Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.584 – 594

RESEARCH ARTICLE

ENHANCED ADAPTIVE SECURITY PROTOCOL IN LTE AKA

Uwaya Fidelis (M.Tech)
Jawaharlal Nehru Technological University JNTUH, Hyderabad, India
Electronics and Communication Engineering

Madhavi Kumari (Associate Professor)
Jawaharlal Nehru Technological University JNTUH, Hyderabad, India
Electronics and Communication Engineering

ABSTRACT: A Telecommunication systems trust and privacy is as good as its security mechanism. Its security design keep evolving over time as new treats and technology evolve. LTE/SAE is 3GPP's wireless Communication new DNA, a move away from a hybrid of packet switched and circuit switched network which 3G networks possess, though with room for backward compatibility. LTE/SAE's new architecture is a flat IP architecture; it therefore comes with all security issues inherent in IP network coupled with the design having non-3GPP heterogeneous technologies integrated into it. Its' security cryptography, rides on the good features of 3GPP AKA cryptographic algorithms, used in UMTS and added new ones. Some major security concerns in LTE/SAE from several researchers work points to, user privacy concerns, threats to UE/USIM tracking, base stations and handovers, broadcast or multicast signaling, denial of service (DOS), manipulation of control plane, unauthorized access to network, compromise of eNB credential and physical attack on an eNB protocol attack on eNB and attack on the core network and eNB location based attacks. In this paper, we will be analyzing, LTE/AKA architecture and its vulnerability, after which we will be proposing a protocol, referred to as Security Enhanced Adaptive Protocol (SEAP-AKA), which is to prove to eliminate the importance of synchronization between a cell station and its home system. SEAP-AKA specifies six flows sequence with respect to execution environment. Entities of the new protocol possess flexibility as it adaptively picks out flow for execution, which helps to optimize this efficiency both in the home network and Mobile network.

More so, SEAP-AKA will show a Security Enhanced Authentication along with Key Agreement dependent on Wireless Public Key National infrastructure (WPKI). Then, the brand new protocol shall be proved with the formal verification method, and the proof result shall demonstrates the new protocol and how it satisfies the security along with efficiency properties from the LTE/SAE buildings note that, existing 128 bit encryption existing in UMTS is same used here in LTE.

Keywords: LTE, Security, AKA, 3GPP, 4G

1.0 Introduction

3GPP's decision to create ubiquitous wireless broadband network –LTE-A also known as 4G has brought about some security concerns among operators and consumers considering its ubiquity and new DNA-LTE/SAE which happens to be an open network both as an IP protocol network carrying both voice and data and as an open network to Non – 3GPP network on a separate domain.

From 3GPP's design, LTE-A promises to deliver low latency, high speed data rate of 1Gbps on low mobility and 100MB on high mobility, good quality of service and good coverage with the use of smart Antennas (MIMO) on Multiple Radio Access technology (RAT) [16]. Much effort and resources has been invested in bandwidth optimization and efficiency gain techniques, flexible bandwidth allocation scheme and modulation approaches at the base station, which allows for differing service levels depending on the end user device. Femtocell- a small user home or business location base station is another added innovation to improve indoor coverage and capacity [13]. In spite of security concerns, LTE deployment has being gaining popularity since 2012 and many more countries are already working on deploying theirs. According to Ericsson's estimate, half the world's population will have LTE coverage by 2017 and many consumer devices—including medical monitors, cameras, and even vehicles—may adopt LTE technology for a new wave of applications [15].This is to confirm that the mobile industry is reacting swiftly to this new technology as more and more mobile phone producers are also producing LTE compatible phone.

With Security concerns top on the list for this new technology, an analysis of various wireless security loopholes and enhancement since inception of mobile technology will be pertinent. first generation (1G) security in mobile technology, which was with a low cost mobile User analogue equipment shows that intruders freely eavesdrop over traffic and can even change identity of mobile phones to gain fraudulent service as a result of its weak security systems[9]. In second generation (2G) cellular system, enhancement of security in design was carried out to guide against the flaws in 1G yet, a few million interaction with SIM card could disclose master security key [9]. GSM, which was 3rd generation technology, was designed with security in mind, it displayed several enhanced security features though several flaws were still noted. A two way process was designed, Authentication and key Management, security design was by challenge and response mechanism whereby the UE proves its identity by providing a response to a time-variant challenge raised by the network. When the UE roams into a foreign network, the home network (HSS) transfers a set of authentication data - triplets to the foreign network. Based on each triplet, the foreign network can authenticate the user without the involvement of the home network. This was noted as a major flaw in GSM AKA, considering authentication is only unidirectional. As a result, the UE is not able to authenticate the serving network. This unidirectional feature of GSM created a weakness whereby intruders created false base station in a network . Furthermore, keys are being reused indefinitely and there is no assurance provided to the user network that authentication information and cipher keys are not being reused. 3GPP AKA used in UMTS happens to be the forerunner of the 4th generation (4G) wireless technology, it happens to be an enhancement to 3GPP AKA, retaining the good security features of its cryptography AKA and adding new ones[11]. It provides freshness assurance of agreed cipher keys and integrity keys and a mutual authentication agreement on integrity keys between users and the serving network .In each authentication vector, a sequence number is always included, which is being verified by the user to achieve freshness assurance of agreed cipher and integrity keys meaning no reuse of keys like in GSM AKA. To facilitate sequence number generation and verification, two counters are maintained for each user: one in the mobile station and the other one in the home network. Normally, the counter in the mobile station has a value less than or equal to the counter in the home network. When a mismatch occurs between the two counters, which may be caused by a failure in the home network, the authentication vectors generated by the home network may not be acceptable by the mobile station. Such a phenomenon is called loss of synchronization and resynchronization is needed

to adjust the counter in the home network. Most designers' problem come from the task of 4G assessing the internet from a fixed location and mobility, coupled with the fact that cryptographic enhancement keeps evolving with new security threat and computation should not override performance [9]. [11] revealed that, 3GPP AKA security enhancement in GSM was with public review of encryption algorithm by the security community, 128 bit encryption key length increased from 64 bits formerly used in GSM, mutual authentication and mandatory integrity between wireless terminals and the network unlike the unidirectional in GSM, and lastly, encryption from terminal to a node beyond the base station

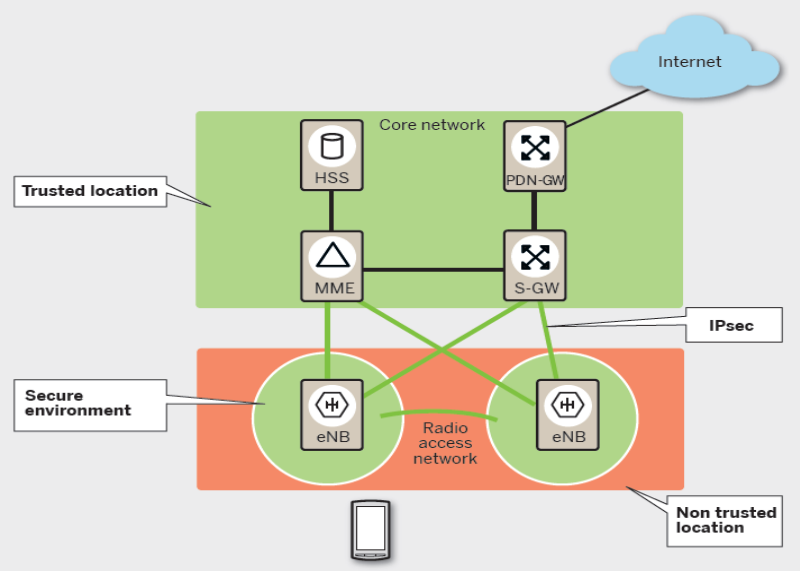
The rest of this paper is organized as follows: section II describes LTE and vulnerabilities, section III discusses previous works and research on LTE Security, section IV discusses our proposal and result, lastly conclusion and future works.

1.1 LTE -A

The LTE System architecture Evolution called, the Evolved Packet System (EPS), is designed as a flat all-IP system delivering high data rates of 1Gbps on low mobility and 100Mbps on very high mobility, with low latencies [10].It supports a meshed network, which allows greater efficiency and performance gain, as a single eNB to communicate with multiple AGWs[10].It's system architecture is a flatter architecture than that of UMTS-3GPP, having no node corresponding to radio network controller (RNC)like in UMTS. Fewer network elements (NE) make up LTE/SAE unlike previous technologies like 3G and UMTS, which host more elements. Elements in LTE are (1) E-UTRAN which single element is eNB, which is LTE enhanced base station,(2)Access gateway (AGW), which incorporates all the functions required for EPC(evolved packet core) which houses several modules – S-GW, P-GW, HSS, MME,[9]. Vendors can integrate this modules as one device or separately as 3GPP standard demands [9].Part of the LTE security architecture evolution is the EAP AKA Authentication and Key Agreement scheme (LTE-AKA) which defines the protocol through which the User Equipment (UE) and the Home Network (HN) are mutually authenticated and the mechanism through which the master encryption keys are generated. These keys form the basis upon which another set of keys are derived and that will be at the heart of confidentiality and integrity of communications between the Evolved Universal Terrestrial Radio Access Network (EUTRAN) Entities. LTE/SAE simplified core network and integrated non 3GPP access technologies called heterogeneous networks with EPC (evolved packet core), so UE security must be terminated in LTE base station- eNB or in a core network node. Sometimes eNB and backhaul links maybe deployed in locations vulnerable to attacks and for this reason additional security IKE (internet key exchange) and IPSec protocol is used by back haul link and eNB when cryptographic protection is required. A graphical design of LTE/SAE is shown in fig1.

Subscriber Authentication in EPS is based on UMTS authentication and key agreement protocol since it provides mutual authentication between UE and core network ensuring robust charging and guaranteeing that no fraudulent entities can pose as valid network node and its should be noted that since GSM AKA is unidirectional, not providing a mutual authentication, GSM SIMs are not allowed in LTE networks [10}. EPS AKA provides a root key from which hierarchy is derived. This key hierarchy is derived using cryptographic function. If 2 keys used in 2 eNB are keys derived from the keys by MME, any attacker who intercepts one key can't get 2nd key because it's in a higher layer in key hierarchy.

Fig 1 LTE SAE

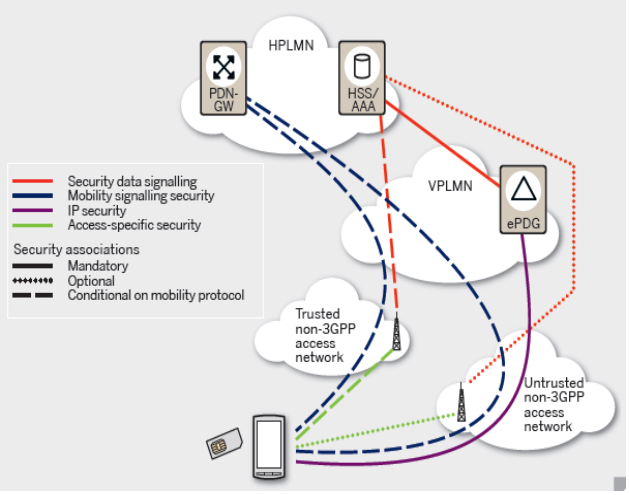


Source: [11]

Keys are never reused in LTE AKA.LTE provides integrity, replay protection and encryption between UE and eNB for radio specific signaling. Internet key exchange (IKE) and IPSec protects the backhaul between eNB and MME and it also provides end to end protection of signaling between MME and UE.IKE/IPsec also protect backhaul from eNB to Serving gateway (S-GW) via user plane traffic. Only encryption is efficient in user plane between UE and eNB as bandwidth overhead is expensive for integrity protection here. For the handover in LTE, between two eNBs, eNB needs transfer security parameter to the target eNB while simultaneously restoring forward and backward security should there be any security branch at any of the eNB. In either case of compromise, core network can provide the target eNB with a new key unknown in the source eNB. Same security context used during Handover between UE and LTE /other 3GPP technologies when initiated. May also be transferred when UE moves between legacy systems like GSM/GERAN, and UTRAN, since LTE includes caching of security contexts as it saves on the number of times a subscriber must be authenticated when a UE rapidly moves back and forth between LTE and UTRAN.

For the Non 3GPP systems, access to EPC is via the use of USIM[10] card and EAP AKA –based mutual authentication is always performed between a USIM and authentication 'authorization and accounting, (AAA) server. The AAA server fetches credential from home subscriber server (HSS). SEAP-AKA also creates cryptographic keys for data keys for data integrity and encryption between UE and network at access point, at IP layer or both. This is to help limit key reuse. Moreso a Non-3GPP can also be treated as trusted or non-trusted. If it can provide all necessary security by itself, it's said to be secured, While unsecured need IPsec tunneling. The figure 2 below shows an overview of non 3GPP access to EPC.
EAP AKA (UMTS) is used for trusted access to create an access level security association between UE and non -3GPP access network, though this is optional, since mobility is based on the dual stack mobile IPv6 protocol –DSMIPv6. DSMIPv6 always uses EAP AKA authentication between UE and MIP home agent, which fulfills the authentication needs. Subsequently, since the security procedures for trusted and untrusted accesses differ, the UE needs to know the "trust value" of the access. This can be made available via the authentication signaling. If no signaling is received, the UE inspects a configuration file on the USIM to determine the trust value. If the UE does not find the access network ID there either, it reverts to a default and assumes the access is untrusted.

fig 2 LTE SAE and Non 3GPP



source : [11]

LTE utilizes 5 different keys, each used for a specific purpose and valid only for certain duration. Different keys are used for communication in the E-UTRAN and the EPS. We believe this approach greatly reduces the effect of any possible security compromise. All the keys are derived using the Key Derivation Function (KDF) [9]. The 5 critical security keys derive their basis from the K key with a number of intermediate keys utilized as well. K is the permanent key stored on the USIM (Universal Subscriber Identity Module) on the UE. CK and IK are the pair of keys derived on the USIM during an AKA exchange. Subsequently, the KASME key is derived from the CK, IK and SN identity using a KDF [9]. The 5 keys are: (i) KNASint and KNASenc integrity and encryption keys respectively are used to protect NAS traffic between the UE and MME (ii) KUPenc key is used to encrypt user data traffic between the UE and eNodeB (iii) KRRCint and KRRCenc integrity and encryption keys respectively are used to protect RRC (Radio Resource Control) traffic between the UE and the eNodeB. [9]

2.0 Related Research

Several research works have been carried out on LTE security and its weaknesses and several propositions have been presented for enhanced security. Nicolas Sklavos et al observed several issues on 4G wireless network and classified them basically as being caused by radio interface characteristics and grouped this issues as threat against users identity and privacy, UE/USIM tracking, base station and handover, DOS, etc [10]. HOKEY WG proposed using faster key reuse and suggesting AKA management take place before handoff when latency is much less critical and when latency is critical both can occur together during handoff [10], but this attracted more computation which obviously isn't our aim for a secured and efficient system.

Hang and Li introduced X-AKA protocol to overcome low bandwidth but the software use involved so much computation which affected efficiency.[14].

Khodo Hamandi et al [12], presented W-AKA as an alternative to LTE AKA as it proved to provide more secured user privacy by taking advantage of the almost omnipresent Wi-FI hotspot in order to establish a secure connection with Home network. He also showed how an alternative to IMSI would be exchanged. His proposal shows that W-AKA is only resilient to passive attacks not active attacks. Hiten Choudhuret al [13,]have proposed a scheme that assures end to end user identity privacy to the users of LTE. In the proposed scheme the knowledge of the permanent identity of the user is restricted to the UE and the HE.

This same ID is not transmitted at any stage (radio or wired path) of the network; thereby relaxing trust requirements that otherwise is a must among the intermediary elements of the network.
J. F Beaumont et al [9], categorized LTE security issues into physical layer issues, Wimax layer security issues, MAC Layer security issues and Higher layer security issues and in this categories, major weaknesses are bandwidth stealing, DOS, Location tracking, service degradation, key management issues, etc. Xiehua et al [4], introduced SE-EPS AKA, which relies on public-key cryptography to encrypt all the transactions made between UE, MME, and HSS. In this manner, the IMSI is hidden and never sent in the clear, which results in a higher degree of privacy. The MME ID known as the serving network ID (SNID) and the Authentication vector (AV) are also encrypted, but this scheme was proven to be weak by [11].

It was also proved in [9], that the fixed 15 digit number IMSI privacy, though enhanced as its sent via a temporary ID over the air as plain text, its GUTI is still vulnerable which makes it user ID privacy vulnerable and attackers can use this weakness to track users location. fake base station, resynchronisation attacks, inter-networking due to heterogeneous Non-3GPP connections and bandwidth stealing also exist.

It is well known that in the public-key based authentication, the authenticator and the authenticate must exchange their digital certificate and validate other side's certificate before the further negotiation. Unfortunately, in current wireless PKI architectures more attention has been paid on how to manage and verify the user's digital certificate as well as identify user's access via public-key mechanism. On the contrary from the perspective of ME, few security mechanisms have been offered for the mobile user, which are used to validate the wireless network's certificate and support wireless roaming without sacrificing user convenience and security. It's given that the change on CA's certificate is rare, a trusted CAs list with corresponding public-key is pre-stored in the USIM card so that users can verify the received certificate from the wireless network. We name it after pre-store method in the following description for convenience. However, in the scenario of the future mobile communication system it is really hard to pre-store all the CA's public-key in user's USIM card in view of the randomness of user mobility and the diversity of trusted domains, What's more, this method can only verify the integrity but not the time-validity of the wireless threat since the security levels provided by different networks are not always the same. The proposed protocol SEAP-AKA specifies a sequence of six flows. Each flow defines a message type and format sent or received by an entity. How the flows are actually carried out and under what conditions entities accept or reject are dependent on the execution environment. In certain scenarios, only two or three flows are carried out in a protocol execution, while in some other scenarios, all the six flows are carried out in the protocol execution. Dependent on the execution environment, entities have the flexibility of adaptively selecting flows for execution. It is in this sense that we call SEAP-AKA, an adaptive protocol. This is different from a conventional two-party or three-party authentication and key agreement protocol in which entities usually execute all the flows specified by the protocol. It is shown that the adaptability helps to optimize the efficiency of SEAP-AKA both in the home network and in foreign network. To solve the aforementioned problems and provide further enhancement on 3GPP AKA, we present an authentication and key agreement protocol which can defeat the redirection attack and may drastically lower the impact of network corruption. The protocol, called SEAP-AKA, also eliminates the need of synchronization between the mobile station and the home network. In SEAP-AKA, the home network does not maintain dynamic states for each individual subscriber. The mobile station can verify whether an authentication vector was indeed requested by a serving network and was not used before by the serving network. The protocol SEAP-AKA specifies a sequence of six flows. Each flow defines a message type and format sent or received by an entity. How the flows are actually carried out and under what conditions entities accept or reject are dependent on the execution environment. In certain scenarios, only two or three flows are carried out in a protocol execution, while in some other scenarios, all the six flows are carried out in the protocol execution.

3.0 PROPOSED SYSTEM

A. SEAP- AKA Initialization

The initialization of SEAP- AKA is aiming at security flaws, this module proposes a Security-Enhanced Authentication and Key Agreement protocol (SE-APA AKA) based on WPKI, using existing 128 bit key encryption as in 3GPP AKA where CA: denotes the Certification Agency; K : denotes the long term key shared between UE and HSS; PK : denotes the public key of UE, MME and HSS; SK: denotes the cipher key of UE, MME and HSS; f 3, f 4, s10 : denotes the key generating functions; ASME K : denotes the intermediate key; ASME KSI : denotes, the key identification allocated by MME for ASME KSI ; sig m : denotes the signature to message m.

B. SEAP- AKA Protocol

In this module based on WPKI, prior to communication, UE, MME and HSS shall acquire the digital certificate via CA, and acquire the public key. The subscriber initiates access request: Firstly, UE uses the HSS public key H PK which is stored in smart card to encrypt IMSI and get A. Then UE sends {A, HSS ID } in access request to MME. After MME receives the access request from subscriber, it adopts the public key H PK to encrypt its own network identity SNID, and derive the encryption information B. Then A and B are regarded as authentication data request and delivered to HSS. After receiving the authentication data request from MME, HSS uses its own private key H SK to decrypt A and B to get IMSI and SNID . Then HSS checks the validation of IMSI and SNID from registration subscriber list and authorization service network list maintained in the database. If the MME and SN identities have been verified, HSS will generate the random number array RAND(1, ..., n) , and the group of authentication vector AV (1,...,n).

C. Authentication Request

In this module suppose that s is UE strand, PK is the cipher key set controlled by attacker, U H P PK, and IMSI is originated uniquely by s. The normal node m, m' ∈C, term(m) = {IMSI}PKH and m +m' is the transforming edge of IMSI. According to steps, m is a negative node. Suppose that m is the node of certain MME strand s', m=<s' ,1> , s' = { ' , ' , ' , HSS MME A ID B C' ,D' , RES'} , term(<s' ,1 >) = { }PKH IMSI . Compare the content of strands. Compare term(<s' ,1 >) with the related content in MME strand, it can get A ' = A , ' HSS HSS ID = ID , H S S= H S S'. According to 2nd part of authentication method ASME PK t = D = RAND SNID KSI S −TMSI is used as test component. Therefore m is a regular negative node, term(m) = t1 . Suppose that m is the node of certain initiator s" strand, m=<s",2 > , sign(<s",2 >) = − , term(<s" ,2 >) ={ RAND, SNID} ASME PKU KSI S −TMSI . Compare the contents of s and s", since IMSI is originates uniquely in initiator strand s. Finally it can get SNID = SNID' . It can be seen that, UE can authenticate the identity of MME.

D. Authentication Response

The normal node m ,m' ∈C, PKH term m = SNID , and m+m' is the transforming edge of SNID. According to result of step, the node m is a negative node, therefore m is the node of certain HSS strand, suppose that the initiator strand is s' , ' HSS [' , ' , , , , ,] HSS s = IMSI SNID A B C D ID , pm=<s',2> ,and AQ term(<s' ,2 >) = PKH IMSI. Compare the contents of strands. Through comparing the contents of term <s' ,2> with the related content in HSS strand, ' HSS HSS ID = ID , IMSI = IMSI ' , SNID = SNID' can be derived, and it can be seen that MME can authenticate the identity of HSS. Using the same method, the authentication of MME to UE is also can be validated. According to formal analysis of above mentioned, it is verified that SEAP-AKA protocol realizes the mutual authentication among UE, MME and HSS, protects the transmission of private and confidential information among entities, resolves various safety problems incurred by leakage of IMSI and SNID , and increases the safety strength of session cipher key.

4.0 RESULTS

The concept of this paper is implemented and different results are shown below, The proposed paper is implemented in Java technology on a Pentium-IV PC with minimum 20 GB hard-disk and 1GB RAM. The propose paper's concepts shows efficient results and has been efficiently tested on different Datasets.

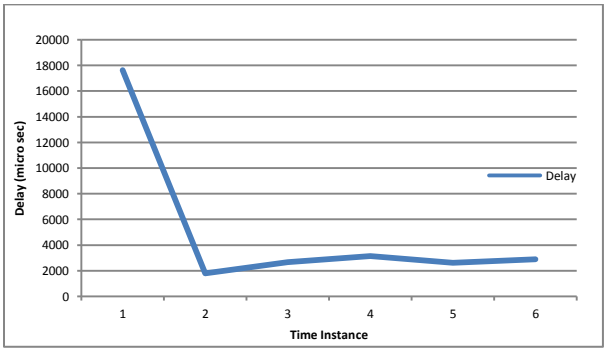


Figure 1: Delay Vs Time Instances

This graph shows delay in microseconds taken by mobile user at different instance of time, delay reduced very low once UE initiates a call and protocol is loaded in mobiles memory. The delay reduces more for other instances of time t1, t2,t3,t4.

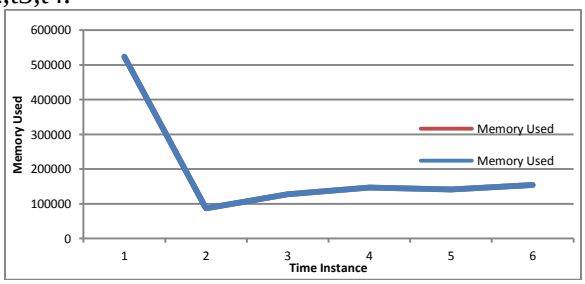


Figure 2: Memory used Vs Time Instance

Memory consumed at different instances of t. Memory consumed in loading protocol after the first drop while consumes large amount of memory but later times , t1,t2,t3, t4…. Memory utilization increases gradually due t communication transfer which needs to save in mobile for some period of time.

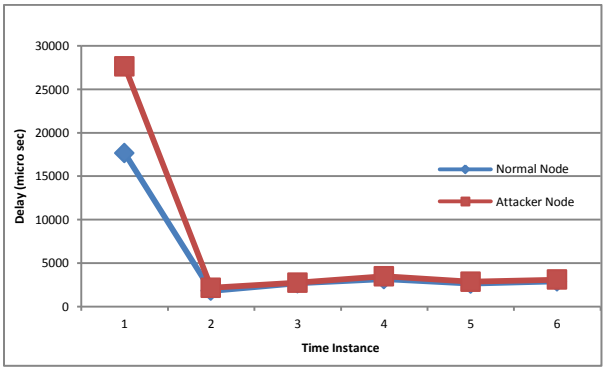


Figure 3: Delay Vs Time Instance (Attack Mode)

This graph shows what happens when an attack node is initiated plotted against when protocol is about to be initiated. So it high at initial point but when loaded its uniform. It observed that when protocol is loaded its delay is uniform meaning even with an attack node delay in communication is same. So proves that attack is null and void. No attack can happen with this protocol.
The graph in figure 4 shows what happens with memory usage when attack node is applied, at initial node its same as delay as protocol is yet to be loaded and when protocol is loaded and attack is initiated, with different time limits, memory usage is insignificantly different. Meaning that an attack will not affect memory usage, so no attack could happen within our enhanced security adaptive protocol.

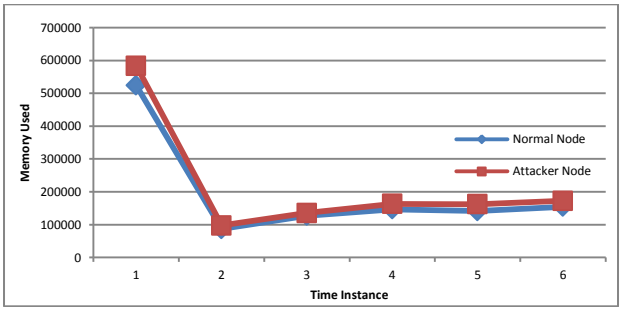


Figure 4: Memory Used Vs Time Instance (Attack Mode)

This paper investigates the security with the LTE AKA protocol and also examines the operational difficulty associated with the string number operations. The LTE AKA protocol is based on the structure of 3GPP AKA and expects to wipe out real and also perceived attacks, especially the so-called false base place attack. Within this paper, we demonstrated that LTE AKA is susceptible to a version of false base station attack. The weaknesses allow an adversary to redirect user traffic derived from one of network to another. It in addition allows an adversary to utilize authentication vectors at a corrupted foreign network to impersonate some other networks. Also, the usage of synchronization in between a cellular station and home circle incurs sizeable difficulty with the normal operation of LTE AKA. To deal with the safety measures problems and supply further development on LTE AKA, we presented a fresh authentication and also key arrangement protocol (SEAP-AKA) which can defeat the redirection strike and drastically mitigates the impact involving network data corruption. The protocol SEAP-AKA in addition eliminates the synchronization between the mobile station plus the home circle. Depending on the execution atmosphere, entities inside protocol hold the flexibility involving adaptively picking flows with regard to execution. We show that the adaptability allows you optimize the efficiency involving SEAP-AKA in the home circle and foreign networks. we also showed removal of synchronization between a cell station and its home system improves efficiency without compromising security.

Future Research

For future work, considering the dynamic and fast evolution of IP and Mobile threat, 256 bits encryption should be considered in the encryption process without compromising computation speed and further efficiency, considering the fact, that the more bit keys is involved in security the more difficult it is for intruders to gain access to a secured system.

Authors Profile

Uwaya Fidelis obtained his Bachelors degree from Nnamdi azikiwe University, Awka Nigeria and presently studying for his M.Tech in Systems and Signal Processing in the department of ECE. His research interest are in Wireless Mobile Security, Mobile Payment Security, Speech processing and Mobil Computing and Communications.

Mrs. Thoomori Madhavi Kumari, obtained her BTECH from ECE JNTU and her MTECH from Computer science. Presently Mrs Madhavi is pursuing her PHD from in Data Security in Language using FPGA. She has being with JNTUH for 13 years and presently an Associate professor cum Assistant Director UGC-ASC JNTUH. She is also associated with AICTE sponsored project on computer networks.

REFERENCES

[1] H. Dake, W. Jianbo, Z. Yu, "User authentication scheme based on selfcertified public-key for next generation wireless network," Proc. IEEE International Symposium on Biometrics and Security Technologies, IEEE Press , 2005, pp.976-980
[2] Stephen Farrell. "The WAP Forum's Wireless Public Key Infrastructure," Information Security Technical Report, vol 5, 2000, . 23-31
[3] Z. Muxing, F. Yuguang. "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans, vol. 4, 2005, pp:734-742
[4] D. Yaping, F. Hong, X Xianzhong, "A secure and efficient group authentication and key agreement protocol for LTE networks," Proc. Elsevier 2013, Computer Networks 57, 2013, pp 3492 – 3510
[5] Third Generation Partnership Paper (3GPP), 3GPP TS 33.102 v8.2.0. "3G Security; Security Architecture (Release 8)," 2009
[6] Third Generation Partnership Paper (3GPP), 3GPP TS 33.401 v8.2.1. "3G System Architecture Evolution (SAE); Security Architecture (Release 8)," 2009
[7] H.H. Ou, M.S. Hwang, J.K. Jan, A cocktail protocol with the authentication and key agreement on the UMTS, Journal of Systems and Software 83 (2) (2010) 316–325.
[8] A. Fu, S. Lan, B. Huang, Z. Zhu, Y. Zhang, A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks, IEEE Communications Letters 16 (11) (2012) 1744–1747.
[9] N. Seddigh et al, Security Advances and Challenges in 4G Wireless Networks, IEEE, 2010, 8th annual international conference on privacy. Page64.
[10] Anastasios N. Bikos, Nicolas klavos,LTE/SAE Security Issues on 4G Wireless Networks:, 2011,www.computer.org/security.
[11] Security in the Evolved Packet System, Rolf Blom et al, keeping wireless communication secure. page 4. 2010.
[12] khodo hamadi et al, W-AKA: Privacy-Enhanced LTE-AKA Using Secured Channel over Wi-Fi,2013 IEEE
[13] Lang Wang et al, Mobility Management Schemes at Radio Network Layer for LTE Femtocells, 2009, IEEE.

[14] C. Huang and J. Li, "AKA protocol for UMTS with low bandwidth consumption," in Proc. of the 19th International Conference on Advanced Information Networking and Applications (AINA), March 2005.
[15]www.technologyreview.com/news /427344/verizon-envisions-4g-wireless-in-just-about-anything.
[16] Ahmad Salahi et al,Enhanced Authentication and Key Agreement Procedureof next Generation 3GPP Mobile Networks. International Journal of Information and Electronics Engineering, Vol. 2, No. 1, January 2012

