centre areas have been covered by hotspots, e.g. Telekom Hotspot-Zone in Hamburg [154] or Google WiFi for Mountain View [155] to provide broadband Internet access. Such WLAN covered areas can be of interest for mobile network operators to offload mobile access networks [156] as well.

A generic hotspot architecture consisting of the hotspot access network and the hotspot controller is presented in Figure 3.21. The hotspot access network is composed of at least one access point (AP) and is connected to the Internet via the hotspot controller (HC). Each user device is connected to the hotspot access network via an AP. However, the user device is not able to communicate with the Internet until user authentication and authorisation is performed successfully.

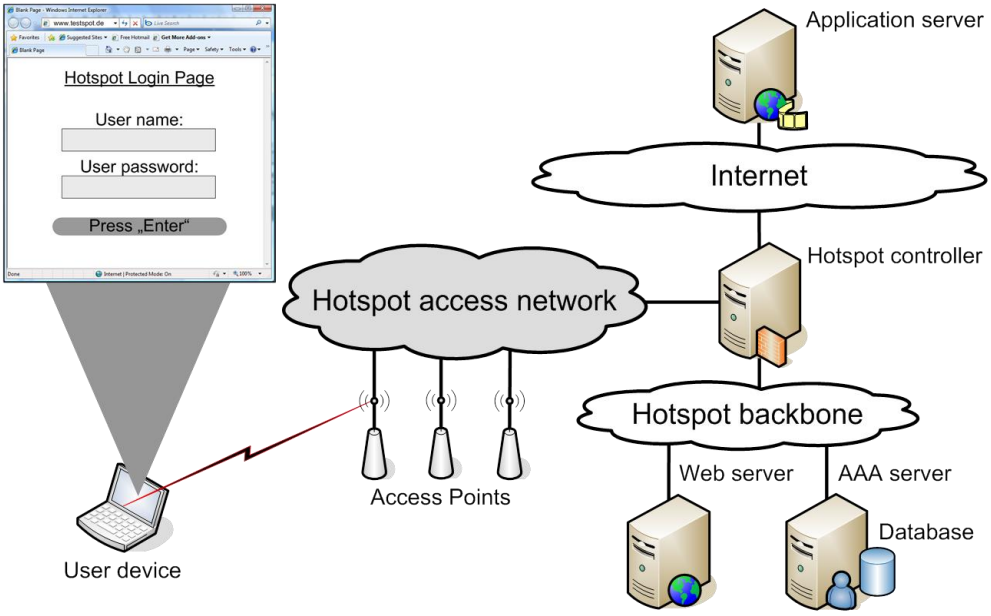


Figure 3.21: Generic hotspot network architecture.

The HC is responsible for Internet access control. Before the access control process is started a successfully established WLAN connectivity among the device and the

hotspot access network is needed. The access control process starts when the WLAN connectivity is established and the user opens the web browser and requests a website on the Internet. As a result of the access control process the hotspot login page (HLP) is pushed to the web browser, if no successful hotspot login process has been performed previously. Independent of the configured start page in the web browser the hotspot controller pushes the HLP. The HLP is hosted on a web server in the hotspot backbone. The backbone can be a local or remote located network which is connected to the HC. The location of the web server depends on the scale and type of hotspot. Small hotspots often host the HLP within a local network, while large hotspots, e.g. [27] and [28] host the HLP remote and central.

The hotspot access control and login process performs user authentication and authorisation based on the entered user credentials on the HLP. An authentication, authorisation and accounting (AAA) server is used to perform user authentication and authorisation by means of stored user credentials in a database (DB). Similar to the location of the web server, the location of the user DB can vary. User data are stored in a DB located within a local hotspot backbone or within a remote located hotspot backbone interconnected via the Internet. Small hotspots as often deployed in campsites or cafés use a local DB to manage their users, while large hotspots, such as [27] and [28] manage their user in centralised DB. After successful user authentication and authorisation the hotspot controller grants Internet access to the user device.

The benefit of a centralised user management is that it enables users to use hotspots at different locations with a single user account. As a result, the account management effort of the user is reduced. This fact motivates users to use hotspot based Internet access at different locations without the need to obtain new user credentials. However, centralised solutions, such as [27] and [28] are not as widely deployed to provide an area-wide coverage of hotspot based Internet access. This means a mix of different hotspot solutions still exists and will most likely increase in the future. There are a lot of commercial and open source solutions of WLAN-based hotspots available today. Some solutions are deployed and managed by operators, such as [27] and [28]. Other solutions are offered by IT equipment vendors, such as Cisco [81] and Mikrotik [82]. Moreover, there are hotspot solutions offered by hotspot providers, such as XCony [83]. Furthermore, open source solutions exist to

setup hotspots, such as CoovaChilli [84]. A challenge of hotspot operators is to motivate users to use their hotspots, even if the hotspots are managed by different owners and the user has no user credentials for this particular hotspot.

Another challenge of network operators is the fact that IP traffic in mobile networks has increased in the past years and will still increase in the coming years [26] This behaviour is based on the fact that the market penetration of smart phones and tablet PCs has increased and will continue to increase [ibid]. The challenge of mobile network operators is to provide application service delivery to the user in satisfying quality, even if the network load increases. This means, even if the network load increases, the remaining network access resources and capabilities have to assure application service delivery which satisfies the quality of experience of the user. As a result, network operators try to offload mobile networks to avoid overload situations and network congestions [157]. An ability to discharge mobile access networks is cellular traffic offloading by means of WLAN [156] and WLAN-based hotspots. However, before this really becomes reality, hotspots have to overcome some drawbacks. A non-technical drawback is the high hotspot fee which demotivates users to use hotspots. A technical related drawback is the usability concerning the way of payment and the usability of getting logged-in to the hotspot. The usability of public WLAN-based Internet access in hotspots is not convenient as users expect the usability from private WLANs, such as switch on WLAN interface and Internet access is available. In addition users are spoiled by mobile networks and their behaviour of getting Internet access. Accordingly, the aim of network operators is to simplify the way of providing WLAN-based network access. Approaches designed to address some drawbacks of hotspot login are, e.g. the extensible authentication protocol - subscriber identity module (EAP-SIM) method [158] and the so called wireless Internet service provider roaming (WISPr) clients/methods [159]. EAP-SIM is an approach which enables automated login to WLAN-based hotspots. However, it will take time to equip all existing hotspots and devices with this mechanism. WISPr clients enable auto-login to the hotspot without the need to enter user credentials, such as user name and password on the hotspot login page manually. The WISPr approach requires an application on the user device, which is accepted by the users in today's 'app-world'. However, a disadvantageous issue is that the user has to have the user credential in advance of hotspot use. Thus, hotspot

flat-rate accounts are beneficial for WISPr use cases. This means, that the user has to have a contract with the Internet service provider (ISP). As a result, the WISPr approach is not utilizable for users without an existing contract with the ISP, even if they would like to use the hotspots.

Hotspots offer paid Internet access in, e.g. restaurants, cafés, stations, airports, hotels, campsites or within public transportations, such as high speed trains. Basically, there are two types of hotspot payment possible, such as post-paid and prepaid. In the post-paid solution the customer pays the hotspot use according to the consumed login time. In the prepaid solution the customer pays for the duration of hotspot use in advance. Hotels often use post-paid hotspot solutions. In post-paid solutions the billing of the Internet access is added to the overall hotel bill or is cleared by means of Internet service providers, e.g. Telekom [27] and Kabel Deutschland [28] which provide the WLAN infrastructure. Restaurants, cafés and campsites most often use the prepaid type of hotspot solutions. As confirmation of payment the customer receives a voucher containing the information about duration of hotspot use as well as the user credentials, such as login name and login password. A challenge of hotspot operators is to attract the way of providing the user credentials to the user to use their hotspots.

In general today's hotspot solutions lack convenience in terms of user credential obtainment, entering of credentials and flexibility, such as point of time and duration of hotspot use. It can be assumed that improved usability of hotspots, such as convenient login processes as well as flexible and easy way of payment will stimulate users to use WLAN-based hotspots more often than today. As a result, WLAN-based hotspots would be able to contribute to the offload strategy of mobile network operators.

3.7 Service Provisioning to Users supported by Added Value Services

Today's digital world offers a variety of access networks, application services and different devices types to the user. Each of these devices needs to be configured and managed by the user to be able to connect to an access network in order to communicate with an application service. Table 3.19 gives an overview of today's service and network access provisioning behaviour as well as the customer characteristics.

Application	User	Network
▪ Application services variety is abundant. ▪ Application services are provided by one or multiple providers. ▪ Each application service needs its own agreement. ▪ Each application service comprises its own portfolio. 	▪ Use of multiple devices, e.g. mobile phone, tablet PC, laptop, desktop PC, TV. ▪ Multiple agreements among application service and network access providers ▪ Multiple, independent application service and network access portfolios. 	▪ Several types of access network exist. ▪ Each access network needs its own agreement. ▪ Each access network comprises its own portfolio. ▪ Each technology comprises its own configuration and authentication parameters. 

Table 3.19: Today's application service and network access provisioning behaviour as well as the customer characteristics.

Table 3.19 presents the silos, such as application service, access network and the user with its devices. Each of these silos is more or less separated from each other today and no overarching configuration and management is possible. As a result, the state-of-the-art of today's application service provisioning is not user profile, user device or network aware. This non awareness is based on the missing interaction between the application service, the network and the user as shown in Figure 3.22. For instance service provisioning is performed independent of the knowledge whether the device of the user is able to utilize the requested application service or whether the connecting access network is able to provide the required performance. Moreover, due to the management effort of the application services and network access on multiple devices the user might be less satisfied than could be possible.

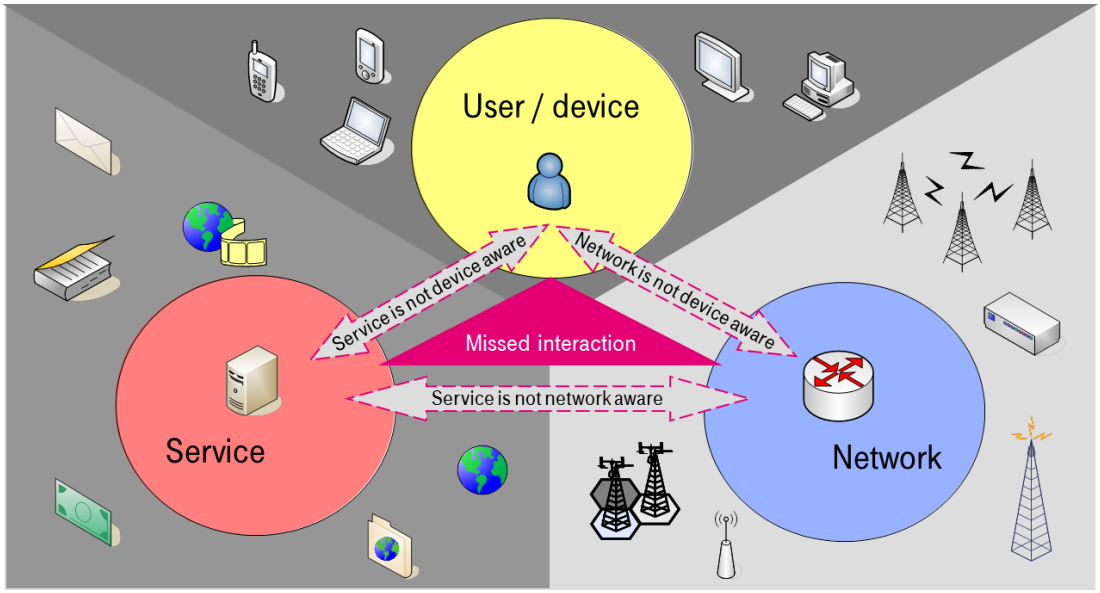


Figure 3.22: Service, network and user / device are not aware of each other.

An important goal of next generation service (NGS) provisioning of network access and service providers is to improve the user satisfaction regarding service quality provisioning as well as the management effort of application service, network access and devices. In this context enabler functionalities become more and more important to gain added value for network and application providers. Enabler functionalities can cover all kinds of topics which are needed to support or improve network services and application services. For instance, throughput improvement or traffic prioritisation could be provided by an enabler functionality for network services to improve the network performance.

Service provisioning in customer satisfying quality is one of the most important issues for network and content providers. This statement is agreed in [1] as “operators need to ensure that applications are delivered correctly over their networks”. Some services, e.g. voice or video demand for specific network performance to fulfil the quality of experience (QoE) of a user with the provided service. Quality of service (QoS) mechanisms can be applied in network architectures to manage network performance to provide the necessary network performance to deliver the service in QoE fulfilling quality. However, in some situations the network capacity is not sufficient in some network segments, e.g. network access, to deliver the application service in expected quality. This behaviour can occur even when QoS mechanisms are applied inside the networks along the data path. As a result, the user is not satisfied with the service provided. Besides that, on

the one hand side the application server is not aware of the degraded network performance to adapt the service to the available network performance and on the other hand side the user is not aware of the realizable service quality to be expected after service initiation.

Recent IP networks (e.g. of a network operator) usually implement mechanisms for QoS support. For instance, these QoS mechanisms may be based on the differentiation of IP packets on selected routers at edges of the operator's network while putting them into different pipes/tunnels based on MPLS or VLAN labels. QoS differentiation is then for instance implemented by using different scheduler mechanisms and scheduling priorities or by special shaping rules for different pipes and queues. In principle the differentiation of the packets is done at the ingress router of a network domain, where special rules and profiles are applied to mark the respective packets. Afterwards the packets are distributed into different queues and are scheduled according to these rules and profiles. Re-marking and classification are done only at egress and ingress level [160]. Any other QoS mechanism can also be applied in the network, either in the core or in the access networks.

Available QoS mechanisms are usually configured statically which means that classification rules are pre-defined and use pre-defined IP addresses and port numbers. Theoretically, traffic classification could also be based on the type of service (TOS) field of the IP header. Nowadays this field has been renamed to the differentiated services code point (DSCP). However, this is not a common praxis in many real networks as the TOS field is usually set by the application and therefore, it is not under the control of the network operator.

In real networks, traffic classification is usually based on IP addresses, protocol types and port numbers (called 5-tuple). This means that QoS provisioning for applications with static IP or port numbers can easily be implemented in this way. However, the implementation of such QoS mechanisms in the data path from the source, e.g. content provider, to the destination, e.g. customer, does not guarantee service provisioning in customer satisfying quality. This is based on the fact that QoS mechanisms are implemented independently from each other in the different network domains. Hence, the QoS mechanisms are not aware of each other and have no knowledge about available network resources within the other network segments. In the case of insufficient network resources in the end-to-end (E2E) data path (e.g. by

local network overload) the delivered E2E service is hence influenced in its quality. As a result, the expected quality of experience of the customer cannot be fulfilled. Moreover, static configuration based on a 5-tuple does not work properly in the case where IP addresses or the port numbers of IP flows change along the data path. A typical example of such a case is video streaming where the source IP address and the destination port number can dynamically be changed depending on the streaming server and client. To enable QoS support for such services in IP networks, an external interface is typically implemented and offered for services for which QoS must be supported in the network.

Beside QoS mechanisms there are frameworks, such as the IP multimedia subsystem (IMS) [161], the resource and admission control subsystem (RACS) [162] and the network attachment subsystem (NASS) [163] which describe functional entities and interfaces to provide and exchange control (and QoS) information and parameters between functional entities. Moreover, there are QoS-related architectures described, such as the ITU-T NGN [164] and Economics and Technologies for Inter-Carrier Services (ETICS) [165] to provide network and application control reference architectures for next generation networks.

These frameworks, such as IMS [161], RACS [162], NASS [163], ITU-T NGN [164] and ETICS [165] describe well defined network and control architectures for next generation networks and next generation service provisioning, including the provisioning and realization of end-to-end QoS-based services. However, the deployment of such frameworks in network and content provider network architectures is still in progress or will even never happen at all. For example, IMS is yet not widely installed and supported. The reason for that can be found in the fact that these architectures are very complex and heavy weight, and require very often a deployment of new systems and devices within the network operator and application provider infrastructures.

There are common interfaces specified to exchange information and parameters between networks or application entities based on protocols or application programmable interfaces (APIs), e.g. GSMA OneAPI [166], enabler release definition for next generation service interfaces [167]. These interfaces can be used to design and implement individual and QoS-related services.

The APIs, such as OneAPI [166] and enabler release definition for next generation service interfaces [167] provide a solid base to develop individual added value services. However, the deployment of new services which require inter-provider communication to exchange service related information is challenging. The setup of new services needs an agreement, e.g. between content provider and network providers on an APIs to be used in the inter-provider communication. Moreover, the integration of new APIs in network architectures causes additional costs for the deployment and for operation.

Features in software, such as video players on user devices are able to control the video quality depending on the configuration of e.g. resolution or codec of the video. Moreover, application servers which recognize the applied web browser on the user device are able to adapt the video quality, e.g. video resolution depending on the web browser information. For instance, the information of a mobile device web browser could indicate that the device is connected via a mobile network, and thus, the network capabilities can be less than e.g. in WLAN based access networks. However, both possibilities the configuration of the software on device side and the recognition on the server side are not able to consider the real existing network performance capabilities to adapt or inform the user about the providable service quality.

The challenge in the creation of new added value services is to obtain the required parameters from other network service providers, application service providers and from the users device to perform the added value service. Moreover, the added value service results which are foreseen to be offered to other providers for further processing is challenging as well. The difficulty in both cases is the transmission of parameters via an interface which is used by the involved service providers. A suitable solution could be to use wide deployed frameworks, protocols or APIs to exchange the parameters. However, not each network service provider, application service provider and user device has the functionalities needed implemented. Even if standardised frameworks and APIs are well defined it seems to be a useful approach to realise added value services by means of easy deployable mechanisms, e.g. based on web-services. A standardisation related approach is network function virtualisation (NFV) [168]. The aim of NFV is to have software-based network functions which can be instantiated and controlled from anywhere in

the operator's network, data centre or end-user premises, without the need to install new or additional hardware equipment in the network architecture.

3.8 Summary of Challenges in User Satisfying Service Quality Delivery

The investigations of this chapter have focused on three topics. The first topic investigates the handover performance in WLAN-based access networks and its influence on data transmission and in particular on VoIP quality. The second topic focuses on the usability of WLAN-based hotspots, while the third topic addresses the aim of network service providers to overcome the fact of just being bit-pipe providers. All three topics have been investigated from the user point view and how the behaviour influences the quality of experience of a user. This section presents the relationships of network capabilities on user perceptions in a service delivery chain, integrated in an overarching view. The overarching view considers as well the presented topics in this section and describes their dependencies. This section will be closed with an outlook to network capabilities which could be improved to archive improved user perceptions.

3.8.1 Investigated Topics

As introduced in Section 3.1 there are different types of mobility, such as terminal, user, session, and service mobility. In the context of seamless service provisioning to users the terminal mobility is the most challenging type of mobility. Terminal mobility is performed when changing the PoA. The required handover process to perform the change of the PoA and to carry out network access control leads to IP communication interruptions as investigated in Section 3.4.

The influence of network security mechanisms involved in WLAN network access control and handover processes in a real network environment was investigated in Section 3.4. Moreover, the influence of wireless configuration tools, such iwconfig and wpa_supplicant on the configuration time as part of the handover time was presented. Figure 3.15 presented the influence of encryption, authentication and authorisation methods as well as configuration tool on the handover time. Due to the measurement results it was assumed that improvements on configuration time can be achieved by means of fitted configuration tool implementations to provide faster wireless card reconfiguration in the handover process. However, the most

connection interruption time intensive authentication and authorisation mechanism WPA2 using EAP-TLS cannot be improved by means of a fitted configuration tool implementation. The measurement results in Figure 3.15 show that WPA2 using EAP-TLS in conjunction with a network external located AAA server has an average time of authentication, authorisation and key derivation of 494 ms. This time is caused by the handshakes between the AP and the remote EAAA server need to perform the authentication and authorisation process. The drawback of this behaviour is while performing the authorisation and authorisation process, no network access is granted and thus, no access to services in the Internet is possible. As a result, this leads to IP communication interruptions and finally to interruptions in real-time services provisioning, e.g. VoIP services or video conferencing which results in decreased QoE of these services.

To investigate the influence of IP-based communication interruption caused by WLAN handover processes, the influence of voice communication interruption on speech quality has been investigated in Section 3.2 by means of the PESQ method. The PESQ value is an indicator to describe the quality of a voice communication. The PESQ method simulates the human speech quality rating by comparing an original speech signal with a transmitted speech signal. Voice communications with determined PESQ values greater than four fulfil the requirements on a carrier grade voice service. In this investigation an original speech signal stored in a wav-file was deformed by Matlab and saved as transmitted speech signal. The conclusion of Section 3.2 is that communication interruptions greater than 40 ms in conjunction with interruption intervals less than 11.7 s lead to PESQ values that are less than four. This means, the voice service would not be delivered at carrier grade quality and thus, the quality of experience of the customer would not be achieved. Considering the measurement results of Section 3.4 that shows data communication interruptions up to 496 ms caused by WLAN handover processes which are much larger than 40 ms.

Beside the investigation of speech quality utilizing deformed audio streams as performed in Section 3.2, the real transmitted audio stream via an IP-based connection has been investigated in Section 3.3. The inserted interruptions in the real IP communication are used to emulate WLAN handovers and to determine the influence of handovers on the IP-based VoIP communication. The determination of

voice quality by means of the PESQ method presents similar results as shown in Section 3.2. The result supports the assumption that interruptions in voice communication leads to decreased voice quality. Due to this is it can be assumed that improved WLAN handover processes can improve voice communications when users are on the move.

Section 3.2 shows that communication interruptions greater than 40 ms in conjunction with interruption intervals of less than 11.7 s lead to non-carrier grade voice quality. Basically, the voice service interruption interval depends on the frequency of WLAN handovers and thus, on the WLAN cell size. In Section 3.5 the electromagnetic wave propagation of WLAN systems in different scenarios, e.g. city with shadowing, urban area, flat areas and its influence on the WLAN cell size has been described. Moreover, customer velocity and the resulting frequency of handovers have been discussed in the relation of the WLAN cell size. The investigation of the most realistic propagation scenario, the urban area scenario, in conjunction with customer velocity result in resident times in WLAN cells that degrades the quality of a voice communication when keeping the results of Section 3.1 in mind. The longest residence time in a WLAN cell is reached when the user moves along the radius of the WLAN cell. However, a user might not go straight through the centre of the cell but rather only touch the edge. The longer the residence time in a WLAN cell the higher the supported device velocity which does not influence the voice quality. In the case of a cell radius of 200 m which results in a covered distance of 400m of the WLAN device, the WLAN device velocity that impacts the voice quality is reached at least at 150 km/h. A cell radius of 60 m and a WLAN device velocity between 40 km/h and 50 km/h impacts the voice quality as well. This means, in a large hotspot scenario with EAP-TLS as the deployed security mechanism and a WLAN device velocity between 40 km/h and 50 km/h would decrease the QoE of an IP-based voice service.

Beside network performance which is needed to deliver application services of satisfying quality to the user, the usability of network operator’s products, e.g. WLAN based hotspots, is of importance. For network operators it is important to attract WLAN hotspots to go one step forward towards the WLAN offloading strategy mentioned in Section 3.6. The intention of WLAN offloading is to unburden mobile networks by reducing traffic in the mobile network and by sending traffic via

WLAN-based access networks, e.g. hotspots. Usability in the context of hotspots is the aspect of how convenient it is to get Internet access. Depending on the usability the QoE of hotspot use is affected. The aspect of how a user gets Internet access in WLAN-based hotspots has been investigated in Section 3.6. It is assumed that improved usability of hotspots will stimulate users to use WLAN-based hotspots more often than today. However, from a deployment and thus, short term point of view today's mechanisms, e.g. WISPr and EAP-SIM are not able to change the usability of hotspots for most users.

Service provisioning in customer satisfying quality is one of the most important issues for network and content providers. However, in some situations the network performance is not sufficient to deliver the application service in expected quality. For that purpose it is important for network operators to develop mechanisms or added value services which are able to improve the QoE of users even in such situations. As described in Section 3.7, the challenge in the creation of new added value services is to obtain the required parameters from all involved actors, e.g. other network service providers, application service providers or from the users device. Until today, a common behaviour of network operators is to set up new services based on standardised frameworks, protocols or APIs. However, this procedure is time consuming and results in long time to market situations. To reduce the time to market of new services and products network operators are looking forward to flexible, efficient and orchestrateable network architectures, such as enabled by means of network function virtualisation techniques.

3.8.2 Network Capabilities Influencing Aspects

Derived from the investigations of Section 3.1 to 3.7, Figure 3.23 illustrates the dependencies of all involved actors and whose entities in the application service delivery chain. The actors are the application, the network and the customer. The application service is delivered to the customer via a network. The application service delivery can be divided into two aspects, the human aspect and the technology aspect. The human aspect of the customer is typified by the user who benchmarks the provided service. For example, the user benchmarks the received service quality of a provided application service, e.g. video service. Another example might be the user that benchmarks the usability of the process to obtain credentials to

get network access, e.g. in a WLAN-based hotspot. In contrast to the human aspect, the technology aspect comprises the technology related issues in the application service delivery chain. Part of the technology aspect is the service data of the application service which are transported to the device via a network. The device typifies the technology aspect of the customer side which receives the IP packets and displays the application service to the user.

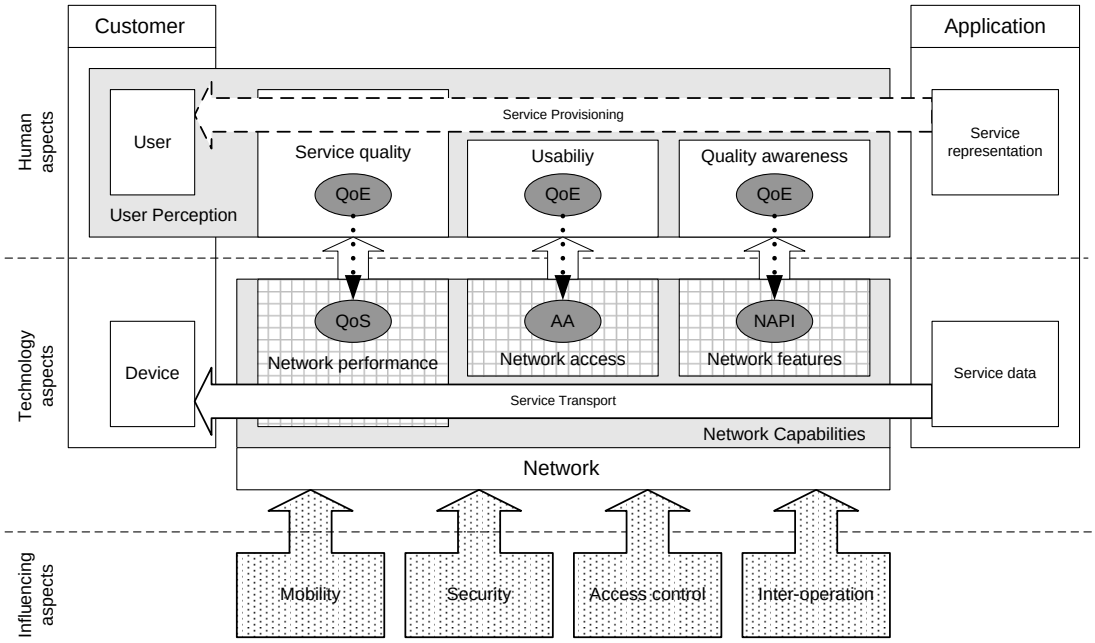


Figure 3.23: Influencing aspects on network capabilities and its relationship with the user perceptions.

A result of investigations in Sections 3.1 to 3.7 is that network capabilities have an influence on user perception. The types of network capabilities are manifold and have to be interpreted in relation to a service which will be provided to a customer, as shown Figure 3.23. This means network capabilities can differ from each other and depend on application service or network service requirements. For example, an application service, e.g. video service, has requirements on the network performance, e.g. a certain amount of bandwidth, delay or packet loss. This means the network performance has a direct influence on the data transport and thus, on the delivered service quality which impacts the user perception. Another example of a network capability which impacts on the user perception is the registration process of a network access service. The requirements on this network capability are e.g. on the registration process rather than on network performance. As a result, the registration

process has direct influence on the usability of the network access service and thus, on the user perception.

This work focuses on the network capabilities and in particular on the network performance, network access and network features. These network capabilities are rated by means of different key performance indicators (KPIs). The KPIs this work focuses on are as follows. The network performance is expressed by the KPI QoS, while the KPI of network access is the registration process (RP). The KPI of network features is expressed by means of the network programmable interface (NPI). The network capabilities and KPIs respectively are influenced by different aspects, as shown in Figure 3.23. The influencing aspects are manifold and depend on the constrains of a particular use case. In this work the influencing aspects are mobility, security, access control and inter-operation.

The relationships among the network capabilities and the user perception are shown in Figure 3.23. The network capability network performance with its KPI QoS has an influence on the QoE service quality. The network capability network access with its KPI RP has an influence on the QoE usability, while the network capability network features with its KPI NPI has an influence on the QoE quality awareness in relation to the application services.

The influence of the network capabilities on the user perception is an important fact for network operators. Network operators can use this fact to improve the user perception with its services and even more the network operator can evolve its service portfolio to offer added value services to third party providers to improve their application services. However, the network operator has to be aware which network capabilities are needed to achieve an improvement of user perception. The behaviour of being aware and the relationship among user perception and network capabilities is shown in Figure 3.23 with dotted arrows. Starting from a specific facet of user perception, e.g. QoE service quality a requirement onto the corresponding network capability, such as KPI network performance can be derived. Depending on the level of QoE which should be reached the corresponding KPI has to be defined.

3.8.3 Outlook to Improved Network Capabilities

The results of this Chapter are used to highlight the room for network capability improvements. The outcome of this Chapter presents topics which are of interest for

network operators. It was shown that improvements of these topics can enrich network operator's assets. WLAN handover processes have a significant influence on the voice quality when users are on the move in WLANs. As pointed out a significant factor that influences the IP communication interruption is the authentication and authorisation process in the handover process. It can be assumed that improved WLAN handover performance leads to improved voice quality in WLAN mobility scenarios. This fact is of interest for network operators when they are looking forward to large deployed WLAN hotspots or City-WLANs.

Network operators have spent a significant amount of money to deploy WLAN-based hotspots. However, the hotspots are not highly utilised. Many users are not satisfied with the payment process and the way in which they are to obtain user credentials to get access to the Internet via hotspots. Improved usability of hotspot registration processes can attract users to use hotspots more often. This can be of interest for network operators when they are facing the question of how to improve existing WLAN access network assets.

One aim of network operators is to overcome the fact of being 'just a bit pipe provider'. For that purpose network operators are searching for opportunities and new services which enable the creation of new businesses. A major topic in this context is to use the network operators assets to develop such new services. It can be assumed that new services, e.g. added values services, are able to enrich network operators service portfolio which leads to new revenue. Moreover, such new services can contribute to overcoming the challenge of being 'just a bit pipe provider'.

4 Enhanced Quality of Experience based on Improved Network Capabilities

A specific use case (UC) with its application services requires a set of network capabilities to fulfil the quality of experience of a user with respect to this specific use case. Network capabilities are key assets of network operators. However, Section 3.8.3 shows room for network capability improvements. These improvements offer to enhance their customer's quality of experience based on improved network capabilities. The investigations in Chapter 3 result in a clustering of network capabilities which is shown in Figure 3.23. The derived clusters are network performance, network access and network features.

The objective of this chapter is to introduce solutions which improve network capabilities in relation to a specific use case. The focus is on three use cases which have different requirements on the network capability network performance, network access and network features. For each use case a solution is proposed with the intention to reduce existing short comings of network capabilities as described in Section 3.8.3. The relation of network capability and use case is illustrated in Figure 4.1. A common objective of all solutions is to improve the QoE of an application service in the specific use case.

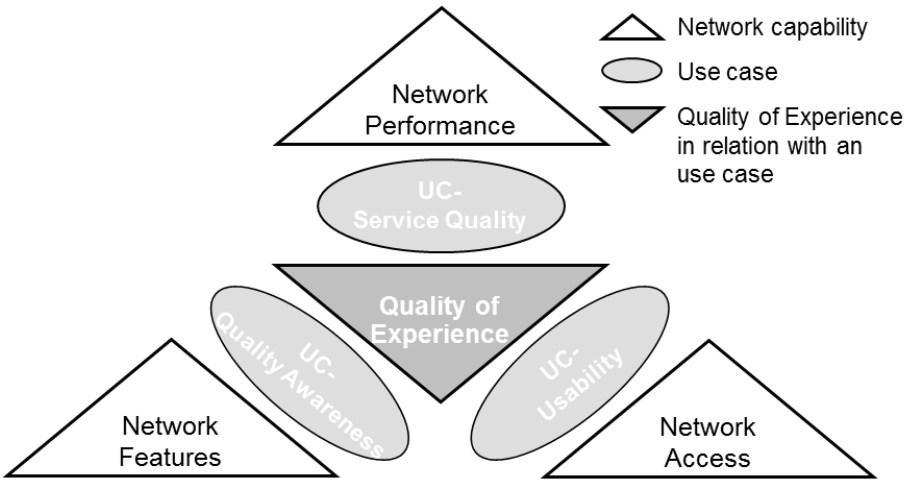


Figure 4.1: Relation among focused network capabilities and use cases.

The use cases are UC-Service Quality, UC-Usability and UC-Quality Awareness. More details about the UCs, related network capabilities and the objectives are presented in Table 4.1.

Name of Use Case	Short Description of Use Case	Network Capability	Focus of Improvement	Objective related to QoE
UC-Service Quality	VoIP communication in WLAN when users are on the move	Network Performance	Enhanced authentication and authorisation method in WLAN handover processes	Better VoIP quality when users are on the move in WLANs
UC-Usability	WLAN Hotspot registration process, obtaining of user credential and login process	Network Access	Provisioning of user credentials on demand and Hotspot auto-login method	Improved hotspot comfort - flexible use and user-friendly login
UC-Quality Awareness	Application service delivery and the quality received by the user	Network Features	Distributed data collection system and a user information system	User gets informed about the application service quality to be expected in advance

Table 4.1: Details about use cases, related network capabilities and objectives.

UC-Service Quality focuses on VoIP communication when users are on the move in WLANs. Section 3.8.3 presents drawbacks in the authentication and authorisation method in WLAN handover processes. This type of drawback relates to the network capability network performance. The objective of the introduced solution is to improve the network performance by means of enhanced authentication and authorisation method in WLAN handover processes.

UC-Usability addresses the WLAN hotspot registration process, the obtaining of user credentials and the login process. Section 3.8.3 presents drawbacks in the current ways to get access to the Internet via public WLAN-based hotspots. These drawbacks relate to the network capability network access. The objective of the introduced solution is to improve the hotspot network access by means of provisioning of user credentials on demand and to enable hotspot auto-login. The user benefit is a more user-friendly handling of WLAN-based hotspots which results in enriched hotspots.

UC-Quality Awareness focuses on application service delivery and the quality received by the user. Section 3.8.3 presents drawbacks of IP-based application service delivery and the fact that the user is not aware of the quality to be delivered.

This type of drawback relates to the network capability network features. The objective of the introduced solution is to enrich network features by means of a distributed data collection system and a user information system. The user benefit is that the user gets informed about the application service quality to be expected in advance before the content provider starts service delivery.

The reminder of this chapter is structured as follows. Section 4.1 presents the sequential authentication solution to reduce the data communication interruption time during the network access authentication and authorisation in the WLAN handover process. The barcode initiated hotspot auto-login solution which enables hotspot user credential request on demand and provides an automated hotspot login mechanism is described in Section 4.2. In Section 4.3 the graceful denial of service solution to provide a busy signal for IP-based applications is presented to inform the user about the expectable application service quality before an application service is started. A summary of this chapter is given in Section 4.4.

4.1 Sequential Authentication Solution

In this section the sequential authentication solution (SAS) is presented which reduces authentication and authorisation time in a WLAN handover processes. SAS focuses on the network capability network performance and is related to the use case service quality, as shown in Figure 4.1. The objective of the use case service quality is to improve application service delivery to end-users in WLANs when they are on the move.

Section 3.4 highlights the significant influence of IEEE 802.1X using EAP-TLS method on the WLAN handover performance. Based on the analyses and results of Section 3.4 the sequential authentication solution has been developed. SAS reduces the influence of authentication and authorisation time of the state-of-the-art IEEE 802.1X using the EAP-TLS method on WLAN handover performance. The SAS combines both network access control methods WPA2 PSK and WPA2 EAP-TLS.

The objective of the sequential authentication solution is described in Subsection 4.1.1 while the requirements on this solution are highlighted in Subsection 4.1.2 before the technical solution is described in Subsection 4.1.3

4.1.1 Objectives

The objectives of the sequential authentication solution are presented in Table 4.2 and Table 4.3. Table 4.2 shows the objectives which are of relevance from the users point of view.

Objective Number	Description
SAS-obj-user-1	VoIP service provisioning in satisfying quality when users are on the move in WLAN access networks

Table 4.2: Objective of sequential authentication solution from user perspective.

The objectives of the sequential authentication solution which are of relevance for network operators are shown in Table 4.3.

Objective Number	Description
SAS-obj-op-1	Network capability 'network performance' that enables SAS-obj-user-1
SAS-obj-op-2	Time of data communication interruptions in WLAN handover processes that enables SAS-obj-user-1

Table 4.3: Objectives of sequential authentication solution from network operator perspective.

VoIP service provisioning in satisfying quality when users are on the move in WLAN access networks is the objective of the sequential authentication solution from user perspective (SAS-obj-user-1) as shown in Table 4.2. SAS-obj-user-1 is responsible for the name of the use case service quality which is shown in Table 4.1. The first objective of the sequential authentication solution from the operator perspective (SAS-obj-op-1), as shown in Table 4.3 is to provide a network capability 'network performance' that enables SAS-obj-user-1. SAS-obj-op-2 describes the character of the needed network capability 'network performance' to enable SAS-obj-user-1. The description of SAS-obj-op-2 is the result of investigations in Section 3.4.

4.1.2 Requirements

The objectives of SAS are described in Subsection 4.1.1. Beside the objectives, there are general and technical requirements on the sequential authentication solution which are listed in Table 4.4 and Table 4.5.

Requirement Number	Description
SAS-gen-req-1	Avoid unauthorised network access
SAS-gen-req-2	High level of trust among user and access network
SAS-gen-req-3	Privacy of user and confidentiality
SAS-gen-req-4	Use state-of-the-art mechanisms
SAS-gen-req-5	Use of standardised mechanisms
SAS-gen-req-6	Support of real-time services

Table 4.4: General requirements on sequential authentication solution.

The general requirements on the sequential authentication solution (SAS-gen-reg-X) in Table 4.4 are requirements on an AAA solution to enable a carrier grade network access control system with high constrains on security. SAS-gen-reg-1 ‘Avoid unauthorised network access’ is the fundamental requirement of a network access control solution which needs to be ensured. SAS-gen-reg-2 ‘High level of trust among user and access network’ is desired to ensure a trusted relationship among user and access network which avoids device connectivity to malicious access networks. SAS-gen-reg-3 ‘Privacy of user and confidentiality’ aims to avoid intercepting of user data by malicious users. SAS-gen-reg-4 ‘Use state-of-the-art mechanisms’ aims to use mechanisms which are technically most up to date. SAS-gen-reg-5 ‘Use of standardised mechanisms’ aims to avoid proprietary solutions which do not conform to existing carrier infrastructures and user equipment. SAS-gen-reg-6 ‘Support of real-time services’ is needed to deliver real-time services when users are on the move in access networks. The technical requirement on the sequential authentication solution is shown in Table 4.5.

Requirement Number	Description
SAS-tech-req-1	Reduce time of data communication interruptions in WLAN handover processes which are induced by authentication and authorisation methods

Table 4.5: Technical requirements on sequential authentication solution.

SAS-tech-req-1 describes the challenge which has to be solved by the sequential authentication solution to support use case service quality shown in Table 4.1. The objective is to reduce the time of data communication interruptions in WLAN handover processes which are induced by authentication and authorisation methods, especially when using the EAP-TLS method. As shown in Subsection 3.4.6, EAP-TLS is the most time consuming authentication and authorisation method.

4.1.3 Technical Solution

This subsection presents a novel sequential authentication solution to reduce the consumed authentication and authorisation time in the IEEE 802.1X using EAP-TLS network access control process. The reduced authentication and authorisation time will achieve shortened handover process times that finally lead to significant real-time service provisioning improvements when users are on the move in WLANs. The sequential authentication solution combines the network access control methods WPA2 PSK and WPA2 EAP-TLS. The aim is to use both methods in the behaviour as described in the standards. This means, no additional protocol interactions are integrated in the sequential authentication solution.

The SAS fulfils the general requirements on the carrier grade access network presented in Table 4.4. SAS-gen-reg-1 ‘Avoid unauthorised network access’ is provided by WPA2-PSK and WPA2 EAP-TLS. SAS-gen-reg-2 ‘High level of trust among user and access network’ is provided due to mutual authentication by EAP-TLS. SAS-gen-reg-3 ‘Privacy of user and confidentiality’ is enabled by WPA2 with PSK and WPA2 with EAP/TLS. Both methods have the same strong wireless encryption key of the WLAN link. SAS-gen-reg-4 ‘Use state-of-the-art mechanisms’ and SAS-gen-reg-5 ‘Use of standardised mechanisms’ are fulfilled by WPA2-PSK and WPA2 EAP-TLS as well. SAS-gen-reg-6 ‘Support of real-time services’ is realised by a ‘sequential authentication solution’, which is described in the following.

WPA2 with PSK and WPA2 with EAP-TLS have the same strong wireless encryption key. However, the deployment of both mechanisms in WLAN architectures differs from each other. Due to the configuration effort of the PSK in large scale WLANs the management effort increases with the number of access points in the network. Accordingly a reconfiguration of the PSK leads to a high management effort. Besides the benefit of mutual authentication using the WPA2 with EAP-TLS mechanism the management effort can be reduced even in large scale WLAN architectures due to the centralised storage of user authentication data in the network.

The timing diagram in Figure 4.2 presents the generic behaviour of data delivery in wireless access networks when the UE exchanges the point of attachments. In more detail, the relation among handover process, network access and data

communication is shown. During a handover process the network access is not granted, as shown in Figure 4.2 and thus, the data communication is interrupted. This means services, especially real-time services, such as voice over IP, are influenced by this effect. Basically, a voice communication suffers from the length of communication interruption. Depending on the frequency as well as on the length of communication interruption the user will be unsatisfied with the service quality. Consequently, the users QoE of a voice service will not be achieved. The disaffection has a direct impact on the service acceptance as well and influences the decision of the user to use the service in the future again. With the objective to fulfil SAS-gen-req-6 the time of data communication interruption has to be reduced. To decrease the downtime of network access the handover process has to be improved. A reduced handover process time leads to decreased network access downtime and thus, to reduced data communication interruption.

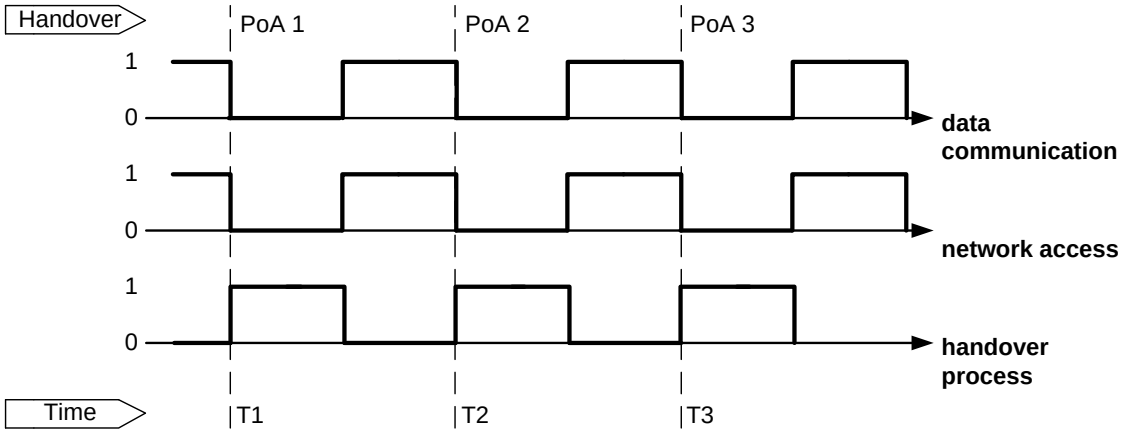


Figure 4.2: Interruption of data communication while handover process.

Figure 4.3 shows the timing diagram of a handover process and its influence on network access and data communication as well as interruption respectively. In more detail, scanning, authentication, association and high layer authentication and authorisation are presented as parts of a handover process. Generally, a network access control process consists of the part authentication, association and in the most cases higher layer authentication and authorisation to investigate the authority of a UE or user respectively to evaluate whether the network access will be granted. Scanning is not involved in a network access control process, but mostly in a wireless handover process to discover available surrounding PoAs. Scanning occurs in a handover process if this feature is activated in the WLAN driver setup.

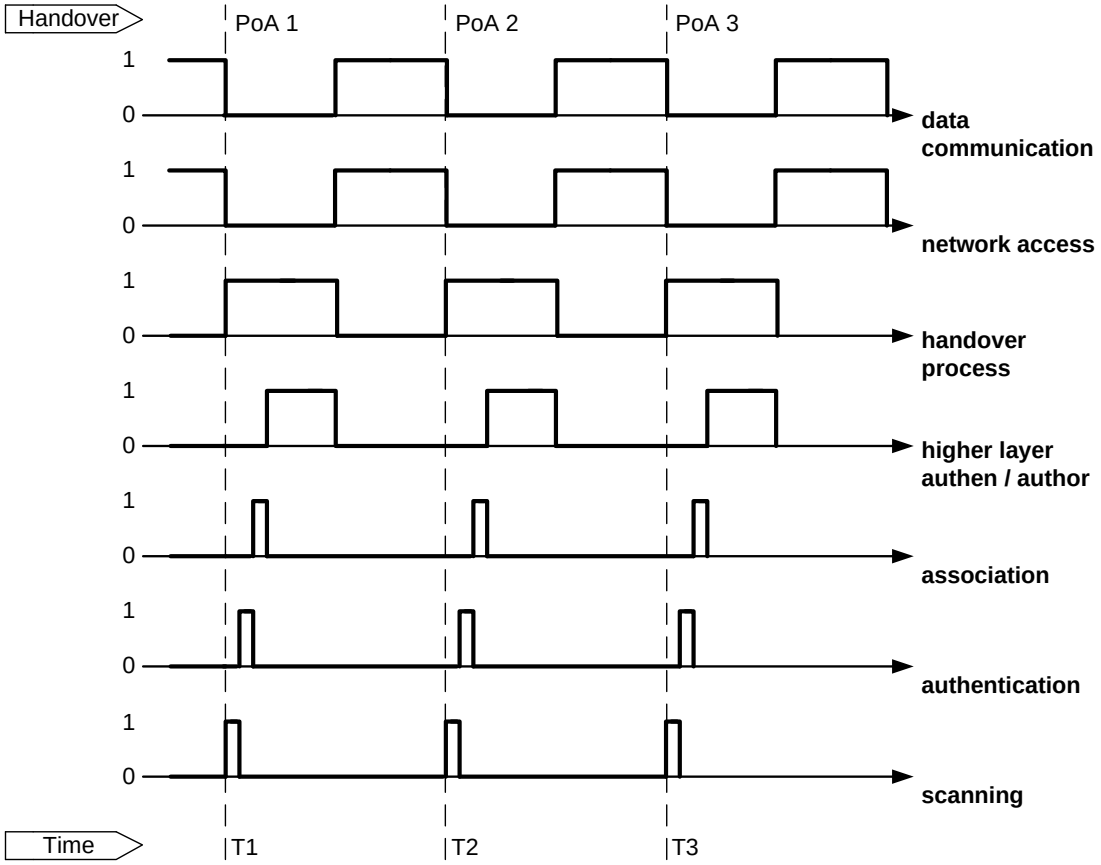


Figure 4.3: Interruption of data communication due to traditional network access control mechanisms.

There are several processes, such as scanning, authentication, association and high layer authentication and authorisation involved in a handover, as shown in Figure 4.3. Each process has its own processing time which contributes to the overall handover processing time. The handover process time t_{HO} is described by (4-1) and consists of the parameters scanning time, t_{scan}, authentication time, t_{auth}, association time, t_{ass} and high layer authentication and authorisation time, t_{hlaa}.

$$t_{HO} = t_{scan} + t_{auth} + t_{ass} + t_{hlaa} \tag{4-1}$$

The most handover time influencing parameter is the high layer authentication and authorisation time as illustrated in Figure 4.3. Own measurements as well as related work [122] and [62] show a high layer authentication and authorisation time of several hundred milliseconds, as shown in Figure 3.15. The authentication time and association time is less handover time influencing, as both times takes only a few milliseconds as presented in [55]. In general the scanning phase can result in a high scanning time as well, but there are approaches to reduce the scanning time by means

of location based handover triggers. Furthermore, the scanning time can be reduced by using known channel parameters of surrounding PoAs provided by the network attachment subsystem. In the case of known channel parameters of surrounding PoAs the UE is able to configure the wireless interface based on these parameters. Thus, no further scanning is necessary.

Figure 4.3 shows in the row data communication that network access is granted and thus, data communication is allowed after the handover process is accomplished. The objective of the sequential authentication solution is to reduce the impact of the higher layer authentication and authorisation time on the handover time. The intention of the sequential authentication solution is to reduce the higher layer authentication and authorisation time by means of two authentication processes followed by each other. The timing diagram of the SAS is presented in Figure 4.4. SAS has two authentication and authorisation processes, shown by the rows higher layer authentication and authorisation phase 1 and higher layer authentication and authorisation phase 2 in Figure 4.4. Both authentication phases are performed sequentially. After successful higher layer authentication and authorisation phase 1 the authentication window (AW), as shown in row authentication window in Figure 4.4, is activated and the higher layer authentication and authorisation phase 2 is initialised. The benefit of this approach is to grant network access already after the first authentication phase. Basically, several types of authentication mechanism could be used in both authentication processes to provide network access control. However, with regard to the state-of-the-art the most secure and BSI recommended mechanisms [76] for business WLAN environments, is the IEEE 802.11i methods that are used in the SAS to fulfil SAS-gen-reg-4 and SAS-gen-reg-5.

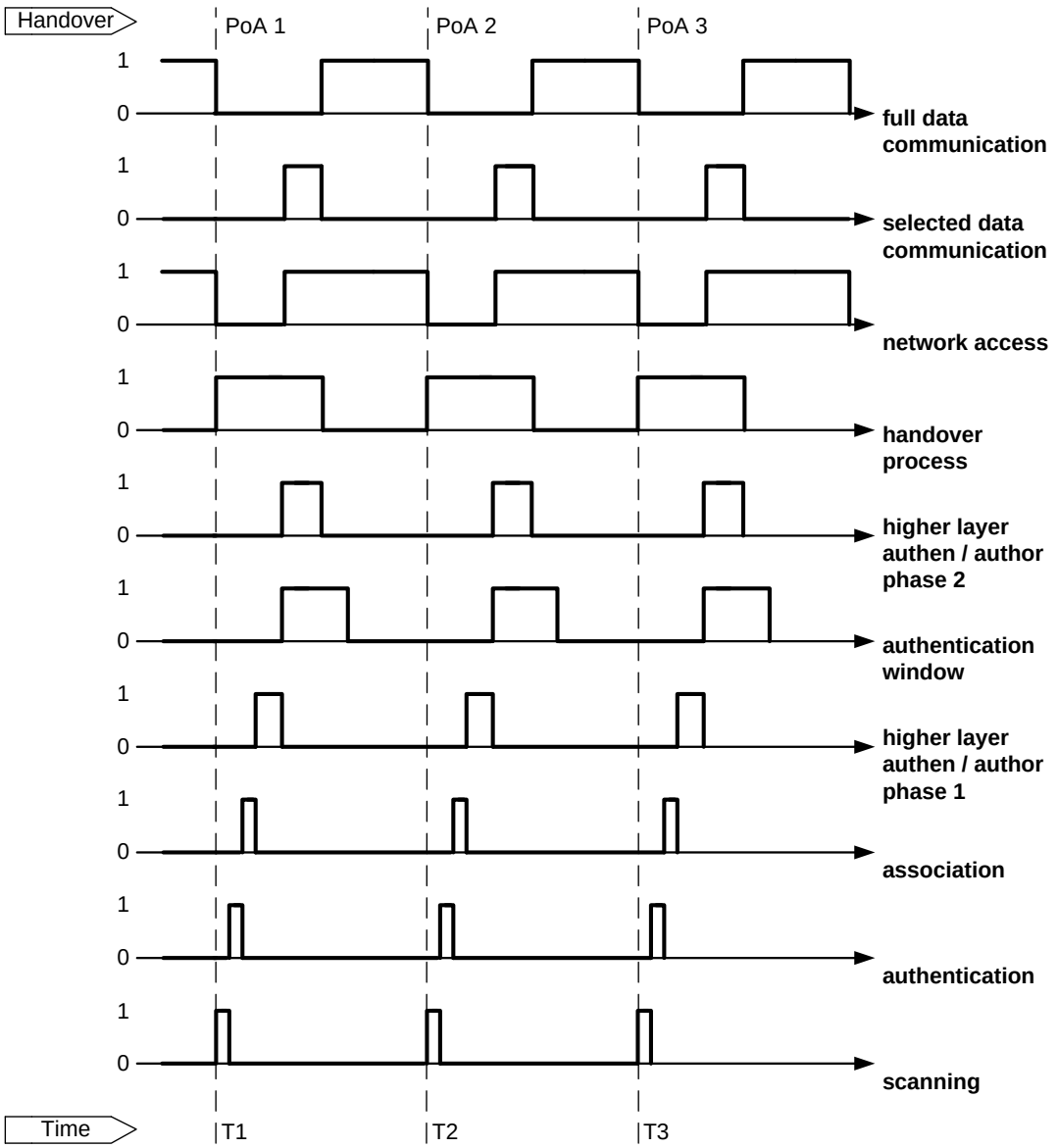


Figure 4.4: Interruption of data communication in SAS.

The higher layer authentication and authorisation phase 1 should provide the shortest authentication time possible considering the requirement SAS-tech-req-1 to provide a reduced time of data communication interruptions in WLAN handover processes. Nevertheless, the WLAN recommendations of BSI [76] have to be considered in the higher layer authentication and authorisation phase 1 as well. BSI [ibid] recommends applying IEEE 802.11i to achieve most secured WLAN architectures. The IEEE 802.11i using IEEE 802.1X with EAP-PSK fulfils these requirements. EAP-PSK use in IEEE 802.11i provides fast possible network access authentication and authorisation, as shown in Figure 3.15 in conjunction with most WLAN secure wireless link encryption.

Approaches, such as [169] describe optimistic network access control. By means of optimistic network access the UE gets network access granted without authentication and authorisation. This behaviour used in the higher layer authentication and authorisation phase 1 would reduce the authentication and authorisation time to a minimum. However, the requirements of SAS-gen-req-1 up to SAS-gen-req-3 of a carrier grade access network would not be fulfilled, because user authentication and authorisation that enables unauthorised network access would not be carried out. Moreover, the privacy of customers and confidentiality would not be provided due to non-secured wireless communication. On the contrary the use of IEEE 802.11i with PSK in the sequential authentication solution provides network access control as well as secure wireless communication. As a result, SAS-gen-req-1 'Avoid unauthorised network access' and SAS-gen-req-3 'Privacy of user and confidentiality' is fulfilled.

The SAS-gen-req-2 'High level of trust among user and access network' is realised in the higher layer authentication and authorisation phase 2 by means of the mutual authentication process of IEEE 802.11i using IEEE 802.1X with EAP-TLS. EAP-TLS uses certificates on the access point and client side to exchange entity identities. The certificates are used on both sides to carry out mutual authentication. However, IEEE 802.1X with EAP-TLS requires time to carry out the whole authentication and authorisation process due to the necessary handshakes, as described in Subsection 3.4.8 and presented in Figure 3.15. Basically, during the IEEE 802.1X process network access in denied for service data exchange, such as VoIP communication, only IEEE 802.1X data exchange, such as handshakes are allowed. To maintain the benefit of the secure but also fast higher layer authentication and authorisation phase 1 followed by granted network access, the higher layer authentication and authorisation phase 2 will not demolish the already granted network access due to the behaviour of the IEEE 802.1X using IEEE 802.1X with EAP-TLS method in higher layer authentication and authorisation phase 2. To avoid restricted network access while carrying out the IEEE 802.1X EAP-TLS method, the sequential authentication solution uses the introduced authentication window. The intention of the AW is to still grant network access while performing the higher layer authentication and authorisation phase 2. The AW is configurable for a certain time. Depending on the required time of the IEEE 802.1X authentication

and authorisation process the time of the AW can be adjusted. Thus, the AW can be used to adjust the SAS to the existing network capabilities and the location of the AAA entities in the network. As a result, the AW can be arranged to be as long as necessary to carry out IEEE 802.1X authentication successfully and as short as possible the carry out mutual authentication. In the case of successful IEEE 8011X with EAP-TLS authentication the granted network access will continue. The SAS process for this access requesting device is finished by closing the AW. In the case of non-successful passing the mutual authentication process the granted network access will be revoked after the higher layer authentication and authorisation phase 1 and thus, the network access is barred for this device. Moreover, the AW is closed. Hence, the sequential authentication process is finished unsuccessfully.

The device is able to gain network access again by reinitiating the sequential authentication process. This fact can be used to start a denial of service attack of a device on the sequential authentication concept. To avoid this, the sequential authentication solution limits the number of authentication initiation repetitions in a certain configurable interval. In the case that a device is not able to carry out the sequential authentication process successfully within the defined authentication repetitions the media access control (MAC) address of the UE will be blocked on the access point for a configurable duration.

In the case a malicious user gets knowledge about the PSK needed to successfully carry out the higher layer authentication and authorisation phase 1. The sequential authentication solution envisions policy based network access. This means the privileges of network access after the higher layer authentication and authorisation phase 1 and 2 differs from each other, as shown in Figure 4.4 by means of the row selected data communication. With the aim to avoid data injected by a malicious user before the sequential authentication process is finished only selected data communication is allowed after the higher layer authentication and authorisation phase 1. All other communication towards the access network will be restricted. Full data communication is allowed after the successful higher layer authentication and authorisation phase

4.2 Barcode Initiated Hotspot Auto-login

In this section the barcode initiated hotspot auto-login (BIHA) solution is presented which enables hotspot use on demand, a hotspot auto-login process, and payment of hotspot use by means of SMS fees. BIHA focuses on the network capability network access and is related to the use case usability, as shown in Figure 4.1. The objective of the use case usability is to improve hotspot comfort in terms of flexible use and user-friendly login.

Section 3.6 WLAN-Based Hotspot describes today's hotspot solution. In general today's hotspot solutions lack of convenience in terms of obtainment of user credentials, entering of credentials and flexibility, such as point of time and duration of hotspot use. Based on the analyses and results of Section 3.6 the barcode initiated hotspot auto-login solution has been developed. BIHA overcomes some drawbacks of today's hotspot solutions and provides flexible delivery of user credentials as well as offers an auto-login mechanism for WLAN-based hotspots. The objective of the barcode initiated hotspot auto-login solution is described in Subsection 4.2.1, while the requirements on this solution are highlighted in Subsection 4.2.2. Then the technical solution is described in Subsection 4.2.3.

4.2.1 Objectives

The BIHA approach is an extension of a generic WLAN-based hotspot architecture, as shown in Figure 3.21. The objectives of the barcode initiated hotspot auto-login are presented in Table 4.6 and Table 4.7. Table 4.6 shows the objectives which are relevant from the users' point of view.

Objective Number	Description
BIHA-obj-user-1	Automated hotspot login
BIHA-obj-user-2	Hotspot use on demand
BIHA-obj-user-3	No barrier of hotspot use for new users
BIHA-obj-user-4	User-friendly way of hotspot payment

Table 4.6: Objective of barcode initiated hotspot auto-login solution from the user perspective.

The first objective from user perspective (BIHA-obj-user-1) is to logon to a hotspot automatically without the need to enter a user name and password in the HLP, as shown in Table 4.6. The second objective (BIHA-obj-user-2) has the intention to provide hotspot use on demand without the need to register at the hotspot portal in an

inconvenient way, such as buying a voucher by means of paying by cash or credit card. The aim of the third objective (BIHA-obj-user-3) is to reduce the barrier for users to use the hotspot even if the user has no login credentials as well as in the case where the user has no customer relationship with the hotspot provider. The fourth objective (BIHA-obj-user-4) envisions a user-friendly way of paying the hotspot fees without the need to enter, e.g. credit card credentials. The objectives of the barcode initiated hotspot auto-login which are of relevance to network operators are shown in Table 4.7.

Objective Number	Description
BIHA-obj-op-1	Enhanced hotspot attraction for users without existing hotspot accounts
BIHA-obj-op-2	Enhanced quality of experience of hotspot usability
BIHA-obj-op-3	Positive side effects, e.g. offloading
BIHA-obj-op-4	Network capability 'network access' that enables BIHA-obj-user-1 till BIHA-obj-user-4

Table 4.7: Objectives of barcode initiated hotspot auto-login solution from the network operator perspective.

As shown in Table 4.7, the first objective from the network operator perspective (BIHA-obj-op-1) is to enhance hotspot attraction for users, even if the user has no contract with the hotspot provider and no user credentials are available at this point. It is assumed that adapted and contemporary hotspot fees and the convenient way of payment via SMS fees will improve the willingness of hotspot use. As a result, hotspots would be used more frequently, which results in additional revenue for the hotspot operator. The second objective (BIHA-obj-op-2) QoE of hotspot usability is to enhance hotspot attraction as well. It is expected that the BIHA improves the hotspot usability. As a result, hotspots will be noticed by the user as a convenient and suitable way to get broadband Internet connectivity with comparable performance as at home. This means, content delivery in QoE satisfying quality can be provided as well. The third objective (BIHA-obj-op-3) envisions positive side effects, e.g. offloading which are stimulated by BIHA-obj-op-2. Due to the assumed fact of BIHA-obj-op-2 that users will increase the hotspot use to get Internet connectivity, it is expected that such user behaviour can contribute to offload mobile networks. As a result, improved hotspot usability would have the positive effect to foster mobile network offloading. The fourth objective (BIHA-obj-op-4) is to provide a network

capability network access that enables BIHA-obj-user-1 to BIHA-obj-user-4 inclusively.

4.2.2 Requirements

The objectives of BIHA are described in Subsection 4.2.1. Beside the objectives, there are general and technical requirements on the barcode initiated hotspot auto-login solution which are listed in Table 4.8 and Table 4.9.

Requirement Number	Description
BIHA-gen-req-1	Avoid unauthorised hotspot network access
BIHA-gen-req-2	Provide traceability of hotspot use
BIHA-gen-req-3	Use state-of-the-art mechanisms
BIHA-gen-req-4	Use of standardised mechanisms

Table 4.8: General requirements on the barcode initiated hotspot auto-login solution.

The general requirements on the barcode initiated hotspot auto-login solution BIHA-gen-reg-X in Table 4.8 are the requirements on an AAA solution. These requirements are used to set the boundaries of a carrier grade network access control system with high barriers for malicious network access. BIHA-gen-reg-1 ‘Avoid unauthorised hotspot network access’ is the fundamental requirement of a hotspot network access control solution which needs to be ensured. BIHA-gen-reg-2 ‘Provide traceability of hotspot use’ is desired to conform to the Telemediengesetz [171] in the case of misuse or violation of an existing law by a hotspot user. BIHA-gen-reg-3 ‘Use state-of-the-art mechanisms’ aims to use mechanisms which are technically most up to date. BIHA-gen-reg-4 ‘Use of standardised mechanisms’ aims to avoid proprietary solutions which do not conform to existing carrier infrastructures and user equipment. The technical requirements on the barcode initiated hotspot auto-login solution are shown in Table 4.9.

Requirement Number	Description
BIHA-tech-req-1	Automated hotspot login
BIHA-tech-req-2	Hotspot use on demand
BIHA-tech-req-3	No barrier of hotspot use for new users
BIHA-tech-req-4	User-friendly way of hotspot payment

Table 4.9: Technical requirements on the barcode initiated hotspot auto-login solution.

The technical requirements are based on the user objectives presented in Table 4.6. BIHA-tech-req-1 to BIHA-tech-req-4 describe the challenges which need to be solved by the barcode initiated hotspot auto-login solution to support usability as

defined in Table 4.1. BIHA-tech-req-1 envisions an automated hotspot login mechanism, BIHA-tech-req-2 a hotspot use on demand, BIHA-tech-req-3 avoids barriers for new hotspot users and BIHA-tech-req-4 enables user-friendly hotspot payment.

4.2.3 Technical Solution

This subsection presents a novel hotspot login approach which enables hotspot use on demand, hotspot auto-login process and payment of hotspot use by means of SMS fees. Figure 4.5 shows the use case diagram of the barcode initiated hotspot auto-login approach which is described in the following.

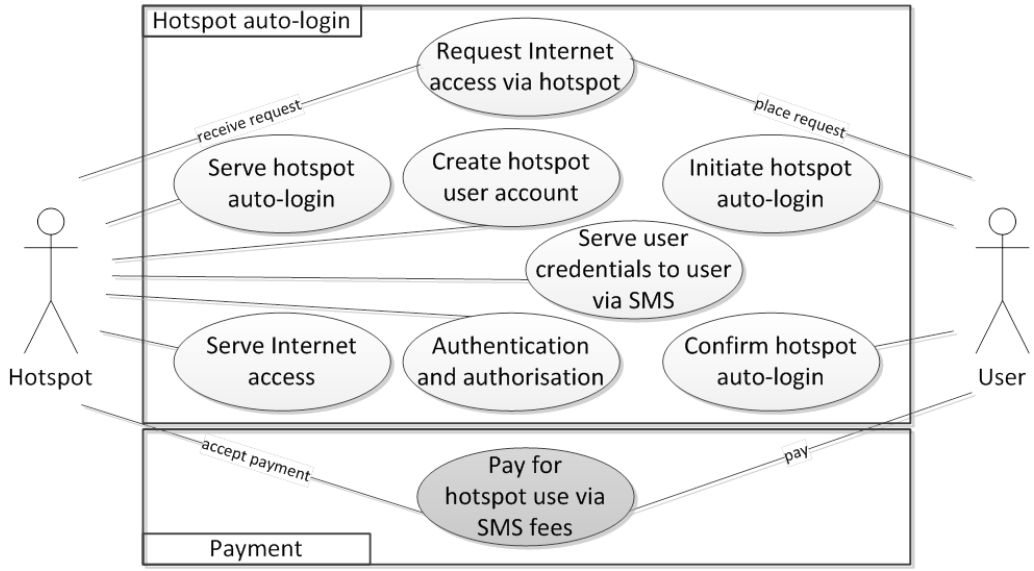


Figure 4.5: Use case diagram of the barcode initiated hotspot auto-login approach.

The use case diagram in Figure 4.5 shows the hotspot auto-login and the payment system. The system hotspot auto-login and payment exists separately from each other. This means the payment system is not mandatory for the hotspot access system. However, from a revenue creation point of view the payment system is necessary. In the following both systems are described from a high level point of view.

Hotspot auto-login system: The functions of the hotspot auto-login system and the order of processing are as follows. 1. The user places a request to get Internet access via the connected hotspot. 2. The hotspot receives the Internet access request and serves the hotspot auto-login method to the user. 3. The user initiates the hotspot auto-login by using the single device or double device auto-login method and

sending a SMS to the hotspot. 4. The hotspot creates a user account. 5. The hotspot sends the user credentials to the user via a SMS. 6. The user confirms hotspot auto-login and continues with the login process. 7. The hotspot performs authentication and authorisation of the user. 8. Internet access is granted.

Payment system: The function of the payments system is as follows. 1. The user pays for the hotspot use through premium SMS fees. The hotspot operator receives the payment from the premium SMS provider.

Figure 4.6 shows the barcode initiated hotspot auto-login architecture which consists of several network segments and entities. The network segments are the hotspot access network and the hotspot backbone network. The hotspot entities are WLAN-based access points, a hotspot access entity and a hotspot core entity. The hotspot access entity consists of a hotspot controller and a web server, while the hotspot core entity consists of an authentication, authorisation and accounting (AAA) server, a database, a voucher server and an information exchange server. The user device is connected to the hotspot via a WLAN-based access point. The hotspot is connected to the Internet via the hotspot access entity. Finally, the user device communicates through the Internet with a content provider (CP).

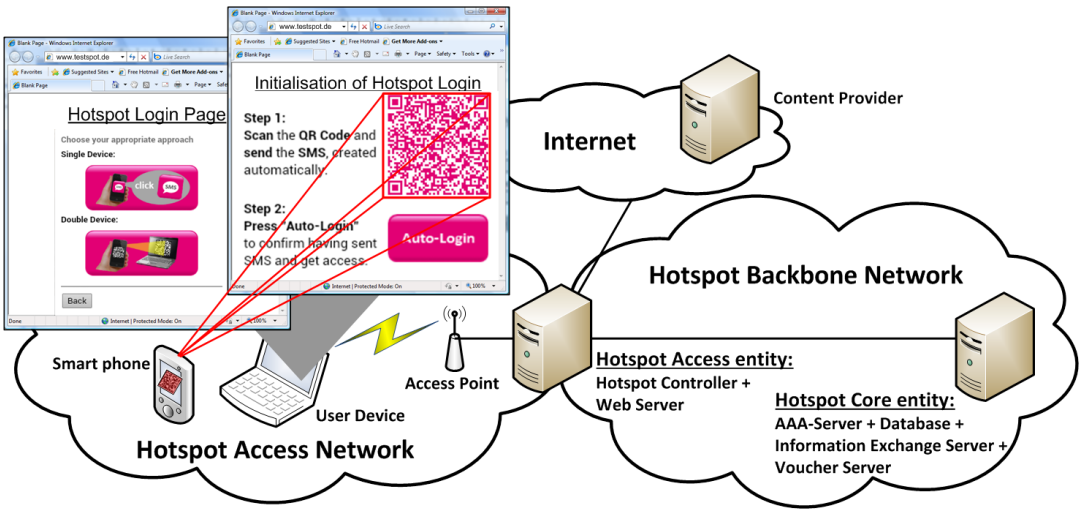


Figure 4.6: Barcode initiated hotspot auto-login architecture.

By means of the BIHA solution the user logs on to the hotspot automatically without entering of user name and password on the hotspot login page. In addition to the automated hotspot logon process the user receives the user name and password via a SMS. Preferably, no extensions of the software or hardware are required on the end user device side. The identification of user and its devices is carried out by

applying double standards. The user with its mobile phone is identified by the mobile phone number, while the hotspot connecting device is identified by means of an identifier (ID), e.g. the MAC address of the WLAN interface or IP address of the WLAN interface.

To access the Internet via the hotspot service the user is connected with their device to an access point of the hotspot architecture. The landing page of the hotspot is presented to the user after the user starts the web browser and requests a URL by means of the browser. In most of today's landing pages the user gets offered a login area. In this login area the user is able to enter the user credentials, such as the user name and password. After entering the user credentials the authentication and authorisation process is started. As described, in this method the user needs to be aware of the user name and password beforehand. Moreover, the logon procedure has to be performed manually. There is no mechanism to request the user credentials and to provide an auto-logon to the hotspot.

Before the user is able to use the barcode initiated hotspot auto-login solution, they have to connect to the WLAN of the hotspot. Moreover, the user has to start the web browser and needs to request a URL. Due to the redirect mechanism of the hotspot solution the web browser is redirected to the landing page of the hotspot, which provides the possibility for the user to logon to the hotspot by means of entering the user credentials, such as user name and password. This hotspot logon behaviour is as usual. By means of the BIHA solution the user sees, in addition to the traditional login area, an auto-login area on the landing page.

The auto-login area offers two methods to the user to initiate the auto-logon process for getting access to the hotspot. The first method envisages a single device such as a tablet PC with a SIM-card inside. The second method envisages two devices, such as the hotspot connecting device e.g. laptop or tablet PC without a SIM-card and a mobile phone with a SIM-card. The first method addresses users who use a single device to consume Internet services. The annotation of this method is that the user device contains a SIM-card. The second method double device addresses users who consume services in the Internet on a user device which contains no SIM-card and is thus, not able to send SMS. For the purpose of sending SMS the user uses a smart phone in addition to the user device. Both methods use SMS. The sending party (the user) is identified by its mobile phone number. This number is

used to build a relation between mobile phone user and hotspot user. The first method uses an automatic generated SMS link presented on the login page to open a SMS tool on a smart phone. The second method uses an automatic generated barcode, e.g. a QR code, which is presented on the login page. To obtain the SMS a barcode or a QR code reading application [172] on the smart phone is used to trigger the opening of the SMS tools.

The first auto-login method is initiated by clicking on a predefined link in the auto-login area. This link is used to trigger the opening of the SMS tool on the device. All the information needed for SMS creation is comprised in the link. This information will be filled in the SMS tool of the device automatically after clicking on the link. The information in the link is e.g. user-identifier, device-identifier, network-identifier, mobile phone identifier and voucher server identifier.

The second auto-login method is initiated by scanning the barcode, e.g. a Quick Response (QR) code, in the auto-login area. Further information about the barcode is described in Appendix A.1. For this auto-login approach a state-of-the-art barcode scanning tool, e.g. i-nigma [ibid] is needed. The barcode reading application is used to trigger the opening of the SMS tool on the mobile phone. All the information needed for SMS creation is contained in the barcode. The information in the barcode is e.g. user-identifier, device-identifier, network-identifier, mobile phone identifier and voucher server identifier.

In both auto-login approaches the created SMS is used to trigger the user account creation in the hotspot backbone architecture. The SMS is received by the voucher server. The voucher server is addressed by a phone number specified in the link or barcode. Based on the received SMS, the voucher server creates a new user account in the hotspot user database. The user account is described by means of several identifiers, such as user-identifier, device-identifier, network-identifier and mobile phone identifier. The user name to log into the hotspot is set to the mobile phone identifier, such as the mobile phone number. The password is set to a randomly created value.

After the user account creation, the voucher server sends the user name and password back to the user's SMS sending device. As a result, the user knows the hotspot login credentials. The user is now able to enter the hotspot login credentials manually in the hotspot login area. Furthermore, by means of the BIHA solution the

user is able to click on the auto-login button in the auto-login area which will logon the connected device automatically to the WLAN hotspot. As a result, the user and the device get logged into the hotspot without the need to enter the user credentials on the hotspot login page.

Figure 4.7 presents the sequence of the BIHA solution applying the double device method. It is assumed that a WLAN-based connection between the device e.g. a laptop or tablet PC and the hotspot access point is established.

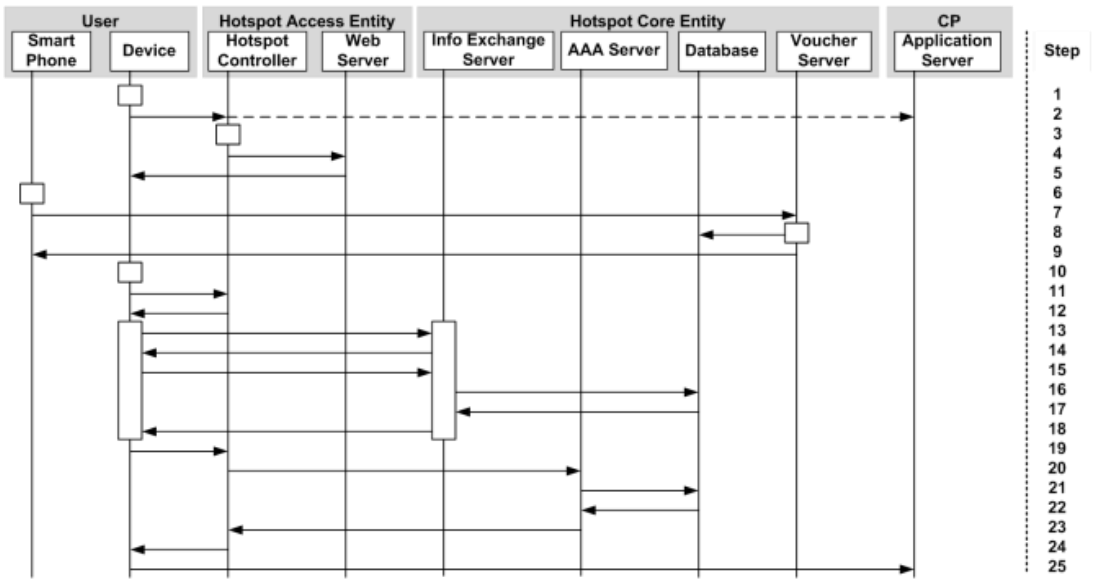


Figure 4.7: Sequence diagram of BIHA solution.

In step 1, shown in Figure 4.7 the web browser on the device is opened. The web browser aims to open a website in step 2 and initiates an http request to an application server (AS) located in the Internet. In step 3, the hotspot controller (HC) recognises that the user device is not authorised to get Internet access until now. Due to this, the HC forward the http request of the web browser to the web server (WS) of the hotspot in step 4. In step 5, the WS answers with the hotspot login page comprising the hotspot auto-login functionalities in addition to the manual login approach (entering of user name and password). The barcode is presented in the web browser according to the selected auto-login method double device. In step 6, the user uses its smart phone camera and the installed barcode reader software to scan the displayed barcode. The barcode is generated automatically and exclusively for the currently connected user device by the barcode generation entity inside the web browser. The information contained in the barcode is the network identifier of the hotspot, the hashed value of the MAC address of the user device and additional

verification parameters which allows the identification of the type of device, e.g. smart phone or user device. In step 7, the user sends a SMS to the voucher server (VS). The VS is equipped with a general packet radio service (GPRS) interface and is addressed by a phone number specified in the barcode (identifier of voucher server). The SMS is received by the SMS receiving and sending entity. In step 8, the hotspot user database is checked by the hotspot account checking entity to verify whether or not the user does already exist. The user is identified by their mobile phone number. In the event that the user already exists in the database, the hotspot account updating entity deactivates the previous user account and a new user account is created by the hotspot user account creation entity. A hotspot user account in the database is described by the parameters nasID (network identifier), HMAC (hashed MAC address of user device), user name (the user's mobile phone number) and password (a randomly generated value). The nasID and HMAC values are extracted from the SMS received. In step 9, the SMS receiving and sending entity of the voucher server sends the created user credentials to the user's smart phone by SMS. The SMS includes user name and password which can be used to logon to the hotspot manually by entering of user name and password. The user name is equal to the user's mobile phone number.

In step 10, the user presses the auto-login button on the login page to initiate the auto-login process. In step 11, a client status update request is sent from the user's web browser to the hotspot controller. This request verifies whether or not the user is already logged on. In step 12, the HC sends back a response to the browser. The response includes the current client status and also the current challenge which is needed for the challenge authentication protocol (CHAP). The parameter challenge, client state, location name, original URL, log out URL, client's IP address and client's MAC address is sent back. After retrieving the current challenge and client state, in step 12, the web browser is ready to initiate the auto-login process by communicating with the information exchange server. The aim of this communication is to send the required verification information (nasID, HMAC, challenge) and to receive the user name and challenge handshake authentication protocol (CHAP) password for the auto-login process. The CHAP password only works for the current session and user device. For that purpose, in step 13 and step 14 the information channel is established. In this implementation the WebSocket

[173] communication protocol is selected due to its simplicity, efficiency and minimal transport time of the protocol. After successful establishment of the information channel, the browser sends the verification information nasID, HMAC and challenge as a text message via the WebSocket connection to the information exchange server in step 15. The verification information (nasID, HMAC and challenge) are extracted by the information exchange server and are used to prepare a user verification process which checks the existence of a user account in the database. The parameters nasID and HMAC are used to query the database in step 16, to retrieve the related user credentials. In the event that the user account exists, the related user credentials, such as user name and password are taken from the database and are sent to the information exchange server in step 17. Based on the parameters challenge and password, received in step 10 and step 12, the information exchange server generates a CHAP password utilizing the CHAP authentication technique [174]. In step 18, the information exchange server sends the login credentials back to the user's web browser via the information channel.

After successful credential delivery to the web browser a CHAP login attempt is triggered automatically by the login module which runs in the web browser. In step 19, the login module initiates a CHAP login process by sending the user credentials to the hotspot controller. The HC receives the CHAP logon request from the login module and processes it automatically by submitting an access-request to the AAA server as performed in step 20. The communication protocol between the hotspot controller and AAA server is the RADIUS protocol. To perform the authentication and authorisation process, the AAA server obtains the password from the database in step 21 and step 22. The user is identified by the user name, which is the phone number of the user's smart phone. The result of the authentication and authorisation process is sent from the AAA server to the HC in step 23. In the case of a successful user authentication and authorisation, the HC grants Internet access for this specific user device. In step 24, the user gets informed about the authentication status in the web browser. As a result, interaction between user device and application server is in step 25 possible.

Charging in the BIHA solution can be carried out by means of a premiums SMS service. Premium SMS solutions are often used in conjunction with micropayment of logos, ringtones or mobile voting. With regard to the barcode initiated hotspot auto-

login, the premium SMS service enables a flexible pricing of the hotspot use. The premium SMS service is transparent for the BIHA solution. This means no change to the BIHA solution is needed. A premium SMS service allows the hotspot owner to design the pricing according to his demands, which only depends on the premium SMS service agreement with the provider. The implementation of the barcode initiated hotspot auto-login solution is described in Section 5.2.

4.3 Graceful Denial of Service for IP-based Application Services

This subsection presents a novel added value service called graceful denial of service (GDoS) which acts as a service quality indicator. GDoS is a kind of busy signal for IP-based services which informs the user about the application service quality to be expected before an application service is started. For that purpose information about the application service requirements on network performance and the available network capabilities are needed to derive the GDoS feedback for the user. The GDoS philosophy is equal to the busy signal in traditional telephony. This means, the GDoS feedback is presented to the user only in the case that the application service is not providable at the user requested quality. GDoS focuses on the network capability network features and is related to the use case quality awareness, as shown in Figure 4.1. The objective of the use case quality awareness is to inform the user about the application service quality to be expected in advance before an application service is started.

Section 3.7 described today's situation of service delivery in user satisfying quality. Most of today's application services are not network and device aware. Based on the analyses and results of Section 3.7 the graceful denial of service has been developed. GDoS can be understood as an added value service which enables awareness among network capabilities and application requirements which results in information feedback to a user.

With the intention to improve the ability to develop network services, application services and added value services in a more convenient manner as well as to structure and separate these services from each other, the service enhancement functional area with its service enhancement functions has been introduced. The GDoS solution is presented as an example and presents how the methodology of

service enhancement functions can be applied in the context of new service developments.

4.3.1 Service Enhancement Functional Area

Major challenges of today's network operators are on the one hand side to deliver application services in end-user satisfying quality as highlighted in Section 3.7 and on the other hand to overcome the fact to be just bit-pipe providers as described in Section 3.8. A useful approach to overcome the fact just to be bit-pipe providers is to use existing assets of the network operators architecture and to build new services and added value services in a flexible way which are adjusted to the use case requirements. For this purpose the service enhancement functional area (SEFA) methodology is introduced with the intention to support the development of new added value services for application and network services.

Satisfied users in next generation service (NGS) provisioning and novel service perception will depend on the ability to provide flexible, user-friendly and personalized services (FUPS). Moreover, the privacy aspect will become more and more important in NGS. Figure 4.8 presents the background of FUPS and describes what FUPS means, what the benefits are and what the characteristics are as well as which preconditions are needed to achieve FUPS in future NGS architectures. The base to enable FUPS will be the use of overarching application service and network service control mechanisms. In the context of the SEFA methodology these overarching control mechanisms are called service enhancement functions (SEFs).

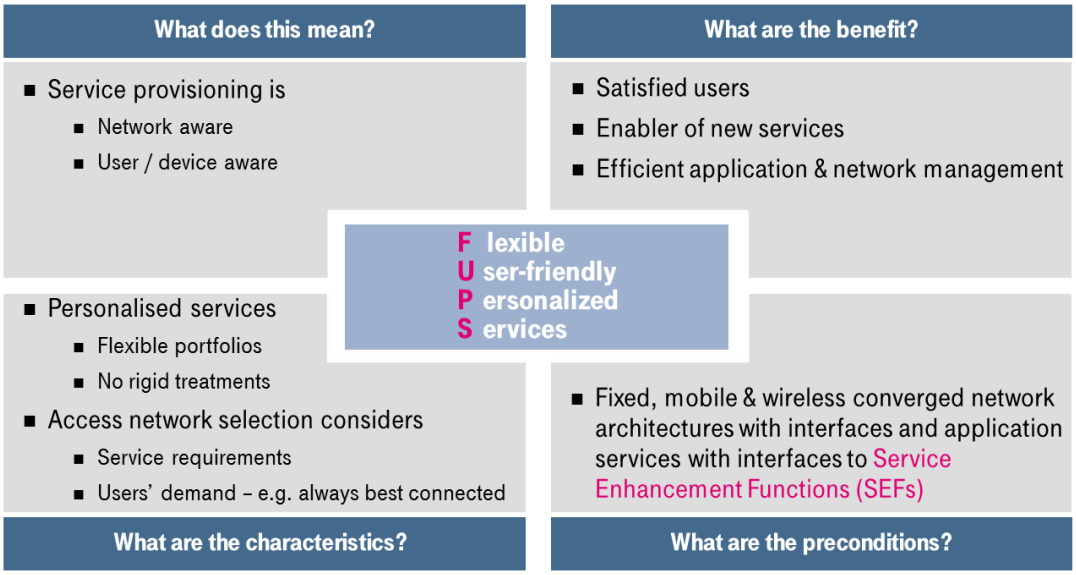


Figure 4.8: FUPS as key factors of next generation service provisioning.

FUPS enabler will be the precondition of next generation service provisioning, as shown in Figure 4.8. Such FUPS enabler will be realised by overarching application services and network service control mechanisms. Each enabler performs a specific task to realise the required added value service which enriches an application service or network service. In the context of the SEFA methodology these enablers are called service enhancement functions (SEFs) which are applied to instantiate and coordinate an added value service. A SEF can be understood as an intermediate function between device, customer profile, network service and application service which is needed to perform a specific task, as shown in Figure 4.11. From the network architectural point of view the SEF is a placeholder that is used to describe a required mechanism, process and functionality to realise a certain added value service which enriches an application or network service. Figure 4.9 a) presents the location of the SEFA in relation to application and network plane while in Figure 4.9 b) three SEFs are shown, which support application service 1 and 2.

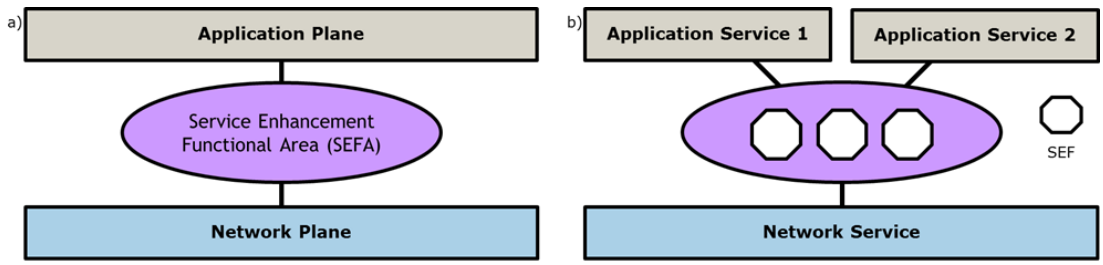


Figure 4.9: Service enhancement functional area in relation to application and network plane.

The service enhancement functional area can be understood as an abstract container of use case specific functionalities called service enhancement functions to enable new services in the application and network plane. SEFA defines, according to the use case, the place to enrich the network and application plane functionalities by means of the use case required SEFs, as shown in Figure 4.9 b). SEFs are able to interact between the actors of a use case, such as e.g. content service provider, network service provider and end-user device. A specific added value service is represented and instantiated by means of one or several use case specific service enhancement functions, as shown in Figure 4.10. These SEFs gather and combine information or parameters to create the specific added value service or to provide information and parameters to other services which are not involved in this added value service itself. The generation of added value is based on the interaction

between SEFs, network, application, devices and user. Each specific added value service requires individual SEF implementations and specific parameter sets to support a specific use case.

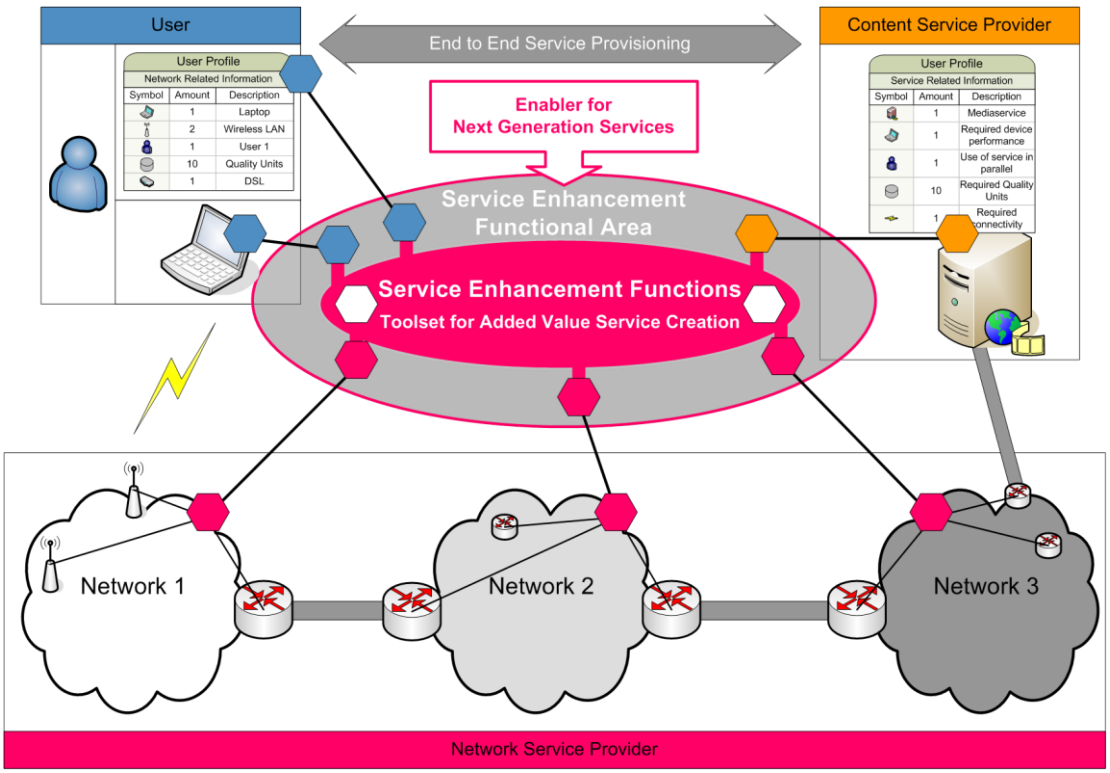


Figure 4.10: Example: several service enhancement functions to realise a certain use case.

In addition there are no restrictions regarding the type of functionalities which the specific SEF performs or the plane it belongs to. As a consequence SEFs can be application service functions or network service functions. SEF examples in the network plane are resource admission control functions, routing functions or capacity sharing functions. An application plane SEF could be for instance session handling, session specific accounting and billing functionalities. A high-level definition of the SEFA and its purpose is:

- SEFA is an abstract area of a deployed network architecture that extends the existing architecture towards specialized added value services.
- These added value services can be used to produce and enrich higher layer application services as well as network services.
- SEFA interacts with planes, e.g. data, control, network service business and management plane to gather, trigger, combine and control added value service specific parameters and actions.

- The specific added value service is represented and instantiated by means of one or more individual service enhancement function (SEF) inside the SEFA.
- SEFA is an abstract functional area that contains all possible SEFs.

In this context the service enhancement function can be understood as follows:

- The SEF represents a full or a part of a specific added value service or function realized by means of an individual implementation.
- SEF has value added service specific interfaces to application and network services.
- In general the SEF consists of two components:
  - Logic: The entirety of functionalities that characterize and form the specific service enhancement function.
  - Interface: Communication between SEFs within the SEFA and information and parameter providing to external units or systems, e.g. RACS [162] or NASS [163].
- Multiple SEFs can interact with each other or can be combined to more complex added value service.

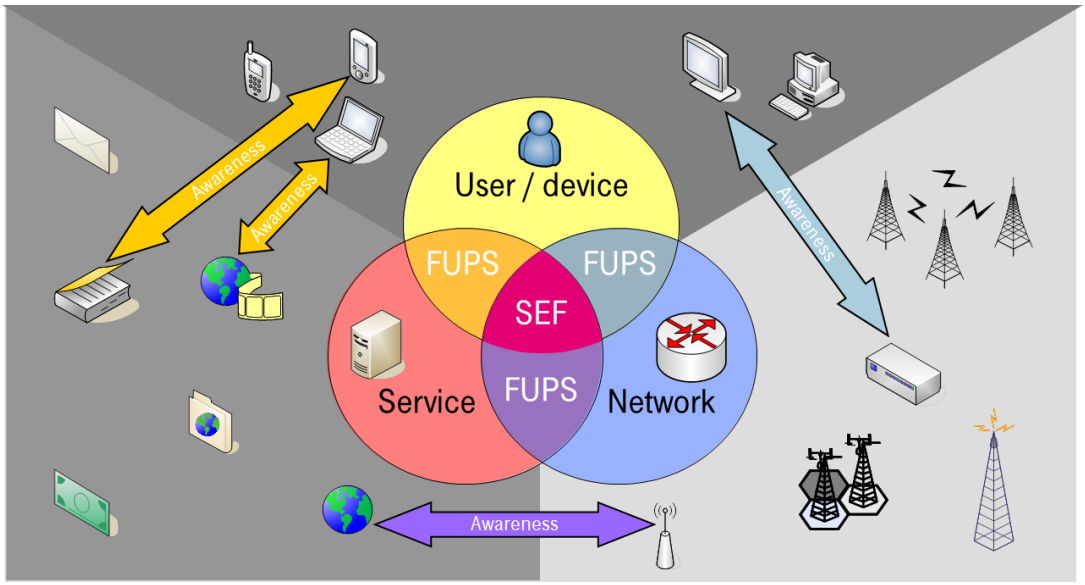


Figure 4.11: Mutual awareness of service, network and customer based on SEF.

In general the SEF can be designed and implemented proprietary depending on the functionality needed. As a result, the SEF can be realised based on the requirements of the network or application providers to enable added value in the revenue chain. However, with regard to future proofness and extensibility it will be useful and necessary to design the SEF to be conformable with next generation

network and next generation mobile network architectures. In this context the provisioning of interfaces to interact among the required entities and to exchange added value related information is necessary as well. With regard to standard compliance in the presented approach in Figure 4.12 the SEF interacts with the network attachment subsystem (NASS), resource and admission control subsystem (RACS) and IP multimedia subsystem (IMS). The NASS, RACS and IMS are standardised by ETSI TISPAN and have different responsibilities.

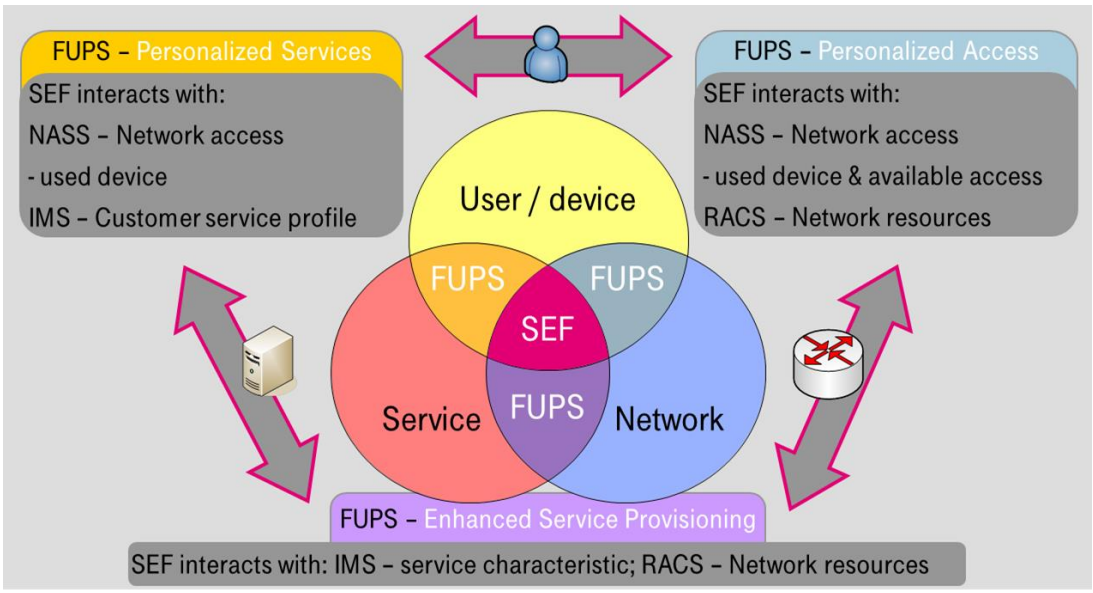


Figure 4.12: SEF as intermediate entity among standardised frameworks, such as NASS, RACS and IMS.

The IMS architecture provides the basic platform to introduce service and network convergence. Initially the IP multimedia subsystem was developed as a call control framework for packet-based services over 3G mobile networks as part of 3GPP, i.e. an overlay over GPRS to provide IP services. After that it was extended to include WiFi roaming and additional services, such as the presence and instant messaging in release 6 [161]. The IMS introduces a common session control plane, suitable for any access technology capable of transporting session initiation protocol (SIP) messages, providing an access independent service delivery platform. The IMS core consists of SIP entities called call session control functions (CSCF) and a central user database, the home subscriber server (HSS). IMS extends SIP to be the signalling protocol to control real time and non-real time multimedia sessions of provided services.

The IMS is being standardised by the TISPAN in ETSI as a converged multimedia network and thereby as the core architecture of their next generation network [176].

The standardisation process defines multiple subsystems that enable fixed access networks to interface the IMS. TISPAN closely interacts with 3GPP to leverage the IMS specification over wireless networks. In detail, TISPAN introduced the network attachment subsystem (NASS) [163] responsible for authentication, authorisation and access management, and the resource and admission control subsystem (RACS) [162] which is responsible for QoS resource reservation, admission control and policy enforcement.

The RACS abstracts access network related details from an application function (AF), e.g. IMS proxy call state control function (P-CSCF) as described in [ibid]. Moreover, the RACS intends that the policy enforcement resource control enforcement function (RCEF) ensures that the associated user traffic remains in accordance with the policy decision. The access resource and admission control function (A-RACF) supports the resource reservation methods, admission control and final policy decisions. In general user traffic is only admitted if three constraints are met: (i) the user profile is stored in the NASS, (ii) operator-specific policies and resource availabilities are met, and (iii) border gateway functions (e.g. network address translation) are clarified.

The NASS provides user authentication prior or during the IP address allocation procedure. Dynamic provisioning of IP address or equipment configuration parameters, e.g. DHCP is carried out by the NASS as well. Moreover, the authorisation of network access is performed based on user profile. In this context, the access network configuration is realised based on user profile as well. Beside the location management the NASS is responsible for the interaction with QoS control entities, e.g. RACS, to deliver QoS information to setup user related QoS performance in the network.

Figure 4.13 presents an overview about the NGN control architecture subsystems, such as the network access control related NASS, the QoS related RACS and service control related IMS described in [176]. In this context the relations between the subsystems as well as the application, user equipment, transport functions and other networks is shown. Moreover, the depiction of user profiles indicates the importance of user information regarding NGN network access and service provisioning.

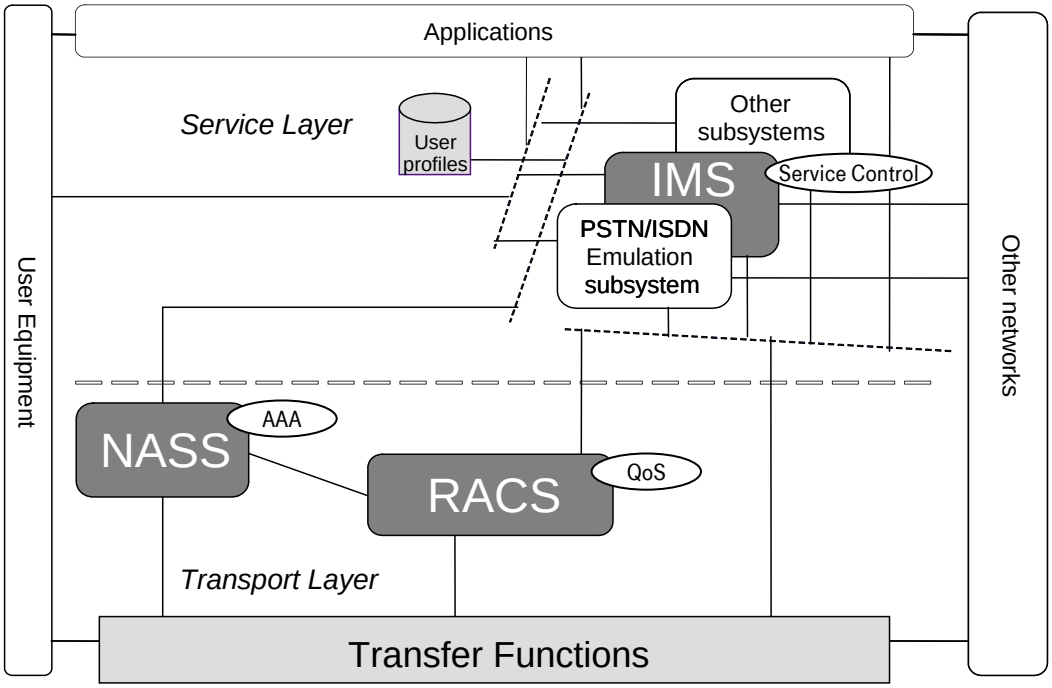


Figure 4.13: ETSI TISPAN NGN architecture overview.

The layered architecture of IMS allows the definition of service enablers (e.g. presence, group and list management) and common control functions (e.g. provisioning, security, charging, operation and management) that can be reused for multiple applications. However, the integration and deployment of new business models and business processes is hard, because these models often require provider specific processes that are not mapable to a generic IMS architecture. At this point the SEF is used as an intermediate function interacting with the IMS, RACS and NASS to collect and evaluate business model related information with the goal to control network or application services in line with the provider business model and process constraints. In any case, the SEF concept is not limited to the subsystems, such as IMS, RACS and NASS. It is also possible to design the SEF without interacting with these subsystems. In such a case the SEF will obtain network or application related information by means of a proprietary systems to deploy the desired business model. As a result, the SEF concept is also useful for non-IMS based service architectures and thus, can enable flexible and provider individual service provisioning.

As shown in Figure 4.12 the FUPS (flexible, user-friendly and personalized services) are split in three parts, personalized service, personalized access and enhanced service provisioning. In the case of FUPS - enhanced service provisioning -

the SEF interacts with the IMS and the RACS to investigate the current network performance and service characteristic with the aim e.g. to determine the best application service quality that can be supported by the network architecture. As a result, the service quality e.g. can be adapted depending on the available network performance. Even if the service quality, e.g. the video resolution, is not as high as possible the service can be provided without disturbance. Thus, the adaptation of service and the non-disturbance of service provisioning contributes to the enhancement of quality of user experience. Concerning the FUPS – personalized access – the SEF interacts with the NASS and the RACS to survey the currently connected type of device and available network interfaces within the device. Moreover, the current network performance in the different access networks is investigated. The goal of the personalized access is e.g. to select the most suitable network interface to realise, for instance different use cases of connectivity, such as best bandwidth or cheapest connection. In the case of FUPS - personalised services - the SEF interacts with the NASS and the IMS to survey the currently connected type of the device and the application service profile of the user with the aim to offer personalized services or information, such as "Dear user your device is able to display the currently viewed video in higher quality. Are you interested in the HD version?".

The SEFA methodology aims to separate the use case requirements which can be different from one use case to another. The intention of the methodology is to develop added value services which are light weight and requirement driven without the need to deploy an entire, complex framework. Of course, parts of existing frameworks can and should be part of the developed added value service solution. The set of SEFs which are needed for a certain use case provide that amount of awareness among all actors and network segments which are needed to provide a added value service for this specific use case. One assumption of this methodology is that actors participating in a specific added value service are willing to deploy non-standardised solutions in their architecture to achieve a benefit in terms of simplicity and time to market for an added value service.

A SEF that combines the aspects of FUPS – enhanced service provisioning, – personalized access, – personalised services will achieve the maximal of mutual awareness among user characteristics, service requirements and network

performance. The precondition of the SEF to provide mutual awareness among user, device, application service and network service is the ability to get information of all of these actors. This means, the preparation and provisioning of such information is important. The retrieval of application and network related information in the context of SEFA/SEFs is described by means of the introduced added value service graceful denial of service in the following sections.

4.3.2 Objectives

The GDoS solution is an information service which informs the user about to be expected application quality that is delivered in advance. The objectives of the graceful denial of service solution are presented in Table 4.10 and Table 4.11. Table 4.10 shows the objectives which are of relevance from users point of view.

Objective Number	Description
GDoS-obj-user-1	Information about application quality to be delivered

Table 4.10: Objective of graceful denial of service solution from user perspective.

The first objective from a user perspective (GDoS-obj-user-1) is to be informed about the delivered application quality to be expected in advance to decide whether to start the application service or not, as shown in Table 4.10. The objectives of the graceful denial of service solution which are of relevance for network operators are shown in Table 4.11.

Objective Number	Description
GDoS-obj-op-1	Enhanced quality of experience in application service delivery
GDoS-obj-op-2	Creation of added value out of network operator assets
GDoS-obj-op-3	Positive side effects, e.g. service bundling
GDoS-obj-op-4	Network capability ‘network features’ that enables GDoS-obj-user-1

Table 4.11: Objectives graceful denial of service solution from network operator perspective.

As shown in Table 4.11, the first objective from network operator perspective (GDoS-obj-op-1) is to enhance the quality of experience in application service delivery by means of a feedback system which informs the user about the expected application service quality. The intention of GDoS is not to influence or restrict the service delivery process itself, but rather to provide a feedback to the user which does not exit. The GDoS offers the user the opportunity to decide how to continue with its service request taking the expected application quality into account. The

second objective (GDoS-obj-op-2) has the intention to use network capabilities, e.g. information about the network performance in certain network segments to create added value out of the network operator assets. The GDoS could be such an added value service which supports sensitising users and to illustrate what network performance means in the context of application service delivery to the user. As a result, users could become more aware about the influence of application service requirements on network performance and the influence of network performance on delivered application service quality. The third objective (GDoS-obj-op-3) is to derive positive side effects based on the created added value services to achieve unique selling points. For instance, the SQI can be bundled with a video service of a third party provider. As a result, the user will be informed whether a video of the third party provider will be provided in requested quality or not. The fourth objective (GDoS-obj-op-4) is to provide a network capability network features that enables GDoS-obj-user-1.

4.3.3 Requirements

The objectives of GDoS are described in Subsection 4.3.2. Beside the objectives, there are general and technical requirements on the graceful denial of service solution which are listed in Table 4.12 and Table 4.13.

Requirement Number	Description
GDoS-gen-req-1	Use state-of-the-art mechanisms and protocols
GDoS-gen-req-2	Use of standardised mechanisms and protocols

Table 4.12: General requirements on graceful denial of service solution.

The general requirements on the graceful denial of service solution (GDoS-gen-reg-X) in Table 4.12 are requirements on a distributed and information collecting solution to enable an added value service which interacts with several involved parties and with high constrains on system integration. GDoS-gen-req-1 describes the use of state-of-the-art mechanisms and protocols which are technically most up to date. GDoS-gen-req-2 envisions the use of standardised mechanisms and protocols that aim to improve the integration into the infrastructures and systems of the involved parties. The technical requirements on the graceful denial of service solution are shown in Table 4.13.

Requirement Number	Description
GDoS-tech-req-1	Graceful denial of service processing entity
GDoS-tech-req-2	Provide application service requirements on network performance to graceful denial of service processing entity
GDoS-tech-req-3	Provide available network capabilities to graceful denial of service processing entity
GDoS-tech-req-4	Offer graceful denial of service result to user

Table 4.13: Technical requirements on graceful denial of service solution.

The technical requirements are based on the user objectives presented in Table 4.10. GDoS-tech-req-1 till GDoS-tech-req-4 describes the challenges which need to be solved by the graceful denial of service solution to support the use case quality awareness illustrated in Table 4.1. GDoS-tech-req-1 envisions a graceful denial of service processing entity, GDoS-tech-req-2 the provisioning of application service requirements on network performance to the graceful denial of service processing entity, GDoS-tech-req-3 the provisioning of available network capabilities to the graceful denial of service processing entity and GDoS-tech-req-4 the offering of graceful denial of service results to the user.

4.3.4 Technical Solution

This subsection presents a technical solution to the novel added value service graceful denial of service (GDoS) which acts as a service quality indicator. A generic network architecture applying the graceful denial of service is shown Figure 4.14 and consists of several inter-connected network segments, such as the information service provider (InfSP), edge network service provider (ENSP) 1 and 2, and home network (HN). The CP is connected to ENSP1 while the home network is connected to ENSP2. Data transmission from CP to the end-user is realised by the inter-connection of ENSP1 and ENSP2. It is possible that other network service providers (NSPs) are involved in inter-connecting ENSP1 and ENSP2. The end-user with its device is connected to the HN. Exemplarily, the GDoS solution is described in relation with a video delivery scenario.

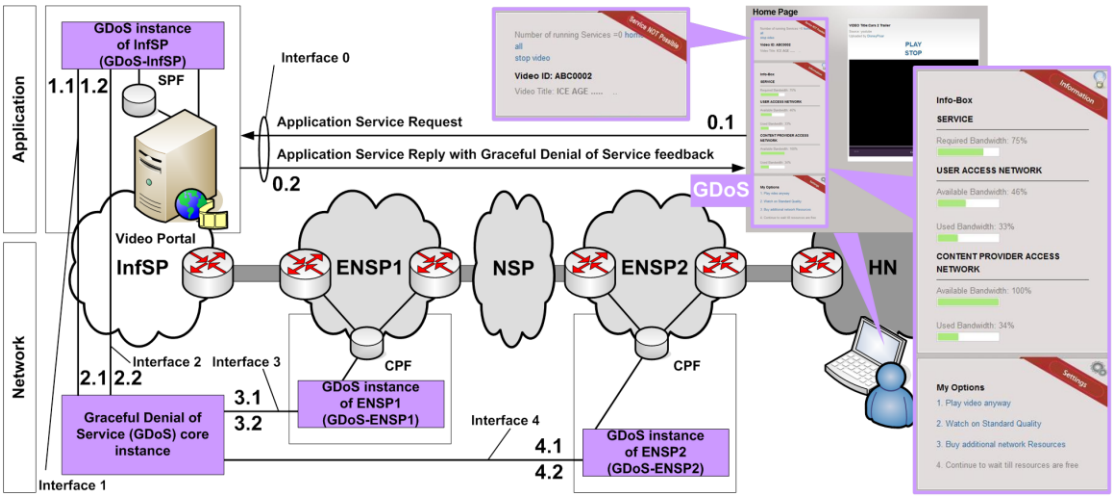


Figure 4.14: High-level view on graceful denial of service architecture.

A video portal is located in the content provider network, as shown in Figure 4.14. The network segments ENSP1 and ENSP2 comprise of a connectivity profile database (CPDB). The CPDB contains network performance capability information of the connected customer, e.g. the CP and the end-user. Network performance capability information is, e.g. delay, jitter, packet loss as well as bandwidth characteristics of other inter-connecting network segments. Besides that, the content provider uses a service profile data base (SPDB). The SPDB contains, e.g. application service requirements on the network performance (e.g. delay, jitter, packet loss and bandwidth) which are needed to deliver the application service in the requested quality.

In the example illustrated, the user requests an application service, e.g. video on demand (VoD), in high definition (HD) quality from the content provider. The application server recognizes the service request of the user device via interface 0 (0.1). The application server sends a graceful denial of service evaluation request (trigger) via the interface 1 (1.1) to the graceful denial of service core entity to initiate the evaluation process regarding the availability of network resources for a HD video on demand service along the data delivery path. The network segments of CP, ENSP1 and ENSP2 consists of a graceful denial of service instance according to the required functionalities which are needed in a network segment. The GDoS core instance can be located wherever it is useful. It can be assumed that the GDoS core instance is hosted by the actor that aims to offer the added value service GDoS to their users.

The GDoS core instance requests, by means of an interface 2 (2.1), the application service related network performance requirements from the GDoS instance of the InfSP. The GDoS-InfSP obtains the application service requirement information from the service profile database of the InfSP and sends this information back to the GDoS core instance via interface 2 (2.2). Moreover, the GDoS core instance requests by means of the interface 3 (3.1) and interface 4 (4.1) InfSP and user connectivity related network capability information from the GDoS instance located in the network of the ENSP1 and ENSP2. The GDoS instance of ENSP1 and ENSP2 obtains the network performance capability information from the CPDB of ENSP1 and ENSP2 and sends this information back to the GDoS core instance via interface 3 (3.2) and interface 4 (4.2).

After the GDoS core instance has received all required information from the InfSP and of the network segments ENSP1 and ENSP2 the evaluation process is started. The GDoS core instance compares the available network performance capabilities in the network of ENSP1 and ENSP2 with the application service requirements on network performance. The result of the evaluation process is sent back from the GDoS core instance to the GDoS instance of the InfSP via interface 1 (1.2). The information service provider is now aware whether the application service that has been requested by the user is deliverable in the user requested quality.

The InfSP is now able to use the result of the evaluation process as service quality indication information to inform the user whether the requested application service is deliverable with the requested quality or not. The service quality indication feedback is provided via interface 0 (0.2) to the user device by means of, e.g. a popup web page. Another possibility to deliver the feedback to the user is to integrate the feedback information in the application software that receives the application service.

The presented high-level view on the graceful denial of service use case scenario in Figure 4.14 is described by means of the sequence diagram in Figure 4.15 in more detail. The sequence diagram depicts the different actor roles involved in the GDoS scenario which are needed to perform the engaged signal. Moreover, the service enhancement functions of the GDoS solutions are shown in Figure 4.15. In the presented sequence diagram the GDoS core instance is located in the actor NSP1 network.

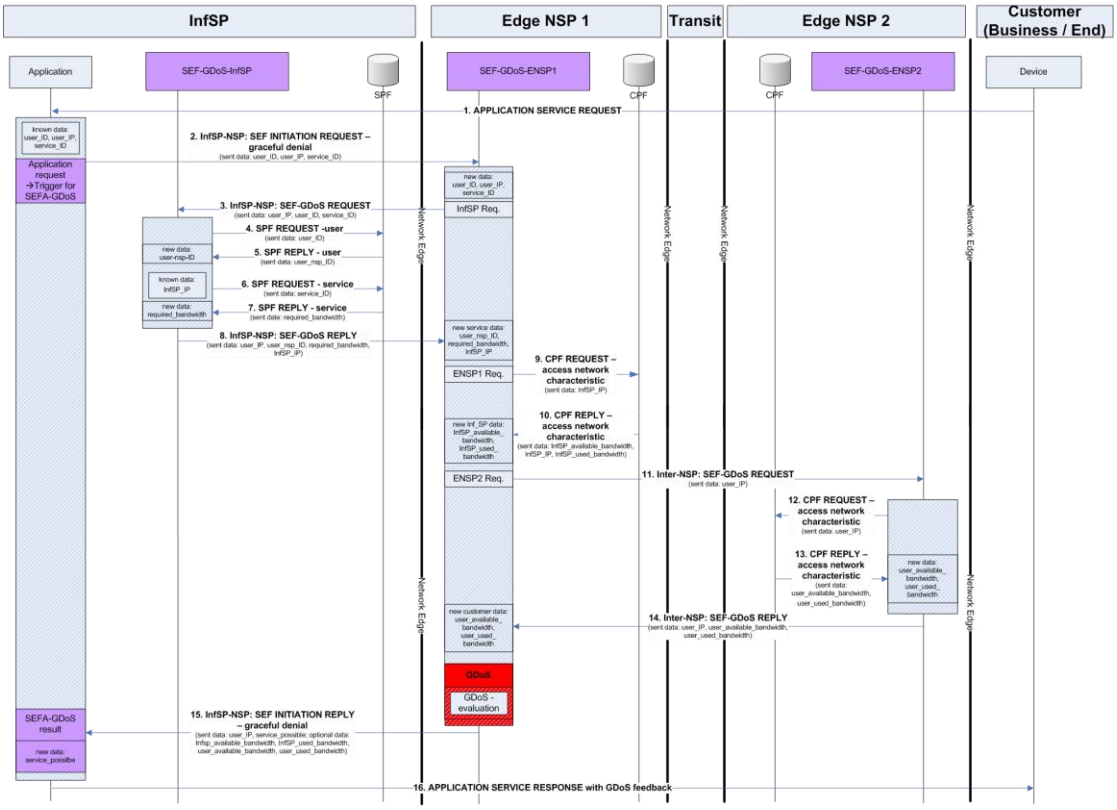


Figure 4.15: Sequence diagram of graceful denial of service solution.

In the following the steps of in the GDoS sequence diagram are described. It is assumed that an IP-based connectivity among the device and the InfSP video portal has been established. In step 1 the customer device sends an application service request to the application, e.g. video service. The customer's request is received by the application controller (AC) which triggers the added value service GDoS. The parameters received by the AC are user_IP, service_ID, and user_ID. In step 2 the AC sends SEF INITIATION REQUEST – graceful denial to the SEF-GDoS-ENSP1 to start the added value service GDoS. The parameters received by the SEF-GDoS-ENSP1 are user_ID, user_IP, service_ID. In step 3 the SEF-GDoS-ENSP1 sends the SEF-GDoS Request to the SEF-GDoS-InfSP to request application service requirements on network performance. The parameters obtained by the SEF-GDoS-InfSP are user_ID, user_IP, service_ID. In step 4 SEF-GDoS-InfSP sends SPF REQUEST – user to the service profile function (SPF) to request the point of attachment information of the user. The SPF receives the parameter user_ID and determines by means of the user_ID the user_nsp_ID which is the user connecting NSP. In step 5 SPF sends SPF REPLY – user to the SEF-GDoS-InfSP. The parameter returned to the SEF-GDoS-InfSP is the user_nsp_ID. In step 6 SEF-

GDoS-InfSP sends SPF REQUEST – service to the SPF to request the application service requirements on network performance. The requirement on network performance is indicated by the required_bandwidth which is needed to deliver the application service from the InfSP to the user. The SPF receives the parameter service_ID and determines by means of the user_ID the required_bandwidth of the application service. In step 7 SPF sends SPF REPLY – service to the SEF-GDoS-InfSP. The parameter received by the SEF-GDoS-InfSP is the required_bandwidth. In step 8 the SEF-GDoS-InfSP sends a SEF-GDoS Reply to the SEF-GDoS-ENSP1. The parameter received by the SEF-GDoS-ENSP1 is the application service requirements on network performance, such as the required_bandwidth. Further parameters received by the SEF-GDoS-ENSP1 are user_IP, user_nsp_ID and InfSP_IP. In step 9 SEF-GDoS-ENSP1 sends a CPF REQUEST – access network characteristic to the connectivity profile function (CPF) located in the NSP1 network to request the current performance of the connectivity among InfSP and ENSP1. The CPF receives the parameter InfSP_ID and determines by means of the InfSP_ID the InfSP_available_bandwidth and InfSP_used_bandwidth. In step 10 CPF sends CPF REPLY – access network characteristic to the SEF-GDoS-ENSP1. The parameters received by the SEF-GDoS-ENSP1 are InfSP_IP, InfSP_available_bandwidth and InfSP_used_bandwidth. In step 11 SEF-GDoS-ENSP1 sends a SEF-GDoS REQUEST to SEF-GDoS-ENSP2 to request the current performance of the connectivity among the user and ENSP2. The received parameter by the SEF-GDoS-ENSP2 is user_IP. In step 12 SEF-GDoS-ENSP2 sends a CPF REQUEST – access network characteristic to the CPF located in the NSP2 network to request the connectivity capabilities of the user. The CPF receives the parameter user_IP and determines by means of the user_IP the user related parameters user_available_bandwidth and user_used_bandwidth. In step 13 CPF sends a CPF REPLY – access network characteristic to the SEF-GDoS-ENSP2. The received parameters by the SEF-GDoS-ENSP2 are user_available_bandwidth and user_used_bandwidth. In step 14 SEF-GDoS-ENSP2 sends a SEF-GDoS REPLY to SEF-GDoS-ENSP1 which provides the performance information of the connectivity among user and ENSP2. The received parameter by the SEF-GDoS-ENSP1 is user_IP, user_available_bandwidth and user_used_bandwidth. After receiving the parameters from SEF-GDoS-ENSP2, all parameters required to perform the added

value service GDoS are available. SEF-GDoS-ENSP1 performs the added value service GDoS in relation to the user which has requested the video service. In step 15 SEF-GDoS-ENSP1 sends a SEF INITIATION REPLY – graceful denial containing the GDoS evaluation result to the application controller. The parameters returned to the AC are user_IP and service_possible. The parameter service_possible indicates whether or not the requested application service is deliverable via the NSP1 and NSP2 network in requested quality. Optional parameters which can be received by the AC are InfSP_available_bandwidth, InfSP_used_bandwidth, user_available_bandwidth and user_used_bandwidth. All parameters received by the AC are used to create the GDoS feedback to the user. In step 16 AC sends an APPLICATION SERVICE RESPONSE with GDoS feedback to the device.

Through the GDoS feedback the user gets informed about the expectable service quality before the application service starts. If network capabilities are sufficient to deliver the application service in the requested quality the application service will start without the GDoS feedback. However, in the case of non-sufficient network capabilities the GDoS feedback is shown to the user, as presented in Figure 4.14. The GDoS feedback provides information about the reason why the requested application service might be delivered in reduced quality. A first reason can be that the user has other services already running which results in non-sufficient available network capabilities in the connectivity among home network and edge network service provider. A second reason might be that the user has generally less network capabilities available and a third reason can be that the connectivity of the information service provider to the edge network service provider has less network capabilities than required. Beside the GDoS feedback, additional options are offered to user. This means the user is able to decide, whether or not to start the service or wait until more network resources are available. As a result, the user will not be surprised about reduced application service quality delivered in the case of non-sufficient available network capabilities. Furthermore, optional network features, e.g. a bandwidth on demand service can be offered to the user which enables them to request additional bandwidth to provide sufficient network capabilities to deliver the requested application service in user satisfying quality.

4.4 Summary

The intention of the presented solutions was to develop network capabilities which enable and support a certain use case. These use cases are UC-service quality, UC-usability and UC-quality awareness, as shown in Table 4.1.

The use case UC-service quality focuses on an enhanced authentication and authorisation method in the WLAN handover processes to achieve better VoIP quality when users are on the move in WLANs. For that purpose the sequential authentication solution in Section 4.1 has been proposed to realise network capabilities which provide the required network performance that is needed. The intention of the sequential authentication solution is to overcome the drawback of long authentication times arising from the communication between the authenticator and remote AAA server, the behaviour of a secure WPA2 PSK authentication followed by a WPA2 EAP-TLS authentication is combined. This combines the benefits of both methods while avoiding the time of blocked network access that occurs in the traditional IEEE 802.1X authentication phase. Firstly, the benefit of WPA2 PSK method is used to provide secure wireless link encryption but with a focus on short authentication time. Secondly, the WPA2 EAP-TLS authentication currently provides the most secure authentication method to carry out mutual authentication between the supplicant and AAA server. Due to the reduced authentication time a handover process can be enhanced. This means the QoS requirement, such as the packet-loss of the service, e.g. VoIP, can be fulfilled because of the reduced handover time. As a result real-time service provisioning can be enabled in user expected quality even in UE mobility scenarios.

The use case UC-usability focuses on the provisioning of user credentials on demand and an auto-login method for WLAN-based hotspots to achieve improved hotspot comfort with regard to flexible use and user-friendly login. For that purpose the barcode initiated hotspot auto-login solution in Section 4.2 has been proposed to realise a network capability which provides the network access that is needed for the use case WLAN Hotspot registration process, obtaining of user credential and auto-login process. The intention of the barcode initiated hotspot auto-login solution is to enable hotspot use on demand, payment of hotspot use by means of SMS fees and to perform automated hotspot logon. The BIHA solution avoids that the user has to

enter user name and password on the hotspot login page. By means of an automatically generated link or barcode on the login page, the hotspot auto-login process is initiated. After opening the SMS tool on the smart phone, triggered by the link or barcode, and the creation of the hotspot user account, the user gets logged in automatically.

The UC-quality awareness focuses on a distributed data collection system and a user information system to inform the user about the application service quality to be expected before the application service is started. For that purpose the graceful denial of service quality solution in Section 4.3 has been proposed to realise a network capability which provides the required network features that are needed for the use case application service delivery and the quality received by the user. The intention of the graceful denial of service solution is to realise service quality indication feedback for the user which behaves similarly to a busy signal in traditional telephony. The GDoS solution gathers the application requirements of network performance from an information service provider and available bandwidth network information from a network service provider who connects a user to the Internet to derive the GDoS feedback.

5 Implementation

This chapter presents the proof of concept implementations of the proposed solutions in Chapter 4. Section 5.1 presents the implementation of the sequential authentication solution of Section 4.1. Section 5.2 describes the barcode initiated hotspot auto-login solution proposed in Section 4.2 while Section 5.3 presents the graceful denial of service solution developed in Section 4.3.

5.1 Sequential Authentication Solution

Subsection 3.4.5 shows that today's most secure WLAN encryption and authentication as well as authorisation mechanism, such as WPA2, is not able to perform a handover process with a delay of less than several hundreds of milliseconds. These hundreds of milliseconds in the handover process lead to an interruption of data connectivity that is insufficient for real-time services, such as VoIP. The description of the handover keying (HOKEY) re-authentication problem in [177] underpin the existing handover problem in terms of required authentication and authorisation time when using WPA2 with IEEE 802.1X and EAP-TLS. To eliminate the problems in handover processes that arise due to the long interruption of data connectivity the novel sequential authentication solution is introduced Subsection 4.1.1. In this section the implementation of the sequential authentication solution is described. The implementation will enable a fast as possible handover from one access point to another in terms of authentication and authorisation process, without reducing the level of network security in terms of encryption.

With regard to the time of interruption when using WPA2 with IEEE 802.1X and EAP-TLS, as presented in Subsection 3.4.6 and 3.4.8, a reduction of interruption time can be reached by a change of the authentication server location. The closer the authentication server is located to the authenticator the shorter the consumed authentication and authorisation time and thus, the data communication interruption time, as shown in Figure 3.15. Another approach to reduce the time of interruption is to extend the existing IEEE 802.1X protocol as described in Subsection 3.4.5. The implementation of the novel sequential authentication concept presented in

Subsection 3.4.5 is described in the following. The sequential authentication solution has been realised by means of extending the software hostapd in version 0.6.4 [179] and wpa_supplicant in version 0.6.6 [178].

A solution that reduces the data communication interruption while a handover process is needed. With focus on the network access control part of the handover process, a solution that avoids the impact of runtime in the authentication and authorisation process has to be achieved. As described in Subsection 3.4.8 IEEE 802.1X uses a controlled port and an uncontrolled port for data transmission. Via the controlled port user data are transmitted only, while the uncontrolled port is responsible to transmit authentication and authorisation information. However, transmission of user data is granted after successful authentication and authorisation process via the controlled port only. A solution to overcome the drawback of interruption time is the ability to transmit user data in parallel to the authentication and authorisation phase.

In contrast to the controlled port the transmission of authentication and authorisation data via the uncontrolled port is possible even if the controlled port is closed for user data transmission. To eliminate the interruption of data connection, it would be possible to use the uncontrolled port for transmission of all data. As a result, for example, data of a VoIP communication could be forwarded after an established IP connectivity in a handover process, even if the authentication and authorisation process is still in process. This means that user data would be immediately forwarded from the new access point in parallel to the data communication of user authentication and authorisation. However, this solution has several serious weaknesses. The wireless connection is unencrypted from the time of the wireless client association with the access point until the authentication and authorisation process is completed. This means, transmitted user data via the uncontrolled port is interceptable by a malicious user surrounding the access point. This behaviour of unprotected data access must be avoided. Another drawback of this approach is that no network access control can be performed. Due to this, each malicious user can get network access at this point in time. Even if the network access is limited to the moment of authentication and authorisation by the AAA server, a short period of time remains in which a malicious user has access to the network until the authenticator disconnects the client. This behaviour must be

avoided as well. In addition, a malicious user could re-connect to the network immediately and would ask again for network access, even if the network access would be available for a short time only.

To prevent this short-term non-encrypted and uncontrolled network access while keeping the ability of data communication in parallel to the authentication and authorisation process an additional port has to be implemented. This additional temporary port will provide network access control and encryption of the wireless link as well. The illustration of this new parallel port in the authenticator is represented in Figure 5.1.

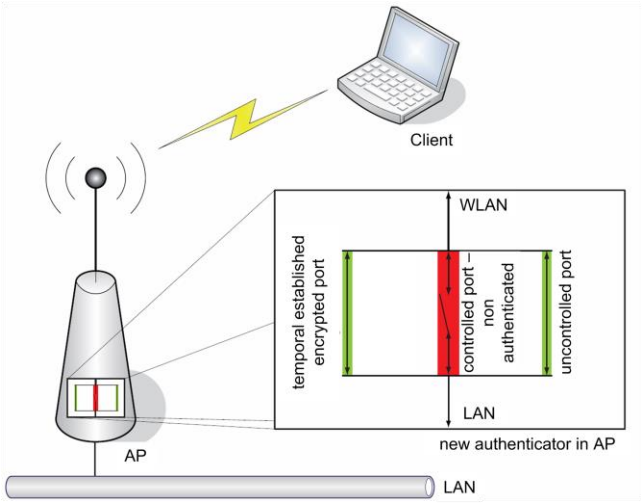


Figure 5.1: Temporal activated port in authenticator of sequential authentication solution.

Should a user connect to the access point, network access authentication and authorisation for the temporary port is performed. In the case of granted network access the user data will be transmitted. The transmission of user data is encrypted. For this approach an additional key is necessary that has to be configured on the client and access point side. This key is used to perform network access control and to derive data transmission keys. The authenticator in the access point grants network access only if the client uses this key for wireless link connectivity establishment. This is the first step of network access control in the sequential authentication solution corresponding to the row higher layer authentication / authorisation phase 1 in Figure 4.4. The higher layer authentication / authorisation phase 1 is the precondition of performing the sequential authentication solution successfully.

In parallel to the granted data communication due to the successful performance of the higher layer authentication / authorisation in phase 1 the authentication and

authorisation of the user by means of IEEE 802.1X with EAP-TLS method has to be performed. The execution of IEEE 802.1X with EAP-TLS method corresponds to the row higher layer authentication / authorisation phase 2 in Figure 4.4, the second step of sequential authentication solution.

Parallel to IEEE 802.1X with EAP-TLS process initiation the authentication window is activated, as shown in the row authentication window in Figure 4.4. The IEEE 802.1X with EAP-TLS process has to be performed within the authentication window. Otherwise, the wireless client will be disconnected from the access point. The disconnection of the client is performed with the assumption that the client is not able to authenticate themselves against the authentication server. Thus, the probability is high that the client is a malicious user and has to be disconnected from the access network.

After the successful EAP-TLS process, as described in Subsection 3.4.7, the 4-way-handshake is performed by means of the derived PMK. The result of this 4-way-handshake is a new key that is used for further wireless data encryption. The successful execution of EAP-TLS and 4-way-handshake process results in the closing of the controlled port. Thus, data transmission of user data is granted. This means that the previously initiated temporal port is no longer needed and will be deactivated, as shown in Figure 5.2.

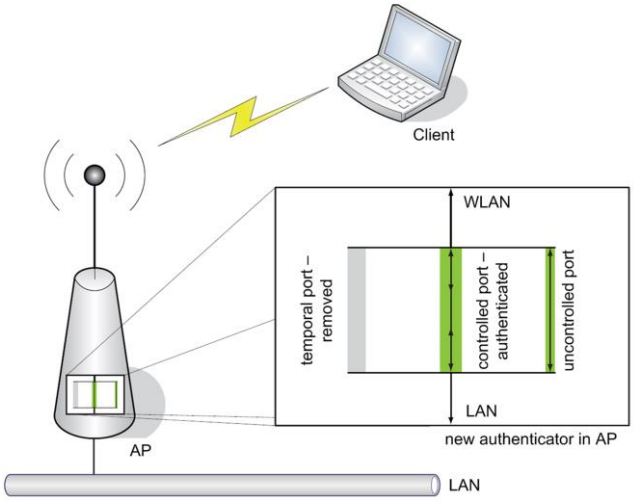


Figure 5.2: Deactivated temporal port in authenticator after successful authentication and authorisation.

In contrast to the approach that uses the uncontrolled port for the short-term communication, in this approach a wireless encryption is active and performed. Moreover, network access is granted only if the key used on the access point is

known and configured on the client side. By means of the used pre-shared key a kind of network access control is performed. However, due to the fact that a previously distributed pre-shared key cannot be excluded, the temporal activated port has to be constructed with additional restrictions. These additional restrictions contribute to the avoidance of permanent network access by malicious users. With the aim to restrict unauthorised permanent network access by malicious users a timeout is introduced in the sequential authentication solution. With regard to Figure 4.4 the timeout corresponds to the authentication window. The authentication window is activated after successfully performing the first step of the sequential authentication solution or as shown in Figure 4.4 after successfully performing of the row higher layer authentication / authorisation in phase 1. Within the authentication window the wireless client has to authenticate themselves against the authentication server. Thus, the IEEE 802.1X with EAP-TLS process has to be carried out within the authentication window successfully. Otherwise, the wireless client will be disconnected from the access point. In the case a malicious user is aware of the pre-shared key that is used in the first step of the sequential authentication where the timeout introduced will restrict network access to a predefined time. Due to the fact that the malicious client is not able to process the EAP-TLS successfully network access is only granted within the authentication window. Past the authentication window the MAC address of the client is blocked for a predefined time within the access point, as shown in Figure 5.3. The blocking of clients MAC address avoids re-connection of the client and thus, network access as well.

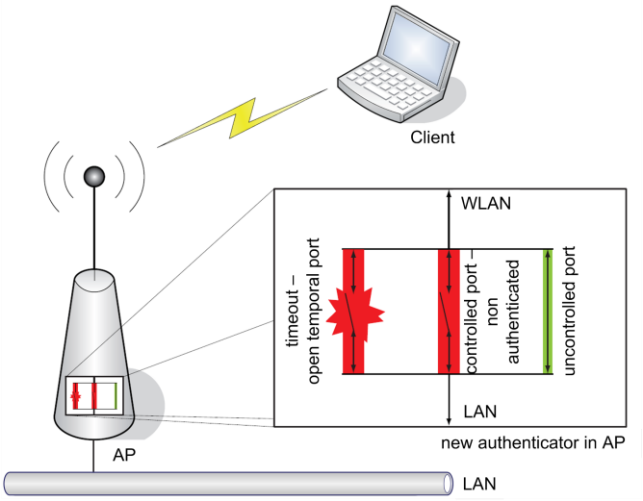


Figure 5.3: Opened temporal port after expired timeout.

After the elapsed blocking time the client is able to request network connectivity again. The implementation of the sequential authentication protocol with the aim to overcome the data interruption in an EAP-TLS process is realised based on existing methods and implementations. The benefit of setting up the sequential authentication solution on existing methods is that these methods, such as EAP-PSK and EAP-TLS are well known and sufficiently validated in the WLAN community and are seen as the most secure WLAN security mechanisms from today's point of view, as stated in [76]. In addition, the existing EAP methods for authentication can be applied without the need of changing the protocol.

The investigation results of the handover interruption times in Subsection 3.3.2 and 3.4.6 shows that a VoIP communication can be provided in good quality, even in the case of an handover when using the WPA-PSK mechanism. Based on this the WPA-PSK mechanism will be used to realise the implementation of the temporal port within the authenticator. The WPA-PSK mechanism consists of the necessary capabilities to setup a temporary port. The WPA-PSK mechanism performs:

- Network access control
- Encryption of the wireless link
- Quick setup of IP connectivity after performed handover

Furthermore, the WPA-PSK mechanism is described in the standard IEEE 802.11i and is classified as safe [ibid]. Before the temporal port is activated on the access point side a 4-way-handshake among client and access point has to be performed based on the PSK. In the case of a successful authentication and authorisation a configurable time is implemented that opens the temporal port. Within this period the client has to authenticate themselves against the authentication server by means of the EAP-TLS method. In the case the client is not able to authenticate themselves against the authentication server a method in the sequential authentication solution is triggered to deny WLAN connectivity for a configurable time. The flow chart in Figure 5.4 illustrates the procedure of the sequential authentication solution.

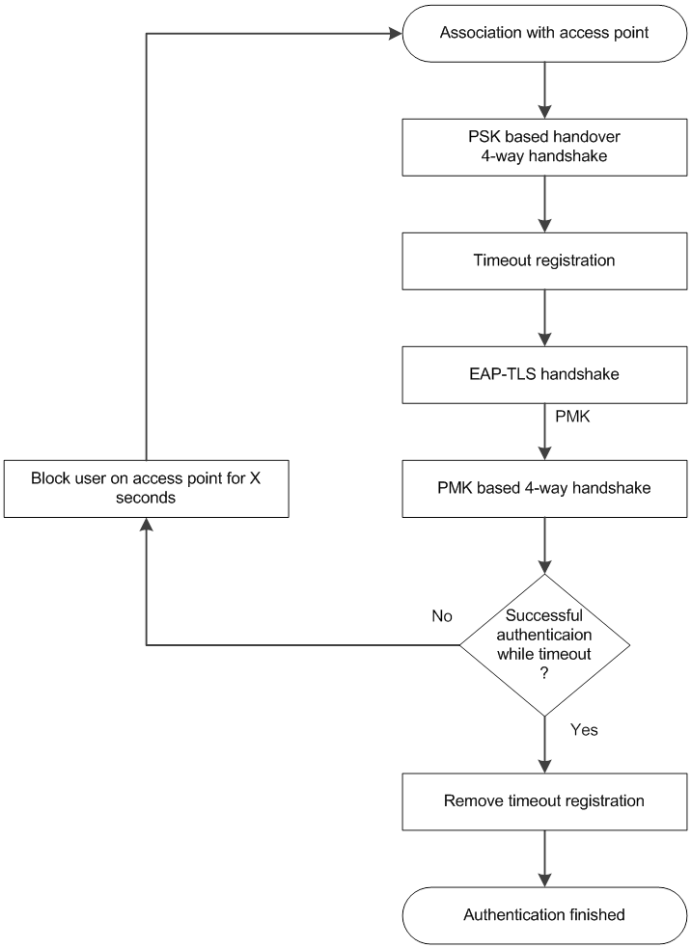


Figure 5.4: Flow diagram of sequential authentication solution.

The implementation of the 4-way handshake is based on WPA-PSK and is performed before the EAP-TLS authentication starts. The combination of WPA-PSK and WPA using EAP-TLS leads to the new protocol flow illustrated in Figure 5.5.

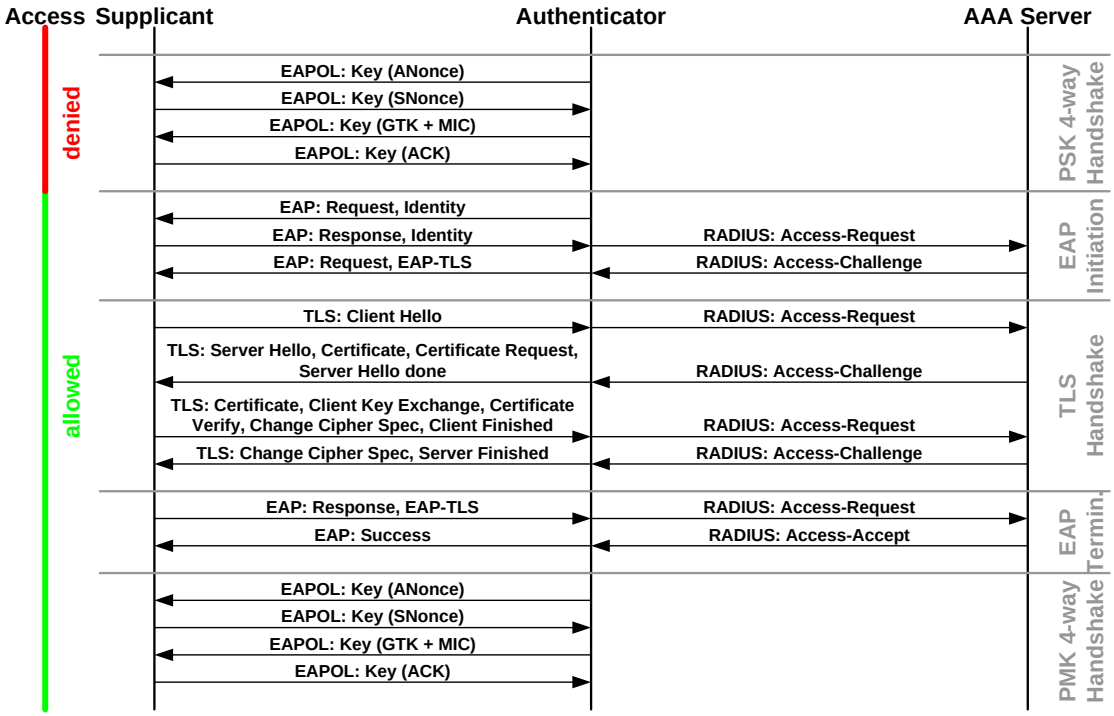


Figure 5.5: Flow chart of sequential authentication concept using WPA-PSK and 802.1X with EAP-TLS and RADIUS server.

Figure 5.5 presents the behaviour to provide network access authentication and authorisation. The two-coloured line named access on the left side shows that after a successfully performed WPA-PSK 4-way handshake network access is granted and then user data communication can take place. After the WPA-PSK authentication, the 802.1X EAP-TLS method is performed using a RADIUS server for user authentication. After successful user authentication and authorisation the 4-way handshake is performed. The PMK used for the 4-way handshake is built on the first 256 bits of the AAA-key.

The sequential authentication solution is based on two standardised and well known mechanisms of the IEEE 802.11i standard, such as IEEE 802.11i PSK and EAP-TLS. The utilisation and requirements of both methods are described in detail in IEEE 802.11i. The work flows of the methods are illustrated by means of state machine diagrams. The state machine shows the steps involved in performing an authentication and wireless encryption key derivation process. The most important part of the novel sequential authentication solution implementation is the authenticator state machine. With the aim to combine the IEEE 802.11i PSK and EAP-TLS method it is very useful to look in detail at the state machine diagrams of

both methods. Figure 5.6 shows the state machine of the IEEE 802.11i PSK method while Figure 5.7 shows the state machine of IEEE 802.11i EAP-TLS method.

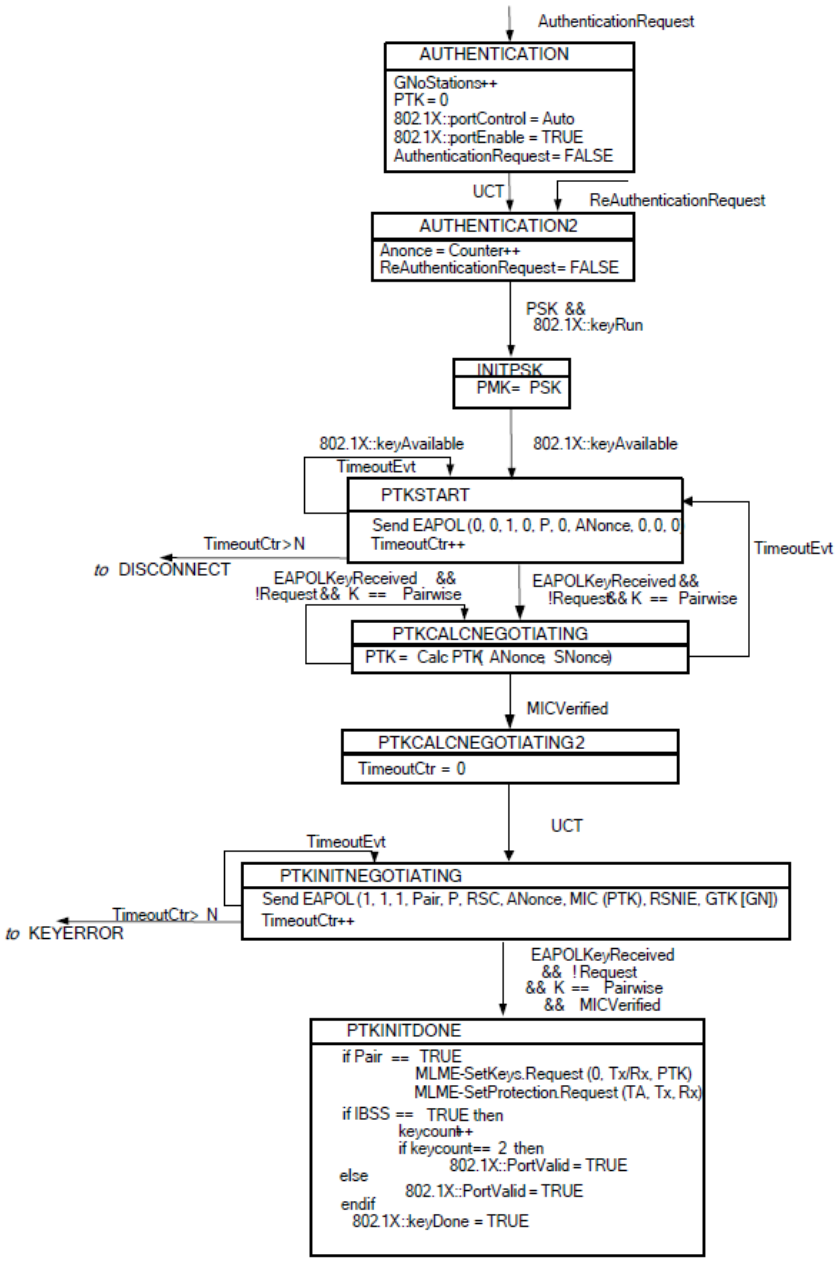


Figure 5.6: State machine of IEEE 802.11i PSK method.

The comparison of the IEEE 802.11i PSK and IEEE 802.11 EAP-TLS state machines shows that both state machines are nearly identical. The most important difference of both state machines is the preparation of the PMK as shown in step INITPSK in Figure 5.6 and INITPMK in Figure 5.7. In the IEEE 802.11i PSK method the PMK is set to the value of the PSK, as shown in Figure 5.6 step INITPSK. This is very important. Based on this authenticator state machine

characteristic it is possible to design an authenticator state machine independent of the applied PSK and PMK methods.

In the case of the application of the EAP-TLS method in parallel to the 802.1X state machine, as shown in Figure 5.7, an EAP-TLS state machine is started to perform the EAP related communication. This EAP state machine delivers as the result the AAA-key. The first 256 bits are used to derive the PMK. By means of the PMK the remaining steps of the 802.1X state machine are processed. As result the wireless link is encrypted.

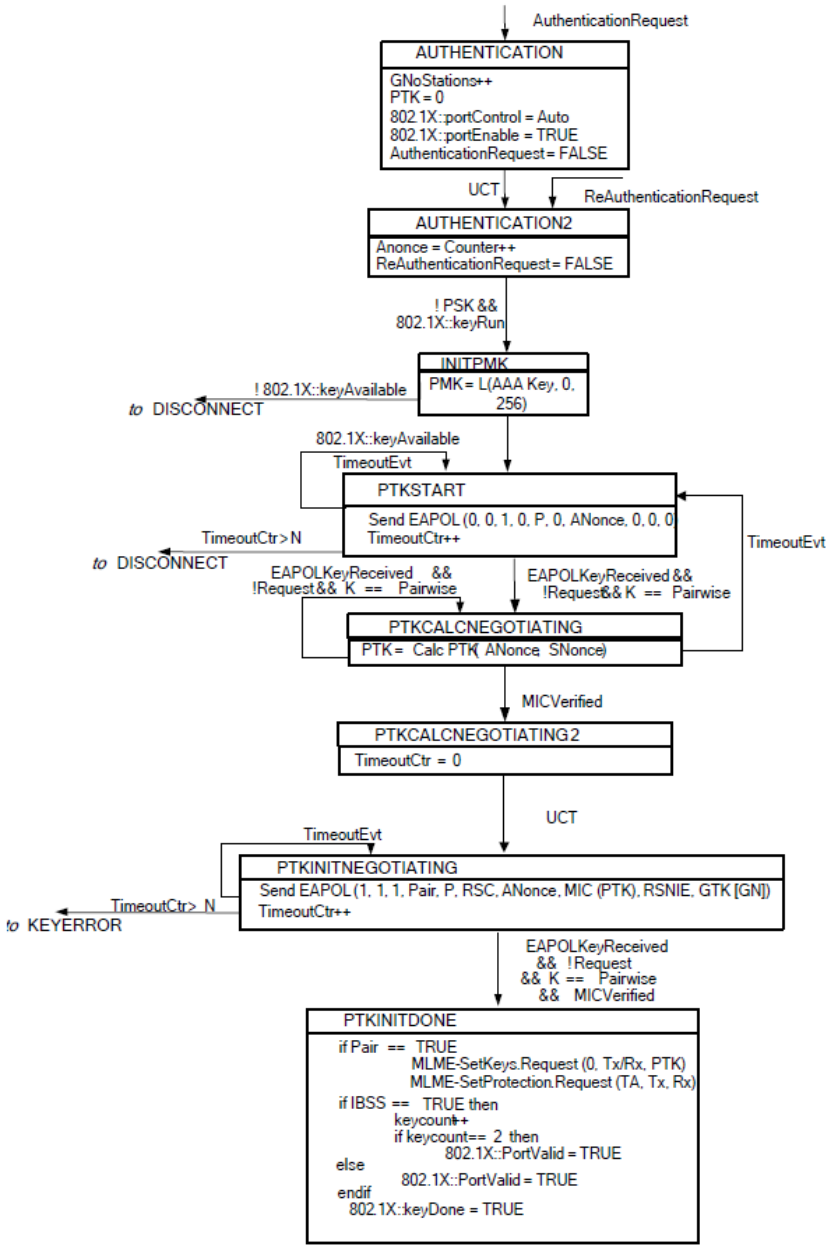


Figure 5.7: State machine of IEEE 802.11i PMK method.

The abstracted flow diagram of the sequential authentication solution in Figure 5.4 is realised by the previously presented IEEE 802.11i PSK and IEEE 802.11i PMK authenticator state machines. Combining both state machines result in the new authenticator state machine as shown in Figure 5.8. At first the IEEE 802.11i PSK state machine and then the IEEE 802.11i PMK state machine is applied. Beside the functionalities of the IEEE 802.11i PSK and IEEE 802.11i PMK authenticator state machines the new authenticator state machine uses additional states to enable the temporal limitation of the temporal port. Figure 5.6, Figure 5.7 and Figure 5.8 is based on Figure 43 on page 103 of IEEE standard 802.11i-2004 [74]. The protocol flow chart of the new authenticator is shown in Figure 5.5.

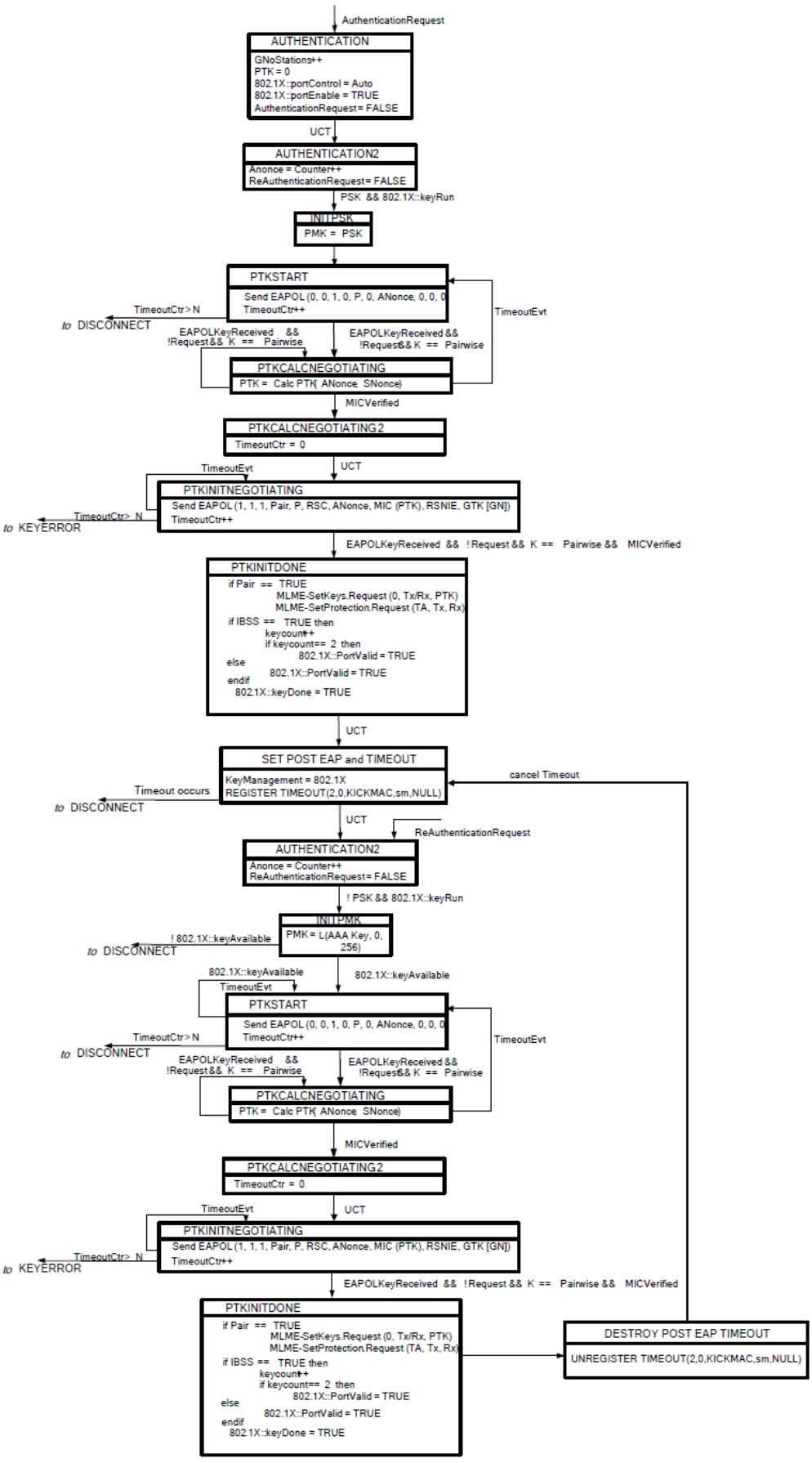


Figure 5.8: New state machine of sequential authentication solution.

The realisation of the new sequential authentication solution based on the traditional 802.1X state machines enables the application of any EAP method in the standard. This means network administrators are able to provide RADIUS server based authentication based on the most suitable EAP method for a particular network architecture. As a result, the sequential authentication solution does not only reduce the handover time of the IEEE 802.1X EAP-TLS method, but rather supports all EAP methods specified in the IEEE 802.1X standard. Figure 5.9 shows the flow chart of the sequential authentication solution using PSK and PMK 4 way handshake without a specified EAP method.

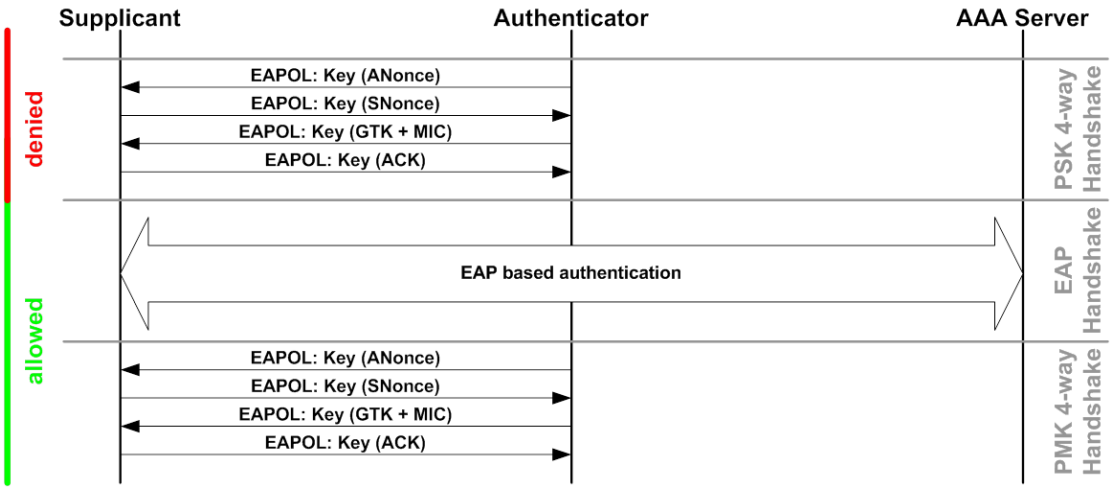


Figure 5.9: Flow chart of sequential authentication solution using PSK and PMK 4-way handshake without specified EAP method.

5.2 Barcode Initiated Hotspot Auto-login

The barcode initiated hotspot auto-login solution has been introduced in subsection 4.2.3. In the following the components of the implemented BIHA solution are described. Figure 5.10 presents the component diagram of the BIHA solution.

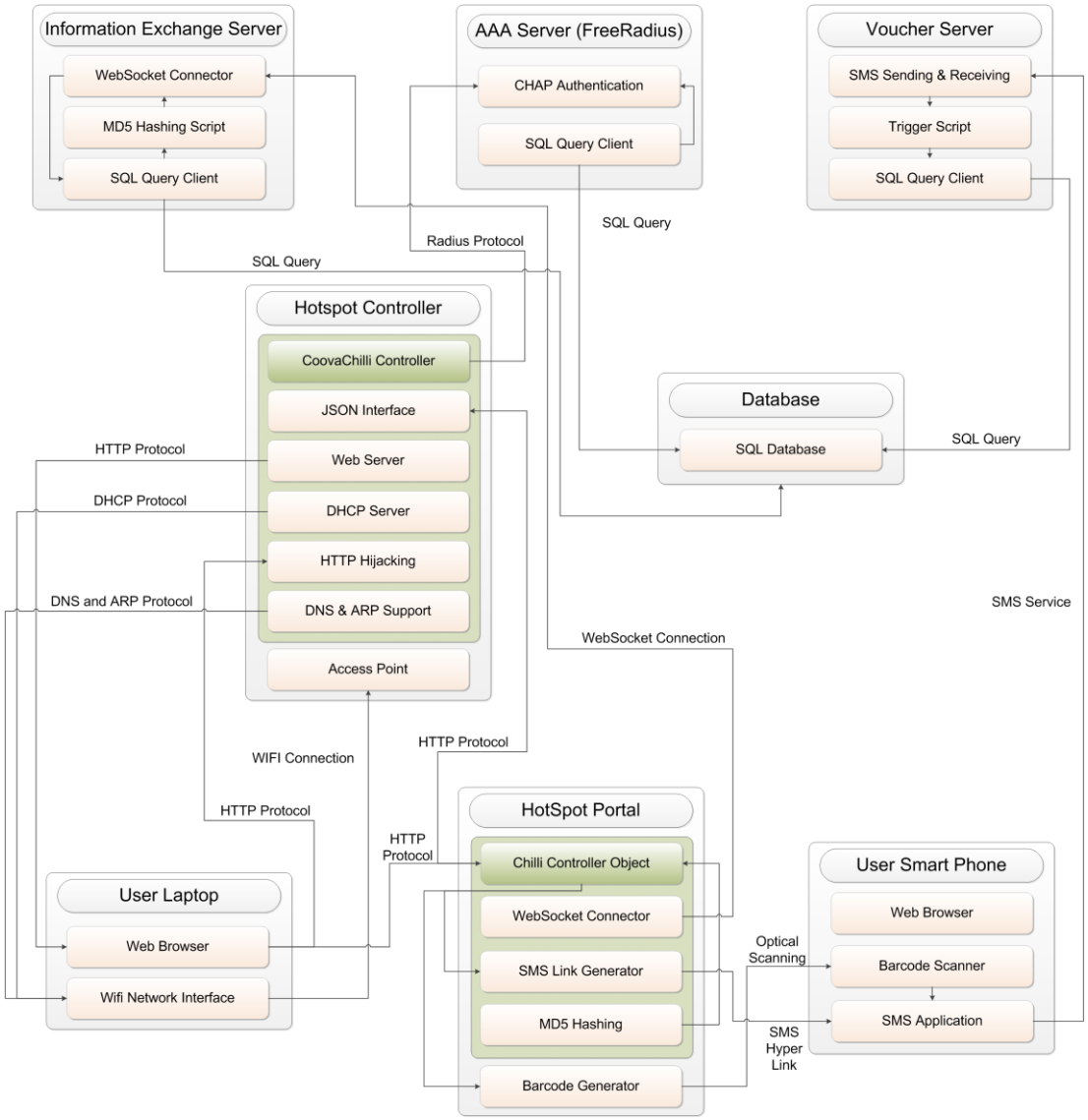


Figure 5.10: Component diagram of barcode initiated hotspot auto-login solution.

The components of the BIHA solution are the information exchange server, the AAA server, the voucher server, the hotspot controller, the hotspot portal, the user laptop and the user smart phone. In the following these components are described in more detail.

Information Exchange Server:

The information exchange server is responsible for the setup of the information channel and the CHAP password generation, as presented in setup 13 till 18 in Figure 4.7. The following modules are part of the information exchange server.

- WebSocket connector: This module handles the connection establishment and information channel message transfers between the connected clients and the server. It delivers the messages from the user's browser to the SQL query and

hashing script modules and vice versa. The communication protocol and handshakes are based on the WebSocket protocol [173].

- MD5 hashing script: This module performs MD5 [180] hashing functions and CHAP [174] password generation.
- SQL query client: This module handles the communication between the information exchange server and the MySQL database.

AAA Server:

The AAA server performs user authentication and authorisation in the hotspot logon process. The following modules are part of the AAA server:

- FreeRADIUS [181] server: The FreeRADIUS server performs user authentication and authorisation. The FreeRADIUS server is selected due to its popularity as an AAA server.
- CHAP [174] authentication: This module handles the CHAP authentication protocol by validating the authentication requests received from the clients through the hotspot controller.
- SQL query client: This module performs the communication between the FreeRADIUS server and the MySQL database.

Voucher Server:

The voucher server receives and sends SMS and is furthermore responsible for the user account creation and user account update. The following modules are part of the voucher server:

- SMS sending and receiving: This module is responsible for continually querying the GSM modem for newly received SMS messages as well as sending the user credentials via SMS back to the users. For that purpose the SMS server tools 3 [182] are applied.
- Trigger script: This module is an add-on to the existing SMS server tools 3 package and was developed specifically for the BIHA solution. The trigger script is called whenever a new SMS is received by the voucher server and it handles user account generation and updates the user account information in the MySQL database.
- SQL query client: This module handles the communication between the voucher server and the MySQL database.

Hotspot controller:

The hotspot controller is literally the heart of the BIHA system which consists of two main modules and several sub-modules as follows:

- CoovaChilli [85]: CoovaChilli is an open-source access controller, able to control network access of e.g. WLANs. Version 1.3.0 is applied in the current implementation and the following modules are used in the BIHA solution in addition:
  - JSON [183] interface: The JSON interface is used to transfer data from CoovaChilli to the browser. It has less overhead than XML which is typically used in AJAX applications. The JSON interface serves a login page to the end-user which contains a username and password field. This authentication data is then forwarded by the CoovaChilli to the FreeRADIUS server using e.g. either password authentication protocol (PAP), CHAP, or MSCHAPv2. By means of the JSON interface login and logoff to or from the captive portal or hotspot portal can be triggered. Moreover, status information about the connection among user devices and the CoovaChilli can be requested.
  - Web Server: CoovaChilli has its own internal web server to host specific scripts and the hotspot portal web pages needed for authentication. It is limited to a few file types such as JavaScript, images and html pages and utilizes the program “haserl” to realize the server side CGI scripting.
  - DHCP server: The internal DHCP server of CoovaChilli provides a DHCP service to the user device connecting interface (e.g. the Wi-Fi interface) to assign suitable IP addresses for the connected clients.
  - HTTP hijacking: This module will continually monitor each packet sent from the user device before they are authenticated to push the captive portal to the client’s web browser. As soon as an http request from the client side is detected the client is automatically forwarded to the hotspot portal page.
  - DNS and ARP: CoovaChilli support both ARP and DNS protocol on the LAN interface. This enables the connected user devices to have communication with the network and as well the public Internet.
- Access point: This module is employed as the WLAN interface for CoovaChilli and works as a WLAN access point in the hotspot access network. In the current

implementation it is realized by using a PCMCIA network card and the software hostapd to configure the PCMCIA network card in access point mode.

MySQL database:

MySQL [184] is an open-source relational database management system. In the current BIHA implementation the version 5.1.73-1 is used as the backbone database for the authentication system. The database includes several tables to be used for the overall authentication, authorization and accounting. The most important table concerning the authentication process is the table radcheck which contains the columns presented in Table 5.1 for each created user account.

Id	NasID	HMAC	username	attribute	op	Value

Table 5.1: Table radcheck of MySQL database.

Parameters attribute and op have the default values of Password. The parameter id is the sequential number for each created user account which will be incremented automatically by the database for each new created user account.

Hotspot portal:

The hotspot portal is the most important element of the BIHA solution which the user needs to interact with. All the user related functionalities are realized within this portal. It is loaded automatically in the user's web browser as soon as the web browser on the user device tries to open a website. The portal consists of two main modules and several sub-modules.

- ChilliController object: This module is the main part of the hotspot portal and contains most required sub-modules that are needed for the hotspot portal to work. It is a combination of several JavaScript libraries and functions hosted on the hotspot controller internal web server. The ChilliController object is loaded automatically into the user's web browser while the visual frontend of the portal is loading. The object comprises the following sub-modules:
  - WebSocket connector: This module is responsible for establishing a WebSocket connection with the information exchange server to initiate the auto-logon process. The trigger functions are included within the hosted JavaScript libraries while the main part of the connection establishment and message exchanges are handled by the web browser itself. The JavaScript trigger functions communicate with the internal web browser modules via the available platform APIs in the browser.

  - SMS link generator: This module consists of several JavaScript functions which dynamically gather the required verification information, such as Nas ID and hashed device MAC address from the user and browser environment. Then this information is integrated into a specific hyperlink and displayed to the user in the hotspot portal. The hyperlink is recognized by mobile phones and tablet PCs automatically and the SMS application is opened upon being clicked. The hyperlink will automatically fill in all required information such as the NAS ID and hashed device MAC address in the user's SMS application.
  - MD5 hashing: This module handles the required MD5 [180] hashing functions, such as CHAP [174] password generation and user device MAC address hashing.
- Barcode generator: This is an external JavaScript library [185] which is responsible for generating device specific QR Codes. The JSQR library [ibid] is separate from the CoovaChilli libraries but is loaded into user's browser at the same time as when the other ChilliController JavaScript libraries are loaded by the hotspot portal. The barcode generator module works similar to the SMS link generator module. It gathers the required verification information, such as Nas ID and hashed device MAC address, from the environment and then generates the QR code from this information. The QR code is then displayed to the user in the hotspot portal.

User device:

The user device has to have the following capabilities to be used in the BIHA solution. The user device can be, e.g. a laptop, a tablet PC or a smart phone.

- Web browser: The user needs to have a web browser on his user device to initiate the logon process. The browser should support JavaScript and the WebSocket protocol. The web browser is used to view the hotspot portal and to communicate with the hotspot controller and the rest of the BIHA system.
- Wi-Fi network interface: The user device must contain a Wi-Fi network card to connect to the wireless hotspot which is controlled by CoovaChilli.

User smart phone:

The users smart phone has to have the following capabilities to be used in the BIHA solution.

- Web browser: The user needs to have a web browser on his smart phone to initiate the logon process in the auto-login approach single device. The browser should support JavaScript and the WebSocket protocol. The web browser is used to view the hotspot portal and to communicate with the hotspot controller and the rest of the BIHA system.
- Barcode scanner: In the case of the double device auto-login approach, the user needs to have a barcode scanning application, e.g. i-nigma [172] on his smart phone to scan the generated QR code on the hotspot portal. The barcode reader scans the QR code and loads the scanned information into a SMS sending application on the smart phone.
- SMS application: Regardless of the selected auto-login approach (single device or double device) the user needs to have a smart phone and a SMS sending application on the smart phone to be able to communicate with the voucher server via SMS.

The activity diagram of the BIHA solution is presented in Figure 5.11. The diagram presents all the steps which are involved in the traditional hotspot login process and BIHA solution.

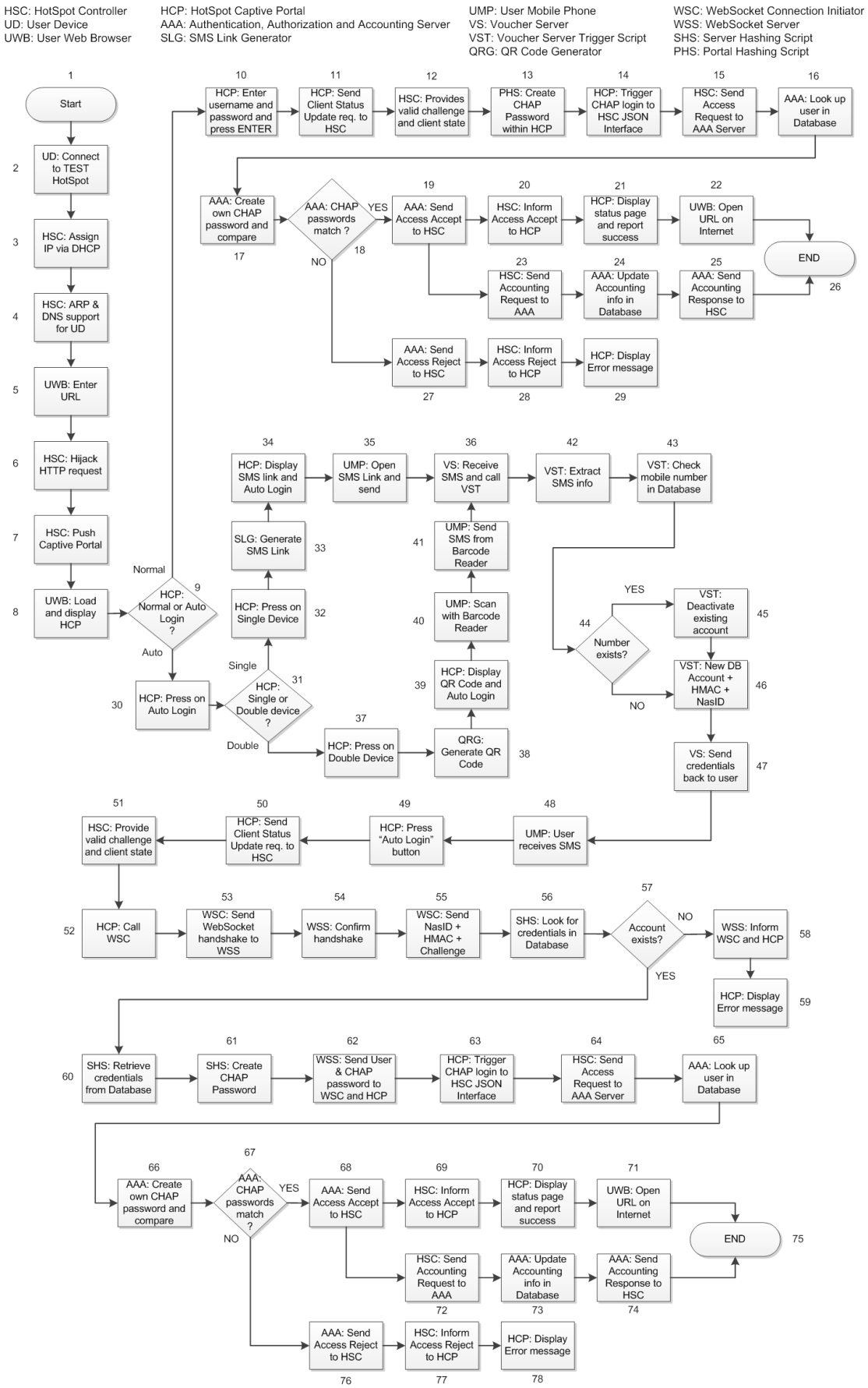


Figure 5.11: Activity diagram of barcode initiated hotspot auto-login solution.

Next a description of the steps performed in the activity diagram is given.

Common steps of traditional hotspot login and BIHA process:

1. The user turns on the device and the Wi-Fi interface.
2. The user searches for Wi-Fi and connects to the SSID Test-Hotspot.
3. CoovaChilli automatically assigns an IP address to the user device via DHCP.
4. CoovaChilli provides ARP and DNS protocols support for the clients on the Wi-Fi link.
5. The user tries to open a website on the Internet by entering the address in web browser.
6. CoovaChilli intercepts (hijacks) the HTTP request by monitoring the incoming packets.
7. CoovaChilli redirects the web browser website request to the address of the hotspot captive portal. This address includes several parameters, such as the MAC address, NasID and challenge.
8. The user's web browser loads the hotspot captive portal automatically.
9. The user decides whether he wants to use the barcode initiated hotspot auto-login or the traditional hotspot login process.

Use of traditional hotspot login:

10. The user enters the username and password in the logon box and presses enter
11. The ChilliController JavaScript object will send a status update request to CoovaChilli to verify the current client state and retrieve a valid challenge. The client state refers to the user logon status which could be either "1" or "0" which means "Authorized" and "Non-Authorized" respectively.
12. CoovaChilli responds the status update request from user's web browser, with a JSON formatted message including the challenge and client state.
13. The ChilliController JavaScript object from the hotspot portal, which is running inside the user's web browser, will use the entered password and the retrieved challenge to create a CHAP password based on the CHAP authentication method.
14. The ChilliController JavaScript object, will trigger the CHAP logon at the CoovaChilli (hotspot controller) by sending the username and CHAP password via the JSON logon interface to CoovaChilli.

15. CoovaChilli will send an access-request to the AAA (Radius) server including several parameters such as challenge, user name, CHAP password, client MAC address, IP address and network location.
16. The AAA server will look up the requested username in the database and will retrieve the password for that username.
17. The AAA server will create its own CHAP password by using the received challenge from CoovaChilli and the retrieved password from the database (not the CHAP password received from user).
18. The AAA sever will compare his own CHAP password with the CHAP password received from the client to verify if the user has provided a valid password.
19. AAA server will send an access-accept message to CoovaChilli to report successful authentication.
20. CoovaChilli will send an authentication success message to the portal in the user's web browser and change the client state to "1" which means that the user has logged in and can access the Internet.
21. The hotspot captive portal will display the status page for the client, which shows a successful logon and some additional information, such as log-off link and some usage statistics.
22. The user is now connected to the Internet and can start surfing.
23. CoovaChilli will send an accounting-request to the AAA server, which includes information about hotspot usage such as start time, username, MAC address.
24. The AAA server will update the received information in the database.
25. The AAA server will send an accounting-response message to CoovaChilli to confirm the updating of accounting data in the database.
26. End of logon process for the traditional hotspot login case.
27. The AAA server will send an access-reject message to CoovaChilli to report unsuccessful authentication due to password mismatch.
28. CoovaChilli will send an authentication failure message to the hotspot portal in user's web browser and keeps the client state at "0" which means user has not logged in and has no access to the Internet.
29. The captive portal will display an error message to user and notifies about unsuccessful logon.

Use of barcode initiated hotspot auto-login:

30. The user presses on the auto-login button to start the auto-login process.

31. The user decides whether he wants to use the single device or the double device approach.

Single device approach related steps of barcode initiated hotspot auto-login:

32. The user presses on single device button to trigger the single device auto-login process.

33. The SMS generation script will use the information held in CoovaChilli JavaScript object and generate a dynamic hyperlink which includes the hashed client mac address - HMAC, the network location ID - NasID and the voucher server's telephone number as well.

34. The hotspot captive portal will display the SMS link and the auto-login button to the user and asks him to click on the link and send SMS.

35. The user clicks on the SMS link and this automatically opens the SMS application of the mobile phone with the required verification information already filled in the SMS application. The user needs to press send SMS.

36. The voucher server will receive the text message from the user and a trigger script will be called to complete the remaining steps.

Double device approach related steps of barcode initiated hotspot auto-login:

37. The user presses on the double device button to trigger the double device auto-login process.

38. The QR code generation script will use the information held in the CoovaChilli JavaScript object and generate a QR code which includes the hashed client mac address - HMAC, the network location ID - NasID and the voucher server's telephone number as well.

39. The hotspot captive portal will display the QR code and the auto-login button to the user and ask him to scan the code using a barcode reader application and to send the SMS afterwards.

40. The user scans the QR code using a barcode reader application on his mobile phone.

41. After successful scanning, the user sends the scanned information via SMS. The SMS sending is triggered from the barcode reader application menu.

Common steps of barcode initiated hotspot auto-login:

42. The trigger script of voucher server will extract the following information from the received SMS: user's telephone number, hashed client MAC address, HMAC, network location ID, NasID.

43. The trigger script will look up the user's mobile phone number in the database.

44. The script will verify if the user already has an account in the database.

45. If the user has an existing account in the database, it will be deactivated.

46. A new user account will be created for the user. The username will be his phone number, the password will be a random value, and the HMAC and NasID values will be updated as well.

47. The voucher server sends the created credentials (user name and password) back to the user via SMS reply.

48. The user receives the SMS containing the user credentials (user name and password) and is now aware that a new account has been created for him. The user credentials will work to login using both traditional hotspot login and the novel barcode initiated hotspot auto-login.

49. The user presses the auto-login button to trigger the BIHA logon process.

50. The ChilliController JavaScript object will send a status update request to CoovaChilli to verify the current client state and to retrieve a valid challenge. The client state refers to the user logon status which could be either "1" or "0" which means authorized and non-authorized.

51. CoovaChilli responds the status update request from the user's web browser, with a JSON formatted message including the challenge and client state.

52. The hotspot captive portal will trigger the BIHA logon process by starting to open a WebSocket connection from the user's web browser to the external WebSocket server, to retrieve the logon credentials from the database automatically.

53. A WebSocket handshake will be sent to the external WebSocket server to start a WebSocket connection. The handshake includes a WebSocket security key.

54. The WebSocket server accepts the handshake and replies with a WebSocket accept key. This key protects this connection from being interfered or tampered with. However, it is still possible to view the packet content unless a WebSocket secure (WSS) connection is used.

55. The Portal will send the verification information to the WebSocket server. The WebSocket message contains: NasID, MD5 hashed client MAC address and the CHAP challenge. A sample message might look like:
cred+nas01+ee42005a8305edb02b7bbccf83045f37+d98555ea5b7ab4cb864e4f70be247ec1

56. After receiving the information, the server hashing script (SHS) on WebSocket server will extract the NasID, the HMAC and the challenge values from the message. By using NasID and hashed MAC address as the search key, the MySQL database can be queried for the proper credentials of the user.

57. The hashing script verifies whether there is an account related to the verification information (NasID and hashed MAC address) provided.

58. In case there is no user account, the script will notify the WebSocket server and the hotspot portal respectively.

59. The hotspot portal will display an error message to the user and asks him to send the verification information via SMS.

60. If a user account is available, the hashing script will retrieve the credentials from the database.

61. The hashing script will create a CHAP password for the user by using the received challenge from CoovaChilli and the retrieved password from the database.

62. The WebSocket server will send the credentials back to the hotspot portal. It includes the user's mobile phone number as the username and the created CHAP password.

63. The ChilliController JavaScript object, will trigger the CHAP logon to CoovaChilli by sending the username and CHAP password via the JSON logon interface to CoovaChilli.

64. CoovaChilli will send an access-request to the AAA radius server including several parameters such as challenge, user name, CHAP password, client MAC address, IP address and network location.

Similar steps as in the traditional hotspot login process:

65. The AAA server will look up the requested username in the database and will retrieve the password for that username.

66. The AAA server will create its own CHAP password by using the received challenge from CoovaChilli and the retrieved password from the database (not the CHAP password received from user).
67. The AAA sever will compare his own CHAP password with the CHAP password received from the client to verify if the user has provided a valid password.
68. The AAA server will send an access-accept message to CoovaChilli to report successful authentication.
69. CoovaChilli will send an authentication success message to the portal in the user's web browser and changes the client state to "1" which means user has logged in and can access the Internet.
70. The captive portal will display the status page for the client, which shows successful logon and some additional information such as the log-off link and some usage statistics.
71. The user is now connected to the Internet.
72. CoovaChilli will send an accounting-request to the AAA server, which includes information about hotspot usage such as: start time, username and MAC address.
73. The AAA server will update the received information in the database.
74. The AAA server will send an accounting-response message to CoovaChilli to confirm the update of the accounting data in the database.
75. End of the logon process for the BIHA logon case.
76. The AAA server will send an access-reject message to CoovaChilli to report an unsuccessful authentication due to password mismatch.
77. CoovaChilli will send an authentication failure message to the portal in the user's web browser and keep the client state at "0" which means the user has not logged in and access to the Internet is denied.
78. The captive portal will display an error message to the user and confirm the unsuccessful logon.

The implementation of the barcode initiated hotspot auto-login solution supports the traditional hotspot login process, which requires the customer to enter his user name and password manually. However, the novelty of the implementation is the single device and the double device approach which enable automated hotspot logon processes. The single device approach initiates the hotspot auto-login process by clicking on a solution specific link on the login page, while the double device

approach is initiated by scanning a barcode from the login page by means of a smart phone. Both approaches, the single and the double device, sends a SMS to the voucher server in the hotspot backbone to create a new user account. After creating the new user account the user name and password is sent back the users smart phone via SMS. At this point in time the user is able to click on the button auto-login on the login page to get logged-on to the hotspot automatically without the need to enter user name and password manually. This simplifies the login procedure significantly while at the same time overcoming the need to obtain a login voucher.

5.3 Graceful Denial of Service for IP-based Application Services

The graceful denial of service solution has been introduced in Subsection 4.3.4. In the following the implemented GDoS solution is presented. Figure 5.12 shows the implementation of the SEFA-GDoS system architecture. The InfSP consists of the SEF-GDoS-InfSP module, the database InfSP and the application service represented by means of a video portal. The database InfSP contains the table SPF, user and config. The user connects with the device to the video portal. The ENSP2 comprises the SEF-GDoS-ENSP2 module and the database ENSP2. The database ENSP2 contains the table CPF and config. The ENSP1 comprises the SEF-GDoS-ENSP1 module, the database ENSP1, and the business process execution language (BPEL) process which orchestrates requesting all GDoS relevant parameters from the several SEF-GDoS modules. The database ENSP1 contains the table CPF and config. The visualizer is used to illustrate the interactions and transmission of parameters transmitted via the interfaces involved.

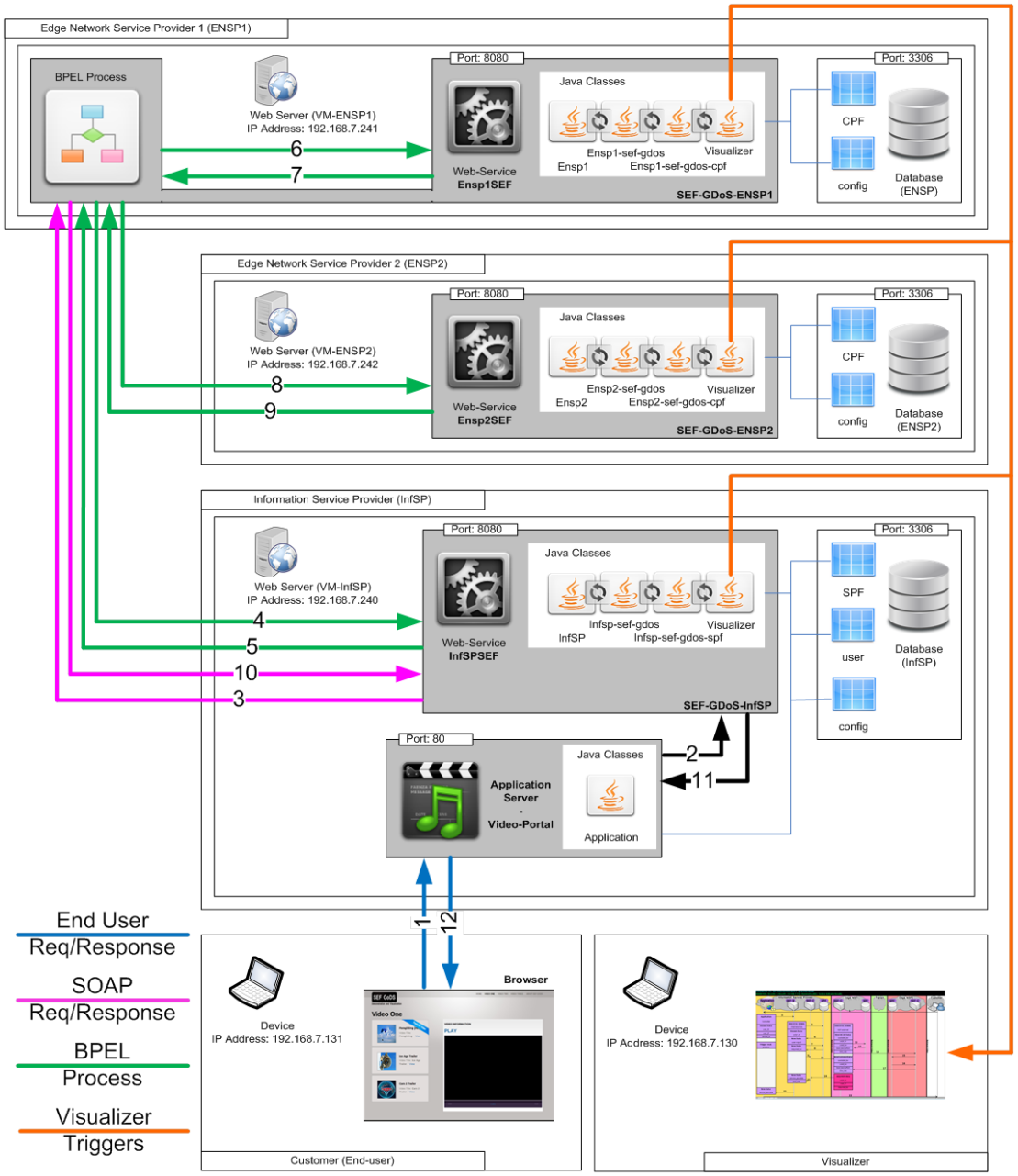


Figure 5.12: GDoS system architecture.

The functionality and the functional sequence of the presented GDoS system architecture, shown in Figure 5.12 are described by means of the following steps:

1. The end-user requests an application service, such as video on demand, in high definition (HD) quality from the video portal of the InfSP. The information received by the video portal from the end-user includes user_IP, user_ID and service_ID.

2. The video portal recognizes the service request of the device. The video portal triggers the SEF-GDoS-InfSP to initiate the GDoS evaluation process to evaluate the availability of network resources for a HD VoD service along the data path.

3. The SEF-GDoS-InfSP sends a graceful denial of service evaluation request to the BEPL process of the SEF-GDoS-ENSP1 to start the GDoS evaluation process.
4. The BPEL process of the SEF-GDoS-NSP1 requests the application service related network performance requirements from the SEF-GDoS-InfSP. The request consists of the parameters user_IP, user_ID and service_ID.
5. The web-service of the SEF-GDoS-InfSP obtains the application service requirement information from the SPF and sends this information back to the BPEL process of the SEF-GDoS-ENSP1. The reply consists of the parameters user_IP, user_nsp_ID, required_bandwidth, InfSP_IP, InfSP_passphrase.
6. The BPEL process of the SEF-GDoS-NSP1 requests network performance information of the connected InfSP (InfSP-ENSP1-connectivity) from the web-service of SEF-GDoS-ENSP1. The request comprises the parameters InfSP_IP.
7. The web-service of SEF-GDoS-ENSP1 obtains network performance information of InfSP-ENSP1-connectivity from CPF and sends this information back to the BPEL process of SEF-GDoS-ENSP1. The reply consists of the parameters available_bandwidth, InfSP_IP, used_bandwidth, level_best_effort and ASQ_info of the InfSP.
8. The BPEL process of SEF-GDoS-NSP1 requests network performance information of the connected end-user (end-user-ENSP2-connectivity) from the web-service of SEF-GDoS-ENSP2. The request consists of the parameters user_IP.
9. The web-service of SEF-GDoS-ENSP2 obtains the network performance information of end-user-ENSP2-connectivity from the CPF and sends this information back to the BPEL process of SEF-GDoS-ENSP1. The reply consists of the parameters available_bandwidth, user_IP, used_bandwidth, level_best_effort and ASQ_info of the end-user.
10. After receiving all required information the graceful denial of service evaluation process is performed by the BPEL process of the SEF-GDoS-NSP1. The BPEL process compares the available network performance capabilities with the application service requirements on network performance. The GDoS result is then sent to the SEF-GDoS-InfSP.
11. The SEF-GDoS-InfSP provides the video portal with the graceful denial of service evaluation result information.

12. The feedback of the graceful denial of service evaluation result is shown to the end-user. The end-user is now informed whether the requested service is providable in the requested quality or not.

The SEFA-GDoS added value service is realised by means of several SEF-GDoS modules. The functionality of these modules depends on the location where these modules are installed and thus, in which actor domain the SEF-GDoS module is located. In the following the purpose of the actors (InfSP, ENSP1 and ENSP2) as well as the SEF-GDoS modules (SEF-GDoS-InfSP, SEF-GDoS-ENSP1 and SEF-GDoS-ENSP2) is described. Moreover, the functionalities as well as the parameters utilized in the different web-services and Java classes shown in Figure 38 and Figure 39 are described.

Information Service Provider:

The information service provider might for example run a portal that offers video content to the customer via a web-based frontend. Beside the video portal, the InfSP runs the SEF-GDoS-InfSP module that consists of a web-service InfSPSEF and the database InfSP. The Java classes of the web-service are Infsp, Infsp-sef-gdos and Infsp-sef-gdos-spf. The utilised database InfSP consists of a table named SPF. Moreover, the video portal contains a SEF-GDoS module consisting of a Java class application which triggers the initiation of the SEFA-GDoS added value service in the case of receiving a video request from the end-user. In the following the Java class and its functionality in the application server contained in the packet application is described.

Functionality of class application:

The application class is part of the package application and is located inside the application server. The added value service SEFA-GDoS is requested by the method request_SEFA_service when an application service request is detected. The detection of a service request is performed by the method application_service_request when the end-user clicks the play button on the video portal. To request the corresponding SEFA added value service the parameter SEFA_service_ID is used. The result of the SEFA-GDoS added value service is delivered back to the class application by means of the parameter SEFA_service_result. In the SEFA-GDoS use case the parameter SEFA_service_result indicates whether the application service (in this example the

video service) can be provided in user requested quality. The SEFA-GDoS result is presented in the video portal.

Parameters:

- application_instance_ID: Indication of a specific application instance, e.g. the video ‘XYZ’
- application_server_IP: IP address of the application server
- user_ID: Identifier of the user used by information service provider
- user_IP: IP address of the user provided by ENSP2
- SEFA_service_ID: SEFA identifier is used to determine the responsible SEFA added value service
- SEFA_service_result: Result of the SEFA added value service (depends on the processed SEFA added value service)

In the following the Java classes and the functionalities of the web-service InfSPSEF contained in the packet InfSP are described.

Functionality of Class Infsp:

The Infsp class is part of the package InfSP and is located inside the web-service InfSPSEF in the information service provider domain. Based on the parameter SEFA_service_ID the method find_SEFA_service_coordinator the service provider requests the SEFA-GDoS added value service. The obtained parameter SEFA_service_coordinator_IP from the method find_SEFA_service_coordinator is used to trigger the SEFA-GDoS by means of the method initiate_SEFA_service. The SEFA-GDoS coordinator is located in ENSP1. SEFA-GDoS is requested by means of the interface Sefa_service_initiation. To perform the InfSP part of SEFA-GDoS, when requested via the interface Ensp1-sef-gdos_infsp-nsp, the method select_SEFA_service is performed to request SEFA-GDoS related methods of the InfSP, which are contained in the class Infsp-sef-gdos. Selection of the SEFA-GDoS is determined based on the parameter SEFA_service_ID, which is received via the interface Ensp1-sef-gdos_infsp-nsp. The result of SEFA-GDoS is delivered to the class Application by utilising the method delivery_of_SEFA_service_result.

Parameters:

- infsp_ID: Classifier for information service provider

- application_instance_ID: Indication of a specific application instance, e.g. the video ‘XYZ’.
- application_requirements: Describes the requirements on network performance which is needed to deliver the application service in user satisfying quality.
- application_server_IP: The IP address of the application server.
- user_ID: Identifier of the user used by information service provider.
- user_IP: The IP address of the user provided by ENSP2.
- user_nsp_ID: Identifier of the network service provider of the end-user.
- SEFA_service_ID: The SEFA identifier is used to determine the SEFA added value service.
- SEFA_service_coordinator_IP: The IP address of the entity which is coordinating and starting the SEFA added value service.
- SEFA_service_result: The result of the SEFA added value service (depending on the processed SEFA added value service).

Functionality of class InfSP-sef-gdos:

The InfSP-sef-gdos class is part of the package InfSP and is located inside the web-service InfSPSEF in the information service provider domain. The methods of this class are used to obtain application service related information needed for SEFA-GDoS. The method get_application_service_requirements is used to obtain the application requirements on network performance. The application requirements are determined by means of the parameter application_instance_ID and are stored in the parameter application_requirements. The method get_ensp_of_customer is used to obtain the network service provider of the end-user. The network service provider is determined by means of the parameter user_ID and is stored in the parameter user_nsp_ID. The methods, get_application_service_requirements and get_ensp_of_customer obtain the requested parameters by means of the method request_db_spf in class Infst-sef-gdos-spf.

The method deliver_parameters_to_sefa-gdos_coordinator is used to send the obtained parameters application_requirements and user_nsp_ID to class Ensp1-sef-gdos in package Ensp1 via the interface Ensp1-sef-gdos_infsp-nsp.

Parameters:

- infsp_ID: Classifier for the information service provider.

- application_instance_ID: Indication of a specific application instance, e.g. the video ‘XYZ’.
- application_requirements: Describes the requirements on the network performance which are needed to deliver the application service in user satisfying quality.
- application_server_IP: The IP address of the application server.
- user_ID: The identifier of the user used by the information service provider.
- user_IP: The IP address of the user provided by ENSP2.
- user_nsp_ID: The identifier of the network service provider of the end-user.
- SEFA_service_ID: The SEFA identifier is used to determine the SEFA added value service.
- SEFA_service_result: Result of the SEFA added value service depending on the processed SEFA added value service.

Functionality of class InfSP-sef-gdos-spf:

The InfSP-sef-gdos-spf class is part of the package InfSP and is located inside the web-service InfSPSEF in the information service provider domain. The method request_db_spf of this class is used to obtain application service related information needed for SEFA-GDoS. The application requirements on network performance are determined by means of the parameter application_instance_ID requested by the method get_application_service_requirements. The application requirements are stored in the parameter application_requirements. The network service provider of the end-user is determined by means of the parameter user_ID requested by the method get_ensp_of_customer. The obtained network service provider information is stored in parameter user_nsp_ID.

Parameters:

- application_instance_ID: Indication of a specific application instance, e.g. the video ‘XYZ’.
- application_requirements: Describes the requirements on the network performance which is needed to deliver the application service in user satisfying quality.
- user_ID: Identifier of the user used by information service provider.
- user_IP: The IP address of the user provided by ENSP2.

- user_nsp_ID: Identifier of network service provider of the end-user.

Edge Network Service Provider 1:

The edge network service provider 1 (ENSP1) connects the InfSP to the Internet. The ENSP1 runs the SEF-GDoS-ENSP1 module that consists of a web-service Ensp1SEF and the database ENSP1. The Java classes of the web-service are Ensp1, Ensp1-sef-gdos and Ensp1-sef-gdos-cpf. The utilised database ENSP1 consists of a table named CPF. In the following the Java classes and the functionalities of the web-service Ensp1SEF, contained in packet Ensp1, are described.

Functionality of class Ensp1:

The Ensp1 class is part of the package Ensp1 and is located inside the web-service Ensp1SEF in the domain of the edge network service provider 1. The coordination entity of the SEFA-GDoS added value service is located in ENSP1. The SEFA-GDoS is requested by means of the interface Sefa_service_initiation. Based on the received parameter SEFA_service_ID and the method select_SEFA_service the method sefa_gdos_coordination in the class Ensp1-sef-gdos is requested to start and coordinate the SEFA-GDoS. The result of SEFA-GDoS provided by the method perform_sefa_gdos in class Ensp1-sef-gdos and is delivered to the class Infsp via the interface Sefa_service_initiation.

Parameters:

- infsp_ID: The classifier for information service provider.
- application_instance_ID: Indication of a specific application instance, e.g. the video ‘XYZ’.
- application_requirements: Describes the requirements on the network performance that is needed to deliver the application service in user satisfying quality.
- application_server_IP: The IP address of the application server.
- user_ID: Identifier of the user used by the information service provider.
- user_IP: The IP address of the user provided by ENSP2.
- user_nsp_ID: The identifier of the network service provider of the end-user.
- SEFA_service_ID: SEFA identifier is used to determine the responsible SEFA added value service.

- SEFA_service_result: Result of the SEFA added value service depending on the processed SEFA added value service.

Functionality of class Ensp1-sef-gdos:

The Ensp1-sef-gdos class is part of the package Ensp1 and is located inside the web-service Ensp1SEF in the domain of the edge network service provider 1. The method sefa_gdos_coordination requests by means of methods get_application_requirements_from_infsp, get_access_network_capabilities_from_ensp2 and get_access_network_capabilities_of_infsp the required information to derive the result of the SEFA-GDoS. For that purpose the method get_application_requirements_from_infsp requests through the parameters user_ID, user_IP, application_service_ID and SEFA_service_ID via the interface Ensp1-sef-gdos_infsp-nsp the application related information. This information is the application requirements stored in parameter application_requirements and the network service provider of the end-user stored in parameter user_nsp_ID. The method get_access_network_capabilities_of_infsp requests by means of parameter application_server_IP and method request_db_cpf in class Ensp1-sef-gdos-cpf the access network capabilities of the connection between InfSP and ENSP1. The access network capabilities of the InfSP – ENSP1 connectivity are stored in the parameter available_bandwidth_of_InfSP. The method get_access_network_capabilities_from_ensp2 requests with parameter user_IP via interface Ensp2-sef-gdos_nsp-nsp the access network capabilities of the connection between ENSP2 and the end-user. The access network capabilities of the end-user – ENSP2 connectivity are stored in the parameter available_bandwidth_of_user.

After receiving all parameters needed to derive the SEFA-GDoS result the method perform_sefa_gdos is requested. The method perform_sefa_gdos investigates the available bandwidth conditions of the connectivity end-user – ENSP2 and InfSP – ENSP1. Moreover, these conditions are compared to the application requirements. In case the network capabilities are sufficient to deliver the requested service in satisfying quality, the SEFA-GDoS result is service possible. Otherwise, the SEFA-GDoS result is service not possible. The result of SEFA-GDoS is stored in the parameter SEFA_service_result.

Parameters:

- infsp_ID: Classifier for the information service provider.
- application_instance_ID: Indication of a specific application instance, e.g. the video ‘XYZ’.
- application_requirements: Describes the requirements on the network performance which is needed to deliver the application service in user satisfying quality.
- application_server_IP: The IP address of the application server.
- available_bandwidth_of_InfSP: Information about available bandwidth of connection InfSP – ENSP1.
- user_ID: Identifier of the user used by information service provider.
- user_IP: The IP address of the user provided by ENSP2.
- user_nsp_ID: Identifier of network service provider of the end-user.
- available_bandwidth_of_user: Information about the available bandwidth of the connection of the end-user – ENSP2,
- SEFA_service_ID: The SEFA identifier is used to determine the responsible SEFA added value service.
- SEFA_service_result: The result of the SEFA added value service depending on the processed SEFA added value service,

  Functionality of the class Ensp1-sef-gdos-cpf:

The Ensp1-sef-gdos-cpf class is part of the package Ensp1 and is located inside the web-service Ensp1SEF in the domain of the edge network service provider 1. The method request_db_cpf of this class is used to obtain the network capabilities of the connection between InfSP and ENSP1. The network capabilities are determined by means of the parameter application_server_IP requested by the method get_access_network_capabilities_of_infsp. The information about the network capabilities is stored in the parameter available_bandwidth_of_InfSP.

Parameters:

- application_server_IP: The IP address of the application server,
- available_bandwidth_of_InfSP: Information about available bandwidth of connection InfSP – ENSP1.

Edge Network Service Provider 2:

The edge network service provider 2 (ENSP2) connects the end-user to the Internet. The ENSP2 runs the SEF-GDoS-ENSP2 module that consists of a web-service Ensp2SEF and the database ENSP2. The Java classes of the web-service are Ensp2, Ensp2-sef-gdos and Ensp2-sef-gdos-cpf. The utilised database ENSP2 consists of a table named CPF. In the following the Java classes and the functionalities of the web-service Ensp2SEF, contained in packet Ensp2 are described.

Functionality of class Ensp2:

The Ensp2 class is part of the package Ensp2 and is located inside the web-service Ensp2SEF in the domain of the edge network service provider 2. To perform the ENSP2 part of SEFA-GDoS, when requested via the interface Ensp2-sef-gdos_nsp-nsp, the method select_SEFA_service is performed to request the SEFA-GDoS related methods of the ENSP2, which are contained in class Ensp2-sef-gdos. The selection of the SEFA-GDoS is done based on the parameter SEFA_service_ID, which is received via the interface Ensp2-sef-gdos_nsp-nsp.

Parameters:

- user_IP: The IP address of the user provided by ENSP2.
- SEFA_service_ID: The SEFA identifier is used to determine the responsible SEFA added value service.
- available_bandwidth_of_user: Information about the available bandwidth of the connection of the end-user – ENSP2.

Functionality of class Ensp2-sef-gdos:

The Ensp2-sef-gdos class is part of the package Ensp2 and is located inside the web-service Ensp2SEF in the domain of the edge network service provider 2. The methods of this class are used to obtain the network capabilities of the connection between the end-user and ENSP2. The method get_access_network_capabilities_of_end-user is used to obtain the network capabilities of the connection between the end-user and the ENSP2. The network capabilities are determined by means of the parameter user_IP and are stored in the parameter available_bandwidth_of_end-user. The method get_access_network_capabilities_of_end-user obtains the requested parameter by means of the method request_db_cpf in class Ensp2-sef-gdos-cpf. The method deliver_parameters_to_sefa-gdos_coordinator is used to send the obtained parameter

available_bandwidth_of_end-user to class Ensp1-sef-gdos in package Ensp1 via interface Ensp2-sef-gdos_nsp-nsp.

Parameters:

- user_IP: The IP address of the user provided by ENSP2.
- available_bandwidth_of_user: Information about the available bandwidth of the connection end-user – ENSP2.

Functionality of class Ensp2-sef-gdos-cpf:

The Ensp2-sef-gdos-cpf class is part of the package Ensp2 and is located inside the web-service Ensp2SEF in the domain of the edge network service provider 2. The method request_db_cpf of this class is used to obtain the network capabilities of the connection between the end-user and the ENSP2. The network capabilities are determined by means of the parameter user_IP requested by the method get_access_network_capabilities_of_end-user. The information about the network capabilities is stored in the parameter available_bandwidth_of_end-user.

Parameters:

- user_IP: The IP address of the user provided by the ENSP2.
- available_bandwidth_of_user: Information about the available bandwidth of the connection end-user – ENSP2.

5.4 Summary

The implementation of the novel sequential authentication solution in Section 5.1 is designed to overcome the drawback of long authentication times in WLAN handovers processes. The most influencing factor on interruption time is the handshake among the authenticator on the AP and the RADIUS server on the AAA server. It has been shown that varying the location of the AAA server, such as network local or network external have a significant impact on the consumed authentication time and thus, on the communication interruption time. The novel sequential authentication solution introduced overcomes the large handshake times by combining two network access control and WLAN security mechanisms, such as IEEE 802.11i PSK and IEEE 802.11i EAP-TLS. In the first step of network access control the use of the PSK method enables a secure and WLAN link with encrypted network access. However, in the new sequential authentication solution PSK based WLAN access is granted only for a configurable time window. Within this time

window the client has to perform EAP-TLS authentication in the background. In the second step, after successful EAP-TLS authentication the client is granted network access and reconnects to the WLAN by means of the newly derived EAP-TLS WLAN encryption key. The sequential authentication solution has been realised by means of extending the software hostapd in version 0.6.4 [179] and wpa_supplicant in version 0.6.6 [178].

The implementation of a novel barcode initiated hotspot auto-login solution in Section 5.2 is developed to enable hotspot use on demand, payment of hotspot use by means of SMS fees and to perform automated hotspot login. The BIHA solution avoids an entering of a user name and password on the hotspot login page. By means of an automatically generated link or barcode on the hotspot login page, the hotspot auto-login process is initiated. After opening the SMS tool on the smart phone, triggered by the link or barcode and the creation of the hotspot user account the user gets logged in automatically. The barcode initiated hotspot auto-login solution has been realised by means of the software CoovaChilli [85], SMS server tools 3 [182], FreeRADIUS [181], MySQL, barcode generator [185] and barcode scanner [172].

The implementation of the graceful denial of service solution in Section 5.3 realises a service quality indication feedback for the user. This informs the user about the expected application service quality in advance of the service. The implemented GDoS behaves as a busy signal known from the traditional telephony. The GDoS solution gathers application requirements of the network performance from an information service provider and available bandwidth network information from a network service provider to derive the GDoS feedback. The graceful denial of service solution has been implemented by means of the business process execution language (BPEL), web services and a MySQL database.

6 Results

In this chapter the verification and benchmarking of the proof of concept implementations of Chapter 5 based on the novel concepts presented in Chapter 4 is carried out. Section 6.1 presents the verification while Section 6.2 presents the benchmarking results of the implemented solutions. In Subsection 6.1.1 and 6.2.1 the sequential authentication solution of Section 4.1 is investigated which is related to the service quality. In Subsection 6.1.2 and 6.2.2 the barcode initiated hotspot auto-login solution of Section 4.2 is investigated which is related to usability. In Subsection 6.1.3 and 6.2.3 the graceful denial of service solution of Section 4.3 is investigated which is related to quality awareness.

6.1 Verification

In this section the verification of the proposed the sequential authentication solution, the barcode initiated hotspot auto-login solution and the graceful denial of service solution of Section 4.1 is performed.

6.1.1 Sequential Authentication Solution

The verification of the sequential authentication solution is done based on the technical requirements presented in Table 4.5 and the general requirements presented in Table 4.4. The proposed sequential authentication solution provides the status quo of the most secure WLAN encryption based on standardised network access control mechanisms, such as WPA2 PSK and WAP2 EAP-TLS. This means no additional protocol interactions are integrated in the sequential authentication concept which might change the behaviour of WPA2 PSK and WAP2 EAP-TLS in its general manner. The concept includes no mechanisms that improve handover performance, such as pre-authentication of IEEE 802.11i or IEEE 802.11r. The reason for not including such mechanisms is to avoid an additional network load generated by the exchange information among the entities involved. Furthermore, the applicability in inter-provider handover scenarios will not be at risk due to the required link layer connectivity of e.g. IEEE 802.11i pre-authentication. Due to the known operation

behaviour of WPA2 PSK and WPA2 EAP-TLS the implementation of the sequential authentication solution in a real testbed focused on demonstrating the proper operation instead of evaluations that are merely based on simulations.

The first phase of the sequential authentication solution carries out network access control by means of WPA2 PSK. In the case of successful user authentication the network access will be granted and a temporal port will be established. The temporal port is valid for a configurable time only. After this timeout the wireless client will be disconnected and blocked for a configurable duration. The temporal port is used to enable the transport of the payload, such as VoIP traffic, while the second phase of sequential authentication solution will be performed. In the second phase the WPA2 EAP-TLS authentication will be carried out. In the case of successful authentication the network access will be granted and the temporal port will be released. The benefit of the sequential authentication solution is the possibility of transmitting payload after the successful completion of the first authentication phase.

Figure 6.1 presents the sequence diagram of the sequential authentication solution. Compared to the traditional IEEE 802.1X method the sequential authentication solution comprises of five sequences to carry out device authentication instead of the traditional four sequences. The first sequence is the PSK 4-way handshake to authenticate the device against authenticator and to derive the wireless encryption key for further secure communication. The following sequences, such as EAP Initiation, TLS handshake, EAP termination and PMK 4-way handshake are to the same as the traditional IEEE 802.1X authentication using EAP-TLS. In general no redesign of the standardised mechanisms WPA2 PSK and EAP-TLS is needed for the novel concept.

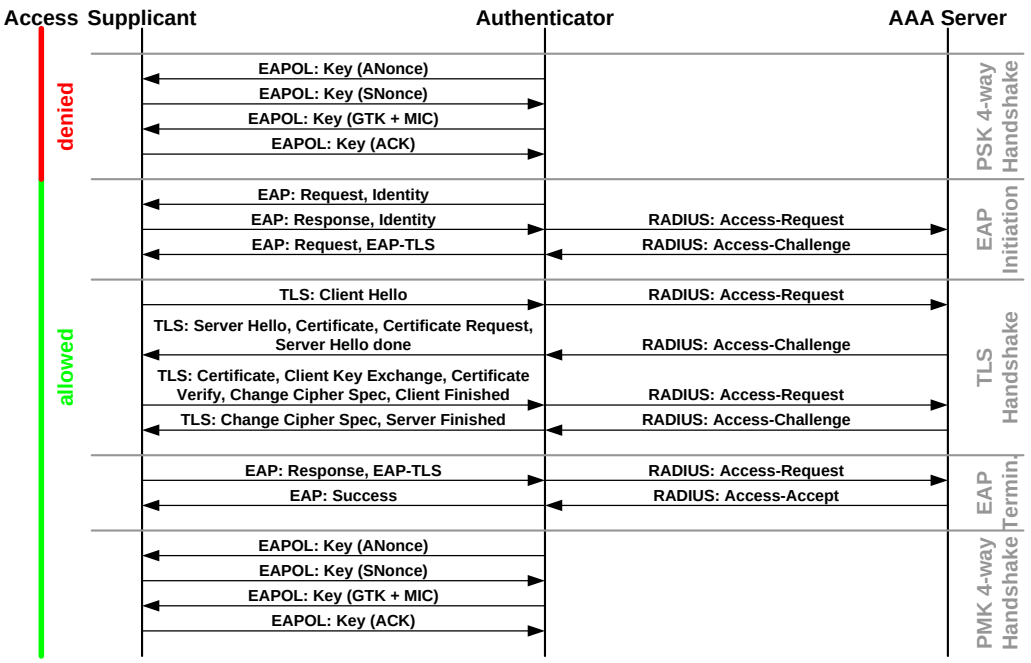


Figure 6.1: Sequence diagram of sequential authentication solution.

The dark (red) and bright (green) marked line called access, in Figure 6.1, shows that network access will already be granted after a successful WPA2 PSK authentication - PSK 4-way handshake. As a result, data communication, such as VoIP traffic, can be provided with IEEE 802.1X using EAP-TLS authentication. This means a handover is carried out and network access is granted after the 4-way handshake of the PSK method. As a result, the active real-time service session is no longer influenced by network authentication or re-association process of the EAP-TLS method.

The technical requirement SAS-tech-req-1 in Table 4.5 ‘Reduce time of data communication interruptions in WLAN handover processes which are induced by authentication and authorisation methods’ on the sequential authentication solution has been achieved when the authentication and authorisation method EAP-TLS is used. More details about the achieved result are presented in Subsection 6.2.1 benchmarking of sequential authentication solution.

The general requirements SAS-gen-req-1 till SAS-gen-req-5 in Table 4.4 are met due to the state-of-the-art mechanisms WPA2 PSK and WPA2 EAP-TLS. SAS-gen-req-1 to avoid unauthorised network access is provided by the WPA2 PSK and WPA2 EAP-TLS mechanism itself. SAS-gen-req-2 high level of trust among user and access network has been achieved by using the EAP-TLS method which provides mutual authentication to ensure a high level of trust among the user and the

access network. SAS-gen-req-3 privacy of user and confidentiality is provided by WPA2 which performs encryption to avoid intercepting of user data by malicious users. SAS-gen-req-4 the use state-of-the-art mechanisms is realised by applying WPA2 PSK and WPA2 EAP-TLS. The Federal Office for Information Security (BSI) of Germany advises in [76] the employment of WPA2 in WLANs to achieve a secure wireless network. From today's point of view WPA2 comprises the strongest algorithms to carry out encryption and to provide data integrity. SAS-gen-req-5 the use of standardised mechanisms is realised by using WPA2 PSK and WPA2 EAP-TLS. Today's most securing mechanisms for WLAN architectures are specified in the IEEE 802.11i standard [74]. A subset of the IEEE 802.11i specifications are comprised in the Wi-Fi Alliance specification WPA2. SAS-gen-req-6 is achieved due to the proposed sequential authentication solution which combines both mechanisms of WPA2 PSK and WPA2 EAP-TLS to improve WLAN handovers which results in better support of real-time application services.

With regard to SAS-gen-req-1 to avoid unauthorised network access, the device is able to gain network access again by reinitiating the sequential authentication process. This could be used to start a denial of service attack on the sequential authentication solution. To eliminate this risk, the sequential authentication solution limits the number of authentication initiation repetitions in a certain interval. In the presented solution this interval is fully configurable to be prepared for different attack scenarios. In the case that a device is not able to carry out the sequential authentication process successfully within the defined authentication repetitions the MAC address of the UE will be blocked by the access point for a configurable duration.

In the case of a malicious user obtaining knowledge about the PSK needed to carry out the higher layer authentication and authorisation phase 1 successfully the sequential authentication solution envisions policy based network access. This means the privileges of network access after the higher layer authentication and authorisation phase 1 and 2 differs from each other, as shown in Figure 4.4 by means of row selected data communication. To avoid data injected by a malicious user before the sequential authentication process is finished only selected data communication is allowed after the higher layer authentication and authorisation phase 1. All other communication towards the access network will be restricted. Full

data communication is allowed only after successfully higher layer authentication and authorisation phase 2.

6.1.2 Barcode Initiated Hotspot Auto-login

The verification of the barcode initiated hotspot auto-login solution is carried out based on the technical requirements presented in Table 4.9 and the general requirements presented in Table 4.8. The proposed barcode initiated hotspot auto-login solution is able to provide a hotspot login mechanism which avoids entering of the user name and password on the hotspot login page and provides user credentials on demand. In Figure 6.2 the graphical user interface to logon to the hotspot is presented. The hotspot login page is the initial page of the graphical user interface which will be shown to the user upon his first http request. By means of the hotspot login page, the user is able to select between the traditional hotspot login or the barcode initiated hotspot auto-login solution.

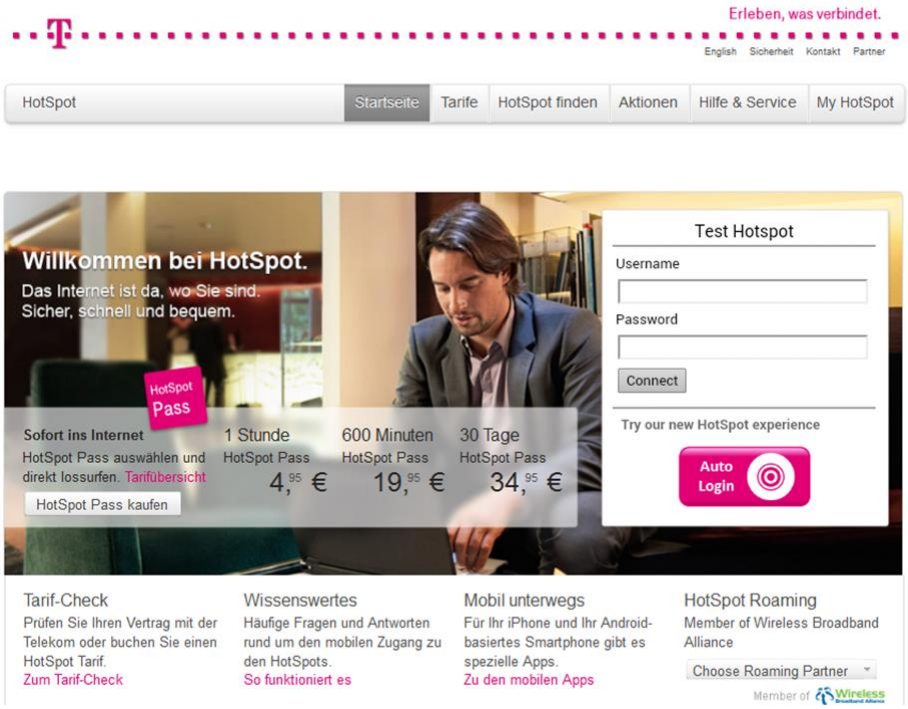


Figure 6.2: Graphical user interface: hotspot login page with option to select barcode initiated hotspot auto-login solution for hotspot login.

In Figure 6.3 the graphical user interface presenting the BIHA front-end to the user is shown. By means of the BIHA front-end, the user has the ability to go through the hotspot auto-login process by scanning the barcode and sending the verification information via SMS in step 1 and then pressing on the Auto-Login button in step 2.

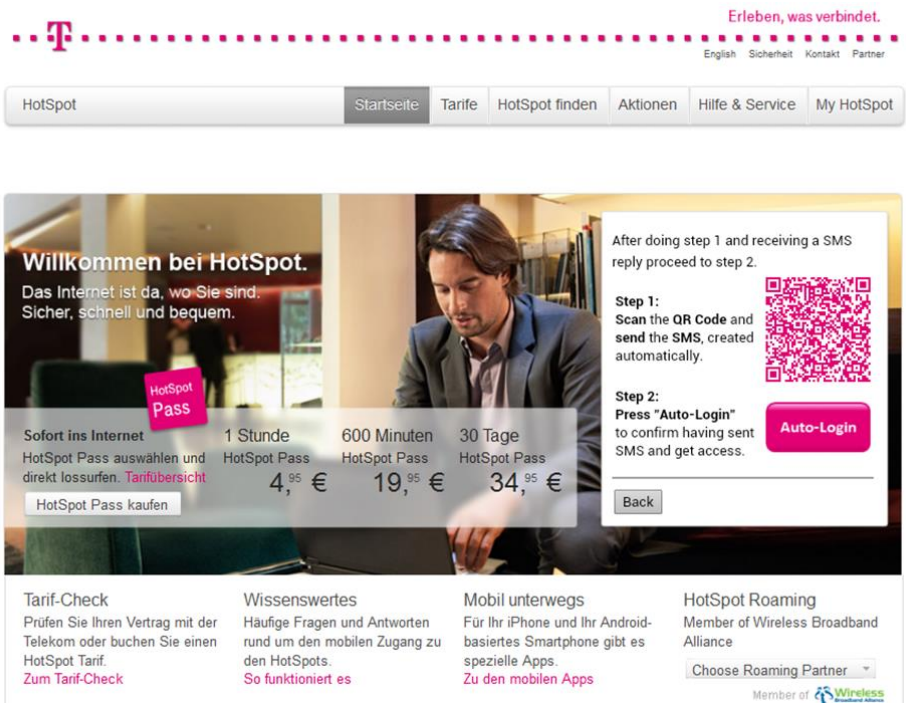


Figure 6.3: Graphical user interface: barcode initiated hotspot auto-login front-end to the user on the hotspot login page.

By pressing the Auto-Login button, the device and user can be authenticated and authorised by the hotspot system. In the case of a successful authentication and authorisation process the device is then logged in to the hotspot which is presented in Figure 6.4.

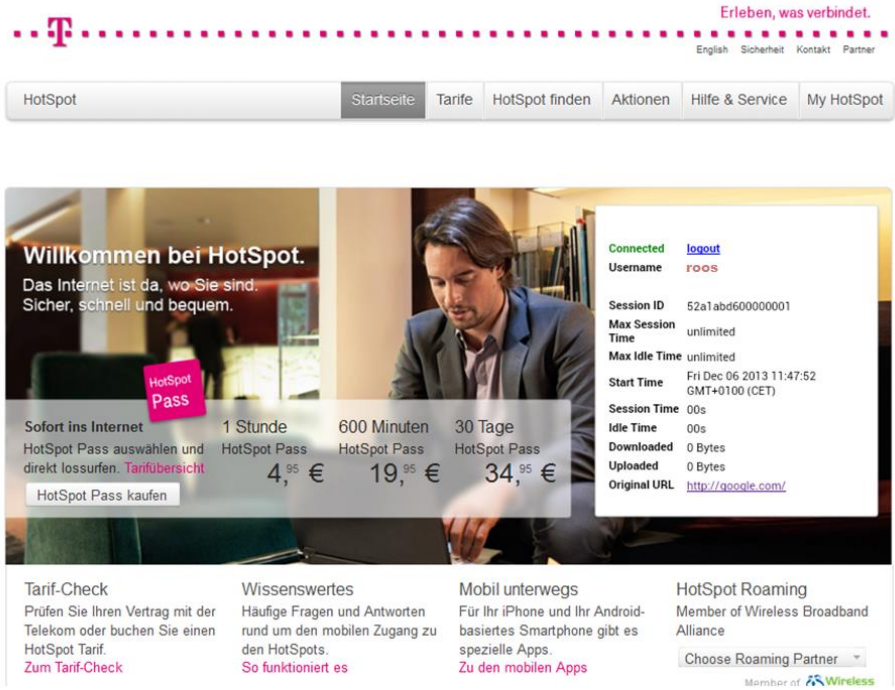


Figure 6.4: Graphical user interface: hotspot login page with information from a successfully performed hotspot logon.

In the following the capabilities of the barcode initiated hotspot auto-login (BIHA) solution are compared with the behaviour of today's hotspot solutions, as shown in Table 6.1. The compared characteristics are usability for user (voucher exists), usability for user (voucher does not exist), flexible use, availability of voucher, administration conditions of the hotspot, economic aspects of the hotspot carrier, the economic aspects of the user, and the ecological aspects.

Characteristics	BIHA	Traditional
Usability for user (voucher exists)	+	+
Usability for user (voucher does not exist)	+	-
Flexible use	+	-
Availability of voucher	+	-
Administration conditions of the hotspot	+	+
Economic aspects of the hotspot carrier	+	-
Economic aspects of the user	+	-
Ecological aspects	+	-

Table 6.1: Comparison of barcode initiated hotspot auto-login solution with traditional hotspot voucher solutions.

Usability for user (voucher exists) – the point of time of hotspot use is flexible in the case of BIHA as well as traditional hotspot voucher. All necessary information, such as user credentials, are available to initiate the hotspot login process manually or in the case of BIHA the login process can be performed automatically.

Usability for user (voucher does not exist) – in the case of a traditional hotspot voucher the point of time of hotspot use is not flexible and not arbitrary by the user. This behaviour is different in the proposed BIHA solution. The availability of the displayed barcode on the hotspot login page provides the possibility to get a voucher and the user credentials on demand via a SMS. This means that the voucher is provided in a comfortable way without the need to obtain the printed or traditional voucher e.g. from the reception of a hotel or campsite.

Flexible use – the BIHA solution provides flexible use of the hotspot. This means in the case of an expired hotspot session the use of the barcode on the hotspot login page enables the request of new hotspot user credentials. As a result, the hotspot use can be used in a very flexible way depending on the user's needs. This behaviour differs from the traditional hotspot voucher solutions. In the case of an expired hotspot session, a new voucher with login information is needed. Thus, the user has to obtain a new voucher. This means, the duration of hotspot use is not as flexible

and not as comfortable as in the novel BIHA solution because the user has to decide in advance how long to stay in the hotspot.

Availability of voucher – the BIHA solution provides the highest availability to request a voucher. Due to the depicted barcode on the hotspot login page the user is able to initiate the hotspot auto-login process on demand and at any time. In comparison to the BIHA solution the traditional voucher might not always be easily or comfortably availability as the hotspot service personal needs to be contacted or registration on an online portal is required including the transmission of payment details.

Administration conditions of the hotspot – The administration effort of the BIHA solution and the traditional voucher is comparable particularly when the hotspot fees have to be adjusted. In the case of centralised hotspot management the reconfiguration of hotspot fee specifications can be carried out with proportionally less effort while in the BIHA solution the premium SMS needs to be changed according to the new hotspot fees.

Economic aspects of the hotspot carrier – the BIHA solution combines the benefit of a paperless voucher system. Consequently, the paper and print cost as well as logistic costs can be avoided. This is not the case for the traditional voucher. Updated information, e.g. new hotspot fees specifications, lead to invalidity of the existing vouchers and requires new vouchers which will result in additional costs.

Economic aspects of the user – the BIHA solution enables hotspot use on demand. In contrast to the traditional voucher scenario the BIHA solution avoids the necessity to buy vouchers in advance. The consequence is that the requirement for voucher bought in advance can be avoided. Moreover, expiration of the validity of existing vouchers due to non hotspot use can be avoided as well.

Ecological aspects – considering the characteristics of the *economic aspects of the hotspot carrier* the BHIA solution provides the highest contribution to save natural resources. In comparison to the traditional voucher the BHIA solution requires no paper, no ink and no transportation of vouchers.

The technical requirement in Table 4.9, such as BIHA-tech-req-1 automated hotspot login, BIHA-tech-req-2 hotspot use on demand, BIHA-tech-req-3 no barrier of hotspot use for new users and BIHA-tech-req-4 user-friendly way of hotspot payment have been achieved using the novel barcode initiated hotspot auto-login

solution. The user is able to use the hotspot on demand by scanning the barcode on the hotspot login page and by sending an SMS (step 1), as shown in Figure 6.3. By means of the BIHA solution the user get logged in automatically after scanning the barcode on the hotspot login page and sending the SMS (step 1) and clicking on the Auto-login button afterwards (step 2). The BIHA solution provides no barrier of hotspot use for new users, only a mobile phone with a barcode reader application is needed. A user-friendly way of hotspot payment has been achieved by the BIHA solution by using a premium SMS for hotspot fee payment. The full details outlining the benchmarking result achieved are presented in Subsection 6.2.2.

The general requirements BIHA-gen-req-1 till BIHA-gen-req-4 in Table 4.8 are completely fulfilled by the BIHA solution. BIHA-gen-reg-1 to avoid unauthorised hotspot network access is provided by the applied hotspot controller CoovaChilli which performs network access control. Only a user with valid user credentials has Internet access granted. BIHA-gen-reg-2 to provide traceability of hotspot use is required to conform to the Telemediengesetz [171] in the case of misuse or violation of state law by a hotspot user is supported by the BIHA solution. The BIHA solution utilises the mobile phone number as the hotspot login user name. In the case of misuse or violation of state law by a hotspot user, further information, such as name of the user and address can be request by the mobile operator to identify the user. However, a direct relation between the hotspot user name and the name of the user cannot be determined by the hotspot operator without requesting this information from the mobile operator of the user. This ensures the privacy of the hotspot user. BIHA-gen-reg-3 is the use of state-of-the-art mechanisms and BIHA-gen-reg-4 is the use of standardised mechanisms and this is achieved by utilising well known software, mechanisms and protocols in the BIHA solution, such as CoovaChilli [85], FreeRADIUS [181], CHAP [174], MySQL [184] and WebSocket [173].

6.1.3 Graceful Denial of Service for IP-based Application Services

The verification of the graceful denial of service solution is carried out based on the technical requirements presented in Table 4.13 and the general requirements presented in Table 4.12. The intention of the graceful denial of service solution is to provide an application service quality indication feedback to the user which informs him about the expected application quality in advance of the application service

starts. The GDoS solution is realised as a kind of busy signal known from the traditional telephony service. The GDoS solution does not restrict the application service delivery process itself in the case of non-sufficient available network resources. However, GDoS provides an application quality indication feedback to the user which does not exit and offers the opportunity to the user to decide how to continue with its application service request taking the expected application quality feedback into account. In Figure 6.5 the graphical user interface of an example video portal is presented. The page shown is the start page of the video portal which presents the offered videos to the user. Whenever a user clicks on the 'view' button next to the video image, the GDoS process starts in the backend.

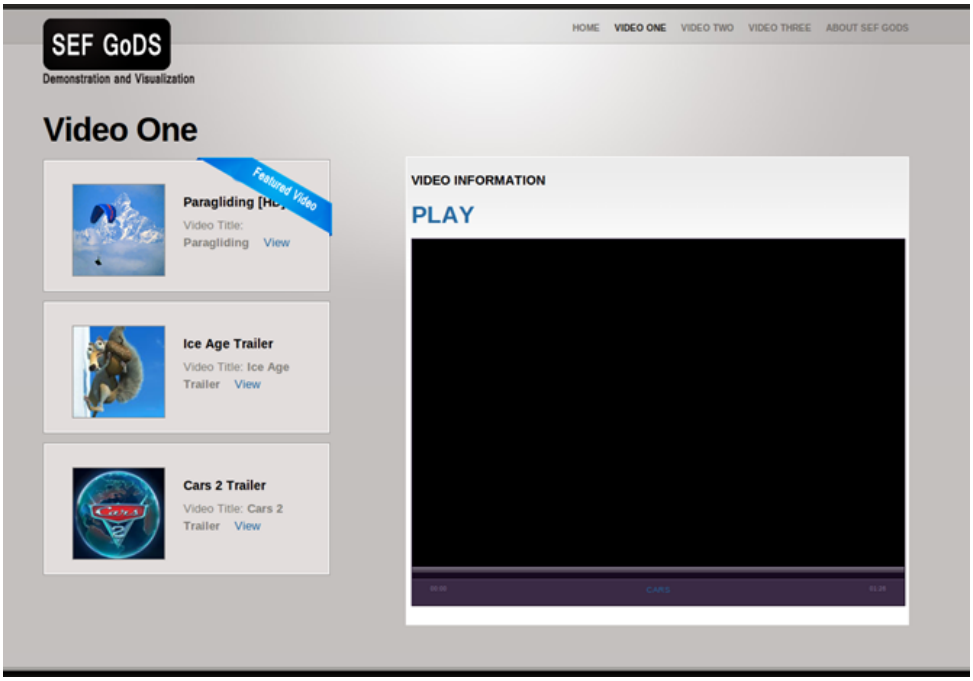


Figure 6.5: Graphical user interface: start page of exemplary video portal.

In Figure 6.6 the graphical user interface of the video portal is shown, in the case that the user has requested a video and the GDoS evaluation process has determined that there are sufficient available network resources to deliver the video. After clicking on the 'view' button, as shown in Figure 6.5, the video starts and the feedback on the service possible is given to the user.

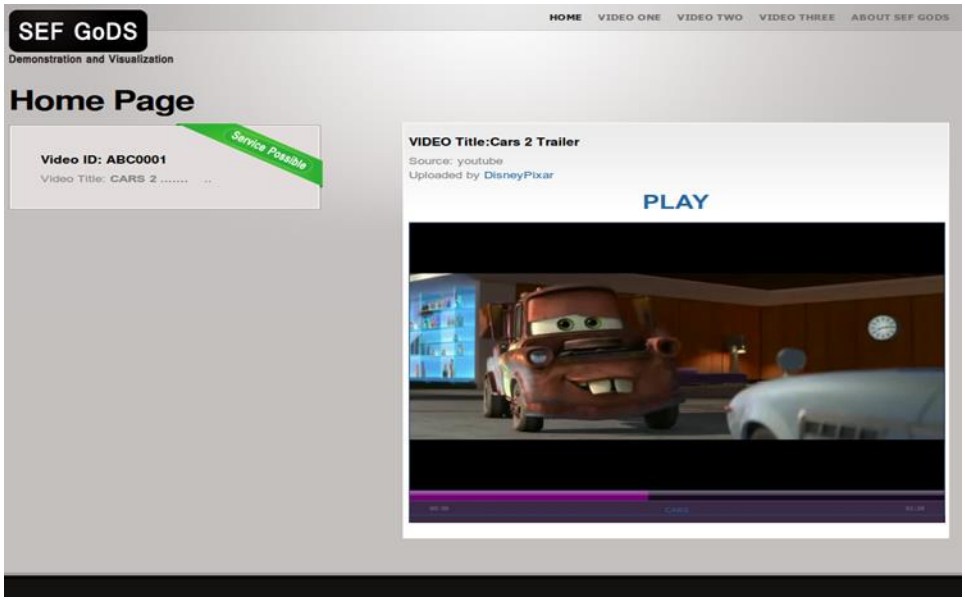


Figure 6.6: Graphical user interface: started video in the case of sufficient available network resources in the network.

In Figure 6.7 the graphical user interface of the video portal is shown, in the case that the user has requested a video and the GDoS evaluation process has determined non-sufficient available network resources to deliver the video content. After clicking on the ‘view’ button, as shown in Figure 6.5, the video does not start and the feedback shows that the service is not possible for the user. As mentioned above, GDoS does not have the intention to restrict application service delivery, and due to this, there are some options provided to the user. The options are ‘play video anyway’, ‘watch in standard quality’, ‘buy additional network resources’ or ‘continue to wait till resources are free’. The option ‘buy additional network resources’ has not been implemented yet. However, mentioning of this option here and in conjunction with the network resource information in the ‘info-box’, Figure 6.7 should illustrate how the GDoS solution can contribute to providing facts about the network capabilities to the user and which might motivate of the user to buy additional network resources. This case is a good example to demonstrate that GDoS is an added value service which provides benefit for the user in terms of providing the application service quality indication and for the network service provider in terms of selling extra or more network resources to the user. The ‘info-box’ presents information about the required bandwidth of the application service, the available and used bandwidth of the content provider access network as well as the available and used bandwidth of the user access network.

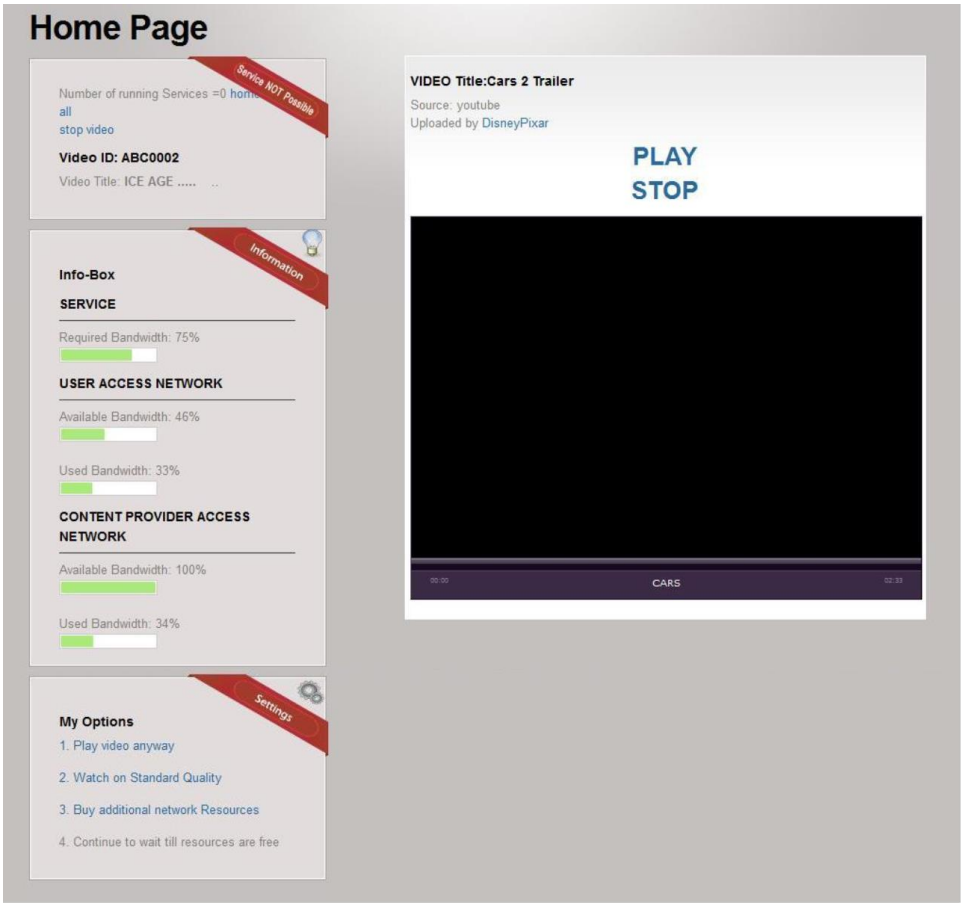


Figure 6.7: Graphical user interface: non-started video in the case of non-sufficient available network resources in the network.

The technical requirement in Table 4.13 on the graceful denial of service solution has been achieved. GDoS-tech-req-1 the graceful denial of service processing entity is realised by means of the business process execution language (BPEL) which is used to orchestrate the GDoS web-services. GDoS-tech-req-2 to provide application service requirements on network performance to the graceful denial of service processing entity and GDoS-tech-req-3 to provide available network capabilities to the graceful denial of service processing entity are each achieved with a web-service. GDoS-tech-req-4 to offer graceful denial of service result to user is realised by means of a web-based feedback as shown in Figure 6.7. The full details outlining the benchmarking result achieved are presented in Subsection 6.2.3.

The general requirements GDoS-gen-req-1 and GDoS-gen-req-2 in Table 4.12 are fulfilled by the GDoS solution. GDoS-gen-req-1 the use of state-of-the-art mechanisms and protocols and GDoS-gen-req-2 the use of standardised mechanisms and protocols is achieved by utilising well known software, mechanisms and protocols in the GDoS solution, such as BPEL, web-services, html and MySQL.

6.2 Benchmarking

In this section the benchmarking of the proposed sequential authentication solution, the barcode initiated hotspot auto-login solution and the graceful denial of service solution of Section 4.1 is performed and the results are analysed.

6.2.1 Sequential Authentication Solution

In the following the benchmarking of the sequential authentication solution is performed. The validation is based on 100 measurements using a LAAA server for the authentication purpose. The measurement is performed as described in Subsection 3.4.2. Figure 6.8 presents the authentication communication between the UE and authenticator as well as the ping communication between the UE and the communication server. The light (yellow) marked rows represent the packets from the RADIUS server forwarded by the authenticator to the UE. Frame number seven presents the first transmitted packet after the handover. Frame number seven, eight, nine and ten represents the PSK 4-way handshake of the WPA2 PSK authentication followed by the start of WPA2 EAP-TLS authentication in frame eleven. With regard to SAS-tech-req-1 to reduce the time of data communication interruptions in WLAN handover processes which are induced by authentication and authorisation methods, the benefit of the sequential authentication solution can be seen in frames number 15 and 16. The first ping request after the handover and WPA2 PSK authentication is sent in frame number 15 and the ping reply is provided in frame number 16. This means, network access is granted while the second authentication phase with WPA2 EAP-TLS is still in progress. However, network access is already granted after 12 ms, calculated from the time delta between frames number 7 and 15. The IEEE 802.1X authentication ends with frame number 41 followed by the PMK 4-way handshake. In frame number 46 the successful WPA2 EAP-TLS authentication is presented. Therefore, Figure 6.8 presents the correct operation of the sequential authentication solution.

The configuration time of the wireless card still exists and takes 293 ms. However, the impact of WPA2 EAP-TLS authentication time on the handover performance has been avoided. In the case of applying the sequential authentication solution the handover process influencing communication interruption time takes 12

ms due to the WPA2 PSK authentication process. As a result, the sequential authentication solution enables real-time service continuity after 12 ms of interruption. Due to the reduced interruption time the SAS solution is able to contribute to service quality improvement in WLAN mobility scenarios. This means freezing effects or artefacts in IPTV sessions can be reduced or fully avoided and enhanced voice quality in VoIP communication can therefore be achieved.

No.	Time	Time Delta	Source	Destination	Protocol	Info
5	0.018	0.008	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
6	0.018	0.000	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply
7	*REF*	*REF*	3com_37:f7:b0	3com_37:f7:af	EAPOL	Key
8	0.005	0.005	3com_37:f7:af	3com_37:f7:b0	EAPOL	Key
9	0.006	0.000	3com_37:f7:b0	3com_37:f7:af	EAPOL	Key
10	0.007	0.001	3com_37:f7:af	3com_37:f7:b0	EAPOL	Key
11	0.008	0.000	3com_37:f7:b0	3com_37:f7:af	EAP	Request, Identity [RFC3748]
12	0.008	0.000	3com_37:f7:af	3com_37:f7:b0	EAP	Response, Identity [RFC3748
13	0.010	0.002	3com_37:f7:b0	3com_37:f7:af	EAP	Request, EAP-TLS [RFC2716]
14	0.011	0.000	3com_37:f7:af	3com_37:f7:b0	TLSv1	Client Hello
15	0.012	0.001	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
16	0.013	0.000	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply
17	0.020	0.007	3com_37:f7:b0	3com_37:f7:af	TLSv1	Server Hello, Certificate,
18	0.024	0.003	3com_37:f7:af	3com_37:f7:b0	EAP	Response, EAP-TLS [RFC2716]
19	0.025	0.000	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
20	0.025	0.000	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply
21	0.029	0.003	3com_37:f7:b0	3com_37:f7:af	TLSv1	Server Hello, Certificate,
22	0.029	0.000	3com_37:f7:af	3com_37:f7:b0	EAP	Response, EAP-TLS [RFC2716]
23	0.034	0.004	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
24	0.034	0.000	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply
25	0.035	0.000	3com_37:f7:b0	3com_37:f7:af	TLSv1	Server Hello, Certificate,
26	0.048	0.013	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
27	0.048	0.000	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply
28	0.055	0.006	3com_37:f7:af	3com_37:f7:b0	TLSv1	Certificate, Client Key Exc
29	0.057	0.001	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
30	0.057	0.000	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply
31	0.059	0.001	3com_37:f7:b0	3com_37:f7:af	EAP	Request, EAP-TLS [RFC2716]
32	0.060	0.000	3com_37:f7:af	3com_37:f7:b0	TLSv1	Certificate, Client Key Exc
33	0.069	0.009	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
34	0.070	0.000	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply
35	0.081	0.011	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
36	0.082	0.000	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply
37	0.089	0.007	3com_37:f7:b0	3com_37:f7:af	TLSv1	Change Cipher Spec, Encrypt
38	0.091	0.002	3com_37:f7:af	3com_37:f7:b0	EAP	Response, EAP-TLS [RFC2716]
39	0.092	0.000	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
40	0.092	0.000	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply
41	0.097	0.004	3com_37:f7:b0	3com_37:f7:af	EAP	Success
42	0.097	0.000	3com_37:f7:b0	3com_37:f7:af	EAPOL	Key
43	0.097	0.000	3com_37:f7:af	3com_37:f7:b0	EAP	Response, EAP-TLS [RFC2716]
44	0.103	0.005	3com_37:f7:af	3com_37:f7:b0	EAPOL	Key
45	0.103	0.000	3com_37:f7:b0	3com_37:f7:af	EAPOL	Key
46	0.105	0.002	3com_37:f7:af	3com_37:f7:b0	EAPOL	Key
47	0.106	0.000	192.168.1.100	192.168.1.200	ICMP	Echo (ping) request
48	0.107	0.001	192.168.1.200	192.168.1.100	ICMP	Echo (ping) reply

Figure 6.8: EAP and ping communication in sequential authentication concept.

Furthermore, the characteristic of the sequential authentication solution avoids the location influence of the remote located AAA servers on the handover performance. Due to the second authentication phase that performs WPA2 EAP-TLS in parallel to the already granted network access after the first WPA2 PSK authentication phase the required EAP-TLS negotiations do no longer affect the communication interruption time. Network access is still granted after the successful first authentication phase and an application service can be provided. As a result, the authentication time of 494 ms, as shown in Figure 3.15, using EAP-TLS in its traditional mode of behaviour does not influence the handover time any longer. The novel authentication method has already granted network access after 12 ms.

6.2.2 Barcode Initiated Hotspot Auto-login

In the following the benchmarking of the barcode initiated hotspot auto-login solution is performed. The measurement results are based on the implemented BIHA solution described in Section 5.2. The measurements performed cover two types of aspects. The first aspect is from a user point of view which focuses on the time needed to get logged into the hotspot. The second aspect is from the system internal communication point of view which focuses on the amount of data transmission introduced by the BIHA solution.

Benchmarking from user point of view:

In the following the benchmark results from the user point of view are presented. The results shown in Table 6.2 are partly quantitative and partly qualitative because of the nature of the measurements which include user interaction that varies from user to user and for different devices.

Characteristics	Laptop	Tablet
Device start up time	60-120 s	30 s
Login time using traditional hotspot login approach	15-20 s	15-20 s
Login time using BIHA solution	35-85 s	35-85 s

Table 6.2: Benchmarking from user point of view: time to get logged into the hotspot.

The device start up time shown in Table 6.2 refers to the time in which user is trying to get connected to the wireless hotspot prior to the hotspot authentication process. It will roughly take 30 s to 120 s to successfully connect to the WLAN hotspot and begin the authentication process, depending on the user device and the WLAN interface which the user is using. In the case the user is trying to connect via a mobile device or tablet pc, it should take around 30 s until the user will turn on the WLAN interface and search for the proper hotspot WLAN and connect to it. If a laptop is used it might take up to 120 s to turn the laptop on and connect to the WLAN hotspot. After successful connection to the hotspot WLAN network, the hotspot portal will be pushed automatically to the user's web browser after they try to access a website through an HTTP request. Depending on the portal design, images and etc. this will take around 1 s to 2 s.

The user has two options to perform the hotspot login process. First, in the case where the user has obtained the hotspot credentials previously they can proceed with

the traditional hotspot login process by entering their username and password and by clicking the connect button. After clicking the connect button it will take less than 1 s until they are logged into the hotspot and gets access to the Internet. The time of entering the user credentials in traditional hotspot login behaviour is presented by 'Login time using traditional hotspot login approach' in Table 6.2 and takes 15 to 20 s, depending on the user behaviour. Second, in case the user does not have any previous credentials they can proceed to the BIHA solution by clicking on the 'Auto Login' button on the hotspot login page. Depending on the user interaction speed, it will take around 15 s to 60 s until they are able to scan the displayed barcode and then send the verification information via SMS. After the user has successfully sent the SMS to the voucher server it takes roughly between 20 s and 25 s until the credentials are created for the user by the BIHA solution and the user has received a reply back from the voucher server. Measurements have shown that this takes from 20 s to 25 s depending on safety timeouts included in the voucher server implementation. Also, it should be noted that a reduction to about 10 s is possible. The time of using the BIHA solution to request user credentials and get logged to the hotspot is presented by 'Login time using BIHA solution' in Table 6.2 and takes 35 s to 85 s depending on the user behaviour. Upon receiving the SMS reply from the voucher server, the user can complete the authentication process by clicking on the 'auto login' button which will trigger the authentication process of the BIHA solution. The authentication process will take less than 1 s until the user is logged into the hotspot and gets access to the Internet.

Table 6.2 presents a time benefit of the traditional hotspot login process when compared to the novel BIHA solution. However, it needs to be kept in mind that the time benefit only exists when the user has the user credentials already available. Moreover, the user credentials have to be entered manually. It can be assumed that the usability of the barcode initiated hotspot auto-login solution when obtaining the user credentials and auto-login is more convenient in comparison to the traditional hotspot voucher behaviour. In the case of non-available user credentials in the traditional hotspot approach, the novel BIHA solution has a time benefit.

Benchmarking from a system internal communication point of view:

The following presents the benchmarking results of the system internal communications including different aspects, such as timing, number of packets and

the size of the packets. The measurements are divided into several parts which correlates to Figure 4.7 presented in Subsection 4.2.3. In the measurements the entities are connected to the network via wireless and wired high speed links. The user device is connected to the Wi-Fi access point via a 54 Mb wireless connection while the hotspot access entity and the hotspot core entity are connected to each other using a 100 Mb Ethernet connection. The measurements focus only on the authentication process and give a comparison between the traditional hotspot authentication method and the new BIHA solution. The hotspot login page loading was disregarded because it is out of the scope of this thesis. Furthermore, it is highly dependent on the hotspot portal graphical design.

The auto-login method of the BIHA solution is a complementary approach to the traditional hotspot authentication method which means that in the case of the auto-login method a series of communications will take place between different entities in the hotspot architecture to retrieve the required user credentials and provide them to the user's web browser. Afterward, the remainder of the authentication process will happen in the same way as in the traditional hotspot login approach. Due to this the measurements are divided into two parts: User credential retrieval via the information channel and traditional hotspot authentication

Table 6.3 and Table 6.4 present the measurement results of the whole authentication processes of the traditional hotspot login and the BIHA solution. Each table shows one of the communication links. In Table 6.3 the communication between the user device and the hotspot controller is presented. Table 6.4 presents the communication between the hotspot controller and hotspot core entity including the AAA Server and the Information Exchange Server. The measurements have been carried out using Wireshark [145]. It should be noted that most of the background processing times and gaps are ignored because the timings are in orders of milliseconds and the transferred packets are only a few kilobytes on high speed links.

	Traditional approach	BIHA
Packet count	12	45
Total packet size [bytes]	2127	8013
Transfer time [ms]	18	123

Table 6.3: Communication between user device and hotspot controller.

	Traditional approach	BIHA
Packet count	4	26
Total packet size [bytes]	740	4903
Transfer time [ms]	6	70

Table 6.4: Communication between hotspot controller and hotspot core entity.

As shown in Table 6.3 and Table 6.4, the BIHA solution adds some traffic to the hotspot login communication. Around 6 kB of data and around 100 ms of delay are added to the communication between the user device and the hotspot as presented in Table 6.3, and around 4 kB of data and around 60 ms of delay are added to the communication between the hotspot controller and the hotspot core entity as shown in Table 6.4. The added amount of data is negligible on a wireless or wired link which is able to transfer several MB per second. Moreover, the added delay does not influence the experience of the user when using the BIHA solution, because the delay is too small to be noticeable.

6.2.3 Graceful Denial of Service for IP-based Application Services

In the following the benchmarking of the graceful denial of service solution is performed. The measurement results are based on the implemented GDoS solution as described in Section 5.3. Beside the functional tests already presented, performance and scalability investigations of the over-all system have been carried out. The performance analysis of the GDoS run time has been carried out to determine how long a user has to wait for the GDoS feedback. Moreover, the bandwidth consumption of interface 1, 2, 3 and 4, shown in Figure 4.14, has been analysed.
The measurements have been performed 50 times for a 1, 2, 5, 10, 50, 100, 150, 200, 250 and 300 users which are simultaneously requesting the application service at the same time. The interval of simultaneous requests is 10 s. To create simultaneous users, the tool siege [186] has been used. Siege is an http load testing and benchmarking utility. It is designed to let a web developer measure their code under stress and to test how it will behave under the load on the Internet. Figure 6.9 presents the overall GDoS run time which starts at interface 1.1, shown in Figure 4.14 (and SEF INITIATION REQUEST (step 2) in Figure 4.15), until the GDoS result is provided at interface 1.2, shown in Figure 4.14 (and SEF INITIATION REPLY (step 15) in Figure 4.15). The measurement results of the communications

between the BPEL process and the web-services, such as interface 2.1 / 2.2, interface 3.1 / 3.2 and interface 4.1 / 4.2 are presented in Appendix A.7.

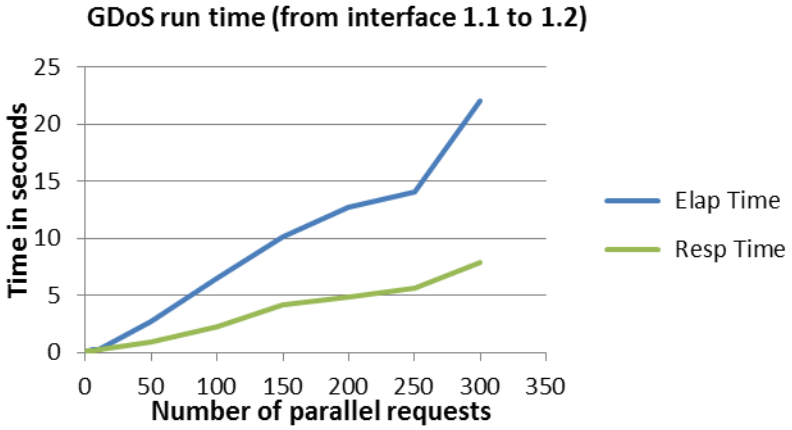


Figure 6.9: GDoS run time - measured form SEF INITIATION REQUEST (step 2) to SEF INITIATION REPLY (step 15).

The elapsed time in Figure 6.9 is the duration of the entire siege test and is measured from the time that siege invokes a user until the last simulated user completes his transactions. The response time is the average time it took to respond to each simulated user's requests. The elapsed time depends on the response time and is the longest time it took a request to respond. The measurements have been carried out under the condition that the SPF and CPFs have already obtained the parameters needed and no processing time is required to obtain this information. As shown in Figure 6.9 the response time of the overall system gradually increases with the number of users. The requests of 300 parallel users result in a GDoS run time of 8 s. With regard to the requested application service, e.g. a video service which has a duration of several minutes, it is assumed that a user is willing to wait 8 s because the GDoS feedback indicates whether the requested application service is deliverable or not.

For the purpose of evaluating the scalability the bandwidth consumption of interface 1, 2, 3 and 4, shown in Figure 4.14 has been investigated. The tool Wireshark [145] has been used to capture the packets sent to the web-services of each network segment. The measurement results presented in Table 6.5 show the bandwidth demand on the interfaces in relation to the interfaces as shown in Figure 4.14. The results present the reassembled TCP packet size of each interface.

Interface	Measurement point	TCP packet size [bytes]
1.1	SEF-GDoS-InfSP – SEF-GDoS (Request)	856
1.2	SEF-GDoS-InfSP – SEF-GDoS (Response)	725
2.1	SEF-GDoS – SEF-GDoS-InfSP (Request)	956
2.2	SEF-GDoS – SEF-GDoS-InfSP (Response)	875
3.1	SEF-GDoS – SEF-GDoS-ENSP1 (Request)	1007
3.2	SEF-GDoS – SEF-GDoS-ENSP1 (Response)	878
4.1	SEF-GDoS – SEF-GDoS-ENSP2 (Request)	827
4.2	SEF-GDoS – SEF-GDoS-ENSP2 (Response)	722

Table 6.5: Bandwidth demand of GDoS interfaces.

Based on the results of Table 6.5 it can be stated that 1000 requests require less than 1 MB transmission volume. This does not have a significant effect on the network performance of the inter-connected links among the involved actors.

6.3 Summary

The results of the verification and benchmarking of the sequential authentication solution implementation presented in Section 4.1, the barcode initiated hotspot auto-login solution developed in Section 4.2 and the graceful denial of service solution introduced in Section 4.3 were presented. The results of this chapter were analysed according to the use cases and network capabilities as presented in Figure 4.1. The use case service quality focuses on WLAN VoIP communication when users are on the move. Section 3.8.3 presents drawbacks in the authentication and authorisation method in the current WLAN handover processes. These drawbacks relate to the network performance. The validation of the sequential authentication solution performance, in Subsection 6.1.1 and 6.2.1, has shown that in a real network environment a reduction of 97.5 % of data communication interruption can be achieved compared to the traditional WPA2 EAP-TLS behaviour. The novel sequential authentication method granted network access already after 12 ms. This is beneficial for real-time services, such as VoIP services in the case of users that are on the move in WLAN covered areas. A major contributor to data interruption in a handover process is the WPA2 EAP-TLS influence on the handover performance. As a result, the proposed sequential authentication solution based on WPA2 PSK and WPA2 EAP-TLS decreases the influence of authentication time in a handover process. Thus, the impact of IEEE 802.1X EAP-TLS process is overcome by the sequential authentication solution. As a result, the network performance can be improved by the novel sequential authentication solution presented in this work.

The use case usability addresses the WLAN hotspot registration process, the obtaining of user credentials and the login process. Section 3.8.3 presents drawbacks in the behaviour to obtain Internet access via public WLAN-based hotspots. This type of drawback relates to the network access capability. The validation of the barcode initiated hotspot auto-login solution performance, in Subsection 6.1.2 and 6.2.2, has shown that hotspot user credentials can be requested on demand, and based on the requested user credentials, an automated hotspot login can be performed without the need to enter a user name and password. Moreover, the payment of the hotspot fees can be carried out using a premium SMS service eliminating the need to hand over banking information to another party. The added amount of 10 kB data traffic does not influence the performance of the hotspot network architecture. The proposed barcode initiated hotspot auto-login solution is able to improve the user experience of hotspots. Therefore, the network access capability can be improved by the barcode initiated hotspot auto-login solution.

The use case quality awareness focuses on application service delivery and the quality received by the user. Section 3.8.3 presents drawbacks of current IP-based application service delivery and the fact that the user is not aware of the quality to be delivered. This type of drawback relates to the network features capability. The validation of the graceful denial of service solution performance, presented in Subsection 6.1.3 and 6.2.3, has shown that service quality indication feedback can be realised which informs the user about the application service quality to be expected in advance of service delivery. The time needed to gather the necessary application requirements concerning the network performance from the information service provider and the available bandwidth network information from the network service provider as well as to derive the GDoS feedback takes around 8 s. It is assumed that the quality of experience in application service provisioning can be improved by the graceful denial of service solution, even if the user has to wait 8 s, because the GDoS feedback indicates whether the requested application service is deliverable in the user requested quality or not. In this case, the network features capability can be improved by the graceful denial of service solution.

7 Conclusions

This chapter presents the specific and general conclusions of the novel sequential authentication solution proposed in Section 4.1, the innovative barcode initiated hotspot auto-login solution introduced in Section 4.2 and the new graceful denial of service solution of Section 4.3. After that ideas are presented on how this body of work might be extended further.

7.1 Specific Conclusions

Next the specific conclusions are presented. Drawbacks of existing solutions in the area of this work are recapped and it is shown how the new methods presented in this work are able to overcome these drawbacks. The novel solutions are described in summary while the results achieved are highlighted.

7.1.1 Sequential Authentication Solution

The novel sequential authentication solutions presented in this work overcomes the drawback of a long authentication time in the handover procedure required by a generic IEEE 802.1X process using the EAP-TLS method to carry out network access control. The authentication time arises from several handshakes among the wireless station, the authenticator within the point of attachment, and the authentication server to provide certificate-based mutual authentication of the wireless station and the authentication server. As long as the IEEE 802.1X process has not been completed successfully the payload cannot be transmitted and thus, the data communication will be interrupted. The developed sequential authentication solution combines the benefit of fast authentication of Wi-Fi Protected Access 2 (WPA2) with a pre-shared key and the mutual authentication used in WPA2 EAP-TLS. From the reduction of the authentication time point of view the novel sequential authentication solution, combining WPA2 PSK and WPA2 EAP-TLS, has the capability to decrease the communication interruption time of a handover process. An interruption time of 12 ms has been achieved using the presented method instead of 494 ms required by the traditional approach. As a result, a reduction of the

interruption time by 97 % in comparison to the traditional WPA2 EAP-TLS authentication is reached. This reduces the effects on real-time communications significantly and leads to reduced freezing effects, artefacts or interruptions in many multimedia sessions, including IPTV or VoIP. Even if, in the first authentication phase of this novel concept no mutual authentication of the user device and the AAA server is performed, from today's point of view the presented sequential authentication solution provides a high level of network access control and communication security. The transmitted data is encrypted throughout the handover process even during the first authentication phase due to the utilised WPA2 PSK method. The novel solution requires no redesign of the WPA2 PSK and WPA2 EAP-TLS mechanisms. Only a reimplementation combining both mechanisms is required. Thus, the sequential authentication solution is easily deployed in existing network architectures using simple software updates of the supplicant and authenticator. Furthermore, it has been shown that the network performance capability can be improved by this novel sequential authentication solution.

7.1.2 Barcode Initiated Hotspot Auto-login

Today's hotspot solutions have the drawbacks that customers must plan their hotspot use in advance. This means no spontaneous hotspot use is possible. Besides the point of time, the duration the hotspot might be used has to be scheduled in advance. Additionally, in many cases users have to leave their current location to obtain the hotspot login information from the hotspot service personal or have to register on an online portal. The novel barcode initiated hotspot auto-login (BIHA) solution proposed in this work enables users to request hotspot user credentials on demand and it performs an automated hotspot login without the need to enter a user name and password. The payment of the hotspot fees can be carried out through a SMS premium service. This combination of a flexible login functionality in conjunction with a premium SMS solution enables flexible pricing of the hotspot use. As a result, a hotspot operator is able to design an individual pricing structure. Therefore, the proposed barcode initiated hotspot auto-login solution is able to improve the user experience of hotspots and as a result, the network access capability can be significantly improved by the barcode initiated hotspot auto-login solution. Furthermore, by using a SMS premium solution to carry out the hotspot payment, the

hotspot operator does not get any information about the user, such as e.g. the credit card number or the real user name. All user related information, such as a user's name and bank account information are only known to the mobile network operator of the user's mobile phone. This ensures confidentiality of the user's personal data while at the same time conforming to existing laws which require that law enforcement agencies are able to obtain user data.

7.1.3 Graceful Denial of Service for IP-based Application Services

Users demand for high quality services in IP-based applications and application services are constantly increasing. Whether it is online gaming or high definition video streaming there is a need to ensure the quality of these application services to obtain a reliable revenue stream. In today's service provisioning scenarios a user is not aware of the application service quality to be expected prior to starting an IP-based service. The novel GDoS solution is able to overcome this drawback and allow a forecast of the service quality before the service starts. As a result, the user gets feedback about the anticipated service quality in advance of using a service. This means the user is able to decide, whether or not to start the service or wait until more network resources are available. Due to the feedback provided the GDoS solution enhances the QoE of a user significantly. The implementation presented in this thesis shows that the GDoS solution can be realised by means of distributed web services. Therefore, the network features capability can be improved by the graceful denial of service solution.

7.2 General Conclusions

In this section the specific results presented in this work are taken and are put into context for the wider community. In particular beneficial side effects of the proposed solutions are highlighted. Moreover, other possible uses which were not the focus of this work are proposed.

7.2.1 Sequential Authentication Solution

The location of an authentication and authorisation entity in the network architecture influences the authentication and authorisation time of a client. The sequential authentication solution overcomes the demand of positioning of hierarchical

distributed authentication and authorisation entities in the best possible way within network architectures. Due to the reduced authentication time in a handover process there is no longer the need to locate the authentication and authorisation entity as close as possible to the client. As a result, the authentication and authorisation entity can be located centralised in a network architecture without influencing the authentication and authorisation time. This reduces the deployment and operational cost for network operators. Moreover, the centralised storage of AAA data is beneficial for the management of the AAA data as these data sets can economically be kept consistent and up-to-date.

The IEEE 802.1X standard envisions EAP as the authentication protocol. The sequential authentication solution is designed and implemented to use this IEEE 802.1X authentication method. As a result, the sequential authentication solution is not limited to the EAP-TLS method, but can furthermore be used with any EAP method to control network access. The sequential authentication mechanism is of a generic nature and is not specific to IEEE 802.11 networks. Furthermore, the novel mechanisms presented are not limited to devices with a single active interface as the mechanism is fully scalable for devices with multiple active interfaces.

7.2.2 Barcode Initiated Hotspot Auto-login

The barcode initiated hotspot auto-login solution is not limited to network operators which deploy a significant number of hotspots. It is also possible to integrate the presented BIHA solution in standalone hotspot architectures, e.g. in hotels, restaurants or campsites, that are not integrated in a network operators hotspot architecture. The user-friendly method to obtain hotspot user credentials by means of a digital voucher present in this thesis can stimulate users to avail of hotspots more often in comparison to the traditional hotspot login behaviour, while at the same time reducing costs to issue login credentials.

7.2.3 Graceful Denial of Service for IP-based Application Services

The graceful denial of service solution proposed in this thesis is beneficial for a number of reasons and is not limited to the presented video delivery scenario. The solution can be applied in all application service delivery scenarios where the available network resources are limited. The GDoS solution can be used to enable

absolute quality guarantees in end-to-end IP-based service provisioning, e.g. in IP mass market networks by avoiding network resource overbooking. For example, in a multi-person household which is connected to the Internet via VDSL, GDoS is able to inform each member in the household about the available as well as the remaining access line resources. This GDoS information can then be used by the persons in the household to avoid overbooking the access line resources. Thus, GDoS is able to support the prevention of demand induced overload of network capacities for services which are requested at the same period of time. As a result, mutual quality interference of services will be prevented which can occur when users share one Internet gateway while requesting several services at the same time. In addition, the GDoS can be applied in networks which support different types of traffic classes, e.g. gold, silver and bronze, where the gold class represents quality traffic while the bronze class corresponds to best effort traffic. In this case the GDoS can be used to indicate whether enough gold class resources are available for a requested application service which is intended to be transmitted in gold class quality.

The drawback of the current situation where the user has no information about the application quality to be delivered is overcome by the GDoS solution. Such a GDoS solution will contribute to enhance the user satisfaction with their network provider. In this context GDoS is useful for network service providers to improve the QoE for IP-based services. Moreover, network service providers are able to offer GDoS to information service providers and content providers to enhance the QoE of their customers. In this regard, the GDoS solution can be seen as a unique selling point for a network operator. For example, when an edge network service provider connects customers of a content provider, the GDoS solution can be of value to the content provider. The benefit to the content provider customer is to be informed about the expected application quality to be delivered. The benefit to the content provider is the awareness by the customer that the delivered service quality is not reduced due to limited capabilities of the content provider service platform, e.g. overloaded application servers.

7.3 Future Work

The sequential authentication solution has focused on an improved authentication and authorisations time in a WLAN handover process. However, there is an impact

of the WLAN supplicant implementation on the WLAN card re-configuration time in the handover process which influences the handover performance as was shown in Subsection 3.4.6. The configuration time of the wireless card was shown to take 293 ms. To improve handover performance even further it would be necessary to improve the WPA supplicant implementation in terms of the re-configuration time of the WLAN card.

The proof of concept implementations of the barcode initiated hotspot auto-login and graceful denial of service solution have provided good results in laboratory tests. An improvement of the quality of experience of the users in each of the area of work can therefore be expected. To investigate the user acceptance of the barcode initiated hotspot auto-login solution, a field trial in a real hotspot environment must be carried out. Such a field test could also be used to verify the scalability of the BIHA solution in real life situations.

A field test of the graceful denial of service solution in a real content delivery platform should also be carried out. Such a field test could also be used to verify the scalability of the GDoS solution in a real life environment, besides investigation of the user acceptance of the GDoS solution. Furthermore, investigations into how such an added value service can be applied in a software defined network [187] and network function virtualisation supported architectures [188] are worthy of further study.

The previous three suggestions for further expansion of this work were a direct continuation of the existing research. However, there are also other directions that could be taken to expand this body of work into new areas. For example, even so Chapter 7.1.1 has shown that the handover time of several hundred ms could be reduced to approximately 15 ms, there is still a card configuration delay of about 100 ms. This delay is caused by the software driver and the wireless card. Here it should be possible to significantly reduce this configuration delay by implementing the driver directly into an application specific integrated circuit or a field programmable gate array.

Another possible avenue for further research could be the investigation of the quality of experience from a user’s perspective. Here qualitative research methods might be used to look at the human decisions that lead to the use of a certain

provider, hotspot or service. Furthermore, it might be investigated how these human decisions change if the technology is varied.

References

[1] Ericsson, “Ericsson White Paper - Differentiated Mobile Broadband – enhance user experience and drive revenue growth,” January 2011. [Online]. Available: http://www.ateshow.com/agile_assets/311/Differentiated_Mobile_Broadband_%E2%80%93_enhance_user_experience_and_drive_revenue_growth.pdf. Accessed on: Jan. 26, 2015.

[2] Ericsson, “Ericsson White Paper – Policy and Charging,” May 2013. [Online]. Available: http://www.ericsson.com/res/docs/whitepapers/wp-personalized-charging-and-policy-control.pdf. Accessed on: Jan. 26, 2015.

[3] R. Gupta and S. Parida, “Challenges and Opportunities: Mobile Broadband,” in Proc. *International Journal of Future Computer and Communication*, Vol. 2, No. 6, Dec. 2013, pp. 660 - 664.

[4] Netcraft “December 2011 Web Server Survey” [Online]. Available: http://news.netcraft.com/archives/2011/12/09/december-2011-web-server-survey.html#more-5158. Accessed on: Jan. 26, 2015.

[5] Pingdom, “Internet 2010 in numbers” [Online]. Available: http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/. Accessed on: Jan. 26, 2015.

[6] *Internet Protocol*, IETF RFC 791, September 1981.

[7] Alon Cohen and Lior Haramaty, “Audio Transceiver,” United States Patent, *Patent Number US5825771*, Oct. 1994.

[8] Alliance for Telecommunications Industry Solutions (ATIS), “ATIS IPTV Exploratory Group Report and Recommendation to the TOPS Council,” July 2005. [Online]. Available: http://www.atis.org/tops/IEG/ATIS_IPTV_EG_RPT_final.pdf. Accessed on: Jan. 26, 2015.

[9] ITU IPTV Focus Group (FG IPTV). [Online]. Available: http://www.itu.int/en/ITU-T/focusgroups/iptv/Pages/default.aspx. Accessed on: Jan. 26, 2015.

[10] M. Amberg, M. Hirschmeier and J. Wehrmann, “The Compass Acceptance Model for the analysis and evaluation of mobile services”, in *Proc. International Journal of Mobile Communications*, Vol. 2, No. 3, 2004, pp.248–259.

[11] C.-C. Wang, Y. Hsu and W. Fang, "Acceptance of technology with network externalities: an empirical study of internet instant messaging services." in *Proc. Journal of Information Technology Theory and Application (JITTA)*, Vol. 6, No. 4, 2005, pp. 15 - 28.

[12] D. Collins, “Carrier grade voice over IP, second edtion,” published by McGraw-Hill Professional, September 2002.

[13] 3GPP, “LTE,” [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/98-lte. Accessed on: Jan. 26, 2015.

[14] *IEEE Standard for Local and Metropolitan Area Networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 5: Enhancements for Higher Throughput*, IEEE 802.11n-2009, October 2009.

[15] WiMAX Forum. [Online]. Available: http://www.wimaxforum.org/. Accessed on: Jan. 26, 2015.

[16] *IEEE Standard for local and metropolitan area networks; Part 16: Air Interface for Broadband Wireless Access Systems*, IEEE Std. 802.16-2009, May 2009.

[17] ICT project of the European Union 7th framework, “CARrier grade MEsh Networks (CARMEN)”. [Online]. ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/future-networks/projects-carmen-factsheet_en.pdf. Accessed on: Jan. 26, 2015.

[18] I. F. Akyildiz and X. Wang, "A Survey on Wireless Mesh Networks," *IEEE Communications Magazine*, vol. 43, no. 9, pp. 23-30, September 2005.

[19] Deutsche Telekom AG, “Informationen zu LTE”. [Online]. Available: http://www.telekom.de/netzqualitaet?ActiveTabID=verfuegbarkeit&wt_mc=alias_9998_lte. Accessed on: Jan. 26, 2015.

[20] Vodafone, “LTE”. [Online]. Available: http://www.vodafone.de/lte/. Accessed on: Jan. 26, 2015.

[21] Project of Federal Ministry of Education and Research, “Enabler of Ambient Services and Systems Part C – Wide area Coverage (EASY-C)” [Online]. Available: http://www.easy-c.de. Accessed on: Jan. 26, 2015.

[22] Project of Federal Ministry of Education and Research, “ScaleNet: Scalable, efficient and flexible next generation converged mobile, wireless and fixed access networks” [Online]. Available: http://www.pt-it.pt-dlr.de/de/1038.php. Accessed on: Jan. 26, 2015.

[23] A. Roos, A. Th. Schwarzbacher, S. Wieland, "Broadband Wireless Internet Access in Public Transportation," in Proc. *VDE Kongress - Innovations in Europe*, Aachen, Germany, Vol. 1, Oct. 2006. pp. 65-70.

[24] T. Nakata, Y. Noguchi, Y. Suda, K. Okanoue, and S. Yamazaki, “BBRide - Broadband Internet Access Onboard Rapid Transportation”, in Proc. *7th International Symposium on WPMC 2004*, Abano Terme, Italy, Sep. 2004, pp. 92 - 96.

[25] Cisco WhitePaper, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010–2015”. [Online]. Available: http://tmfassociates.com/blog/wp-content/uploads/2013/02/Cisco-mobile-VNI-Feb-2011.pdf. Accessed on: Jan. 26, 2015.

[26] Cisco WhitePaper, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018”. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html. Accessed on: Jan. 26, 2015.

[27] Deutsche Telekom AG, “Hotspot der Telekom”. [Online] Available: http://www.t-mobile.de/hotspot. Accessed on: Jan. 26, 2015.

[28] Kabel Deutschland, “Kabel Deutschland Hotspots”. [Online]. Available: https://www.hotspot.kabeldeutschland.de/. Accessed on: Jan. 26, 2015.

[29] J. Bicket, S. Biswas, D. Aguayo, and R. Morris, “Architecture and Evaluation of the MIT Roofnet Mesh Network (DRAFT),”. [Online] Available: http://pdos.csail.mit.edu/~rtm/roofnet-b.pdf . Accessed on: Jan. 28, 2015.

[30] Förderverein Freie Netzwerke e.V., “Freifunk.net” [Online] Available: http://freifunk.net/. Accessed on: Jan. 28, 2015.

[31] N. Bayer, A. Roos, R. Karrer, B. Xu, and C. Esteve, "Towards Carrier Grade Wireless Mesh Networks for Broadband Access," in Proc. First *IEEE International Workshop On Operator-Assisted (Wireless Mesh) Community Networks 2006 (OPCOMM '06)*, Berlin, Germany, Sep. 2006, pp. 1- 10.

[32] *Integrated Services Digital Network (ISDN), General Structure*, ITU-T Recommendation I.120, March 1993.

[33] R. Schatz, T. Hoßfeld, L. Janowski, and S. Egger, "From packets to people: quality of experience as a new measurement challenge," in *Data traffic monitoring and analysis*, Springer Berlin Heidelberg, 2013, pp. 219-263.

[34] R. Schatz, and S. Egger, "Vienna Surfing – Assessing Mobile Broadband Quality in the Field," in Proc. *ACM SIGCOMM Workshop on Measurements Up the STack (W-MUST)*, Toronto, Canada, 19 August 2011, pp. 19 - 24.

[35] L. T. Nguyen, R. Harris and J. Jusak, "A Pilot Study to Assess Quality of Experience Based on Varying Network Parameters and User Behaviour," International Proceedings of *Computer Sciences and Information Technology*, vol.5, 2011, pp. 30 -34.

[36] R. Schatz, S. Egger and A. Platzer, "Poor, Good Enough or Even Better? Bridging the Gap between Acceptability and QoE of Mobile Broadband Data Services," in Proc. *IEEE International Conference on Communications (ICC)*, Kyoto, Japan, 5-9 June 2011, pp. 1 – 6.

[37] J. A. Hassan, S. K. Das, M. Hassan, C. Bisdikian, D. Soldani, "Improving quality of experience for network services," *IEEE Network: The Magazine of Global Internetworking - Special issue on improving quality of experience for network services*, vol. 24, no. 2, pp. 4 – 6, March/April 2010.

[38] IEEE Communications Society, "Special issue on quality of experience issues in media delivery," *IEEE COMSOC Multimedia Communication Technical Committee E-Letter*, vol. 6, no. 8, August 2011.

[39] *Performance, QoS and QoE*, ITU-T Study Group 12. [Online]. Available: http://www.itu.int/ITU-T/studygroups/com12/index.asp. Accessed on: Jan. 28, 2015.

[40] Organisation for economic co-operation and development (OECD), "Convergence and Next Generation Networks – Ministrial Background

Report DSTI/ICCP/CISP(2007)2/FINAL," OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17-18 June 2008.

[41] *Next Generation Networks – Frameworks and functional architecture models, General overview of NGN*, ITU-T Recommendation Y.2001, December 2004.

[42] *Next Generation Networks – Frameworks and functional architecture models, General principles and general reference model for Next Generation Networks*, ITU-T Recommendation Y.2011, December 2004.

[43] G. Camarillo, M.-A. Garcia-Martin, "The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds," published by John Wiley & Sons, December 2005.

[44] M. Poikselkä, "The IMS: IP multimedia concepts and services in the mobile domain," published by John Wiley & Sons, January 2009.

[45] J. I. Agbinya, "IP Communication and Services for NGN," published by CRC Press, December 2009.

[46] Ericsson White Paper, "IMS – IP Multimedia Subsystem; The value of using the IMS architecture," October 2004. [Online]. Available: http://www.citmo.net/library/Ericsson%20IMS.pdf. Accessed on: Jan. 26, 2015.

[47] J. Li Salina and P. Salina, "Next Generation Networks Perspectives and Potentials," published by John Wiley & Sons, January 2008.

[48] A. Cuevas, J. Moreno, P Vidales, and H Einsiedler, "The IMS Service Platform: A Solution for Next Generation Network Operators to be More than Bit Pipes", *IEEE Communication Magazine*, vol. 44, no. 8, pp. 75–81, August 2006.

[49] S. Horvath, "Aktueller Begriff – Mobiles Internet," scientific services of Federal Parliament of Germany. [Online]. Available: http://www.bundestag.de/dokumente/analysen/2010/mobiles_internet.pdf. Accessed on: Dez. 30, 2012.

[50] Gartner Press Releases, "Gartner Says Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 Percent Year-on-Year; Smartphone Sales Grew 74 Percent" August 2011. [Online]. Available: http://www.gartner.com/it/page.jsp?id=1764714. Accessed on: Jan. 26, 2015.

[51] Skype. [Online]. Available: http://www.skype.com. Accessed on: Jan. 26, 2015.

[52] Apple iPhone. [Online]. Available: http://www.apple.com/iphone/. Accessed on: Jan. 26, 2015.

[53] Google Hangouts. [Online]. Available: http://www.google.com/tools/dlpage/res/talkvideo/hangouts/. Accessed on: Jan. 26, 2015.

[54] M. Schel, "Konvergenz der Zugangsnetz," In *WissenHeute*, October 2007.

[55] H. Velayos, G. Karlsson, "Techniques to Reduce IEEE 802.11b MAC Layer Handover Time," Telecommunication Systems Laboratory, Department of Microelectronics and Information Technology (IMIT), KTH, Royal Institute of Technology, Stockholm, Sweden, April 2003.

[56] A. Mishra, M. Shin and W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," in *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 2, ACM, 2003, pp. 93 – 102.

[57] J.-O. Vatn, "An experimental study of IEEE 802.11b handover performance and its effect on voice traffic", Telecommunication Systems Laboratory, Department of Microelectronics and Information Technology (IMIT), KTH, Royal Institute of Technology, Stockholm, Sweden, July 2003.

[58] *IEEE Standard for Local and Metropolitan Area Networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11, July 1999.

[59] *IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control*, IEEE Standard 802.1X, Stand 2001.

[60] *Extensible Authentication Protocol (EAP)*, IETF RFC 3748, June 2004.

[61] *PPP EAP TLS Authentication Protocol*, IETF RFC 2716, October 1999.

[62] I. Martinovic, F. A. Zdarsky, A. Bachorek and J. B. Schmitt, "Measurement and Analysis of Handover Latencies in IEEE 802.11i Secured Networks", In Proc. of *European Wireless 2007*, Paris, France, April 2007.

[63] *G.114 – one-way transmission time*, ITU-T Recommendation, 2003.

[64] A. Roos, S. Wieland, A. Th. Schwarzbacher, "Investigation of security mechanisms and mobility influence on VoIP Quality – Towards VoIP Quality Improvements," In Proc. of *Science Days 2008* – HfTL, Leipzig, Germany, Nov .2008.

[65] *Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codec*, ITU-T Recommendation P 862, 2001.

[66] N. Bayer, D. Hock, A. Roos, M. Siebert, B. Xu, V. Rakocevic and J. Habermann, "VoIP performance in „MeshBed" – a Wireless Mesh Network Testbed," in Proc. of *Vehicular Technology Conference (VTC) Spring 2008*, May 2008, pp. 2218 - 2222.

[67] D. Niculescu, S. Ganguly, K. Kim and R. Izmailov, "Performance of voip in a 802.11 wireless mesh network, " in *Proc. 25th IEEE International Conference on Computer Communications (INFOCOM) 2006*, Barcelona, Catalunya, Spain, April 2006, pp. 1 - 11.

[68] TELCAT MULTICOM, „Hotel WLAN". [Online]. Available: http://www.telcat.de/Hotel-WLAN.649.0.html. Accessed on: Jan. 26, 2015.

[69] YouTube. [Online]. Available: http://www.youtube.com. Accessed on: Jan. 26, 2015.

[70] M. Kaul, R. Khosla and Y. Mitsukura, "Intelligent Packet Shaper to Avoid Network Congestion for Improved Streaming Video Quality at Clients," *Computational Intelligence in Robotics and Automation*, Kobe, Japan, 16 - 20 July, 2003. In Proc. 2003 IEEE International Symposium on (vol. 2), 988 - 993 vol.2.

[71] X. Lu, R. O. Morando and M. E. Zarki, "Understanding Video Quality and its use in Feedback Control," in Proc. *Packet Video Workshop 2002*, Pittsburgh, PA, USA 2002.

[72] Cisco - IPTV Solutions for Wireline Carriers, "White Paper - Delivering Video Quality in Your IPTV Deployment". [Online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns610/net_implementation_white_paper0900aecd8057f290.pdf. Accessed on: Jan. 26, 2015.

[73] P.-J. Huang, Y.-C. Tseng, and K.-C, "A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks," in Proc. *IEEE Vehicular Technology Conference 2006-Spring (VTC2006-Spring)*, vol. 2, 2006, pp. 966–970.

[74] *IEEE Standard for Local and Metropolitan Area Networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)*

Specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Standard 802.11i, July 2004.

[75] *Counter with CBC-MAC (CCM)*, IETF RFC 3610, September 2003.

[76] Federal Office for Information Security (BSI) of Germany: M 2.384 Auswahl geeigneter Kryptoverfahren für WLAN. [Online]. Available: https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/m/m02/m02384.html. Accessed on: Apr. 14, 2010.

[77] M. Kassab, A. Belghith, J.-M. Bonnin and S. Sassi, "Fast Pre-Authentication Based on Proactive Key Distribution for 802.11 Infrastructure Networks," in Proc. of the *1st ACM Wireless Multimedia Networking and Performance Modeling (WMuNeP)*, Montreal, Quebec, Canada, October 13, 2005, pp. 46 – 53.

[78] A. Dutta, D. Famolari, S. Das, Y. Ohba, V. Fajardo, K. Taniuchi, R. Lopez, H. Schulzrinne, "Media-independent pre-authentication supporting secure interdomain handover optimizsation," *IEEE Wireless Communications*, vol. 15, no. 2, pp. 55 - 64, April, 2008.

[79] *Recommended Practice for Multi-Vendor of Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation*, IEEE 802.11f-2003, 2003.

[80] *Remote Authentication Dial In User Service (RADIUS)*, IETF RFC 2865, June 2000.

[81] Cisco Wireless Control System. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-control-system/product_data_sheet0900aecd802570d0.pdf. Accessed on: Jan. 26, 2015.

[82] Mikrotik RouterOS. [Online]. Available: http://www.mikrotik.com/pdf/what_is_routeros.pdf. Accessed on: Jan. 26, 2015.

[83] XCONY: World WLAN. [Online]. Available: http://worldwlan.com. Accessed on: Jan. 26, 2015.

[84] Chillispot. [Online]. Available: http://www.chillispot.info. Accessed on: Jan. 26, 2015.

[85] Coova: CoovaChilli. [Online]. Available: http://www.coova.org/CoovaChilli. Accessed on: Jan. 26, 2015.

[86] *Media and Content Distribution - MCD Framework; Part 9: Content Delivery Infrastructures*, Draft ETSI TR 102 688-9 V0.5.2, December 2010. [Online]. Available: http://docbox.etsi.org/zArchive/MCD/Open/Latest_Drafts/tr_10268809v000502p.pdf. Accessed on: Jan. 26, 2015.

[87] Akamai Technologies. [Online]. Available: http://www.akamai.de. Accessed on: Jan. 26, 2015.

[88] Edgecast. [Online]. Available: http://www.edgecast.com. Accessed on: Jan. 26, 2015.

[89] C. Kobel, W. B. Carcia, J. Habermann, N. Bayer and D. Sivchenko, "Dynamic channel bundling in 802.11a based media-transport mesh networks," in Proc. *IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, USA, 8 - 11 January, 2011, pp. 979 – 980.

[90] VideoLan Organisation – VLC media player [Online]. Available: http://www.videolan.org/vlc/. Accessed on: Jan. 26, 2015.

[91] *Next Generation Networks – Frameworks and functional architecture models, Functional requirements and architecture of next generation netnworks*, ITU-T Reccommendation Y.2012, April, 2010.

[92] K. Kilkki, "Quality of Experience in Communication Ecosystems", in *Journal of Universal Computer Science*, vol. 14, no. 5, pages 615 - 624, 2008.

[93] A. Bouch, M. A. Sasse, and H. DeMeer, "Of packets and people: a user-centered approach to quality of service," in Proc. IEEE 2000 Eight International Workshop on Quality of Service (IWQOS), Pittsburgh, PA, USA, 5 -7 June, 2000, pp. 189 – 197.

[94] Terms and definitions related to quality of service and network performance including dependability, ITU-T Rec. E.800, 1994.

[95] K. Kilkki, "Differentiated Services for the Internet," Macmillan Publishing Co., Inc., Indianapolis, IN, USA, 1999. [Online]. Available: http://kilkki.net/3. Accessed on: Jan. 26, 2015.

[96] N. Muhammad, D. Chiavelli, D. Soldani and M. Li, "Introduction, in QoS and QoE Management in UMTS Cellular Systems," (eds D. Soldani, M. Li

and R. Cuny), John Wiley & Sons, Ltd, 2006, Chichester, UK. doi: 10.1002/9780470034057.ch1.

[97] Network Aspects (NA); General aspects of Quality of Service (QoS) and Network Performance (NP), ETSI ETR 003 second edition, October 1994.

[98] *Communications quality of service: A framework and definitions*, ITU-T Recommendation G.1000, November 2001.

[99] *End-user multimedia QoS categories*, ITU-T Recommendation G.1010, November 2001.

[100] N. Bayer, M. C. de Castro, A. Kassler, Y. Kouchergavy, P. Mitoraj, D. Staehle, "VoIP service performance optimization in pre-IEEE 802.11s Wireless Mesh Networks," in Proc. IEEE International Conference on *Circuits and Systems for Communications (ICCSC ´08)*, Shanghai, China, 26 – 28 May 2008, pp. 75 – 79.

[101] ITU-T, "Definition of Quality of Experience (QoE)", International Telecommunication Union, Liaison Statement, Ref.: TD 109rev2 (PLEN/12), January 2007.

[102] Online dictionary with Collins, [Online]. Available: http://dictionary.reverso.net/english-definitions/. Accessed on: Sep. 18, 2009.

[103] S. Talbott, "From Mechanism to a Science of Qualities," the Nature Institute. [Online]. Available: http://www.natureinstitute.org/txt/st/mqual/. Accessed on: Jan. 26, 2015.

[104] *Diameter base protocol*, IETF Standard RFC 3588, September 2003.

[105] *Next Generation Networks – Frameworks and functional architecture models, Network attachment control functions in next generation networks*, ITU-T Reccommendation Y.2014, March 2010.

[106] Research project, "Usability in Germany"´. [Online]. Available: http://www.usability-in-germany.de/. Accessed on: Jan. 26, 2015.

[107] Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11: Guidance on usability, International Organization for Standardization (ISO) 9241-11, March 1998.

[108] *Ergonomic of human-system interaction – Part 210: Human-centred design for interactive systems*, International Organization for Standardization (ISO) 9241-210, March 2010.

[109] Pro Context, “Usability und user experience“. [Online]. Available: http://www.procontext.com/aktuelles/2010/03/usability-und-user-experience-unterscheiden.html. Accessed on: Jan. 26, 2015.

[110] Nokia Siemens Networks, “Building business beyond flat rates”, 2009. [Online]. Available: http://networks.nokia.com/sites/default/files/Businessbeyondflatrate.pdf. Accessed on: Jan. 26, 2015.

[111] Reuter, “Telecoms executives see end of flat rates - survey”. [Online]. Available: http://uk.reuters.com/article/2010/08/23/telecoms-mobile-flatrate-idUKLDE67M1M420100823. Accessed on: Jan. 26, 2015.

[112] Android TV. [Online]. Available: https://www.android.com/tv/. Accessed on: Jan. 26, 2015.

[113] Maxdome. [Online]. Available: http://www.maxdome.de. Accessed on: Jan. 26, 2015.

[114] Amazon Prime Instant Video. [Online]. Available: http://www.amazon.de/Prime-Instant-Video. Accessed on: Jan. 26, 2015.

[115] Cisco WhitePaper, “Cisco Visual Networking Index: Forecast and Methodology, 2013–2018”. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html. Accessed on: Jan. 26, 2015.

[116] Cisco WhitePaper, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast 2013–2018”. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html. Accessed on: Jan. 26, 2015.

[117] Deutsche Telekom AG, “Entertain. Das neue Fernsehen, das alles möglich macht”. [Online]. Available: http://www.entertain.de. Accessed on: Jan. 26, 2015.

[118] Project Economics and Technologies for Inter-Carrier Services (ETICS) as part the Seventh Framework Programme (FP7) founded by the European Commission. [Online]. Available: http://www.ict-etics.eu/. Accessed on: Jan. 26, 2015.

[119] Nokia Siemens Networks, “White Paper - Are you ready for new growth opportunities in saturated mobile markets?”. [Online]. Available: http://networks.nokia.com/system/files/document/Mobile_Growth_White_Paper_0.pdf: Accessed on: Jan. 26, 2015.

[120] N. Kano, N. Seraku, F. Takahashi, and S. Tsuji, “Attractive Quality and Must-be Quality,” *Journal of the Japanese Society for Quality Control*, vol. 14, no. 2, 1984, pp. 39 - 48.

[121] P. Dely, A. Kassler, N. Bayer, H.-J. Einsiedler and D. Sivchenko, “FUZPAG: A Fuzzy-Controlled Packet Aggregation Scheme for Wireless Mesh Networks,” in Proc. *International Conference on Fuzzy Systems and Knowledge Discovery (FSKD’10)*, Yantai, China, 10 -12 August, 2010, pp. 778 – 782.

[122] L. Richter, “Untersuchung und Bewertung von Netzzugangssteuerungen auf Basis des Standards 802.1x (Port-Based Network Access Control),” Diploma thesis at Technical University of Chemnitz, Chemnitz, Germany, 2005.

[123] S. Pack, Y. Choi, “Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1x Model”, In Proceedings of IFIP TC6 Personal Wireless Communications 2002, Singapore, October 2002.

[124] *Definition of categories of speech transmission quality*, ITU-T Recommendation G.109, 1999.

[125] *The E-model: a computational model for use in transmission planning*, ITU-T Recommendation,”G.107”, 1998.

[126] *Methods for subjective determination of transmission quality*, ITU-T Recommendation P.800, 1996.

[127] T. Ulseth and F. Stafsnes, “VoIP speech quality – Better than PSTN?,” in Real-time communication over IP, Telektronikk 1.2006, pp. 119 - 129, 2006.

[128] *Pulse code modulation (PCM) of voice frequencies*, ITU-T Recommendation, G.711, November 1988.

[129] Linux Debian. [Online]. Available: http://www.debian.org/. Accessed on: Jan. 26, 2015.

[130] VoIP client SJphone. [Online]. Available: http://www.sjlabs.com/sjp.html. Accessed on: Jan. 26, 2015.

[131] Asterisk - The Open Source Telephony Projects. [Online]. Available: http://www.asterisk.org. Accessed on: Jan. 26, 2015.

[132] Debian package iproute. [Online]. Available: https://packages.debian.org/search?keywords=iproute. Accessed on: Jan. 26, 2015.

[133] W. Liang and W. Wang, "A Quantitative Study of Authentication and QoS in Wireless IP Networks," in Proc. of *INFOCOM 2005*, March 2005, pp. 1478 - 1489.

[134] A. Passito, E. Mota, R. Aguiar, I. Biris and E. Mota, "Evaluating Voice Speech Quality in 802.11b Networks with VPN/IPSec," in Proc. *13th IEEE International Conference on Networks (ICON)*, Kuala Lumpur – Malaysia, 2005, pp. 151 - 155.

[135] D. A. Westcott, B. E. Harkins, S. M. Jackman, "802.11i Security amendment and WPA Certifications," in *CWSP Certified Wireless Security Professional Official Study Guide: Exam PW0-204*, John Wiley & Sons, 2010, pp. 17 - .18 [Online]. Available: https://books.google.de/books?id=0ZWLn57EdpsC. Accessed on: Jan. 26, 2015.

[136] M. Cox, T. Czwornog, R. Fraumann, O. Ghopeh, D. Spellmeyer, F. Winslow, "Glossary," in *Good Informatics Practices (GIP) Module: Security*, Healthcare Information and Management Systems Society (HIMSS), 2011, pp. 86. [Online]. Available: https://books.google.de/books?id=-kcwBQAAQBAJ. Accessed on: Jan. 26, 2015.

[137] E. Tews, R.-P. Weinmann and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds," in *Information Security Applications*, Springer Berlin Heidelberg, 2007, pp. 188 – 202.

[138] Aircrack-NG. [Online]. Available: http://www.aircrack-ng.org/. Accessed on: Jan. 26, 2015.

[139] Aircrack-ptw. [Online]. Available: http://www.wirelessdefence.org/Contents/Aircrack-ptw.htm. Accessed on: Jan. 26, 2015.

[140] Iwconfig. [Online]. Available: http://linuxcommand.org/man_pages/iwconfig8.html. Accessed on: Jan. 26, 2015.

[141] Linux WPA/WPA2/IEEE 802.1X Supplicant. [Online]. Available: http://hostap.epitest.fi/wpa_supplicant/. Accessed on: Jan. 26, 2015.

[142] LINKSYS [Online]. Available: http://www.linksys.com: Accessed on: Jan. 26, 2015.

[143] DD-WRT [Online]. Available: http://www.dd-wrt.com: Accessed on: Jan. 26, 2015.

[144] CACE Technologies – AirPcap [Online]. Available: http://www.cacetech.com/. Accessed on: Jan. 26, 2015.

[145] WIRESHARK. [Online]. Available: http://www.wireshark.org/. Accessed on: Jan. 26, 2015.

[146] The MadWifi project – ticket #980. [Online]. Available: http://madwifi-project.org/attachment/ticket/980/fix-980.diff. Accessed on: Jan. 26, 2015.

[147] Sourceforge - WLAN Driver "MadWifi v0.9.4". [Online]. Available: http://downloads.sourceforge.net/madwifi/madwifi-0.9.4.tar.gz. Accessed on: Jan. 26, 2015.

[148] Developers' documentation for wpa_supplicant and hostapd. [Online]. Available: http://w1.fi/wpa_supplicant/devel/index.html. Accessed on: Jan. 26, 2015.

[149] *The Transport Layer Security (TLS) Protocol Ver. 1.1*, IETF RFC 4346, April 2006.

[150] A. Mishra, M. Shin, and W. Arbaugh, "Proactive Key Distribution using Neighbor Graphs", in IEEE Wireless Communications, February 2004 Vol 11 Issue 1, pages 26-36, 2004.

[151] T. Schneider, "Modelle zur Berechnung der Ausbreitung von Funksignalen, Teil 1," in *WissenHeute*, vol. 8, pp. 4 - 12, 2009.

[152] Harald T. Friis, "A note on a simple transmission formula," in Proc. *IRE*, vol. 34, no 5, May, 1946, pp. 254 - 256.

[153] T. Schneider, "Modelle zur Berechnung der Ausbreitung von Funksignalen, Teil 2," in *WissenHeute*, vol. 9, pp. 36 - 44, 2009.

[154] Telekom, "Telekom macht Hamburg zum Surferparadies". [Online]. Available: http://www.hotspot.de/content/news_tcity2.html. Accessed on: Jan. 26, 2015.

[155] Google WiFi. [Online]. Available: http://wifi.google.com/. Accessed on: Jan. 26, 2015.

[156] S. Dimatto, P. Hui, B. Han, and V. O.K. Li, "Cellular Traffic Offloading through WiFi Networks". [Online]. Available: http://www.deutsche-telekom-laboratories.de/~panhui/publications/mass11offload.pdf. Accessed on: Jan. 26, 2015.

[157] Financial Times, "Data overload threatens mobile networks". [Online]. Available: http://www.ft.com/cms/s/0/caeb0766-9635-11e1-a6a0-00144feab49a.html#axzz2blR3BqNt. Accessed on: Jan. 26, 2015.

[158] *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*, IETF RFC 4186, January 2006.

[159] Wireless Broadband Alliance., "WISPr 2.0". [Online]. Available: http://www.wballiance.com/resource-center/specifications/. Accessed on: Jan. 26, 2015.

[160] A. J. Elizondo, M. L. Garca, H. J. Einsiedler, R. Roth, M. Smirnov, M. Bartoli, P. Castelli, B. Varga and M. Krampell, "Service Models and Realisation of Differentiated Services Networks", in Proc. SPIE 4524, Quality of Service over Next-Generation Data Networks, 159, 27 July, 2001.

[161] *Universal Mobile Telecommunications System (UMTS); Technical Specifications and Technical Reports for a UTRAN-based 3GPP system*, 3GPP TS 21.101 version 6.10.0 Release 6, January 2010.

[162] *European Telecommunications Standards Institute (ETSI) Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), Resource and Admission Control Subsystem (RACS) Release 3: Functional Architecture*, Technical Report ETSI ES 282 003 v3.5.1, April 2011.

[163] *European Telecommunications Standards Institute (ETSI) Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): Network attachment subsystem (NASS) Release 3*, ETSI ES 282 004 v3.4.1, March 2010.

[164] *Functional requirements and architecture of next generation networks*, International Telecommunication Union (ITU), Recommendation ITU-T Y.2012, April 2010.

[165] Economics and Technologies for Inter-Carrier Services (ETICS), INFSO-ICT-248567, Deliverable D4.2 – ETICS architecture and functional entities high level design, June 2011.

[166] GSM World, „GSMA OneAPI“. [Online]. Available: http://www.gsmworld.com/oneapi/. Accessed on: Jan. 26, 2015.

[167] Open Mobile Alliance, „Enabler Release Definition for Next Generation Service Interfaces“. [Online]. Available: http://technical.openmobilealliance.org/Technical/technical-information/release-program/release-program-copyright-notice?rp=2164&r_type=technical&fp=Technical/Release_Program/docs/NGSI/V1_0-20101207-C/OMA-ERELD-NGSI-V1_0-20101207-C.pdf. Accessed on: Jan. 26, 2015.

[168] ETSI, “Network Functions Virtualisation - Introductory White Paper," June 2013. [Online]. Available: http://portal.etsi.org/NFV/ NFV_White_Paper.pdf. Accessed on: Jan. 26, 2015.

[169] T. Aura and M. Roe, “Reducing Reauthentication Delay in Wireless Networks”, in Proc. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM’05)*, 5 -9 September, 2005, pp. 139 - 148.

[170] *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS)*, IEEE 802.11r-2008, July 2008.

[171] Bundesministeriums der Justiz und für Verbraucherschutz, “Telemediengesetz (TMG)," August 2014. [Online]. Available: http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf. Accessed on: Jan. 26, 2015.

[172] 3GVisioin - i-nigma. [Online]. Available: http://www.i-nigma.com/hp.html. Accessed on: Jan. 26, 2015.

[173] *The WebSocket Protocol*, IETF RFC 6455, December 2011.

[174] *PPP Challenge Handshake Authentication Protocol (CHAP)*, IETF RFC 1994, August 1996.

[175] *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture*, ETSI ES 282 001 v3.4.1 European Telecommunications Standards Institute, September 2009.

[176] *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture*, ETSI ES 282 007 v2.1.1 European Telecommunications Standards Institute, November 2008.

[177] *Handover Key Management and Re-Authentication Problem Statement*, IETF RFC 5169, March 2008.

[178] wpa_supplicant v0.6.6. [Online]. Available: http://hostap.epitest.fi/releases/wpa_supplicant-0.6.6.tar.gz. Accessed on: Jan. 26, 2015.

[179] hostapd v0.6.4. [Online]. Available: http://hostap.epitest.fi/releases/hostapd-0.6.4.tar.gz. Accessed on: Jan. 26, 2015.

[180] *The MD5 Message-Digest Algorithm*, IETF RFC 1321, April 1992.

[181] FreeRadius: The FreeRadius project. [Online]. Available: http://freeradius.org/. Accessed on: Jan. 26, 2015.

[182] SMS Server Tools 3. [Online] Available: http://smstools3.kekekasvi.com/. Accessed on: Jan. 26, 2015.

[183] *The application/json Media Type for JavaScript Object Notation (JSON)*, IETF RFC 4627, July 2006.

[184] MySQL. [Online]. Available: http://www.mysql.de. Accessed on: Jan. 26, 2015.

[185] JSQR – JavaScript Quick Response Code Encoder Library. [Online] Available: http://www.jsqr.de/. Accessed on: Jan. 26, 2015.

[186] Siege. [Online]. Available: http://www.joedog.org/siege-home/. Accessed on: Jan. 26, 2015.

[187] Open Networking Foundation "Software-Defined Networking (SDN) Definition". [Online]. Available: https://www.opennetworking.org/sdn-resources/sdn-definition. Accessed on: Jan. 26, 2015.

[188] ETSI ISG NFV, “Our Role & Activities”. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/nfv. Accessed on: Jan. 26, 2015.

[189] Heise: 2D-Barcode, der mobile Link ins Internet. [Online]. Available: http://www.heise.de/ix/meldung/2D-Barcode-der-mobile-Link-ins-Internet-181474.html. Accessed on: Jan. 26, 2015.

[190] G. Eichler, K.-H. Lüke, A. Aydin, R. Schwaiger, “Barcode application innovation for smartphones”, in Proc. *3rd Workshop on Mobile and Embedded Interactive Systems (MEIS'09)*, Lübeck, Germany, Sept. 28. - Oct. 2, 2009, pp. 2198 - 2201.

[191] Deutsche Post: DV-Freimachung - Matrix-Code. [Online]. Available: https://www.deutschepost.de/de/d/dv_freimachung/faq_datamatrix_code/zertifizierung_datamatrixcode0.html. Accessed on: Jan. 26, 2015.

[192] Mobile Barcodes. [Online]. Available: http://www.mobile-barcodes.com. Accessed on: Jan. 26, 2015.

[193] Visalead. [Online]. Available: http://www.visualead.com/invx/. Accessed on: Jan. 26, 2015.

[194] Upcodeworld. [Online]. Available: http://www.upcodeworld.com/. Accessed on: Jan. 26, 2015.

[195] Seamcode. [Online]. Available: http://semacode.com/your-own-semacode/. Accessed on: Jan. 26, 2015.

[196] Quickmark. [Online]. Available: http://www.quickmark.com.tw. Accessed on: Jan. 26, 2015.

[197] Semacode Technical white paper. [Online]. Available: http://giswiki.hsr.ch/images/d/d2/Best_2D_Barcode.pdf. Accessed on: Jan. 26, 2015.

[198] Wi-Fi Alliance, ”WPA2”. [Online]. Available: http://www.wi-fi.org/knowledge-center/glossary/wpa2%E2%84%A2. Accessed on: Jan. 3, 2012.

Authors Publications

Patents

[1] A. Roos, S. Drüsedow, M. Ilaghi, “Method and system for trust level based data storage in a distributed storage environment and trust level based access to the storage environment,” European Patent Office, Application No. / Patent No. 14182116.5 / - in 2014.

[2] A. Roos, M. H. Amirsalari, “Method and system for barcode and link initiated Hotspot auto-login in WLANs,” European Patent Office, Application No. / Patent No. 14170605.1 / -, in 2014.

[3] A. Roos, I. Korthals, U. Grundhoefer, O. Bonness, S. Dhakal, D. Sivchenko, N. Bayer, H.-J. Einsiedler, “Method and system for service quality indication in end-to-end delivery of IP based services,” European Patent Office, Application No. / Patent No. 12159195.2 / EP2640006 in 2013.

[4] N. Bayer, A. Roos, D. Sivchenko, “Method and system for network-centric control of network connectivity for mobile terminals in IEEE 802.11 based networks,” European Patent Office, Application No. / Patent No. 11168896.1 – 1249 / EP2533573 in 2011.

[5] I. Korthals, H. J. Einsiedler, A. Roos, N. Bayer, D. Sivchenko, “Method, apparatus and system for triggering and/or enabling QoS support for selected applications in IP based networks,” European Patent Office, Application No. / Patent No. 11168661.4 – 1244 / EP2530884 in 2011.

[6] N. Bayer, H. J. Einsiedler, D. Sivchenko, B. Xu, F.-P. Brück, M. Reumann, P. Wolf, K. Hammer, A. Roos, “Method and system enabling seamless connectivity in WLAN based Hotspots,” European Patent Office, Application No. / Patent No. 09153658.1 – 2413 / 2205013 in 2009.

[7] B. Xu, E. Bogenfeld, M. Grigat, M. Siebert, N. Bayer, D. Sivchenko, A. Roos, B. Hahn, S. Robitzsch, “A system and a method for providing improved quality of a communication service,” European Patent Office, Application No. / Patent No. 08156992.3 – 2416 / EP2129061 in 2008.

[8] M. Siebert, B. Xu, J. Kraus, N. Bayer, D. Sivchenko, A. Roos, “Method and system for optimising the information content of multimedia transmissions based on dynamically complementary source selection,” European Patent Office, Application No. / Patent No. 08102702.1 - 1522 / EP2104352 in 2008.

Journal Publications

[1] Ch. Esteve and A. Roos, "A Review of Policy-Based Resource and Admission Control Functions in Evolving Access and Next Generation Networks," In: Journal of Network and Systems Management, VOL 16, NO 1 March 2008, Springer Netherlands, pp. 14 - 45.

Peer Reviewed Publications

[1] A. Roos, T. Rettig, H. J. Einsiedler, O. Bonness, S. Wieland and A. Schwarzbacher, “Bandwidth on Demand in Fixed Access Networks - Application Service aware and User initiated Internet Connectivity,” In Proceedings of 20. ITG Fachtagung Mobilkommunikation, Osnabrück, Germany, 7. - 8. May 2015.

[2] A. Roos, S. Drüsedow, M. I. Hosseini, G. Coskun and S. Zickau, “Trust Level Based Data Storage and Data Access Control in a Distributed Storage Environment,” In Proceedings of IEEE 3rd Mobile Cloud Conference 2015, San Francisco, USA, 30. March - 3. April 2015.

[3] A. Roos, M. H. Amirsalari, S. Wieland, A. Schwarzbacher, “Barcode Initiated Hotspot Auto-login Mechanism For WLAN-Based Access Networks,” In Proceedings of 25th Irish Signals and Systems Conference 2014, Limerick, Ireland, 26. - 27. June 2014.

[4] H. J. Einsiedler, N. Bayer, K. Haensge, R. Szczepanski, M. Kurze, T. Rettig, F. Gonzalez-Garcia, A. Roos, S. Berg and J. I. Morenoz “Efficient Transmission of Smartphone Application Traffic in Wireless Access Networks,” In Proceedings of IEEE Mobile Cloud Conference 2014, Oxford, England, 8. -11. April 2014.

[5] A. Roos, O. Bonness, S. Dhakal, H. Lonsethagen, I. Korthals, S. Wieland, A. Schwarzbacher, “Application Service Quality Indication to End-Users in IP based Networks as Added Value Service,” In Proceedings of Future Network & MobileSummit conference 2013, Lisbon, Portugal, 3. - 5. July 2013.

[6] N. Bayer; D. Sivchenko; H. J. Einsiedler; A. Roos; A. Uzun; S. Göndör and A. Küpper, “Energy Optimisation in Heterogeneous Multi-RAT Networks,” In Proceedings of ICIN conference 2011, Berlin, Germany, 4. - 7. October 2011.

[7] A. Roos, M. Flegl, S. Wieland, A. Th. Schwarzbacher, H. J. Einsiedler, "Semacode based Voucher Concept enabling flexible and user-friendly Hotspot Login on demand," In Proceedings of 15. ITG Fachtagung Mobilkommunikation, Osnabrück, Germany, 19. - 20. May 2010.

[8] S. Massner, A. Roos, N. Graf, "Optimierung von WLAN Zugangsnetzen durch richtlinienbasierte Ressourcensteuerung," In Proceedings of 15. ITG Fachtagung Mobilkommunikation, Osnabrück, Germany, 19. - 20. May 2010.

[9] A. Roos, A. Keller, A. Th. Schwarzbacher, S. Wieland, "Sequential Authentication Concept to Improve WLAN Handover Performance," In: Communications in Computer and Information Science 53, Intelligent Interactive Assistance and Mobile Multimedia Computing, November 2009, Springer Berlin Heidelberg, pp. 295 – 306.

[10] A. Roos, S. Wieland and A. Th. Schwarzbacher, “Investigation of security mechanism and mobility influence on voice over IP quality,” In Proceedings of Science Days 2008, Leipzig, Germany, 17. – 18. November 2008.

[11] A. Roos, S. Robitzsch, B. Xu, S. Wieland and A. Th. Schwarzbacher, "Service Quality Improvement based on Network Attachment Subsystem extensions and Service Enhancement Function - Mesh Networks as an example," In Proceedings of Networks 2008, Budapest, Hungary, 28. September - 2. October 2008.

[12] N. Bayer, D. Hock, A. Roos, M. Siebert, B. Xu, V. Rakocevic and J. Habermann, "VoIP performance in "MeshBed" - a Wireless Mesh Network Testbed," In Proceedings of the 67th IEEE Vehicular Technology Conference (VTC) Spring 2008, Marina Bay, Singapore, May 2008.

[13] A. Roos, S. Wieland and A. Th. Schwarzbacher, “Herausforderungen an AAA Funktionalitäten für die Mobilitätsunterstützung in Mesh Zugangsnetzwerken,” In Proceedings of Science Days 2007, Leipzig, Germany, 25. – 26. September 2007.

[14] A. Roos, A. Th. Schwarzbacher, S. Wieland, B. Xu, "Time behaviour and network encumbrance due to authentication in wireless mesh access networks," In Proceedings of the 65th IEEE Vehicular Technology Conference (VTC) Spring 2007, Dublin, Ireland, April 2007.

[15] A. Roos, A. Th. Schwarzbacher, S. Wieland, "Broadband Wireless Internet Access in Public Transportation," In Proceedings of the VDE Kongress - Innovations in Europe, Vol. 1, pp. 65-70, Aachen, Germany, Oct. 2006.

[16] N. Bayer, A. Roos, R. Karrer, B. Xu, C. Esteve, "Towards Carrier Grade Wireless Mesh Networks for Broadband Access," In Proceedings of the OpComm 2006, Berlin, Germany, Sep. 2006.

Appendix

A.1 Barcode

A barcode is the representation of data or information in an optical machine readable format. Barcodes contain information in the form of 1 dimensional (1D) or 2 dimensional (2D) symbols. 1D barcodes formats the numeric and alphanumeric information by means of parallel lines with different spaces among the lines as well as different line widths. Whereas, 2D barcodes comprise numeric and alphanumeric information represented by means of e.g. squares or dots. However, 2D barcodes have a larger capability to represent data. Mostly numeric and alphanumeric barcodes are used to request information from databases and web servers [189].

The types of barcode applications for mobile phones can be described as receptive (recognition) and productive (generation) [190]. For example, the 2D barcode named Aztec Code is used by Deutsche Bahn for tickets sold online and printed out by customers containing customer and ticket information [189]. Other 2D barcodes are Quick Response (QR) Code and Data Matrix Code. QR Code is specified in ISO/IEC 18004:2006 and Data Matrix Code in ISO/IEC 16022:2000. QR code is common in Japan [ibid]. Most Japanese mobile phones are able to read the QR code with their camera. Whereas the Data Matrix code is recommended by the Electronic Industries Alliance (EIA) to label small electronic components. The US Department of Defence uses the Data Matrix code for the unique identification of items, whereas Deutsche Post uses the Data Matrix code for digital postmarks [191]. Moreover, Data Matrix format is used by Semacode to encode data.

QR code and Semacode is often used in context of convenience oriented applications in conjunction with mobile phone users. The QR Code and Semacode are able to comprise messages, addresses and URLs presented on poster, signs, in magazines, buses or business cards. Moreover, these barcodes can comprise information about objects in e.g. museum or exhibitions as well. Figure A.1 presents exemplarily the 2D barcodes QR code and Data Matrix / Semacode. Both barcodes comprise the message “www.mobilfunktagung.de”.

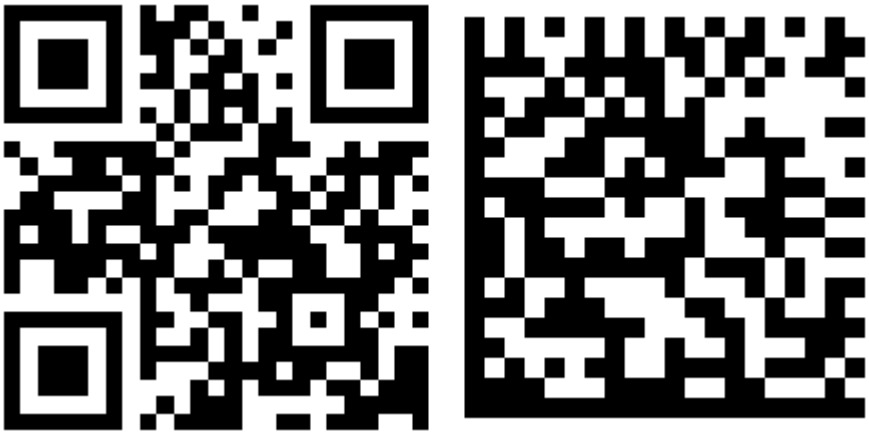


Figure A.1: 2D barcodes: QR code (left) and Data Matrix / Semacode (right); barcode content: “www.mobilfunktagung.de”.

A mobile phone equipped with a camera and the reader software scans a barcode. The reader software extracts the data from the barcode and presents the information on the display or launches the web browser of the mobile phone redirecting it to the programmed URL. There are several websites, such as [192], [193], [194], [195], [196] providing a QR Code or Semacode generator as well as barcode reader software for mobile phones, such as [172], [194] or [196].

The comparison of QR code and Data Matrix code in [197] state that Data Matrix code is more efficient than QR code. The conclusion of [ibid] is that Data Matrix code is 30% to 60% more efficient when encoding the same data. This means that the barcodes fit more easily onto pages or screens. Moreover, the Data Matrix code has a larger third-party industry support for both creation and decoding of barcodes. This was the reason why this work implemented the novel barcode initiated hotspot auto-login solution using Semacode.

A.2 Access Point Configuration

LINKSYS [142] WRT54G access points are used in the test bed and in the measurement series. The applied firmware is DD-WRT [143] in the version 23.

Access point configuration with WEP encryption:

The configuration of access point 1 and 2 is presented in Figure A.2 and Figure A.3. The WEP method requires the configuration of a static encryption key.

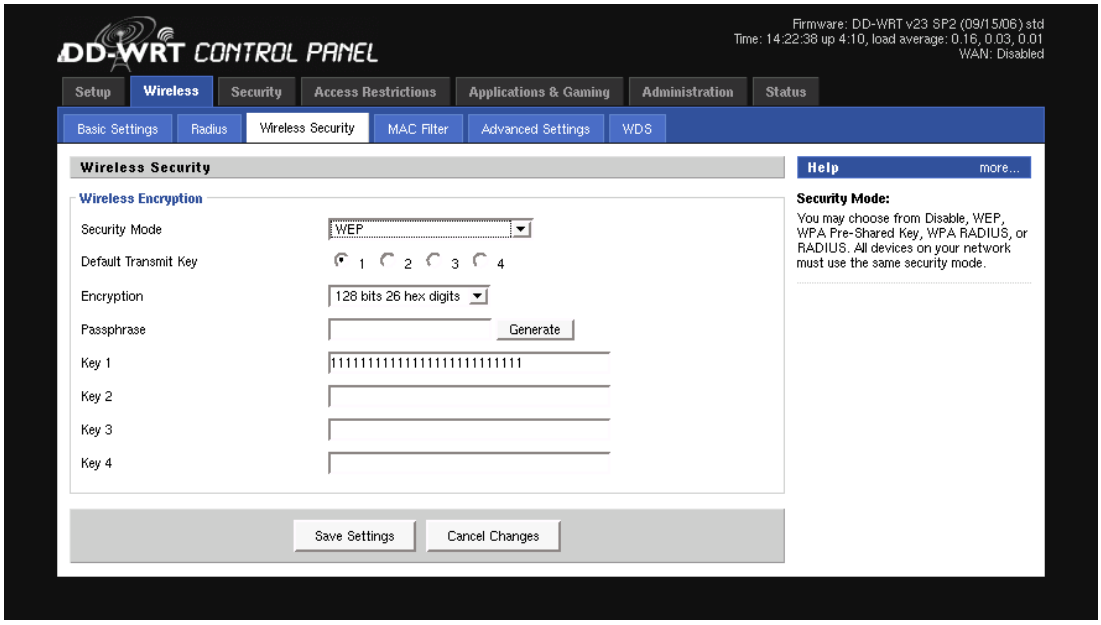


Figure A.2: WEP configuration of access point 1.

The difference between both access point configurations is the WEP encryption key used. Each access point uses another WEP encryption key.

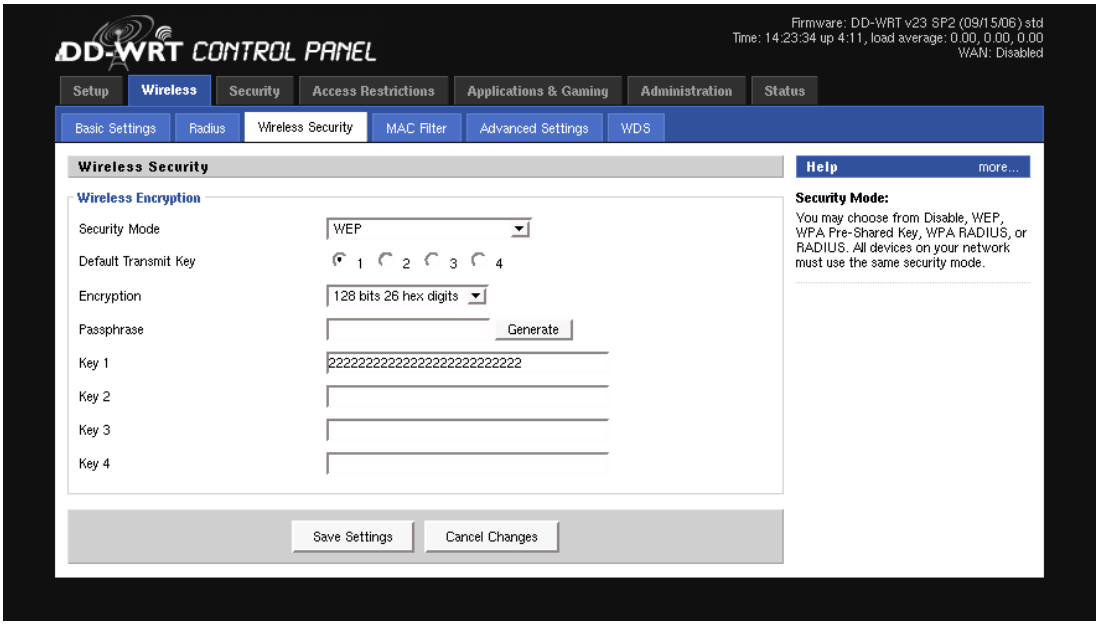


Figure A.3: WEP configuration of access point 2.

Access point configuration with WPA2 (EAP-TLS) encryption:

The configuration of access point 1 and 2 is presented in Figure A.4. The WPA2 (EAP-TLS) configuration requires no static encryption key. This encryption key is derived while performing the EAP-TLS handshakes. However, a key (WPA shared key) for the successful communication among access point and the RADIUS server is needed.

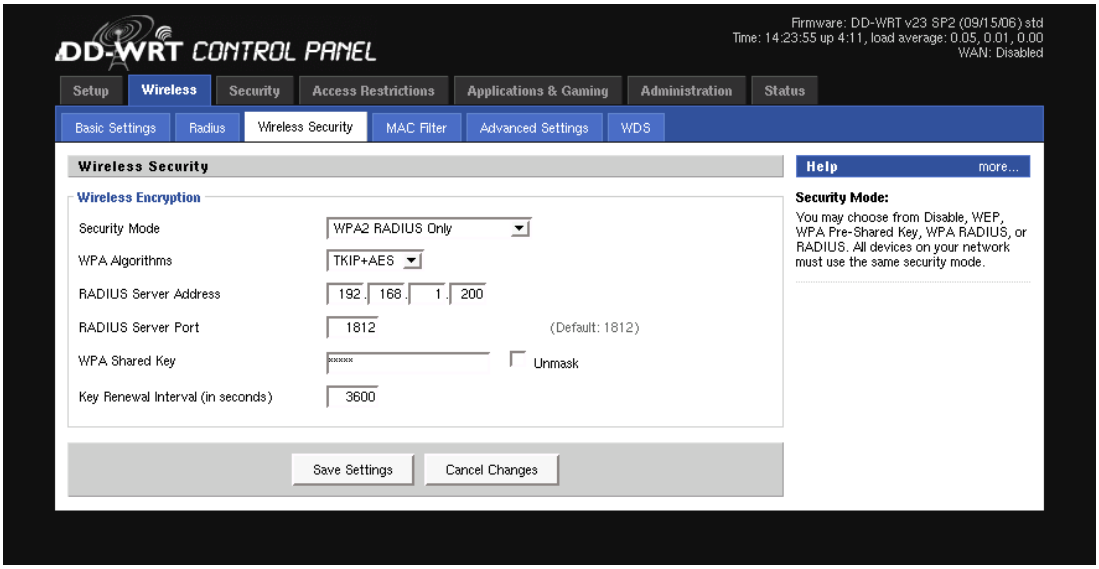


Figure A.4: WPA2 (EAP-TLS) configuration of access point 1 and 2.

A.3 Measurement Preparations

By means of the Patch «fix-980.diff» [146] the Madwifi Driver v0.9.4 [147] was changed to prevent of the channel scanning process from starting. The patch changes file *net80211/ieee80211_scan_sta.c* of the Madwifi project [ibid]. To integrate the patch in the Madwifi driver the following command is executed in the folder of the Madwifi project followed by re-compilation of the driver.

```
#patch < fix980.diff
#make clean
#make all
#make install
```

Configuration of wireless card in WEP mode:

The following code box contains the configuration of the wpa_supplicant to configure the wireless land card in WEP mode.

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
network={
ssid="LINKSYS_AP1"
scan ssid=0
key_mgmt=NONE
wep_tx_keyidx=0
wep_key0=11111111111111111111111111
}n
etwork={
ssid="LINKSYS AP2"
scan_ssid=0
key_mgmt=NONE
wep_tx_keyidx=0
wep_key0=22222222222222222222222222
}
```

Configuration of wireless card in WPA2 (EAP-TLS) mode:

The following code box contains the configuration of the wpa_supplicant to configure the wireless land card in WPA2 (EAP-TLS) mode.

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
network={
ssid="LINKSYS_AP1"
scan_ssid=1
key_mgmt=WPA-EAP
eap=TLS
identity="root"
ca_cert="/root/certs/cacert.pem"
client_cert="/root/certs/client-cert.pem"
private_key="/root/certs/client-cert.pem"
private_key_passwd="radio2005"
}n
etwork={
ssid="LINKSYS_AP2"
scan_ssid=1
key_mgmt=WPA-EAP
eap=TLS
identity="root"
ca_cert="/root/certs/cacert.pem"
client_cert="/root/certs/client-cert.pem"
private_key="/root/certs/client-cert.pem"
private_key_passwd="radio2005"
}
```

A.4 WEP Investigations of Handover Time Behaviour

WEP encryption using iwconfig:

Figure A.5 illustrates part of a ping trace, listing all ping request and ping replies, of a handover process using WEP encryption and the wireless configuration tool iwconfig. The dark (red) marked row highlights the first successfully sent ping request from UE to the CS after the carried out handover. The third column time delta of the dark (red) marked row shows the time difference between the current send ping request and the previous received packet ping reply before the handover has taken place. In this case the IP communication is interrupted for 84 ms.

No.	Time	Time Delta	Source	Destination	Protocol	Info
1	0.000	0.000	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
2	0.000	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
3	0.008	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
4	0.009	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
5	0.017	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
6	0.019	0.001	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
7	0.027	0.007	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
8	0.027	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
9	0.037	0.009	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
10	0.038	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
11	0.047	0.009	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
12	0.049	0.001	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
13	0.133	0.084	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
14	0.134	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
15	0.142	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
16	0.142	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
17	0.151	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
18	0.151	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
19	0.160	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
20	0.160	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply

Figure A.5: Ping trace of handover; iwconfig (WEP).

To assess the consequences of the handover the last packet before the handover occurs, shown as frame No.12 in Figure A.5, and the first packet after the handover, shown as frame No. 13 in Figure A.5, is now investigated in more detail.

```
⊞ Frame 12 (98 bytes on wire, 98 bytes captured)
⊞ Ethernet II, Src: SmdInfor_b2:60:30 (00:40:48:b2:60:30), Dst: 3com_37:f7:32 (00:1a:c1:37:f7:32)
⊞ Internet Protocol, Src: 192.168.1.200 (192.168.1.200), Dst: 192.168.1.110 (192.168.1.110)
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0 ()
    Checksum: 0x05fd [correct]
    Identifier: 0x3f6a
    Sequence number: 6 (0x0006)
```

Figure A.6: Frame No. 12 of ping trace using iwconfig (WEP).

Figure A.6 presents details of the last successfully received packet before the handover occurs. In this case it is frame No. 12 of the ping series that is the ping reply from the CS server. At this point the most important information is the sequence number of the packet. In a ping series the sequence number increments with each ping request packet sent. The ping request and the appropriate ping reply bear equal sequence numbers. Frame No. 12 in Figure 3.9 has sequence number six. Therefore, so far all ping requests of the ping series have been answered by a ping reply.

```
⊞ Frame 13 (98 bytes on wire, 98 bytes captured)
⊞ Ethernet II, Src: 3com_37:f7:32 (00:1a:c1:37:f7:32), Dst: SmdInfor_b2:60:30 (00:40:48:b2:60:30)
⊞ Internet Protocol, Src: 192.168.1.110 (192.168.1.110), Dst: 192.168.1.200 (192.168.1.200)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0 ()
    Checksum: 0x97a8 [correct]
    Identifier: 0x3f6a
    Sequence number: 12 (0x000c)
```

Figure A.7: Frame No. 13 of ping trace using iwconfig (WEP).

Figure A.7 presents frame No. 13 of the ping series after the handover process was carried out. Frame No. 13 has sequence number twelve. Taking sequence number six of frame No. 12 into account it shows that sequence number seven to

eleven is missing in the ping series. Due to the WLAN card configuration process which results in interrupted IP connectivity between UE and AP five ping request packets were lost.

WEP encryption using wpa_supplicant:

The use of wpa_supplicant is not required to setup a WEP encrypted connection to a WLAN. However, to compare the handover behaviour of the wpa_supplicant with iwconfig it is essential to investigate the wpa_supplicant with the same encryption method as iwconfig. The ping trace shown in Figure A.8 depicts ping requests and ping replies of a handover process using WEP encryption and the wireless configuration tool wpa_supplicant. The dark (red) marked row highlights the first successfully send ping request of UE to the CS after the successful handover. The time delta in the dark (red) marked row shows again the time difference between the current send ping request and the previously received packet ping reply before the handover process has been carried out. The measurement shows a communication interruption for 283 ms.

No.	Time	Time Delta	Source	Destination	Protocol	Info
1	0.000	0.000	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
2	0.000	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
3	0.008	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
4	0.009	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
5	0.018	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
6	0.019	0.001	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
7	0.303	0.283	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
8	0.304	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
9	0.312	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
10	0.313	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
11	0.321	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
12	0.322	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
13	0.335	0.013	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
14	0.336	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
15	0.345	0.009	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
16	0.347	0.001	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
17	0.355	0.007	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
18	0.358	0.003	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
19	0.367	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
20	0.375	0.008	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply

Figure A.8: Ping trace of handover; wpa_supplicant (WEP).

The detailed analysis of the ping trace in Figure A.8 confirms the increased communication interruption time. To assess the communication interruption of the handover the last packet before the handover occurs, shown as frame No. 6 in Figure A.9 and the first packet after the handover, shown as frame No. 7 in Figure A.10, is now investigated in more detail.

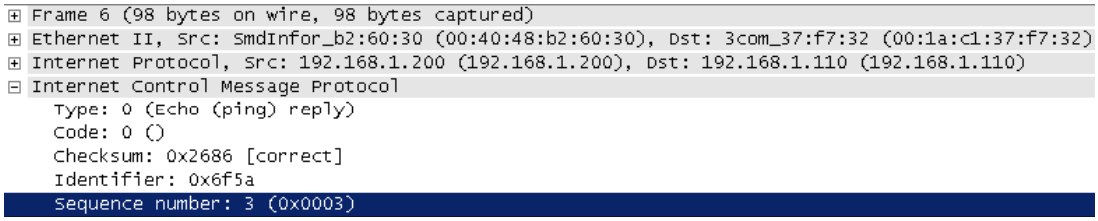


Figure A.9: Frame No. 6 of ping trace using wpa_supplicant (WEP).

The last packet sent before the handover has been carried out is frame No. 6 presented in Figure A.9. Frame No. 6 is a ping reply with the sequence number three. Therefore, so far all ping requests have been answered.

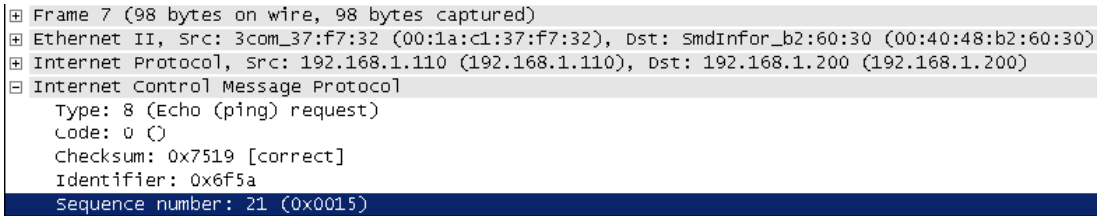


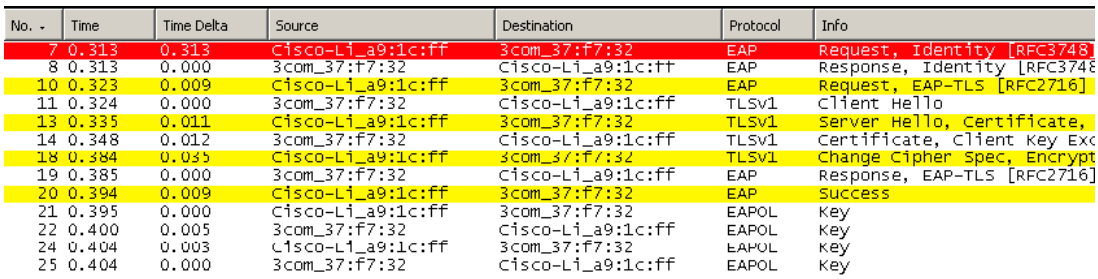
Figure A.10: Frame No. 7 of ping trace using wpa_supplicant (WEP).

Figure A.10 presents the first sent packet with frame No. 7 after the carried out handover. Frame No. 7 is a ping request with the sequence number 21. This means the sequence number four to 20 got lost.

A.5 WPA2 Investigations of Handover Time Behaviour

WPA2 encryption and EAP-TLS authentication with local AAA server:

A deeper insight into the communication interruption, the authentication communication and the ping communication is done by means of WIRESHARK in Figure A.11 and Figure A.12. In Figure A.11 the authentication communication induced by IEEE 802.1X using EAP-TLS among UE, PoA and LAAA server respectively is shown. Figure A.12 presents the Ping communication among UE and CS.



No.	Time	Time Delta	Source	Destination	Protocol	Info
7	0.313	0.313	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAP	Request, Identity [RFC3748]
8	0.313	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAP	Response, Identity [RFC3748
10	0.323	0.009	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAP	Request, EAP-TLS [RFC2716]
11	0.324	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	TLSv1	Client Hello
13	0.335	0.011	Cisco-Li_a9:1c:ff	3com_37:f7:32	TLSv1	Server Hello, Certificate,
14	0.348	0.012	3com_37:f7:32	Cisco-Li_a9:1c:ff	TLSv1	Certificate, Client Key Exc
18	0.384	0.035	Cisco-Li_a9:1c:ff	3com_37:f7:32	TLSv1	Change Cipher Spec, Encrypt
19	0.385	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAP	Response, EAP-TLS [RFC2716]
20	0.394	0.009	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAP	Success
21	0.395	0.000	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAPOL	Key
22	0.400	0.005	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAPOL	Key
24	0.404	0.003	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAPOL	Key
25	0.404	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAPOL	Key

Figure A.11: EAP-TLS communication; internal AAA server scenario.

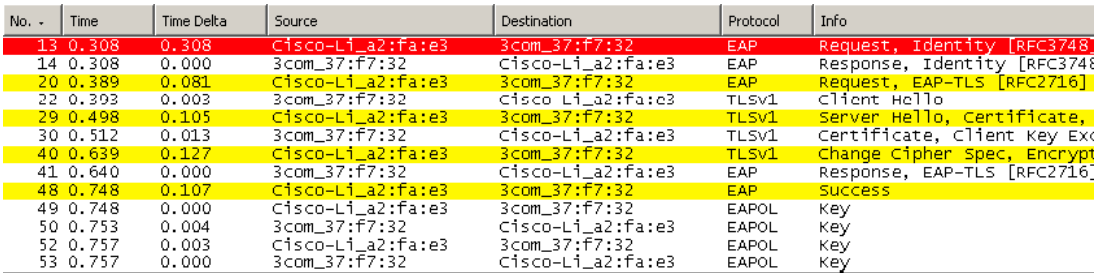
The ping communication via the Internet control message protocol (ICMP) in Figure A.11 is suppressed to enable a clearer analysis of the EAP authentication communication. The dark (red) marked frame number six in Figure A.12 shows the last successfully ping packet sent before the handover process has started. In Figure A.11 the dark (red) marked frame number seven presents the first successfully transmitted IP packet after the handover was carried out. The bright (yellow) marked rows highlight the packets sent from the AAA server and forwarded from the PoA to the UE. The time between frame number six, in Figure A.12, and frame number 7, in Figure A.11, is 313 ms. This time difference of 313 ms corresponds to the wireless card configuration time. However, in contrast to the WEP handover process there is no communication with the network possible after the wireless card configuration was carried out. This is shown in Figure A.12 when frame number nine, twelve, 15, 16, 17 and 23 are taken into account. The ping requests are sent to the network by the UE but no ping reply from the CS occurs. This depends on the IEEE 802.1X mechanism that only allows interaction of authentication messages between the UE and the PoA, as can be seen in Figure A.11. Full network access is granted after successful UE authentication. The bright (green) marked frame number 26 in Figure A.12 shows the first successfully transmitted ping request packet to the CS after full network access is granted by the authenticator. To determine the additional communication interruption time due to WPA2 EAP-TLS authentication in a local authentication scenario a reference point is set at frame 9. The consumed authentication time in this measurement is the time between this reference point in Figure A.12 and frame number 26. In this example the authentication time takes 96 ms.

No.	Time	Time Delta	Source	Destination	Protocol	Info
5	0.018	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
6	0.018	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
9	*REF*	*REF*	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
12	0.016	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
15	0.032	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
16	0.048	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
17	0.063	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
23	0.082	0.018	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
26	0.096	0.013	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
27	0.096	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
28	0.105	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
29	0.105	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply

Figure A.12: Ping communication; internal AAA server scenario.

WPA2 encryption and EAP-TLS authentication with external AAA server:

In Figure A.13 again the ping ICMP packets are suppressed to provide a clearer analysis. Figure A.13 presents the EAP-TLS authentication process among the UE and the PoA.



No.	Time	Time Delta	Source	Destination	Protocol	Info
13	0.308	0.308	Cisco-Li_a2:fa:e3	3com_37:f7:32	EAP	Request, Identity [RFC3748
14	0.308	0.000	3com_37:f7:32	Cisco-Li_a2:fa:e3	EAP	Response, Identity [RFC3748
20	0.389	0.081	Cisco-Li_a2:fa:e3	3com_37:f7:32	EAP	Request, EAP-TLS [RFC2716]
22	0.393	0.003	3com_37:f7:32	Cisco-Li_a2:fa:e3	TLSv1	Client Hello
29	0.498	0.105	Cisco-Li_a2:fa:e3	3com_37:f7:32	TLSv1	Server Hello, Certificate,
30	0.512	0.013	3com_37:f7:32	Cisco-Li_a2:fa:e3	TLSv1	Certificate, Client Key Exc
40	0.639	0.127	Cisco-Li_a2:fa:e3	3com_37:f7:32	TLSv1	Change Cipher Spec, Encrypt
41	0.640	0.000	3com_37:f7:32	Cisco-Li_a2:fa:e3	EAP	Response, EAP-TLS [RFC2716]
48	0.748	0.107	Cisco-Li_a2:fa:e3	3com_37:f7:32	EAP	Success
49	0.748	0.000	Cisco-Li_a2:fa:e3	3com_37:f7:32	EAPOL	Key
50	0.753	0.004	3com_37:f7:32	Cisco-Li_a2:fa:e3	EAPOL	Key
52	0.757	0.003	Cisco-Li_a2:fa:e3	3com_37:f7:32	EAPOL	Key
53	0.757	0.000	3com_37:f7:32	Cisco-Li_a2:fa:e3	EAPOL	Key

Figure A.13: EAP-TLS communication; external AAA server scenario.

The dark (red) marked frame number 12 in Figure A.14 shows the last successfully ping packet sent before the handover process has been started. In Figure A.11 the dark (red) marked frame number 13 presents the first successfully transmitted IP packet after the handover. The comparison of column time delta of Figure A.13 with the column of Figure A.11 shows the increased time. By means of the ping packets the communication interruption time is determined. In this measurement the wireless card configuration time is the time difference between frame number 12, in Figure A.14, and frame number 13, in Figure A.13, and results in 308 ms. As well as in the WPA2 EAP-TLS with the local AAA server scenario there is no communication possible with the network after the wireless card is configured. This behaviour is due to the continuing authentication process of EAP-TLS and is shown in Figure A.14 when frame number 15 to 51 are taken into account. The ping requests are sent by the UE but no ping reply from the CS occurs. The bright (green) marked frame 54 in Figure A.14 presents the first successfully ping request packet transmitted to the CS that is answered by the ping reply in frame number 55 after fully granted network access by the authenticator. To determine the additional communication interruption time due to WPA2 EAP-TLS authentication in an external authentication scenario a reference point is set at frame number 15. The authentication time consumed in this measurement is the time between reference point in Figure A.14 and frame number 54. In this example the authentication time takes 456 ms.

No.	Time	Time Delta	Source	Destination	Protocol	Info
11	0.045	0.007	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
12	0.045	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
15	*REF*	*REF*	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
16	0.016	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
17	0.031	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
18	0.047	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
19	0.063	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
21	0.080	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
23	0.096	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
24	0.111	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
25	0.128	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
26	0.144	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
27	0.159	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
28	0.175	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
31	0.201	0.025	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
32	0.215	0.014	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
33	0.231	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
34	0.247	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
35	0.263	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
36	0.279	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
37	0.295	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
38	0.311	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
39	0.328	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
42	0.344	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
43	0.361	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
44	0.375	0.014	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
45	0.391	0.016	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
46	0.407	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
47	0.423	0.015	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
51	0.443	0.019	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
54	0.456	0.013	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
55	0.457	0.001	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply

Figure A.14: Ping communication; external AAA server scenario.

WPA2 encryption without full EAP-TLS authentication process:

In comparison to the authentication time in the local and external EAP-TLS authentication scenario, shown in Table 3.11 and Table 3.12, the authentication time in Figure A.15 occurs due to the re-key process only. Figure A.15 shows that no certificate exchange among the UE and the AAA server takes place except for the four-way handshake among the UE and the PoA.

No.	Time	Time Delta	Source	Destination	Protocol	Info
186	9.972	0.025	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
187	9.973	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
188	*REF*	*REF*	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAPOL	Key
189	0.005	0.005	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAPOL	Key
190	0.008	0.002	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAPOL	Key
191	0.008	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAPOL	Key
192	0.011	0.002	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
193	0.011	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
194	0.019	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
195	0.020	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply

Figure A.15: WPA2 re-keying process using EAP-TLS; no AP reboot.

WPA2 encryption with PSK:

Figure A.16 presents the four way handshake between the UE and the AP. The dark (red) marked frame 538 is the first successfully sent packet after the wireless card re-configuration. The four-way handshake based on the PSK is initiated by the AP and presented in frame 538. As expected Figure A.16 presents a comparable packet loss as WPA2 with EAP-TLS in the no AP reboot scenario.

No.	Time	Time Delta	Source	Destination	Protocol	Info
536	9.894	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
537	9.895	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
538	*REF*	*REF*	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAPOL	Key
539	0.005	0.005	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAPOL	Key
540	0.005	0.000	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
541	0.007	0.002	Cisco-Li_a9:1c:ff	3com_37:f7:32	EAPOL	Key
542	0.007	0.000	3com_37:f7:32	Cisco-Li_a9:1c:ff	EAPOL	Key
543	0.020	0.012	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
544	0.021	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply
545	0.030	0.008	192.168.1.110	192.168.1.200	ICMP	Echo (ping) request
546	0.031	0.000	192.168.1.200	192.168.1.110	ICMP	Echo (ping) reply

Figure A.16: WPA2 PSK re-keying process.

Frame number 540 is a ping request. However, due to the incomplete re-keying process the ping request is not answered at this time. The bright (green) marked frame 543 in Figure A.16 is the first successfully sent ping request after the completed re-keying process. The granted network access is recognisable through the ping reply in frame 544. The authentication time in this measurement is 20 ms.

A.6 Wi-Fi Alliance - WPA2 statement

The original Wi-Fi Alliance statement concerning WPA2 [198] is given as follows: “Wi-Fi Protected Access 2. The follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the ratified IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1X-based authentication. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA. Like WPA, WPA2 uses the 802.1X/EAP framework as part of the infrastructure that ensures centralized mutual authentication and dynamic key management and offers a pre-shared key for use in home and small office environments. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, multi-band and multi-mode. (See WPA2-Enterprise, WPA2-Personal).”

A.7 Graceful Denial of Service Measurement

The overall GDoS run time is shown in Figure 6.9. The run time of the involved communications between the BPEL process and the web-services according to the

interface 2.1 / 2.2, interface 3.1 / 3.2 and interface 4.1 / 4.2 as shown in Figure 4.14 are presented in the following. Figure A.17 presents the communication between BPEL process and web-service at InfSP which starts at interface 2.1 (and SEF-GDoS REQUEST (step 3) in Figure 4.15) and ends at interface 2.2 (and SEF-GDoS REPLY (step 8) in Figure 4.15).

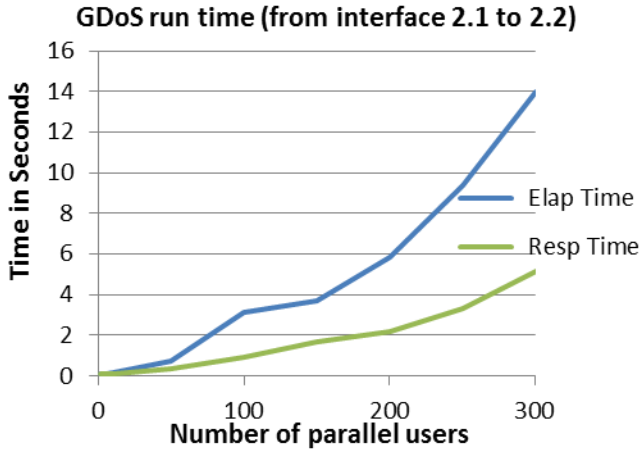


Figure A.17: GDoS run time - measured form interface 2.1 to interface 2.2.

Figure A.18 presents the communication between BPEL process and web-service at ENSP1 which starts at interface 3.1 (and CPF REQUEST - access network characteristic (step 9) in Figure 4.15) and ends at interface 3.2 (and CPF REPLY - access network characteristic (step 11) in Figure 4.15).

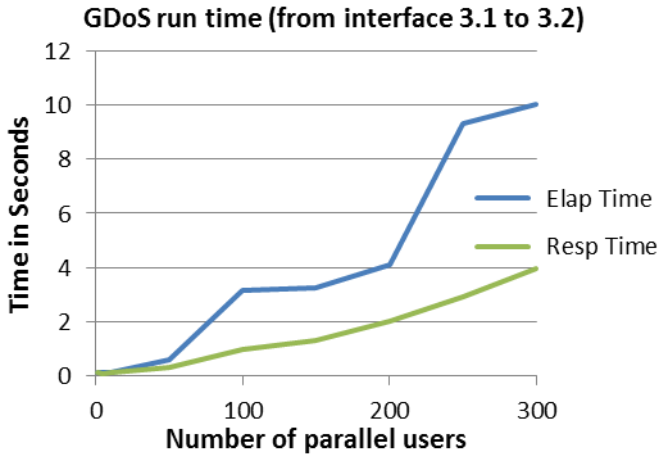


Figure A.18: GDoS run time - measured form interface 3.1 to interface 3.2.

Figure A.19 presents the communication between BPEL process and web-service at ENSP2 which starts at interface 4.1 (and SEF-GDoS REQUEST (step 11) in Figure 4.15) and ends at interface 4.2 (and SEF-GDoS REPLY (step 14) in Figure 4.15).

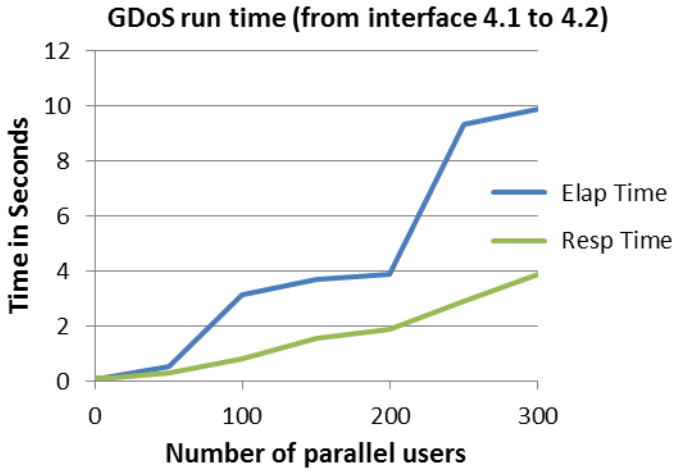


Figure A.19: GDoS run time - measured from interface 4.1 to interface 4.2.