Indian J.Sci.Res. 17(2): 300-305, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

A HIGHLY SECURE CRYPTO – KEY MODEL (SCKM) FOR 4G/LTE NETWORKS

[1]Sahera Ambreen,[2]F Asma Begum,[3]Zubeda Begum
[1,2,3] Department of Electronics and Communication Engineering, Nawab Shah Alam Khan College of Engineering and Technology, Hyderabad.

***Abstract*:** The fourth generation cellular networks are raising trend in the present world is the fourth generation (4G) cellular network. It is the result of the evolution termed as the long term evolution (LTE), hence also known as the 4G/LTE networks. The 4G/LTE network posse's extremely high data transfer speeds to handle the heavy loads of data. The high-speed attracts hackers and crackers to the networks, who always try to find the vulnerabilities in the existing networks to exploit them. In the performance evaluation of the existing models, we have evaluated that the predictive key management scheme, which is based upon the computational engine is more prone the hitch or guessing attack and can offer the early exposure to the hacking attempts over the non-predictive non-crypto scheme. In this paper, we have proposed the non-predictive crypto-key management scheme to ensure the security of the 4G/LTE networks. The proposed model has been named as highly secure crypto – key Model (SCKM) scheme.

***Keywords*:** 4G/LTE security, authentication, pre-setup authentication, post-setup authentication, multi-level authentication, secure access

I. Introduction

Both 2G and 3G systems were basically anticipated for emphasize telephones; for voice calls and messages, as conflicting to information. The 4G LTE innovation covers a more far-reaching scope of frequencies and can possibly be up to 100 hundred times speedier than slower 2G and 3G systems, however this prolonged velocity includes some significant pitfalls - security. In any case, 4G was planned particularly to send and getting information, making it more prepared for the employment. While this makes it speedier, the systems taken to accomplish these paces additionally make it more vulnerable.

The elementary security issue with 4G systems is that client data can turn out to be fluently available to programmers. As they can put themselves either between two oblivious sufferers or between the client and the application or even between two machines. This gives the assailants full access to the information being sent over the system, and a few programmers might even control it.

A notable new jeopardy to flexible clients originates from the change to IP (Internet Protocol).Thorough multi-layer security ought to be a vital piece of any LTE to convey the level of security firm with the numerous points of interest of 4G [10].

4G versatile systems are all-IP, while 3G systems are a mix of IP and portable conventions (SS7). IP is significantly more transparent, and has been effectively battered by programmers for a long time, opening up various approaching dangers. There could be a colossal augmentation in the complexity and exhibit of spam and phishing assaults offering programmers new systems to convey, for example, through 'video spam' assaults. For instance, convenient administrators will soon be dispatching new administrations on top of 4G, including voice and video conferencing.

The LTE system embraces an all-IP, Internet based configuration, offering much higher access speed (e.g., 100– 300 Mbps). In LTE, two voice solutions are proposed appropriately: CSFB (Circuit-Switched Fallback) [10] and VoLTE (Voice over LTE) [9]. LTE transporters have been utilizing a famous answer for voice supervision, called circuit-exchanged fallback (CSFB) [1]. It transfers LTE voice calls to the legacy 3G/2G arranges and empowers CS-based voice administration. CSFB influences the sent 3G/2G framework and its CS conveyance.

II. Related Work

[1]Corresponding Author

Ivan Damgård et. Al. proposed technical administration protected key for cloud computing situations focusing on the safety levels on hypothesis and security models. Seddigh Nabil et. al. presents an assessment of safety advances and difficulties of advanced remote 4G rise treated with an overview on the 4G advanced remote security system and its difficulties Add to package association interface alongside the sender. On collector side, these novel codes will be confirmed utilizing code checking computation strategy.

This method uses random Key table of two, Alezabi, Kamal Ali,et.al proposed powerful EPS-Alias assention (EEI-AKA) to defeat these issues. The proposed Convention relies on upon the pass Exponential Key Exchange (SPEKE) straightforward tradition. [1]

Zongwei Zhou et. al. proposed "a Key administration calculation named as Key It Simple and Secure (KISS). This article presents another key modeling with extensive customer empower, reliable, clear, and key administration warned.

Ramaswamy Chandra mouli et. Al. took cryptographic key management issues and challenges in cloud services. A review of the basic condition of the routine cryptographic operations that give these security capabilities discovers that the administration of cryptographic keys multifaceted covers an additional quality in contrasting situations with large cloud computing situations of the company due to (a) individual distinction (between consumers and cloud providers) and (b) control of the foundations on which both the key management system (KMS).

N. Suganthi, V. Sumathy proposed the calculation of three kinds of keys for each sensor hub, an individual key communicated to the base station, imparted to neighboring sensor hub and a gathering of key that is shared by each of the centers in the system.

A question key, which carries an answer key $K_{A.}$ All of the keys in the table (question/answer keys) are generated using a random function which is non-track-able and non-trace- able. The new scheme will add least overhead because it will not generate key at every time. It will generate the key table on the starting phase and will share the key table with the neighbor nodes. Each node will share a key only during the first packet exchange of a packet stream between two mobile nodes. This scheme will be capable of handling both DoS and DDoS attacks.

Algorithm 1: Key generation

1. A large prime number is generated from the p and q which are classified as the large prime numbers. The minimum length acceptable for the large number generation has been set default to 512 values each and maximum of 1024 digits in both p and q.

2. Then modulus depicted n undergoes the Computation on the basis of input values of p and q.

3. Then the quotient is calculated n,Φ(n).

4. Further, The range is defined to produce the public key, where the range is denoted by [3, Φ (n))] and a common divisive value is assigned at 1 with Φ (n) and defined as the mandatory prime number value only.

5. In the next step, the private key defined on the basis of Φ (n), because of the existence of the prime number mentioned on step 4 as 1 with Φ (n) with respect to the modulus calculated as mod Φ (n).

The decryption is always done on the basis of opposite key combination used for the encryption methods.

III. Experimental Design

In this paper, we offer a genuine change in the SAD-SJ technique to make it ready to secure the particular scrambling to react to numerous hubs undertaking to join the system in conjunction say (DDoS). This convention will create different arbitrary extraordinary codes and

Algorithm 2: RSA Enc/Dec Process

1. At very first step, the plaintext is transformed into the cipher wise information using the encoding method.

The key k and data d remains the primary inputs to the RSA function, which can be written as following

$$F(m,k)=mk \bmod n \quad (9)$$

2. The RSA produces the data in the form of two cases; one is the encryption with public key and other for private key. Both the methods can be termed as the mirrored methods to each other. Both the methods can be described with the following statements:

a. If encryption uses the public key, the decryption will be done using the private key.

b. If encryption uses the private key, the decryption will be performed with the public key.

3. The encryption method can be elaborated in form of following formulas: Fn(mx,ex)=md modulus(n=cx)

Where mx defines the plaintext message, ex for the public key and cx depicts the cipher data produced after the encryption process.

4. The decryption process can be elaborated in the form of following mathematical formula:

Fn(cx,dx)=cd_modulus_n=mx.

Primary Key Gen Algorithm: The proposed model is termed as the SCKM which uses the following mathematical equation for the purpose of the key table population generation.

Algorithm 3: Generate Key algorithm

1. Provide the input to the generation function which is depicted as the seed value S

2. The seed value undergoes the sin function and the sin value is returned.

3. Value obtained from Sx is returned and saved.

4. Then the seed value undergoes the calculation of LOG and the value is returned and saved in the corresponding variable.

5. Perform the multiplication over the values obtained in the Step 2, 3 and 4.

6. Do negation if it's negative.

7. The key is converted to non decimal

8. Further, the final key value is produced by rounding the value of Main Key produced variable produced at the step 7.

Key Management Policy

Algorithm 4: Key Scheme Algorithm Sequence for Function Calling

1. The LTE base station when receives the request for a call from some other nodes, it initiates the authentication process.

2. The mobile node who receives the request replies with the connection setup request.

3. If LTE base station (LTE-BS) replies to the setup request once it is accepted and the acknowledgement code is replies.

a. Then the LTE-BS asks for the pre-shared Information with mobile stations node.

b. The MT packs the pre-shared information in the packet and return to the LTE-BS.

4. If pre-shared information is successfully verified a. The communication successfully starts

5. Else

a. The communication request is rejected

6. Once the pre-setup phase is successfully completed a. The seed value is handed over to the MT

b. The seed value exchange bit enabled Assigning the positive bit.

7. The key exchange timer t is started

8. When the timer gets expired

a. The key exchange is performed

9. If key matches successfully

a. The communication begins successfully.

10. Else

a. Communication is terminated.

Robust Crypto-Key Management Algorithm

SCKM scheme has been designed to calculate the attack threat from the authorized or unauthorized sources. SCKM scheme design has been given below:

Algorithm 5: SCKM Algorithm

1. The IDS (Ix) calculates the available bandwidth on the node.

2. The Ix scans for the active connections with the node being analyzed.

3. The Ix checks for the input data volumes D= {dv1, dv2, dv3 … dvx} coming from the different nodes.

4. The Ix decides the threshold The value by computing upon the D matrix.

5. The individual data volumes are then scanned against the threshold value Th to find the traffic abnormalities.

6. The traffic streams with abnormal traffic volumes are noticed and analyzed individually.

7. The traffic volume is calculated against the assigned individual connection bandwidth (AConBan)

8. If the traffic volume is found more than AConBan Overhead traffic filtered

9. Otherwise

1. The traffic is permitted

IV. Result Analysis

The SCKM scheme has been well tested under various situations in the sensor network simulation. The proposed energy based routing protocol on sensor network has been well tested for the performance parameters of delay, throughput, and network load.

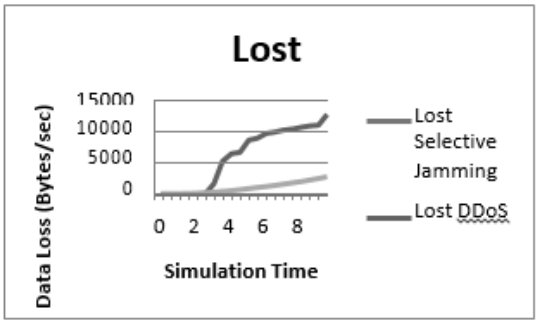

Figure 1: Data Loss comparison between all three simulations

In Figure 1 Data Loss comparison between all three simulations. The performance of SCKM scheme is found most efficient against the DDoS attack and least against the selective jamming in case of data loss. SCKM efficiency in mitigating the DDoS attack shows the effectiveness of the SCKM scheme in mitigating the most dangerous attack over any kind of networks.

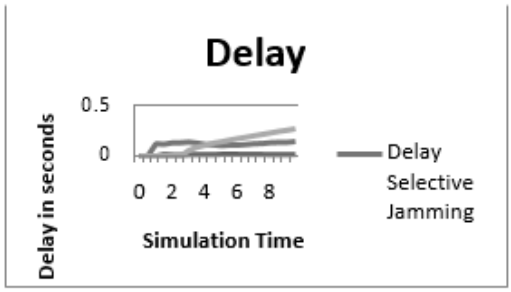

Figure 2: Delay based comparison between all three simulations

In figure 2: The SCKM scheme has been deeply evaluated on the basis of all of the attacks individually in Delay based comparison between all three simulations, above, the minimum delay has been recorded in the case of DDoS simulation, whereas the maximum delay has been recorded against the black hole attack.

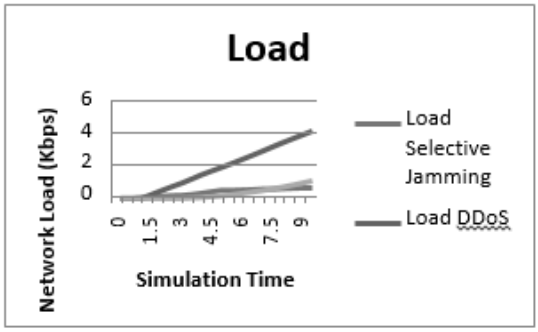

Figure 3: Load based comparison between all three simulation results

In Figure 3 Load based comparison between all three simulations. The SCKM scheme has been found the most efficient against the selective jamming and black hole attacks.

In Figure 4 PDR based comparisons between all three simulations, the performance evaluation has been done on the basis of the packet delivery ratio. The SCKM scheme has been found efficient for the DDoS attack against the black hole or selective jamming.

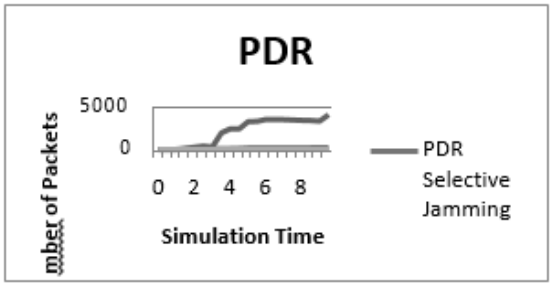

Figure 4: PDR based comparison between all three simulations

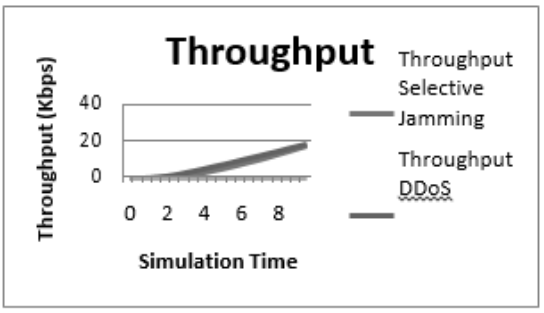

Figure 5: Throughput based comparison between all three simulations

In Figure 5 above, again the throughput has been recorded higher than the other two due to the similar reasons as per figure 5 (packet delivery ratio).

Comparison With Existing Models

Black hole Comparison: Defense against black hole attack in the sensor network under SCKM scheme has been tested and compared with the existing black hole detection and prevention model. SCKM comparison has been listed as below:

Table 1: The comparative analysis of SCKM against existing model for black hole attack

	Norm al Flow	Under black hole attack existing	Under black hole attack proposed
End-to- End Delay (ms)	31.22	35.25	19.09
Through put (bps)	70099.91	65072.06	143440

SCKM has been found efficient. The comparative analysis proves the efficiency of SCKM scheme for detection and prevention of the black hole attack.

V. Conclusion

SCKM scheme developed as the intrusion detection system (IDS) and intrusion prevention system (IPS) for the wireless sensor networks. Designed in the multi-layered model with inter- nodal relationship competence. In SCKM every node or every host is handling the intrusion detection and prevention on itself, which can be also categorized in the self-adaptive mechanism to filter out the attacker nodes from the network in the initial phase. SCKM scheme is based upon the multi-hop authentication scheme, where the intermediate hops remains invisible between the two nodes, while the authentication process is going on between two non-neighbor nodes.

SCKM scheme is offering the crypto key based authentication using the dynamic key generation policy. The RSA encryption, which is public-key cryptosystem, and based upon the public and private keys, where the data is encrypted using the public key and decrypted using the private key and vice-versa. The RSA cryptosystem is named after the inventors Ron Rinvest, Adi Shamir and Leonard Adleman.

SCKM scheme has been designed to analyze the anomalies in the traffic to avoid the attack on the sensor networks. To detect and mitigate the blackhole, selective jamming and distributed denial of service (DDoS) attacks on the sensor networks in order to run the error-free service.

VI. Future Work

In future, more innovative methods can be used for enhanced authentication and high level traffic analysis and attack pattern detection models. SCKM scheme can be improved using the intelligent algorithm based upon the swarm intelligent computing. The particle swarm optimization, grey wolf optimizer, mobile ant colony optimization, etc. can be used for the intelligent improvement in SCKM scheme for the swarm intelligent addition

References

[1] Alezabi, Kamal Ali, et al. "An efficient authentication and key agreement protocol for 4G (LTE) networks." Region 10 Symposium, 2014 IEEE. IEEE, 2014.

[2] Bikos, Anastasios N., and Nicolas Sklavos. "LTE/SAE security issues on 4G wireless networks." Security & Privacy, IEEE 11.2 (2013): 55-62.

[3] Chandramouli, Ramaswamy, Michaela Iorga,and Santosh Chokhani. Cryptographic Key Management Issues and Challenges in Cloud Services. Springer New York, 2014.

[4] Damgård, Ivan, et al. "Sescure key management in the cloud." Cryptography and Coding. Springer Berlin Heidelberg, 2013. 270-289.

[5] Ma Ma, Maode. "Security Investigation in 4G LTE Wireless Networks." School of Elecrical

andElectronicbEngineering,NanyangTechnologica l University,Singapore (2012).

[6] N. Suganthi, N., and Sumathy Vembu. "Energy Efficient Key Management Scheme forWireless Sensor Networks." International Journal of Computers Communications & Control 9.1 (2014): 71-78.

[7] GPP. TS23.272: CSFB in EPS, 2012.

[8] Seddigh, Nabil,et al. “Security advances and challenges in 4GWireless networks.” Privacy security and Trust (PST),2010 Eight Annual International Conference on IEEE, 2010.

[9] Zhou, Zongwei, et al. KISS: “Key it Simple and Secure” Corporate Key Management, Trust and Trustworthy Computing. Springer Berlin Heidelberg, 2013. 1-18

[10] VoiceoverLTE.http://www.gsma.com/ technicalprojects/volte