WILEY

Second Edition

LTE Security

Dan Forsberg | Günther Horn
Wolf-Dietrich Moeller | Valtteri Niemi

LTE SECURITY

LTE SECURITY

Second Edition

Dan Forsberg
Poplatek Oy, Finland

Günther Horn
Nokia Siemens Networks, Germany

Wolf-Dietrich Moeller
Nokia Siemens Networks, Germany

Valtteri Niemi
University of Turku and Nokia Corporation, Finland

WILEY
A John Wiley & Sons, Ltd., Publication

This edition first published 2013

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

LTE security / Gunther Horn . . . [et al.]. – 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-118-35558-9 (cloth)
1. Long-Term Evolution (Telecommunications) 2. Global system for mobile communications.
I. Horn, Gunther.
TK5103.48325.L74 2013
621.3845′6–dc23
2012025771

A catalogue record for this book is available from the British Library.

ISBN: 9781118355589

Set in 10/12pt Times by Laserwords Private Limited, Chennai, India

Contents

Preface

This is the second edition of the book *LTE Security* whose first edition appeared in the autumn of 2010.

Since 2010, LTE has established itself as the unrivalled mobile broadband technology of the fourth generation (4G), with significant commercial deployments around the world and a fast-growing market. The subject of this book is hence even more relevant than it was at the time of the first edition.

The basic specifications for LTE in general, and LTE security in particular, have proven remarkably stable since their first versions were published in 2008 as part of 3GPP Release 8. Nevertheless, as is quite common in the standardization process, a number of corrections to the LTE security specifications have been agreed since to fix shortcomings that had become apparent during the development and deployment processes.

More importantly, new features have been added to LTE to enhance support for new types of deployment scenarios and applications. From a security point of view, the most important of these additions are the support for relay nodes and for machine-type communications. We therefore devote two new chapters to them.

A number of other new features have been added to LTE security since 2010, one example being the addition of a third family of cryptographic algorithms for LTE. These new features have been added to the chapters that had existed already in the first edition of the book.

This book focuses on LTE security, but also gives a thorough introduction to its predecessors, GSM security and 3G security. The second edition updates the reader on recent developments in these areas. While things were quite calm on the 3G security front, confidence in the strength of some cryptographic algorithms used with GSM has been further eroded by live hacking demonstrations at a number of public events. These developments suggest that it is now time to take those stronger GSM algorithms into use that have already been standardized and are available in products.

Some of the topics mentioned in the last chapter of the first edition that provided an outlook have matured in the meantime and been included in the other chapters of the book. The outlook has been updated accordingly.

Summing up, this second edition includes the following updates with respect to the first edition:

- Two new chapters, on relay nodes and machine-type communications, have been added.

- All enhancements to LTE security specified for 3GPP Releases 10 and 11 have been included.
- All corrections to the specifications up to and including Release 11 and approved by 3GPP by June 2012 have been taken into account as far as they affect the text in the book.
- Major developments since 2010 affecting GSM security and 3G security are explained.
- The last chapter of the book providing an outlook to future developments has been updated.

Foreword to the First Edition

The early to mid-1980s saw the commercial opening across Europe of public-access mobile communications systems. These cellular systems all used analogue technology, but outside of the Nordic countries no attempt was made to standardize the systems – so the technology adopted differed from country to country. Unfortunately, one thing they did have in common was a total absence of adequate security features, which made them open to abuse by criminals, journalists and all manner of opportunists. Users' calls could be eavesdropped on the air using readily available and comparatively inexpensive interception devices, and there were celebrated cases of journalistic invasion of privacy. A well-known example was the 'squidgy' tapes, where mobile telephone calls between members of the British royal family were recorded. Mobile telephone operators and their customers became very concerned.

The operators also had another problem with serious financial consequences. When a mobile phone attempted to connect to a network, the only check made on authenticity was to see that the telephone number and the phone's identity correctly corresponded. These numbers could be intercepted on the air and programmed to new phones creating clones of the original. Clones were used by criminals to run up huge charges for calls which had nothing to do with the legitimate owner. Cloning became very widespread, with criminals placing their 'cloning' equipment in cars parked at airports to capture the numbers from business people announcing their arrival back home to their families. It represented a serious financial problem for operators who ended up covering the charges themselves. The problems caused by lack of security in European analogue systems were a significant factor in accelerating the creation and adoption of GSM.

GSM is a standard for digital mobile communications, designed originally for Europe but now adopted all over the world. Being an international standard it brings economy of scale and competition, and it enables users to roam across borders from one network to another. Being digital it brings transmission efficiency and flexibility, and enables the use of advanced cryptographic security. The security problems of the original analogue systems are addressed in GSM by encryption on the air interface of user traffic, in particular voice calls, and authentication by network operators of their customers on an individual basis whenever they attempt to connect to a network, irrespective of where that network may be. From both a technical and a regulatory perspective, the use of cryptography in GSM was groundbreaking. Initially manufacturers and operators feared it would add too much complexity to the system, and security agencies were concerned that it may be abused by criminals and terror organizations. The legitimate fears and concerns constrained what was possible, especially with the encryption algorithm, which was designed against a philosophy of ‘minimum strength to provide adequate security’. Despite this, and the continuing efforts of organized hackers, eavesdropping on the air of GSM calls protected using the original cipher has still to be demonstrated in a real deployment, and with a stronger cipher already available in the wings, any future success will be largely pointless. This doesn’t mean that GSM is free from security weaknesses – the ability to attack it using false base stations is very real.

GSM is the first in an evolving family of technologies for mobile communications. The second member of the family is 3G (or UMTS, as it is often referred to in Europe) and the third, and most recent, is LTE EPS to give it its proper title which is used throughout the main body of this book). With each technology evolution the security features have been enhanced to address learning from its predecessor, as well as to accommodate any changes in system architecture or services. The underlying GSM security architecture has proved to be extremely robust, and consequently has remained largely unchanged with the evolving technology family. It has also been adapted for use in other communications systems, including WLAN, IMS and HTTP. It is characterized by authentication data and encryption key generation being confined to a user’s home network authentication centre and personal SIM, the two elements where all user-specific static security data is held. Only dynamic and user session-specific security data goes outside these domains.

3G sees the addition to the GSM security features of user authentication of the access network – to complement user authentication by the network, integrity protection of signalling and the prevention of authentication replay. Start and termination of ciphering are moved from the base station further into the network. Of course, the false base station attack is countered. A new suite of cryptographic algorithms based on algorithms open to public scrutiny and analysis is introduced, and changes of regulation governing the export of equipment with cryptographic functionality make their adoption easier for most parts of the world.

LTE heralds the first technology in the family that is entirely packet-switched – so voice security has to be addressed in an entirely different way from GSM and 3G. LTE is a much flatter architecture, with fewer network elements, and is entirely IP-based. Functionality, including security functionality, is migrated to the edge of the network, including encryption functionality which is moved to the edge of the radio network, having been moved from the base station to the radio network controller in the evolution from GSM to 3G. While maintaining compatibility with the security architecture developed for GSM and evolved for 3G, the security functionality has been significantly adapted, enhanced and extended to accommodate the changes that LTE represents, as well as security enhancements motivated by practical experience with 3G. Much of this plays back into 3G itself as new security challenges arise with the advent of femto cells – low-cost end nodes in exposed environments that are not necessarily under the control of the operator of the network to which they are attached.

The book takes the reader through the evolution of security across three generations of mobile, focussing with clarity and rigour on the security of LTE. It is co-authored by a team who continue to be at the heart of the working group in 3GPP responsible for defining the LTE security standards. Their knowledge, expertise and enthusiasm for the subject shine through.

Professor Michael Walker
Chairman of the ETSI Board

Acknowledgements

This book presents the results of research and specification work by many people over an extended period. Our thanks therefore go to all those who helped make Long Term Evolution (LTE) possible through their hard work. In particular, we thank the people working in 3GPP, the standardization body that publishes the LTE specifications, and, especially, the delegates to the 3GPP security working group, SA3, with whom we were working to produce the LTE security specifications over the past years.

We would also like to express our gratitude to our colleagues at Nokia and Nokia Siemens Networks for our longstanding fruitful collaboration. We are particularly indebted to N. Asokan, Wolfgang Bücker, Devaki Chandramouli, Jan-Erik Ekberg, Christian Günther, Silke Holtmanns, Jan Kåll, Raimund Kausl, Rainer Liebhart, Christian Markwart, Kaisa Nyberg, Martin Öttl, Jukka Ranta, Manfred Schäfer, Peter Schneider, Hanns-Jürgen Schwarzbauer, José Manuel Tapia Pérez, Janne Tervonen, Robert Zaus and Dajiang Zhang who helped us improve the book through their invaluable comments.

Finally, we would like to thank the editing team at Wiley whose great work turned our manuscript into a coherent book.

The authors welcome any comments or suggestions for improvements.

Copyright Acknowledgements

The authors would like to include additional thanks and full copyright acknowledgement as requested by the following copyright holders in this book.

Please see the individual figure and table captions and the footnotes to extracts from 3GPP specifications for copyright notices throughout the book.

1

Overview of the Book

Mobile telecommunications systems have evolved in a stepwise manner. A new cellular radio technology has been designed once per decade. Analogue radio technology was dominant in the 1980s and paved the way for the phenomenal success of cellular systems. The dominant second-generation system Global System for Mobile Communications (GSM, or 2G) was introduced in the early 1990s, while the most successful third-generation system, 3G – also known as the Universal Mobile Telecommunications System (UMTS), especially in Europe – was brought into use in the first years of the first decade of the new millennium.

At the time of writing, the fourth generation of mobile telecommunications systems is being commercially deployed. Its new radio technology is best known under the acronym LTE (Long Term Evolution). The complete system is named SAE/LTE, where SAE (System Architecture Evolution) stands for the entire system, which allows combining access using the new, high-bandwidth LTE technology with access using the legacy technologies such as GSM, 3G and High Rate Packet Data (HRPD). The technical term for the SAE/LTE system is Evolved Packet System (EPS), and we shall be using this term consistently in the book. The brand name of the new system has been chosen to be LTE, and that is the reason why the title of the book is *LTE Security*.

With the pervasiveness of telecommunications in our everyday lives, telecommunications security has also moved more and more to the forefront of attention. Security is needed to ensure that the system is properly functioning and to prevent misuse. Security includes measures such as encryption and authentication, which are required to guarantee the user's privacy as well as ensuring revenue for the mobile network operator.

The book will address the security architecture for EPS. This is based on elements of the security architectures for GSM and 3G, but it needed a major redesign effort owing to the significantly increased complexity, and new architectural and business requirements. The book will present the requirements and their motivation and then explain in detail the security mechanisms employed to meet these requirements.

To achieve global relevance, a communication system requires world-wide interoperability that is easiest to achieve by means of standardization. The standardized part of the system guarantees that the entities in the system are able to communicate with each other even if they are controlled by different mobile network operators or manufactured

LTE Security, Second Edition. Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller and Valtteri Niemi.

by different vendors. There are also many parts in the system where interoperability does not play a role, such as the internal structure of the network entities. It is better not to standardize wherever it is not necessary because then new technologies can be introduced more rapidly and differentiation is possible among operators as well as among manufacturers, thus encouraging healthy competition.

As an example in the area of security, communication between the mobile device and the radio network is protected by encrypting the messages. It is important that we standardize how the encryption is done and which encryption keys are used, otherwise the receiving end could not do the reverse operation and recover the original content of the message. On the other hand, both communicating parties have to store the encryption keys in such a way that no outsider can get access to them. From the security point of view, it is important that this be done properly but we do not have to standardize how it is done, thus leaving room for the introduction of better protection techniques without the burden of standardizing them first. The emphasis of our book is on the standardized parts of EPS security, but we include some of the other aspects as well.

The authors feel that there will be interest in industry and academia in the technical details of SAE/LTE security for quite some time to come. The specifications generated by standardization bodies only describe *how* to implement the system (and this only to the extent required for interoperability), but almost never inform readers about *why* things are done the way they are. Furthermore, specifications tend to be readable by only a small group of experts and lack the context of the broader picture. This book is meant to fill this gap by providing first-hand information from insiders who participated in decisively shaping SAE/LTE security in the relevant standardization body, 3rd Generation Partnership Project (3GPP), and can therefore explain the rationale for the design decisions in this area.

The book is based on versions of 3GPP specifications from March 2012 but corrections approved by June 2012 were still taken into account. New features will surely be added to these specifications in later versions and there will most probably also be further corrections to the existing security functionality. For the obvious reason of timing, these additions cannot be addressed in this book.

The book is intended for telecommunications engineers in research, development and technical sales and their managers as well as engineering students who are familiar with architectures of mobile telecommunications systems and interested in the security aspects of these systems. The book will also be of interest to security experts who are looking for examples of the use of security mechanisms in practical systems. Both readers from industry and from academia should be able to benefit from the book. The book is probably most beneficial to advanced readers, with subchapters providing sufficient detail so that the book can also be useful as a handbook for specialists. It can also be used as textbook material for an advanced course, and especially the introductory parts of each chapter, when combined, give a nice overall introduction to the subject.

The book is organized as follows. Chapter 2 gives the necessary background information on cellular systems, relevant security concepts, standardization matters and so on. As explained earlier, LTE security relies heavily on security concepts introduced for the predecessor systems. Therefore, and also to make the book more self-contained, Chapters 3–5 are devoted to security in legacy systems, including GSM and 3G, and security aspects of cellular–WLAN (Wireless Local Area Network) interworking.

Chapter 6 provides an overall picture of the EPS security architecture. The next four chapters provide detailed information about the core functionalities in the security architecture. Chapter 7 is devoted to authentication and key agreement which constitute the cornerstones for the whole security architecture. Chapter 8 shows how user data and signalling data are protected in the system, including protecting confidentiality and integrity of the data. A very characteristic feature in cellular communication is the possibility of handing over the communication from one base station to another. Security for handovers and other mobility issues is handled in Chapter 9. Another cornerstone of the security architecture is the set of cryptographic algorithms that are used in the protection mechanisms. The algorithms used in EPS security are introduced in Chapter 10.

In the design of EPS, it has been taken into account already from the beginning how interworking with access technologies that are not defined by 3GPP is arranged. Also, interworking with legacy 3GPP systems has been designed into the EPS system. These two areas are discussed in detail in Chapter 11.

The EPS system is exclusively packet based; there are no circuit-switched elements in it. This implies, in particular, that voice services have to be provided on top of Internet Protocol (IP) packets. The security for such a solution is explained in Chapter 12.

Partially independently of the introduction of EPS, 3GPP has specified solutions that enable the deployment of base stations covering very small areas, such as in private homes. This type of base station may serve restricted sets of customers (e.g. people living in a house), but open usage in hotspots or remote areas is also envisaged. These home base stations are also planned for 3G access, not only for LTE access. Such a new type of base station may be placed in a potentially vulnerable environment not controlled by the network operator and therefore many new security measures are needed, compared to conventional base stations. These are presented in detail in Chapter 13.

Chapter 14 introduces the security for relay nodes, a new feature introduced in Release 10 of 3GPP specifications. Relay nodes enable extensions for network coverage.

Chapter 15 addresses machine-type communication (MTC), also called machine-to-machine communication. The chapter provides an introduction to MTC security at the network level, the application level and the level of managing security credentials. First enhancements for the benefit of MTC appeared in 3GPP Release 10, after which further enhancements were done in Release 11 and still more are in the pipeline for Release 12. These all are discussed in the chapter.

Finally, Chapter 16 contains a discussion of both near-term and far-term future challenges in the area of securing mobile communications.

Many of the chapters depend on earlier ones, as can be seen from the descriptions given here. However, it is possible to read some chapters without reading first all of the preceding ones. Also, if the reader has prior knowledge of GSM and 3G systems and their security features, the first four chapters can be skipped. This kind of knowledge could have been obtained, for example, by reading the book *UMTS Security* [Niemi and Nyberg 2003]. The major dependencies among the chapters of the book are illustrated in Figure 1.1.

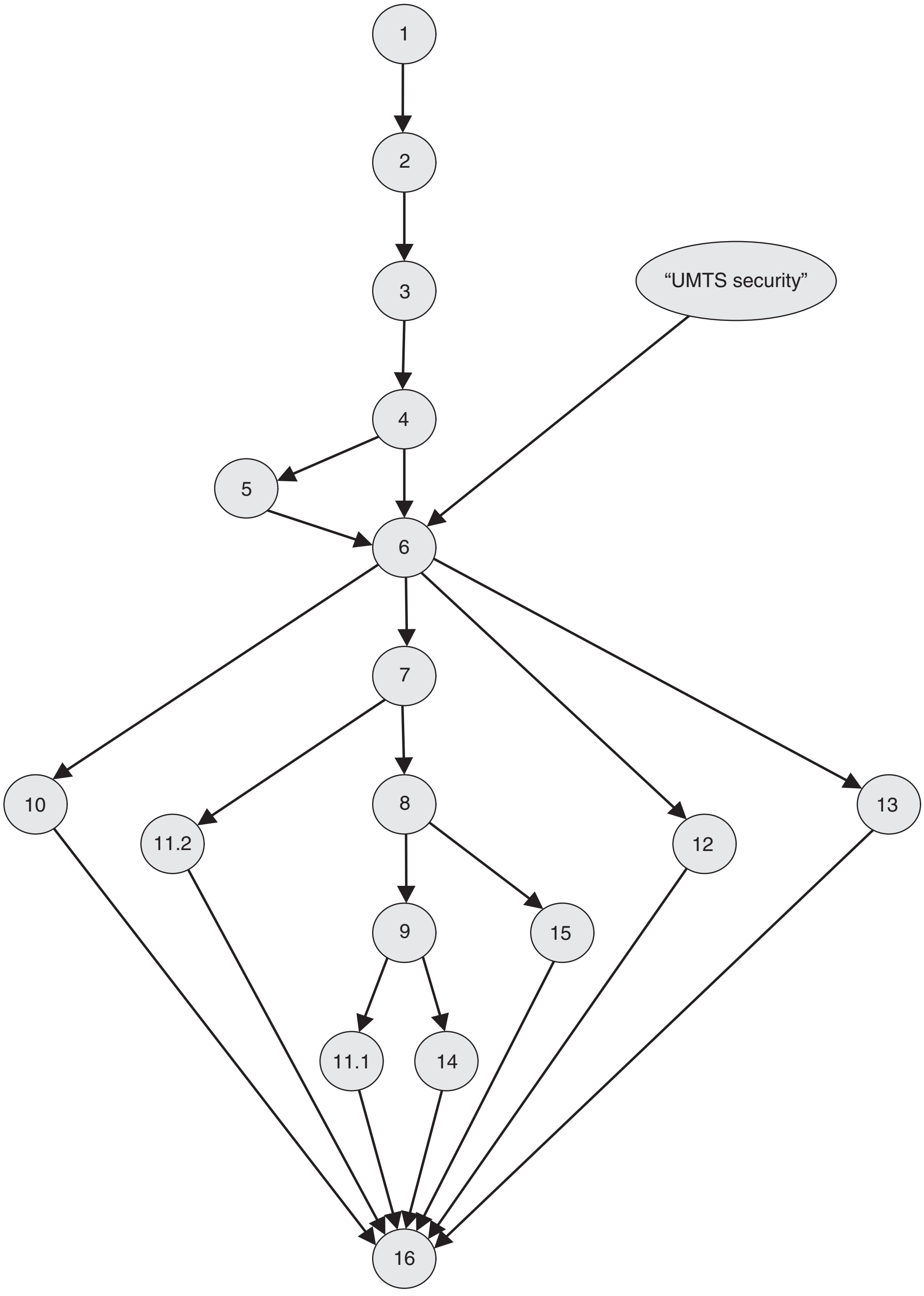

Figure 1.1 Major dependencies among chapters.

2

Background

2.1 Evolution of Cellular Systems

Mobile communications were originally introduced for military applications. The concept of a cellular network was taken into commercial use much later, near the beginning of the 1980s, in the form of the Advanced Mobile Phone System (AMPS) in the United States and in the form of the Nordic Mobile Telephone system (NMT) in northern Europe. These first-generation cellular systems were based on analogue technologies. Simultaneous access by many users in the same cell was provided by the Frequency Division Multiple Access (FDMA) technique. Handovers between different cells were already possible in these systems, and a typical use case was a phone call from a car.

The second generation of mobile systems (2G) was introduced roughly a decade later, at the beginning of the 1990s. The dominant 2G technology has been the Global System for Mobile (GSM) communications, with more than 3.5 billion users worldwide at the time of writing. The second generation introduced digital information transmission on the radio interface between the mobile phone and the base station (BS). The multiple access technology is Time Division Multiple Access (TDMA).

The second generation provided an increased capacity of the network (owing to more efficient use of radio resources), better speech quality (from digital coding techniques) and a natural possibility for communicating data. Furthermore, it was possible to use new types of security feature, compared to analogue systems.

Again roughly one decade later, at the beginning of the twenty-first century, the third-generation (3G) technologies were introduced. Although GSM had become a phenomenal success story already at that point, there were also other successful 2G systems, both in Asia and in North America. One of the leading ideas for 3G was to ensure fully global roaming: to make it possible for the user to use the mobile system services anywhere in the world. A collaborative effort of standards bodies from Europe, Asia and North America developed the first truly global cellular technologies in the 3rd Generation Partnership Project (3GPP). At the time of writing, there are almost half a billion 3G subscriptions in the world.

LTE Security, Second Edition. Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller and Valtteri Niemi.

The third generation provided a big increase in data rates, up to 2 Mbps in the first version of the system that was specified in Release 99 of 3GPP. The multiple-access technology is Wideband Code Division Multiple Access (WCDMA).

Both GSM and 3G systems were divided into two different domains, based on the underlying switching technology. The circuit-switched (CS) domain is mainly intended for carrying voice and short messages, while the packet-switched (PS) domain is mainly used for carrying data traffic.

One more decade passed, and the time was ripe for taking another major step forward. In 3GPP the development work was done under the names of Long Term Evolution (LTE) of radio technologies and System Architecture Evolution (SAE). Both names emphasized the evolutionary nature of this step, but the end result is in many respects a brand new system, both from the radio perspective and from the system perspective. The new system is called Evolved Packet System (EPS) and its most important component, the new radio network, is called Evolved Universal Terrestrial Radio Access Network (E-UTRAN).

The EPS contains only a PS domain. It offers a big increase in data rates, up to more than 100 Mbps. The multiple-access technology is again based on FDMA, namely, Orthogonal Frequency Division Multiple Access (OFDMA) for the downlink traffic (from the network to the terminal) and Single Carrier Frequency Division Multiple Access (SC-FDMA) for the uplink traffic (from the terminal to the network).

2.1.1 Third-Generation Network Architecture

In this section, we give a brief overview of the 3GPP network architecture. A more thorough description of the 3G architecture can be found elsewhere [Kaaranen *et al*. 2005].

A simplified picture of the 3GPP Release 99 system is given in Figure 2.1.

The network model consists of three main parts, all of which are visible in Figure 2.1. The part closest to the user is the terminal, which is also called the User Equipment (UE). The UE has a radio connection to the Radio Access Network (RAN), which itself is connected to the Core Network (CN). The CN takes care of coordination of the whole system.

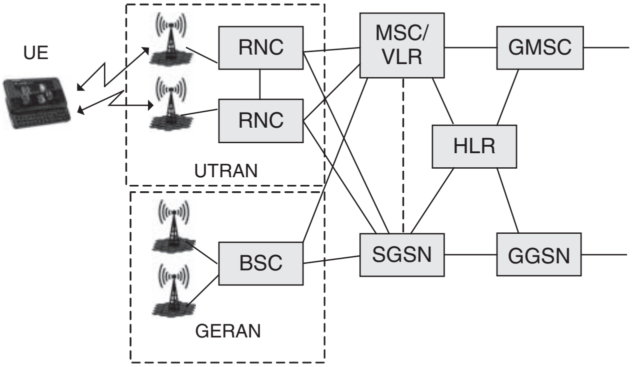

Figure 2.1 The 3G system.

The CN contains the PS domain and the CS domain. The former is an evolution of the General Packet Radio Service (GPRS) domain of the GSM system, and its most important network elements are the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). The CS domain is an evolution from the original CS GSM network with the Mobile Switching Centre (MSC) as its most important component.

In addition to the various network elements, the architecture also defines interfaces or, more correctly, reference points between these elements. Furthermore, protocols define how different elements are able to communicate over the interfaces. Protocols involving the UE are grouped into two main strata: the Access Stratum (AS) contains protocols that are run between the UE and the access network, while the Non-Access Stratum (NAS) contains protocols between the UE and the CN. In addition to these two, there are many protocols that are run between different network elements.

The CN is further divided into the home network and the serving network. The home network contains all the static information about the subscribers, including the static security information. The serving network handles the communication to the UE (via the access network). If the user is roaming, then the home and the serving network are controlled by different mobile network operators.

2.1.2 Important Elements of the 3G Architecture

The UE consists of two parts: the Mobile Equipment (ME) and the Universal Subscriber Identity Module (USIM). The ME is typically a mobile device that contains the radio functionality and all the protocols that are needed for communications with the network. It also contains the user interface, including a display and a keypad. The USIM is an application that is run inside a smart card called Universal Integrated Circuit Card (UICC) [TS31.101]. The USIM contains all the operator-dependent data about the subscriber, including the permanent security information.

There are two types of RAN in the 3G system. The UTRAN is based on WCDMA technology and the GSM/EDGE Radio Access Network (GERAN) is an evolution of GSM technology.

The RAN contains two types of element. The BS is the termination point of the radio interface on the network side, and it is called Node B in the case of UTRAN and Base Transceiver Station (BTS) in GERAN. The BS is connected to the controlling unit of the RAN, which is the Radio Network Controller (RNC) in UTRAN or the Base Station Controller (BSC) of GERAN.

In the CN, the most important element in the CS domain is the switching element MSC that is typically integrated with a Visitor Location Register (VLR) that contains a database of the users currently in the location area controlled by the MSC. The Gateway Mobile Switching Centre (GMSC) takes care of connections to external networks, an example being the Public Switched Telephone Network (PSTN). In the PS domain, the role of MSC/VLR is taken by the SGSN, while the GGSN takes care of connecting to Internet Protocol (IP) services within the operator network and to the outside world, such as the Internet.

The static subscriber information is maintained in the Home Location Register (HLR). It is typically integrated with the Authentication Centre (AuC) that maintains the permanent security information related to subscribers. The AuC also creates temporary authentication and security data that can be used for security features in the serving network, such as authentication of the subscriber and encryption of the user traffic.

In addition to the elements mentioned here and illustrated in Figure 2.1, there are many other components in the 3G architecture, an example being the Short Message Service Centre (SMSC) that supports storing and forwarding of short messages.

2.1.3 Functions and Protocols in the 3GPP System

The main functionalities in the 3GPP system are:

- Communication Management (CM) for user connections, such as call handling and session management,
- Mobility Management (MM) covering procedures related to user mobility, as well as important security features and
- Radio Resource Management (RRM) covering, for example, power control for radio connections, control of handovers and system load.

The CM functions are located in the NAS, while RRM functions are located in the AS. The MM functions are taken care of by both the CN and the RAN.

The division into user plane and control plane (also called signalling plane) defines an important partition among the protocols. User plane protocols deal, as the name indicates, with the transport of user data and other directly user-related information, such as speech. Control plane protocols are needed to ensure correct system functionality by transferring necessary control information between elements in the system.

In a telecommunication system, in addition to the user and control planes, there is also a management plane that, for example, keeps all elements of the system in operation. Usually, there is less need for standardization in the management plane than there is for the user plane and the control plane.

The most important protocols for the Internet are IP, User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). In the wireless environment there is a natural reason to favour UDP over TCP: fading and temporary loss of coverage make it difficult to maintain reliable transmission of packets on a continuous basis. There is also a 3GPP specific protocol that is run on top of UDP/IP. This is the GPRS Tunnelling Protocol (GTP). It has been optimized for data transfer in the backbone of the PS domain.

The interworking of the different types of protocol can be illustrated by a typical use case: a user receiving a phone call. First the network pages for the user. Paging is an MM procedure; the network has to know in which geographical area the user could be found. After the user has successfully received the paging message, the radio connection is established by RRM procedures. When the radio connection exists, an authentication procedure may follow, and this belongs again to the MM. Next the actual call set-up (CM procedure) occurs during which the user may be informed about who is calling. During the call there may be many further signalling procedures, such as for handovers. At the end of the call, the call is first released by a CM procedure and after that the radio connection is released by the RRM.