International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
July 2017

# Implementation Cryptographic Algorithm in 4g LTE/SAE Networks

**Ahmed Fadhil Qutaif**
Department Of M. S.C.IS
Osmania university, Hyderabad, India
Foundation of Technical Education, Iraq
Email:- ahmed.fadhel1979@gmail.com
**Mr. T. Ramdas Naik**
Assistant Professor (B.E, MCA, M.Tech, Ph.D)
Department Of IT Nizam College
Hyderabad, Telangana, India
Email: ramdas_teja@gmail.com

## ABSTRACT

Frequently in wireless communications the cryptographic algorithm is considered as 'the security arrangement' all things considered it is just the core. The methods for utilizing the cryptographic algorithm is the "key" utilized by the calculation. In this manner administration of keys and security there-of is an imperative issue. The security of the key administration arrangement ought not hinder versatility of gadgets by including undue postponements. Subsequently, secure and quick key administration amid portability is a vital issue for the third generation partnership project (3GPP) activity on system architecture evolution / long-term evolution (SAE/LTE). In this paper we audit portability and security issues with the concentration of key administration in SAE/LTE and show conceivable existing arrangements together with their investigation.

## INTRODUCTION

Over the past fewyears, the colossal ubiquity of the Internet has created a critical boost to P2P document sharing frameworks. For instance, BitTorrent constitutes approximately 35 percent of all activity on the Internet. There are two classes of P2P frameworks: unstructured and organized. Unstructured P2P systems, for example, Gnutella and Freenet don't allocate duty regarding information to particular hubs. Hubs join and leave the system as indicated by some free guidelines. At present, unstructured P2P systems' record inquiry technique depends on either flooding where the question is engendered to all the hub's neighbors, or irregular walkers where the inquiry is sent to haphazardly picked neighbors until the document is found. In any case, flooding and arbitrary walkers can't ensure information area. Organized P2P systems , i.e., Distributed Hash Tables (DHTs), can beat the downsides with their components of higher productivity, adaptability, and deterministic information area.

They have strictly controlled topologies, and their data placement and lookup algorithms are precisely defined based on a DHT data structure and consistent hashing function. The node responsible for a key can always be found even if the system is in a continuous state of change. Most of the DHTs require *O(log n)* hops per lookup request with *O(log n)* neighbors per node, where n is the number of nodes in the system. A key criterion to judge a P2P file sharing system is its file location efficiency. To improve this efficiency, numerous methods have been proposed. One method uses a super peer topology, which consists of super nodes with fast connections and regular nodes with slower connections. A super node connects with other super nodes and some regular nodes, and a regular node connects with a super node. In this super-peer topology, the nodes at the center of the network are faster and therefore produce a more reliable and stable backbone. This allows more messages to be routed than a slower backbone and, therefore, allows greater scalability. Super-peer networks occupy the middle-ground between centralized and entirely symmetric P2P networks, and have the potential to combine the benefits of both centralized and distributed searches. Another class of methods to improve file location efficiency is through a proximity-aware structure.

A logical proximity abstraction derived from a P2P system does not necessarily match the physical proximity information in reality. The shortest path according to the routing protocol (i.e., the least hop count routing) is not necessarily the shortest physical path. This mismatch becomes a big obstacle for the deployment and performance optimization of P2P file sharing systems. A P2P system should utilize proximity information to reduce file query overhead and improve its efficiency. In other words, allocating or replicating a file to a node that is physically closer to a requester can significantly help the requester to retrieve the file efficiently. Proximity-aware clustering can be used to group physically close peers to effectively improve efficiency.

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.

This separation keeps a session key compromised in one base station from 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 herein referred to as a desynchronization attack. A desynchronization attack prevents a target eNodeB from maintaining the freshness of the handover key.

**The main contributions of this paper are threefold:**

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.

## LTE/SAE:

Along with 3G LTE - Long Term Evolution that applies more to the radio access technology of the cellular telecommunications system, there is also an evolution of the core network. Known as SAE - System Architecture Evolution. This new architecture has been developed to provide a considerably higher level of performance that is in line with the requirements of LTE.

As a result it is anticipated that operators will commence introducing hardware conforming to the new System Architecture Evolution standards so that the anticipated data levels can be handled when 3G LTE is introduced. The new SAE, System Architecture Evolution has also been developed so that it is fully compatible with LTE Advanced, the new 4G technology. Therefore when LTE Advanced is introduced, the network will be able to handle the further data increases with little change.

## Reason for SAE System Architecture Evolution

The SAE System Architecture Evolution offers many advantages over previous topologies and systems used for cellular core networks. As a result it is anticipated that it will be wide adopted by the cellular operators.

SAE System Architecture Evolution will offer a number of key advantages:

1. ***Improved data capacity:*** With 3G LTE offering data download rates of 100 Mbps, and the focus of the system being on mobile broadband, it will be necessary for the network to be able to handle much greater levels of data. To achieve this it is necessary to adopt a system architecture that lends itself to much grater levels of data transfer.
2. ***All IP architecture:*** When 3G was first developed, voice was still carried as circuit switched data. Since then there has been a relentless move to IP data. Accordingly the new SAE, System Architecture Evolution schemes have adopted an all IP network configuration.
3. ***Reduced latency:*** With increased levels of interaction being required and much faster responses, the new SAE concepts have been evolved to ensure that the levels of latency have been reduced to around 10 ms. This will ensure that applications using 3G LTE will be sufficiently responsive.
4. ***Reduced OPEX and CAPEX:*** A key element for any operator is to reduce costs. It is therefore essential that any new design reduces both the capital expenditure (CAPEX)and the operational expenditure (OPEX). The new flat architecture used for SAE System Architecture Evolution means that only two node types are used. In addition to this a high level of automatic configuration is introduced and this reduces the set-up and commissioning time.

## SAE System Architecture Evolution basics

The new SAE network is based upon the GSM / WCDMA core networks to enable simplified operations and easy deployment. Despite this, the SAE network brings in some major changes, and allows far more efficient and effect transfer of data.

There are several common principles used in the development of the LTE SAE network:

-  A common gateway node and anchor point for all technologies.
-  An optimised architecture for the user plane with only two node types.
-  An all IP based system with IP based protocols used on all interfaces.
-  A split in the control / user plane between the MME, mobility management entity and the gateway.
-  A radio access network / core network functional split similar to that used on WCDMA / HSPA.
-  Integration of non-3GPP access technologies (e.g. cdma2000, WiMAX, etc) using client as well as network based mobile-IP.

The main element of the LTE SAE network is what is termed the Evolved Packet Core or EPC. This connects to the eNodeBs as shown in the diagram below.

## LTE SAE Evolved Packet Core

As seen within the diagram, the LTE SAE Evolved Packet Core, EPC consists of four main elements as listed below:

**Mobility Management Entity, MME:** The MME is the main control node for the LTE SAE access network, handling a number of features:

- Idle mode UE tracking
- Bearer activation / de-activation
- Choice of SGW for a UE
- Intra-LTE handover involving core network node location
- Interacting with HSS to authenticate user on attachment and implements roaming restrictions
- It acts as a termination for the Non-Access Stratum (NAS)
- Provides temporary identities for UEs
- The SAE MME acts the termination point for ciphering protection for NAS signaling. As part of this it also handles the security key management. Accordingly the MME is the point at which lawful interception of signalling may be made.
- Paging procedure
- The S3 interface terminates in the MME thereby providing the control plane function for mobility between LTE and 2G/3G access networks.
- The SAE MME also terminates the S6a interface for the home HSS for roaming UEs.

It can therefore be seen that the SAE MME provides a considerable level of overall control functionality.

***Serving Gateway, SGW:*** The Serving Gateway, SGW, is a data plane element within the LTE SAE. Its main purpose is to manage the user plane mobility and it also acts as the main border between the Radio Access Network, RAN and the core network. The SGW also maintains the data paths between the eNodeBs and the PDN Gateways. In this way the SGW forms a interface for the data packet network at the E-UTRAN.

Also when UEs move across areas served by different eNodeBs, the SGW serves as a mobility anchor ensuring that the data path is maintained.

- **PDN Gateway, PGW:** The LTE SAE PDN gateway provides connectivity for the UE to external packet data networks, fulfilling the function of entry and exit point for UE data. The UE may have connectivity with more than one PGW for accessing multiple PDNs.
- **Policy and Charging Rules Function, PCRF:** This is the generic name for the entity within the LTE SAE EPC which detects the service flow, enforces charging policy. For applications that require dynamic policy or charging control, a network element entitled the Applications Function, AF is used.

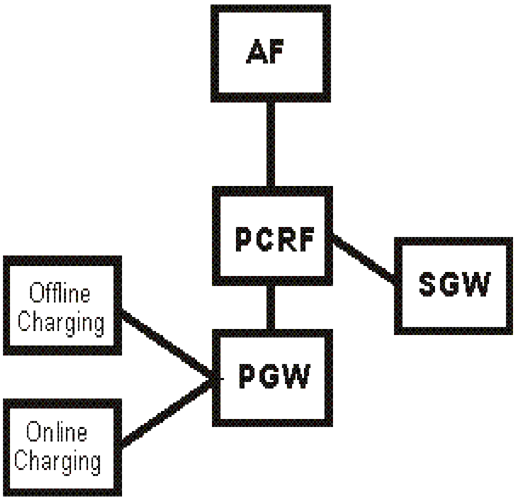


Figure 1.1: LTE SAE PCRF Interfaces

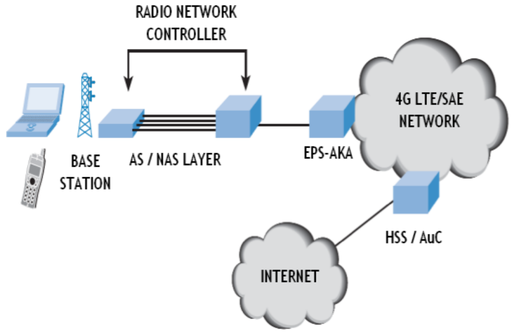
## 1.1. LTE SAE Distributed intelligence

In order that requirements for increased data capacity and reduced latency can be met, along with the move to an all-IP network, it is necessary to adopt a new approach to the network structure. For 3G UMTS / WCDMA the UTRAN (UMTS Terrestrial Radio Access Network, comprising the Node B's or basestations and Radio Network Controllers) employed low levels of autonomy. The Node Bs were connected in a star formation to the Radio Network Controllers (RNCs) which carried out the majority of the management of the radio resource. In turn the RNCs connected to the core network and connect in turn to the Core Network.

To provide the required functionality within LTE SAE, the basic system architecture sees the removal of a layer of management. The RNC is removed and the radio resource management is devolved to the base-stations. The new style base-stations are called eNodeBs or eNBs. The eNBs are connected directly to the core network gateway via a newly defined "S1 interface". In addition to this the new eNBs also connect to adjacent eNBs in a mesh via an "X2 interface". This provides a much greater level of direct interconnectivity. It also enables many calls to be routed very directly as a large number of calls and connections are to other mobiles in the same or adjacent cells. The new structure allows many calls to be routed far more directly and with only minimum interaction with the core network. In addition to the new Layer 1 and Layer 2 functionality, eNBs handle several other functions. This includes the radio resource control including admission control, load balancing and radio mobility control including handover decisions for the mobile or user equipment (UE). The additional levels of flexibility and functionality given to the new eNBs mean that they are more complex than the UMTS and previous generations of base-station. However the new 3G LTE SAE network structure enables far higher levels of performance. In addition to this their flexibility enables them to be updated to handle new upgrades to the system including the transition from 3G LTE to 4G LTE Advanced.

The new System Architecture Evolution, SAE for LTE provides a new approach for the core network, enabling far higher levels of data to be transported to enable it to support the much higher data rates that will be possible with LTE. In addition to this, other features that enable the CAPEX and OPEX to be reduced when compared to existing systems, thereby enabling higher levels of efficiency to be achieved.

## SYSTEM ARCHITECTURE:



## EXISTING SYSTEM:

Existing analyzes the authentication and key agreement protocol adopted by Universal Mobile Telecommunication System (UMTS), an emerging standard for third-generation (3G) wireless communications. 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. Moreover, we demonstrate that the use of synchronization between a mobile station and its home network incurs considerable difficulty for the normal operation of 3GPP AKA.

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.

## PROPOSED SYSTEM:

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.

The main contributions of this paper are threefold:

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.

## CONCLUSION

In this paper, we were concerned that forward key separation in handover key management in the 3GPP LTE/SAE network can be threatened because of what are known as rogue base station attacks. Although periodically updating the root key minimizes the effect of the attacks, selecting an optimal key update interval is an ill-defined problem because of the difficulty of achieving a balance between the signaling load and the volume of exposed packets. We have derived a mathematical framework for selecting an optimal handover key update interval that helps a network operator select an optimal value that fits best with network management policies.

## REFERENCE:

1. “3GPP System Architecture Evolution (SAE); Security Architecture (Release 11),” 3GPP TS 33.401, Version 11.2.0, Dec. 2011.
2. “3G Security, Security Architecture (Release 8),” 3GPP TS 33.102, Version 11.1.0, Dec. 2011.
3. M. Zhang et al., “Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol,” IEEE Trans. Wireless Comm., vol. 4, no. 2, pp. 734-742, Mar. 2005.
4. C.B. Sankaran, “Network Access Security in Next-Generation 3GPP Systems: A Tutorial,” IEEE Comm. Magazine, vol. 47, no. 2, pp. 84-91, Feb. 2009.
5. V. Niemi et al., “3GPP Security Hot Topics: LTE/SAE and Home (e)NB,” Proc. ETSI Security Workshop, Jan. 2009.
6. Y. Park et al., “A Survey of Security Threats on 4G Networks,” Proc. IEEE GlobeCom Workshop Security and Privacy in 4G Networks, Nov. 2007.
7. Bilogrevic et al., “Security and Privacy in Next Generation Mobile Networks:

LTE and Femtocells," Proc. Int'l Femtocell Workshop, June 2010.
8. S.-Y. R. Li and R. W. Yeung, "Linear network coding," IEEE Transactions on Information Theory, vol. 49, pp. 371–381, 2003.
9. T. Noguchi, T. Matsuda, and M. Yamamoto, "Performance evaluation of new multicast architecture with network coding," IEICE Trans. Commun, vol. E86-B, pp. 1788–1795, 2003.
10. Y. Zhu, B. Li, and J. Guo, "Multicast with network coding in application-layer overlay networks," IEEE Journal on Selected Areas in Communications, vol. 22, pp. 107–120, 2004.
11. Li Q, Aslam J, Rus D, "Online Power-aware Routing in Wireless Ad-hoc Networks," Proceedings of Int'l Conf. on Mobile Computing and Networking (MobiCom'2001), 2001.
12. Stojmenovic I, Lin X. "Power-Aware Localized Routing in Wireless Net108 works," IEEE Trans. Parallel and Distributed Systems 2001; 12(11):1122-1133.
13. Doshi S, Brown TX, "Minimum Energy Routing Schemes for a Wireless Ad Hoc Network," Proceedings of the Conference on Computer Communications (IEEE Infocom 2002), 2002.
14. Woo K, Yu C et al., "Localized Routing Algorithm for Balanced Energy Consumption in Mobile Ad Hoc Networks," Proc. of Int'l Symp. on Modeling, Analysis and Simulation of Computer and Telecommunication Systems 2001,117-124.
15. Toh C-K,"Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad hoc Networks," IEEE Communications Magazine, vol. 39, no. 6, pp. 138-147, June 2001.
16. M. Adamou and S.Sarkar, "A Framework for Optimal Battery Management for Wireless Nodes," Proceedings of IEEE INFOCOMP 2002, pp. 1783-1792.