POLITECNICO DI TORINO
Repository ISTITUZIONALE

Formal verification of LTE-UMTS and LTE–LTE handover procedures

Original
Formal verification of LTE-UMTS and LTE–LTE handover procedures / BETTASSA COPET, P., Marchetto, G., Sisto, R., Costa, L.. - In: COMPUTER STANDARDS & INTERFACES. - ISSN 0920-5489. - STAMPA. - 50:(2017), pp. 92-106. [10.1016/j.csi.2016.08.009]

Availability:
This version is available at: 11583/2659528 since: 2017-05-12T16:23:48Z

Publisher:
Elsevier

Published
DOI:10.1016/j.csi.2016.08.009

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright
Elsevier postprint/Author's Accepted Manuscript

© 2017. This manuscript version is made available under the CC-BY-NC-ND 4.0 license
http://creativecommons.org/licenses/by-nc-nd/4.0/.The final authenticated version is available online at:
http://dx.doi.org/10.1016/j.csi.2016.08.009

(Article begins on next page)

10 October 2026

Formal Verification of LTE-UMTS and LTE-LTE Handover Procedures

Piergiuseppe Bettassa Copet[a], Guido Marchetto[a,*], Riccardo Sisto[a], Luciana Costa[b]

[a] *Dipartimento di Automatica e Informatica, Politecnico di Torino - Corso Duca degli Abruzzi, 24 - 10129 Torino, ITALY*
[b] *Telecom Italia Information Technology, Italy*

Abstract

Long Term Evolution (LTE) is the most recent standard in mobile communications, introduced by 3rd Generation Partnership Project (3GPP). Most of the works in literature about LTE security analyze authentication procedures, while handover procedures are far less considered. This paper focuses on the procedures that are activated when a mobile device moves between different LTE cells and between LTE and the older Universal Mobile Telecommunications System (UMTS) networks and completes previous results with a deeper formal analysis of these procedures. The analysis shows that security properties (secrecy of keys, including backward/forward secrecy, immunity from off-line guessing attacks, and network components authentication) hold almost as expected in nominal conditions, i.e. when all backhaul links are secured and all backhaul nodes are trusted. The paper also analyses how these security properties are affected by possible anomalous situations, such as a compromised backhaul node or a misconfiguration by which a backhaul link becomes not protected and can be accessed by an attacker. The analysis shows that some security properties hold even in these adverse cases while other properties are compromised.

Keywords: LTE; UMTS; security; formal verification; ProVerif; handover

*Corresponding author
Email addresses: piergiuseppe.bettassa@polito.it (Piergiuseppe Bettassa Copet), guido.marchetto@polito.it (Guido Marchetto), riccardo.sisto@polito.it (Riccardo Sisto), luciana.costa@it.telecomitalia.it (Luciana Costa)

1. Introduction

Fourth generation (4G) mobile networks are rapidly spreading out. Long Term Evolution (LTE), which is an evolution of the previous third generation (3G) Universal Mobile Telecommunications System (UMTS), is already available in many countries. For a considerable period of time these two technologies will co-exist, because the new devices on the market, such as smartphones, at this time support both connection technologies.

Enabling seamless user mobility is a key factor in the LTE and UMTS standards defined by the 3GPP (3rd Generation Partnership Project)[1]. Different procedures have been specified in order to ensure continuity of service to users who move, for example, from an area which is covered by an LTE cell to an area covered by another adjacent LTE cell. Similarly, the standards define procedures to seamlessly move from an area where both 4G and 3G networks are available to an area with only 3G network coverage (or vice versa). In particular, these scenarios where different technologies are cooperating require non-trivial procedures. In fact, an important difference between 3G and 4G networks is that the latter have a flat-IP architecture (all network devices communicate over IP technology), unlike 3G, where communications between devices use radio channels with multiple access technologies.

Formal verification is a well-known technique that can be used to perform a thorough analysis of a communication protocol, in order to identify the presence of bugs in its design or to prove its correctness. In the case of cryptographic protocols, formal verification can identify possible attacks on the protocol or prove that no attacks are possible under certain assumptions. In the past, formal verification has already been applied to security protocols for mobile networks. In particular, many works in the literature have formally analyzed the basic procedures for authenticating users in 3G and in 4G networks, while a smaller number of studies has been devoted to the procedures that allow user mobility in these networks. As a consequence, not all the possible mobility scenarios already

have a formal analysis.

The 3GPP defines as IRAT (Inter-Radio Access Technology) handover the procedures in which it is necessary to map the existing security context (ciphering keys, user data) in the transition between two different technologies (such as for example from LTE to UMTS). Instead, the procedures activated when a connection must be seamlessly moved between two LTE network nodes are called Intra-Handover procedures.

Intra-Handover procedures have been formally analyzed in [3], while recently we presented the results of a formal analysis of the IRAT handover procedures that enable users to seamlessly switch from a 3G to a 4G connection, and vice versa [4].

This paper provides a thorough formal analysis of LTE-LTE and LTE-UMTS procedures, which extends and completes the results previously provided in [3] and in our previous conference paper [4]. In particular, our analysis of LTE-LTE handover procedures includes the verification of aspects that were not considered in [3], including a wider set of security properties, a more accurate model of the procedures, including the possible presence of emergency calls during the handover, and the analysis of anomalous situations where some links or nodes are compromised. Instead, for what concerns the analysis of LTE-UMTS and UMTS-LTE handover procedures, although some of the results presented here were already presented in [4], in this paper we extend those results by using more accurate models, where the possibility that emergency calls are executed during the handover procedures is considered. Moreover, in this paper we provide a thorough description and motivation of all the formal models used for our analysis and the underlying design choices, which were presented only in part and in much less detail in [4], for the previously used models.

The tool used for formal analysis is ProVerif [5], which is an automatic formal verifier for cryptographic protocols. In this paper we exploit many of the features of ProVerif which were not used in previous papers about LTE-LTE handover procedures analysis. Specifically, in addition to basic security properties such as secrecy of all the keys used before, during and after the handovers, secrecy of

payloads exchanged, and authentication between network components, we also analyse backward and forward secrecy of keys, conditional secrecy of payloads (i.e. secrecy that must hold only when optional encryption of data is enabled) and immunity from off-line guessing attacks. The results that have been obtained show that in some particular scenarios the aforementioned security properties are only in part assured in the models that have been developed, which sheds some more light on the security of LTE handover procedures. In particular, in this paper we analyze particular situations that may arise because of misconfiguration errors in the operator networks or eNodeB nodes that are compromized by attackers (some LTE cells are especially designed in order to cover small areas and to be placed in relatively easily accessible places, e.g. indoor premises). In these cases, confidentiality of user data traffic is not always provided, and the lack of authentication between network elements makes injection of fake signaling messages possible. This kind of result may be interesting especially for mobile operators, who have to assess security risks in their networks.

The remainer of the paper is organized as follows. Section 2 gives some background about the LTE and UMTS networks and about ProVerif, and Section 3 discusses related work. Section 4 introduces the main security properties that have to be ensured in the LTE-related handover procedures and discusses security threats. Then, Section 5 presents the formal modeling of procedures and the formal property specifications based on ProVerif, while Section 6 presents the results of the formal analysis. Finally, Section 7 concludes.

2. Background

2.1. UMTS and LTE overview

This section presents the basic concepts of 3G and 4G mobile networks, which are essential in order to understand the work presented in this paper. For further details, refer to the 3GPP specifications [1].

2.1.1. UMTS overview

Figure 1a shows the architecture of a UMTS network. The different components are grouped into three domains: the Mobile Station (MS), Serving Network (SN) and Home Network (HN). The mobile station domain is composed of the Mobile Equipment (ME), which is the mobile device, and the Universal Subscriber Identity Module (USIM). The latter contains a worldwide unique identification number, called International Mobile Subscriber Identity (IMSI), and other information shared with the Authentication Center (AuC) of the mobile operator (more details to follow). The Universal Terrestrial Radio Access Network (UTRAN) is the access network for UMTS networks. The UTRAN is composed of Radio Network Controllers (RNCs) and base stations, called NodeB. The RNC is the control unit of the UTRAN network (a single RNC can control a large number of NodeB, which have minimal functionality and mainly propagate messages between MS and RNC). The SN may belong to the same provider of the USIM or to another provider, in areas not covered by the provider of the USIM. The SN is composed of Mobile Switching Centers (MSC) and Visitor Location Registers (VLR). An MSC is able to manage several UTRAN networks. The VLR records information of the MS attached to the network and keeps track of the MS positions. The home network contains the MSC (the operation is similar to those of the SN), and Home Location Registers (HLR), which contain persistent information on registered operator users, and records the locations of users. Finally, the Authentication Center (AuC) is used to generate the authentication data. For each subscriber identified by the IMSI, it contains the security algorithms and an individual key (K_i) which is a copy of the K_i permanently stored on the USIM card of the subscriber. The IMSI value is public, and can be read from the device that mounts the USIM. The key, however, must remain secret, and must never be revealed by USIM and AuC. For this reason, the USIM provides functions, accessible to the ME, that can be used during the authentication phase in order to obtain temporary keys from K_i. In this way, the secret K_i is never revealed to the ME.

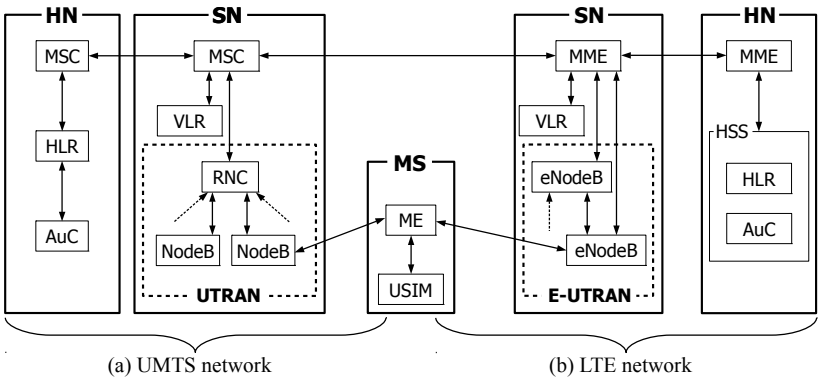

Figure 1: UMTS and LTE network architectures

2.1.2. LTE overview

Figure 1b depicts the architecture of an LTE network. Unlike the UTRAN, where a RNC controls many NodeB, the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) is composed of only one type of element: the Evolved NodeB (eNodeB or eNB). A Home-eNB (HeNB) performs the same function of an eNodeB, but is optimized for deployment for smaller coverage than macro eNodeB, such as indoor premises and public hotspots. Thus, in the following of the paper the acronym eNB will be used to refer both to eNodeB an Home-eNB. The eNB are "logically" connected directly to the Mobility Management Entity (MME). In reality, if the eNB-MME connections are protected with IPsec, as 3GPP specification recommends, security gateways are placed between E-UTRAN and MME to terminate IPsec tunnels. However, using IPsec tunnels is at discretion of network operators (if a connection is physically protected, the IPSec protection can be omitted).

A major difference of the system architecture between LTE and UMTS network is that features that were performed by RNC in the UMTS have now been distributed between eNB and MME. The MME is the main control component for the access network and initiates the authentication process, keeps track of the positions of MS, retrieves subscriptions of MS by HN, and manages connectivity. In LTE, the "concatenation" of HLR and AuC is represented

by the Home Subscriber Server (HSS), a single component that combines the functionality of HLR and AuC.

2.1.3. Key hierarchies in LTE and UMTS

Both in LTE and in UMTS, the first procedure done by a mobile device that wants to connect to the network is the Authentication and Key Agreement (AKA) procedure. The objective of this procedure is to establish the keys to be used in cryptographic operations during communication between mobile device and network. The keys are derived from the shared key K_i and from some randomly generated values. Details of authentication procedures can be found in [1] (TS 33.401). The keys are renewed periodically, in order to prevent possible attacks due to encryption of large volumes of data with the same keys.

The AKA procedure in UMTS networks determines two keys: the Cipher Key (CK) and the Integrity Key (IK), respectively used to encrypt and check the integrity of data exchanged between MS and RNC. UMTS defines only one class of traffic between MS and the network. Thus, only one pair of keys is established (Figure 2, right side), which is used for all communications between MS and RNC.

The LTE technology introduces significant differences in key management [1] (TS 33.821). LTE uses different keys for different protocols used between the terminal and the different components of the serving network. These keys are organized in a hierarchy as shown in Figure 2 (left side). At the top (root), the key K_i shared between USIM and AuC. The other keys are derived from K_i, following the levels of the hierarchy from top to bottom. Each level of the hierarchy indicates which parts of the network know the keys in the level. As expected, the mobile device knows all the keys except K_i. As in UMTS, starting from the key K_i, the CK and IK keys are derived, even if they are not actually used for encryption and integrity in LTE networks, but rather are used to derive the successive keys. Following the hierarchy, the K_{ASME} key, generated during authentication, is derived by the HSS and then sent to the MME (in the same way, the MS derives the same key). The K_{eNB} key is derived by MS and MME,

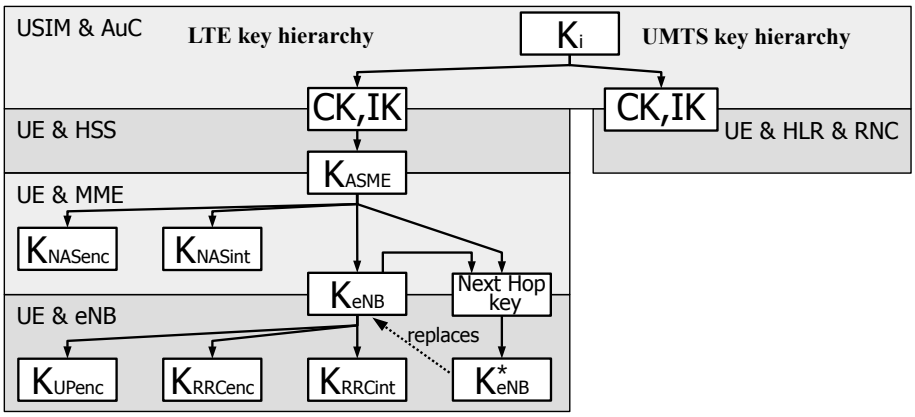

Figure 2: LTE and UMTS key hierarchies

starting from K_{ASME}, and then sent to the eNB, which can thus activate the security procedures between eNB and MS. However, K_{ASME} and K_{eNB} are not directly used in cryptographic operations. LTE provides two mechanisms of protection for two different classes of control traffic (Control Plane): Non Access Stratum (NAS) traffic, and Access Stratum (AS) traffic. NAS traffic consist of communications between MME and MS (forwarded in a "transparent" way through the eNB), while AS traffic (also called Radio Resource Control (RRC) traffic) includes the control messages between MS and eNB. For this reason, two keys are derived from K_{ASME}: K_{NASenc}, used for encryption, and K_{NASint}, used for integrity checking of NAS messages. Similarly, from K_{eNB}, the keys K_{RRCenc} and K_{RRCint} are derived and used for AS messages. The user traffic (User Plane), is encrypted using a different key, called K_{UPenc}. Integrity protection is not supported for this class of traffic.

Finally, after a successful handover of the MS between two neighbor eNB, it is necessary to renew the K_{eNB} [1] (TS 33.401). To do this, the MME derives a new value from the key K_{ASME}, called Next Hop key, which is used, along with the previous K_{eNB}, to generate the K_{eNB} key (called $K^{\star}_{eNB}$) used by the target eNB after the handover. Further details on these procedures and their analysis can be found in [1] (TS 23.401 and TS 33.401) and [3] respectively.

2.1.4. Handover procedures

Handover procedures are activated by the serving network (eNB in LTE, RNC in UMTS) when the strength of the radio signal between a mobile station and the current eNodeB/NodeB becomes too much degraded. The decision of performing a handover is taken by the eNB or RNC, which selects the target eNB/RNC from a list of neighbors (the list is previously known). When a neighbor with the same technology (LTE/UMTS) is not available for the handover, then a handover to a network with other technology is executed. Intra-Handover procedures are adopted when a user moves between different LTE cells, while Inter-RAT procedures are adopted while moving from a radio access technology (GSM, UMTS, LTE, WiMAX or any other wireless technology) to another. These procedures are described in the 3GPP TS 23.401 and TS 33.401 specifications [1]. eNBs can be directly connected by an X2 interface which can be used to perform handover procedures. Every eNB is connected to the MME via the S1 interface. Both interfaces are IP based.

2.2. ProVerif overview

ProVerif [5] is a tool for automatic verification of cryptographic protocols, using theorem-proving techniques, where the protocol actors and the attacker are modeled according to the symbolic approach defined by Dolev and Yao [7]. In this model, the attacker has complete control over communications channels and can read, delete, modify messages in transit or forge new messages. The symbolic representation of data and cryptography implies that encryption is considered ideal: the attacker can decipher an encrypted message only when he knows the right key.

As the possible behaviors of the attacker are already pre-defined by the Dolev-Yao approach, when using ProVerif it is enough to model the trusted actors of the protocol, while the attacker model is already available inside ProVerif. An important feature of ProVerif is its ability to model and analyze an unlimited number of sessions of the protocol, even running in parallel.

Because of the inherent undecidability of the formal verification problem [6],

ProVerif may report false attacks, i.e. attacks which in reality are not possible. As a consequence, when an attack is reported by ProVerif, in the form of an execution trace that violates the specified property, it is necessary to carefully analyze it in order to understand if it is a real attack. However, if a property is reported as satisfied, then it is guaranteed to be true (ProVerif builds a formal proof for it), and no attack is feasible in the model.

3. Related work

Ben Henda and Norrman [3] recently used ProVerif to analyze the LTE procedures related to session management (used to establish security algorithms between the mobile device and the network) and mobility (handover between two LTE cells). The procedures analyzed are: Network Access Stratum (NAS) security control procedure, i.e. security algorithm negotiation between MS and MME, NAS Service Request Procedure (security algorithm negotiation between MS and eNodeB), X2 handover, and S1 handover. The reported results show that secrecy and agreement properties hold as expected. However, differently from our work, the analysis proposed in [3] does not consider the possibility that data encryption may be disabled and that some channels may lack IPSec protection, as allowed by the standard [1] (TS 33.401). Moreover, Ben Henda and Norrman do not consider the possibility of having emergency calls, nor that an attacker may control one or more eNBs. Finally, we check a wider set of properties, including, for example, weak-secrecy, i.e. the inability of the adversary to distinguish a correct guess of a secret term from an incorrect guess.

The research community mainly focused on analyzing the Authentication and Key Agreement (AKA) procedure and on proposing improvements in that procedure [11], [12], [13] and [9]. LTE and UMTS authentication procedures are very similar, and only computation of keys and used algorithms differ. The UMTS AKA was formally analyzed using BAN logic in TS 33.902 [1] and, due to the similarity of the procedures, all analysis results carry over to LTE AKA.

Arapinis et al. [2] used ProVerif to analyze privacy aspects of UMTS. However,

the paging procedure analyzed is the same in LTE and UMTS technologies, so the results should be valid for both networks.

Qachri et al. [10] propose and analyze a system for handovers between different wireless network technologies (e.g. 3G, 4G, WiFi, WiMax). The proposed system has been formally verified with ProVerif. However, the paper does not provide an analysis of the LTE network defined by the 3GPP standards.

4. Security requirements and threats

The handover procedures have different security requirements, as specified by the 3GPP standards. All the procedures, assuming that the mobile device is authenticated with the network components (MSC in UMTS, eNB and MME in LTE) before the handover begins, must guarantee the validity of the same authentication properties after the handover is completed, in the destination network. Similarly, all the procedures must keep the secrecy of all the keys used before, during and after the handover in the mobile device and in the operator network. Consequently, the procedures for handover always activate the protection of the data transmitted with the exception for unauthenticated emergency call when integrity checks and ciphering procedures cannot be applied.

Security threats derive from different causes. While physical damages and technical failures are out of the scope of this work, our analysis considers malicious threats originated by attackers who can eavesdrop, alter and drop communications between the mobile device and the operator network, and among some components of the operator network, considering also the case when emergency calls are ongoing. In this scenario, the threat consequences, in the handover procedures, may be the disruption of authentication between components and loss of data privacy.

In order to counter security threats, communication among components of the home and serving network should be secured by the mobile operators that own the networks. While the risk of attacks on the MSC-MSC, MME-MME, MME-MSC and MSC-RNC links is not very relevant, because the involved

nodes are not physically accessible, the same is not true for the eNB-MME and eNB-eNB links, especially in the case of HeNBs, because these nodes are often located in publicly accessible locations, and hence they may be tampered with by a malicious attacker. The 3GPP TS 33.820 and 33.401 [1] specifications specify that the eNB-MME and eNB-eNB connections should be protected by IPsec, which guarantees authentication, integrity and confidentiality of data. Moreover, Security Gateways (SeGW) should be used to handle the IPsec connections in the serving network. However, the 3GPP TS 33.401 [1] specification reports that, if the interfaces are trusted (e.g. physically protected), the use of IPsec based protection is not needed, depending on operator evaluations. In practice, the promiscuity of IPSec protected connections and physically protected connections, summed to the fact that the number of LTE cells is rapidly growing, increases the probability of misconfiguration in the networks, thus leading to possible situations where some channels that should be protected by IPsec are not, thus being accessible by malicious attackers. Moreover, some operators underestimate the security issues and avoid using IPsec on their networks even when the risk of attacks on the channels is not negligible. Reasons might be several: some operators fear that IPsec would increase both network complexity and traffic latency, others simply underestimate the problem as, for example, they assume that encryption is performed by applications, which is not always true. A clear presentation of all the possible motivations that are leading several network operators to avoid using IPsec, and data about the adoption rate of IPSec, is available in [8].

Finally, as HeNB are specifically designed to be placed in indoor spaces and public hotspots, in some cases they can be easily physically accessed by malicious attackers. The 3GPP TS 33.820 [1] specification describes all the security requirements that that must be fulfilled by eNBs and HeNBs. An external attacker should not be able to access the sensitive data (e.g. private keys) stored in the eNB, even if he gets physical access to the hardware of the eNB. However, considering the complexity of eNBs (produced by different manufactures), and the increasing diffusion of them, it is practically impossible to

ensure that all the eNBs are immune to external attacks. For this reason, the risk of having compromised eNBs controlled by an attacker should be considered.

5. Modeling handover procedures for security verification

5.1. Modeling choices

This section presents the main modeling choices made in developing the formal models of the handover procedures. The final aim is to create models that faithfully represent the procedures to be analyzed but that are as simple as possible, so as to efficiently exploit the analysis tool ProVerif.

5.1.1. Omitting non-relevant data and operations

When modeling handover procedures for analyzing their security, only the data and operations related to cryptography and authentication need to be included in the models, while information related to resource allocation and relocation is not relevant for the security analysis and can be omitted.

5.1.2. Abstracting algorithms and algorithm identifiers in key derivation functions

Since perfect cryptography is assumed in the Dolev-Yao attacker model, the handover models consider only whether encryption is enabled or not, no matter which algorithm is chosen. Therefore, the algorithms and the algorithm identifiers are abstracted away from key derivation functions.

5.1.3. Using a single fresh value to represent an IMSI

An IMSI consists of three parts [1] (TS 23.003): (i) Mobile Country Code (MCC), which identifies the country of domicile of the subscriber, (ii) Mobile Network Code (MNC), which identifies the HN of the subscriber, and (iii) Mobile Subscriber Identification Number (MSIN), which identifies the subscriber within the HN. As the splitting of an IMSI into its components is not relevant for our analysis, in this work a single value is used to represent the IMSI. As subscribers are uniquely identified by their IMSI, an IMSI is modeled as a fresh value, i.e. as

a value generated before the start of the protocol and guaranteed to be unique. Fresh values are considered by ProVerif initially unknown and unguessable by the attacker, while in practice an active attacker can obtain a subscriber's IMSI using so-called IMSI catchers. In order to take this into account, in the models the MS sends its IMSI in clear over the public channel in the first message. Thus, the attacker can learn the IMSI by eavesdropping on the public channel.

5.1.4. Modeling AKA procedures

As the handover procedures can be activated at any time, when the MS is already authenticated with the serving network, and the previous authentication state is important, the model cannot just include the procedures themselves, but it needs to represent what may happen before the procedures are activated. Most notably, the model should include the last AKA procedure that has been executed by the entities involved in the handover. As the inclusion of a full AKA procedure model would make the overall model too complex to be analyzed[1], the initial authentication is not fully modeled, but it is substituted by an equivalent model, which creates the same security context that is assumed to be established by the executed AKA procedure. This modeling choice was also adopted in [3].

In each AKA equivalent model, a fresh term used as IMSI is first generated by the MS, and whether to activate encryption or not is non-deterministically chosen, so as to consider both cases.

In the LTE to UMTS, LTE X2 and LTE S1 handover models each MS also generates a fresh term used as K_{ASME} (that in reality is established during the AKA). Encryption selection and K_{ASME} are inserted as values in private perfect hash tables, shared only with the MME and called `capab` and `keys`. In these tables, the corresponding IMSI is used as key for selecting the corresponding values. So, the MME can retrieve the correct values for each MS from these hash tables, by using the IMSI value (which is public). In other words, the agreement

[1]The inclusion of the complete model of AKA procedure caused the non-termination of the ProVerif analysis.

achieved by the initial AKA context setup is replaced by the two shared tables. Such tables, being private, cannot be accessed by the attacker. Here are the ProVerif code segments that represent the handling of the shared data:

```
(* define two tables *)
table keys(ident , asmeKey).
table capab(ident , bool).

(* generate fresh IMSI *)
new imsi: ident;
(* nondeterministically chose a value between true and false *)
let cap_ue: bool suchthat mem(cap_ue , uecaps) in
(* generate a fresh term used as KASME *)
new kasme: asmeKey;
(* insert new terms into the tables *)
insert capab(imsi, cap);
insert keys(imsi, kasme);

(* retrieve terms from the tables, using IMSI as key *)
get keys(=imsi, kasme_recv) in
get capab(=imsi, cap_recv) in
```

Instead, in the UMTS to LTE models, in addition to nondeterministically selecting whether encryption is enabled or not, the MS also generates two fresh terms used as ciphering and integrity keys in UMTS (CK,IK), that in reality are established during the AKA. Similarly to the previous case, the selected encryption capability and the (CK,IK) key pair are inserted as values in private perfect hash tables, shared only with the MSC, called `capab` and `keys`. The corresponding IMSI value (which is public) is used as key for addressing these tables, thus allowing the MSC to retrieve the correct values for each MS.

5.1.5. Modeling communication channels

Communication channels are modeled according to the considerations made in Section 4, i.e. considering that the MSC-MSC, MME-MME, MME-MSC and MSC-RNC links are generally not physically accessible to attackers, while the eNB-MME and eNB-eNB links may be accessible either because of misconfigurations (i.e. not using IPsec on non physically protected links) or because an attacker compromises one or more eNBs thus obtaining control of the commu-

nication channels connected to those eNBs. Accordingly, in our analysis we assume that the MSC-MSC, MME-MME, MME-MSC and MSC-RNC links are secure channels, i.e. not accessible by the attacker, whereas for the eNB-MME and eNB-eNB links we explore both the case that the channels are secured, and hence actually not accessible by the attacker, and the case that an attacker may be able to control the channels.

One simple possible way of modeling a secure channel in ProVerif is to use a private channel, which, by definition, cannot be accessed by the attacker. A second possible way is by encrypting the data that flow through the channel with secret keys that are shared by the end-points of the channel, are not known to the attacker, and are never disclosed. With this solution, the impossibility for the attacker to access the secure channel is guaranteed by the Dolev-Yao attacker model which assumes perfect cryptography. The latter method is more complex than the one using a private channel. For this reason, the ProVerif models used in this work adopt the former approach:

```
free pubChannel: channel. (* public channel used to connect MS and eNB/RNC *)
free secureChannelEnbMme: channel [private]. (* private channel *)
```

Since the processes (corresponding to eNBs) that have been defined in the ProVerif models used in this analysis do not create any fresh term (using the ProVerif `new` statement), the scenario where an eNB is compromised and controlled by the attacker corresponds exactly to the scenario where all the channels connected to that eNB are not secure (i.e. defined as ProVerif public channels).

5.1.6. Modeling message headers

Each message has a header that identifies the type of message content. In our model, headers are defined as constants. Each process that receives a message checks if the message header matches the one expected for the current input instruction. If it does not match, the message is immediately discarded by the process:

```
const HO_REQUIRED: msgHdr. (* message header definition *)
in(=HO_REQUIRED, ...)      (* message input with header filter *)
```

This solution faithfully represents the way input messages have to be checked but at the same time it keeps a low footprint on the state space size of the model.

5.1.7. Modeling capabilities

As in Dolev-Yao models the details about ciphering algorithms are omitted, the same is done here: the model only represents whether the MS activates encryption (`true` value) or not (`false` value), but it does not represent other choices (e.g. encryption algorithm). Note that encryption is optional, but integrity protection is mandatory in LTE Control Plane (User Plane does not support integrity protection). Hence, only the encryption capability has to be represented. As said, the boolean value of this capability is nondeterministically chosen by the MS, so that the analysis considers both cases. The selected value of the capability is disclosed to the attacker in the first message sent by the MS.

```
(* create a set containing only true and false values *)
let uecaps = consset (true, consset (false, emptyset)) in

(* nondeterministically chose a value in the set *)
let cap_ue: bool suchthat mem(cap_ue , uecaps) in
```

5.1.8. Omitting temporary identifiers

In the model, the IMSI is used to identify the MS, while in reality temporary identifiers are used, i.e. Temporary Mobile Subscriber Identity (TMSI) in UMTS, and Globally Unique Temporary Identifier (GUTI) in LTE. This abstraction does not alter the security properties of the procedures, because the attacker can obtain the IMSI from temporary identifiers, as demonstrated by Arapinis et al. [2].

5.1.9. Representing data message exchanges

Before and after the handover procedures take place, data messages can be exchanged. This is taken into account, but only the exchange of two data messages is included, one before the procedure starts and one after its completion, because exchanging more messages would not add anything significant to the

model. These messages are also used to check the secrecy of the data traffic when encryption is enabled.

5.1.10. Using a fresh term to model a counter

The LTE to UMTS handover uses a counter to derive the UMTS CK′ and IK′ keys. This counter is called NAS downlink count, and represents the NAS protocol message counter. The counter is bounded, and when it is about to wrap around a new AKA procedure is activated, in order to generate a new set of keys (K_{ASME}, K_{eNB} and all derived keys). Integer values are not directly supported by ProVerif. The increment of the NAS downlink count value is therefore modeled as the creation of a fresh new value, which is disclosed to the attacker in the next message, as shown in the following ProVerif code:

```
new nasDownlinkCount: bitstring;
let ck': ckKey =  kdf_ck'(kasme,nasDownlinkCount) in
let ik': ikKey =  kdf_ik'(kasme,nasDownlinkCount) in
out(pubChannel,nasDownlinkCount);
```

The disclosure operation models the fact that a counter can be eventually guessed by an attacker, because it is a bounded integer value. Using a private fresh term does not correctly represent a counter in the model, because a fresh term is unguessable. Disclosing the fresh term used as counter is an acceptable approximation because it adds the counter value to the attacker knowledge database, and covers the case when the attacker guesses the counter value. This design choice was already adopted in [3].

5.1.11. Simplifying transmission paths

In order to reduce the complexity of the analysis, some messages in the models do not follow the real path from source to target, but they follow a simplified path. For example, the HANDOVER COMMAND message (in the LTE to UMTS and UMTS to LTE procedures) is directly exchanged between MS and MME in the model. In reality, this message passes through the eNB node, but the eNB does not alter the contents of the message, unless some physical parameters, and the ciphering and integrity checking, done with the K_{RRCenc}

and K_{RRCint} keys. Modeling the path through the eNB, with the additional ciphering and integrity checking, is possible, but leads to models that cause the inability of ProVerif to terminate successfully. This problem has been avoided by introducing a public direct channel between MS and MME, which replaces the sequence of MS-eNB (public channel) and eNB-MME (private channel if protected with IPSec or physical barriers, public otherwise) channels that in reality exist in the network. This replacement is a sound approximation of reality, because it enlarges the possible attacks on the protocol (the MS-MME channel is public, and the ciphering and integrity checking done with the K_{RRCenc} and K_{RRCint} keys is omitted). Hence, if a security property holds on this model, it must hold a fortiori when the real channels are used. Note that the encryption of messages between MS and MME with the K_{NASenc} key is still modeled, when required.

5.1.12. Modeling emergency sessions

LTE redefines the management of emergency calls. Emergency services are handled by the IP Multimedia Subsystem [1] (TS 23.167), and can be activated even if the user is not authenticated (i.e. the MS does not mount a USIM card). During emergency calls, a handover from LTE to UMTS can be performed if necessary, while the handover from UMTS to LTE is not supported [1] (TS 23.401). The ProVerif models of the LTE to UMTS handover consider the possibility that a user may activate emergency mode, in order to verify if an attacker can exploit data acquired during the emergency session handovers to break the security of legitimate communications. Similarly, the models of LTE to LTE handovers consider emergency sessions. Emergency session have been modeled as separate processes, one for each actor, where encryption and integrity checks are disabled. The same IMSI is used to start a MS process that models an emergency terminal (unauthenticated), and one process that follows the authenticated session. By adopting this approach, the models consider the possibility that the same IMSI is used at the same time for an authenticated session and for an emergency session. This possibility in reality may happen if

an attacker uses the IMSI to start an emergency session, while the legitimate user is connected to the network.

5.2. Procedure models

The next subsections give an informal description of the procedure models used for security verification, in the form of charts. The models have been derived from the procedure descriptions given in 3GPP TS 23.401 and TS 33.401 [1] specifications, but omitting non security relevant data and operations and following the design choices detailed above.

The equivalent model that substitutes the AKA procedures is inserted at the beginning of each handover procedure model, in order to represent the establishment of the security context assumed before starting the handover procedure itself. Just after the first two messages representing the initial AKA equivalent model, a third message exchange is inserted before starting each handover procedure itself. This message represents a user data exchange between MS and eNB/MME/RNC, done before the handover procedure itself. These initial messages can be seen, for example, in the chart in Figure 3, which represents the messages exchanged during a LTE to UMTS handover.

An excerpt of the ProVerif model used to verify the LTE to UMTS handover procedure is shown in Appendix A while the complete handover models are available for download at the URL `http://staff.polito.it/riccardo.sisto/lte.umts.handover/fullmodels.zip`

5.2.1. LTE to UMTS

Figure 3 depicts the simplified message exchange flow performed during Inter-RAT handover from LTE to UMTS technologies, and represents the ProVerif model used for the verification of the handover procedure.

After the first three context messages already explained, the handover is activated by the eNB with the HANDOVER REQUIRED message, which informs the MME that the procedure must be performed for the user identified by the *IMSI* contained in the message. The MME derives the new CK' and IK'

UMTS keys from the previous K_{ASME} and the *NAS downlink count* value. The FORWARD RELOCATION REQUEST message provides the target MSC with the two keys and the *IMSI*. The MSC provides the target RNC with the keys just received and the user identity (RELOCATION REQUEST message). Now the RNC has all information required to communicate with the MS. RELOCATION REQUEST ACK and FORWARD RELOCATION RESPONSE messages are used to inform that the target UMTS network is ready to accept the connection from MS. The HANDOVER COMMAND is a NAS message that provides the MS with the data (*NAS downlink count*) required for the derivation of CK' and IK' in the MS. Then the MS sends a HANDOVER TO UTRAN COMPLETE message to the target RNC for signalling that the MS is ready to use the UMTS network. Finally, two messages are used to establish agreement upon the encryption algorithm, using the SMC (SECURITY MODE COMMAND) and the SMC COMPLETE messages. The last message represents data exchange after the handover, as already discussed.

5.2.2. UMTS to LTE

Handover from UMTS to LTE (Figure 4) is similar to the LTE to UMTS handover, but with the network roles reversed.

Handover is activated by the RNC with the RELOCATION REQUIRED message, which informs the MSC that the procedure must be performed for the user identified by the IMSI contained in the message. The MSC forwards the data received from the MSC to the target MME, using the FORWARD RELOCATION REQUEST. The MME computes the new LTE keys following these steps: (i) generates a fresh nonce, (ii) uses a derivation function to obtain a K'_{ASME} key from the nonce, CK and IK received from MSC, (iii) derives the new K_{eNB}, K_{NASenc} and K_{NASint} keys from K'_{ASME}. The K_{eNB} is sent, along with the IMSI and the nonce, to the target eNB (HANDOVER REQUEST message), which confirms the reception with the HANDOVER REQUEST ACKNOWLEDGE message. The eNB can therefore derive the K_{RRCenc}, K_{RRCint} and K_{UPenc} keys from the received K_{eNB}. Then, the MME sends the FORWARD

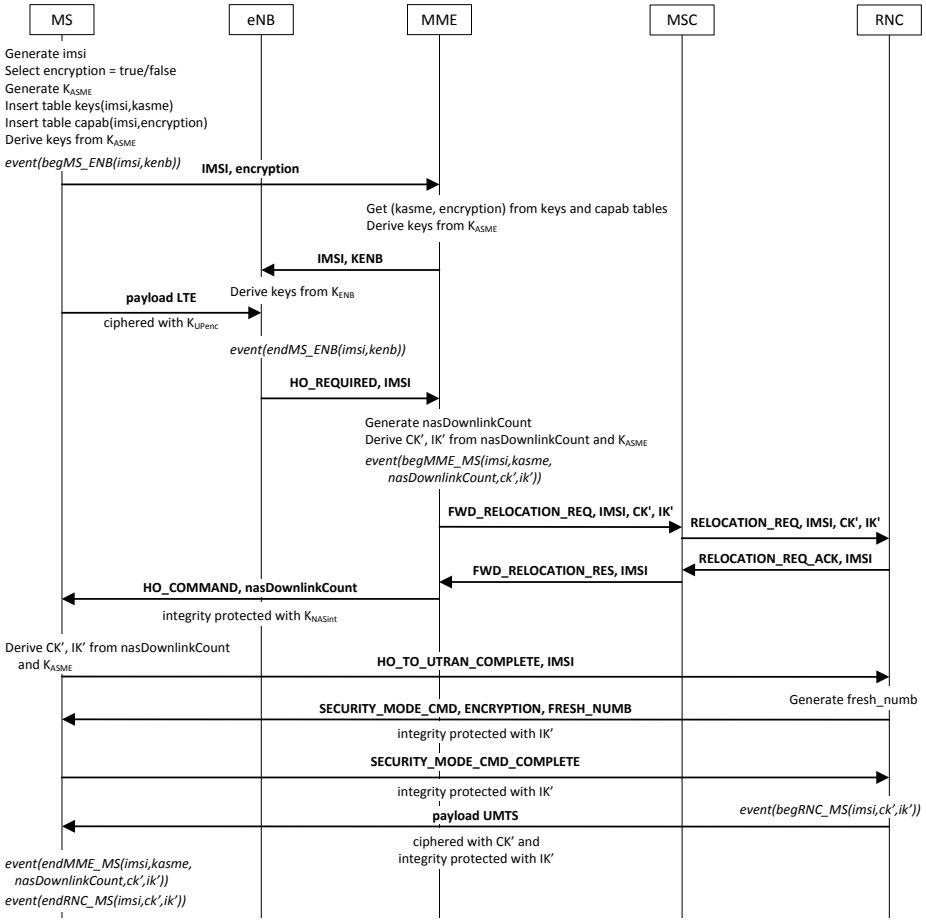

Figure 3: LTE to UMTS handover

RELOCATION RESPONSE to the MSC, which forwards the nonce to the MS with the HANDOVER COMMAND. Now the MS can derive the complete set of LTE keys from the received nonce and the previous CK and IK. When the derivation process is completed, the MS informs the target eNB with the HANDOVER TO E-UTRAN COMPLETE message. The next four messages activate the security (i.e. agree upon the security algorithms) of the Access Stratum and Non Access Stratum security, respectively between MS and eNB, and between MS and MME. The messages HANDOVER NOTIFY, FORWARD RELOCATION COMPLETE and FORWARD RELOCATION COMPLETE

ACKNOWLEDGE completes the handover procedure by signalling to the MSC that the handover completed successfully. Finally, the last message represents data exchange after the handover.

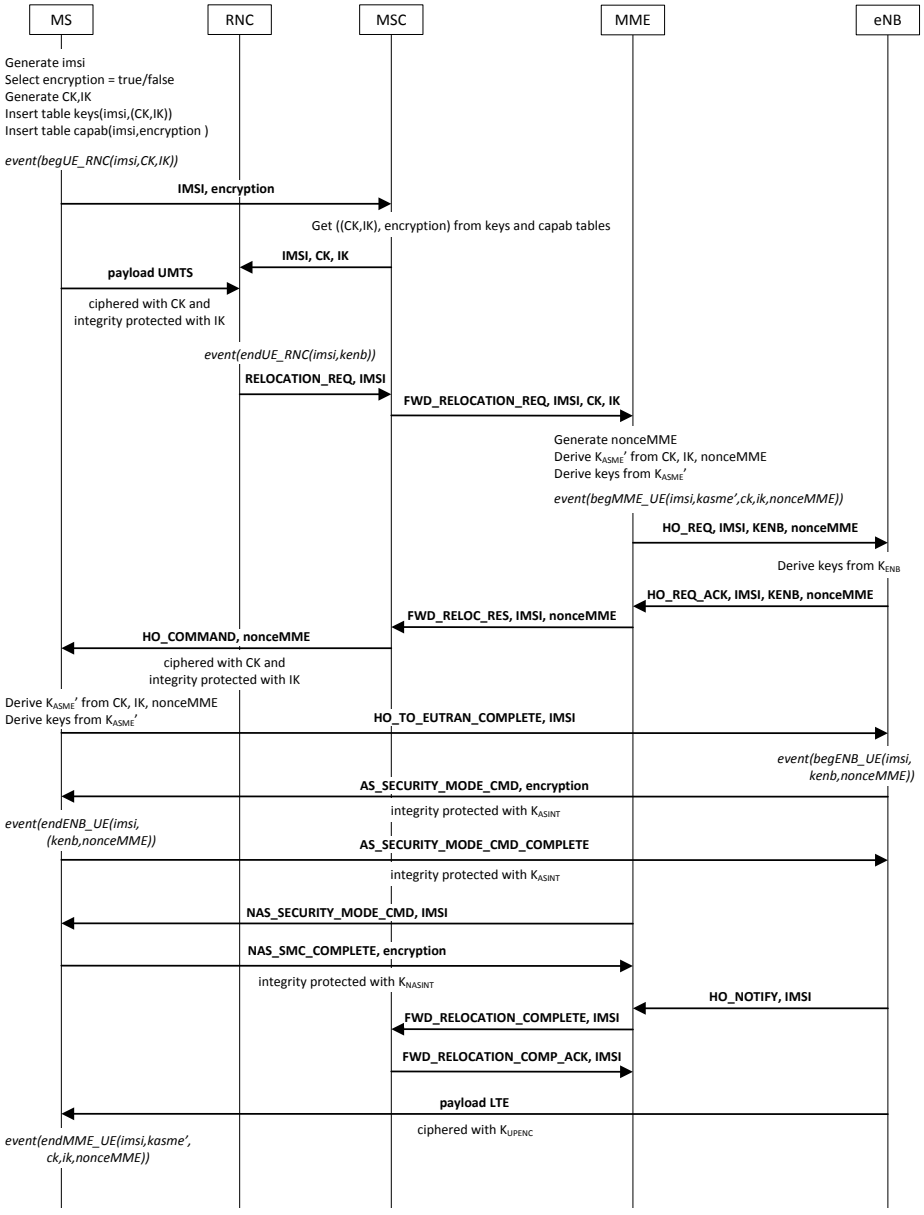

Figure 4: UMTS to LTE handover

5.2.3. LTE X2

The X2 handover (Figure 5) is an LTE to LTE handover procedure. The fundamental characteristic of the X2 procedure is the fact that the handover is performed between two eNB, without MME intervention. Indeed, the MME is informed that the handover has been performed after the procedure completed. An X2 handover can be executed between two eNB only if they are directly connected via the X2 interface. Otherwise, an S1 handover must be performed (Section 5.2.4).

The X2 handover is initiated by the SeNB (Source eNodeB) deriving the $K^{\star}_{eNB}$ key from the current K_{eNB} and the Target Cell ID, an identifier that is associated by the SeNB to the TeNB (Target eNodeB). The Target Cell ID is modeled as a fresh term that is disclosed to the attacker, because this ID is known by any MS that connects to the eNB, thus the attacker can obtain it by starting a legitimate connection to the eNB. The SeNB informs the TeNB that the handover is starting, by sending $K^{\star}_{eNB}$, MS identity and encryption capability in the HANDOVER REQUEST message.

The TeNB derives the new set of keys (K_{RRCenc}, K_{RRCint} and K_{UPenc}) from the received $K^{\star}_{eNB}$, and informs the SeNB that it is ready to accept the connection from MS (HANDOVER REQUEST ACKNOWLEDGE message). Then, the SeNB sends all the information required (encryption capability, that the MS checks to be corresponding to the value selected at the beginning, and Target Cell ID) to the MS in a RRC CONNECTION RECONFIGURATION message. Now the MS can derive the new $K^{\star}_{eNB}$ key and all the subsequent keys (K_{RRCenc}, K_{RRCint} and K_{UPenc}) that are used to communicate with the TeNB. Thus, the MS disconnects from the SeNB and sends a RRC CONNECTION RECONFIGURATION COMPLETE message to the TeNB. When the TeNB receives this message, it can start to communicate with the MS. Then, the TeNB informs the MME that an X2 handover has been performed with the PATH SWITCH REQUEST. The MME derives two new keys, called next hop key 1 (from K_{eNB} and K_{ASME}) and next hop key 2 (from next hop key 1 and K_{ASME}).

The next hop key 2 is sent to the TeNB in the PATH SWITCH REQUEST ACKNOWLEDGE message, and must be used by the TeNB to derive another $K^{\star}_{eNB}$ for the next handover. This implies a two-step forward key separation, because even though the SeNB can derive the key used for the TeNB, it cannot derive a key for the next target eNB. Finally, the last message represents data exchange after the handover.

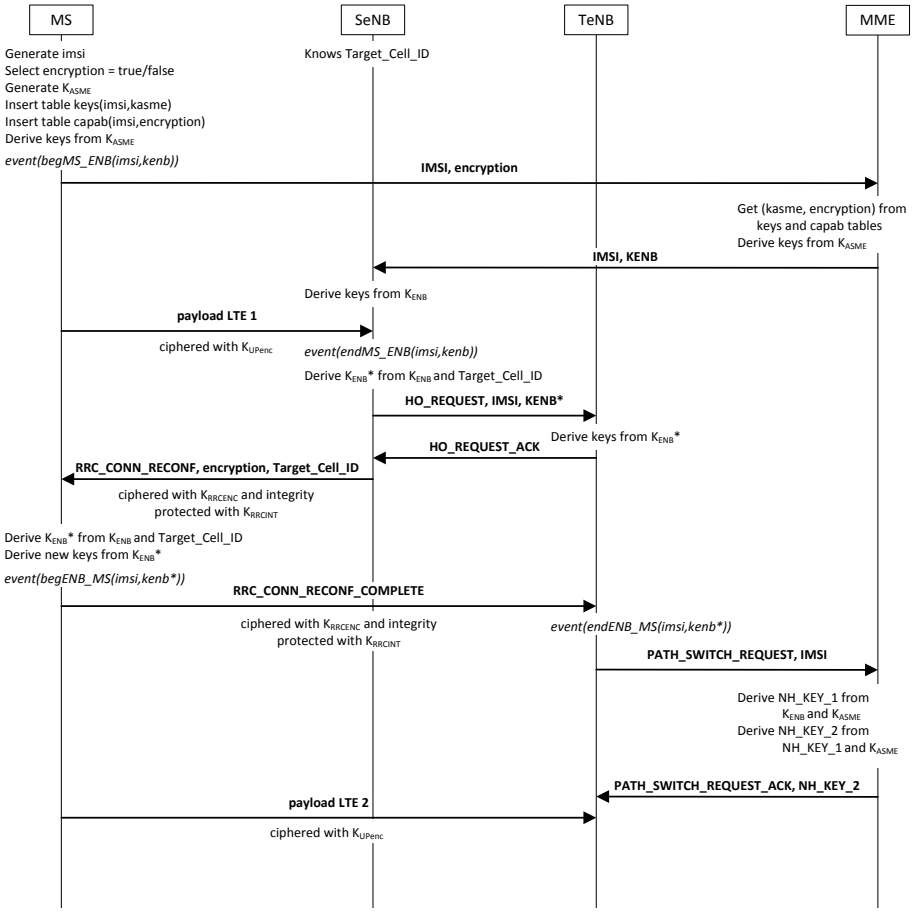

Figure 5: LTE X2 handover

5.2.4. LTE S1

The S1 handover (Figure 6) is an LTE to LTE handover procedure. Differently from the X2 handover (Section 5.2.3), the S1 handover procedure requires the

intervention of the MME.

The S1 handover is initiated by the SeNB deriving the $K^{\star}_{eNB}$ key from the current K_{eNB} and the Target Cell ID (an identifier that is associated by the SeNB to the TeNB, modeled as a fresh term that is disclosed to the attacker). The SeNB informs the MME of the necessity that a handover is required, by sending $K^{\star}_{eNB}$, MS identity and encryption capability in the HANDOVER REQUIRED message.

The MME derives two new keys, called next hop key 1 (from K_{eNB} and K_{ASME}) and next hop key 2 (from next hop key 1 and K_{ASME}). The next hop key 2 is sent to the TeNB, along with the MS identity (IMSI) in the HANDOVER REQUEST message. The TeNB derives the new $K^{\star}_{eNB}$ key from the received next hop key 2 and the Target Cell ID, which is known from the beginning for simplicity. Then, the TeNB derives the following K_{RRCenc}, K_{RRCint} and K_{UPenc} keys. Meanwhile, the MME sends the HANDOVER COMMAND message to the SeNB, which forwards to the MS the message along with the encryption capability (that the MS checks to be equal to the value selected at the beginning) and the Target Cell ID.

The MS can derive the new set of keys: the K_{RRCenc}, K_{RRCint} and K_{UPenc} keys will be used to communicate with the TeNB. Then, the MS disconnects from SeNB and initiates the message exchange with the TeNB by sending the HANDOVER CONFIRM message.

Finally, the last message represents data exchange after the handover.

The S1 handover procedure implies a one-step forward key separation: the SeNB cannot derive the key used in TeNB when the handover is completed, because the keying material of the TeNB is provided directly by the MME.

5.3. Security properties specification

The main security properties that the handover procedures are expected to guarantee have been specified as follows (the way these properties have been expressed in ProVerif is shown in Appendix A):

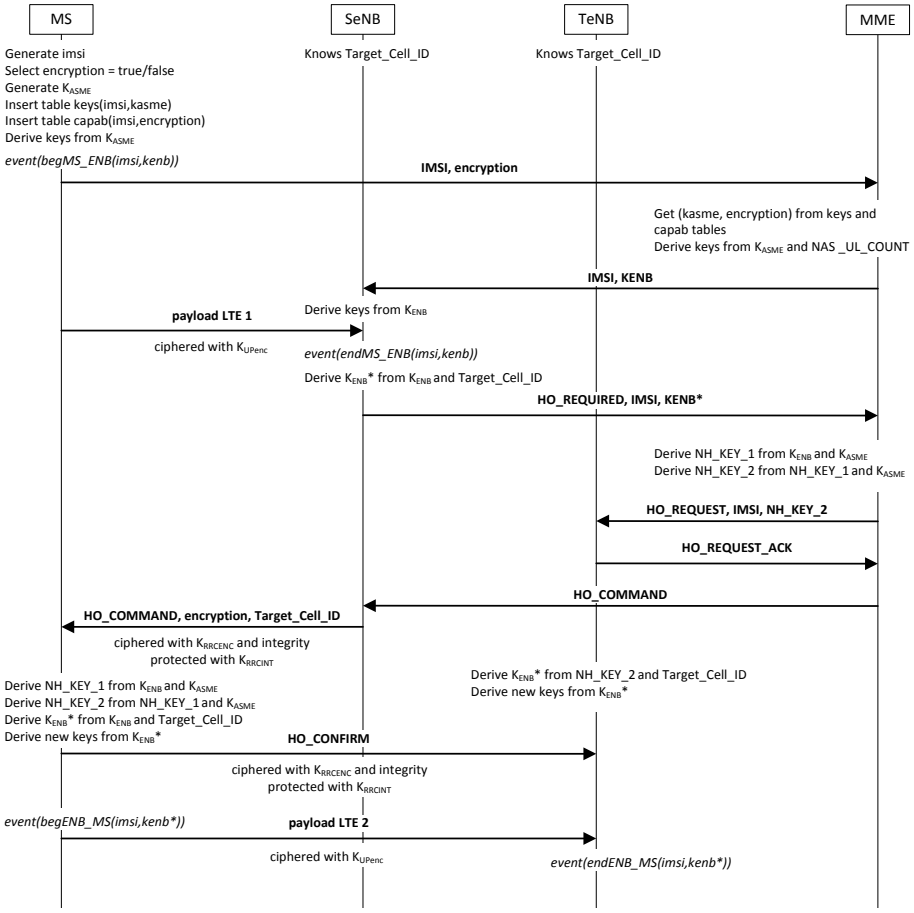

Figure 6: LTE S1 handover

- *Secrecy of keys*: all the keys involved in the handover procedures must remain secret.
- *Conditional secrecy of payloads*: in UMTS and LTE, encryption of data between MS and SN is optional, unless an emergency call without authentication is running, in which case encryption is disabled. Accordingly, the terms `payloadLTE` and `payloadUMTS`, used to represent the data transferred between MS and eNB/RNC (when an emergency session is not active), must be kept secret if encryption is enabled. Note that the secret payload referred by this property is not the payload of emergency sessions

messages, which is represented in the model by another term and is not protected (the attacker can read and modify it).

- *Forward secrecy and backward secrecy of keys*: the compromise of a secret key must not affect the confidentiality of future keys (forward secrecy) and of earlier keys (backward secrecy). In the handover from LTE to UMTS, forward secrecy is specified as the inability of the attacker to derive UMTS keys (CK', IK') when he knows K_{eNB}. Likewise, in the handover from UMTS to LTE, forward secrecy is specified as the inability of the attacker to derive LTE keys (K'_{ASME}, K_{eNB}) when he knows CK and IK. In both X2 and S1 LTE to LTE handovers, forward secrecy is specified as the inability of the attacker to derive the $K^{\star}_{eNB}$ key used in the target eNB when he knows the K_{eNB} used in the source eNB. Backward secrecy is defined as the inability of the attacker to derive K_{eNB} from CK' and IK' in the first case, to derive CK and IK from K_{eNB} in the second case, and to derive K_{eNB} from $K^{\star}_{eNB}$ in the LTE S1 and X2 cases.
- *Immunity to off-line guessing attacks*: a term is a weak-secret if it is vulnerable to brute-force off-line guessing, and the attacker has the ability to verify if a guessed value is indeed the weak-secret without further interaction after an execution of the protocol. In the handover models, the payloads are data that could be guessed, so it is specified that they must not be weak-secrets.
- *Authentication*: in the LTE to UMTS and UMTS to LTE handover models, the following authentication properties between the MS and the SN (eNB and RNC) are specified : (i) the MS is authenticated to the source network, (ii) the MS is authenticated to the target network (if the handover procedure has completed successfully), (iii) each time the MS successfully concludes a handover, then the MME previously derived the same keys (K'_{ASME} or CK'/IK'). In the LTE to LTE handover models (both X2 and S1), two authentication queries similar to the first two ones of the LTE to UMTS and UMTS to LTE handovers have been defined: (i) the MS is authenticated to the source eNB, and (ii) the MS is authenticated to the target eNB

(if the handover procedure has completed successfully). The third query about the identity of derived keys is useless in this case, because no new key is derived, but the K_{ASME}, K_{NASenc} and K_{NASint} keys, shared between MS and MME, do not change during the handover.

6. Verification results

As already explained, all handover types have been analyzed considering both the case that the eNB-MME link includes IPsec or physical protection, and the case that it does not. This produces two different models for each handover type: the two models differ only in the definition of the eNB-MME channel (private in the first case, public in the latter case).

It is worth noting that each property has been verified independently. This is necessary not only for limiting the complexity of the analysis, but also because different properties require different assumptions. For example, when verifying backward/forward secrecy, some keys are intentionally disclosed to the attacker, while the same must not happen when verifying other properties.

6.1. LTE to UMTS

Table 1 resumes the results of the formal analysis of the LTE to UMTS handover model.

The second column of Table 1 contains the results of the analysis when the channel between eNB and MME is private, i.e. the adversary has no access to it. These results confirm that all the expected properties hold: all keys (K_{ASME}, K_{eNB} and derived) remain secret; forward and backward secrecy are valid; the payloads are conditionally secret and are not weak-secrets, and authentication properties hold.

The third column of Table 1 refers to the case of a public eNB-MME channel (the adversary can spoof, delete and transmit new messages over the channel). In this scenario, the attacker can know a subset of the LTE keys: K_{eNB} and the derived keys K_{RRCenc}, K_{RRCint} and K_{UPenc}. However, K_{ASME} and the UMTS

keys (CK′/IK′) are kept secret. The disclosure of K_{eNB} makes the LTE payload not secret (the attacker can derive the ciphering key K_{UPenc}), which also invalids the immunity to guessing attacks on the LTE payload. Instead, the secrecy of the UMTS payload is preserved, because CK remains secret, as well as the immunity to guessing attacks on the UMTS payload. In this scenario, backward secrecy is not valid: the attacker directly knows K_{eNB}. Instead, forward secrecy is kept: the attacker never knows K_{ASME}, so he has no way to derive CK′ and IK′. Finally, the authentication between MS and eNB does not hold: an attacker can force a handover of the MS from LTE to UMTS. In fact, the attacker, knowing the IMSI and having access to the eNB-MME channel, can initiate an arbitrary handover by sending a forged HANDOVER REQUIRED message to the MME. The MS cannot recognize the attacker because the handover procedure continues as in a regular handover, and receives a genuine HANDOVER COMMAND message from the network. The attacker never knows K_{ASME}: if the handover completes in the MS, then the MME must have previously derived, in a corresponding session, the CK′ and IK′ keys from K_{ASME}, so MME and MS are correctly authenticated during the handover. Similarly, the attacker has no access to the 3G serving network and, from the previous properties, to the CK′ and IK′ keys: the attacker cannot alter communications between RNC and MS and, when the handover procedure completes, the MS and the UMTS SN are authenticated.

6.2. UMTS to LTE

The same considerations made for the two previous scenarios are also applicable to the other handover procedure, from UMTS to LTE (second and third column in Table 2), with only some differences. The only results that differ are the ones about forward and backward secrecy. In this handover scenario, forward secrecy does not hold because if the attacker knows CK and IK, he can decrypt all the messages between MS and the UMTS network. In this way, the adversary can read the nonce, transmitted from the RNC to the MS, that is used by MME and MS, along with CK and IK, to derive the K'_{ASME} key, and subsequently all the LTE keys. Instead, backward secrecy holds: an attacker

	LTE to UMTS	
eNB-MME channel	private	public
Secrecy of keys	true	false for K_{eNB} and keys derived from K_{eNB}
Conditional secrecy of LTE payload	true	false
Conditional secrecy of UMTS payload	true	true
Forward secrecy	true	true
Backward secrecy	true	false
Immunity to off-line guessing attacks	true	false for payloadLTE, true for payloadUMTS
Auth. MS-eNB	true	false
Auth. MS-MME	true	true
Auth. MS-RNC	true	true

Table 1: Analysis results: LTE to UMTS handover

who knows K_{eNB} cannot derive the previous CK and IK keys.

The results about authentication are the same, albeit their explanation is different. Lack of authentication between MS and eNB, in the last scenario, makes the adversary able to alter all subsequent Access Stratum and User Plane communications between MS and eNB. However, the attacker cannot read and modify Non Access Stratum messages between MS and MME. For this reason MS-MME authentication remains valid: if the handover completes in the MS, then the MME ran a session where the K_{ASME} key was derived, so MME and MS are authenticated during the handover. Finally, before starting the handover, MS-RNC are authenticated, as confirmed by the last query, because the attacker has no access to the UMTS network.

6.3. LTE X2

Table 3 resumes the results of the formal analysis of the LTE X2 handover model.

	UMTS to LTE	
eNB-MME channel	private	public
Secrecy of keys	true	false for K_{eNB} and keys derived from K_{eNB}
Conditional secrecy of LTE payload	true	false
Conditional secrecy of UMTS payload	true	true
Forward secrecy	false	false
Backward secrecy	true	true
Immunity to off-line guessing attacks	true	false for payloadLTE, true for payloadUMTS
Auth. MS-eNB	true	false
Auth. MS-MME	true	true
Auth. MS-RNC	true	true

Table 2: Analysis results: UMTS to LTE handover

In this handover scenario, for the three channels has been considered the possibility that each channel may be insecure. Thus, a total of eight combinations are possible, when channels are alternatively considered as private or public channels. In certain cases, ProVerif is not able to verify all the properties ("unres", i.e. unresolved, cells in Table 3).

In the X2 handover, forward secrecy never holds, as already known from the specifications [1] (TS 33.401).

The columns of Table 3 confirm that the security properties of the current handover procedure are not influenced by the protection on the TeNB-MME channel: this can be explained because the only key that is transmitted on that channel is the Next Hop Key 2, which will be eventually used in the next handover. However, the next handover may be compromised if the attacker has the Next Hop Key 2. If this happens, during the following handover the security properties will not hold.

The fourth and fifth columns consider the case when the the SeNB-TeNB

channel is protected while the SeNB-MME channel lacks protection. In this scenario, the attacker obtains K_{eNB} from the second message, and can derive all the subsequent keys. Moreover, if the TeNB-MME channel is also unprotected (fifth column), the attacker can read the Next Hop Key 2 sent by the MME. Conditional secrecy of payloads is not true, because the ciphering keys are disclosed (ProVerif is not able to resolve the query about payload 2). This implies that the payloads are also reported as weak-secrets, because the attacker knows the exact values from the previous point. Similarly, backward secrecy is not valid because K_{eNB} is directly known by the attacker. Finally, authentication does not hold: the attacker obtains all the keys needed in the handover procedure, thus he can act as fake SeNB and TeNB. Unfortunately, ProVerif cannot resolve the query about the authentication between MS and SeNB, i.e. it cannot complete this verification. However, it can be argued that if the attacker has K_{eNB}, he can replicate the behaviour of the SeNB, thus invalidating this authentication.

The sixth to ninth columns of Table 3 consider the case when the channel between SeNB and TeNB (the X2 interface) is not protected. In this scenario it is clear that the attacker always knows $K^{\star}_{eNB}$. The direct effect is that the authentication between MS and TeNB never holds: in fact the attacker may operate as fake TeNB because all the keys are derived from $K^{\star}_{eNB}$. In particular, the attacker can arbitrarily force a handover execution, by sending a forged HANDOVER REQUEST message to the TeNB. Moreover, Table 3 shows that the protection of the TeNB-MME channel does not influence the security properties apart from the fact that the Next Hop Key 2 is disclosed if the TeNB-MME and SeNB-TeNB channels are public. When the SeNB-MME channel is private (the attacker does not know K_{eNB} and K_{UPenc}), the conditional secrecy of payload 1 (sent before the handover begins) holds, while payload 2 (sent after the handover completion) is always known by the attacker (because it is ciphered with the K_{UPenc} derived from $K^{\star}_{eNB}$), thus the conditional secrecy of payload 2 is false (ProVerif is not able to resolve the queries when the the SeNB-MME channel is public). Similarly, backward secrecy holds only if the SeNB-MME channel is private. Otherwise, the attacker can obtain K_{eNB} and invalidate the property.

Moreover, payload 1 cannot be guessed if the SeNB-MME channel is private: the attacker cannot derive K_{UPenc} because he does not know K_{eNB}. Finally, authentication between MS and SeNB holds only if the SeNB-MME channel is protected. If it is not, the attacker can behave as a fake SeNB (ProVerif is not able to resolve this query).

6.4. LTE S1

Table 4 resumes the results of the formal analysis of the LTE S1 handover model.

In this handover scenario, for the SeNB-MME and TeNB-MME channels, both the case of protected channel and the case of unprotected channel have been considered, for a total of four different scenarios (note that in this kind of handover there is no SeNB-TeNB channel, see Section 5.2.4).

The second column of Table 4 considers the case when both channels are private: all the security properties are verified. Conversely, if both channels are modeled as public channels, none of the properties is verified (ProVerif is not even able to resolve all the queries), as reported in the fifth column of Table 4.

If the SeNB-MME channel is private and the TeNB-MME channel is public (third column of Table 4), the attacker may obtain all the keys used in the TeNB, because all the keys are derived from the Next Hop 2 and the Target Cell ID (which is public). The attacker does not know the keys used in the SeNB, which implies that the conditional secrecy of payload 1 holds. ProVerif is not able to resolve the query about payload 2. However, payload 2 is known by the attacker because he knows all the keys used in the TeNB. The fact that the attacker has all the keys derived in the TeNB also falsifies the queries about forward secrecy (because the attacker may derive $K^{\star}_{eNB}$), and about the MS-TeNB authentication (the attacker has all the keys to act as TeNB). Backward secrecy is verified, which can be explained because the attacker has no way to obtain the initial K_{eNB}. Finally, payload 1 cannot be guessed offline, but payload 2 is known by the attacker because it is received by the TeNB, and the attacker has the keys used in th TeNB.

	LTE X2							
SeNB-TeNB channel	private				public			
SeNB-MME channel	private		public		private		public	
TeNB-MME channel	private	public	private	public	private	public	private	public
Secrecy of keys	true	true	false for K_{eNB} and derived	false for K_{eNB} and derived and NH2 key	false for $K^{\star}_{eNB}$ and derived	false for $K^{\star}_{eNB}$ and derived	false (except K_{ASME} and NH1 key)	false (except K_{ASME}, NH1 and NH2 keys)
Conditional secrecy of LTE 1 payload	true	true	false	false	true	true	false	false
Conditional secrecy of LTE 2 payload	true	true	unres	unres	false	false	unres	unres
Forward secrecy	false	false	false	false	false	false	false	false
Backward secrecy	true	true	false	false	true	true	false	false
Immunity to off-line guessing attacks	true	true	false	false	true for payload 1, false for payload 2	true for payload 1, false for payload 2	false	false
Auth. MS-SeNB	true	true	unres	unres	true	true	unres	unres
Auth. MS-TeNB	true	true	false	false	false	false	false	false

Notes:
unres = unresolved, i.e. ProVerif cannot resolve the query
NH1 = Next Hop 1 key
NH2 = Next Hop 2 key

Table 3: Analysis results: LTE X2 handover

The last scenario, which results are reported in the fourth column of Table 4, considers the case when the SeNB-MME channel is public and the TeNB-MME channel is private. ProVerif is not able to resolve the queries about the secrecy of the keys. However, from the model it is clear that the attacker knows K_{eNB} (from the second message sent by the MME to the SeNB), and is able to derive all the keys used by the SeNB. Thus, the attacker can obtain payload 1, which falsifies its conditional secrecy and off-line guessing resistance. Finally, the attacker may act as SeNB: the authentication between MS and SeNB is not verified by ProVerif, and the attacker can force a handover execution, by sending a forged HANDOVER REQUIRED message to the MME (this is also possible when both channels are public, fifth column). Since the TeNB-MME channel is private, the attacker does not know the keys used in the TeNB. Payload 2 remains conditionally secret and resistant to off-line guessing. Similarly, forward secrecy holds, which can be explained because $K^{\star}_{eNB}$, derived from TeNB, is not known by the attacker, while the backward secrecy query is falsified because the attacker directly knows K_{eNB} from the second message (sent by the MME to the SeNB). Finally, the authentication between MS and TeNB holds, which can be explained because the attacker is not able to obtain the keys used in the TeNB.

7. Conclusions

LTE is the most recent standard in communication systems developed by 3GPP. This paper presented a thorough formal security analysis of handover procedures activated when a mobile device moves between LTE and UMTS networks or between LTE nodes. The tool used to formalize models and to verify procedures is ProVerif, which uses symbolic models based on perfect cryptography assumptions. The results about UMTS-LTE handovers already presented in [4] have been extended with the analysis of new verification scenarios in the presence of emergency calls (in order to check if an attacker can exploit emergency sessions to break the security of the network) and by giving full details about the formal models used for verification and the design choices

	LTE S1			
SeNB-MME channel	private		public	
TeNB-MME channel	private	public	private	public
Secrecy of keys	true	unres for HH2 and TeNB keys	unres	unres
Conditional secrecy of LTE 1 payload	true	true	unres	unres
Conditional secrecy of LTE 2 payload	true	unres	true	unres
Forward secrecy	true	false	true	false
Backward secrecy	true	true	false	false
Immunity to off-line guessing attacks	true	true for payload 1, false for payload 2	true for payload 2, false for payload 1	false
Auth. MS-SeNB	true	true	unres	unres
Auth. MS-TeNB	true	false	true	false

Table 4: Analysis results: LTE S1 handover

adopted in their definition. The results about LTE to LTE handovers (X2 and S1) that were available in the literature have been completed with new results that consider new kinds of properties and new assumptions not previously considered in the literature. In particular, the results already presented by Ben Henda and Norrman [3], regrading authentication and secrecy in LTE X2 and S1 handovers, have been confirmed by this work. For all the considered handover procedures, secrecy of ciphering and integrity keys, conditional secrecy of payloads, forward and backward secrecy of keys, immunity to guessing attacks on payloads and authentication between network components have been analyzed.

3GPP specifies that mobile operators can decide to omit IPsec protection on eNB-MME and eNB-eNB channels, if the interfaces are trusted. However, a definition of "trusted" is not given by 3GPP specifications, but it is left to the mobile operators' discretion. As currently several operators do not protect the eNB-MME and eNB-eNB channels, as reported in [8], the analysis was conducted by considering both the cases of protected and unprotected eNB-MME and eNB-eNB channels. Moreover, since HeNB are often placed in easily accessible locations, the analysis considered the possibility that an attacker succeeds in obtaining the control of the HeNB.

Results confirm that, under the assumptions made, almost all the properties that have been considered hold when eNB-MME and eNB-eNB channels are protected in all the four handover procedures. The only property that does not hold is forward secrecy (as defined in Section 5.2) in the UMTS to LTE and the X2 handovers. Moreover, it is possible to confirm that the emergency sessions do not disclose to the attackers data that can be used to break network security during handover procedures.

In the case of unprotected eNB-MME or eNB-eNB channels, or if the eNB connected to those channels is controlled by the attacker, results show which properties are broken and which remain valid under the assumptions made. When having access to the eNB-MME channels, an attacker can force a handover from LTE to UMTS, or control the Access Stratum and User Plane communications after a handover from UMTS to LTE. However, the main LTE key (K_{ASME}) and

the UMTS keys (CK′/IK′) are kept secret.

In the LTE to LTE procedures a greater number of combinations are possible, because the channels that may be considered insecure are 2 (S1 handover), or 3 (X2 handover). In both the handover cases, the attacker can alter sections, or the entire handover process, depending on which channels he controls.

Finally, results highlight that the handover procedure from UMTS to LTE does not provide forward secrecy of the keys, with respect to the definition given in Section 5.2. Similarly, the X2 handover never guarantees forward secrecy, but this is a precise 3GPP design choice in order to obtain a very fast handover procedure, which is particularly useful for fast-moving users and devices.

A total of 16 ProVerif models have been analyzed. All the handover procedure were verified considering the possibility that the attacker can control the channel between eNB and MME and between eNB and eNB.

References

[1] 3rd Generation Partnership Project (3GPP), cited December 2014. 3GPP specifications. `http://www.3gpp.org/specifications`.

[2] Arapinis, M., Mancini, L., Ritter, E., Ryan, M., Golde, N., Redon, K., Borgaonkar, R., 2012. New Privacy Issues in Mobile Telephony: Fix and Verification. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security. CCS '12. ACM, New York, NY, USA, pp. 205–216.

[3] Ben Henda, N., Norrman, K., 2014. Formal Analysis of Security Procedures in LTE - A Feasibility Study. In: Stavrou, A., Bos, H., Portokalidis, G. (Eds.), Research in Attacks, Intrusions and Defenses. Vol. 8688 of Lecture Notes in Computer Science. Springer International Publishing, pp. 341–361.

[4] Bettassa Copet, P., Marchetto, G., Sisto, R., Costa, L., July 2015. Formal Verification of LTE-UMTS Handover Procedures. In: Computers and Communication (ISCC), 2015 IEEE Symposium on. p. To appear.

[5] Blanchet, B., 2001. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In: 14th IEEE workshop on Computer Security Foundations. pp. 82–96.

[6] Comon, H., Shmatikov, V., 2002. Is it possible to decide whether a cryptographic protocol is secure or not? Journal of Telecommunications and Information Technology, 5–15.

[7] Dolev, D., Yao, A. C.-C., 1983. On the security of public key protocols. IEEE Transactions on Information Theory 29 (2), 198–207.

[8] Donegan, P., 2013. The Security Vulnerabilities of LTE: Risks for Operators. Juniper Networks white paper.

[9] Fang, J., Jiang, R., Sept 2010. An analysis and improvement of 3GPP SAE AKA protocol based on strand space model. In: Network Infrastructure and Digital Content, 2010 2nd IEEE International Conference on. pp. 789–793.

[10] Qachri, N., Markowitch, O., Dricot, J.-M., 2013. A Formally Verified Protocol for Secure Vertical Handovers in 4G Heterogeneous Networks. International Journal of Security and Its Applications.

[11] Tang, C., Naumann, D. A., Wetzel, S., 2012. Symbolic Analysis for Security of Roaming Protocols in Mobile Networks. In: Rajarajan, M., Piper, F., Wang, H., Kesidis, G. (Eds.), Security and Privacy in Communication Networks. Vol. 96 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer Berlin Heidelberg, pp. 480–490.

[12] Tsay, J.-K., Mjølsnes, S., 2012. A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols. In: Kotenko, I., Skormin, V. (Eds.), Computer Network Security. Vol. 7531 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 65–76.

[13] Zhang, M., Fang, Y., March 2005. Security analysis and enhancements of 3GPP authentication and key agreement protocol. Wireless Communications, IEEE Transactions on 4 (2), 734–742.

Appendix A. Proverif Models

Figure A.7 contains an excerpt of the ProVerif model used to verify the LTE to UMTS handover procedure. The LTE to UMTS handover ProVerif model

is used here for describing how the security properties specified in section 5.3 have been expressed in ProVerif. All the other handover models follow the same modeling technique.

The security properties specified in section 5.3 have been expressed in ProVerif as follows (line numbers refer to the LTE to UMTS ProVerif code in Figure A.7):

- *Secrecy of keys*: secrecy is expressed by means of the ProVerif attacker query (lines 4, 5).
- *Conditional secrecy of payloads*: the fact that the terms `payloadLTE` and `payloadUMTS`, used to represent the data transferred between MS and eNB/RNC (when an emergency session is not active), must be kept secret if encryption is enabled is expressed using an equivalent formulation: if the attacker knows the secret payload, then the event `disableEnc` must have been previously executed (lines 13, 14).
- *Forward secrecy and backward secrecy of keys*: ProVerif provides a dedicated feature (the `phase` instruction) for checking forward and backward secrecy. The following lines show how forward secrecy is verified in the LTE to UMTS handover [2]:

```
...
(* verify forward secrecy *)
query attacker(payloadUMTS) phase 1.
...
let processMS(uecaps:bset) =
 (* complete handover procedure *)
 ...
 phase 1;
 out(pubChannel,(kenb_ue));
 0.
...
```

The `phase` instruction in the `processMS` process breaks the protocol into two phases: phase 0 (the default phase) contains all the instructions and communications that are performed before reaching the instruction `phase 1`. When the latter instruction is reached (i.e. the handover has completed

[2] these lines are not displayed in Figure A.7 for simplicity

successfully) a new phase (phase 1) begins. In phase 1, only the statements defined after the `phase 1` instruction are executed (in this case, the K_{eNB} key is disclosed), but the adversary keeps all the knowledge acquired during the previous phase (e.g. all the messages exchanged), and integrates it with new terms, if possible (the K_{eNB} key in the example). Similarly, the queries that specify a `phase n` condition are evaluated only after the beginning of phase *n*. In this excerpt of code, ProVerif evaluates the query when the attacker knows K_{eNB}.

- *Immunity to off-line guessing attacks*: The query `weaksecret`, available in ProVerif to specify that a term must not be a weak-secret, i.e. that the adversary must not be able to distinguish a correct guess of the secret term from an incorrect guess, is used to specify that the payloads must not be weak secrets (lines 16, 17).
- *Authentication*: Authentication properties are specified as correspondence queries in ProVerif (lines 6 - 12, 29). For example, the authentication requirement expressed as

  `inj-event(endMS_ENB(x1,x2))` ⇒ `inj-event(begMS_ENB(x1,x2))`

  means that each time the event `endMS_ENB(x1,x2)` in the eNB process occurs, the MS process has previously started a session of the protocol (i.e. event `begMS_ENB(x1,x2)` has occurred).

```
free pubChannel: channel. free secureChannelEnbMme: channel [private].
const HO_REQUIRED:msgHdr. const FWD_RELOC_REQ:msgHdr. const ID:msgHdr.
table keys(ident , asmeKey). table capab(ident , bool).
query attacker(new kasme_ue).
query attacker(kdf_enb(new kasme_ue)).
query x1: ident, x2: enbKey;
 inj-event(endMS_ENB(x1, x2)) ==> inj-event(begMS_ENB(x1, x2)).
query x1: ident, x2: ckKey, x3: ikKey;
 inj-event(endRNC_MS(x1, x2, x3)) ==> inj-event(begRNC_MS(x1, x2, x3)).
query x1: ident, x2: asmeKey, x3: bitstring, x4: ckKey, x5: ikKey;
 inj-event(endMME_MS(x1, x2, x3, x4, x5))
                      ==> inj-event(begMME_MS(x1, x2, x3, x4, x5)).
query attacker(payloadLTE) ==> event(disableEnc).
query attacker(payloadUMTS) ==> event(disableEnc).
...
weaksecret payloadLTE.
weaksecret payloadUMTS.
...
let processMS(uecaps:bset) =
 new imsi_ue: ident;
 let cap_ue: bool suchthat mem(cap_ue , uecaps) in
 new kasme_ue: asmeKey;
 insert capab(imsi_ue, cap_ue); insert keys(imsi_ue, kasme_ue);
 (* key derivation from Kasme *)
 let knasenc_ue: nasEncKey = kdf_nas_enc(kasme_ue) in
 let knasint_ue: nasIntKey = kdf_nas_int(kasme_ue) in
 let kenb_ue: enbKey = kdf_enb(kasme_ue) in
 ...
 event begMS_ENB(imsi_ue, kenb_ue);
 out(pubChannel, (ID, imsi_ue, cap_ue));
 if cap_ue = true then ( (* encryption enabled inside this branch *)
  ...
 )else(
  if cap_ue = false then ( (* encryption disabled inside this branch *)
   event disableEnc;
   ...
  )else ( 0 )
 ).
...
let processMME =
 in(pubChannel, (=ID, imsi_mme: ident, cap_mme_recv: bool));
 get keys(=imsi_mme, kasme_mme) in ( get capab(=imsi_mme, cap_mme) in
  let knasenc_mme: nasEncKey = kdf_nas_enc(kasme_mme) in
  new nasDownlinkCount: bitstring;
  let ck'_mme: ckKey = kdf_ck'(kasme_mme,nasDownlinkCount) in
  let ik'_mme: ikKey = kdf_ik'(kasme_mme,nasDownlinkCount) in
  ...
 ).
process
 let uecaps = consset (true, consset (false, emptyset)) in
 ((!processMS(uecaps)) | (!processENB) | (!processMME) |
  (!processMSC) | (!processRNC))
```

Figure A.7: An excerpt of the LTE to UMTS handover