Journal of Engineering and Applied Sciences 13 (Special Issue 12): 9503-9507, 2018
ISSN: 1816-949X

Hierarchical Hand off Management and Public Reported Approach Protocol for Analyzing the 4G Long Term Evolution (LTE) Communication

Abidulkarim K. I. Yasari
College of Engineering, Al-Muthanna University, Samawah, Iraq

Abstract: Nowaday's mobile telecommunication placed a crucial role for making the effective communication, data, voice, images and video transfer. For these multipurpose, telecommunication effectively utilize the different generation of networks. Among the various generation, 4G Long Term Evolution (LTE) has been widely utilized in present technology. The developed 4G/LTE is developed by increasing the previous generations functionality. Even though the 4G transmit the information very fast, the network has facing several problems such as intermediate attacks, vulnerabilities and the Quality of Service (QoS). These vulnerabilities are overcome by applying the first publicly reported practical protocol with handoff management hierarchical IPv6 protocol for eliminating the intermediate attack. The first publicly introduce practical approach examines the network in semi, active and passive LTE for eliminating the intermediate attacks. In addition, the handoff management process maintains the connection between the nodes and Quality of Service (QoS) while moving from one access point to another using the hierarchical IPv6. The first publicly reported practical protocol with handoff management hierarchical IPv6 protocol is implemented using the software (Intel i7 processor and Ubuntu 14.04 OS) and hardware configuration (USRP B210 device) and the system ensures the effective results which is done by using the experimental results and the system achieves high security such as 96.45% with minimum time 6.98 msec.

Key words: Mobile telecommunication, Long Term Evolution (LTE), Quality of Service (QoS), first publicly reported practical protocol with handoff management hierarchical IPv6 protocol, vulnerabilities, intermediate

INTRODUCTION

In the developing technology 4G based communication process placed a crucial role in the various applications such as video conferencing, mobile TV, gaming process and so on. This 4G based communication prosess developed with the help of the Long Term Evolution (LTE) at Stockholm, Norway, Oslo and Sweden in 2009 (Shukla, 2011). The 4G communication process developed based on the previous generation 2 and 3G communication process but the functionality of this 4G has been increased due to the various disappointments present in the previous generations.

The 2G communication systems having the very low authentication between the network implementer and work which leads to create the various intermediate attacks in the communication process (Alezabi *et al*., 2014). This authentication problem is recovered by International Mobile Subscriber Identifier (IMSI) which transmits the signaling messages to the user subscriber for identifying the user that helps to enhance the authentication process. Some situations the authentication is still one of the issues due to the absence of the IMSI, the attacker may hack the base station (El Idrissi *et al*., 2012). Then the 2G communication process is further enhanced with the help of the 3G-partership project communication process for increasing the security during the communication. The 3G process implement the authentication between the user and network with the help of the cryptographic encryption process. Even though the 3G system ensures the security, privacy it is fail to manage the intermediate attack in LTE (Lai *et al*., 2013). Due to the disadvantages present in the communication process, the 4G based communication process has been developed for improving the security strength processing. Even though the 4G system ensures the security, the intermediate attacks are managed by analyzing the first practically attacks in terms of examining the location leaks, denial of services in the network. Different researches analyzing the intermediate attacks influenced in the network while making the communication process. Nandini Aggarwal *et al.* analyzing the various attacks present in the 4G/LTE for making the effective communication process. The network facing several hijacking attacks while requesting and making the voice call transaction. These hijacking attacks are overcome by applying the effective

communication protocols such as extensible authentication protocol authentication and key agreement, evolved packet system authentication and key agreement and simple password exponential key exchange. These protocols are effectively managing the authentication as well as user privacy in 4G/LTE. At last the merits and demerits are discussed for improving the authentication process. Rui Fortio analyzing and implementing the internet protocol security based communication system for improving the authentication and privacy process in the 4G communication system. During the communication process the method examines each communication component related elements such as Security Gateway (SecGW), LTE core side and so on. These components are examined with the help of the public key infrastructure, certificate based authentication and asymmetric key digital signature process. Further, the authentication system has been implemented with the help of the TWAMP evaluation laboratory environment. Thus the author introduces system ensures and manages the security while making the transaction. Mathi and Dharuman (2016) preventing the desynchronization attack present in the 4GLTE communication process. Initially researcher analyzes the effects present in this kind of attack in the handover key management system. Based on the impact of the attack researcher introduces the system that uses the neighboring changing count values for making the effective communication process in LTE. Then, the performance of the system is implemented with the help of experimental results which is developed by using the network simulator and the system maintains the security, LTE authentication with significant communication cost. According to the above researcher's discussions, the 4G/LTE communication process handles several intermediate attacks while making the communication process. Then, the study analyzes different attacks present in the system as well as the authentication management protocol along with the quality of service which is explained.

MATERIALS AND METHODS

Secure 4G/LTE communication process using first publicly introduce practical approach: The 4G/LTE communication process contains the various network access processes while making the transaction from base station to mobile device (Wang *et al*., 2014). During this process LTE infrastructure has several components such as User Equipment (UE), Evolved Packet Core (EPC) and Evolved Universal Terrestrial Radio Access Networks (E-UTRAN). These components are commonly called as the Evolved Packet System (EPS). In LTE communication process, UE is mainly referred as the user communication device that is commonly as smart phone which contains the Universal Subscriber Identity Module (USIM). The USIM referred as the IMSI that used to save the user personal and credential information. So, USIM involved in the communication process with authentication protocol to ensures the security while accessing the information. The other component is E-UTRAN that helps to manage the communication between UE and other EPC because it consists of collection of base station. The base station is denoted as the evolved-NodeB (eNodeB) which contains the bunch of access protocol namely referred as the Access Stratum (AS). AS used to transmit the signaling message to the UE because it has Radio Resource Control (RRC) message protocol (Han and Choi, 2014). More over the E-UTRAN is ability to involved in the paging UEs, data connectivity in physical layer, handovers and air-security. Last component is EPC which consists of collection of IP mobile core network that helps to making the effective functionalities while requesting the communication process using the Mobility Management Entity (MME). The MME deals authentication process by eliminating the intermediate attack, after performing the related authentication process, the network provides the resources to the Users (UE). The discussed components are developed in the geographical locations using mobile carriers for providing the LTE services (Krishnamoorthy and Mathi, 2015). The mobile service region consists of Tracking Areas (TA) which is managed by MME. It has several cells in which each cell is controlled with the help of the eNodeB. In addition to this, the eNodeB transmits several information's such as Mobile Country Code (MCC), Tracking Area Code (TAC), Mobile Network Code (MNC) and cell Id to the user UE for recognizing the network operator with effective manner. The UE uses the attach procedure for making the attach with the network and Tracking Area Update (TAU) procedure for continuously update the area information to network services. This LTE infrastructure provides the different services to the user but the security is one of the main issues which is reduced by identifying the subscribers with the help of Globally Unique Temporary Identifier (GUTI). The GUTI is ascribing to the UE while attaching process which helps to continuously monitor the network traffic because the intermediate attack hack the user credential information in the network. In addition, to this security and privacy has been established by applying the enhanced authentication and key agreement protocol (Zhao *et al*., 2010) during the communication process. Initially, the protocol choses the random values u and d from the UE components for generating the key value. Before that MME estimates the B value as $B = g^m$

mod p. The computed B value has been sent to the UE with the help of the eNodeB. Then the user calculate the key by using the random values as follows, $A = g^u \bmod p$. After estimating the key value, the received B value is used to identify the shared key as follows, $K_{um} = B^u \bmod p$. With the help of the key values, the Protected IMSI (PIMSI) is calculated as follows, $PIMSI = fK_{um}(IMSI, R_u)$. During this calculation, R_u is choosen as random nonce then the values such as R_u, A, RIMSI to MME. From the response message from UE, the MME analyzes the shared key $K_{um} = A^m \bmod p$ and it has been transmitted to the home subscriber server with relevant K_{um}, RIMSI, R_u. Based on the received information the Home Subscriber Server (HSS) computes the shared key, $K_{uh} = K_{um} \oplus K$ in which the K value is denoted as the pre-shared key from UE and HSS. Then, the verification value and expected response has been generated with the help of created key values which is calculated as follows: $HSSV = f1_{Kuh}(R_u, R_h)$ in this R_h is the random value and expected response has been calculated as: $f^2_{Kuh}R_h$. The estimated value is transmitted to the MME. Then, the MME generate the verification value as $f_1(K_{um})$ (HSSV, R_m) and the estimated values are transmitted to the UE. Finally, the UE verifies the HSSV and MMEV values for authenticate the HSS and MME. If the values are matched each other then it generates the $RES = f2_{Kuh}(R_h)$ that is sent to MME. If the received message matches the success message transmitted to the UE else the failure message is transmitted to the user. This process is repeated continuously while requesting the services from the LTE which success fully eliminates the intermediate attacks such as passive, active and semi-passive attacks with effective manner. Even though the key management protocol establishes the authentication process, the quality of services is controlled and managed with the help of the hierarchical IPv6 protocol. The protocol reduces the traffic present in the network for improving the quality of services in the 4G LTE communication system. The hierarchical IPv6 protocol first divides the internet into different region and every region is interconnected with the help of the IP network which is commonly referred as the Mobility Anchor Point (MAP). At the time of communication process, the node has been maintained two addresses such as regional care of address and local care of address. First the regional care of address is stored in the MAP region and each mobile node is communicated with other node by using the regional address. While moving the node from one region to another region, the regional address has been fetched from MAP which is advertised in the new regional location information. This location address has been continuously updated for effectively access services from the base station without providing the space to the intermediate attacks. Thus, the first publicly reported practical protocol with handoff management hierarchical IPv6 protocol effectively access the information from the network without having the intermediate attacks also this process ensures the quality of services. Then, the excellence of the system is analyzed using the following experimental results.

RESULTS AND DISCUSSION

Experimental results: The first publicly reported practical protocol with handoff management hierarchical IPv6 protocol has been implemented with the help of the Mobility Management Entity (MME), User Equipment (UE) and evolved-NodeB (eNodeB) component. These components are integrated by using the USRP B210 device which is connected to the Intel i7 processor and Ubuntu 14.04 OS Software for making the effective communication process. During the communication process, the intermediate attacks are recognized and effectively provides the services to the user in terms of examining the network traffic because the minimized traffic improves the quality of services. At the time of this process, the network ensures the services with minimum cost, minimum time and high security. The communication cost has been defined by calculating the entire amount spending for each component involved while making the communication. Then the obtained cost value is shown in Table 1.

From Table 1, clearly shows that the various securities establish methods present in the 4G/LTE communication process. Among the several methods, first publicly reported practical protocol with handoff management hierarchical IPv6 Protocol consumes minimum communication cost when compared to the other methods. Then the graph representation of the communication cost is shown in Fig. 1.

Table 1: Communication cost

Methods	Communication cost (rupees)
Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKP)	1764
Evolved Packet System Authentication and Key Agreement (EPS-AKA)	1683
Simple Password Exponential Key Exchange (SPEKE)	1549
First Publicly Reported Practical Protocol With Handoff Management Hierarchical IPv6 Protocol (FPRP-HIPv6)	876

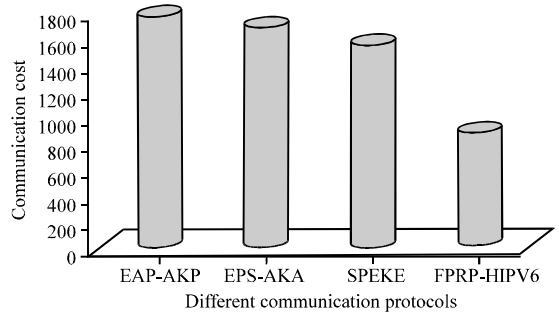

Fig. 1: Communication cost

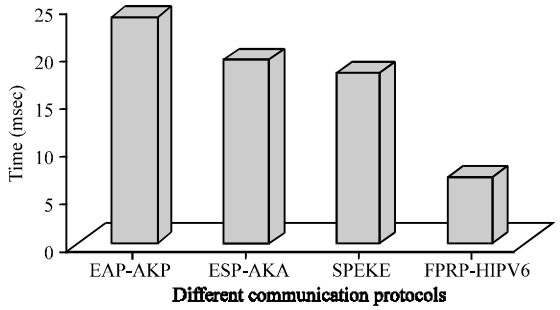

Fig. 2: Time

Table 2: Time

Methods	Time (msec)
Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKP)	23.78
Evolved Packet System Authentication and Key Agreement (EPS-AKA)	19.32
Simple Password Exponential Key Exchange (SPEKE)	17.98
First Publicly Reported Practical Protocol With Handoff Management Hierarchical IPv6 Protocol (FPRP-HIPV6)	6.98

Based on Fig. 1, the first publicly reported practical protocol with handoff management hierarchical IPv6 Protocol has establishes the communication with minimum amount (876) when compared to the other methods such as EAP-AKP-1764, EPS-AKA-1683 and SPEKE-1549. Even though the methods consumes minimum amount while making the communication, the network has attains the services from minimum time which measure by starting and stopping time estimation process at the time of initiating communication that is shown in Table 2.

Depending on Table 2, clearly shows that the various securities establish methods present in the 4G/LTE communication process with minimum time. Among the several methods, first publicly reported practical protocol with handoff management hierarchical IPv6 Protocol consumes minimum time IPv6when compared to the other methods. Then the graph representation of the communication cost is shown in the Fig. 2.

Based Fig. 2, the first publicly reported practical protocol with handoff management hierarchical IPv6 protocol attains the communication process with minimum time (6.98 msec) when compared to the other methods such as EAP-AKP-23.78 msec, EPS-AKA-19.32 msec and SPEKE-17.98 msec. Thus, the method establishes the communication with minimum cost and minimum time. In addition to this key management protocol ensures the security while making the communication process. Then the security accuracy is estimated by using the true positive, true negative, false positive and false negative values which are defined as follows:

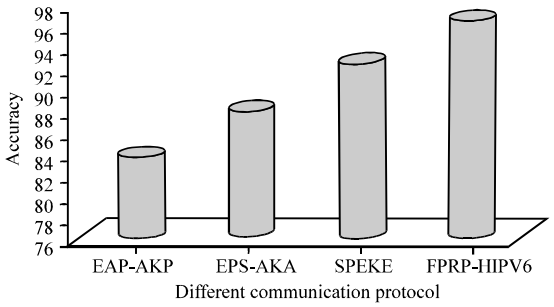

Fig. 3: Accuracy

Table 3: Accuracy

Methods	Accuracy (%)
Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKP)	83.56
Evolved Packet System Authentication and Key Agreement (EPS-AKA)	87.95
Simple Password Exponential Key Exchange (SPEKE)	92.43
First Publicly Reported Practical Protocol With Handoff Management Hierarchical IPv6 Protocol (FPRP-HIPv6)	96.45

$$\text{Accuracy} = \frac{\text{Number of true positive} + \text{Number of true negative}}{\text{Number of true positive} + \text{False positive} + \text{False negative} + \text{True negative}} \quad (1)$$

From the above Eq. 1, true positive is represented as the properly identified malicious nodes, false positive is wrongly identified legitimate node, false negative is wrongly not identified a malicious nodes and true positive is properly not identified a legitimated node while making the transmission in the wireless system. Then the obtained security accuracy is shown in Table 3.

Based on Fig. 3, it clearly shows that the First Publicly Reported Practical Protocol with Handoff Management Hierarchical IPv6 Protocol (FPRP-HIPv6) achieves the high security to the user credential information with high accuracy 96.45% when compared to the other methods such as EAP-AKP-83.56%, EPS-AKA-87.95% and SPEKE-92.43%.

CONCLUSION

Thus, the study examines the First Publicly Reported Practical Protocol with Handoff Management Hierarchical IPv6 Protocol (FPRP-HIPv6) based communication process in the 4G LTE. The communication system uses the different components while requesting the service form the base station. During this process the each component generate the authentication key with the help of the user credential information. This gives the authentication as well as eliminates the intermediate attacks. In addition to this the system manages the handoff management while moving from access point to another using the Mobility Anchor Point (MAP). Then the efficiency of the system is implemented with the help of the USRP B210 device which is connected to the Intel i7 processor and Ubuntu 14.04 OS software for making the effective communication process. Thus the FPRP-HIPv6 method establishes the effective communication services with minimum cost, minimum time and high accuracy of security.

REFERENCES

Alezabi, K.A., F. Hashim, S.J. Hashim and B.M. Ali, 2014. An efficient authentication and key agreement protocol for 4G (LTE) networks. Proceedings of the 2014 IEEE 10 Symposium on Region, April 14-16, 2014, IEEE, Kuala Lumpur, Malaysia, pp: 502-507.

El Idrissi, Y.E.H., N. Zahid and M. Jedra, 2012. Security analysis of 3GPP (LTE)-WLAN interworking and a new local authentication method based on EAP AKA. Proceedings of the 2012 1st International Conference on Future Generation Communication Technology (FGCT), December 12-14, 2012, IEEE, London, UK., ISBN:978-1-4673-5859-0, pp: 137-142.

Han, C.K. and H.K. Choi, 2014. Security analysis of handover key management in 4G LTE/SAE networks. IEEE. Trans. Mobile Comput., 13: 457-468.

Krishnamoorthy, V. and S. Mathi, 2015. Security enhancement of handover key management based on media access control address in 4G LTE networks. Proceedings of the 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), December 10-12, 2015, IEEE, Madurai, India, ISBN:978-1-4799-7848-9, pp: 868-872.

Lai, C., H. Li, R. Lu and X.S. Shen, 2013. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. Comput. Netw., 57: 3492-3510.

Mathi, S. and L. Dharuman, 2016. Prevention of desynchronization attack in 4G LTE networks using double authentication scheme. Proc. Comput. Sci., 89: 170-179.

Shukla, A., 2011. Super-Fast 4G wireless service launching in South Korea. Asia-Pacific Buisness and Technology, Kuala Lumpur, Malaysia. http://www.biztechreport.com/story/1619-super-fast-4g-wireless-service-launching-south-korea

Wang, J., Z. Zhang, Y. Ren, B. Li and J.U. Kim, 2014. Issues toward networks architecture security for LTE and LTE-A networks. Intl. J. Secur. Appl., 8: 17-24.

Zhao, J.L., Z.H. Gao and S.W. Jia, 2010. Improved Mobile IPv6 switching management scheme. Commun. Technol., 43: 103-105.