POLITECNICO DI TORINO
Repository ISTITUZIONALE

Formal Verification of LTE-UMTS Handover Procedures

Original
Formal Verification of LTE-UMTS Handover Procedures / BETTASSA COPET, P., Marchetto, G., Sisto, R., Costa, L.. - STAMPA. - (2015), pp. 738-744. (20th IEEE Symposium on Computers and Communications (ISCC) Larnaca, Cyprus 6-9 July 2015) [10.1109/ISCC.2015.7405602].

Availability:
This version is available at: 11583/2621605 since: 2016-09-08T16:05:25Z

Publisher:
IEEE

Published
DOI:10.1109/ISCC.2015.7405602

Terms of use:

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

Publisher copyright

(Article begins on next page)

13 June 2026

©2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. This is the author's postprint version (i.e. as edited by the author after refereeing but without copy-editing, proofreading and formatting added by IEEE). The final version of this paper can be accessed at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7405602

Formal Verification of LTE-UMTS Handover Procedures

Piergiuseppe Bettassa Copet, Guido Marchetto, Riccardo Sisto
Dipartimento di Automatica e Informatica
Politecnico di Torino
Italy
Email: piergiuseppe.bettassa,guido.marchetto,riccardo.sisto@polito.it

Luciana Costa
Telecom Italia Information Technology
Italy
Email: luciana.costa@it.telecomitalia.it

***Abstract*—Long Term Evolution (LTE) is the most recent standard in mobile communications, introduced by 3rd Generation Partnership Project (3GPP). Most of the formal security analysis works in literature about LTE analyze authentication procedures, while interoperability is far less considered. This paper presents a formal security analysis of the interoperability procedures between LTE and the older Universal Mobile Telecommunications System (UMTS) networks, when mobile devices seamlessly switch between the two technologies. The ProVerif tool has been used to conduct the verification. 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, if all the protections allowed by the LTE standard are adopted. If backhauling traffic is not protected with IPSec, which is a common scenario since the use of IPSec is not mandatory, some security properties still hold while others are compromised. Consequently, user's traffic and network's nodes are exposed to attacks in this scenario.**

***Index Terms*—Formal verification; LTE; UMTS; ProVerif; handover; security**

I. 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.

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. The differences between the two technologies require non-trivial procedures for 3G-4G interoperability. The 3GPP (3rd Generation Partnership Project)[1] has defined such procedures, in order to ensure continuity of service to users who move, for example, from an area which is covered by both 4G and 3G networks to an area with only 3G network coverage or vice versa.

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 which allow user mobility in these networks. As a consequence, not all the possible mobility scenarios already have a formal analysis.

The so called Intra-Handover procedures adopted when a user moves between different LTE cells have been recently analyzed in [2], while a formal analysis of the handover procedures that enable users to seamlessly switch from a 3G to a 4G connection, and vice versa, have not yet been analyzed.

This paper presents a formal analysis that fills this gap. The procedures analyzed in this paper have been defined by 3GPP as IRAT (Inter-Radio Access Technology) handover procedures, i.e. 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). The tool used for formal analysis is ProVerif [3], which is an automatic formal verifier for cryptographic protocols. ProVerif is based on symbolic Dolev-Yao models [4], where cryptography is assumed to be perfect (e.g. the attacker cannot decipher a message unless he knows the correct deciphering key) and the attacker is assumed to have full access to public communication channels, on which he can read, delete and send messages (any message that the attacker can create with its current knowledge can be sent by the attacker on public channels).

The security properties that are considered in this paper are secrecy of all the keys used before, during and after the handovers, secrecy of payloads exchanged and authentication between network components. In addition to the bare security properties mentioned above, this work also analyses some more specific cryptographic properties: 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, allowed by the standards, and common in real

network deployments where IP network security mechanisms are omitted, the aforementioned security properties in the models that have been developed are only in part assured. In these cases, confidentiality of user data traffic is not always provided, and the lack of authentication between network elements makes injection of fake signalling messages possible. This kind of result may be interesting especially for mobile operators, who have to assess security risks in their networks.

The complete ProVerif handover models are available for download at the URL http://staff.polito.it/riccardo.sisto/lte.umts.handover/models.zip

The remainer of the paper is organized as follows. Section II gives some background about LTE and UMTS network architectures, key hierarchies and ProVerif. Then, Section III explains the handover procedures that have been analyzed and Section IV the expected security properties that have been specified. Finally, Section V presents the results of the formal analysis and the potential threats that could be used to break into the networks, Section VI discusses related work and Section VII concludes.

II. Background

A. LTE and UMTS 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].

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 MS 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 network of 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 AuC contains authentication data shared with the USIM. These data are stored permanently in the USIM and AuC when the USIM is made, in addition to the information

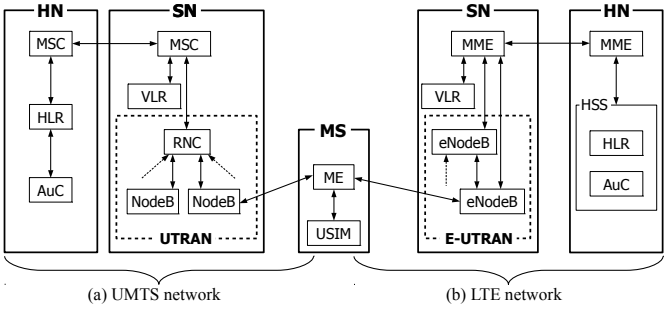

Fig. 1. UMTS and LTE network architectures

of the operator, IMSI and the secret key K_i. 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 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 and 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. 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.

Key hierarchy in LTE and differences with UMTS. The first procedure done by a mobile device that wants to connect to the network is the authentication and key agreement procedure (called AKA). 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 some randomly generated values. Details of authentication procedures can be found in [1] (TS 33.401). The keys are renewed periodically to prevent possible attacks due to encryption of large volumes of data with the same keys.

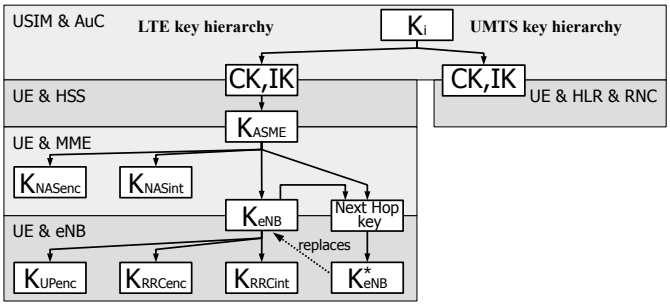

Fig. 2. LTE and UMTS key hierarchies

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), that 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. LTE provides two mechanisms of protection for two different classes of control traffic (Control Plane): the first is the Non Access Stratum (NAS), and the second is the Access Stratum (AS). 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) represents the control messages between MS and eNB. For this reason, two keys are derived from K_{ASME}, K_{NASenc} and K_{NASint}, respectively used for encryption and 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, which belongs to the 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 [2] respectively.

B. ProVerif overview

ProVerif [3] is a tool for automatic formal verification of cryptographic protocols based on theorem-proving, where the protocol actors and the attacker are modeled according to the symbolic approach defined by Dolev-Yao [4]. In this model, the attacker has complete control over public communications channels and can read, delete, and modify messages in transit over them or forge new messages. Private channels, instead, are not accessible by the attacker. They are used to model secure channels (e.g. channels with wire-level protection). The symbolic representation of data and cryptography implies that encryption is considered ideal.

As the possible behaviors of the attacker are already predefined 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, differently from model checkers, which can only analyze bounded systems.

Because of the inherent undecidability of the formal verification problem, 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.

III. Handover procedures

Handover procedures are activated by the serving network (eNB in LTE, RNC in UMTS) when the strength of the radio signal between mobile station and the current eNB/RNC becomes too much degraded. The decision of performing an 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 an handover to a network with other technology is executed.

Inter Radio Access Technology (Inter-RAT) handovers allow voice and data service to maintain the connection while moving from a radio access technology (GSM, UMTS, LTE, WiMAX or any other wireless technology) to another.

Figure 3 depicts the simplified message exchange flow performed during Inter-RAT handover from LTE to UMTS, as modeled in ProVerif for the verification of the handover procedure. This model has been derived from the 3GPP TS 23.401 and TS 33.401 [1] specifications but it contains only data and operations related to cryptography and authentication, while resource allocation and relocation have been omitted, because they are not relevant for the analysis performed by ProVerif.

Figure 3 starts with a set of interactions between MS and MME which are not real message exchanges but are used in the model in order to create the same security context

that is assumed to be established by the AKA procedure. In particular, for each protocol session, a fresh IMSI is generated, a nondeterministic choice is made to decide whether encryption will be activated or not for that session, and a fresh K_{ASME} key (which in reality is established during the AKA) is generated. Encryption selection and K_{ASME} are inserted as values into two perfect hash tables named `capab` and `keys`, bound to the corresponding IMSI, which is used as a key in the tables. These tables are private, i.e. not accessible by the attacker, and shared with the MME. In this way it is ensured that in this phase the K_{ASME} is not revealed to the attacker but it is shared by MS and MME, as guaranteed by the AKA procedure. At the same time, IMSI and encryption selection are also transmitted on the public channel from MS to MME thus allowing the attacker to get them, as their secrecy is not guaranteed by the AKA procedure. Key K_{eNB} is derived from K_{ASME} and transmitted on the channel between MME and eNB.

The third message (named `payloadLTE`) represents a user data plane exchange between MS and eNB done before the handover procedure. 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 the 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 the 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 an 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 and agree upon the encryption algorithm, using the SMC (SECURITY MODE COMMAND) and the SMC COMPLETE messages. The last message (named `payloadUMTS`) represents data exchange after the handover.

The handover from UMTS to LTE is similar to the previous one, but with the network roles reversed. The RNC takes the decision to initiate an handover, and sends a RELOCATION REQUIRED message to the connected MSC. The core of the procedure is still carried out by the MME, which receives a FORWARD RELOCATION REQUEST containing the MS identity and the UMTS CK/IK keys. 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}. Then, the MME sends the identity of the MS and the K_{eNB} key to the target eNB, which can activate the access procedures with the SECURITY MODE COMMAND message.

Communication among components of the home and serving network should be secured by the mobile operators who own the networks. While the risk of attacks on the 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 HeNB-MME link, because Home-eNB nodes are often located in publicly accessible locations, and hence they may be tampered by a malicious attacker. The 3GPP TS 33.820 [1] specification specifies that the eNB-MME connection 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, several operators avoid using IPsec on their networks. Reasons might be several: some 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 is available in [5]. Given this scenario, in our analysis we assume that the MME-MSC and MSC-RNC links are secure channels, not accessible by the attacker, whereas for the eNB-MME link we explore both the case that the channel is secured by IPsec, and hence not accessible by the attacker, and the case that an attacker may be able to control the channel between eNB and MME, which is a possibility if the operator does not use the IPsec protection for this channel and the attacker succeeds in having access to a trusted interface.

IV. Security properties

The main security properties that the handover procedures are expected to guarantee have been specified as follows:

- *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, but integrity protection is mandatory. Accordingly, the private (i.e. initially not known to the attacker) terms `payloadLTE` and `payloadUMTS`, used to represent data transfer between MS and eNB/RNC, must be kept secret if encryption is enabled.
- *Forward secrecy and backward secrecy* are properties of key-agreement protocols. Forward secrecy means that the compromise of a secret key must not affect the confidentiality of future keys. In the same way, backward secrecy means that the compromise of a secret key must not affect the confidentiality of earlier keys. 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

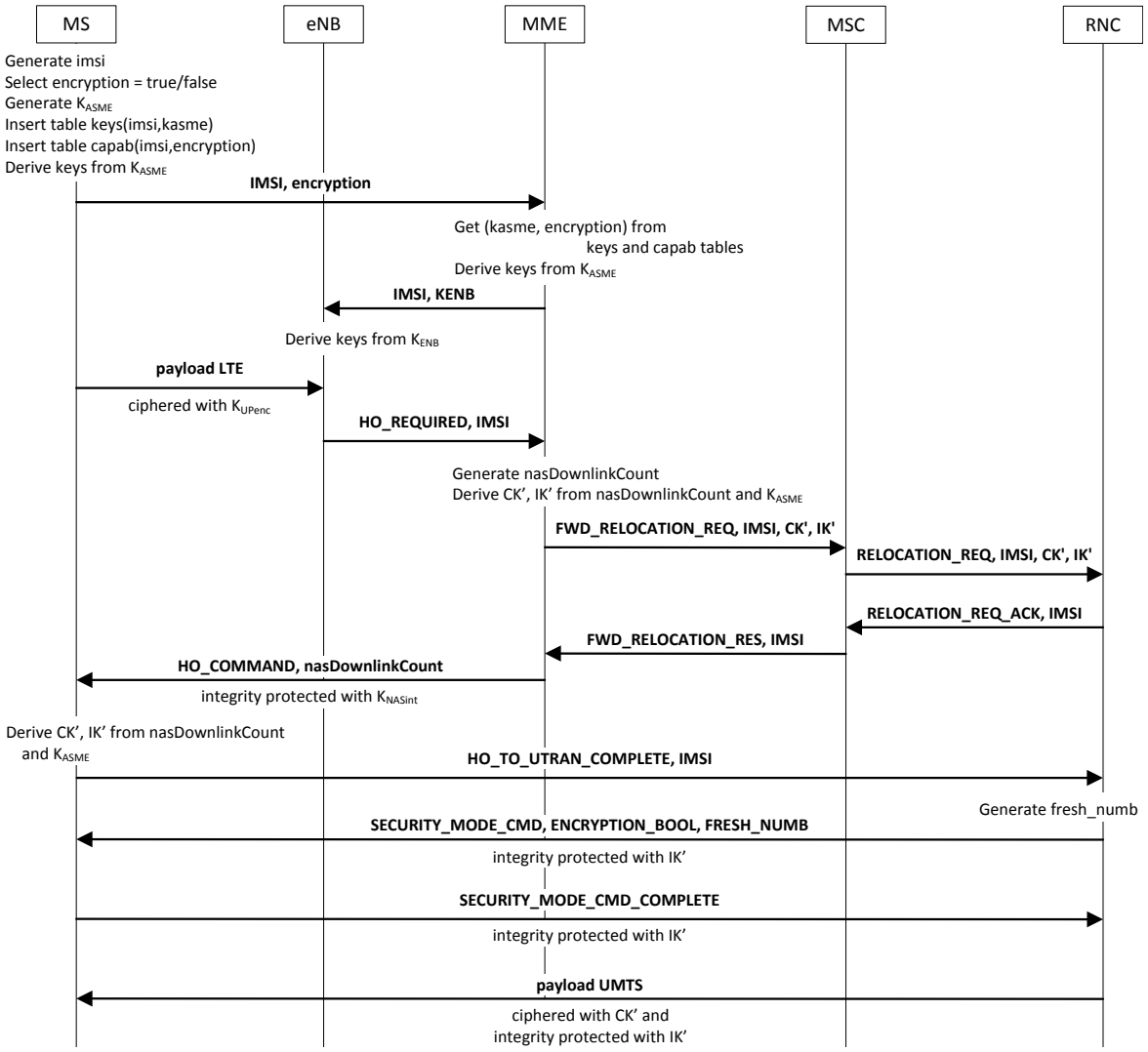

Fig. 3. LTE to UMTS handover

inability of the attacker to derive LTE keys (K'_{ASME}, K_{eNB}) when he knows CK and IK. Backward secrecy is defined as the inability of the attacker to derive K_{eNB} from CK' and IK' in the first case, and to derive CK and IK from K_{eNB} in the second case.

- *Immunity from 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 `payloadLTE` and `payloadUMTS` represent data that could be guessed, so it is specified that they must not be weak-secrets.
- *Authentication*: the following authentication properties between the MS and the SN (eNB and RNC) are specified in the model: (i) the MS is authenticated to the source network, (ii) the MS is authenticated to the target network, (iii) each time the MS successfully concludes an handover, then the MME previously derived the same keys (K'_{ASME} or CK'/IK').

As already explained, both the handover types have been analyzed, considering both the possibility that the eNB-MME link includes IPsec protection, or lacks it. 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).

The complete ProVerif handover models are available for download at the URL http://staff.polito.it/riccardo.sisto/lte.umts.handover/models.zip

V. Results and security issues

Table I resumes the results of the formal analysis of the handover models.

The second column of Table I contains the results of the analysis of the handover from LTE to UMTS, when the channel between eNB and MME is private (i.e. IPsec protection is enabled). These results confirm that all the expected properties hold: all keys (K_{ASME}, K_{eNB} and derived) remain secret; forward

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

TABLE I
ANALYSIS RESULTS

and backward secrecy are valid; the payloads are conditionally secret and are not weak-secrets, and authentication properties hold.

The third column of Table I refers to the same LTE to UMTS model, but with 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 from guessing attacks on the LTE payload. Instead, the secrecy of the UMTS payload is preserved, because CK remains secret, as well as the immunity from 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 an 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 the K_{ASME} key: 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, MS and UMTS SN are authenticated.

The same considerations made for the two previous scenarios are also applicable to the other handover procedure, from UMTS to LTE (fourth and fifth columns in Table I), with only some differences. The only results that differ are the ones about forward and backward key 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 who knows K_{eNB} cannot derive the previous CK and IK keys. It is worth noting that each property has been verified independently, this implies that, for example, the secrecy of the UMTS payload holds even if the attacker is assumed to know CK and IK when performing the backward secrecy verification in the UMTS to LTE handover. In fact, when verifying backward/forward secrecy, the keys are intentionally disclosed to the attacker, while the same does not happen during verification of other properties.

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.

VI. RELATED WORK

The most closely related work is a recent paper by Ben Henda and Norrman [2] who used ProVerif to analyze the LTE

procedures for 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 security control procedure, i.e. security algorithm negotiation between mobile device and MME, NAS Service Request Procedure (security algorithm negotiation between mobile device and eNodeB), X2 handover (handover between two eNodeB without MME intervention), and S1 handover (handover between two eNodeB with MME intervention). Results of the analysis show that secrecy and agreement properties hold as expected. Differently from our work, the analysis in [2] does not consider the possibility that data encryption may be disabled as allowed by the standard [1] (TS 33.401) nor does it check immunity from guessing attacks.

In general, the research community manly focused on analyzing the AKA procedure and on proposing improvements in that procedure ([6], [7], [8] and [9]). LTE and UMTS authentication procedures are very similar. 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. [10] used ProVerif to analyze privacy aspects of UMTS. As the paging procedure analyzed is the same in LTE and UMTS technologies, the results are valid for both networks.

Qachri et al. [11] proposed and analyzed 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 3GPP standards.

VII. Conclusion

LTE is the most recent standard in communication systems developed by 3GPP. This paper presented a formal security analysis of handover procedures between LTE and UMTS networks using symbolic models based on perfect cryptography assumptions. The tool used to formalize models and to verify procedures is ProVerif. Up to our knowledge, this is the first work that has formally analyzed the security of LTE-UMTS handover procedures. The properties that have been verified are: secrecy of ciphering and integrity keys, conditional secrecy of payloads, forward and backward secrecy of keys, immunity from guessing attacks on payloads and authentication between network components.

3GPP specifies that mobile operators can decide to omit IPsec protection on eNB-MME 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 channels, the analysis was conducted by considering both the cases of protected and unprotected eNB-MME channels.

Results confirm that, under the assumptions made, almost all the properties that have been considered hold when eNB-MME channels are protected. The only property that does not hold is forward secrecy (as defined in Section IV) in the UMTS to LTE handover. Instead, all properties hold in the LTE to UMTS handover.

In the case of unprotected eNB-MME channels, 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 an handover from LTE to UMTS, or control the Access Stratum and User Plane communications after an handover from UMTS to LTE. However, the main LTE key (K_{ASME}) and the UMTS keys (CK'/IK') are kept secret.

Future works will address the verification of other LTE handover procedures, for example handover between LTE and other network technologies (e.g. WiFi, WiMax).

References

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

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

[3] B. Blanchet, "An Efficient Cryptographic Protocol Verifier Based on Prolog Rules," in *14th IEEE workshop on Computer Security Foundations*, 2001, pp. 82–.

[4] D. Dolev and A. C.-C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–207, 1983.

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

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

[7] J.-K. Tsay and S. Mjølsnes, "A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols," in *Computer Network Security*, ser. Lecture Notes in Computer Science, I. Kotenko and V. Skormin, Eds. Springer Berlin Heidelberg, 2012, vol. 7531, pp. 65–76.

[8] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *Wireless Communications, IEEE Transactions on*, vol. 4, no. 2, pp. 734–742, March 2005.

[9] J. Fang and R. Jiang, "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*, Sept 2010, pp. 789–793.

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

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