



LTE key management analysis with session keys context

Dan Forsberg*

Aalto University, School of Science and Technology, Department of Computer Science and Engineering, P.O. Box 15400, FI-00076 Aalto, Finland

ARTICLE INFO

Article history:

Available online 7 July 2010

Keywords:

LTE security
Key management
Handovers
Session keys context
Key separation

ABSTRACT

Handover key management in mobile wireless networks targets to minimize the effects of a possible key compromise in the access points. We describe and analyze how the new 3GPP Long Term Evolution (LTE) security architecture and handover keying management fulfills this target. We discuss possible LTE handover key management enhancements and implementation alternatives without losing interoperability over the air interface. We have chosen to compare it with our session keys context concept to see what the strengths in both are to get some perspective for deployments that benefit from distributed key management.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

Key management for wireless mobile networks has been an active topic. In the past IEEE groups like 802.11 Task Group R, 802.21, and 802.16 (WiMAX) have been working to improve and specify key management techniques. Extensible Authentication Protocol (EAP) working group in the IETF has been working with key hierarchies and key derivation issues [1,2]. IETF PANA (Protocol for carrying Authentication for Network Access) working group has been tackling the issue of mobility optimizations for the PANA protocol [3–5]. Handover keying working group (HOKEY) is also working on efficient key management for handovers [2,6–9].

One of the key requirements in the key management area is to have cryptographically separate keys for every Access Point (AP) [10]. There are different proposals to fulfill this requirement, which is important especially in cases when the encryption of the user plane data packets terminates in the AP (e.g. in LTE, WiMAX, WLAN, and GSM), and not deeper in the network (e.g. like in UMTS). The requirement stems from the threat that if one AP is compromised the effect of the key compromise is as local as possible. However, minimizing the effect of key compromise can be achieved also with e.g. very short-term keys (e.g. renewing key hierarchy with re-authentication).

In this paper, we describe the LTE security architecture [11,12], list handover key management requirements, and describe the keying management in LTE. We compare this with the session keys context (SKC) key management mechanism [13] and analyze how the LTE implementations could be simplified and enhanced without losing the air interface interoperability.

The rest of this paper is organized as follows. Next we describe the LTE system and security architectures, and the LTE key management (Chapter 2). Then, we provide an analysis and different implementation alternatives of the LTE key management (Chapter 3). We describe SKC and compare it with the LTE (Chapter 4). In the end we describe existing key delivery mechanisms for mobile networks and their relation for LTE. Finally, we conclude our paper (Chapter 5).

2. LTE architecture

Third Generation Partnership Project (3GPP) has standardized E-UTRAN as part of the Long Term Evolution (LTE) [14] work based on UMTS [15–17] and GSM. Correspondingly 3GPP also standardized a new Evolved Packet System (EPS) architecture as part of the system architecture evolution work based on UMTS and GSM architecture evolution. LTE and EPS include several enhancements especially from security perspective compared to UMTS and GSM [18].

LTE System Architecture includes LTE radio base stations called as E-UTRAN Node Bs, i.e. eNBs. However, in this paper we refer to base stations, eNBs, and e.g. WLAN APs with the AP term. LTE consists of APs connected to one or multiple control plane Mobility Management Entities (MME) and user plane gateways (SAE GWs). MME is the Key Distributor (KD) in LTE. Both MME and SAE GW reside in the EPS network and connect to the APs through many-to-many S1 interface (see Fig. 1).

LTE is fully optimized for packet data access and it also supports quality of service for different data transfer needs (like VoIP, browsing, download, etc.). There are several new functionalities in LTE radio compared to UMTS. They are namely: (1) higher user data plane bandwidth, (2) longer MN¹ connected state duration, (3)

* Tel.: +358 404835507.

E-mail address: dforsber@gmail.com

¹ Note that MN is called User Equipment (UE) in LTE.

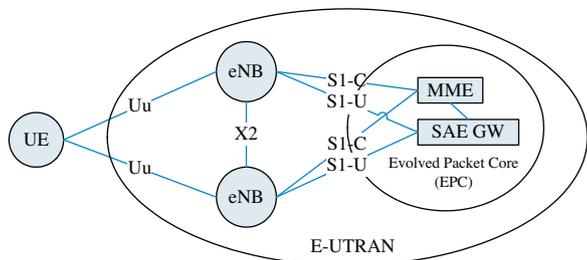


Fig. 1. LTE (E-UTRAN) system architecture.

use of Discontinuous Reception (DRX) in connected state, (4) no MN Medium Access Control (MAC) level identity, and (5) X2, the direct interface between APs, and (6) no Radio Network Controller (RNC).

Fig. 2 shows the LTE protocol architecture. In LTE the Non-Access Stratum (NAS) signaling protection terminates in the EPS core network, whilst the RRC and user plane protection terminate in the AP. User plane carries IP data packets (over Packet Data Convergence Protocol, PDCP), like for HTTP browsing and Voice over IP.

The X2 interface makes E-UTRAN considerably different compared to UTRAN, which does not have a similar interface between APs. The reason for having X2 is that it allows APs to co-ordinate the RAN in a distributed manner, making the centralized UTRAN Radio Network Controller (RNC) unnecessary and thus reducing the number of network elements for LTE. This also results having RRC protocol termination in the AP instead of the RNC as in UTRAN. Confidentiality and integrity protection is on the PDCP layer for RRC and user plane. The signaling security between the MN and the core network (NAS layer, see below) is implemented in the signaling protocol itself.

In LTE security is important and targeted to be in the same or higher level compared to UTRAN [17]. Security on the radio link (Uu interface) during handovers is the main focus of our paper.

2.1. LTE security architecture

LTE security and privacy requirements are based on the respective requirements for UTRAN architecture, grouped in five feature groups [16,17,19], including (I) network access security, (II) network domain security, (III) user domain security, (IV) application domain security, and (V) visibility and configuration security. For the analysis and comparison of LTE key management, we are only interested on the first group, network access security. Network access security provides following security features on radio access link: (1) user identity confidentiality (privacy), (2) entity authentication, (3) confidentiality, and (4) data integrity.

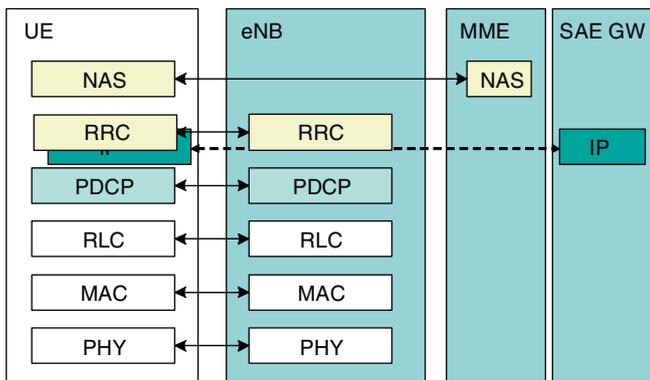


Fig. 2. LTE protocol stack illustration.

LTE has made a lot of architectural changes and introduced new features compared to UTRAN as discussed above. Some of the changes are described and analyzed from security point of view in [18].

The LTE security architecture [11] is described in Fig. 3. There are multiple security associations (SA) in the system. Network SAs (N-SA1 – N-SA5) protect the signaling and data between network elements. MN SAs (UE-SA1 – UE-SA3) provide three-layered security for the system. From network perspective the first security layer is between the MN and the APs (again, called eNBs in LTE). This layer protects the control plane signaling and the user plane data, but only the control plane is integrity protected whilst both are encrypted. This control plane between MN and AP is also called Access Stratum (AS) signaling. Second layer security is for the control plane connection between MN and the MME, i.e. the KD. This is called Non-Access Stratum (NAS) level signaling. Third layer is the long term SA between the MN and the home network (Home Subscriber Server, HSS) of the subscriber, i.e. the home authentication server.

The long-term security association between the MN and its home network is the origin for the key hierarchy. The EPS authentication and key agreement (AKA) protocol uses the long-term key K between authentication server and the MN and produces 128 bit CK and 128 bit IK and further the key hierarchy root 256 bit K_{ASME} , which is bound to the serving network identity. This serving network specific K_{ASME} key is sent from authentication server to the KD. Both the KD and the MN create a 256 bit K_{eNB} from the K_{ASME} and KD transfers this key to the AP. 128 bit AS level control plane and user plane protection keys are derived from the K_{eNB} in AP and the MN. Also, 128 bit NAS level control plane keys are created in KD and MN from the K_{ASME} . For both NAS and AS level control plane there are separate encryption and integrity protection keys. For the user plane only encryption is specified, thus only an encryption key is derived for it. The key hierarchy is summarized in the Fig. 4.

LTE has specified that two security algorithms for control plane and user plane protection must be supported. The mandatory ones are AES [20] and SNOW 3G [21]. Encryption algorithms use stream cipher modes and the input parameters are defined along the lines of UMTS system, namely: 1 bit direction, bearer identifier, 32 bit COUNT, and length. Direction is either up or down. Bearer id is an identifier for one of the radio link connections (bearers) between MN and the network. COUNT consist an increasing sequence number carried in each packet plus a hyper frame number that is maintained in both end points and increased every time the sequence number overflows. COUNT is specific for each bearer and direction. To avoid the key stream repetition a fundamental requirement is that with the same key one of the parameters must always be fresh. This is achieved by using the increasing sequence number with the hyper frame number to assure that every packet has fresh input parameters for the key stream initialization. For encryption the key stream is bitwise XORed with the actual data. For integrity protection the data is fed to the integrity algorithm and the output is 32-bit integrity checksum for every transferred packet. Integrity protection has similar input parameters, except that instead of the length parameter it takes the message itself as input parameter. It is important to know the input parameters to the ciphering and integrity protection as these affect the freshness of the key stream.

The K_{eNB} is specific for an AP and MN, and the derived control plane and user plane keys are specific also for a radio cell. During a handover from source AP to the target AP, the K_{eNB} is further transformed to a new K_{eNB}^* with a Key Derivation Function (KDF). Further details on the K_{eNB} handling are explained later in this paper.

There are different lifetimes for the keys in the key hierarchy. The long-term key K is valid for the whole subscription lifetime

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات