AUTHENTICATION AND KEY AGREEMENT IN 3GPP NETWORKS

Krishna Prakash and Balachandra

Department of Information and Communication Technology
Manipal Institute of Technology, Manipal University, Manipal, India
kkp_prakash@yahoo.com
bala_muniyal@yahoo.com

ABSTRACT

The huge demand for mobile communications with broad band and usage of new wireless applications motivated the development of new wireless access technologies. The recent expansion of wireless technologies, novel applications and the advancement in mobile technology after UMTS-3G has been taken up to the next level by the 3GPP Long Tem Evolution/System Architecture Evolution (LTE/SAE). It has achieved the realisation of better bandwidth, full interworking with other access/backend systems using all-IP architecture with well-defined interworking with circuit switched system. The system is defined to work across multiple access networks (3GPP and non 3GPP) may be trusted or non-trusted. The security mechanism in wireless area has evolved from original analog systems through GSM and UMTS. The GSM has focussed the security for radio path whereas UMTS has enhanced it in to network functionalities. The future networks based on IP mechanism demands more security features, since the threats related to IP are also possible.

KEYWORDS

3GPP, LTE, SAE, UMTS, AKA

1. INTRODUCTION

Mobile computing provides flexibility of computing environment over physical mobility. The user of a mobile computing environment will be able to access the data, information or other logical objects from any device in any network while on the move. To make the mobile computing environment ubiquitous, it is necessary that the communication bearer is spread over both wired and wireless media.

The emerging mobile industry expected to be characterised by increasingly personalised and location based services. The availability of user preferred information despite of location made mobile computing successful. The advancement of mobile technology has revolutionised the way people use mobile devices in their day to day activity.

David C. Wyld et al. (Eds) : ACITY, DPPR, VLSI, WiMNET, AIAA, CNDC - 2015
pp. 143–154, 2015. © CS & IT-CSCP 2015 DOI : 10.5121/csit.2015.51313

Mobile computing offers a various services for the user over physical mobility. The user of a mobile computing environment will be able to access to data, information or other logical objects from any device in any network while on the move. To make the mobile computing environment ubiquitous, it is necessary that the communication bearer is spread over both wired and wireless media.

2. THE LTE/SAE 4TH GENERATION (4G) NETWORK SECURITIES ARCHITECTURE

Fig1 and Fig 2 demonstrate the LTE Network architecture. It is comprised of the Evolved Packet Core (EPC) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN). The EPC is an all IP and fully packet switched backbone network in LTE system. The IP Multimedia System takes care of voice service. When a User Equipment (UE) connects to the EPC, the Mobility Management entity takes care of mutual user authentication. It is equivalent to the Universal Terrestrial Radio Access Networks(UTRAN) Serving General Packet Radio Support Node (SGSN) enables the transfer of subscription and authentication data for the authentication and authorization of user access [1][2]. The Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) consists of a node called eNode-B which has the functionality of node B and Radio Network controller of UTRAN and communicates with user equipment.

Following are some new functionality introduced by The LTE networks compared to the 3G wireless networks.

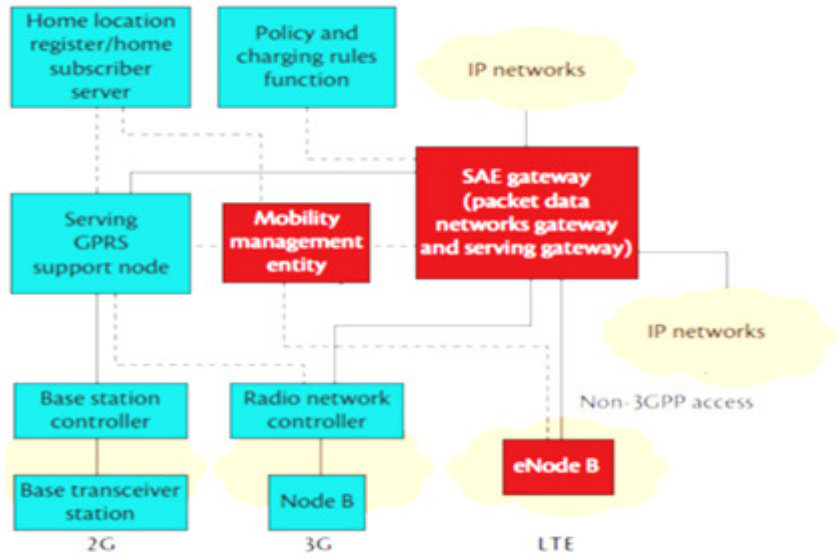

Fig 1: The SAE EPS architecture

1. A new type of base station called Home eNodeB (HeNB), and it is suggested by the 3GPP committee to improve the indoor coverage and capacity of the network. HeNB is a low power access point installed by the subscriber in the residence or small working areas to increase the coverage of voice and high speed data. It is connected to the EPC over internet via broad band backhaul [3].

2. In addition to the E-UTRAN, the LTE-A system supports non 3GPP access networks such as Wireless Local Area Networks(WLAN) and Code Division Multiple Access (CDMA) systems are allowed to connect to EPC. The two types of non 3GPP access networks namely trusted and non-trusted exists in use and for untrusted non 3GPP access networks the UE needs to pass a evolved packet data gateway(ePDG) connected to the EPC.

3. The LTE-A system supports a new type of data communication between entities called as Machine Type Communication (MTC) capable of data exchange without any human intervention. It is the communication between different devices (usually sensors) and the core network. The MTC user and the MTC Server are the two entities involve in the system and the MTC user uses the services provided by the one or more MTC servers for the operation of MTC devices. The MTC server is connected to the LTE network for the communication with Machine Type Communication Devices (MTCD)

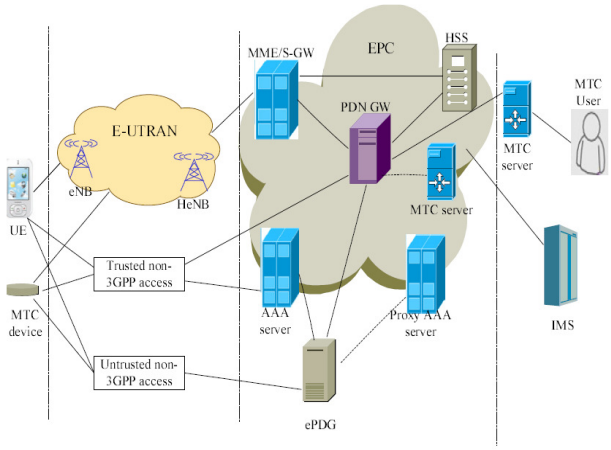

Fig 2: The LTE Network Architecture

3. LTE SECURITY ARCHITECTURE AND KEY HIERARCHY IN EPS

The basic security principles of smart phones and common PC are different. The device hosts multiple applications and allows the user to access internet irrespective of location. The complex software and infrastructure used in mobile device make the system more vulnerable and also the data exchanged between devices is a point of concern. The limited resources such as CPU and memory limit the sophistication of possible security solutions. A complex security algorithm that is used for real life applications cannot be directly ported and used in mobile devices.

3.1 LTE Security Architecture

The Fig 3 shows five different security levels defined by 3GPP committee for LTE architecture.

They are:

I .Network access security
II. Network domain security
III. User domain security
IV. Application domain security

V. Non 3GPP domain security

The following paragraphs briefly discuss the aforementioned functionalities.

I. Network Access Security

These security features facilitates the UEs for the secure access to EPC and protects possible attacks on radio link through integrity protection and ciphering between the USIM, ME, E-UTRAN and entities of EPC (both serving networks and home networks).

II. Network domain security

The set of security features protects possible attack on wire line networks and enables the data exchange in secure manner.

III. User domain security

The mutual authentication of USIM and ME is supported using a secret PIN before they can access each other.

IV. Application level security

These are the set of security features that enables the application in UE and the service provider domain for the secure exchange of messages.

V. Non 3GPP domain security

These are the set of features enables the UEs to securely access to the EPC via non 3GPP access networks and provide security protection on the access link.

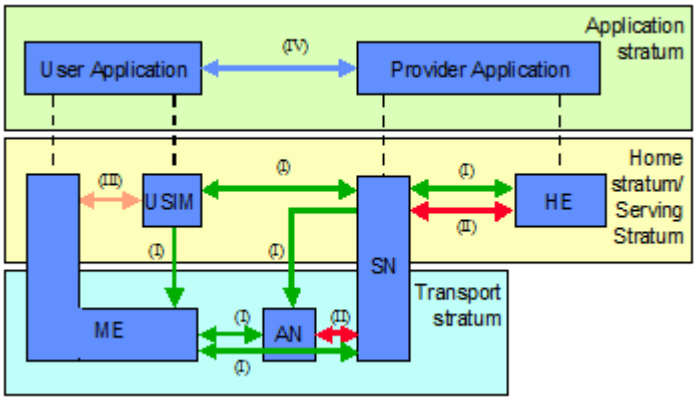

Fig 3: The LTE Security Architecture

3.2 Keys and Key Hierarchy

In the Evolved Packet Core Authentication and Key Agreement (EPS AKA) protocol, all the keys that are needed for various security mechanisms are derived from intermediate key K_{ASME} which is viewed as local master key for the subscriber in contrast to permanent master key K. In the

network side, the local master key K_{ASME} is stored in the MME and permanent master key is stored in the AuC [4]. This approach provides the following advantages.

1. It enables cryptographic key separation, where the usage of each key in one specific context and knowing one key does not deduce the second one.

2. The system is improved by providing key freshness and it is possible to renew the keys used in security mechanism. The EPS AKA is need not be run every time when the key to be renewed for protecting the radio interface and also the home network is not involved every time. This introduces a security versus complexity trade-off situation. For EPS, the security benefits of using an intermediate key overweigh the added complexity which was not true in 3G.

The base station eNB stores another key K_{eNB} and the addition of K_{eNB} makes it possible to renew keys for protection of radio access without involving MME.

3.3 Key Derivations

Figure 4 shows the hierarchy of keys used in EPS. The hierarchy contains one root key (K), several intermediate keys such as CK, IK etc. and a set of leaf keys [5]. The purpose of the different keys are explained below.

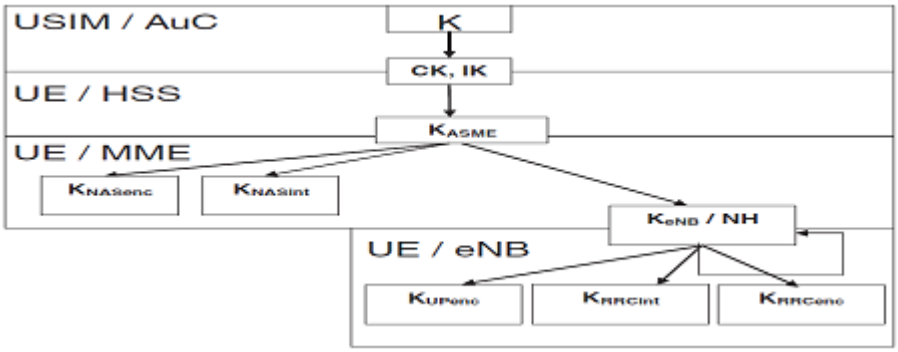

Fig 4: EPS Key Hierarchy

1. K is a random bit string and it is a subscriber specific master key stored in USIM and AuC.
2. CK and IK are 128 bit keys derived from K using additional input parameters.
3. K_{ASME} is derived from CK and IK using two additional parameters, the serving network id and bitwise sum of two additional parameters (SQN and AK from the EPS AKA procedure). The K_{ASME} serves as local master key.
4. K_{eNB} is derived from K_{ASME} and the additional input a counter. This additional parameter is needed to ensure that each new key K_{eNB} derived differs from the earlier key.
5. NH is another intermediate key derived from $K_{ASME,}$ and used in handover situations. It is derived from K_{eNB} for the initial NH derivation or previous NH as an additional input.
6. K_{RRCenc}, K_{RRCint} and K_{UPenc} are used for the encryption and integrity of RRC and Users.The complex key hierarchy achieves the key separation and prevents related key attack. The key hierarchy achieves key renewal very easily without affecting the other keys. When one key is changed, only the keys dependent on it have to be changed and others may remain same.

4. AUTHENTICATION AND KEY AGREEMENT PROTOCOL IN EPS (EPS AKA)

Authentication is a mechanism where the system verifies the identity of a user, who wishes to access it for availing some services. Mutual authentication is performed if both the communicating parties want to confirm each other. LTE/SAE architecture uses IP based mobility control technology and which has two components namely the access network and the core network. The access network is called evolved universal terrestrial radio access network (E-UTRAN) and the core network is called evolved packet core (EPC). Access security in E-UTRAN consists of following different components.

1. Mutual authentication between the network and UE.
2. Key derivation for ciphering and integrity protection.
3. Ciphering, integrity and replay protection of signalling between UE and MME, UE and enodeB.
4. Use of temporary identities in order to prevent the sending of permanent user identity over radio link.

4.1 User and Terminal Identification and Confidentiality

Similar kind of subscriber identity is used by 2G, 3G and EPS. It is composed of 3 parts (MCC, MNC, IMSI). Using IMSI the permanent authentication key K used in EPS AKA is identified. The IMEI is used to identify the terminals. The confidentiality of user identity against passive attacks is protected by assigning a temporary identity called TMSI in 2G and 3G. The EPS also adopts same mechanism to protect the actual UE id and it is called as Globally Unique Temporary UE Identity (GUTI). The GUTI has following components.

1. GUMMEI (Globally Unique MME Identifies) for the global unique identification of MME that allocated the GUTI.

2.M-TMSI uniquely identifies the UE within the MME that allocated the GUTI.

The GUMMEI is constructed from the MCC, MNC and MME identifier.

In GSM and 3G there is no user confidentiality protection from active attacks. In active attack, the attacker would use a device known as 'IMSI catcher', incorporates a false base station for sending an identity request message to UE [6]. The UE may respond with IMSI. The identity request is needed to recover from the cases where the network lost the association between temporary user identity and IMSI such as MME crash. Without such recovery the user could be permanently locked out from the system. 3GPP discussed the means by the use of public key certificates in UE. For roaming cases when the MME reside in another operators network may need the existence of public key infrastructure spanned across the operators with mutual agreement. In EPS, the UE not transmitting IMEI to the network upon network request before NAS security has been activated [7].

4.2 Authentication and Key Agreement (EPS AKA)

The EPS AKA mechanism is shown figure 5 and it is a combination of following three procedures.

1. A method to generate EPS Authentication vectors in the HSS up on request from the MME and distribute to MME.
2. A procedure to mutually authenticate and establish a new shared key between serving network and UE.
3. The mechanism to distribute authentication data inside and between serving networks.

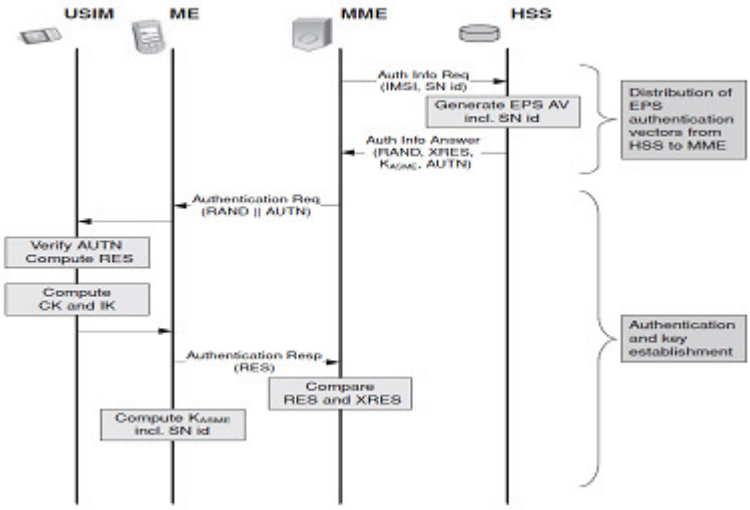

Fig 5: EPS AKA Protocol

4.3 Generation and distribution of Authentication Vector from HSS to MME

The MME invokes a procedure by requesting authentication vectors from the HSS. The authentication information request includes the IMSI, serving network id SN id of requesting MME with an indication of authentication information request from EPS. The SN id is required for the computation of K_{ASME} in HSS.

Up on the request of authentication vectors, the HSS may compute it or retrieve the pre computed values from the HSS database [8][9]. TS33.401 recommends the sending of one authentication vector at a time, because the need for frequently contacting HSS for fresh AV is reduced in EPS through the usage of local master key, K_{ASME} . Based on local master key and the keys derived from it an MME can offer secure services. The pre computed AVs are not usable when the user moves to a different serving network owing to the binding of local master key to the serving network id. Pre computation is useful when the next AV request is likely to be issued by an in the same serving network, when the user is in home network.

The Fig 6 demonstrates the authentication vector generation procedure. An EPS AV consists of a Random number RAND, an expected response XRES , local master key K_{ASME} and an authentication token AUTN. Both UMTS AV and EPS AV play a major role in EPS AKA. The HSS outside the AuC derives the K_{ASME} key from the cipher and integrity keys CK and IK. The AuC starts generating a fresh sequence number SQN and a random challenge RAND. For each user the HSS keeps track of counter $SQN_{HE.}$

An Authentication Management Field (AMF) is included in the authentication token of each authentication vector. The AuC computes following values after it receives a request from HSS.

1. Message Authentication Code (MAC) =f1(K||SQN||RAND||AMF), where f1 is a message authentication function.
2. Expected response, XRES = f2 (K||RAND), f2 is a truncated message authentication function.
3. A Cipher Key, CK = f3 (K||RAND), using a key generating function f3.
4. An Integrity Key, IK = f4 (K||RAND), f4 is a key generating function.
5. Anonymity Key, AK = f5 (K||RAND), f5 is a key generating function.
6. Authentication Token, AUTN = (SQN XOR AK) ||AMF||MAC.

If the operator decides no concealment of SQN, then f5=0 (AK=0).

After the receiving UMTS authentication vectors from AuC, using the Key Derivation Function, KDF and CK, IK, SNid, (SQN XOR AK) are used for producing K_{ASME}. The CK, IK are deleted from HSS and it is only used for the computation of EPS authentication vectors and not allowed to leave HSS.

The usage of AMF are

1. Indicating the algorithm and key used to generate a particular authentication vectors when multiple algorithms and permanent keys are used.
2. Change of parameter relating to SQN verification in the USIM.
3. Setting threshold values for key lifetimes.

The length of authentication parameters CK, IK, RAND and K all are 128 bit long and it is expandable up to 256 bits if needed in the future.

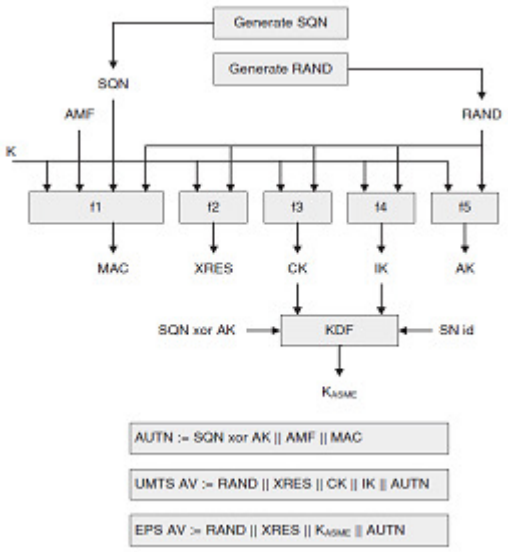

Fig 6: Generation of Authentication Vectors

4.4 Mutual Authentication and Establishment of a Shared Key between serving network and UE

After successful completion of the authentication of the user and generation of new local master key, K_{ASME} between MME and UE, the USIM performs verification of freshness of the authentication vector and authentication of its origin (User Home network). The K_{ASME} is used for the generation of further keys in subsequent procedures.

The MME invokes the procedure by using next unused EPS authentication vector in the MME database if more than one available. If the MME has no EPS AV, it requests one from the HSS. The MME sends a random challenge RAND and the authentication token for the network authentication AUTN from the selected EPS authentication vector to the mobile equipment which forwards it to the USIM. The USIM performs verification as follows.

The USIM first computes the anonymity key AK and retrieves the sequence number. The USIM next computes XMAC and verifies the MAC included in the AUTN as shown in Fig 7. The USIM verifies the retrieved sequences are in correct range or not for the satisfaction of following conditions.

1. Once the USIM has successfully verified an AUTN it shall not accept another AUTN with same sequence number to prevent the multiple usage of sequence number SQN.
2. It is required to allow out of order use of sequence numbers. Out of order usage of sequence numbers may occur when two different entities such as SGSN MSC/VLR request a batch of authentication vectors from HSS and use these in the interleaved fashion for AKA run with UE to reduce the synchronization failure rate.
3. The USIM may reject time based sequence numbers if it was generated too long ago.
4. The SQN verification mechanism may reject the SQN a jump from last successfully verified SQN is too big.

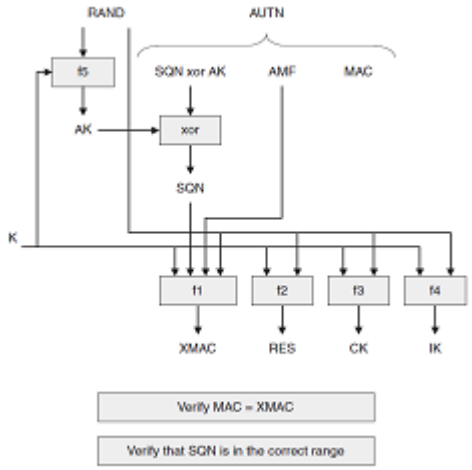

Fig 7: User Authentication Function in USIM

5. SECURITY THREATS AND VULNERABILITIES IN LTE

The EPS AKA scheme lacks a privacy protection under multiple instances of disclosure of IMSI[10]. When an UE registers to the network for first time/current MME cannot be contacted/ IMSI cannot be retrieved due to synchronization failure when it roams to new MME, the current MME or new MME requests the IMSI of UE as shown in messages 1 and 2 of Fig 8, then the UE must transmit IMSI in plaintext format and the disclosure of it may incur severe security problems [11][12]. Once the IMSI is captured, the adversary may attempt to tamper the information, subscriber or location information and then disguise the real UE and may launch attacks such as DOS to destroy the network.

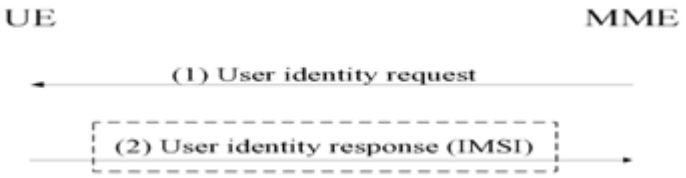

Fig 8: IMSI request process

The EPS AKA scheme cannot prevent DoS attacks. The MME forwards UEs request to the HSS/AuC before the UE has been authenticated by the MME as shown in message 3, and MME can only authenticate the UE after it receives RES from UE as shown in Fig 9. Using these two conditions the opponent can launch DoS attack between HSS and MME. The attacker can disguise a legitimate UE to constantly send fake IMSI to overwhelm HSS/AuC. Because of this, HSS consumes its computational power for the generation of authentication vectors for UE and MME consumes its memory buffer to wait overly long period of time for a legitimate or false response from the corresponding UE.

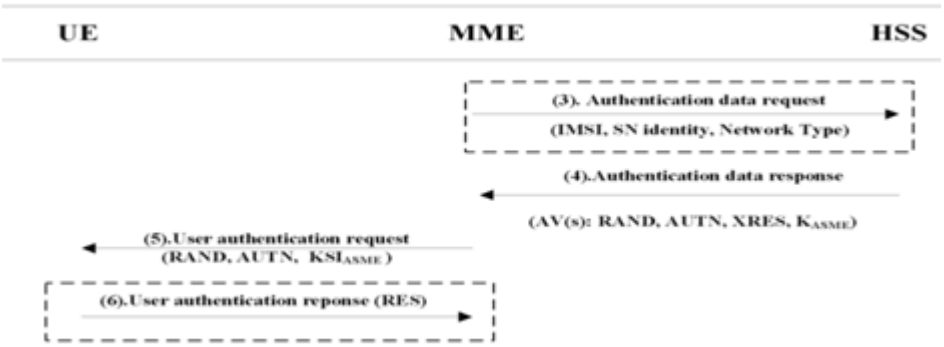

Fig 9: Authentication Data request and Mutual Authentication

In the EPS AKA as shown in Fig 9, the SN turns to HN for request of another set of authentication vectors when the UE stays in the SN for longer period of time and exhausts its set of authentication vector for authentication results in the bandwidth consumption and authentication signalling overhead between SN and HN, storage consumption in the SN.

The EPS AKA protocol is a delegated protocol, where almost all authentication authorities are delegated from home network to visited network requires strong trust relationship between

operators. The increased number of roaming entities and other access systems, in the heterogeneous networks the trust assumptions seems to be outdated [13].

5.1 Other Vulnerabilities in LTE/SAE

The vulnerabilities in LTE/SAE is classified under the following categories [14].

1. Threats against user identity and privacy
2. Threats of USIM/UE tracking
3. Threat related to handovers and base stations
4. Threats related to denial of service
5. Threats of unauthorised access to the network
6. Compromise of eNB credentials and physical attack on eNB
7. Attacks on core networks, including eNB location based attack

6. CONCLUSION

The last few years have witnessed a huge growth in wireless mobile industry. In the near future it can be expected that the mobile terminals are treated like internet terminals. The number of users using smart phones for various purposes has been increasing tremendously for m-commerce applications.

The mobile network security needs to be adopted from the entire mobile network point of view rather than a single device. From the history of mobile communication, attempts have been made to reduce a number of technologies to a single global standard. The first two generations has fulfilled basic mobile voice with capacity and coverage. Third generation opened the gate for the experience of high data transfer speed followed by fourth generation with added functionalities. The fifth generation is under research, aiming for high quality of service with more speed.

REFERENCES

[1] Gunter Schafer, “Security in Fixed and Wireless Networks-An Introduction to Securing Data Communication”, Second Edition, Wiley Publishers.
[2] Randall K Nichols et al., “Wireless Security-Models, Threats, and Solutions”, TaTa Mcgraw Hill Edition.
[3] 3rd Generation Partnership Project- Technical Specification Group Services and System aspects: Service requirements for Home Node (HNB) and Home eNode B(HeNB) (Rel 11), 3GPP TS 22.220 V11.6.0 Sep. 2012.
[4] Masoumeh Purkhiabani et al., “Enhanced Authentication and Key agreement Procedure of Next Generation Evolved Mobile Networks”, IEEE Journal, 2011.
[5] Jin Cao et al., “A Survey on Security Aspects of LTE and LTE-A networks”,IEEE Communications Survey and Tutorial, Vol. 16, No 1, Frist Quarter 2014.
[6] Sankaran C.B. “ Network Access Security in Next Generation 3GPP Systems”, IEEE Communications Magazine, February 2009.
[7] Ivan Stojmenvovic ,“ Handbook of Wireless Networks and Mobile Computing” , ISBN:0-471-41902-8.
[8] Hakima Chauchi ,“ Wireless and Mobile Network Security”, John Wiley Publications.
[9] Xinghua Li et.al., “A USIM based uniform access authentication framework in mobile Communications” Research Article,EURASIP Journal onWireless Communications and Networking, 2011.

[10] Li Xiehua "Security Enhanced Authentication and Key Agreement protocol for LTE/SAE Network" IEEE Journal, 2011.
[11] Zahra Ahmadian et al., "Security Enhancements against UMTS-GSM interworking attacks" ScienceDirect, 2010.
[12] Mariantonietta La Polla et al., " A Survey on Security for Mobile devices" IEEE Communications Surveys and Tutorials", 2013.
[13] Anastasios N. Bikos "LTE/SAE Security issues on 4G Wireless Networks", IEEE Computer and reliable societies, 2013.
[14] Inhyok cha et al., "Trust in M2M Communications-Addressing New Security Threats" IEEE Vehicular Technology Magazine, 2009.