IPHV8I1023X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

SECURITY AND PRIVACY PROTECTION IN 4G NETWORKS

[#1]PEDDI KISHOR-Associate Professor, HOD, Dept of CSE

[#2]P.SANGEETHA, Dept of CSE,

SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, T.S., INDIA.

Abstract: Future generation 4G network is considered to bring most seamless data and internet access across different devices and networks. 3G network architecture incorporates several mechanism for continues connectivity. 4G networks abstracts the communication as any form of digital data including but not limited to voice and video calls, media streaming, content sharing, cloud computing and distributed services. 4G network offers a seamless collaboration between core 3G data network, local WiMax networks, GSM networks and so on. Every core network follows it's own architecture and protocols. Therefore switching from one network to another requires techniques that ensures optimum performance and quick switching. In this research first explain evolved authentication and key agreement protocol for next generation Long term evolution/ System Architecture Evolution(LTE/SAE)networks and compared its enhancements with contrast to Universal Mobile Terrestrial System- Authentication and Key Agreement(UMTS-AKA), then, offers a new improvement protocol which increases performance of authentication procedure. The current 3GPP LTE –AKA has some shortcomings, including bandwidth consumption between a serving networks and a user's home network, computation overhead and imperfect mutual authentication. in fact the new proposed protocol by sharing serving network with Home Subscription Server(HSS) for execution of authentication procedure and increasing a little computation in Mobility Management Entity(MME) and generated joined authentication vectors in both MME and HSS can remove aforementioned problems during authentication process. The proposed scheme is analyzed and its advantages have been verified by simulation. Our new proposed protocol can satisfy security requirements and simulation result shows in the proposed-AKA with contrast to original-AKA, the more MS and service request rate, the more considerable deduction of authentication load for HSS.

Keywords: 4G, QoS, Vertical Handoff, Bandwidth, Signal Strength, Link Quality, EPS, LTE-Advance.

I.INTRODUCITON

Connectivity among multiple Wireless networks is becoming an increasingly important and popular way for providing seamless connectivity to the mobile users. Current technologies vary widely in their bandwidths, latencies, frequencies, and media access methods. In simple words there are several wireless networks in place and in use with different architecture, MAC protocol, services, Bandwidth, Cost and accessibility. Unfortunately, no technology in and of itself makes possible the best available network at all times. For example a WLAN may be better at internet connectivity over GSM cellular network, but when it comes to voice calls, the second clearly outperforms the first. No single network technology provides a low-latency, high-bandwidth and wide-area connection for all the services over the whole access time to a huge number of users. Therefore 4G networks are built around the idea of making the best network available to an end user. In the other conventional networks, for example 2G and 3G horizontal handoff system, a handoff or passing the services from one to another peer was designed to support the mobility and the handoff is generally a designed phenomenon between two base stations such that when a mobile device leaves a cell, the current base station handoffs the connection to the base station of the cell that the mobile device is currently on.

But in the 4G network, at a same time several connections may be available to a particular node for a particular service. The end user or the network node is initiated Vertical Handover, that is supported by the designed protocols. Few studies said that opting for a handover depending upon the access cost. Such as for connectivity of internet, a Cellular Gateway and a WLAN gateway are available to the end user. When the end user needs high speed connectivity, it can use WLAN which will cost more and when he requires a low speed low cost connection, he can switch back to cellular gateway. Competition is increasing among the wireless service providers and the infrastructure cost coming down, cost becomes a secondary metric to the quality in connections. Therefore in this work we focus on designing a system for measuring and quantifying the Quality of Service at the end

node and selecting an appropriate network based on the best QOS available from a network. We estimate the quality of service by calculating the bandwidth between links from available gateways to the end node and by measuring the received signal power. Even though Handoff is easy for theoretical claims, it passes on several challenges which include detection of handoff need and initiating the handoff process.

In order to provide secure services over wireless networks with high QoS, security mechanisms such as authentication and encryption are deployed. EPS provides security feathers in a similar way as UMTS and GSM. As one of the most widely used security mechanisms, authentication is a process to identify a mobile user. Considering the large changes made in the mobile network 3.xG, one of the main issues in these networks is discussion of security against various threats, which by progress and increase the growing complexity of networks and entry various services such as new multimedia services, Internet and e-commerce features, tried to improve the security mechanism. For instance, one of the most evolved security mechanisms is authentication and key agreement protocol (AKA) in 3.xG mobile networks which have been mutual. During the AKA protocol, parties (user and network) authenticate each other and agreed on the encryption and integrity keys, by the specific and complex mechanisms and algorithms (function f).Also, during authentication process in next generation mobile networks, key separation and key hierarchy has been added. Because of the importance of authentication protocol in the access network, to be more complex in terms of computational, and increasing different types of traffics (voice, data and multimedia) as well as integration of various networks and following that, increased traffic due to added handover between different networks and within a network as one of the authentication trigger on the access network, the authentication signalling overhead volume has been very high. So in terms of evaluation authentication protocol traffic in next generation mobile networks (LTE) and finding ways to improve the efficiency of mobile networks in terms of traffic overhead and decrease traffic without damage to network security is very important. Therefore, in this paper after research of the standard EPS-AKA authentication protocol in the LTE network, to improve its performance in terms of efficient use of bandwidth, and decrease wasted computation overhead, an improved protocol is recommended. The proposed protocol follows not only the security framework of the standard protocol, but also even in some security cases works better. In compare of the standard protocol, the quantity of improvement of proposed protocol is calculated and presented by computer software. A few research have been proposed to study the effect of number of authentication vectors [2] [3], the waiting probability of a new authentication vector [4], and the time interval needed to maintain an unused authentication vector [5]. Yan Zhang pointed out that a subsequent authentication event after all previous authentication vectors have been used must wait until the authentication vector arrays have been fetched from the authentication server[4].The authors showed that their proposed pre-authentication scheme decreases the authentication delay with minor increased signaling overhead.

II.RELATED WORK

Pedro et al. [1] proposes two different procedures in the handover preparation phase in IEEE 802.11, candidate access technologies discover and resources availability check, can be performed only in one procedure, optimizing the handover process.

Inwhee Joe et al.[2] propose a mobility-based prediction algorithm with dynamic LGD (Link Going Down) triggering for vertical handover by applying the IS (information server) of IEEE 802.21 MIH (media independent handover). The proposed algorithm predicts a possible moving area (PMA) of the mobile terminal based on mobility information (the velocity, coordinate values, position, movement detection, etc) in IS. Since the PMA indicates a next target cell for handover, it can advance the LGD trigger point dynamically to prepare for handover beforehand.

Khan [3] proposes an approach build on IEEE 802.21 standard for service negotiation. SIP and IPv6 based flow management approaches are discussed, the later approach is implemented using OPNET modeller simulator. The performance of our approach is compared with Long-term contractual approach in terms of users throughput, users' cost, operators' revenue and call blocking probability.

In [4] Ferrus et al. develop a comprehensive framework to categorize interworking solutions by defining a generic set of interworking levels and its related key interworking mechanisms. The proposed framework is used to analyze some of the most relevant interworking solutions being considered in different standardization bodies. More specifically, I-WLAN and GAN approaches for WLAN and cellular integration, solutions for WiMAX and 3GPP LTE/SAE interworking, and the forthcoming IEEE 802.21

standard are discussed from the common point of view provided by the elaborated framework.

Lampropoulos [5] discusses enhanced handover functionality is described for integrated Wi-Fi/WiMAX networks, based on the recently established IEEE 802.21 standard that serves to glue together heterogeneous wireless access technologies. Moreover, alternative implementation choices are introduced with an emphasis on the mapping of primitives between the IEEE 802.21 standard and the various underlying access network technologies. As a result, optimized media-independent handover operations are provided alongside highlighted possible improvements to the related standards.

Shin-Jer Yang and Sao-Uen Chen [6] proposed IQDE (Improved QDE) to mitigate service interruption and improve the performance via following new features: (1) Adding IEEE 802.21 MIH parameters; (2) Adopting IQDE to shorten the QoS path reestablishment time for improving service continuity problems on the MIPv6. the simulation results indicate that PFMIPv6 with IQDE can provide stable Packet Transfer Delay (PTD), obtain higher Throughput (TH), and lower Packet Delay Variance (i.e., Jitter) than other two handover protocols, FMIPv6 and PFMIPv6.

Buiati et. al. [7] Proposes a new Media Independent Handover (MIH) standard Using the IEEE 802.21; this letter proposes a new neighbor network discovery mechanism, considering a hierarchical view of the network information. Atanasovski[8] discusses novel methods for resource management in heterogeneous network. They propose techniques for media handover and management specially in wireless management.

Guang Lu [9] presents a solution using IEEE 802.21 to enable seamless mobility for data and video streaming sessions. The solution was implemented and evaluated using commercial wireless networks and mobile devices. Lab and field trial results show minimal handover delay and improved user experience.

V. Kumar [10] presents a novel vertical handover scheme applicable for IEEE 802.11 (WLAN) and Universal Mobile Telecommunication System (UMTS) based on IEEE 802.21. UMTS is a 3GPP (Third Generation Partnership Project) technology, which is being used in cellular networks. WLAN is a LAN technology which supports smaller coverage area than the cellular networks. Vertical handover between these two is needed because they have different RAT.

Jiann-Liang Chen[11] develops a novel IEEE 802.21 MIH (Media Independent Handover) mechanism for next generation vehicular multimedia network. An adaptive QoS management mechanism is also proposed. By obtaining received signal strength parameters, the proposed MIH framework can determine the best available network. The adaptive QoS mechanism substantially improves the performance of real-time multimedia applications. The simulation results show that average handover time is slower than both UMTS and WiMAX when the MIH mechanism is used in vehicular network. However, the simulation results confirm that using the IEEE 802.21 MIH mechanism can increase overall throughput. Increased throughput is satisfactory compensation for increased handover time.

Jun Yuan et al. [12] proposes a novel scheme using IEEE 802.21 MIH services to improve packet loss performance by utilizing the active links to maintain the data flow. The MIH services, Link_Action and MIH_Link_Action, are extended and an MIH event named Link_PDU_Receive_Status is added. A complete message exchange in handover procedure is provided. Numerical analysis shows that the proposed scheme performs better in terms of packet loss comparing with the traditional independent FMIPv6 scheme.

Obreja [13] presents a solution for mobility management in heterogeneous networks which is based on the MIH framework. It is presented the architecture and the simulation testbed used for system validation. QualNet simulator was chose to implement the proposed solution.

III. EVOLVED PACKET SYSTEM (EPS)

EPS is an evolution of UMTS system in order to satisfy a huge demand of high-speed data rates and provide support for a constantly increased number of cellular users. In contrast with previous generations, LTE has been designed considering all the services as IP data traffic, voice calls included, facilitating integration of user data traffic into operator core network but fostering new well-known attacks for IP networks. 3GPP has developed a robust system, adapted to provide services with high requirements of data bandwidth and able to cope the growth of mobile-phone users. Their effort is also focused on security issues to consider the previous UMTS threats in order to prevent future menaces in LTE.

Between the characteristics of the latest release of LTE Advanced, a few innovations are highlighted:

IPHV8I1023X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

_ Carrier aggregation, providing a flexible and more efficient use of the spectrum.

_ Enhanced downlink Multiple Input/Multiple Output (MIMO), increasing the cell throughput.

_ Enhanced Inter-Cell Interference Coordination (ICIC), enhancing interference management between cells.

_ Relay Nodes (RNs), used to cover wider areas.

_ Home E-UTRAN Node-B's (HeNBs), improving indoor data rates.

LTE-Advanced system should target peak rates of 1 Gbps/500 Mbps for the downlink/uplink respectively, accord-ing to the theoretical expectations [1], exceeding the 300 Mbps/75 Mbps rates of LTE standard and supporting mobile speeds up to 350 km/h.

A. Architecture

The whole system is divided in two parts: Evolved Packet Core (EPC) in figure 1 and Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) in figure 2. Compatibility with old network infrastructures is provided, based on 3GPP or non-3GPP technologies, being them classified as trusted or non-trusted accessing networks [2]. This classification describes the way to authenticate the users, defines how to migrate their security contexts during a handover process and establishes the behaviour of the core network towards the user.

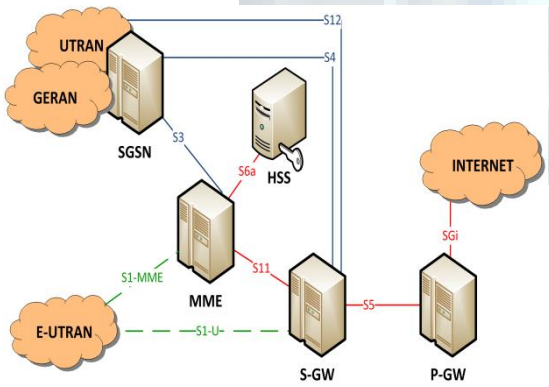


Fig. 1. The EPC architecture

As specifications describe [3][4], core network is composed of:

Mobility Management Entity: MME is the process unit to manage communications between UE and e-NodeBs, identify and authenticate the user, assign bearers, establishing downlink/uplink and NAS security, storing key material and providing services.

Home Subscriber Service: HSS coordinates the functions of the authentication centre, stores the subscription-related information to support the network entities handling calls and ses-sions. It generates fresh key material over demand.

Serving Gateway: S-GW is the local mobility anchor, controlling the packet routing and forwarding tasks, beside of other transport level functions. It implements quality-of-service (QoS) functions and lawful interception fea-tures.

Packet Data Network Gateway: P-GW acts as intermediate between the operator network and Internet, providing IP address for each UE and recording service charges.

Serving GPRS Support Node: SGSN provides compatibility with packet switching services of old access networks, such GERAN (GSM system) or UTRAN (UMTS system).

On the other hand, the radio access network acts as a link between the User Equipment (UE) and the core network. EUTRAN Node B (eNB) entities provide services to the end user, by means of the radio channels. After release 10, support for Relay Nodes (RNs) and Home EUTRAN Node B (H-eNB) or femtocell are added to provide a wide coverage area without minimising QoS. A group of H-eNBs may be gathered and addressed to a Home EUTRAN Node-B Gateway, reducing the number of interfaces linked directly with the core network.

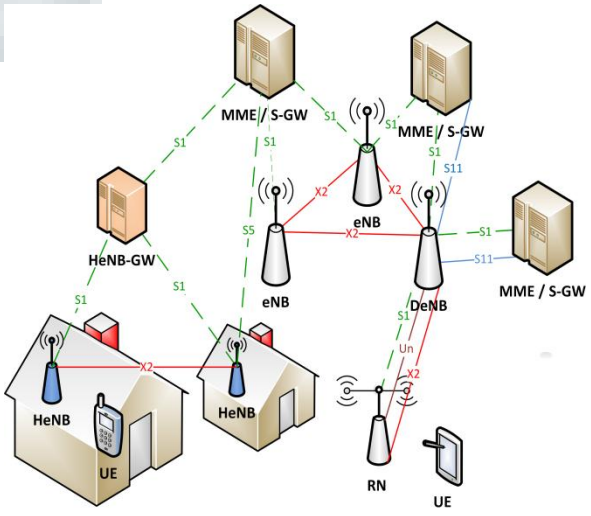


Fig. 2. E-UTRAN architecture

IPHV8I1023X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

B. Security Features

Security architecture groups the security features into five categories [5], establishing their scopes:

- Network access security, to provide a secure access to the services by the user.

- Network domain security, to protect the network ele-ments and secure the signalling and user data exchange.

- User domain security, to control the secure access to mobile stations.

- Application domain security, to establish secure commu-nications over the application layer.

- Visibility and configuration of security, bring the oppor-tunity for the user to check if the security features are in operation.

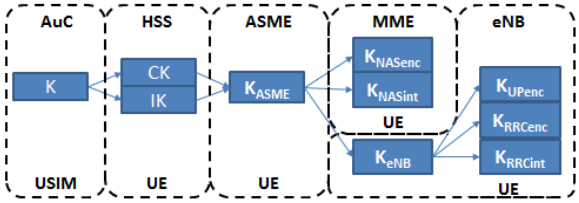


Fig. 4. Key hierarchy for E-UTRAN

Although, 3GPP enumerates the security and privacy requirements in which the system bases its reliability [6]. In term of security, the EPS should provide a high level of security equal or better than the current systems, protection against threats and attacks including Internet menaces and the assurance of any user are able to gain access to the serving network without being authorized previously.

IV. SECURITY THREATS

A. User Identity: User-identity transference in clear-text during the initial attach procedure compromises the entire system, creating a security gap which exploitation allows an eavesdropper to track the user cell-location or perform an man-in-the-middle attack between the UE and the eNB by means of user IMSI impersonation and relay of user messages.

B. Femtocells: Femtocells becomes a great risk, as they are the only core-network devices out of the operator control. These devices are located inside the user home installations, connected to a local e-NodeB to provide wide coverage extension, but being physically accessible by the customer. Tampering the device to avoid software updates, or mod-ifying their usual behaviour may create an important breach inside the core network [7]. Once the device software is mod-ified without the operator consciousness, UE may be driven to use clear-text communications during the AKA process, faking the security capabilities to force a null encryption.

C. Interoperability: 3GPP establishes the conditions to migrate security contexts associated to an user, considering the classification of the access network. Direct context transference is only possible when the two technologies belong to 3GPP trusted access networks, but for a limited period of time. UE must be re-authenticated once the migration process is completed without interrupt the service.

Nevertheless, multi-access and seamless mobility requires a strong collaboration between the different operators and a restricted interoperability policy to avoid unauthorized access to the system. Furthermore, compatibility with legacy systems is also an acceptance of their vulnerabilities. GSM is a clear example of a vulnerable system, with remarkable weaknesses identified, such as a man-in-the-middle attack (MITM) [8].

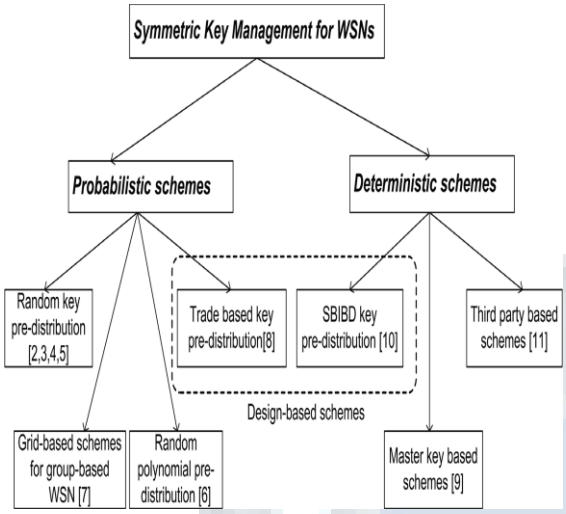
D. RRC signaling: 3GPP specifications files include a few RRC signalling messages whose transmission happens in clear-text, before the security domain is established. These messages can be easily sniffed, and replied towards the eNB several times to collapse the system with a traffic-injection attack. The serving network is unable to detect the attack and process all the petitions, reducing the resources to attend real service request. The attacker simulates a usual behaviour of a legitimate UE with a direct consequence, a deny-of-service (DoS) attack [9].

E. Other threats: Being an all-IP networks makes the system vulnerable against IP attacks, such Deny of Service (DoS) over the public IP addresses of the core network interfaces, traffic eavesdropping and injection attacks. Selective flooding attacks may reduce the QoS or even cut the service of the legitimate users.

Furthermore, physical protection over the access network infrastructure must be considered, besides of the core-network elements and wired connections. Specially for HeNBs, as we pointed out above, where the devices are easily accessible by bad-intentioned users.

IPHV8I1023X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

V.SYMMETRIC KEY MANAGEMENT



Key management problems in WSNs have been extensively studied in the literature and several solutions have been proposed . In this work, we mainly classify symmetric schemes into two categories: *probabilistic* schemes and *deterministic* ones (see Figure 1). In *deterministic* schemes, each two neighboring nodes are able to establish a direct secure link which ensures a total secure connectivity coverage. In *probabilistic* schemes, the secure connectivity is not guaranteed because it is conditioned by the existence of shared keys between neighboring nodes. We give in table I the definition of the five considered evaluation metrics, while we summarize in table II the main used symbols.

A. Probabilistic schemes

In probabilistic key management schemes, each two neighboring nodes can establish a secure link with some probability. If two neighboring nodes cannot establish a secure link, they establish a secure path composed of successive secure links. Eschenauer and Gligor proposed in the basic Random Key Pre-distribution scheme denoted by RKP. In this scheme, each node is pre-loaded with a key ring of k keys randomly selected from a large pool S of keys. After the deployment step, each node i exchanges with each of its neighbor j the list of key identifiers that it maintains. This allows node j to identify the keys that it shares with node i. The values of the key ring size k and the key pool size $|S|$ are chosen in such a way that the intersection of two key rings is not empty with a high probability. This basic approach is CPU and energy efficient but it requires a large memory space to store the key ring. Moreover, if the network nodes are progressively corrupted, the attacker may discover a large part or the whole global key pool. Hence, a great number of links will be compromised. Chan *et al.* proposed in a protocol called Q-composite scheme that enhances the resilience of RKP. In this solution, two neighboring nodes can establish a secure link only if theyshare at least Q keys. The pairwise session key is calculated

TABLE

SUMMARY OF NOTATIONS

S The global key pool

$|S|$ The size of the global key pool

KRi The key ring of node i

$|KRi|$ The size of the node i key ring

n The network size (number of nodes)

l The key size

Q The minimum number of common keys required to establish a secure link in the Q-composite scheme

m The design order (SBIBD and Unital)

k Key ring size & Block size of a given design

(q, k) The two parameters of the Ruj *et al.* trade construction (k is also the block size) $p(i)$ The probability that two nodes share exactly I keys in their subset of keys Pc The probability that two nodes can establish a secure link Rx The network resiliency when x nodes are captured as the hash of all shared keys concatenated to each other:

$Ki,j = Hash(Ks1Ks2 ..._Ksq)$ where $Ks1,Ks2$, $...Ksq$

_are the $q_$ shared keys between the two nodes i and j ($q_ \geq Q$).

This approach enhances the resilience against node capture attacks because the attacker needs more overlap keys to break a secure link. However, this approach degrades the network secure connectivity coverage because neighboring nodes must have at least Q common keys to establish a secure link.

Chan *et al.* proposed also in a perfect secure pairwise key pre-distribution scheme where they assign to each possible link between two nodes i and j a distinct key Ki,j. Prior to deployment, each node is pre-loaded with $Pc \times n$ keys, where

n is the network size and *Pc* is the desired secure coverage probability. Since we use distinct keys to secure each pairwise link, the resiliency against node capture is perfect and each captured node does not reveal any information about external links. The main drawback of this scheme is the non scalability because the number of the stored keys depends linearly on the network size.

VI. CONCLUSION

Mass effort has been made in order to protect and guarantee secure mobile communications towards LTE infrastructure since the earlier releases of 3GPP specifications. However, future improvement is required to neutralize the actual attacks and vulnerabilities that may compromise the user identity, data privacy, signalling traffic as well as access and core-network equipment. This study of security issues in 4G networks has revealed that both WiMAX and LTE security architectures are at advanced stage of specification. This study focused primarily on MAC layer vulnerabilities for WiMAX and LTE. Both standards also have some physical layer vulnerabilities to interference and scrambling techniques. At the MAC layer, WiMAX is susceptible to DoS attacks, eavesdropping, replay attack, service degradation, and vulnerabilities due to faulty key management. Some of these vulnerabilities have been addressed in subsequent versions of the standard (e.g., 802.16e and 802.16m). LTE also has a set of potential vulnerabilities at the MAC layer. Examples of specific vulnerabilities include: illegal use of user and mobile equipment, location tracking, DoS attacks and data integrity attacks.

The robustness and effectiveness of end-to-end security approaches in Wi MAX and LTE will become clear only after deployment. While both standards improve on their predecessors, there is clearly still work to be done. We believe there is a strong need for continued study on 4G security issues and development of appropriate counter measures. To date, majority of the research work has focused on studies or preliminary simulations. We suggest that there is a critical need to augment this initial research with emulation and test-bed related studies which will likely reveal further issues and challenges to be addressed.

REFERENCES

[1] 3rd Generation Partnership Project TS 36.913, Technical Specification Group Radio Access Network; Requirements for further advancements for Evolved Universal Terrestrial Radio Access (E-UTRA) (LTE-Advanced), ver.10.0.0, release 10. (2011)

[2] 3rd Generation Partnership Project TS 33.402, Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses. Security, ver.11.2.0, release 11. (2011)

[3] 3rd Generation Partnership Project TS 36.300, Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2. Sophia, ver.10.5.0, release 10. (2011)

[4] 3rd Generation Partnership Project TS 36.401, Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Ac-cess Network (E-UTRAN); Architecture description. Control, ver.10.3.0, release 10. (2011)

[5] 3rd Generation Partnership Project TS 33.401, Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture. Network, ver.11.2.0, release 11. (2011)

[6] 3rd Generation Partnership Project TS 22.278, Technical Specification Group Services and System Aspects; Service requirements for the Evolved Packet System (EPS), ver.12.0.0, release 12. (2011)

[7] Bilogrevic, I., & Jadliwala, M. & Hubaux, J.-pierre., Security and Privacy in Next Generation Mobile Networks : LTE and Femtocells. 2nd International Femtocell Workshop, Luton (2010)

[8] 3rd Generation Partnership Project TS 33.801, Technical Specification Group Service and System Aspects; Access Security Review, ver.1.0.0, release 7. (2005)

[9] Yu, D., Non-access-stratum request attack in E-UTRAN. Computing, Communications and Applications, 48-53. (2012)

[10] Mun, H., Han, K., & Kim, K. 3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA. Wireless Telecommunications Symposium. WTS2009 (pp. 18). IEEE. (2009)

[11] Vintila, C., & Patriciu, V. Security Analysis of LTE Access Network. ICN 2011, The Tenth International, (c), 29-34. (2011)

[12] Xiehua, L., & Yongjun, W. Security Enhanced Authentication and Key Agreement Protocol for LTE / SAE Network. 7th International Confer-ence onNetworking and Mobile Computing Wireless Communications (WiCOM), 0-3. (2011)

[13] Køien, G. M., Mutual Entity Authentication for LTE. Wireless Commu-nications and Mobile Computing Conference (IWCMC), 689-694. (2011) [14] Zheng, Y., He, D., Yu, W., & Tang, X. Trusted Computing-Based Secu-rity Architecture For 4G Mobile Networks. 6th International Conference
on Parallel and Distributed Computing Applications and Technologies (PDCAT05), 251-255. Ieee. doi:10.1109/PDCAT.2005.243 (2005)

[15] Zheng, Y., He, D., & Tang, X. AKA and Authorization Scheme For 4G Mobile Networks Based on Trusted Mobile Platform. , Information, 5th International Conference on Communications and Signal Processing, 976-980. (2005)