International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V68I11P112

Volume 68 Issue 11, 79-82, November 2020

Original Article

A Study on QoS and Security techniques of 4G Wireless Network

Amrutha K S[1], Gripsy Paul[2]

[1,2] *Department of CSE, Adi Shankara Institute of Engineering and Technology, Kalady.*

Received Date: 14 October 2020
Revised Date: 22 November 2020
Accepted Date: 24 November 2020

Abstract **-** *Nowadays, mobile networks have become an essential part of our day-to-day life. Secure communication networks with desired QoS and high reliability must be assured while sharing information. Hence, scheming 4G networks that provide a secure service by managing constraints is a difficult task. This paper discusses a cognitive framework for increasing security and QoS, a privacy-preserving handover mechanism, Group Based Secure Authentication, and Key Agreement that decreases the authentication delay and prevention from malware attacks. Enhanced encryption method with AES algorithm for securing data transmission, distributed security architecture using The Elliptic Curve Diffie–Hellman (ECDH) protocol for authenticating the mobile nodes, a Secured Vertical Hand-off Decision (Sec-DVHD) scheme using Public Key Infrastructure (PKI) algorithm that ensures high throughput and a Secure Mesh Mode Protocol to enhance the security of 4G Networks*.

Keywords **-** *QoS, cognitive framework, Handover, ECDH, Sec-DVHD*

I. INTRODUCTION

4G refers to the fourth generation of cellular communications, that offers speed about ten times faster than 3G networks[15]. Due to high-speed, it is easier to use in smartphones, similar to PCs. 4G network infrastructure uses IP as a common protocol to guarantee that every user will utilize every application and environment[12]. The major characteristics of 4G services include application adaptability and high dynamism, which implies that different services can be delivered and available to users and support the user traffic, air interfaces, quality of service, and radio environment [16]. The advantages of 4G networks are listed below:

- Improvement in Technology Performance: Provides higher throughput with fewer network capabilities and latency
- Enablement of New Mobile Application: Creating a new mobile application by enhancing existing ones
- Differentiated Customer Experience: It manages the user expectation and experience with required features and services.
- Business Model Evolution: 4G wireless technology will be the key to facilitating the alternative partnership and monetization models.

Terminal mobility should be incorporated in the 4G network structure for using wireless services anywhere and anytime. This allows users to move across the geographical boundaries of wireless networks. Terminal mobility should consider location management and hand-off management. Location management should handle all the information regarding the roaming terminals, authentication information, and QoS capabilities. Whereas hands-off management maintains ongoing communications when the terminal traverses. This hand-off method results in an increase in system load, high handover latency, and packet losses. 4G wireless environments have a problem in integrating this IP and non-IP based system.

QoS guarantees for end-to-end services need to be addressed, which is not easy to tackle when time-sensitive or multimedia applications are considered[13]. There should be security measures in 4G networks that ensure data transmission to be as safe as possible because of the nature of the 4G network have an increased chance of security attacks[11] and hence increased requirements for authentication is necessary to protect data while transmitted across the network[8].

This paper discusses the various techniques to ensure high QoS and security in the 4G networks. A cognitive framework for increasing QoS and security, a privacy-preserving handover mechanism, Group Based Secure Authentication, and Key Agreement that decreases the authentication delay and prevention from malware attacks, and enhanced encryption method with AES algorithm for data transmission, distributed security architecture with Elliptic Curve Diffie–Hellman (ECDH) protocol for authenticating the mobile nodes, a Secured Vertical Hand-off Decision (Sec-DVHD) scheme using the PKI algorithm that

ensures high throughput and a Secure Mesh Mode Protocol to enhance the security of 4G Networks.

II. BACKGROUND STUDY

A. Swarm intelligence-based security system

This paper [1] discusses a cognitive framework with a swarm intelligence that ensures interoperability, scalability, and security against Denial of Service attacks in 4G networks. An optimal setting based on a cost function provides high QoS and security when the swarm agent communicates to BS and gathers information about the mobile user's neighbors. Optimal setting utilizes the threshold of performance parameters, and successful call placements with high packet delivery rate and delay are done. The current resource availability of mobile equipment is detected whenever a call is placed. The swarm agents are spread randomly across the network. Swarm agents communicate with each other using pheromones, and the optimized path is regarded as QoS and resources. Based on the performance of the agent, the pheromone deposition is calculated. The movement of swarm agents between mobile equipment and base stations is based on the performance parameter And pheromone deposition in the transition probability.

Swarm agents maintain a tabu-list that includes the route taken by the agents and the specific cost expended. The updated tabu-list is shared among the agents, which helps agents attain time-efficient and globally optimized solutions. The trails formed by the ant agent are dependent on parameters obtained by a combination of both the physical and the MAC layers, thus effectively avoiding DoS on these layers [1].

B. Privacy-preserving Handover Mechanism

A handover technique in 4G network that ensures users' privacy has been discussed in this paper [2]. This technique is performed by changing the temporary identity (ID) of user equipment (UE) as well as the key that the UE uses in each access point to hide the real user's ID [2]. A globally unique temporary ID hides the main user ID. Authentication is performed by the Mobility Management Entity (MME) by constructing the first key to have a secure channel between UE and MME. For connection to first Enhanced ModeB(eNB), UE and MME calculate the key to the next layer that ensures secure communication between UE and eNB. Both UE and eNB use another key, $K_{eNB,}$ to calculate three keys for encryption and ensure integrity in the shared channel. The source eNB calculates the K*eNB and sends it to target eNB to secure UE communication and target eNB. The key derivation is as follows,

$$NH_0 = K^0_{eNB} = KDF\ (K_{ASME}, C_{NAS}) \quad (1)$$

$$NH_1 = KDF\ (K_{ASME}, K^0_{eNB}) \quad (2)$$

$$NH_{NCC+1} = KDF\ (K_{ASME}, NH_{NCC}) \quad (3)$$

$$K^*_{eNB} = KDF\ (NH_{NCC}, PCI, P_{freq}) \quad (4)$$

KDF (key derivation function) is a one-way function. CNAS is a counter value set at the Non-access stratum (NAS), PCI identifies the eNB physical cell identity P_{freq} represents the cell's frequency parameters. Next, Hop (NH) and NH Chaining Counter (NCC) values are proposed in 4G for privacy preservation of the user [2].

C. Group-Based Secure Authentication and Key Agreement

The method proposed in this paper [3] is a group-based secure authentication and key agreement (GBS-AKA) scheme that decreases the authentication delay and prevention from malware attacks. GBS-AKA authenticates multiple machine type communication devices (MTCDs) efficiently [3]. GBS-AKA scheme consists of three phases: prepare phase, GBS-AKA-I phase, and GBS-AKA-II phase. A group header distributes the information in the preparation phase. Group members are based on the group principles and methods, and each group is assigned with a group key and identity by the operator. In the GBS-AKA-I phase, the group header performs the authentication and agreement procedure fully. Based on the communication capability, storage status, and battery status of each MTCDs, a group header will be chosen. Finally, in the GBS-AKA-II phase, group members and group header execute authentication with each other.

A unique session secret key is established between HSS and each MTCD. As each MTCD generates random numbers, the authentication procedure is unique, and hence attackers cannot fake the messages by reusing them. Thus, our scheme can defeat the replay attack. To overcome the Man in the Middle Attack, each MTCD computes secret keys such that the attacker cannot require the session keys, even if they can inject each authentication message embedded with a timestamp through the communication channels.

D. Securing Data Transmission

This paper [4] deals with an enhanced encryption method with the AES algorithm by modifying the S-box. For key exchange, RSA and authentication SHA-256 has been used. BPSK modulator modulates data signal, and BPSK demodulator demodulates the signal.

A traditional AES algorithm is used for both encryption and decryption with around function. For 256 bits key, the first part of 128 bits is fed to the round structure, and the second part is given to the AES algorithm. The shift value of the S-box is obtained by XORing the hexadecimal digits of the AES key. Once shift value is obtained, the S-box is rotated by that value, and by using a cipher key static S box is converted into dynamic. To get correct inverse values, the inverse S-box is also modified. AES's round function has the input data split into 128 bits blocks where one block is given as input to the AES section and another block as input to the AES section as per round structure in the next round. This is done for all ten rounds, respectively. The encrypted data of the 256-bit block is formed by combining the outputs. As

AES is applied n times to the block of data in the round structure, it gives a total n different dynamic S-boxes. The dynamic S - the box is applied to the Round structure of AES [4]. Encryption time taken for the same amount of data in one round of AES will be lesser than AES. Using two rounds of Round structure, we can get more complex data with the same encryption time.

E. Distributed Security Architecture

In this paper [5], a distributed security architecture with Elliptic Curve Diffie–Hellman (ECDH) protocol is used for authenticating the mobile nodes within the network through hop by hop authentication utilizing the public key and neighbor authentication. If any new station is connected with the network, the BS will inform the existing stations. A self-certified public-key based AKA should be used for initial authentication. For hop by hop authentication, the resulting public key is used in ECDH.

The public key is generated as follows: Mobile Node (MN) encrypts the data content of MN, ID of BS, and MN with the public key of Base Station (BS) and sends it to BS. On receiving this, BS decrypts the data content of MN and validates the ID of MN. Then BS encrypts the ID of BS and MN and time stamp using the public key of home equipment and sends it to MN requesting MN's public key. MN's home equipment decrypts responses from BS and checks its validity. When the response is verified to be valid, the MN generates its public key, and it is encrypted by HE and sent to BS. Once the response is valid, MN generates its public key, encrypts it using the home equipment public key, and sends it to BS. This Public Key is then used in the hop by hop authentication and neighbor authentication.

For initial authentication, BS and MN create a secure tunnel validated by User Equipment (UE) and then authenticates it by using the key set used in the network. It will be considered as a valid member of the network if MN gets authenticated. In the neighbor authentication scheme, BS broadcasts MN information to all members as soon as MN enters the network. If the new MN finds any MN, it will check if the MN is trustworthy by verifying MN's ID. The new MN will send its public key if the ID is valid. The neighbor nodes get authenticated when both MN create uplink and downlink digital signatures and exchange it. Data security is ensured as MN and BS are involved in data transmission after this authentication.

F. Secured Vertical Hand-off Decision Scheme

A Secured Vertical Hand-off Decision (Sec-DVHD) scheme is discussed in this paper [6]. This scheme uses a PKI algorithm that shows a good performance in a hand-off blocking rate and throughput. Based on the number or the length of the exchanged messages between entities, the hand-off delay between the mobile node (MN) and the Point of Attachment (PoA) is defined.

In Distributed Vertical Hand-off Decision (DVHD), a Simple Additive Weighting (SAW) method is used such that the computing processing is done in the neighbor networks instead of on MN. When the hand-off process is initiated, the mobile terminal sends hand-off request messages with the ID of MN and profile preferences to all available networks that MN may connect. The hand-off decision metric called Network Quantity Value (NQV) is calculated by the networks connected to MN using the weight and decision matrices based on the SAW method, which is then sent to MN. MN chooses the highest NQV and then reconnects the wireless network [6].

In Secured-Distributed Vertical Hand-off Decision (SEC-DVHD), when MN initiates the hand-off process, it sends Mobile Node Identity (MNID) to each Target Network (TN). Based on this, MN requirements are obtained from the User Profile table, then the SAW decision method is applied on the offered, and required parameters finally encrypt the NQV using the PoA's private key. TN sends the encrypted NQV to the MN decrypts the received messages using the corresponding PoA's PuK. MN picks up the highest NQV value and redirects its connection to the chosen networks after creating a list of PoAs' NQVs by eliminating the NQVs coming from malicious PoA.

G. Secure Mesh Mode Protocol

This paper [7] proposes a protocol to enhance security in Mesh mode to secure initial network entry and achieve privacy between two different network nodes. Advanced Encryption Standard and Biometric Digital Key (AES-BDK) focuses on securing network messages and key distribution where AES is used for the encryption process. BDK generates the shared key. For this, a centralized Mesh network model is used, which consists of Subscriber Station (SS), Service Provider (SP), and Trusted Third Party (TTP), and assumes that the channel between SP and TTP is secured. To be registered in the TTP, the SS user captures its biometric template. TTP saves the biometric template of each SS and is secured.

For generating a cryptographic key, the fingerprint is used as a biometric feature that extracts minutiae, which are used to generate a cryptographic key, Biometric Digital Key (BDK). Then SS generates the initial BDK. This protocol has a modified AES using BDK to achieve a user authentication key exchange scheme. Firstly, SS search for SP's messages, then SS (candidate node) creates a physical neighbor list. The newly joined SS sends a new control message, Secure Channel Request (SCH-Req), which is encrypted by the initial BDK and then sent to the SP. TTP gets the encrypted message via SP, then searches the SS biometric template in the database to generate SS initial BDK. TTP then passes SS initial BDK with date and time to SP via BS. SS sends encrypted MSH-NENT: NetEntryRequest message to SP. Once TTP receives an encrypted message, it verifies the user by comparing its biometric template within the database, and the same process is done as in the first steps.

III. RESULT AND DISCUSSION

The main goals of 4G networks were to enhance quality, provide effective security measures, and ensure that all user's requirements are satisfied without any delays[14]. important to provide seamless service with high QoS. Hence, the 4G network security is of main concern.

Using the technique of cognitive intelligence [1] ensures security and QoS without using any complex methods. This approach is considered an easy way to solve DoS attacks that increase the system's response time and power. DoS is captured with a 96% detection rate with error correction, power control, handover, QoS, and traffic prioritization. In the second technique, the mechanism providing privacy for handovers [2] in 4G networks ensures security and efficiency. It preserves the user's privacy, based on two models of adversaries such as internal and external. It can be used for handover from MME to MME, MME to GW, eNB to eNB/DeNB, and DeNB to eNB/DeNB. The third technique of GBS-AKA [3] reduces the higher bandwidth required during authentication. This scheme can efficiently optimize the system and lessen resource overhead when many devices simultaneously visit the core network. It ensures mutual authentication security between-group header and group member.

For the fourth technique using the AES algorithm, no extra CPU and memory is required for the given algorithm and satisfies the avalanche effect criteria. When the algorithm complexity increases, it makes the system attack resistant and secure data from attackers. The max data rate achieved by the system is 2.2 Mbps [4]. In the fifth technique, a protocol is used by creating public and private keys that create a secure tunnel between the MN and BS [5]. Hop by hop authentication is performed in the network such that it is validated as either trustworthy or not. The sixth technique of Sec-DVHD reduces the processing delay at the MN side. Sec-DVHD [6] avoids the man-in-the-middle attack and shows a good performance in terms of hand-off blocking rate and throughput. The seventh technique uses the secure Mesh Mode Protocol[7]. It avoids malicious sponsor nodes and achieves privacy between two nodes in the Mesh network.

IV. CONCLUSION

Mobile phones and their services are an integral part of our life, especially for performing high-security tasks such as using a payment method or storing private information. Security and efficiency are mandatory to reduce eavesdropping attacks and increased performance in heterogeneous 4G networks. The utilization of swarm intelligence makes it easier to solve DoS attacks and high QoS in 4G networks. GBS-AKA performs a secure and efficient authentication scheme, whereas the AES algorithm As wireless networks, the chances of different attacks are more such as replay attacks[9], a man in the middle attacks, and other phishing attacks[10]. Along with the countermeasures for these attacks and threats, it's also provides secure data transmission in 4G networks. Secured Vertical Hand-off Decision ensures a secure hand-off in a cellular network without hindrance and delays.

In contrast, Secure Mesh Mode Protocol achieves privacy between two nodes in the Mesh network. Future research must enhance security in 4G networks for file transfer, video streaming, and video conferencing. 5G technology will be introduced soon, and so research will be required regarding its security enhancements.

REFERENCES

[1] Rajani Muraleedharan and Lisa Ann Osadciw, Increasing QoS and Security in 4G Networks Using Cognitive Intelligence, Syracuse University, IEEE (2007).

[2] Hasen Nicanfar, Javad Hajipour, Farshid Agharebparast, Peyman TalebiFard, Victor C.M. Leung-Privacy-Preserving Handover Mechanism in 4G: 2013 IEEE Conference on Communication and Network Security.

[3] Jiming Yao, Tao Wang, Mingkai Chen, Lei Wang, Gejuan Chen-GBS-AKA: Group-based Secure Authentication and Key Agreement for M2M in 4G Network: International Conference on Cloud Computing Research and Innovations (2016).

[4] Vikas Kaul, Dr. V. A. Bharadi, P. Choudhari, Dhvani Shah, Dr. S. K. Narayankhedka- Security Enhancement for Data Transmission in 3G/4G Networks: International Conference on Computing Communication Control and Automation (2015).

[5] D.Niranjani, M. Ganaga Durga. Distributed Security Architecture for Authentication in 4G Networks: IEEE International Conference on Advances in Computer Applications (2016).

[6] Rami Tawil, Jacques Demarjie, Guy Pujolle. Secured Vertical Handoff Decision Scheme for the Fourth Generation (4G) Wireless Networks, Marie Curie University, Paris, France, IEEE (2008).

[7] Salwa Elramly, Saeed Ashry, Abdulatief Elkouny, Ahmed Elsherbini, and Hesham Elbadawy- SMSHM: Secure Mesh Mode Protocol To Enhance Security of 4G Networks, IEEE (2013).

[8] Gines Escudero-Andreu, Raphael C.-W. Phan and David J. Parish-Analysis and Design of Security for Next Generation 4G Cellular Networks, Loughborough University, PG Net (2012).

[9] Kaushal P. Makhecha, Kalpesh H. Wandra-4g Wireless Networks: Opportunities and Challenges, Saurashtra University. (2008).

[10] Yongsuk Park, Taejoon Park- A Survey of Security Threats on 4G Networks, Workshop on Security and Privacy in 4G Networks

[11] Hakima Chaouchi, Maryline Laurent-Maknavicius- Wireless and Mobile Network Security Security Basics, Security in On-the-shelf and Emerging Technologies.

[12] Payaswini P, Manjaiah D.H, Challenges and issues in 4G – Networks Mobility Management, International Journal of Computer Trends and Technology 4(5) (2013) 1247-1250.

[13] Ashish Kumar, Ankit Aswal, Lalit Singh- 4G Wireless Technology: A Brief Review.

[14] What is 4G? Everything about 4G Explained.[Online] Available: https://www.broadbandcompared.co.uk/guides/what-is-4g-everythingabout-4g-explained.

[15] How 4G Works [Online] Available: https://electronics.howstuffworks.com/4g.htm

[16] 4G. [Online] Available: https://en.wikipedia.org/wiki/4G