International Journal of Information Processing, 7(3), 58-67, 2013
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Elgamal Signature based Authentication in LTE-Advanced

M Prasad[a], R Manoharan[b]

[a]Research Scholar, Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry 605 007 India, Contact: prasad.psd@gmail.com

[b]Professor, Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry 605 007 India.

The advancements in cellular communication with high speed internet, network coverage and data services lead to the research in securing the data during transmission. Nowadays data processing is mostly done in Smart phones due to their improved processing capability with high speed internet connectivity. This has led to a situation where the data in cellular communication need to be secured. In cellular communication, mobile authentication is done in the initial stage in order to prevent the cloning of Subscriber Identity Module (SIM) so as to protect from the eavesdroppers. The Global System for Mobile Communications (GSM) standard uses a framework that with a key Ki and SIM for authentication. In Long Term Evolution Advanced (LTE-A), the Authentication and Key Agreement (AKA) mechanism retains the framework of GSM authentication with enhancements such as mutual authentication and key Ki between user and the serving network. In this paper we propose an authentication key agreement algorithm which integrates the International Mobile Station Equipment Identity (IMEI) along with integrity key Ki in order to provide mutual authentication. The proposed algorithm reduces the bandwidth utilization for authentication and the number of transactions required for authentication.

Keywords : AKA, Attacks, Digital Signature, GSM, Ki, LTE-A, SIM, 3GPP.

1 INTRODUCTION

The Detroit Police Department radio bureau began experimentation in 1921 with a band near 2 MHz for vehicular mobile service. On April 7, 1928 the Department started regular one way radio communication with patrol cars to communicate a central control point. It established the practicality of land mobile radio for police work and lead to it does adopt throughout the country. Channels in this frequency band soon became crowded. Figure 1 shows the evolution of mobile radio.

In 1933 the police department in Bayonne, New Jersey started regular two way communications with patrol cars [1]. The very high frequency transmitters are placed in patrol cars to enable patrolmen to communicate with headquarters and other cars instead of just receiving calls. Two way communication of police radio became standard throughout the country.

World War II proved [2] that the production of VHF radios was possible, by the end of the 1940s the development of mobile communications systems are initiated. In 1940 new frequencies allocated between 30 - 40 MHz leads to cover a major distance with police radio systems. Police radio major evolution occurred when the Connecticut State Police started operating a two way frequency modulated (FM) [3] system in Hartford is the breakthrough in mobile radio. The state wide two way radio system was developed by Daniel E. Noble of the University of Connecticut and engineers at the Fred M. Line Company greatly reduced the main problem of the amplitude modulated (AM) system. FM mobile radio became standard all over the country. Federal Communications Commission (FCC) allocates 40 MHz of spectrum in range between 30 and 500 MHz for private individuals, companies, and public agencies for mobile services. Late 1940s Bell

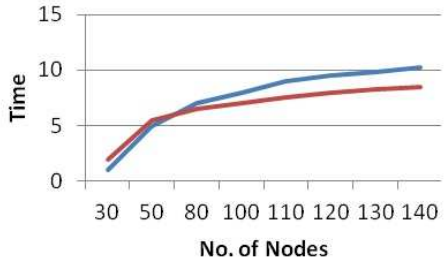

Figure 6. Comparison of AKA

being eavesdropped or modified.

Reduced Bandwidth Consumption: Using Digital Signature, the proposed protocol allows the HLR/AuC to authorize the SGSN for subsequent and mutual authentication. It reduces the traffic between HLS/AuC and the SGSN and the bandwidth consumption is greatly reduced. Bandwidth consumption between 3GPP–AKA and DS–AKA is shown in Figure 4.

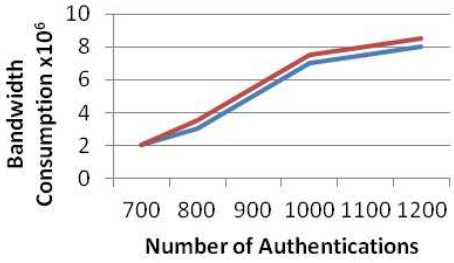

Figure 5. Bandwidth Consumption of 3GPP–AKA and DS–AKA

The proposed DS-AKA is simulated in NS3.14. The main parameter taken in this simulation is time. With respect to time and number of nodes are taken into consideration initially DS-AKA requires more time to authenticate than 3GPP AKA. By increasing the number of nodes in an eNB the DS-AKA gone steady when compared to 3GPP AKA. The graph obtained is shown in Figure 5.

The number of messages transferred for authentication between the eNB and UE is reduced and encrypted. The original key never sent upon the channel between the eNB and UE. The original key is computed in UE and send to eNB. Another key is generated and computed by the eNB and send to UE. The key exchange is based upon the Diffie Hellman Key Exchange algorithm. The original key is never exposed in the radio signals. It makes the proposed protocol more secure.

8 CONCLUSION

Security and implementation requirements for personal communication systems have been discussed. To provide better protection, new protocols with more security features, which reduce the roamers trust on a visited networks capability of protecting roamer-related sensitive data without involving complicated computations, were proposed and then analyzed in this paper.

REFERENCES

1. Advanced Mobile Phone System, *Bell System Technical Journal*, Jan 1979.
2. Bate R. Wireless Broadband Handbook, in *McGraw Hill*, 2011.
3. Bekkers R and Smits J. Mobile Telecommunications, in *Artech*, 2000.
4. Gibson J, *et al.,*. The Communications Handbook, in *CRC Press*, 1997.
5. Gralla. P. How Wireless Works, in *Que*, 2001.
6. Guizzo E. Closing in on the Perfect Code, *IEEE Spectrum*, pages 36-42, March 2004.
7. Jagoe A. Mobile Location Services: The Definitive Guide, in *Prentice Hall*, 2002.
8. Dropman, Ulrich. A Real Step Toward UMTS, *http : //w2.siemens.de/telcom/articles/e0497/497drop.htm.*
9. *http : //www.gsmworld.com/technology/3g_future.htm.*
10. D Seo and P Sweeney. Simple Authenticated Key Agreement Algorithm, *Electron. Lett*, 35(13):1073–1074, Jun 1999.
11. S I Gy. Gdor. Novel Authentication Algorithm Public Key based Cryptography in Mobile Phone Systems, *Int. J. Comput. Sci. Netw. Secur.*, 6(2B):126–134, Feb 2006.

M Prasad received the B.Tech and M.Tech Degree in Information Technology and Information Security from Pondicherry Engineering College, Pondicherry University, Pondicherry in 2008 and 2010 respectively. He is currently working towards the Ph.D degree with the Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry.

R Manoharan Professor in the Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India. He received his Masters in Technology and Ph.D from Pondicherry University in the year 1997 and 2007 respectively. His research interests include Wireless Networking, Mobile Systems, Sensor Networks and Network Security.