INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Five-Point Key Amalgamation for Secure Authentication (FPKA-SA) in 4G networks

Divyanshu Malhotra *
GZSCCET, Bathinda.
malhotradivyanshu19@gmail.com

Dr. Paramjeet Singh
GZSCCET, Bathinda.

Dr. Shaveta Rani,
GZSCCET, Bathinda.

Abstract—The 4G networks are the fourth generation cellular networks and result of the long term evolution (LTE) in the cellular networks area. The fourth generation networks are capable of transferring the user data on higher speeds, which insists the users to have video calls, transfer massive amounts of personal data, etc, which stays at risk while being exchanged between the two nodes. Also, 4G is not only limited to the Smart-phone users, but it is being used for the personal computers (Desktops, Laptops, etc.) using the Mi-Fi interfaces, which adds the high risk of data security. In this paper, a novel authentication mechanism is proposed by using the 5-column key architecture to build and transmit the stronger keys between the two cellular nodes. The proposed model has been evaluated on the basis of various network and authentication performance parameters and compared with the existing 4G authentication models. The proposed model has been found better than the existing model, hence proved to be efficient authentication scheme for 4G networks.

Keywords—4G authentication, Complex Key, Five Point Key Authentication, FPKA, authentication & authorization.

I. INTRODUCTION

Network systems development began means back in Nineteen Seventies, once the configuration of analog-voice minded initial generation networks started. The move to computerised voice and info located Second Generation (2G) frameworks in 1991 denoted the begin of a multi-administration stage from the past mono-administration amount. Low bit-rate info and mono-media frameworks like GSM, cdmaOne, IS-95 and TDMA are still existing in numerous worldwide areas. The 2.5G frameworks (like GPRS), an interval stride somewhere around 2G and 3G, if upgraded channel limit, higher information rate and throughput and advanced packet data transmission improving internet access from diverse remote gadgets. After that, marketed move to 3G framework in 2002 where more individuals-to-machine interactions than person-to-person interactions are prevalent .The main packet network systems like cdma2000 and WCDMA provide higher channel capacity, broadband info up to a pair of Mbps, high speed multimedia transmission and worldwide wandering over a phone system.

This time marked the start of full-fledged immense revenue generating transmission net applications and e-business. On the opposite hand, with the tremendous overall increment in the amount of transportable purchasers each day and with developing requests like fully consumer driven administrations, quick spilling net interactive media administrations (telemedicine, tele-geoprocessing, virtual route and VoIP), consistent worldwide meandering with universal scope and unencumbered QoS bolster, 3G frameworks have begun demonstrating their restrictions with transmission capability accessibility, vary designation, air obstruction pointers and absence of consistent transport instruments between various systems. In addition, diverse short range correspondence frameworks like WLAN, Bluetooth and HIPERLAN and additionally telecast correspondence frameworks with distinctive components crossed amid this point each with its own particular benefits and negative marks specializing in diverse varieties of clients and diverse administration sorts making the circumstance more muddled for 3G frameworks.

These restrictions and drawbacks have created the requirement for associate degree all comprehensive structure as well as all this heterogeneous wired and remote frameworks getting used. This IPv6-based potential 4G structure,

usually represented as MAGIC (Mobile interactive media, Anytime anywhere get to, international skillfulness bolster, Integrated remote arrangement and customised individual administration), would be profoundly dynamic and fundamentally handle the constraints of 3G frameworks on these lines, solid arrangements which will systematically work on the assorted, different systems moving to the 4G environment satisfying the plenty of next generation dream perceptions on executing a straightforward open wireless architecture (OWA), got to be considerably planned. This clearly welcomes new difficulties on each stride and scientists overall face a tough undertaking of planning suitable arrangements.

II. RELATED WORK

Seddigh et al. (2010) studied on 4G remote system security propels and its difficulties. They displayed associate degree investigation of security advances and difficulties connected with new 4G remote advances and created numerous commitments to the sector. To begin with, it targeting the safety benchmarks .Second, security-related standards, design and description for the LTE and WIMAX advances were analyzed. Third, security problems and vulnerabilities mentioned that came in past 4G standards. This meditated centered basically on mackintosh layer weakness for Wi-Max and LTE. Each principles have some physical layer helplessness to obstruction and scrambling techniques. Alezabi et al. (2014) planned a productive EPS-AKA (EEPS-AKA) convention to beat vulnerabilities, for instance, revelation of shopper identity, machine overhead and man-in-the centre attack (MITM) and authentication. The shopper temperament is uncovered once man-in the centre assault has sent clear content in initial association that prompts shopper character attack. In each past system, all keys were created utilizing single key that can be undraped and be a feeble purpose of convention. This planned convention was in lightweight of the essential watchword exponential key exchange (SPEKE) protocol. Damgard et al. (2013) planned a secure key management technique for cloud environments. Authors have studied the amount of security on the premise what they'll and what they cannot get within the security models. And when learning that every one, authors have planned a light-weight protocols achieving outside security, and report on their sensible performance. that they had thought of totally autonomous servers that switch between on-line and offline periods while not act with anyone from outside the cloud and semi-autonomous servers that require a restricted quite help from outside the cloud once doing the transition. Chandramouli et al. (2013) worked on cryptanalytic Key Management problems & Challenges in Cloud Services. associate degree analysis of the common state of observe of the cryptanalytic operations that give those security capabilities reveals that the management of cryptanalytic keys took on a further complexness in cloud environments compared to enterprise IT environments due to: (a) distinction in possession (between cloud shoppers and cloud Providers) and (b) management of infrastructures on that each the Key Management System (KMS) and guarded resources were set.

III. AUTHENTICATION SCHEME

3.1 EEPS- AKA Model

The existing model relies upon the evolved packet system authentication and key agreement (EPS-AKA) and has been improved because the economical EPS-AKA (also EEPS-AKA). The EEPS-AKA model has been comprised of the safety model to safeguard against the data revealing vulnerabilities and man within the middle attack. the present system is two-column based mostly key management authentication model with the elliptic curve cryptography. the present model has been created to share four messages for one spherical of authentication. It utilizes the easy secret exponential key exchange (SPEKE) model of the bottom model implementation and has been developed with sure outlined enhancements.

3.2 FPKA- SA Model

The planned model is 5 purpose Key integration for Secure Authentication. This model has been designed because the strong security design for the 4G networks. The planned model is that the authentication theme for the 4G networks exploitation the advanced key models. The planned model has been developed because the advanced key design wherever the 5 columns based mostly key model has been used for the secure authentication over the 4G networks. The planned model has been offered to guard the voice knowledge and user knowledge within the 4G environments. The key theme has been designed to be used on the point-to-point design exploitation the centralized base transceiver station (BTS) node. The 4G base station ensures its security by exploitation the authentication theme between the mobile nodes and base station. The planned model theme has been non-commissioned as following:

Algorithm: Key Scheme Algorithm Sequence for Function Calling

CASE 1: When mobile node calls out:

1. Mobile node initializes the call setup phase, and request 4G base station to complete the call.
2. The 4G base station initializes the authentication process.

CASE 2: When base station receives the call for mobile node:

1. The 4G base station receives the call for the mobile node.
2. The 4G base station requests the mobile station and verifies the ready state.
3. When mobile node replies with the ready state, 4G base station initializes the authentication process.

MAIN ALGORITHM:

1. The 4G base station infuses the multi-column keys to prepare the query key.
2. The query key is encrypted using the ECC algorithm.
3. The query key is forwarded to the mobile station.
4. The mobile station prepares the reply key by verifying the query key column data and marks the reply key rows.
5. The reply key is prepared by infusing the multiple keys information in the marked columns.
6. The reply key is encrypted using the ECC algorithm.
7. The reply key is forwarded towards the 4G base station.
8. The 4G base station verifies the query key against the reply and prepares the decision.
9. If the verification decision is successful
10. The call setup is complete and call is forwarded to the target mobile station.
11. Time counter (Tc) is initialized
12. Else
13. The call is dropped and the mobile node is informed about the authentication failure.
14. When the timer (Tc) expires, the exchange process is repeated.
15. If key verification is successful
16. The channel stays intact
17. Otherwise
18. The call is terminated

IV. **RESULT ANALYSIS**

4.1 Matlab Simulator

MATLAB, short for Matrix-Laboratory, is a scientific computing environment developed by Math Works. It is mostly used to manipulate matrices, plot functions, implement algorithms, create user interfaces etc. So, it is ideal for computations that require extensive use of arrays and graphical analysis of data.

The design of MATLAB programming language is such that a powerful program can be written in a few lines of code. It can achieve a solution to complex problems in a relatively simple set of statements, as compared to the conventional general-purpose programming languages such as C++ or Java. Due to its vast area of application, it is widely accepted in science, economics and engineering research as well as industries.

4.2 Assumptions

- Transmission delay due to traffic jam is zero.
- Channel assignment is automatic.
- Local processing delay is also assumed to be zero.
- BTS option: (Enable/ Disable)
- Cellular nodes: (Enable/ Disable)
- Number of scenarios: 5
- Number of nodes: [1 5 10 20 50]

4.3 Performance Parameters

4.3.1 Projected Resources

The projected resource is the parameter which indicates the percentage of the cellular network resources being used for the data being transmitted. The lower amount of projected resources indicates the better performance of the LTE network and vice versa. The performance of proposed model i.e. FPKA-SA has been observed on the basis of projected resources with the existing model implementation i.e. EEPS-AKA. FPKA-SA has been considered better than EEPS-AKA as it has scored lower levels of projected resources for the similar levels of attack data over the LTE networks. The detailed results can be seen below:

Scenario 1: In this scenario only one mobile node is connected to the base station.

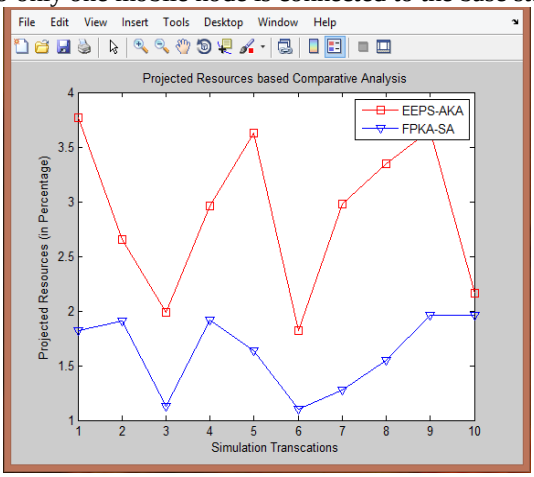

Figure 1: Projected Resources based Comparative Analysis for scenario 1

Scenario 2: In this scenario 5 mobile nodes are connected to the base station.

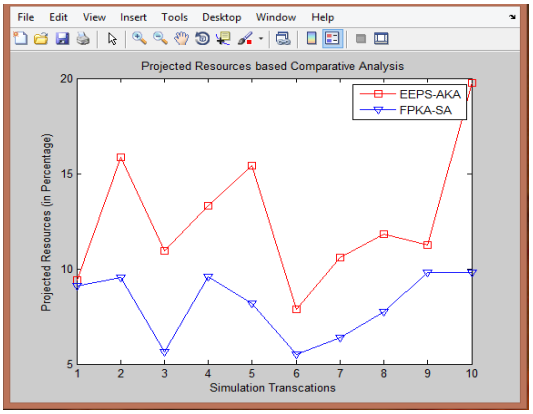

Figure 2: Projected Resources based Comparative Analysis for scenario 2

Scenario 3: In this scenario 20 mobile nodes are connected to the base station.

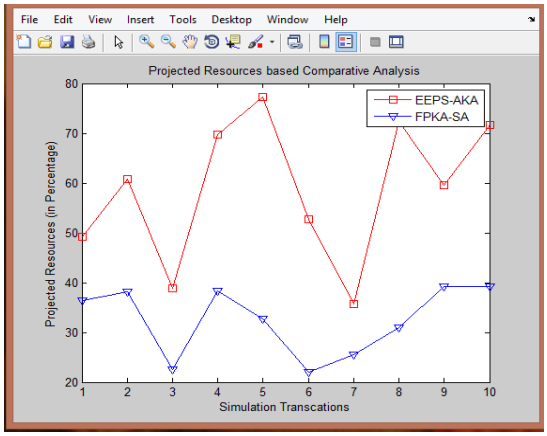

Figure 3: Projected Resources based Comparative Analysis for scenario 3

4.3.2 Entropy

The entropy gives the uniqueness of the keys being exchanged during the communication. More is the value of entropy more is the uniqueness of the keys. The higher uniqueness lowers the risk of guessing or key replication attacks on the communication channels. The entropy has been found higher in the case of the FPKA-SA than EEPS-AKA which shows the proposed model effectiveness in the case of uniqueness of the keys in the key table. The detailed results for entropy can be seen below:

Scenario 1: In this scenario only one mobile node is connected to the base station.

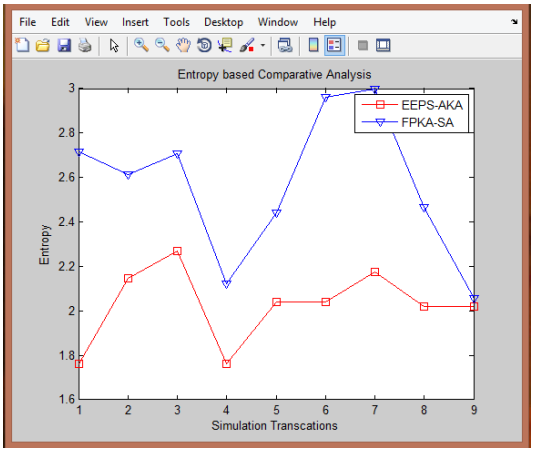

Figure 4: Entropy based Comparative Analysis for scenario 1

Scenario 2: In this scenario 5 mobile nodes are connected to the base station.

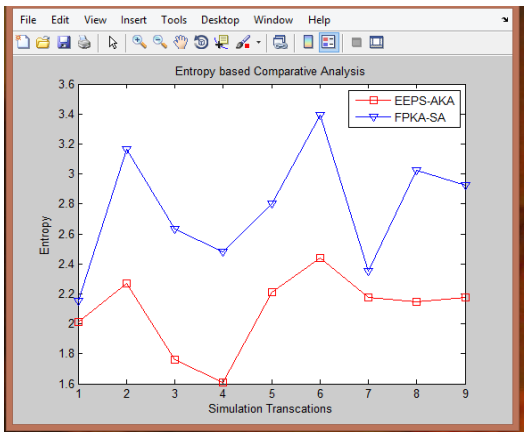

Figure 5: Entropy based Comparative Analysis for scenario 2

Scenario 3: In this scenario 20 mobile nodes are connected to the base station.

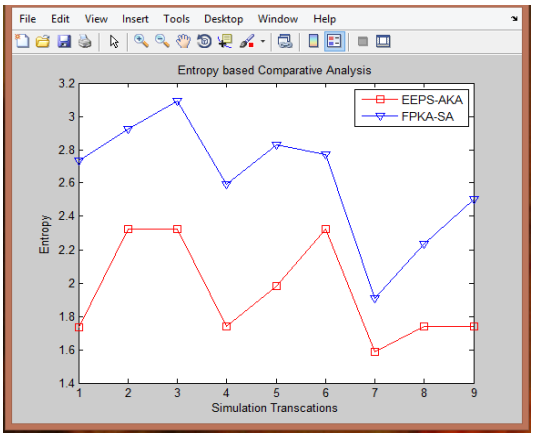

Figure 6: Entropy based Comparative Analysis for scenario 3

IV. CONCLUSIONS

FPKA-SA has been evaluated for the various performance parameters obtained from the proposed model simulation. FPKA-SA has been evaluated against EEPS-AKA which has been implemented along with the proposed model in the similar scenario and same attack situations. The result analysis has been performed over the results obtained from both the simulation of the proposed and existing model. FPKA-SA has been found better on the basis of all of the parameters evaluated under this result analysis. The proposed key management model has been found effective by more than 10 percent improvement from the existing model in all domains (or resulting parameters). The experimental results have proved the effectiveness of FPKA-SA in effectively securing the LTE communication channels under the attack situations in comparison with existing model. In the future the proposed model can be enhanced by adding the data or message level encryption method to ensure the data security. The proposed model performance can be also evaluated against the other effective key management schemes for the LTE networks.

REFERENCES

[1.] Alezabi, Ali K., Hashim F., Hashim S. J. and Ali B.M. (2014) "*An efficient authentication and key agreement protocol for 4G (LTE) networks*." In Region 10 Symposium, 2014 IEEE, pp. 502-507.

[2.] Cao, Jin, Hui Li, Maode Ma, and Fenghua Li. "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks." In *Communications (ICC), 2015 IEEE International Conference on*, pp. 7246-7251. IEEE, 2015.

[3.] Cao, Jin, Hui Li, and Maode Ma. "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks." In *Communications (ICC), 2015 IEEE International Conference on*, pp. 3020-3025. IEEE, 2015.

[4.] Cao, Jin, Maode Ma, and Hui Li. "GBAAM: group-based access authentication for MTC in LTE networks." *Security and Communication Networks* (2015).

[5.] Chandramouli R., Iorga M. and Chokhani S. (2013) "*Cryptographic Key Management Issues & Challenges in Cloud Services"*, Computer Security Division Information Technology Laboratory, NIST.

[6.] Damgard I., Jakobsen T. P., Nielsen J. B. and Pagter J. I. (2013) "*Secure Key Management in sthe Cloud"*, Cryptography and Coding Lecture Notes in Computer Science, vol. 8306, Springer, pp. 270-289.

[7.] Morshed M. M. and Islam M.R. (2013) *"CBSRP: Cluster Based Secure Routing Protocol",* IACC, vol. 3, IEEE, pp. 571-576.

[8.] Seddigh, Nabil, Nandy B., Makkar R. and Beaumont J. (2010) "*Security advances and challenges in 4G wireless networks."* In Privacy Security and Trust (PST), 2010 Eighth Annual International Conference IEEE, pp. 62-71.

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

[10.] Tiloca M.,Guglielmo D.D.,Dini G. and Anastasi G. (2013) *"SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks",* ETFA, vol. 18, IEEE, pp. 1-8.

