TKK Dissertations 244
Espoo 2010

IMPROVING AND DISTRIBUTING KEY MANAGEMENT ON MOBILE NETWORKS

Doctoral Dissertation

Dan Forsberg

Aalto University
School of Science and Technology
Faculty of Information and Natural Sciences
Department of Computer Science and Engineering

TKK Dissertations 244
Espoo 2010

IMPROVING AND DISTRIBUTING KEY MANAGEMENT ON MOBILE NETWORKS

Doctoral Dissertation

Dan Forsberg

Doctoral dissertation for the degree of Doctor of Science in Technology to be presented with due permission of the Faculty of Information and Natural Sciences for public examination and debate in Auditorium T2 at the Aalto University School of Science and Technology (Espoo, Finland) on the 3rd of December 2010 at 12 noon.

Aalto University
School of Science and Technology
Faculty of Information and Natural Sciences
Department of Computer Science and Engineering

Aalto-yliopisto
Teknillinen korkeakoulu
Informaatio- ja luonnontieteiden tiedekunta
Tietotekniikan laitos

Distribution:
Aalto University
School of Science and Technology
Faculty of Information and Natural Sciences
Department of Computer Science and Engineering
P.O. Box 15400 (Konemiehentie 2)
FI - 00076 Aalto
FINLAND
URL: http://www.cse.tkk.fi/
Tel. +358-9-470 23228
Fax +358-9-470 23293
E-mail: dforsber@gmail.com

ISBN 978-952-60-3420-1
ISBN 978-952-60-3421-8 (PDF)
ISSN 1795-2239
ISSN 1795-4584 (PDF)
URL: http://lib.tkk.fi/Diss/2010/isbn9789526034218/

TKK-DISS-2821

Aalto-Print
Helsinki 2010

Aalto University

ABSTRACT OF DOCTORAL DISSERTATION	AALTO UNIVERSITY SCHOOL OF SCIENCE AND TECHNOLOGY P.O. BOX 11000, FI-00076 AALTO http://www.aalto.fi

Author Dan Forsberg

Name of the dissertation

Improving and Distributing Key Management on Mobile Networks

Manuscript submitted 2010-06-04	Manuscript revised 2010-09-21
Date of the defence 2010-12-03	
☐ Monograph	☒ Article dissertation (summary + original articles)

Faculty	Faculty of Information and Natural Sciences
Department	Department of Computer Science and Engineering
Field of research	Communications Systems and Security
Opponent(s)	Professor Gene Tsudik
Supervisor	Professor Antti Ylä-Jääski
Instructor	Doctor N. Asokan

Abstract

We address the problem of mobile network key management and authentication that negatively affects the handoff performance, adds overhead to the system in terms of key exchange signaling, authentication, and key distribution. We aim to improve the efficiency of the key management subsystem and to reduce investment pressure on core network elements. We address all these problems successfully. Our novel SKC key management mechanism is the best key management mechanism among the ones we found in reducing signaling load from the KD and making the mobility system independent of the AP-KD link delay. It is a significant contribution to the mobile network key management with fast handoffs when separate keys for APs are required and has many useful applications.

Our novel receiver and sender ID binding protocol with symmetric keys is new and shows analogy with Identity Based Cryptography. It is a generalization of the identity binding that SKC is using. Furthermore, our distributed AAA architecture with SKC, certificates, and hardware-based security is a disruptive proposal and show how the mobile network KD can be distributed to the edge nodes.

Our quantitative analysis and comparison of SKC and LTE key management is new and not seen before. Our research affected the LTE Security standardization and contributes to the research and development of home base stations, community and municipal Wi-Fi access points.

Keywords	key management, mobile network security, authentication, fast handovers, key distribution	
ISBN (printed)	978-952-60-3420-1	ISSN (printed) 1795-2239
ISBN (pdf)	978-952-60-3421-8	ISSN (pdf) 1795-4584
Language	English	Number of pages 56 p. + app. 68 p.
Publisher	Department of Computer Science and Engineering	
Print distribution	Department of Computer Science and Engineering	
☒ The dissertation can be read at http://lib.tkk.fi/Diss/2010/isbn9789526034218/		

Aalto-yliopisto

VÄITÖSKIRJAN TIIVISTELMÄ	AALTO-YLIOPISTO TEKNILLINEN KORKEAKOULU PL 11000, 00076 AALTO http://www.aalto.fi

Tekijä Dan Forsberg

Väitöskirjan nimi

Avaintenhallinnan kehittäminen ja hajauttaminen mobiiliverkoissa

Käsikirjoituksen päivämäärä 2010-06-04	Korjatun käsikirjoituksen päivämäärä 2010-09-21
Väitöstilaisuuden ajankohta 2010-12-03	
☐ Monografia	☒ Yhdistelmäväitöskirja (yhteenveto + erillisartikkelit)

Tiedekunta	Informaatio- ja luonnontieteiden tiedekunta
Laitos	Tietotekniikan laitos
Tutkimusala	Tietoliikenneturvallisuus
Vastaväittäjä(t)	Professori Gene Tsudik
Työn valvoja	Professori Antti Ylä-Jääski
Työn ohjaaja	Tohtori N. Asokan

Tiivistelmä

Käsittelemme mobiiliverkkojen avaintenhallinnan ja käyttäjän autentikoinnin ongelmaa, joka negatiivisesti vaikuttaa handoverin tehokkuuteen, lisää systeemin kuormaa mm. avainten neuvottelun ja jakelun ja autentikoinnin ansiosta. Tarkoituksemme on parantaa avaintenhallinen tehokkuutta ja samalla vähentää kasvavia sijoituspaineita ydinverkkoelementteihin. Vastaamme näihin ongelmiin onnistuneesti. Uusi SKC (Session Keys Context) -avaintenhallintamenetelmämme on paras löytämiemme joukossa vähentämään signalointikuormaa ja tekemään verkon liikkuvuudenhallinnan riippumattomaksi tukiaseman ja avaintenjakelijan välisestä linkin viiveestä, olettaen että jokaiselle tukiasemalle vaaditaan erilliset avaimet. Se on merkittävä kontribuutio mobiiliverkkojen avaintenhallintaan nopean liikkuvuudenhallinnan kanssa verkoissa, joissa vaaditaan erilliset avaimet jokaiselle tukiasemalle. SKC:llä on myös monia hyödyllisiä sovelluksia.

Meidän lähettäjän ja vastaanottajan identiteettiin sidottu avaintenneuvotteluprotokollamme symmetristen avainten kanssa on uusi ja analoginen identiteettiin pohjautuvan kryptografian (Identity Based Cryptography , IBC) kanssa. Se on yleistys SKC:n käyttämästä identiteetin sitomisesta. Lisäksi meidän hajautettu AAA arkkitehtuurimme SKC:n, sertifikaattien ja laitteistopohjaisen tietoturvan kanssa on disruptiivinen ehdotus ja näyttää miten äärimmillään mobiiliverkkojen avaintenjakelija voidaan hajauttaa verkon reunaelementteihin.

Meidän kvantitatiivinen analyysimme ja vertailu SKC:n ja LTE:n avaintenhallinnan välillä on uutta, eikä sitä ole nähty aikaisemmin. Tutkimuksemme vaikutti LTE tietoturvan standardointiin ja kontribuoi kotitukiasemien kehitykseen ja tutkimukseen, sekä kommuuni- ja kaupunki WiFi verkkojen langattomiin tukiasemiin.

Asiasanat avaintenhallinta, mobiiliverkkojen tietoturva, autentikointi, nopea liikkuvuudenhallinta

ISBN (painettu) 978-952-60-3420-1	ISSN (painettu) 1795-2239
ISBN (pdf) 978-952-60-3421-8	ISSN (pdf) 1795-4584
Kieli Englanti	Sivumäärä 56 s. + liit. 68 s.

Julkaisija Tietotekniikan laitos

Painetun väitöskirjan jakelu Tietotekniikan laitos

☒ Luettavissa verkossa osoitteessa http://lib.tkk.fi/Diss/2010/isbn9789526034218/

Preface

I have always enjoyed learning and finding out new things, especially about operating systems and Internet communications. I realize I have always been interested in the security aspects of the things I have been studying and working with. There is something sizzling about the ways of hacking, using systems creatively, and building up services.

I thank my instructor N. Asokan and the Nokia Research Center for supporting my doctoral studies and research while working there. I am grateful for my professor and supervisor Antti Ylä-Jääski and HUT who also funded the last miles of this dissertation. I thank Valtteri Niemi, who gave me the opportunity to be part of the LTE.

I thank all my colleagues in Nokia, especially, Dajiang Zhang, Silke Holtmanns, Tiina Koskinen, and all highly expert radio and core system engineers for the great work in security standardization in the past years. I thank my colleagues in Nokia Siemens Networks, especially Günther Horn and Marc Blommaert for a very constructive and professional long-term co-operation on LTE Security design and standardization.

I thank all 3GPP SA working group three (SA3) participants for the exciting and interesting security discussions and especially the evening meetings and late dinners. Special thanks to Alec Brusilovsky, Peter Howard, Karl Norrman, Anand R. Prasad, and Alf Zugenmeier. I warmly remember the numerous deep discussions with my friend Alec related to C-RNTI binding. I remember becoming a fan of sushi during one of the late dinners with Anand et al. I remember the evening Peter was navigating the late session on key management requirements. With Karl I had many nice discussions and ping-pongs. I also remember Alf's support and nice discussions about the specification quality.

I want to thank my family, my parents and sisters, who always encouraged me to study and were proud of me. I want to thank my dear friends with whom I've spent numerous evenings playing and chatting.

Finally, I give my gratitude and high appreciation to God who patiently and gracefully leads me on the path of love, learning, and peace.

Dan Forsberg
Helsinki, October 2009

Contents

List of Publications

This dissertation consists of an overview and of the following publications which are referred to in the text by their Roman numerals.

I Wenhui Hu, Dan Forsberg, *Fast Solutions for AP-to-AP Handoffs*, Proceedings of the 11th Nordic Workshop on Secure IT-systems (NordSec'06), 19 - 20 October 2006, Linköping, Sweden.

II Dan Forsberg, *Protected session keys context for distributed session key management*, Springer Journal of Wireless Personal Communications, Vol. 43, Issue 2, p. 665-676, DOI 10.1007/s11277-007-9271-6, October 2007

III Dan Forsberg, Huang Leping, Kashima Tsuyoshi, Seppo Alanärä, *Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface*, The 18th Annual IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'07). September, 3 - 6, 2007, Athens, Greece

IV Dan Forsberg, *LTE Key Management Analysis with Session Key Context*, Elsevier Journal of Computer Communications, Vol. 33, Issue 16, p. 1907-1915, DOI 10.1016/j.comcom.2010.07.002, October 2010.

V Dan Forsberg, *Use Cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding*, IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM'07), 18 - 21 of June 2007, Helsinki, Finland

VI Dan Forsberg, *Secure Distributed AAA with Domain and User Reputation*, The Third IEEE International Workshop on Trust, Security, and Privacy for Ubiquitous Computing, (TSPUC'07), 18 - 21 of June 2007, Helsinki, Finland

The current author is the main author for all publications, except for publication I. Publication III was written with co-authors. Publication I is background for mobile network key management. Publication II describes new mobile network key management technique called Session Keys Context (SKC), compares it with three other existing techniques, and publication IV compares it with the latest cellular network technology LTE. Publication III describes some security weaknesses in the LTE radio. Publication VI uses the results from publication II to further distribute the AAA functionality to the edges of the mobile networks. Publication V builds on the key derivation techniques used in Publication II for SKC, explores the Identity Based Cryptography (IBC), and creates a new protocol that uses symmetric keys with sender or receiver identity bindings.

Other publications

During the research for this dissertation the author also published the following works that were not included in this dissertation as original publications [1].

Books

- Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller, Valtteri Niemi, *LTE Security*, John Wiley & Sons, ISBN-10: 0470661038, ISBN-13: 978-0470661031, Hard cover, 256 pages, December 2010.

Peer Reviewed Publications

- Le Yanqun, Qing Liu, Dan Forsberg, *Diameter user session update procedure for mobile fast node's fast handoff*, The 7th World Multiconference on Systemics, Cybernetics, and Informatics (SCI'03), July 2003, Orlando, USA.
- Dan Forsberg, *Security Pattern: Privilege Separation*, VikingPlop'05, Helsinki, Finland, 2005.
- Dan Forsberg, *RESTful Security*, Web 2.0 Security and Privacy (W2SP'09), May 2009, Oakland, USA.

Tutorials

- Dan Forsberg, Marc Blommaert, Günther Horn (presenter), *T09: Security for 3GPP's Evolved Packet System — A Fourth Generation System*, IEEE Wireless Communications and Networking Conference (WCNC'09), Budapest, Hungary, Apriil 2009.

IETF Internet-Drafts

- Qing Liu, Yanqun Le, Dan Forsberg, *Diameter User Session Mobility Application*, IETF Internet-Draft, work-in-progress (expired), Feb 2003, URL: http://tools.ietf.org/html/draft-liu-aaa-diameter-session-mobility-00
- D. Forsberg, J. Bournelle, R. Marin Lopez, *PANA Mobility Optimizations with Session Keys Context*, IETF Internet-Draft, work-in-progress (expired), October 2005, URL: http://tools.ietf.org/tools/rfcmarkup/rfcmarkup.cgi?draft=draft-forsberg-pana-skc-00

[1] The list is not author's complete list of publications but contributions published during the research of this dissertation work

- J. Bournelle (Ed.), M. Laurent-Maknavicius, R. Marin Lopez, D. Forsberg, J-M. Combes, *PANA Mobility Optimizations Analysis*, IETF Internet-Draft, work-in-progress (expired), October 2005, URL: http://tools.ietf.org/draft/draft-bournelle-pana-mobopts-analysis/draft-bournelle-pana-mobopts-analysis-00.txt

- D. Forsberg (Ed.), Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, *PANA Mobility Optimizations*, IETF Internet-Draft, work-in-progress (expired), October 2005, URL: http://tools.ietf.org/html/draft-ietf-pana-mobopts-01

- H. Tschofenig, A. Yegin, D. Forsberg, *Bootstrapping RFC3118 Delayed DHCP Authentication Using EAP-based Network Access Authentication*, IETF Internet-Draft, work-in-progress (expired), Jully 2008, URL: http://tools.ietf.org/html/draft-yegin-eap-boot-rfc3118-03

IETF Standards

- D. Forsberg, Y. Ohba (Ed.), B. Patil, H. Tschofenig, A. Yegin, *Protocol for Carrying Authentication for Network Access (PANA)*, IETF RFC 5191 Standards Track, May 2008, URL: http://tools.ietf.org/html/rfc5191

3GPP Standards

- *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 8)*, 3GPP Technical Specification 33.401 v8.4.0, June 2008. URL: http://www.3gpp.org/ftp/Specs/html-info/33401.htm

US Patents

- Forsberg Dan, *Methods, systems, devices and computer program products for providing user-access to broadcast content in combination with short-range communication content*, United States Patent 7,536,151 May 2009

- Forsberg Dan, *Method for moving of flows in communication networks*, United States Patent 7,519,738 April 2009

- Forsberg Dan, *Faster authentication with parallel message processing*, United States Patent 7,458,095 November 2008

- Le Yanqun, Liu Qing, Forsberg Dan, *Session updating procedure for authentication, authorization and accounting*, United States Patent 7,266,100 September 2007

- Forsberg Dan, Yang Fan, *System and method for automatic application profile and policy creation*, United States Patent 7,263,353 August 2007

Author's contribution

This dissertation belongs to the field of computer science and engineering, and to the subfield of systems security and privacy. In this section we summarize the author's contributions to the publications included in this dissertation. In Chapter 3 we further discuss the contributions and their limitations, and compare them with the most significant and recent related work.

Publication I (Fast solutions to AP-to-AP handoffs) The author of this dissertation was tutoring the student in a research seminar at Helsinki University of Technology. The student then became the first author of Publication I. The author introduced the student to the research area and selected related art, helped to formulate the problem statement, and to compare the different mobility mechanisms.

Publication II (Protected Session Keys Context for Distributed Session Key Management) describes a new scalable and flexible key management protocol for mobile networks called Session Keys Context (SKC), and analyses and compares it with three other key management protocols. The SKC protocol is flexible and maintains a balance between memory consumption, and signaling load. It removes the link delay factor between the Access Points and the Key Distributor from the time critical handoff. The paper describes and analyses the results of a simple simulation that compares key request and SKC mechanisms together within a cellular (UMTS) radio stack.

Publication III (Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface) lists new security threats to the LTE radio including several user tracking attacks based on signaling messages, and an active service theft attack based on false buffer status reports. The paper proposes solutions to the different problems in order to mitigate the identified security threats to the LTE radio. The author concentrated on the security problems and mitigations. The author worked together with other co-authors to find out the exact solutions.

Publication IV (LTE Key Management Analysis with Session Keys Context) describes and analyses the LTE Security architecture and key management [5]. The paper compares and quantifies the LTE key management with the Session Keys Context (see publication II). The paper also discusses some implementation alternatives for the LTE key management that maintain compliancy with the LTE over-the-air interface specification.

Publication V (Use cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding) explores the identity based asymmetric cryptography and applies it with symmetric keys. The paper describes a new key establishment protocol that provides implicit authentication based on sender ID, receiver ID, or both sender and receiver ID binding. The paper also provides novel high-level use cases for the protocol, e.g., creating keys for Operations & Management server

clients from a root key and client identity, and partial IP packet level authentication with the help of Domain Name System (DNS) [78, 79, 80, 81].

Publication VI (Secure Distributed AAA with Domain and User Reputation) explores the distribution of a AAA system to the edges of the network without violating the requirements put on the AAA systems. It describes a new distributed AAA architecture based on common hardware security and certificates. The paper describes at high level a community based network access control with user reputation and participation. The system utilizes the SKC solution described in Publication II for allowing access routers to act as AAA servers and clients, and achieving a scalable distributed AAA system.

List of Abbreviations

2G	2nd Generation Cellular Network
3G	3rd Generation Cellular Network
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
AAAF	AAA Foreign server
AAAH	AAA Home server
AK	Authenticated Key establishment
AKE	Authenticated Key Establishment
AP	Access Point
AS	Authentication Server
CA	Certificate Authority
CXTP	Context Transfer Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
ERP	EAP Re-authentication Protocol
eNB	Evolved Node-B (LTE base station)
FMIPv6	Fast handovers for Mobile IPv6
F-HMIPv6	Fast handover in Hierarchical Mobile IPv6
GPS	Global Positioning System
GSM	Global System for Mobile communications
HA	Home Agent
HMIPv6	Hierarchical Mobile IPv6
HOKEY	Handover Keying
HTTP	Hypertext Transfer Protocol
ID	Identity
IBC	Identity Based Cryptography
IAPP	Inter-AP Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPv6	Internet Protocol version 6
KD	Key Distributor
KDC	Key Distribution Center
LTE	Long Term Evolution
MIPv6	Mobile IPv6
MME	Mobility Management Entity
MN	Mobile Node
NIST	National Institute of Standards and Technology
OSI/RM	Open System Interconnection Reference Model
P2P	Peer-to-Peer
PGP	Pretty Good Privacy
RFC	Request for Comments

RK	Roaming Key
RNC	Radio Network Controller
SKC	Session Keys Context
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module
UMTS	Universal Mobile Telecommunications System
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

1 Introduction

Mobile wireless access networks are common around the world, mobile devices are spreading from country to country, and people are using their devices more and more to access Internet web services. Operators'investments in wireless network infrastructures are huge, and the regulators and users require protection for the data that is consumed and exchanged over the wireless networks.

Consequently operators do not want to let users access their networks unless they are paying customers, and users do not want to send their personal information over the air without protection or pay for something that they have not bought or agreed to pay. On the other hand, malicious users want to access the network for free, or anonymously, or masquerading as other users, etc. In short there are multiple incentives to provide access control and data protection for wireless access networks, but also to minimize the effects of compromised network nodes or systems, especially on the edge of the network where the wireless access points may reside in public or home environments. As a result the wireless networks require user authentication and session key management for protecting the signaling and user data.

In this dissertation we focus on session key management for wireless access networks. There are multiple definitions for **key management**. Internet RFC 4949 defines it as follows: "*The process of handling keying material during its life cycle in a cryptographic system; and the supervision and control of that process*" [108]. NIST defines it as, "*The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, counters) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving*" [89, 90], and while the Open System Interconnection Reference Model (OSI/RM) describes it in the following way: "*The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy*" [53].

In this dissertation, however, we use the term key management to mean the mechanisms and rules for creating, distributing, deriving, and using cryptographical keys resulting from an authentication procedure, and we limit it to the scope of mobile networks (e.g., GSM [104, 3], UMTS [58, 2, 88], WLAN (802.11) [52], LTE [106, 5], WiMAX (802.16) [11, 51]) that consists of Mobile Nodes (MN); Access Points (AP); Key Distributors (KD); and an Authentication Server (AS). MNs are mobile devices which have a common radio technology with the APs and, while moving, make handoffs from one AP to another. A simple reference architecture is given in Figure 1.1[2].

[2]In cellular networks the AP is named as radio Base Station (BS), NodeB, or evolved NodeB (eNB), the mobile node as User Equipment (UE) or Mobile Terminal (MT), authentication server such as Home Subscriber Server (HSS), and the key distributor is assigned to some other network node like Mobile Management Entity (MME) in LTE, or Serving GPRS Support Node (SGSN) in UMTS and GSM

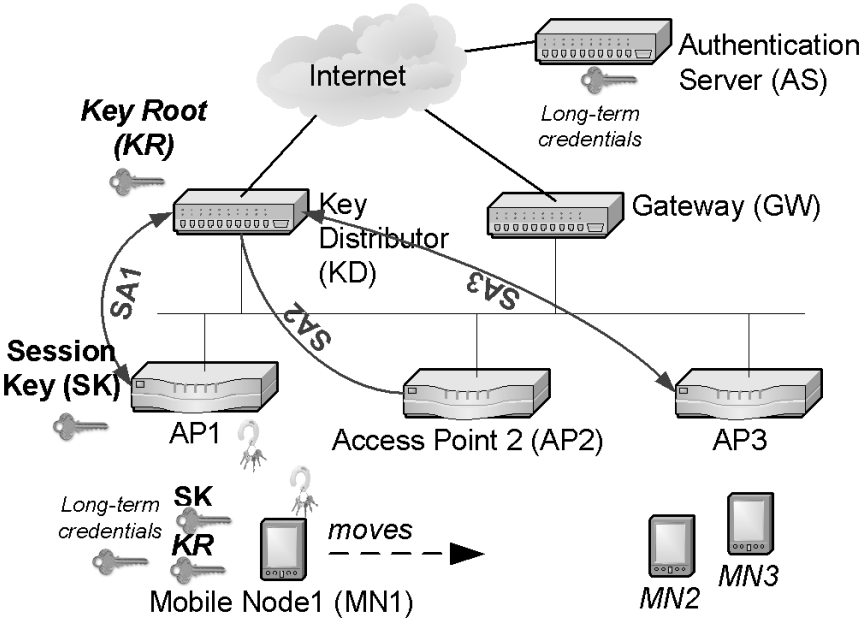

Figure 1.1: Mobile access network reference architecture

1.1 Research Setting

> "*Computer scientists and engineers focus on information, on the ways of representing and processing information, and on the machines and systems that perform these tasks.*" [29] (p. 19)

The **problem** is that the key management and authentication in mobile networks negatively affects the handoff performance, increases time critical overhead in the handoff, and adds overhead to the system in terms of key exchange signaling, authentication, and key distribution. The goal is to find more efficient and secure mobile network key management scheme(s), and to distribute the key distributor functionality to the edges to allow higher key distributor scalability without losing security. In this way the cost and energy efficiency of the key management subsystem is improved by reducing investment pressure on core network elements. Cost efficiency is very important for mobile cellular network operators as the cellular subscription costs for the end users are going down while the data rates are increasing e.g., with 3G modems for laptops. Energy efficiency is also an important issue especially now that global warming has become a worldwide problem.

By key management efficiency we mean that the key management adds minimal delay to the time critical part of the handoff process and in general to the whole system. By distribution we mean that the key management load of the KD can be

shared with other network elements. By scalability we mean that the KD is able to serve more APs and MNs with the same computing and signaling resources.

Key management load includes a number of real-time and non-real-time signaling messages and their processing time. However, we also want to take into account the key management performance requirements set for the network. These include the signaling delay and response time between APs and the KD. Other aspects when evaluating the key management schemes include flexibility in adapting to different types of network deployments and architectures, where signaling delays and links vary.

Vertical handoffs or intersystem mobility issues are outside of the **scope** of this dissertation. Also sensor, ad-hoc, and vehicular networks are not considered. Asymmetric key cryptography is not within the focus of this dissertation as it is still considered too heavy-weight for time critical handoffs. Generally, enabling fast handoffs is a wider common research theme in mobile networks that includes radio level signaling optimizations, handoff predictions, resource pre-allocations, etc.

When **evaluating the results** we answer questions, like "*Does the idea provide a new and more useful capability or greater functionality?*" or "*Is it faster or more efficient?*" [28]. Thus, the **research methodology** is a constructive engineering approach to the problem. We find and explore new solutions and ways of reaching the goal and solving the problem. We compare and analyze the results with previous work and quantify and simulate them.

The nature of the problem does not necessarily require validation with prototyping. Security analysis itself helps to understand the overall effects of key management solutions in the system and to evaluate the different security properties. **Measuring** the effects for system performance and load distribution is also hard, but with analytic comparison and quantitative analysis in relation to related art, general effects can be estimated and concluded.

1.2 Contributions

The dissertation addresses three critical aspects of mobile network key management: distributed and handover efficient key management, decentralized authentication, authorization, and accounting (AAA) architecture, and using key derivations to achieve key separation.

Publications I, **II**, and **IV** discuss about the key management techniques used in mobile networks, especially in the latest mobile network technology called LTE, while **Publication III** concentrates on link layer security issues of the LTE.

Publication V further distributes the key management for mobile networks by utilizing the results in *Publication II* and decentralizing AAA architecture to the edge of the network.

Publication VI generalizes the identity binding mechanisms with similar key derivations used in SKC (*Publication II*) and explores the Identity Based Cryptography (IBC) field.

The main contributions of the dissertation, and of each publication, are the following:

1. Novel distributed and scalable mobile network key management technique called Session Keys Context (SKC) and its comparison with LTE [5]

   (a) **Publication II** describes a new scalable and flexible key management protocol for mobile networks called Session Keys Context (SKC), and analyses and compares it with three other key management protocols.

   It describes and analyses the results of a simple simulation that compares key request and SKC key management mechanisms together within a cellular (UMTS) radio stack.

   The SKC is flexible and can be used to maintain balance between memory consumption and handoff time critical signaling load. It removes the link delay factor between the Access Points and the Key Distributor from the time critical handoffs.

   (b) **Publication III** lists new security threats to the LTE radio including several user tracking attacks based on signaling messages, and an active service theft attack based on false buffer status reports.

   It proposes solutions to the different problems in order to mitigate the identified security threats to the LTE radio.

   (c) **Publication IV** describes and analyses the LTE Security architecture and key management [5], and compares and quantifies the LTE key management with the SKC.

   It discusses implementation alternatives for the LTE key management that maintain compliancy with the LTE over-the-air interface specification.

2. Simple symmetric key establishment protocol with implicit authentication

   (a) **Publication V** explores the identity based asymmetric cryptography and applies it with symmetric keys.

   It describes a new key establishment protocol that provides implicit authentication based on sender ID, receiver ID, or both sender and receiver ID binding. It uses similar key derivations asymmetrically as in *Publication II* with SKC.

   It provides high-level use cases for the protocol, e.g., creating keys for Operations & Management server clients from a root key and client identity, and partial IP packet level authentication with the help of Domain Name System (DNS) [78, 79, 80, 81].

3. Decentralized AAA architecture

   (a) **Publication VI** explores the distribution of a AAA system to the edges of the network without violating the requirements put on the AAA systems.

   It describes a new distributed AAA architecture based on common hardware security and certificates.

   It describes at high level a community based network access control with user reputation and participation.

   The system utilizes the SKC solution described in *Publication II* for allowing access routers to act as AAA servers and clients, and achieving a scalable distributed AAA system.

1.3 Structure of the Thesis

The rest of the dissertation is organized as follows. Chapter 2 provides background on key management requirements and techniques in mobile networks and also lists some cryptographical building blocks used in key management. The contributions of this dissertation are discussed in Chapter 3, and the conclusions with summary in Chapter 4.

The published contributions are presented at the end in separate chapters, *Fast solutions to AP-to-AP handoffs* in Publication I, *Protected Session Keys Context for Distributed Session Key Management* in Publication II, *Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface* in Publication III, *LTE Key Management Comparison with Session Keys Context* in Publication IV, *Use cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding* in Publication V, and *Secure Distributed AAA with Domain and User Reputation* in Publication VI.

2 Key Management Requirements and Mechanisms

2.1 Key Management Requirements for Mobile Networks

There are multiple requirements for key management for mobile networks. The Internet Engineering Task Force (IETF) has created a best current practice document (RFC4962) [45] that describes requirements or guidance for Authentication, Authorization, and Accounting (AAA) [109] key management [30]. IETF has also criteria for evaluating AAA protocols for network access [8]. Also, both WLAN (IEEE 802.11) and WiMAX (IEEE 802.16) follow similar guidelines in their specifications. On the cellular side of the world, the 3rd Generation Partnership Project (3GPP) has defined general security requirements and architectures for the cellular networks like GSM, UMTS, and LTE [1, 4, 7, 5, 6].

The main threat for handover key management is key compromise (e.g., an attacker attacks against an AP to get the keys out of it). To mitigate this threat key separation is required in many levels. Thus, security requirements for handover key management can be summarized in terms of key separation. With key separation we mean cryptographically separate keys where different secret key derivation parameters used (e.g. different secret seeds). In other words keys A and B are separate if key B cannot be derived from key A and key B cannot be derived from key A (based on public parameters or parameters that the key holder has, but not the actual key to be derived). For the key derivation a Key Derivation Function (KDF) is used. KDF must be a one-way function (e.g., a hash function like SHA256).

Partial key separation is achieved if the requirement holds only on one direction but not to the other. In a case when K_1 is used to derive K_2 with a one-way key derivation function, the property K_1—| K_2 holds, but not K_1 |— K_2 (the starting "|" denotes that the key derivation is blocked to that direction; K_1 appears in the key chain before K_2). We call this backward key separation[3] as the key derivation backward in the key chain is blocked. Forward key separation means that K_1 |— K_2 holds, i.e. K_1 cannot be used to derive K_2. When both backward and forward key separations apply, we can denote it as K_1 |—| K_2. The security requirements put on the handover key management, can be summarized as follows:

1. Key separation between access network technologies
2. Key separation between APs
3. Key separation between MNs
4. Key separation between algorithms

[3]Note that this is the reverse of traditional perfect forward secrecy definition

5. Key separation between control and user planes (i.e., signaling messages and user data)

6. Key separation between integrity protection and ciphering

7. Key stream separation between flows and directions (up and downstream)

8. The key stream bits must always be fresh (i.e., the same key stream must not be used twice to integrity protect or cipher the data).

Both the IETF and IEEE require that each AP must not share the same keying material with another AP. GSM does not follow this principle as the same key is transferred between the base stations. UMTS bypasses this requirement by introducing a middle network element above the base stations called the Radio Network Controller (RNC) that terminates the signaling and data protection. The RNC is typically in a physically secure place, which makes it more resistant to physical attacks. As in GSM the RNCs transfer the same keys to the target RNC. Also, during interworking between GSM and UMTS networks the same keys are transferred and thus vulnerabilities in the older GSM network may be imposed to the UMTS network, cf. [73, 72].

The newest 3GPP cellular standard LTE does not have a RNC anymore and signaling and data protection termination happens in the base stations. However, LTE has taken the approach to follow all these requirements.

2.2 Key Management Mechanisms in Mobile Networks

In this section we take a look at the related art of key management in the mobile access networks that aim to fulfill the AAA key management requirements, i.e., especially on how to provide fresh keys for APs.

There are numerous papers on how to speed up re-authentications for MNs. Running the full authentication protocol is not fast enough for handoffs that are time critical (in terms of tens of milliseconds). Hard handoffs are time critical in the sense that the communications channel breaks when the MN switches from the source AP to the target AP (or from source cell to target cell). If the break is big, it negatively affects the quality of real-time services like Voice over IP. With make-before-break handoffs the break can be made smaller as the target AP has been prepared before the actual radio break happens, but the break still remains. The target is to make the handoff as fast as possible and avoid losing any data packets due to the handoff. Since the full authentication protocol run requires signaling to the home Authentication Server (AS) from the access network, the performance is not good enough due to the multiple links and round trips. Also, the load on the AS increases per number of handoffs and MNs and thus is not scalable. The target is to

make the key management scalable with minimum effects on the (critical) handoff signaling time.

When the MN registers on an access network it authenticates itself to the home network (1994) [82]. Typically the home network AS creates a master session key based on the authentication result and derives a further key to be sent to the access network where the MN resides. In the Extensible Authentication Protocol (EAP) key management framework [9] the access network element that gets this key and sends it further to the APs is called Key Distributor (KD) or Key Distribution Center (KDC). The EAP key management framework is a common framework for key management optimizations in the related art along with the WLAN network (802.1X [50]). The MN specific key in the KD is then used as a basis for localized authentications between the access network and the MN. The MN specific key in the KD may also be called root key in the key hierarchy for local key management.

2.2.1 Key Request

Key Request is the simplest form of session key delivery to the AP. The AP sends a key request to the KD when the MN handoffs to it. The KD creates a fresh AP specific session key according to the AAA key management guideline and delivers it to the new AP. A modified mechanism can be used for cases where the handover signaling goes through a centralized element providing the KD functionality (for example a WLAN switch or the MME in EPS). In this case, the source AP sends a key request to the KD along with other mobility signaling, but the KD then sends a fresh key to the target base station, instead of to the source base station. LTE uses this modified key request scheme in S1 handovers and a normal key request mechanism in X2 handovers, except that in X2 handovers the fresh key is used in the next handover and not in the current handover.

One of the newest key-request based protocols is EAP Re-authentication Protocol (ERP) (2008) [85], which originates from the IETF Handover Keying (HOKEY) working group[27]. Xiao and Sarikaya describe some use cases for the ERP (2009) [119] and Marin et al. analyzed and found a replay protection weakness in the HOKEY proposal before the ERP was finalized in (2009) [70].

The key management related delay to the handoff consists of key distribution and authentication, i.e., deriving and getting the right keys to the target AP and taking them into use with the MN. There are proposals to further speed up the handoff by moving the key distribution and part of the authentication away from the time critical handoff-signaling phase. On the other hand, the key request scheme requires a fast KD and a fast link between the KD and the APs, which impacts the network architecture and deployment scenarios. Also, the KD needs to be properly protected from outsiders (compare to WLAN switch).

2.2.2 Pre-distribution

In a **pre-distribution** (or pre-emptive keying) (2003-2004) [12, 75, 77, 60] scenario the KD derives AP specific session keys and distributes them to a number of APs when MN has successfully attached itself to the access network. The specific APs and the number of them included in the pre-distribution scheme can vary (i.e., a certain group of APs) (2004) [77]. This scenario makes the handoff faster as the key is already in the target AP, provided it was in the distribution group of the pre-distribution algorithm.

The main disadvantage of the pre-distribution scheme is that it increases signaling between KD and APs. Also, the KD needs to pre-distribute the keys to the multiple neighboring APs of the MN's current AP, altough the MN may never visit the neighboring APs the keys were pre-distributed to. This way the resources in the APs are wasted and depend on the number of registered MNs in the area. Mishra et al. (2004) [76] use **context pre-distribution** to the neighboring APs from the current AP using neighbor graphs that are generated by the system itself based on handoffs. For example, IETF CXTP [65, 69] and IEEE IAPP [49] protocols can be used between the APs to do the context pre-distribution. The context transfer between APs requires security associations. This is easily handled in intra-domain handoff, but for handoffs between different domains, security associations require co-operation between domain administrators. Bargh et al. (2004) [18] explore this problem space further for intersystem handoffs. Kassab et al. (2008) [61] simulate key pre-distribution with context transfers between APs and conclude that it better supports high velocity MNs compared to the centralized key distribution method from the KD. This may be due to the distributed load to the APs compared to the KD load. However, this depends on the network architecture, i.e., link capacities, propagation delays, and the number of APs per KD.

Prasad and Wang (2005) [103] use a roaming key (RK), derived from the root key to do authentication between the MN and the AP. This way the 802.11i security requirements are met as the RK is used for authentication only and the other derived keys for integrity and confidentiality protection. They do not describe how the roaming key is created from the root key (PMK in 802.11i terms).

Hong et al. (2006) [43] use a two-step **hash key chain** to create new keys from the root key in the KD for new APs. The scheme provides both backward and forward key separation. However, the problem with their setup is that the MN and the network may get out of sync in the key chain derivations, as there are no sequence number indications between the network and the MN. Error identification and recovery is needed. The Hong et al. scheme uses pre-distribution to neighboring APs, but additionally each neighboring AP sends a key request to the KD, increasing the signaling load of the KD significantly. The signaling is multiplied in every handoff because the neighboring APs need to get a new key from the KD after each handoff and cannot use the key they got after the previous handoff. This is a serious weakness in their paper from the KD scalability point of view.

2.2.3 Optimistic Access

Aura and Roe describe a method they call **optimistic access** (2005) [16] in which the network delivers a ticket to the MN. The MN then uses the ticket as a temporary authentication key to get access before the normal authentication procedure is finished with regard to the target AP. This resembles ticket-based methods like the Kerberos (1987) [74, 86] protocol. Ohba and Dutta describe a kerberized handover keying method (2007) [93] in which they also send a ticket to the target AP. Komarova and Riguidel (2007) [63] continue with the same mechanism and use the tickets for fast inter-system roaming and also let the home network provide multiple tickets to multiple visited networks at the same time for the MN.

Kassab et al. (2007) [59] extend the 802.11i key management with a ticket based proactive authentication scheme, where the MN gets a list of neighboring APs from the serving AP and then creates temporary tickets for them. MN sends all the tickets to the serving AP, which then distributes them to the neighboring APs. In a handover the target AP and the MN share a secret that they can use for authentication.

The mechanisms that increase the over-the-air signaling have weaknesses like the complexity of the MN implementation increase, smaller battery life, and increased interoperability testing complexity between terminal and network vendors.

2.2.4 Pre-authentication

Pack and Choi (2002) [94] introduce a **pre-authentication** (2002 - 2009) [94, 91, 92, 95, 110] mechanism where the MN authenticates to multiple APs through a single AP. This way the MN can pre-establish SKs with multiple neighboring APs. This makes the next handoff fast as the keys are already established. However, the MN may have to run pre-authentication with multiple APs as it is not certain which AP the MN will handoff next to. It increases over-the-air signaling (battery life) and AP-to-AP interfaces. Pre-authentication suits well with intersystem handoffs, as the source, and target systems may not support the same key management or authentication mechanisms.

Chien et al. (2008) [26] describe a fast pre-authentication procedure that uses a hash key chain on the KD to create new root keys for target APs. They bind the new target AP key with the link layer addresses of the MN and the target AP, but also add both the MN selected and target AP selected nonces. However, these nonces are not necessary as the hash key chain ensures a fresh key for every handoff. Chien et al. do not find any other reason to use the nonces. Their paper also describes the use of the KD to create a sealed target AP key that is sent to the current AP. The KD seals the secret for the target AP with a target AP specific shared secret. The KD also sends the same secret to the source AP, which can then use this secret to

encrypt the current session key. When the source AP sends the encrypted session key and the sealed target AP secret to the target AP, the target AP is able to unseal the secret and use it to decrypt the session key. This is something similar to what we proposed in our Publication II earlier than Chien. In addition their proposal requires signaling with the KD for each handoff, and seems to be time critical since the MN already knows the target AP identity and no other pre-authentications are done to other APs.

Tseng et al. (2005) [115] propose to use the Global Positionin System (GPS) to predict the next WLAN AP for handoff. However, GPS is not accurate enough (or even unusable) indoors where WLANs are used. What is more, mobility patterns may provide a better estimate of the possible neighboring APs that should be included in the neighboring list. However, GPS could possibly bring some benefit in estimating the next handoff in large cellular networks where cell sizes are geographically large and high velocity MNs have GPS enabled. On the other hand, for fast speed trains, mobility patterns or even just network topology configuration may be simpler.

Our Publication II discusses and compares the key request, pre-distribution, and pre-authentication key management methods further in detail and contrasts them with our new session keys context mechanism.

2.2.5 Public key based

Public key based methods are traditionally not considered because asymmetric cryptographical operations (like decrypting and signing with a secret key of the public key pair) are considered computationally too heavy for mobile devices and radios in which handovers are very time critical. However, public keys can be used for initially authenticating the user and/or terminal [31, 32].

Kim et al. (2007) [62] describe identity based cryptography (IBC) [107] based authentication protocol for mobile networks between MN and AP. Their protocol requires four pairings in elliptic curves and the estimated total time in their example dedicated hardware is 5ms for all four operations. However, dedicated hardware is an additional cost to MN terminals, and also if not run in parallel with other radio handoff procedures is too costly from the total handoff time budget.

3 Improving and Distributing Key Management for Mobile Networks

In this chapter we analyze the contributions of this thesis and highlight the benefits and limitations for mobile network key management. We also contrast the contributions with recent advancements in the research area, and evaluate the results. We start with Publication I and go through all the publications of this thesis.

3.1 Session Keys Context, a Novel Key Management Technique

3.1.1 Fast Solutions to AP-to-AP Handoffs

Summary and contributions. Publication I describes some existing mobility and key management mechanisms for mobile networks and proposes a new approach for authenticated handoffs between APs based on public keys, pre-authentication, and public key caches. Each MN has a public key pair that is used to authenticate the MN for the access network. Optionally, the access network or the AP also has a public key or public key certificate for authentication between APs and even for the MN. The MN and the AP are authenticated before the actual handoff to reduce the time critical signaling during the handoff procedure.

Related art. The paper refers to authentication mechanisms in two Mobile IP [96, 97, 98, 100, 56] extensions, i.e., in Fast Handovers for Mobile IPv6 (FMIPv6)[64], in Hierarchical Mobile IPv6 (HMIPv6) [111], and in their combination called Fast handover in Hierarchical Mobile IPv6 (F-HMIPv6) [57]. All work together with AAA infrastructures [39, 99] that use shared secrets. After that the paper refers to the Kerberos [74] and AP-to-AP credential [16] that both use the MN to deliver keying material or the authorization token for the target AP for successful handoff. Then the paper refers to localized authentications based on different key management mechanisms, namely the key pre-distribution [77, 60] and predictive authentication (or pre-authentication)[94]. Finally the paper refers to authentication between APs [69, 49], meaning that the source AP transfers the keys to the target AP. Note that transferring the same keys to the target AP does not fulfill the AAA key management requirement [45] of having separate keys for different APs.

Discussion and evaluation. The paper uses the term *password based authentication* to mean shared secret based authentication, but this is not critical as the password at high level is a shared secret.

The usage of public keys allows the bypassing of the centralized AAA infrastructure when authenticating the user but requires a public key infrastructure (PKI). However, using only the public keys leaves out the authorization and accounting parts.

On what basis should the authenticated users be authorized to access the network resources? Also, the question arises of how to manage the accounting, i.e., where should the accounting records be stored or sent to? With only PKI infrastructure these are not possible, the AAA infrastructure is also needed. They can be merged of course.

Authorization could be managed on the access network and based on local rules, e.g., based on general contextual information like time and date, but also on user specific history information. From this perspective, Publication VI is a nice follow-up to Publication I and discusses user and domain reputation, i.e., history information about the users. Also, Publication VI discusses AP specific public key certificates, similarly to Publication I, that can be used to authenticate APs to each other. Publication II continues to address the problem statement of improving and distributing key management for mobile networks by describing a new solution.

Accounting is more difficult without a home AAA server as there is no way then to send accounting records to a certain user's *home network*, and thus no entity to send charging records to. Accounting for network access could be simplified if (capped) flat rate charging models become dominant. But then all regulatory requirements for operator networks may not be fulfilled. When public key certificates are considered, the certificate could contain information about where to send the accounting data. But in general the accounting considerations are not the focus of this dissertation as it is a more separate functionality compared to authentication and authorization and happens after them.

From a mobility perspective, the MN must be reachable by corresponding nodes by some means, e.g., by having a home agent [98], anchor point [36, 23], or rendezvous point [83, 66]. These all tend to support network architectures where users have a (virtual) home network, or at least an initial and valid contact point when reachability is required (e.g., compare to offline and online MNs). This is more aligned with AAA infrastructures.

The comparison between the mobility schemes and associated key management methods could have been deeper and more towards quantitative analysis and comparison. There are many issues, as already discussed above, that the paper does not take into account, but which are important when considering the proposal to use public keys. However, the paper identifies the key part of the problem statement of this dissertation and introduces key related-art.

This paper offers some building blocks for achieving the goals of this dissertation. Namely, using the certificates for AP authentication in the network, which is addressed more thoroughly in Publication VI. The mechanism outlined in this paper for pre-authenticated handoffs does not improve the handoff performance compared to other pre-authentication methods as the authentication protocol itself is not computationally more efficient than when using shared keys based authentication methods.

However, as stated in the paper, the public key based authentication method can be easily used to cross the boundaries of network operators.

Notes. The rest of the publications in this dissertation do not consider public key cryptography as a way to do key management for mobile networks as it is considered computationally too heavy-weight and unnecessarily complex for creating session keys in each handoff. For authentication, public keys can be considered e.g., such as in TLS [32], but for time-critical handoffs, even with pre-authentication, doing public key operations with every handoff is not computationally efficient enough compared to symmetric key cryptography. However, with a dedicated hardware public key cryptography may become a viable option for handoffs from a processing speed point of view [55].

3.1.2 Protected Session Keys Context for Distributed Session Key Management

Summary and contributions. This paper describes a new flexible and scalable key management protocol called Session Keys Context (SKC) for mobile wireless networks. It extensively compares SKC with three existing key management mechanisms, i.e., key-request, key pre-distribution, and pre-authentication. In addition the paper shows simple simulation results for key-request and SKC mechanisms. The SKC requires security associations between APs and the KD. For each MN the KD then creates AP specific session keys to be used with each AP into which the MN moves. The KD utilizes the network topology information to create multiple AP specific session keys, encrypting them separately for each AP and sending all the keys to the serving AP. The serving AP then finds its own encrypted session key, decrypts it and uses it for creating further traffic protection keys with the MN (e.g., with a 4-way handshake to ensure key freshness). The SKC contains multiple keys, one for each AP in the area. When handoff occurs, the source AP sends the target AP specific SKC entry to the target AP along with all the other SKC entries. The target AP can then decrypt the AP specific session key and use it with the MN. The MN has a root key, which it uses together with AP identity to derive the AP specific session key. The paper also describes a new way to extend the SKC to also include MN specific AP-to-AP protection keys. The serving AP may also pre-distribute keys to the neighboring APs.

Related art. There are multiple key management methods for mobile networks. The simplest one is key-request, where each AP requests a session key from the KD during the handoff. This is most suitable for cases, where the signaling goes to the KD in every handoff, e.g., as with WLAN APs and WLAN switches. The up-to-date related-art description of key management mechanisms is described in the introduction section as it is the core part of the dissertation. An overview of some of the challenges and issues for next generation systems such as LTE are discussed in (2006) [102].

The SKC extension to protect the AP-to-AP signaling with MN specific keys resembles the Kerberos protocol, which provides tickets that can be used to decrypt the contents. Thus, the SKC has similarities with Kerberos as it contains sealed keys that only certain recipients can open. However, the way the session keys are used and derived and combined in SKC is new as well as the SKC construction and application for mobile networks.

Discussion and evaluation. The MN derives the AP specific session key during the handoff, but the KD has already derived the AP specific session keys and sent them in the SKC to the APs. This way the SKC protocol could be described as a partial and distributed key exchange.

The requirement of having AP specific separate session keys is not always well justified. It is a recommendation in the AAA key management framework [45], and as a security design principle, very good. This key separation can be categorized as both forward and backward key separation. With forward key separation we mean that the serving AP is not able to derive the MN's session key for the target AP. Similarly with backward key separation we mean that the serving AP is not able to derive MN's session key for the previous AP (provided that the current serving AP is not the first AP the MN attached to in the network). Having separate session keys with each AP for all MNs follows the principle that the scope of the session key is kept minimum. Thus, if the session key is compromised in an AP, the scope of the attack is kept to a minimum (in the area of the AP).

The simulation results of the SKC and key-request are not very interesting. The simulation setup is quite simple and the comparison focuses mainly on the size of the keying material that is being transferred between the APs and then also the handoff protocol. The size of the SKC is not very critical either when high-speed backhaul links are used. The radio link scheduling shows up in the simulation as steps on the graphs.

SKC is flexible in the sense that it can be reduced to a key-request scheme when the KD sends only one session key to the AP, namely the session key that is used with the current serving AP. This way the SKC contains only one entry. When the KD increases the number of entries in the SKC, the more memory the SKC requires in the AP, but also the more APs that are covered in the SKC. If the KD has chosen the APs for the SKC wisely, e.g., based on user mobility patterns, there will be no need to request new SKC entries from the KD for a long time. This way the KD can serve more APs in the area. Also, the real-time signaling requirements for the KD are reduced as the SKC entries can be updated before the actual handoffs happen (predictive SKC updates). The paper does not address the issue of mobility patterns and thus more optimized ways of selecting APs for the SKC. This could be studied more. The SKC can be used to balance the memory consumption, real-time signaling load, and general signaling load dynamically. The bigger the SKC is, the more memory is used, and the less signaling happens with the KD.

When the MN moves between two APs, the same session key is used to derive traffic protection keys (e.g., integrity and encryption keys, and optionally even separately for signaling and data traffic). This means that the same traffic protection keys are derived unless the key derivation step includes some randomized parameters. These parameters can, for example, be a random link layer identity or exchanged nonces between the MN and the AP. The paper mentions only nonces.

This paper is a key result in the problem scope of this dissertation. It is the cornerstone of the goal to reach a more scalable and distributed key management for mobile networks. The SKC is also a key component in Publication VI that describes the distributed AAA architecture. The SKC symmetric key derivation mechanism is identity based. This identity binding is further discussed in Publication V, which presents a new authentication and key establishment protocol with implicit sender and receiver ID binding.

3.1.3 Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface

Summary and contributions. This paper lists new security threats on the LTE radio including several user tracking attacks based on signaling messages and an active service theft attack based on false buffer status reports. The paper proposes solutions to the different problems to mitigate the identified security threats on the LTE radio. The author was the editor and main contributor of this publication. The author concentrated on the security problems and mitigations and worked together with other co-authors to find the exact solutions.

Related art. User location privacy is an important and much discussed topic (see e.g., Schilit et al. (2003) [105]. On the other hand, location based services are becoming more common and a core building block for mobile applications and services. When the user location has been identified or mapped to a device identifier, the user or device tracking becomes an issue. Gruteser and Grunwald (2005) [40] enhance the location privacy by proposing to use disposable link layer identifiers in WLAN that uses static link layer identities. Huang L. et al. (2005) [46] propose to enhance wireless location privacy by using a silent period. This means that the station uses a random silent period before continuing communications when it changes to a new link layer identity. Otherwise the attacker is able to correlate between the old and new link layer identity of the same station.

Discussion and evaluation. There are lots of papers related to user privacy, but it is outside the scope of this dissertation. The user tracking and location privacy aspects of radio link layers are not within the scope of this dissertation, but the security analysis of LTE radio in this publication is one part of the security work for the LTE that the author has contributed to the community. The threat mitigations described in the paper use key derivations to create one-time access tokens for the link layer signaling that is not protected by the signaling protection keys. The

token derivation proposal is part of the key management and thus relevant for this dissertation as well.

The paper also shows that security is not perfect and that security measures like key management mechanisms for mobile networks do not cover all security threats. LTE uses network allocated link layer identities in contrast to e.g., 802.11 that uses static station identities on the link layer. However, preventing user tracking based on signaling messages is hard. This paper shows that user tracking can be done in theory in many ways based on signaling message analysis. Related art shows that even radio transmitter fingerprinting can be used to identify devices [114]. Some of these threats can be mitigated, but the added complexity and the required specification and implementation time of the mitigation solutions may not be worth it.

In general active attacks can be hard to resist and a balance between the security measure and cost of a successful attack needs to be found. In this case, a changing radio link identity in each handover, and the network allocation policy for it, seems to be a good enough security measure against user or device tracking. The attacker needs to map the connection with the user ID before tracking can happen. To allow user tracking based on the signaling messages requires that the attacker is close to the radio link and thus can also follow the user based on visual contact.

3.1.4 LTE Key Management Comparison with Session Keys Context

Summary and contributions. This paper describes and analyses the LTE security architecture and key management. At the time of writing this publication, there were no other publications describing the LTE security architecture at this detailed level. The paper compares and quantifies the LTE key management with the Session Keys Context (see Publication II). The paper also discusses some implementation alternatives for the LTE key management that maintain the compliancy with the LTE over-the-air interface specification. This seems to be also the first paper to discuss the implementation alternatives.

Related art. There are not so many publications on LTE Security yet, since the specifications are fresh at the moment. This is one reason why this paper goes through the LTE security architecture at a more detailed level. Prasad et al. (2007) [101] describe LTE key management and mobility at high level in its early stages and mainly push for solutions originating from IETF.

Discussion and evaluation. This publication brings together the new author designed SKC key management mechanism (see Publication II) and the LTE key management that the author was standardizing. The paper compares these together and quantifies the results. This publication is the last one in this dissertation.

The paper analyses the LTE key management and SKC together and thus contrasts the author's contribution to the current cellular network standard. We claim that the

key management with session keys context would have been simpler than the current LTE key management. We also claim that the session keys context provides higher security than LTE key management overall. The X2 handoffs in LTE do not provide forward key separation until two hops, whilst the SKC provides it in all handoff scenarios. We also claim that SKC would have been better suited for different network deployments and implementation options as it can be easily reduced to a plain key request mechanism. However, we also acknowledge that SKC brings more complexity to the KD, and adds requirements on the security associations between the KD and the APs.

3.2 Symmetric Key Establishment Protocol with Implicit Authentication

3.2.1 Use Cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding

Summary and contributions. The paper explores identity based asymmetric cryptography and applies it with symmetric keys. The paper describes a new key establishment protocol that provides implicit authentication based on sender ID, receiver ID, or both sender and receiver ID binding. The paper also provides novel use cases for the protocol, e.g., creating keys for Operations & Management server clients from a root key and client identity, and partial IP packet level authentication with the help of the Domain Name System (DNS) [80, 81].

Related art. The Diffie-Hellman (1976) [33] protocol can be seen as the first key establishment protocol based on public key cryptography. But it does not provide authentication. Protocols that bind together authentication and key establishment are called authenticated key establishment (AK) (2005) [34]. Identity based cryptography (IBC) [107] builds on the basic idea that some unique information about the user is used as the public key (e.g., email address as a string). There are multiple uses for IBC, like an ID-based encryption, signature, and key exchange applications [22, 15, 20]. In the IBC based systems each participant needs to know some public parameters that the keys are based on.

Binding parameters with key derivations functions is a basic building block within key establishment protocols. Binding additional parameters to the key derivation with symmetric keys achieves, for example, channel binding (see e.g., [9]) and reduces the scope of where the keys can be used. Asokan et al. (2003) [14] describe man-in-the-middle attacks on tunneled authentication protocols like the HTTP [37] authentication inside a TLS [32] tunnel. The basic problem is that the authentication protocol running inside the TLS tunnel is not bound to the keys used in the TLS tunnel. In other words the two authentications are not bound to each other at the end points. A solution for this is to require the inner authentication protocol to use

channel binding and bind the keys to the outer secure tunnel at both end points or do re-keying for the outer tunnel based on the inner authentication methods result at both end points.

Shih-I-Huang (2003) [47, 48] presents a simple key derivation based on node identities for reducing the number of keys needed to be stored in sensors for large sensor network deployments. The basic idea is that a node derives a key based on a target node identity and the key it holds. This way the sensor does not have to store the key for the target node. Chan and Perrig describe a key establishment protocol for sensor networks called PIKE (2005) [24]. It reduces the keys needed to be stored in the sensor network to half with the Huang's key derivation method.

Discussion and evaluation. A public key can be readily used to start authenticated and encrypted communications with another party who has the corresponding secret key (see e.g., PGP [120, 38]). However, the communication initiator needs to verify that the public key belongs to the recipient. For this purpose a trusted third party is needed, e.g., a Certificate Authority (CA) that has signed the recipient's public key. In IBC the recipient's identity is used as a public key and a trusted third party is needed to get the right system-wide public parameters for public key creation. The sender and receiver ID binding protocol described in Publication V requires a trusted third party for each authenticated key establishment protocol run. But analogically it also works like IBC in the sense that the sender needs to know only the recipient's identity before starting implicitly authenticated and encrypted communications.

The protocol described in Publication V does not protect against replay attacks because there are no freshness parameters that change over consecutive protocol runs. But this is also similar to what is achieved with public keys. Encrypting a message with a receiver's public key and sending it to the receiver can be replayed. For actual session establishment and data protection, the protocol in Publication V should be extended to support session key negotiation e.g., with exchanged nonces. This is left for further study.

The described use cases in Publication V are at high level and require a lot more work for actual implementation and use case validation. This is left for further study.

This paper contributes to the overall problem statement by showing how the identity binding can be used effectively to derive keys locally. It is a generalization of the key derivation and management ideas of session keys context in Publication II and thus makes the contributions more usable. The two main ideas are identity binding and providing keys for different parties from different parts of the key hierarchy, especially to the communicating parties. This way one peer needs to do more key derivations than the other peer to get to the same level and leaves in the key hierarchy tree.

3.3 Decentralized AAA architecture

3.3.1 Secure Distributed AAA with Domain and User Reputation

Summary and contributions. The paper explores the distribution of a AAA system to the edges of the network without violating the requirements put on AAA systems [8]. The publication splits the problem space of decentralized AAA and addresses these problems separately. Then the paper lists four building blocks that are used for the AAA system distribution. (1) Hardware assisted security (e.g., with Trusted Computing Group's Trusted Platform Module [54] or Mobile Trusted Module [112, 35], ARM TrustZone [10, 13], TI M-Shield [17]) is used for authentication purposes and integrity validation, and reputation mechanisms are used for fine-grained authorization decisions for the usage of the network resources. The system is built on top of (2) two kinds of certificates, domain specific and AP specific. The system also requires (3) AAA backup servers, their discovery and assignment procedures. Finally, the paper suggests using an (4) overlay network among the APs for storing the user profiles. The publication also describes four models on how the certificates can be used to manage control over the system.

Related art. The author, at the time of writing the paper, did not find any other paper that would have tackled the AAA distribution problem in this way, i.e., by actually distributing the AAA server functionality to the edges of the network.

Cellular networks like GSM and UMTS distribute authentication vectors [4] to the visited network so that the visited network can authenticate the user. This is also called delegated authentication. Thus, the authentication procedure is distributed from the home network to the visited network and the signaling to the home network is not in the time critical part of the authentication procedure during the authentication procedure. The home network must trust the visited network before sending the authentication vectors. Until LTE [67, 5, 44], the MN was not able to authenticate the visited network, as the authentication vector in GSM and UMTS is not bound to the visited network identity as in LTE.

Liang and Wang describe a localized AAA control scheme (2004) [68] that allows the visited network to create a local account for the MN and use it for further authentications to remove the load from the real home AAA server. This is not delegated authentication as the visited network becomes like a secondary home network for the user. From the home network point of view, the home network loses the capability to control the number of authentications for the user. Also, the visited network becomes like a secondary home network for the MN, meaning that the MN needs to know when to use the visited network as a secondary home network. This increases complexity and changes the trust models between the visited and home networks.

One of the problems in localized and delegated authentication schemes is that since the authenticated session is not end-to-end between client and the home AAA server,

the home network does not automatically know where the user is and when the user is registered to the network. However, the reachability for the user must be ensured. In GSM/UMTS/LTE the visited network informs the home network about the user's location. In Liang and Wang's localized AAA control scheme something similar needs to be done. In the paper, the distributed AAA architecture is always end-to-end, meaning that there is no reachability problem for the home AAA server, as it always knows where the MN is.

Chang et al. (2007) [25] describe a system with Mobile IP that uses session key sharing between local AAA servers called AAAF. Access networks have multiple AAAFs, which share the MN specific key between them when the MN moves. This is similar to cellular networks like GSM and UMTS where the SGSN provides the ciphering and integrity keys to the next SGSN when MN moves.

Zrelli and Shinoda describe a scheme (2006) [121] that can be used to extend Kerberos to support multiple administrative domains. This is similar to the delegated authentication mechanism, where the home network sends the key to the visited network that the MN also has, except that the MN gets the session key from the home network encrypted with the MN specific key when Kerberos is used.

Ngai and Lyu proposed Certificate Authority (CA) distribution (2006) [87] for wireless ad-hoc networks for a system where public keys are used to authenticate the nodes. They also have the concept of CA reputation, similar to our domain reputation. Their paper also covers the area of CA distribution.

When writing Publication VI, we did not find the following paper from Hecker et al. (2005) [41]. They propose to use a P2P network to store management data of a WLAN AP system. Their Configuration Management P2P-based Access Security System (COMPASS) system does not require any centralized AAA entity. They require the AP to have a signed certificate and bootstrap address for the overlay network. They use a Secure CAN (S-CAN) [42] P2P algorithm with a landmark-ordering method to store data near the APs the data is used with. The WLAN APs can identify their neighbors and get the corresponding link layer identities, which are then used to insert the APs close to each other in the CAN network. This way neighboring APs help each other to store data as they become overlay neighbors and the data retrieval becomes more efficient.

Hecker et al. basically describe a system that has common ideas with our paper, i.e., distributed AAA and secure storage of data for the overlay network. This is encouraging as there are others who have thought about the same problem scope. Hecker et al. do not describe authentication for MNs, for how mobility is solved in general, or multiple autonomous domains as we do. They refer to a paper that describes S-CAN from H.-J. Hof et al. (2004) [42] as a security building block. S-CAN seems to be a useful building block that our ideas can be built upon as well. For example, for finding the candidates for slave AAA servers close to the master AAA server and using the S-CAN secure storage. However, the details are

left for further study as well as the security analysis and suitability of H.-J. Hof et al. proposal.

Tchepnda et al. (2008)[113] describe a multi-hop authentication and credential delivery protocol on layer 2 for vehicular networks based on the EAP authentication protocol and public key infrastructure. They do not consider the AAA server distribution; even though their protocol requires many round trips and public key operations between the client and the AAA server. However, they identified the need to distribute the security functionality and list it as future work.

It is also worth mentioning here the work of Helayos related to autonomic wireless networking (2005) [117] and specifically the methods to create large WiFi deployments working together over IP (2008) [118].

Discussion and evaluation. There are lots of citywide WiFi networks and companies providing infrastructure to build WiFi coverage. These community based networks like FON [116] and SparkNet [84] can benefit from the results of this paper for reducing the authentication server or gateway costs. As of today, FON is preparing to integrate GSM femto base stations into the FON wireless access routers. Their FON router already can host external hard drives and other USB peripherals and can act as a service client in relation to the Internet (like downloading and uploading), allowing the user to close other computers in the household. We believe that the direction in our paper is still a valid and interesting opportunity and that the FON community shares similar ideas. For example, Alcatel-Lucent has an UMTS access router that integrates multiple cellular network elements into one box (2007 - 2009) [19, 21].

The paper addresses the problem of AAA distribution in a constructive way and shows why the distributed AAA architecture described in the paper fulfills the AAA system requirements. The certificate models for both protecting the device integrity and authenticating the domains are also valid. Vendors today use the Internet to update the software of operating systems and applications. Thus, the vendor specific device certificate is not a new idea. However, the AAA master and slave server certificates and their creation or deployment models are new.

The user profile handling and reputation models are described at idea level and are thus a quite lightweight contribution to the paper. There is no validation or background information as to whether this kind of reputation model could actually work in practice.

This paper addresses the distribution part of the problem statement of this dissertation. The AAA architecture is distributed to the APs, but each domain still has a master AAA server and backup AAA server(s). The DNS [71] is used to resolve the backup and master AAA server addresses, and thus it acts as the entry point to the AAA system. The novel key management scheme described in Publication II can be used with this distributed AAA scheme to avoid overloading the master or

backup AAA servers, and thus actually allows them to be deployed in slower and less capable edge network nodes like APs (or wireless access routers).

From this dissertation point of view, broadening the scope of distributed AAA to sensor and vehicular networks would have given more related art to go through. The problem is that both the vehicular and sensor networks have different characteristics than e.g., non-mobile and always-on APs. But there are some synergies in the area of authentication and key agreement. On the other hand, the scope of this dissertation does not cover sensor or ad-hoc networks.

The work in future is to find or create suitable protocols for finding and assigning slave AAA servers, and then registering them to the DNS automatically. Here the paper from Hecker et al. is a nice starting point, i.e., using the overlay network characteristics to find close neighbors.

4 Discussion

Current situation. There have been many papers and standardization efforts in the area of key management for fast handovers already many years back, but only few papers relate to distributing KD and AAA for mobile networks (i.e., not sensor networks). Many papers concentrate on improving one thing, e.g., handoff efficiency but at the same time do not consider KD scalability or signaling efficiency. Some papers propose very complex combinations of different mechanisms in the field but fail to simplify the overall solution. Complex proposals and combinations in many cases come from the fact that an existing system cannot be changed, but patched with minimum effects on the standard (e.g., 802.11). It is important to know the requirements and possible use cases for a protocol and architecture standard when it is being developed. Furthermore, we think that designing extensible protocols is important, but at the same time efficient hardware based implementations must be possible. From a standardization point of view getting the best overall solution is hard as there are multiple parties and differing interests.

Thesis publications. The publications in this dissertation form a combination, but also provide multiple novel research results and topics for further studies. Publication I is not very significant as a whole in the dissertation, but bootstraps the research nicely. The most significant papers in this dissertation are Publication II, V, and VI. They form the core contributions of this dissertation. Publication II describes the novel SKC key management mechanism, and provides an extensive comparison with the other three main key management mechanisms (key request, pre-distribution, and pre-authentication). Publication V takes the ideas in SKC to a more general level, and describes a novel symmetric key identity based key agreement protocol. It also provides some interesting use cases for further studies and evaluation. Publication VI describes the AAA distribution and leverages the benefits of SKC as a suitable distributed key management mechanism for mobile networks. Thus, it extends the SKC usability further and shows its potential with distributed AAA. The last two publications, III and IV, are focused on LTE security research, which was one of the main tasks of the dissertation author while working with this dissertation. Publication III describes security weaknesses in LTE and proposes results related to key management. The last publication concludes the dissertation by showing the differences between SKC and LTE key management. The papers do not overlap each other.

Main results. The SKC is a new key management mechanism that best supports distributed AAA systems, among the various other key management mechanisms. It is also the best mechanism to reduce signaling load from the KD and make the system independent of the AP-KD link delay.

SKC is a significant contribution to mobile key management with fast handoffs when separate keys for APs are required. It supports research for distributed systems and

more cost efficient network architectures. SKC is one of the key enablers for flatter architectures as it removes signaling load from the KD and more importantly AP-KD real-time handoff signaling dependency.

Creating a subscriber specific access controlled mobility area with SKC (AP coverage) is a new idea for authorizing mobility and can be used to create new charging models that are not based on traffic, but on location and access area. Usage of the SKC with mobility patterns and embedding network topology information into the SKC is new. Adding accounting information etc. into the SKC structure is also new, but the details require further research as well as how this mechanism can utilize the overlay networks as a storage.

The receiver and sender ID binding protocol with symmetric keys is new and shows analogy with Identity Based Cryptography. This is also a generalization of the identity binding, which the SKC is also using. The use cases for our protocol are also new and interesting, and can be used for mobile networks. With SKC, for example, the KD could use this protocol for creating keys to seal the AP specific MN's session keys in the SKC. However, the protocol itself does not prohibit replay attacks as it is stateless in nature and mimics the asymmetric key cryptography possibility, where the sender can use the receiver's public key to send encrypted information. Replay protection must be taken care of and analyzed separately. This is left for further study.

Our distributed AAA paper shows that with SKC, certificates, and a hardware based security mobile network, KD can be distributed to the edge nodes (APs) that do not have fast or fat pipes to the Internet. Distributed AAA is one application area for the SKC, but the details require further research and validation. Our distributed AAA architecture is also a simple and novel approach, but requires further validation and analysis. For example the slave AAA selection is not well described and analyzed, but we envisage that there are multiple alternatives for doing this by looking at the p2p algorithms. This is a further research topic.

Our quantitative analysis and comparison of SKC and LTE key management is new and not seen before. Also, the discussion on different implementation alternatives for LTE Security is new, although we think that many vendors do this extensively internally during standardization, implementation, and deployment for different customers.

Learning. SKC did not make it to the LTE. Neither did all the solutions proposed in Publication III that lists security weaknesses in the LTE link layer. However, at a very late stage the requirements of the LTE key management were changed to match with SKC, but at that time the key management protocol was already specified and going back was not possible. The LTE key management was patched with a forward key separation that made it closer to the key request type of protocol and much more dependent on AP-KD delay for each handoff than it was. In LTE, the KD is integrated with the Mobility Management Entity (MME) that takes care

of the location updates from the APs and thus AP-KD delay dependency is not that critical. However, the KD functionality increases the MME load and memory consumption and prevents implementing efficient link layer specific mobility update procedures with multiple base stations, unless less secure horizontal key derivations are used without path switches (i.e., location updates).

LTE base stations have security implementation requirements for the first time in 3GPP history. This reflects the increased trend towards flatter architectures and AP deployments in physically insecure locations (e.g., home base stations, *home eNBs*). This also shows that our research had the right direction and that its contribution is serious input for the future of mobile networks.

Opinions and predictions. As we concluded in the last publication, LTE security is complex and with the SKC would have been a simpler and more efficient system. Disruptive thinking may move the key management load to the edges of the network and thus separate key management and mobility signaling. The KD on the other hand moves towards the core network where it is physically more secure and intra-system mobility happens mostly within the link layer [61].

Femto and home base stations, femto gateways, and WLAN access routers may benefit from having *something to do* with the extra capacity (updating SKC, calculating and optimizing mobility patterns). Relevant research areas for our contributions also include cloud computing and virtualization, municipal/community based Wi-Fi, and the development of home base stations with security implementation requirements. The distributed AAA system can be seen as a cloud of AAA servers that work together to minimize the effects of link delays, server outages, and reachability problems. Our distributed AAA is a direct contribution to the municipal and community based Wi-Fi development as well. Security hardening in base stations with certificates and hardware-based security provides new opportunities for collaborative and distributed systems.

4.1 Summary

We studied how mobile network key management and authentication negatively affect handoff performance, increases time critical overhead in the handoff, and adds overhead to the system in terms of key exchange signaling, authentication, and key distribution. At the same time we wanted to improve the efficiency of the key management subsystem by reducing investment pressure on core network elements. We addressed these problems with success.

Our novel SKC key management mechanism best supports distributed AAA systems among other key management mechanisms. It is the best mechanism to reduce signaling load from the KD and make the system independent of the AP-KD link delay. SKC is a significant contribution to the mobile key management with fast handoffs

when separate keys for APs are required. It supports research for distributed systems and more cost efficient mobile network architectures. Our novel receiver and sender ID binding with symmetric keys is a new protocol and shows analogy with Identity Based Cryptography. This is also a generalization of the identity binding that SKC is using. The use cases for our protocol are also new and interesting, and can be used for mobile networks. Our distributed AAA paper proposes a new architecture that with SKC, certificates, and hardware based security makes it feasible to distribute the mobile network KD to the edge nodes (APs) that do not have fast or fat pipes to the Internet. Distributed AAA is one application area for the SKC and the details require further research and validation. Our quantitative analysis and comparison of SKC and LTE key management is new and not seen before. Also, the discussion on different implementation alternatives for LTE Security is new, although we think that many vendors do this extensively internally during standardization, implementation, and deployment for different customers.

SKC is a contribution to the mobile key management with fast handoffs in the typical case where separate keys for APs are required. It supports distributed systems and more cost efficient network architectures. SKC is one of the key enablers for flatter architectures as it removes signaling load from the KD and more importantly AP-KD real-time handoff signaling dependency. Our new sender and receiver identity binding symmetric key protocol is an optimization mechanism for key management in general and supports the SKC key management for mobile networks.

References

[1] 3GPP. 2002. 3G security; Security threats and requirements. TS 21.133, 3rd Generation Partnership Project (3GPP). URL http://www.3gpp.org/ftp/Specs/html-info/21133.htm.

[2] 3GPP. 2007. General UMTS Architecture. TS 23.101, 3rd Generation Partnership Project (3GPP). URL http://www.3gpp.org/ftp/Specs/html-info/23101.htm.

[3] 3GPP. 2007. GSM/EDGE Radio Access Network (GERAN) overall description; Stage 2. TS 43.051, 3rd Generation Partnership Project (3GPP). URL http://www.3gpp.org/ftp/Specs/html-info/43051.htm.

[4] 3GPP. 2008. 3G security; Security architecture. TS 33.102, 3rd Generation Partnership Project (3GPP). URL http://www.3gpp.org/ftp/Specs/html-info/33102.htm.

[5] 3GPP. 2008. 3GPP System Architecture Evolution (SAE); Security architecture. TS 33.401, 3rd Generation Partnership Project (3GPP). URL http://www.3gpp.org/ftp/Specs/html-info/33401.htm.

[6] 3GPP. 2008. 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses. TS 33.402, 3rd Generation Partnership Project (3GPP). URL http://www.3gpp.org/ftp/Specs/html-info/33402.htm.

[7] 3GPP. 2008. Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE). TR 33.821, 3rd Generation Partnership Project (3GPP). URL http://www.3gpp.org/ftp/Specs/html-info/33821.htm.

[8] B. Aboba, P. Calhoun, S. Glass, T. Hiller, P. McCann, H. Shiino, G. Zorn, G. Dommety, D.Mitton S.Manning M.Beadles P.Walsh X.Chen S.Sivalingham C.Perkins, B.Patil, S.Jacobs B.Lim B.Hirschman A.Hameed, M.Munson, R.Hsu, Y.Xu, E.Campell, S.Baba, and E.Jaques. 2000. Criteria for Evaluating AAA Protocols for Network Access. Number 2989 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc2989.txt.

[9] B. Aboba, D. Simon, and P. Eronen. 2008. Extensible Authentication Protocol (EAP) Key Management Framework. Number 5247 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc5247.txt.

[10] T. Alves and D. Felton. 2004. TrustZone: Integrated Hardware and Software Security – Enabling Trusted Computing in Embedded Systems. Technical report. URL http://www.arm.com/pdfs/TZ_Whitepaper.pdf.

[11] Jeffrey G. Andrews, Arunabha Ghosh, and Rias Muhamed. 2007. Fundamentals of WiMAX: Understanding Broadband Wireless Networking. Prentice Hall PTR, 1 edition. ISBN 0132225522.

[12] William A. Arbaugh. 2003. Handoff Extension to RADIUS. Internet-Draft draft-irtf-aaaarch-handoff-04.txt, Internet Engineering Task Force. URL http://www.watersprings.org/pub/id/draft-irtf-aaaarch-handoff-04.txt. Work in progress.

[13] ARM Ltd. TrustZone Technology Overview. http://www.arm.com/products/esd/trustzone_home.html. URL http://www.arm.com/products/esd/trustzone_home.html.

[14] N. Asokan, Valtteri Niemi, and Kaisa Nyberg. 2003. Man-in-the-Middle in Tunnelled Authentication. In the proceedings of the 11th International Workshop on Security Protocols pages 15—24. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.5.5123.

[15] Giuseppe Ateniese and Breno de Medeiros. 2004. A provably secure Nyberg-Rueppel signature variant with applications. Technical Report 2004/93, Cryptographic ePrint Archive.

[16] Tuomas Aura and Michael Roe. 2005. Reducing Reauthentication Delay in Wireless Networks. In: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, pages 139–148. IEEE Computer Society. ISBN 0-7695-2369-2. URL http://portal.acm.org/citation.cfm?id=1128478.

[17] Jerome Azema and Gilles Fayad. 2008. M-ShieldTM Mobile Security Technology: making wireless secure. Technical report, Texas Instruments Incorporated. URL http://focus.ti.com/pdfs/wtbu/ti_mshield_whitepaper.pdf.

[18] M. S. Bargh, R. J. Hulsebosch, E. H. Eertink, A. Prasad, H. Wang, and P. Schoo. 2004. Fast authentication methods for handovers between IEEE 802.11 wireless LANs. In: Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots, pages 51–60. ACM, Philadelphia, PA, USA. ISBN 1-58113-877-6. URL http://portal.acm.org/citation.cfm?id=1024733.1024741.

[19] Markus Bauer, Peter Bosch, Nidal Khrais, Louis G. Samuel, and Peter Schefczik. 2007. The UMTS base station router. Bell Labs Technical Journal, Special Issue: Wireless Network Technology 11, no. 4, pages 93–111.

[20] Dan Boneh and Matthew K. Franklin. 2001. Identity-Based Encryption from the Weil Pairing. In: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag. ISBN 3-540-42456-3. URL http://portal.acm.org/citation.cfm?id=646766.704155.

[21] Peter Bosch, Alec Brusilovsky, Rae McLellan, Sape Mullender, and Paul Polakos. 2009. Secure base stations. Bell Lab. Tech. J. 13, no. 4, pages 227–243. URL http://portal.acm.org/citation.cfm?id=1527086.

[22] Billy Bob Brumley. 2006. Efficient Three-Term Simultaneous Elliptic Scalar Multiplication with Applications. In: Proceedings of the 11th Nordic Workshop on Secure IT Systems, NordSec'06, pages 105–116. Linköping, Sweden.

[23] Claude Castelluccia. 2000. HMIPv6: A hierarchical mobile IPv6 proposal. SIGMOBILE Mob. Comput. Commun. Rev. 4, no. 1, pages 48–59. URL http://portal.acm.org/citation.cfm?id=360449.360474.

[24] Haowen Chan and A. Perrig. 2005. PIKE: peer intermediaries for key establishment in sensor networks. In: INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, volume 1, pages 524–535. ISBN 0743-166X.

[25] Lin-Huang Chang, Che-Lin Lo, Jui-Jen Lo, Wei-Ting Liu, and Chou-Chen Yang. 2007. Mobility Management with Distributed AAA Architecture. International Journal of Network Security 4, no. 3, pages 241–247.

[26] Hung-Yu Chien, Tzu-Hang Hsu, and Yuan-Liang Tang. 2008. Fast preauthentication with minimized overhead and high security for WLAN handoff. W. Trans. on Comp. 7, no. 2, pages 46–51. URL http://portal.acm.org/citation.cfm?id=1457917.

[27] T. Clancy, M. Nakhjiri, V. Narayanan, and L. Dondeti. 2008. Handover Key Management and Re-Authentication Problem Statement. Number 5169 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc5169.txt.

[28] Committee on Academic Careers for Experimental Computer Scientists, National Research Council. 1994. Academic careers for experimental computer scientists and engineers. ISBN 978-0-309-04931-3.

[29] Computer Science and Telecommunications Board. 1992. Computing the Future. National Academy Press, Washington, D.C.

[30] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, and D. Spence. 2000. Generic AAA Architecture. Number 2903 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc2903.txt.

[31] T. Dierks and C. Allen. 1999. The TLS Protocol Version 1.0. Number 2246 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc2246.txt. Obsoleted by RFC 4346, updated by RFC 3546.

[32] T. Dierks and E. Rescorla. 2008. The Transport Layer Security (TLS) Protocol Version 1.2. Number 5246 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc5246.txt.

[33] W. Diffie and M. Hellman. 1976. New directions in cryptography. Information Theory, IEEE Transactions on 22, no. 6, pages 644–654.

[34] Ratna Dutta and Rana Barua. 2005. Overview of Key Agreement Protocols. Technical Report 2005/289, Cryptology ePrint Archive. URL http://eprint.iacr.org/2005/289.ps.

[35] Jan-Erik Ekberg and Markku Kylänpää. 2007. Mobile Trusted Module (MTM) – an introduction. Technical report, Nokia Research Center, http://research.nokia.com/files/NRCTR2007015.pdf.

[36] E. Fogelstroem, A. Jonsson, and C. Perkins. 2007. Mobile IPv4 Regional Registration. Number 4857 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc4857.txt.

[37] J. Franks, P. Hallam-Baker, J. Hostetler, P. Leach, A. Luotonen, E. Sink, and L. Stewart. 1997. An Extension to HTTP : Digest Access Authentication. Number 2069 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc2069.txt. Obsoleted by RFC 2617.

[38] Simson Garfinkel. 1995. PGP: Pretty Good Privacy. O'Reilly Media, Inc. ISBN 1565920988, 9781565920989.

[39] S. Glass, T. Hiller, S. Jacobs, and C. Perkins. 2000. Mobile IP Authentication, Authorization, and Accounting Requirements. Number 2977 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc2977.txt.

[40] Marco Gruteser and Dirk Grunwald. 2005. Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis. Mobile Networks and Applications 10, no. 3, pages 315–325. URL http://dx.doi.org/10.1007/s11036-005-6425-1.

[41] Artur Hecker, Erik-Oliver Blass, and Houda Labiod. 2005. COMPASS: Decentralized Management and Access Control for WLANs. In: Personal Wireless Communications PWC'05 - Proceedings of the 10th IFIP International Conference, pages 197–204. Colmar, France. URL http://eproceedings.worldscinet.com/9781860947315/9781860947315_0022.html.

[42] Hans-Joachim Hof, Erik-Oliver Blass, Thomas Fuhrmann, and Martina Zitterbart. 2004. Design of a Secure Distributed Service Directory for Wireless Sensornetworks. In: Wireless Sensor Networks, pages 276–290. URL http://www.springerlink.com/content/mpar2cb1qptky4mh.

[43] Kihun Hong, Souhwan Jung, and S. Wu. 2006. A Hash-Chain Based Authentication Scheme for Fast Handover in Wireless Network. In: Information Security Applications, pages 96–107. URL http://dx.doi.org/10.1007/11604938_8.

[44] Günther Horn, Dan Forsberg, and Marc Blommaert. 2009. Tutorial 09: Security for 3GPP's Evolved Packet System - A Fourth Generation System. In: IEEE Wireless Communications and Networking Conference, WCNC'09. Budapest.

[45] R. Housley and B. Aboba. 2007. Guidance for Authentication, Authorization, and Accounting (AAA) Key Management. Number 4962 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc4962.txt.

[46] Leping Huang, K. Matsuura, H. Yamane, and K. Sezaki. 2005. Enhancing wireless location privacy using silent period. In: Wireless Communications and Networking Conference, 2005 IEEE, volume 2, pages 1187–1192 Vol. 2. ISBN 1525-3511.

[47] Shi-I Huang. 2003. Adaptive random key distribution schemes for wireless sensor networks. In: Computer Security in the 21st Century. Taipei, Taiwan.

[48] Shi-I Huang, Shiuhpyng Shieh, and S.Y. Wu. 2005. Adaptive random key distribution schemes for wireless sensor networks. Springer US, Taipei, Taiwan. ISBN 978-0-387-24005-3 (Print) 978-0-387-24006-0 (Online), 91-105 pages.

[49] IEEE. 2003. IEEE trial-use recommended practice for multi-vendor access point interoperability via an inter-access point protocol across distribution systems supporting ieee 802.11 operation.

[50] IEEE. 2004. IEEE 802.1X-2004 IEEE Standard for Local and Metropolitan Area Networksâ Port-Based Network Access Control. IEEE.

[51] IEEE. 2004. IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems.

[52] IEEE. 2007. 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.

[53] International Organization of Standardizaion (ISO). 1989. ISO 7498-2: 1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. URL http://www.iso.org/iso/catalogue_detail.htm?csnumber=14256.

[54] International Organization of Standardizaion (ISO). 2009. Information technology – Trusted Platform Module – Part 1: Overview. URL http://www.iso.org/iso/catalogue_detail.htm?csnumber=50970.

[55] Kimmo Järvinen, Juha Forsten, and Jorma Skyttä. 2007. FPGA Design of Self-certified Signature Verification on Koblitz Curves. In: Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems, pages 256–271. Springer-Verlag, Vienna, Austria. ISBN 978-3-540-74734-5. URL http://portal.acm.org/citation.cfm?id=1421989.

[56] D. Johnson, C. Perkins, and J. Arkko. 2004. Mobility Support in IPv6. Number 3775 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc3775.txt.

[57] HeeYoung Jung and SeokJoo Koh. 2004. Fast handover support in hierarchical mobile IPv6. In: Advanced Communication Technology, 2004. The 6th International Conference on, volume 2, pages 551–554.

[58] Heikki Kaaranen. 2005. UMTS networks. John Wiley and Sons. ISBN 0470011033, 9780470011034.

[59] M. Kassab, J.M. Bonnin, and K. Guillouard. 2007. Securing fast handover in WLANs: a ticket based proactive authentication scheme. In: Globecom Workshops, 2007 IEEE, pages 1–6.

[60] Mohamed Kassab, Abdelfettah Belghith, Jean-Marie Bonnin, and Sahbi Sassi. 2005. Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks. In: Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling, pages 46–53. ACM, Montreal, Quebec, Canada. ISBN 1-59593-183-X. URL http://portal.acm.org/citation.cfm?id=1089737.1089746.

[61] Mohamed Kassab, Safaa Hachana, Jean Marie Bonnin, and Abdelfettah Belghith. 2008. High-mobility effects on WLAN fast re-authentication efficiency. In: Proceedings of the 5th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, pages 1–6. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Hong Kong. ISBN 978-963-9799-26-4. URL http://portal.acm.org/citation.cfm?id=1535641.

[62] Yoohwan Kim, Wei Ren, Ju-Yeon Jo, Yingtao Jiang, and Jun Zheng. 2007. SFRIC: A Secure Fast Roaming Scheme in Wireless LAN Using ID-Based Cryptography. In: Communications, 2007. ICC '07. IEEE International Conference on, pages 1570–1575.

[63] Maryna Komarova and Michel Riguidel. 2007. Optimized ticket distribution scheme for fast re-authentication protocol (fap). In: Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks, pages 71–77. ACM, Chania, Crete Island, Greece. ISBN 978-1-59593-806-0. URL http://portal.acm.org/citation.cfm?id=1298239.1298253.

[64] R. Koodli. 2005. Fast Handovers for Mobile IPv6. Number 4068 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc4068.txt. Obsoleted by RFC 5268.

[65] Rajeev Koodli and Charles E. Perkins. 2001. Fast handovers and context transfers in mobile networks. SIGCOMM Comput. Commun. Rev. 31, no. 5, pages 37–47. URL http://portal.acm.org/citation.cfm?id=1037113.

[66] J. Laganier and L. Eggert. 2008. Host Identity Protocol (HIP) Rendezvous Extension. Number 5204 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc5204.txt.

[67] Pierre Lescuyer and Thierry Lucidarme. 2008. Evolved packet system (EPS). John Wiley and Sons. ISBN 0470059761, 9780470059760.

[68] Wei Liang and Wenye Wang. 2004. A local authentication control scheme based on AAA architecture in wireless networks. In: Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, volume 7, pages 5276–5280 Vol. 7. ISBN 1090-3038.

[69] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli. 2005. Context Transfer Protocol (CXTP). Number 4067 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc4067.txt.

[70] Rafa Marin, Pedro Fernandez, and Antonio Gomez. 2009. 3-Party Approach for Fast Handover in EAP-Based Wireless Networks. In: On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, pages 1734–1751. URL http://dx.doi.org/10.1007/978-3-540-76843-2_43.

[71] M. Mealling and R. Daniel. 2000. The Naming Authority Pointer (NAPTR) DNS Resource Record. Number 2915 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc2915.txt. Obsoleted by RFCs 3401, 3402, 3403, 3404.

[72] Ulrike Meyer and Susanne Wetzel. 2004. A Man-in-the-Middle Attack on UMTS. In: Proceedings of ACM Workshop on Wireless Security (WiSe 2004). ACM.

[73] Ulrike Meyer and Susanne Wetzel. 2004. On the impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks. In: Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2004). IEEE.

[74] S. P Miller, B. C Neuman, J. I Schiller, and J. H Saltzer. 1987. Kerberos authentication and authorization system. http://eprints.kfupm.edu.sa/47456/. URL http://eprints.kfupm.edu.sa/47456/.

[75] A Mishra, M Shin, W Arbaugh, I Lee, and K Jang. 2003. Proactive Key Distribution to support fast and secure roaming. Technical report, IEEE 802.11 Working Group, IEEE-03-084r1-I. URL http://www.ieee802.org/11/Documents/DocumentHolder.

[76] A. Mishra, M. Shin, and W.A. Arbaush. 2004. Context caching using neighbor graphs for fast handoffs in a wireless network. In: INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, volume 1, page 361. ISBN 0743-166X.

[77] A. Mishra, Min Ho Shin, N.L. Petroni, T.C. Clancy, and W.A. Arbaugh. 2004. Proactive key distribution using neighbor graphs. Wireless Communications, IEEE 11, no. 1, pages 26–36.

[78] P.V. Mockapetris. 1983. Domain names: Concepts and facilities. Number 882 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc882.txt. Obsoleted by RFCs 1034, 1035, updated by RFC 973.

[79] P.V. Mockapetris. 1983. Domain names: Implementation specification. Number 883 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc883.txt. Obsoleted by RFCs 1034, 1035, updated by RFC 973.

[80] P.V. Mockapetris. 1987. Domain names - concepts and facilities. Number 1034 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc1034.txt. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592.

[81] P.V. Mockapetris. 1987. Domain names - implementation and specification. Number 1035 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc1035.txt. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2845, 3425, 3658, 4033, 4034, 4035, 4343.

[82] R. Molva, D. Samfat, and G. Tsudik. 1994. Authentication of mobile users. Network, IEEE 8, no. 2, pages 26–34.

[83] R. Moskowitz and P. Nikander. 2006. Host Identity Protocol (HIP) Architecture. Number 4423 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc4423.txt.

[84] MP-MasterPlanet Oy. SparkNET, Corporate and municipal Wi-Fi. http://www.sparknet.fi/. URL http://www.sparknet.fi/.

[85] V. Narayanan and L. Dondeti. 2008. EAP Extensions for EAP Reauthentication Protocol (ERP). Number 5296 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc5296.txt.

[86] B.C. Neuman and T. Ts'o. 1994. Kerberos: an authentication service for computer networks. Communications Magazine, IEEE 32, no. 9, pages 33–38.

[87] Edith C. H. Ngai and Michael R. Lyu. 2006. An Authentication Service Based on Trust and Clustering in Wireless Ad Hoc Networks: Description and Security Evaluation. In: Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, SUTC'06, pages 94–103. IEEE Computer Society. ISBN 0-7695-2553-9-01. URL http://portal.acm.org/citation.cfm?id=1137083.

[88] Valtteri Niemi and Kaisa Nyberg. 2003. UMTS security. John Wiley and Sons. ISBN 0470847948, 9780470847947.

[89] NIST. 2001. Security Requirements for Cryptographic Modules, FIPS PUB 140-2. URL http://csrc.nist.gov/groups/STM/cmvp/standards.html. With change notice 4, 3 December 2002.

[90] NIST. 2003. Recommendation for Key Management, Part 1 General Guideline and Part 2 Best Practices for Key Management Organization, Special Publication 800-57, DRAFT.

[91] Y. Ohba. 2009. Pre-authentication Support for PANA. Internet-Draft draft-ietf-pana-preauth-06, Internet Engineering Task Force. URL http://www.ietf.org/internet-drafts/draft-ietf-pana-preauth-06.txt. Work in progress.

[92] Y. Ohba and G. Zorn. 2009. Extensible Authentication Protocol (EAP) Early Authentication Problem Statement. Internet-Draft draft-ietf-hokey-preauth-ps-09, Internet Engineering Task Force. URL http://www.ietf.org/internet-drafts/draft-ietf-hokey-preauth-ps-09.txt. Work in progress.

[93] Yoshihiro Ohba, Subir Das, and Ashutosh Dutta. 2007. Kerberized handover keying: a media-independent handover key management architecture. In: Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture, pages 1–7. ACM, Kyoto, Japan. ISBN 978-1-59593-784-8. URL http://portal.acm.org/citation.cfm?id=1366932.

[94] Sangheon Pack and Yanghee Choi. 2002. Fast Inter-Ap Handoff Using Predictive Authentication Scheme in a Public Wireless LAN. In: In proceedings of IEEE Networks conference (confunction of IEEE ICN and IEEE ICWLHN). URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.20.138.

[95] Sangheon Pack and Yanghee Choi. 2002. Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model.

IFIP TC6 Personal Wireless Communications pages 175—182. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.19.9564.

[96] C. Perkins. 1996. IP Mobility Support. Number 2002 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc2002.txt. Obsoleted by RFC 3220, updated by RFC 2290.

[97] C. Perkins. 2002. IP Mobility Support for IPv4. Number 3220 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc3220.txt. Obsoleted by RFC 3344.

[98] C. Perkins. 2002. IP Mobility Support for IPv4. Number 3344 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc3344.txt. Updated by RFC 4721.

[99] C. Perkins and P. Calhoun. 2005. Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4. Number 3957 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc3957.txt.

[100] Charles E. Perkins. 1997. Mobile IP: Design Principles and Practices. Prentice Hall PTR. ISBN 0201634694.

[101] A. R Prasad, J. Laganier, A. Zugenmaier, M. Bargh, B. Hulsebosch, E. H Eertink, G. J Heijenk, and J. Idserda. 2007. Mobility and key management in SAE/LTE. http://eprints.eemcs.utwente.nl/10930/. URL http://eprints.eemcs.utwente.nl/10930/.

[102] Anand Prasad. 2006. The Future Re-Visited. Wireless Personal Communications 37, no. 3, pages 187–211. URL http://dx.doi.org/10.1007/s11277-006-9035-8.

[103] A.R. Prasad and H. Wang. 2005. Roaming key based fast handover in WLANs. In: Wireless Communications and Networking Conference, 2005 IEEE, volume 3, pages 1570–1576 Vol. 3. ISBN 1525-3511.

[104] M. Rahnema. 1993. Overview of the GSM system and protocol architecture. Communications Magazine, IEEE 31, no. 4, pages 92–100.

[105] B. Schilit, J. Hong, and M. Gruteser. 2003. Wireless location privacy protection. Computer 36, no. 12, pages 135–137.

[106] Stefania Sesia, Issam Toufik, and Matthew Baker. 2009. LTE, The UMTS Long Term Evolution. John Wiley and Sons. ISBN 0470697164, 9780470697160.

[107] Adi Shamir. 1985. Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., Santa Barbara, California, United States. ISBN 0-387-15658-5. URL http://portal.acm.org/citation.cfm?id=19483.

[108] R. Shirey. 2000. Internet Security Glossary. Number 2828 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc2828.txt. Obsoleted by RFC 4949.

[109] Nicolas Sklavos, Spyros Denazis, and Odysseas Koufopavlou. 2007. AAA and mobile networks: security aspects and architectural efficiency. In: Proceedings of the 3rd international conference on Mobile multimedia communications, pages 1–4. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Nafpaktos, Greece. ISBN 978-963-06-2670-5. URL http://portal.acm.org/citation.cfm?id=1385343.

[110] Dirk Balfanz Smetters, Dirk Balfanz, D. K Smetters, Paul Stewart, and H. Chi Wong. 2002. Talking To Strangers: Authentication in Ad-Hoc Wireless Networks. In: Proceedings of Network and Distributed System Security Symposium NDSS'02. San Diego. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.16.1408.

[111] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier. 2008. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. Number 5380 in Request for Comments. IETF. URL http://www.ietf.org/rfc/rfc5380.txt.

[112] TCG Mobile Working Group. 2007. TCG Mobile Trusted Module Sepecification Version 1 rev. 1.0. URL https://www.trustedcomputinggroup.org/specs/mobilephone/tcg-mobile-trusted-module-1.0.pdf.

[113] C. Tchepnda, H. Moustafa, H. Labiod, and G. Bourdon. 2008. A Layer-2 Multi-Hop Authentication and Credential Delivery Scheme for Vehicular Networks. In: Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, pages 1–6. ISBN 1930-529X.

[114] J. Toonstra and W. Kinsner. 1996. A radio transmitter fingerprinting system ODO-1. In: Electrical and Computer Engineering, 1996. Canadian Conference on, volume 1, pages 60–63 vol.1.

[115] Chien-Chao Tseng, Kuang-Hui Chi, Ming-Deng Hsieh, and Hung-Hsing Chang. 2005. Location-based fast handoff for 802.11 networks. Communications Letters, IEEE 9, no. 4, pages 304–306.

[116] Martin Varsavsky and FON Team. FON, Large WiFi Community and Social Router. http://www.fon.com/. URL http://www.fon.com/.

[117] Hector Velayos. 2005. Autonomic wireless networking. Ph.D. thesis, Royal Institute of Technology (KTH).

[118] Hector Velayos and Gunnar Karlsson. 2008. A Distribution System for Large Scale IEEE 802.11 Wireless LANs. Transylvania, Romania.

[119] X. Zheng and B. Sarikaya. 2009. Handover keying and its uses. Network, IEEE 23, no. 2, pages 27–34.

[120] Philip R. Zimmermann. 1995. The official PGP user's guide. MIT Press. ISBN 0262740176, 9780262740173.

[121] Saber Zrelli and Yoichi Shinoda. 2006. Single sign-on framework for AAA operations within commercial mobile networks. In: Proceedings of the First International Conference on Availability, Reliability and Security, pages 74–81. IEEE Computer Society. ISBN 0-7695-2567-9. URL http://portal.acm.org/citation.cfm?id=1130912.

ISBN 978-952-60-3420-1
ISBN 978-952-60-3421-8 (PDF)
ISSN 1795-2239
ISSN 1795-4584 (PDF)