IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

STUDY ON PROTECTION OF ENTRUST KEY MANAGEMENT IN 4G LTE NETWORKS

S.Sindhu*, L.Gomathi

* Msc.,Mphil Research Scholar in Computer Science,Muthayammal College of Arts and Science,Rasipuram,Tamilnadu,India.

MCA., M.Phil.,Research Supervisor in Computer Science,Muthayammal College of Arts and Science,Rasipuram,Tamilnadu,India.

ABSTRACT

To minimize a security gap in the networks which a single compromised or malicious device can expose an entire mobile network because of the open nature of these networks. The attacker can launch a variety of active and passive attacks. Thus security mechanism is to be defined for call security in 4G/LTE network. The existing scheme includes plain-text certificate key authentication and cryptographic key exchanges. Thus the set of cryptographic key exchange schemes can effectively establish the secure communications between the two nodes and protect against the node emulation attacks. In this paper the traditional key exchange models of 4G/LTE network and hybrid cryptographic key exchange model and the security provided by these are evaluated. The proposed model will protect the 4G network during the initial call setup phase, periodic time based key exchange to ensure the call security and the seed exchange for the other end integrity check. The proposed model will use a pre-shared key group to ensure the security during the call setup phase and will use the random table based non-predictive key exchange model for the purpose of in-call security assurance and receiver integrity check by the caller.

KEYWORDS: evolved NODEb (eNODEb), Mobile Management Entity, Authority Certificate, Target Enb Node, Request/Response, Ciphering Key.

INTRODUCTION

Handover key management in the 3GPP LTE/SAE has been designed to revoke any compromised key(s) and as a consequence isolate corrupted network devices. This paper, however, identifies and details the vulnerability of this handover key management to what is called desynchronization attacks; such attacks jeopardize secure communication between users and mobile networks. Although periodic updates of the root key are an integral part of handover key management, our work here emphasizes how essential these updates are to minimizing the effect of desynchronization attacks that, as of now, cannot be effectively prevented.

OBJECTIVE

The goal of 3GPP Long Term Evolution / System Architecture Evolution (LTE/SAE) is to move mobile cellular wireless technology into its fourth generation.

Our main contribution, however, is to explore how network operators can determine for themselves an optimal interval for updates that minimizes the signaling load they impose while protecting the security of user traffic. Our analytical and simulation studies demonstrate the impact of the key update interval on such performance criteria as network topology and user mobility. Recent increases in mobile data usage and the emergence of new applications drive the motivation to move the 3GPP into the fourth generation of cellular wireless technology. In response, designers of the 3GPP Long Term Evolution/System Architecture Evolution (LTE/SAE) system have announced the Evolved Packet System (EPS) as the fourth generation of the 3GPP mobile network.

The access network used in the EPS network improves radio access technologies of the 3GPP mobile networks so as to offer a higher data rate with low latency. The EPS is also designed to support flat Internet Protocol (IP) connectivity and full interworking with heterogeneous radio access networks and service providers. This architectural design decision brings to the fore implications of LTE/SAE for security. The flat all-IP architecture allows all radio access protocols to terminate in one node called evolved NodeB (eNodeB). In the Universal Mobile Telecommunications System (UMTS), the functionality of eNodeB was divided into NodeB and the Radio Network Controller (RNC). The placement of the radio access protocols in eNodeB makes them vulnerable to unauthorized access because eNodeB is located in unattended place.

Further, internetworking with heterogeneous radio access networks exposes the vulnerability of these networks to direct external threats and carries grave implications for LTE security. The unique characteristics of LTE/SAE gave rise to a number of features in the design of the security mechanism in the EPS network. Of these, key management in handovers and minimizing the security risk involved is the focus of this paper. The main threat to handover key management is that an attack will compromise session keys in a base station. Handover key management typically alleviates this threat through separation of the session keys in a handover between base stations.

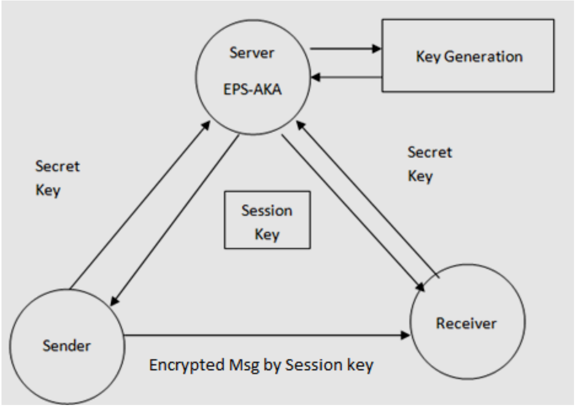


Figure 1. Validation of Session keys

This separation keeps a session key compromised in one base station from any compromising another base station; in other words, the goal is to keep security breaches as local as possible. For reasons of efficiency, handover preparations in LTE/ SAE do not involve the core network. Source eNodeB provides a session key to target eNodeB for use after the handover. In this way, the core network does not need to maintain a state of individual User Equipment (UE). In this design, handing over an unchanged session key would permit target eNodeB to know which session key the source eNodeB used.

To prevent this, the source eNodeB computes a new session key by applying a one-way function to a current session key. This ensures backward key separation in the handover. However, backward key separation blocks an eNodeB only from deriving past session keys from the current session key. Otherwise, this eNodeB would know all session keys used in further sessions in a whole chain of handovers. As a consequence, forward key separation was introduced to ensure that network elements add fresh materials to the process of creating a new session key for the next serving eNodeB. The current eNodeB, unaware of this additive, would be unable to derive the next key. We were able to demonstrate that, under certain circumstances, handover key management fails to ensure forward key separation against a variant attack by a rogue base station; such an attack is referred to as a desynchronization attack.

RELATED WORK

Desynchronization Attack

A desynchronization attack prevents a target eNodeB from maintaining the freshness of the hand over key. The vulnerability of this synchronization to disruption represents a potential security flaw in handover key management that could allow an adversary to compromise all future keys between a specific user and subsequent eNodeBs. This attack may continue until the next update of the root key when handover key materials are generated from scratch instead of by derivation from the previous key. At this point, a potentially devastating effect through a compromised key comes to an end. Without delving into the technical challenges of a specific solution to prevent a desynchronization attack, the most practical remedy is to periodically refresh the root key. A very short-term root key seems an intuitive solution to minimizing the impact of a compromised key.

However, frequent refreshing is not considered the best operational choice because of the signaling load that such root key updating imposes. On the other hand, the longer the update interval the more packets are exposed to a desynchronization attack. The key question network operators and service providers might have is how to effectively choose a root key update interval that is the best balance between the signaling load and the number of user data packets exposed to attack because of a compromised handover key.

The main contributions of this paper are three fold:

1) We identified flaws in the handover key management of the EPS security mechanism;
2) We designed a promising mathematical model for the EPS handover key management to measure the effect of a compromised key; and
3) We investigated the performance criteria (e.g., user mobility, network topology and so on) involved in selecting an optimal operational point for key updating.Extensive simulation results validate the analytical model and reveal how the optimal key update interval changes in practice.

Unfortunately, because this value is so dependent on time and place, a universally acceptable interval does not exist. Nor are there any proven ways to arrive at acceptable tradeoffs appropriate to different circumstances. In the face of this threat to the next generation of cellular networks, the motivation of this paper is to determine how to formulate this value to fit the circumstances of time and place. As a first step toward a formula for an acceptable tradeoff, we diagramed the timing of handover key management in terms of the root key update interval as a way to measure the period during which a compromised key is operative. We then investigated a mathematical model to measure the expected operative period of the compromised key and to represent the expected value of the signaling load and volume of compromised packets during this period.

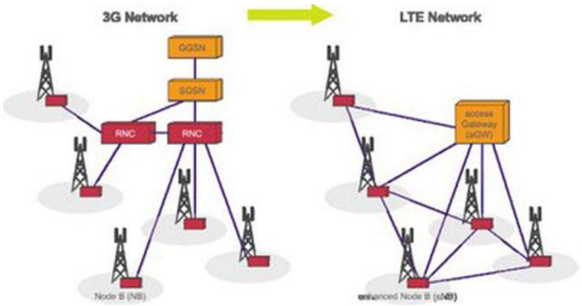


Figure 2. 3G Network Vs LTE Network

Our methodology permits optimal management of the root key update interval according to network policies. This optimal interval is a value that minimizes the signaling traffic overhead required to update the root key while simultaneously limiting the volume of packets exposed to the compromised key.

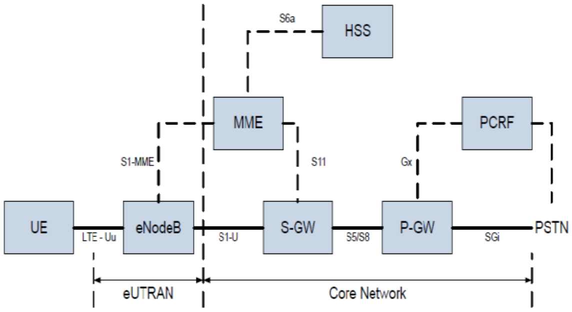


Figure 3. Composing Key between eNodeB

PROBLEM DEFINITION

EPS-AKA

EPS network, an Authentication and Key Agreement (EPS-AKA) occurs between a UE and the MME on behalf of the Home Subscriber Server (HSS)/Authentication Center (AuC). The EPS-AKA is the EPS security mechanism to execute 1) authentication between a UE and an MME on behalf of the HSS/AuC, and 2) a key agreement between a UE and an MME as well as between a UE and eNodeB. Authentication succeeds; the two parties generate the first intermediate key, KASME, from the permanent master key, K. In the course of performing EPS-AKA, the HSS/AuC delivers the first intermediate key to the MME after binding to the serving network identity the evolution to LTE and its flat all-IP core network emphasizes the urgent need for a revision of the trust relationships between operators and network components. Any threats arising from untrusted networks are alleviated in the EPS by a new feature, namely cryptographic network separation. Network separation tries to isolate the impact of any security breach in the local network and prevent its spillover to other networks. This is achieved by binding any cryptographic keys to the identity of the serving network for which the keys are intended. The UE can ensure that it communicates with the intended serving network by authenticating an identity in the current network. In the UMTS, a UE was unable to authenticate a serving network. The local master key, KASME, also called the first intermediate key, is valid at a maximum interval determined by the timing of the next EPS-AKA procedure.

The UE can choose to invoke the EPS-AKA protocol whenever the serving MME changes because of roaming to another serving network. In the same situation, the UE also can choose to transfer the security context between the old and new MMEs in an effort to lower the overhead of the full EPS-AKA. The UE may, of course, also need to run the EPS-AKA protocol periodically without interrupting service. Hence, the frequency of EPS-AKA runs is rather random or configurable by a network operator.

METHODOLOGY

The protocol, known as 3GPP AKA, is based on the security framework in GSM and provides significant enhancement to address and correct real and perceived weaknesses in GSM and other wireless communication systems. 3GPP AKA protocol is vulnerable to a variant of the so-called false base station attack. The vulnerability allows an adversary to redirect user traffic from one network to another. It also allows an adversary to use authentication vectors corrupted from one network to impersonate all other networks. Security problems in the 3GPP AKA, we then present a new authentication and key agreement protocol which defeats redirection attack and drastically lowers the impact of network corruption. The protocol, called AP-AKA, also eliminates the need of synchronization between a mobile station and its home network. AP-AKA specifies a sequence of multiple flows.

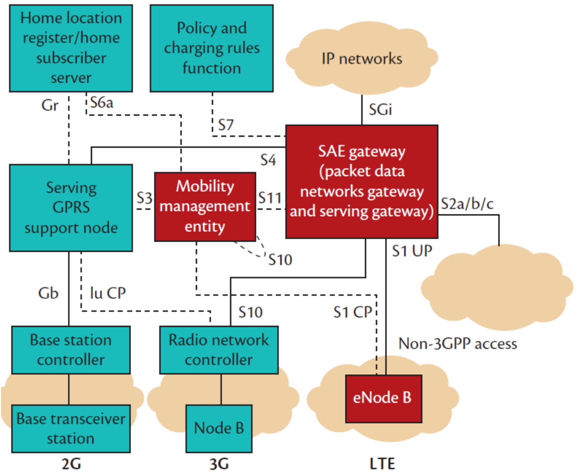

Home location register/home subscriber server
Policy and charging rules function
IP networks
Gr
S6a
S7
SGi
S4
SAE gateway (packet data networks gateway and serving gateway)
Serving GPRS support node
S3
Mobility management entity
S11
S2a/b/c
S10
S1 UP
Gb
Iu CP
S10
S1 CP
Non-3GPP access
Base station controller
Radio network controller
eNode B
Base transceiver station
Node B
2G
3G
LTE

Figure 4. Transfer of messages between nodes.

Our proposed method an unchanged session key would permit target eNodeB to know which session key the source eNodeB used. To prevent this, the source eNodeB computes a new session key by applying a one-way function to a current session key. This ensures backward key separation in the handover. However, backward key separation blocks an eNodeB only from deriving past session keys from the current session key.

Otherwise, this eNodeB would know all session keys used in further sessions in a whole chain of handovers. As a consequence, forward key separation was introduced to ensure that network elements add fresh materials to the process of creating a new session key for the next serving eNodeB. The current eNodeB, unaware of this additive, would be unable to derive the next key.

Benefits In The Proposed System

1) We identified flaws in the handover key management of the EPS security mechanism;
2) We designed a promising mathematical model for the EPS handover key management to measure the effect of a compromised key;
3) We investigated the performance criteria (e.g., user mobility, network topology, and so on) involved in selecting an optimal operational point for key updating.

IMPLEMENTATION

Optimal Key Management

The EPS supports two types of handovers that are referred to as intra- and inter-MME handovers, with the names reflecting the anchor points involved. In the intra-MME handover, preparation for it occurs between the source and target eNodeBs in the same MME through a direct interface between base stations. In contrast, in the inter-MME handover, the preparation occurs via the MME without any direct signaling between base stations. As an alternative to the inter-MME handover, the UE and the MME may decide to run the full EPS-AKA to generate all security contexts from scratch. This alternative is more common in the inter-MME handover for security reasons. If different providers operate the two MMEs, the link between them is far from secure.

In this paper, we only consider the intra-MME handover in discussing the security weakness of key management in the handover because any security risks related to the inter-MME handover can be eliminated by running the full EPS-AKA. Before the next EPS-AKA, a set of KeNB are linked to each other in what is known as handover key chaining to achieve backward key separation, source eNodeB generates the next KeNB from the current one by applying a one-way hash. An MME can provide fresh keying material to the target eNodeB only after the inter-eNodeB handover, and this fresh material is to be used in the next handover.

The result is two-hop forward key separation in which the source eNodeB does not know the target eNodeB key only after two inter-eNodeB handovers. Handover key chaining includes two additional parameters as fresh keying material; these two are the Next Hop (NH) key and the NH Chaining Counter (NCC). An MME recursively generates a new NH key derived from KASME for each handover. NCC is a counter value for the NH key.

Authentication Key Agreement (AKA)

AKA in 3GPP mobile networks have been increasing the possibility of rogue base station (i.e., false base station) attacks in the Global System for Mobile Communications (GSM); these attacks took the form of call stealing on unencrypted networks and call spoofing pointed out that the UMTS security displays vulnerabilities to a variant of rogue base station attacks. To the best of our knowledge, no serious rogue base station attacks on the EPS architecture have been reported in the public literature. Only the 3GPP standard has discussed theoretical rogue base station attacks. A few researchers initially surveyed EPS security. The authors in and provided a tutorial overview of EPS security, including the EPS-AKA and key management into handover key chaining and explored the operation of vertical and horizontal key derivation. The potential for DoS attacks on a specific UE by using radio signals.

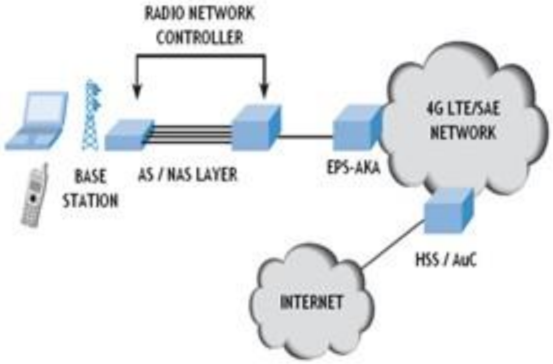


Figure 5. Key Management of 4G Network

Recently, Koien pointed out that the delegation from the authentication server requires strong trust assumptions, which seems outdated in the LTE heterogeneous networks. He presented a mutual authentication directly between the user and the authentication server in online.

Long-Term Evolution Security

Long-Term Evolution (LTE) is an emerging radio access network technology standardized in 3GPP and it is evolving as an evolution of Universal Mobile Telecommunications System (UMTS). It aims to provide seamless Internet Protocol (IP) connectivity between user equipments (UE) and the packet data network (PDN) without any disruption to the end users' applications during mobility.

The system is named evolved packet system (EPS) with two parts:

- System architecture evolution (SAE)
- Evolved packet core (EPC) network

ALGORITHM

SHA-256 CRYPTOGRAPHIC HASH ALGORITHM

We used the EURANE module and a LTE queue development package in the ns-2 simulator to implement the EPS security framework—which includes EPS-AKA, the inter-eNodeB handover described in the KDF operation, we manually added the processing delay that is part of the EPS-AKA by using Hash-based Message Authentication Code (HMAC) with the Secure Hash Algorithm (SHA)-256 as measured by a PolarSSL on an Intel Pentium IV 3.0 GHz with 1 GB of random-access memory.

The average operation speed and standard deviation for HMAC-SHA-256 are 16.635 and 0.081 microseconds, respectively. A source eNodeB and the MME require one HMAC-SHA-256 operation each to calculate a new KeNB and an NH value, respectively. The UE needs to synchronize NCC values by performing HMAC-SHA-256 operations equal to the number of horizontal handovers and computes the current NH value once. The length of all key materials is defined as 128 bits except that KeNB and NH are 256 bits.

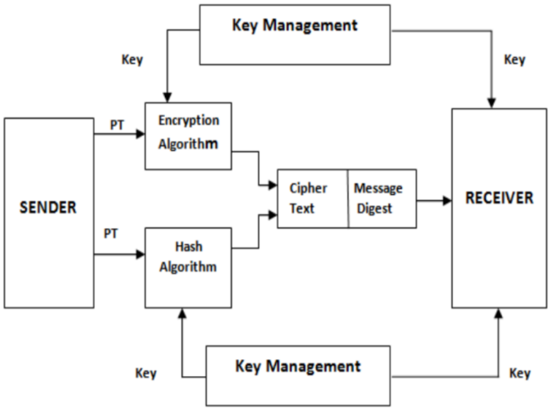
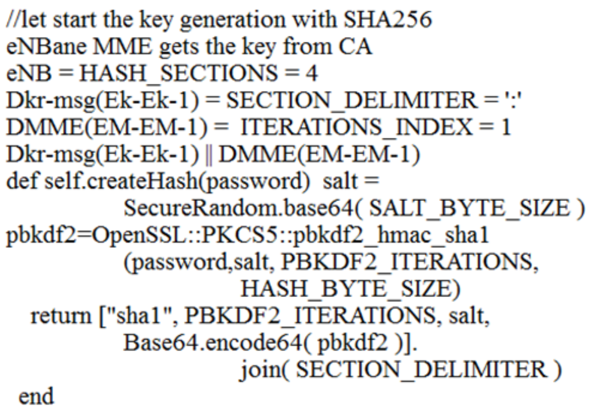


Figure 5. Encryption key Management

SHA-256 is one of the successor hash functions to SHA-1 (collectively referred to as SHA-2), and is one of the strongest hash functions available. While SHA-1 has not been compromised in real-world conditions, SHA-256 is not much more complex to code, and has not yet been compromised in any way.

The 256-bit key makes it a good partner-function for AES. It is defined in the NIST (National Institute of Standards and Technology) standard 'FIPS 180-2'. NIST also provide a number of test vectors to verify correctness of implementation.

This script is oriented toward hashing text messages rather than binary data. The standard considers hashing byte-stream (or bit-stream) messages only.



```
//let start the key generation with SHA256
eNBane MME gets the key from CA
eNB = HASH_SECTIONS = 4
Dkr-msg(Ek-Ek-1) = SECTION_DELIMITER = ':'
DMME(EM-EM-1) =  ITERATIONS_INDEX = 1
Dkr-msg(Ek-Ek-1) || DMME(EM-EM-1)
def self.createHash(password)  salt =
          SecureRandom.base64( SALT_BYTE_SIZE )
pbkdf2=OpenSSL::PKCS5::pbkdf2_hmac_sha1
          (password,salt, PBKDF2_ITERATIONS,
                    HASH_BYTE_SIZE)
  return ["sha1", PBKDF2_ITERATIONS, salt,
          Base64.encode64( pbkdf2 )].
                    join( SECTION_DELIMITER )
 end
```

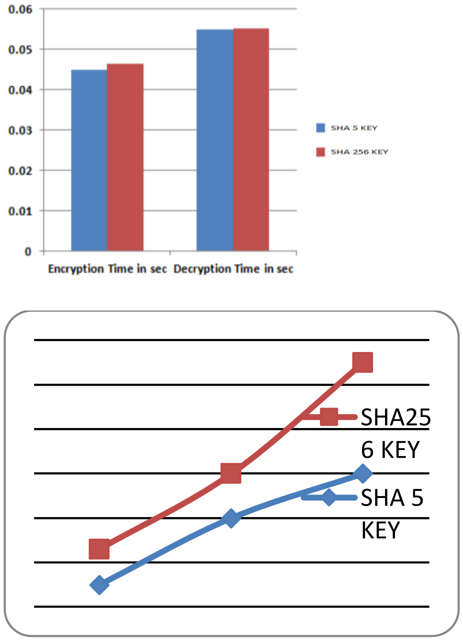


Figure 6. Comparison of key generation

There are 5 security levels

1. **Network access security**

Provide the UEs with secure access to the EPC and protect against various attacks on the radio link.

2. **Network domain security**

Protects against attacks on the wire line network and enable nodes to exchange signaling data and user data in a secure manner

3. **User domain security**

Provide a mutual authentication between the USIM and ME before the USIM access to the ME.

4. **Application domain security**

Security features that enable applications in the UE and the provider domain to securely exchange messages.

5. **Non 3GPP domain security**

The set of features that enables the UEs to securely access to the EPC via non-3GPP access networks and provides security protection on the radio access link.

Text which contains (multi-byte) characters outside ISO 8859-1

CONCLUSION

The proposed idea will protect the 4G network during the initial call setup phase, periodic time based key exchange to ensure the call security and the seed exchange for the other end integrity check. The attacker can launch a variety of active and passive attacks. Thus the key management solution best fits the 4G SAE / LTE architecture. At the same time this system is maintaining a multilayered and multidimensional security approach. The two aspects are the selection of a straight forward ciphering key hierarchy distribution mechanism and providing a layered network security architecture, novel solutions for tackling LTE/SAE security issues on 4G wireless networks. Light weight key management system is the best solution than other alternatives because it offers a fast and secure transmission by adding a minimum design overhead. The key sharing based on the architecture time is used to protect the voice calls 4G. Therefore, there is a significant need for secure key management between the two nodes. Key sharing rules will be shared between the call ends (both nodes to make a call) during the initial handshake. The original key will be obtained and matched for integrity. If the key matches, the data would be exchanged between the two nodes, if the call is terminated flashing message integrity violation on the end of the spammer. In the future, the comparative analysis can be performed with higher level of performance analysis using the higher number of parameters. Also, the techniques under the survey can be improved or mixed in order to improve the overall performance of the scheme.

REFERENCES

[1] Jin Cao, maode ma, IEEE Hui li, Yueyu Zhang and Zhenxing luo: “A survey on security aspects for LTE and LTE-A networks”, IEEE Communications Surveys & Tutorials., VOL.16, May 2014.

[2] chan-kya Han and hyoung-kee choi, “Security Analysis Of Handover Key Management In 4G LTE/SAE Networks”, IEEE Transactions on Mobile Computing ,VOL.13 , NO.2, FEB 2014.

[3] Mohsen M.Tantaway, Adly S.Tag Eldein and Esraa Mosleh Eid:” Performance Analysis of Multicast Security in LTE”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), VOL.2, ISSUE 5, Sept-Oct 2013.

[4] Anand R.Prasad and Xiaowei Zhang: “Overview Of LTE/SAE Security”, IEEE Transactions On Smart Processing And Computing.,vol.2,no.1,February 2013.

[5] Y. Zheng, D. He, L. Xu, and X. Tang: “Security Scheme for 4G Wireless Systems” Proc. Communications, Circuits and Systems, pp. 397- 401, May 2005.

[6] “Cryptography and Network Security” 'William Stallings, Pearson Education, 2007.

[7] International Journal of Electrical, Computing Engineering and Communication (IJECC) Vol. 1, Issue. 2, April – 2015, Security analysis of Handover Key Management among 4G LTE entities Using Device Certification.

[8] International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868, Security Enhancement Algorithms for Data Transmission in 4G Networks.

[9] International Journal of Computer Applications (0975 – 8887) Volume 118 – No.23, May 2015, Performance Evaluation of Secure Asymmetric Key Exchange Mechanisms for 4G Networks.

[10] H. Mun, K.Han, and K. Kim, “3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement Based on EAP-AKA,”Wireless Telecommunications Symp. (WTS 2009), IEEE, 2009; doi:10.1109/WTS.2009.5068983.

[11] N. Sklavos and X. Zhang, eds., Wireless Security & Cryptography: Specifications and Implementations, CRC Press,2007.

[12] L. Hui and B. Shuo, “Research and Implementation of LTE NAS Security,” Proc. Int’l Conf. Educational and Information Technology (ICEIT 10), IEEE, 2010; doi:10.1109/ ICEIT.2010.5607551.

[13] IEEE SECURITY AND PRIVACY MAGAZINE,MARCH 2013, LTE/SAE Security Issues on 4G WirelessNetworks.

[14] J. Cao, M. Ma and H. Li, “A survey on security aspects for LTE and LTE-A networks”, Communications Surveys & Tutorials, vol. 16, no. 1, (2013).

[15] D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom and S. Parkvall, “LTE: The Evolution of Mobile Broadband”, IEEE Commun. Mag., vol. 47, no. 4, (2009).

[16] Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe and T. Thomas, “LTE-advanced: Next-generation Wireless Broadband Technology”, IEEE Wireless Commun., vol. 17, no. 3, (2010).