Review of multi-layer security architectures/models for 4G/LTE networks

Kanica
Research Scholar, CSE Dept.
CGC-College of Engineering, Mohali, Punjab

Anuj Kumar Gupta
Professor, CSE Dept.,
Chandigarh Engineering College, Mohali, Punjab

Abstract — 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. In this paper the focus is given on existing 4G techniques such as EAP-AKA, EPS-AKA, SPEKE, and EEPS-AKA.

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

I. 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, Do Como, Nokia, IEEE, and 4GW-PCC, Mobile VCE, Motorola 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 analogy-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, which 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 Quos 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.

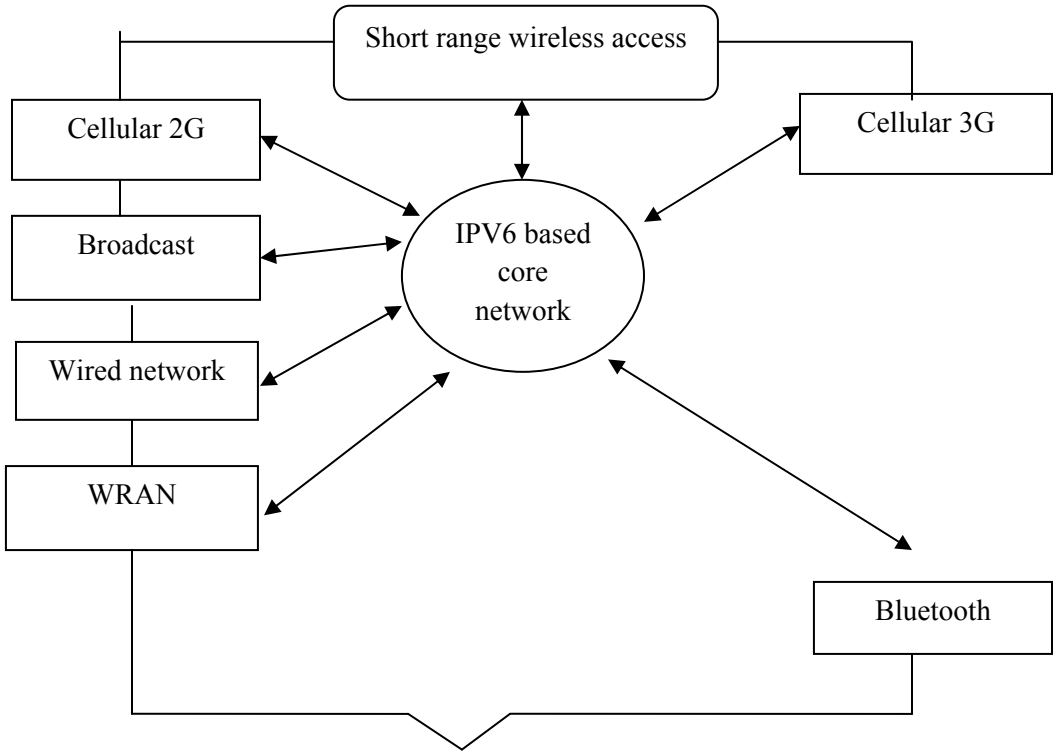

Figure 1. The overview of 4G Network

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 next generation 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.

II. OVERVIEW OF 4G

The 4G networks are the fourth generation cellular networks, which offer 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 authentication protocol for 4G known as EEPS-AKA is used to overcome the security problems. While 3G was revolution, 4G is evolution. The main aim of 4G technology was to enable users with high speed internet access, thus enabling several other features. Also other aim was to converge all the existing networks into one network. It's truly a technological evolution. While 3G was more of an extension to 2G, 4G is entirely new. The entire mobile network was redesigned so as to achieve always on high speed connectivity and also enable operators with various mobile networks to converge into one. 4G wireless network is a pure data connection: that is, it is an end to end internet protocol connection. This provides some real advantages but also some disadvantages. On the one hand a Smartphone simply becomes another data device whose native mode is an internet enabled terminal and that can be managed as such..On the other hand services such as voice require some additional machinations to support effectively. Since voice is not intrinsically data centric and must be converted to data before it can be transferred, voce capable LTE handsets.

III. 4G SECURITY TECHNIQUES

1) EAP-AKA (Extensible Authentication Protocol Authentication and Key Agreement Services):

The method for Universal Mobile Telecommunication System (UMTS) Authentication and Key Agreement (EAP-AKA), is an EAP mechanism for authentication and session key distribution using UMTS Subscriber Identity Module (USIM) EAP-AKA is defined in RFC 4187.It is used for non 3GPP access to a 3GPP core network For example, via wifi, EVDO or WiMax.

2) EPS-AKA (Evolved Packet System-Authentication and Key Agreement):

EPS-AKA protocol is the last version of UMTS-AKA, where the improvements added have raised the degree of security, but made the protocol more complex. The components of EPS-AKA authentication protocol are as follow :

1) UE and Universal Subscriber Identity Module (USIM).
2) Enhanced Node Base station (eNB), and Mobility Management Equipment (MME).
3) Home Subscriber Server (HSS)

3) SPEKE (Simple Password Exponential Key Exchange):

It is a cryptographic method for password authenticated key agreement. It is one of the older and well known protocols in the relatively new field of password authenticated key exchange. It was first described by David Jablon in 1996. In general SPEKE can use any prime order group that is suitable for public key cryptography, including elliptic curve cryptography. However when SPEKE is realized by using elliptic curve cryptography, the protocol is essentially changed by requiring an additional primitive that must securely map a password onto a random point on the designated elliptic curve.

4) EEPS-AKA (Efficient EPS-AKA):

This protocol is based on simple password exponential key exchange (SPEKE) protocol. This method is used to overcome the problems of methods which is described above. As compare to other methods this method is faster as it uses secret key method which is faster than certificate based.

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

S. 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	Offered the Fast authentication and key agreement	Reduces the authentication delay, signalling	Uses elliptic curve cryptography with Diffie-hellman.	Diffie-hellman is highly exposed algorithm Elliptic

	Agreement)	services.	cost. Empowers the security model.	Users the symmetric key cryptosystem.	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.

IV. CONCLUSION

The study of these models has defined the need of several requirements to be made to the one or more schemes in order to create the robust mechanism for the 4G network security. The existing methods have been found inefficient in the case of quick response, reliability factor or level of security. The existing methods of EAP-FAKA and EPS-AKA severely suffer from the several vulnerabilities. This means there is higher probability of these mechanisms being exposed to the hacking techniques. Hence these methods are not capable of being implemented over the real time 4G networks. SPEKE method has been found slower as well as offers the weaker encryption. This method does not incorporate the strong secure hold against most of the hacking attack formations. EEPS-AKA has been found slower due to the lack of data compression or optimization.

Also an authentication scheme may optimize the number of authentication packet by managing the several forms of authentication data inflow. EEPS-AKA has been also found vulnerable to the cryptanalysis attacks. This has been studied that a perfect key management mechanism must be capable of quick response authentication, higher order reliability and highly secure key data propagation between both ends. The minimum delay must be added in order to improve the existing methods. For the purpose of improvement in the existing models the in order to enhance the security of the 4G/LTE networks, the key management scheme must be improved. In the future, the novel method for the 4G security can be proposed with multi-level authentication capabilities. Also the new method is intended to be faster and efficient by using the quick response encryption and propagation mechanisms. The new authentication scheme will be made capable of offering the robust and unbreakable security for the 4G networks.

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." InPrivacy 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.