International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Robust and Flexible Authentication Model with Data Security – A Review

Nandini Aggarwal[1], Abhinav Bhandari[2]

[1]Punjabi University, University College of Engineering, Department of Computer Engineering, Patiala 147001, Punjab, India

[2]Assistant Professor, Punjabi University, University College of Engineering,
Department of Computer Engineering, Patiala 147001, Punjab, India

Abstract: ***The 4G/LTE is the popular cellular model which is getting more popularity and adding more number of users every year. The networks with the higher number of users become the hot pick for the hacking attacks. 4G/LTE is having a higher probability of attracting the users because it also offers the higher bandwidth (data transmission speeds) for the 4G voice or data links, which make it highly prone to the channel hijacking attacks. The proposed model is aimed at solving the problem of voice security by using the periodic authentication between the two users or nodes connected to the 4G/LTE network. The voice call hacking is being popular as there are several call leaks are reported every year, where the calls of the government officials, military personnel, business men, highly priority officials in the bigwigs of the industry, etc have been tracked. To overcome such thing, the proposed model must be capable of security the voice call channel from any kind of the external or internal hacking attempts. The proposed model is empowered with the quick and secure key management model for the 4G/LTE voice model. The proposed model performance will be evaluated on the basis of energy consumption, throughput, data drop rate, etc.***

Keywords: 4G security, key management, data privacy protection, confidentiality protection.

1. Introduction

The number of cellular users is rapidly growing every year. The available link bandwidth for the cellular networks is also increasing with every new cellular standard revision or development. Imagine a situation, where the person carrying mobile phone is connected to the 4G/LTE network in the stationary mode or travelling in any vehicle and using the internet or calling on the cellular networks. The problems of hacking attempts are rising on such networks every day.

With the development of every next cellular generation, the wireless systems are getting more and more intelligent and the user focused systems are rising with every new development. With every new cellular standard development, the number of intelligent user-focused services is getting higher and higher. The users are being offered with the number of new or improved services with higher available bandwidth, which attract the bigger volumes of the users. The 4G wireless technology has initialized its services from various cellular operators across the world in 2010. The industry majors like Alcatel, ITU, WWRF, DoCoMo, Nokia, IEEE, 4GW-PCC, Mobile VCE, Motorolla and Ericsson have adapted and offered the 4G services with local telecom operators in the wider global regions.

The networking era has begun in 1970 with the first analog-signal based voice-oriented network of first generation (1G) took birth. The development in the voice-based networks reached the new milestone with the development of the second generation (2G) cellular systems in the early 90s. The second generation platform offered the multiple services together using the wireless platform for the first time in the wireless history ending the mono-service era. The mono-media models of TDMA, CDMA One or GSM still exist, but with their amalgamation with some other technological standards in order to offer multiple services together. The mono-media models are combined in order to facilitate the users with the multiple of services to its users. The mono-media like GSM, CDMA and TDMA are the low bit rate mediums and offers the efficient services

The GPRS generation (or 2.5G) is the technology evolved between the 2G and 3G models. The 2.5G is offering the high throughput and data rate with optimized transmission models for the higher performance to the wireless users. The cellular networks marked the new development with the evolution of third generation networks (3G) in the early 20s. The 3G technology enabled the human-computer interactions and evolved in the cellular evolutions.

The evolution reached CDMA2000 and WCDMA standards, who were capable of offering the 2Mbps of the channel capacity for its users. These standards broke all of the records of the cellular models.

The new era of CDMA 2000 and WCDMA standards is marked as the huge development in the cellular history. The e-commerce portals initiated their operations during this era. The e-commerce operators offered shopping services on the mobile devices and increase the user experiences of the online shopping. The cellular operators started offering the higher order or user-centric services in the era. The user-centric services such as personalized apps or mobile sites emerged as the major businesses. Also VOIP and QoS became popular in this era over the third generation cellular networks.

Besides, distinctive short range correspondence frameworks like WLAN, Bluetooth and HIPERLAN and telecast correspondence frameworks with diverse elements traversed amid this time each with its own benefits and bad marks focusing on distinctive sorts of clients and distinctive administration sorts [2] making the circumstance more confounded for 3G frameworks.

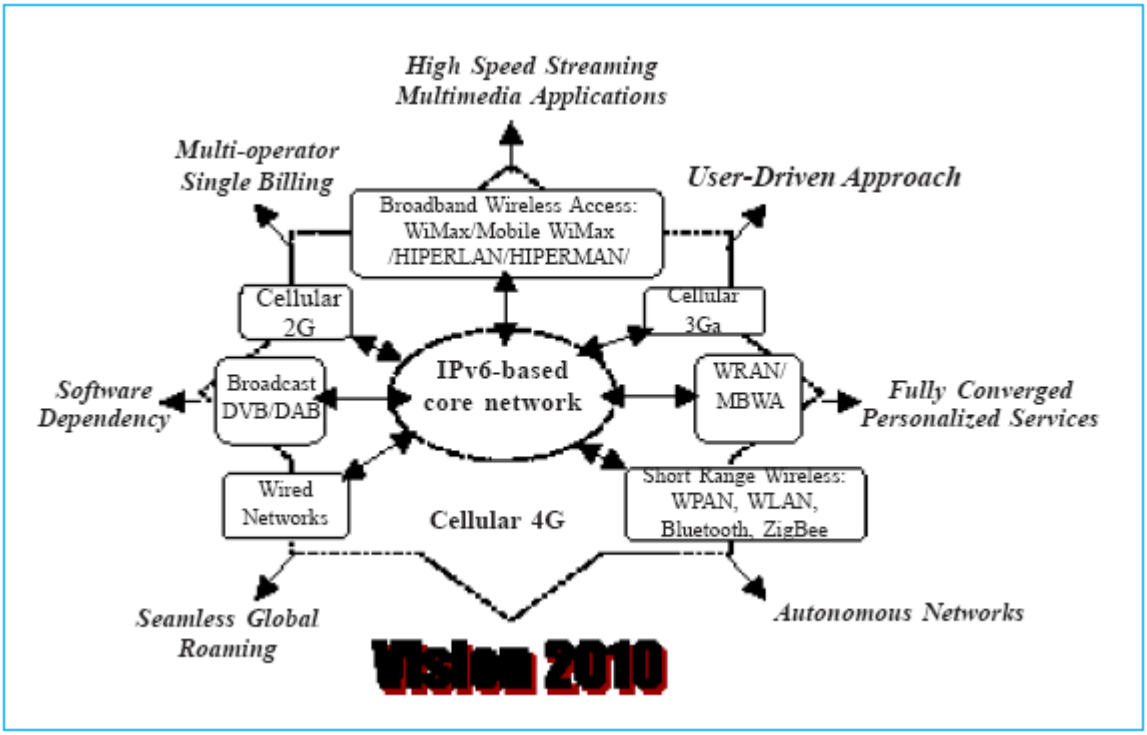

Figure 1: The overview of the 4G network

These confinements and disadvantages have produced the necessity for a general structure including all the current heterogeneous wired and remote frameworks being used. This IPv6-based potential 4G structure, usually portrayed as MAGIC [3] (Mobile mixed media, Anytime anyplace get to, Global versatility bolster, Integrated remote arrangement and Customized individual administration), would be profoundly dynamic and altogether handle the confinements of 3G frameworks. Along these lines, united arrangements that can consistently work on the various, different systems moving to the 4G environment satisfying the plenty of nextgeneration dream representations on executing a straightforward open remote structural planning (OWA), ought to be critically outlined. This clearly welcomes new difficulties on every stride and specialists overall face a tough errand of planning suitable arrangements. Figure 1, shows such a 4G vision.

2. Literature Survey

The 4G networks are the fourth generation cellular networks, which offer high bandwidth and fast speed. The 4G network provide the users with the capability of accessing the internet application alongside a voice or video call. The risk of active or passive information hijacking attacks is always there when a higher bandwidth link is being used for communication. Alezabi, Kamal Ali, et. al. have proposed an authentication protocol for 4G known as EEPS-AKA to overcome the security problems. The proposed convention is in view of the Simple Password Exponential Key Exchange (SPEKE) convention. Contrasted with past proposed strategies, our technique is quicker, since it utilizes a mystery key system which is speedier than endorsement based routines, also, the span of messages traded between User Equipment (UE) and Home Subscriber Server (HSS) is diminished, this lessens confirmation postpone and capacity overhead adequately. Seddigh Nabil et. al. have worked on a survey on 4G wireless network security advances and its challenges. This paper introduces an investigation of security advances and difficulties connected with emanant 4G remote innovations. The paper makes various commitments to the field. Initially, it thinks about the security guidelines advancement crosswise over distinctive eras of remote benchmarks. Second, the security-related principles, structural planning and outline for the LTE and WiMAX advances are broke down. Third, security issues and vulnerabilities introduce in the over 4G norms are talked about. At long last, we indicate potential ranges for future vulnerabilities and assess zones in 4G security which warrant consideration and future work by the examination and propelled innovation industry. Zongwei Zhou et. al. has worked on key management algorithm named as Key it Simple and Secure (KISS). This paper shows another key administration construction modeling, called KISS, to empower thorough, reliable, client certain, and financially savvy key administration. KISS ensures the whole life cycle of cryptographic keys. Specifically, KISS permits just approved applications and/or clients to utilize the keys. Utilizing basic gadgets, overseers can remotely issue confirmed orders to KISS and check framework yield. KISS influences promptly accessible thing equipment and trusted registering primitives to plan framework bootstrap conventions and administration instruments, which shields the framework from malware assaults and insider assaults. N. Suganthi, V. Sumathy, have proposed the algorithm bolsters the foundation of three sorts of keys for every sensor hub, an individual key imparted to the base station, a couple astute key imparted to neighbor sensor hub, and a gathering key that is shared by every one of the hubs in the system. The calculation utilized for building up and redesigning these keys are vitality productive and minimizes the contribution of the base station. Polynomial capacity is utilized as a part of the study. Ivan Damgård et. al. has proposed the secure key management method for cloud

environments. Authors have studied the levels of security on the basis what they can and what they cannot obtain in the security models. And after studying that all, authors have proposed a light-weight conventions accomplishing maximal security, and provide details regarding their useful execution. They have considered completely independent servers that switch in the middle of online and logged off periods without speaking with anybody from outside the cloud, and semi-self-ruling servers that need a constrained sort of help from outside the cloud while doing the move.

Table 1: Comparison of the existing 4G security and authentication models

Sr. No.	*Technique/Protocol Name*	*Purpose of Research*	*Point of Security*	*Effectiveness of AKA-Model*	*Disadvantages*
1	EAP-AKA [9] (Extensible Authentication Protocol – Authentication and Key Agreement)	Offered the Fast authentication and key agreement services.	Reduces the authentication delay, signalling cost. Empowers the security model.	Uses elliptic curve cryptography with Diffie-hellman. Users the symmetric key cryptosystem.	Diffie-hellman is highly exposed algorithm. Elliptic curve make the whole process slower.
2	EPS-AKA [10] (Evolved Packet System – Authentication and Key Agreement)	Works for UTMS-AKA and covers the USIM, enables security for MME and HSS.	Generate random nonce and computes the MAC (message authentication code). Mutual authentication between enhanced node base stations (eNB) and user equipment.	Last AKA version for UTMS-AKA security. Added with improvements and made complex to enhanced the level of security.	Suffers from various vulnerabilities such as disclosure of the user identity, computational overhead, Man In The Middle (MITM) attack and authentication delay.
3	SPEKE [11] (Simple Password Exponential Key Exchange)	Work between peer and authenticator. Designed for easy setup.	The password or Id is saved in the highly secured form where it is not easily detectible.	Resilient to active and passive attacks. Stronger and easier than certificate based authentication.	Security loophole exists due to the weak key scheme. Needs stronger encryption for security hardening.
4	EEPS-AKA [12] (Efficient EPS-AKA)	Follows SPEKE method with enhanced IMSI protection. Uses two random values for key generation.	Strong enhanced mutual authentication between user equipment and HSS. Provides stronger identity protection for IMSI information.	Resilient to MITM attacks. Adds lower signalling overhead. Offers vertical handovers with the same key.	Lacks in the super level encryption. Does not compress data as data compression may harden the security level.

3. Methodology

The 4G/LTE security model is being developed under this research project in the Network Simulator -2 (popularly known as NS-2). The 4G networks are the fourth generation cellular networks, which offer high bandwidth and fast speed. The 4G network provide the users with the capability of accessing the internet application alongside a voice or video call. The risk of active or passive information hijacking attacks is always there when a higher bandwidth link is being used for communication. The light weight key management scheme is the best solution than other alternatives, because it offers quick and secure transmission by adding a minimal computational overhead. The quicker and predictive mathematical equation being key generation scheme is being used for the purposed of the 4G call security. The voice data is the most sensitive information shared between the two users, where the attacks can be targeted. The secure text based communication applications can come with pre-embedded security mechanisms. The voice calls are never offered with the pre-embedded security architecture. The time-span based key sharing architecture will be used in order to protect the 4G voice calls. Hence, there is a strong need of the secure key management between the two nodes. The key sharing rules will be shared among the calling ends (the two nodes making a call) during the initial handshake. Afterwards the calling end will generate a key using a fixed mathematical equation, which will undergo preprocessing. The preprocessing steps include the byte shuffling, bit shift operations, key scrambling and other mechanism to create a unique and secure key. The key when received at the call termination end, it will undergo the exact reversal process as the pre-processing order. The original key will be obtained and matched for the integrity. If key matches, the data would be exchanged between the two nodes, otherwise the call would be terminated flashing the integrity breach message on the spammer's end.

4. Conclusion

The proposed model is based upon the security of the 4G/LTE network using the novel key management scheme. The proposed key management model has been designed to provide a quick, reliable and secure key exchange model based security. The proposed model is supposed to add the minimum delay in the voice communications taking place between the two nodes. The proposed model is intended to solve the security problem at a part in comparison with the existing models. The proposed model is based upon the cryptographic key exchange model, where a robust and quick encryption method used for the key security in the 4G communication between two nodes. The proposed model is aimed at solving the 4G security scheme with a better performance than the existing models. In the future, the proposed model can be improved by using the multi-level highly fast and efficient key exchange model. Also the data encryption can be added for the better level of security for data during the communications.

References

[1] Alezabi, Kamal Ali, Fazirulhisyam Hashim, Shaiful Jahari Hashim, and Borhanuddin M. Ali. "An efficient authentication and key agreement protocol for 4G (LTE) networks." In *Region 10 Symposium, 2014 IEEE*, pp. 502-507. IEEE, 2014.

[2] Seddigh, Nabil, Biswajit Nandy, Rupinder Makkar, and Jean-Francois Beaumont. "Security advances and challenges in 4G wireless networks." In*Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, pp. 62-71. IEEE, 2010.

[3] Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, "KISS: Key it Simple and Secure Corporate Key Management", Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904, pp. 1-18, Springer, 2013.

[4] N. Suganthi, V. Sumathy, "Energy Efficient Key Management Scheme for Wireless Sensor Networks", vol 9, issue 1, pp. 71-78, INT J COMPUT COMMUN, 2014.

[5] Ivan Damgård, Thomas P. Jakobsen, Jesper Buus Nielsen, and Jakob I. Pagter, "Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306, pp. 270-289, Springer, 2013.

[6] Ramaswamy Chandramouli, Michaela Iorga, Santosh Chokhani, " **Cryptographic Key Management Issues & Challenges in Cloud Services",** Computer Security Division Information Technology Laboratory, NIST, 2013.

[7] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi, "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", ETFA, vol. 18, pp. 1-8, IEEE, 2013.

[8] Md. Monzur Morshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol", IACC, vol. 3, pp. 571-576, IEEE, 2013.

[9] Idrissi, Y. E. H. E., Noureddine Zahid, and Mohamed Jedra. "Security analysis of 3GPP (LTE)—WLAN interworking and a new local authentication method based on EAP-AKA." In *Future Generation Communication Technology (FGCT), 2012 International Conference on*, pp. 137-142. IEEE, 2012.

[10] Koien, Geir M. "Mutual entity authentication for lte." In *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pp. 689-694. IEEE, 2011.

[11] Vintilă, Cristina-Elena, Victor-Valeriu Patriciu, and Ion Bica. "Security analysis of LTE access network." In *Proc. 10th Int'l Conf. Networks*, pp. 29-34. 2011.

[12] Alezabi, Kamal Ali, Fazirulhisyam Hashim, Shaiful Jahari Hashim, and Borhanuddin M. Ali. "An efficient authentication and key agreement protocol for 4G (LTE) networks." In *Region 10 Symposium, 2014 IEEE*, pp. 502-507. IEEE, 2014.