A SAMA SCHEME FOR IMPROVING QOS IN 4G MULTIHOPS WIRELESS NETWORKS

Vinoth V. and C. Monica Manoreya
Department of Information Technology, Sathyabama University, Chennai, India
E-Mail: vinothcand2000@gmail.com

ABSTRACT

There exists several `attributes for a data, and among them confidentiality and security is gained by the entity which is termed as Authentication. The defined entity exhibits the involvement of another entity called as identification involving two or more parties, which in turn confirms an identity. Worldwide interoperability for Microwave Access (WiMAX) and Long-Term Evolution (LTE) has been the alluring Fourth Generation (4G) wireless technology in the networking between vehicles providing explicit quality of service (QoS) and security architecture. In spite of its advantage it has some security threats such as denial of service (DOS), node capture attack, etc., which mainly occurs in Multihop wireless networks. It could be alleviated by secured and prompt authentication methods. In the VANET communication, especially in Multihop networks the forwarder node authentication is more important. So, we need to provide authentication for each and every hops. Hop by Hop message authentication is required to provide high level security in VANET. Simultaneously, the address of the data origin known by the attacker leads to node capture attack. So, to avoid this, we have to consider the source anonymity also. To provide Hop by hop authentication and the source anonymity, we are going to use the SAMA on Elliptic Curve Cryptography in VANET.

Keywords: multihop network, worldwide interoperability for microwave access (WiMAX), quality of service (QoS), vehicular Ad Hoc networks (VANET).

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) has shown the distinct importance in the thriving fields in wireless devices used in vehicles. Due to its predominance, it's been applied on Vehicle-to-Vehicle (V2V) and Vehicle to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) [2]. VANETs are application oriented for safety and non-safety range, like enhanced navigation with location-based services, management of vehicular safety, infotainment applications providing access to network communication. Here the road trip is secured by establishing connection between vehicles to vehicle or road side access points. This ensures better convenient mode of travel since the range of communication in the Adhoc network is made shorter by the use of IEEE 802.11p.

But basically for enhanced safety application higher bandwidth and robust authentication is needed in order to support multimedia services in vehicular use. To overcome the issues of wide bandwidth and security, usage of cellular and satellite networks are advised. When comparing cellular and satellite networks, satellite networks are more expensive, but provide lower quality-of-service (QoS) performance (higher delay and lower maximum throughput). On the contrary, the telecommunication industry landscape for cellular networks has shown rapid growth. In 4G networks, Worldwide interoperable for Long-Term Evolution (LTE) and Microwave Access (WiMAX) are two emerging broadband wireless technologies aimed at to providing high-speed Internet of 100 Mb/s at a speed of 340 km/h. Further, 4G wireless standards provide well defined QoS and security architecture. So we have to use, 4G cellular networks are considered up-and-coming technologies for vehicular multimedia applications.

The security aspect, the WiMAX authentication uses Extensive Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS) or EAP Transport Layer Security (EAP-TLS), which allows enterprise customers to use X-509 certificates that contain enterprise-controlled password. On the other hand, the LTE authentication process uses the EAP Authentication and Key Agreement (EAP-AKA) procedure that authenticates only the International Mobile Subscriber Identity (IMSI) burned in a subscriber identity module (SIM) card. Consequently, the LTE security does not meet the enterprise security requirement, as LTE does not authenticate enterprise controlled security.

Although the authentication process is different between WiMAX and LTE, both have well-defined security architecture. In addition, the security key hierarchy is similar in both networks, and they both adopt symmetric key encryption. WiMAX uses either Advanced Encryption Standard (AES) or 3-Digital Encryption Standard (3DES), and LTE uses either AES or SNOW 3G. Nevertheless, there exists a certain hazard like denial of service (DOS), due to the presence of crook node in the 4G networks.

Further, the recent WiMAX and LTE standards have introduced relay nodes in a multihop network to increase network coverage and capacity. However, multi-hop networks also augment the security threats and prolong the transmission delay between the user and the destination. Therefore, the first objective of this research work is to analyze the security architecture in 4G multihop networks and provide QoS aware solutions for the existing security threats.

The main security threats mainly arise in the physical and medium access control (MAC) layers, where the intruders alters the radio frequency in the physical layer as threat. Where as in the MAC layer the intruder's spoofs, or even alters the control messages. In one of the worst case scenarios the attackers take control of the networks by knowing the confidential details in control messages. The usage of internet protocol securities (IPSec) can be opted but it mitigates the Qos performance as IPSec headers exhaust the bandwidth. In order to lower the security threats and performance deterioration, Source Anonymous message authentication (SAMA) is proposed along with the Elliptical curve cryptography. The results showed that it did not affect the QoS performance and provide much security in 4G single-hop WiMAX networks.

2. RELATED WORK

Efficient authentication over lossy channel paper proposed TESLA and EMSS scheme [1] to provide sender high scalability, authentication, minimal overhead, strong loss robustness and cost of slightly delayed verification. Attacking a cryptographic proposal in order to attain surveillance in sensor networks that provides increased resilience threshold while maintaining performance.

R.L. Rivest, A. Shamir, and L. Adleman [2] introduce a blueprint for Digital Signature and Public Key Cryptosystems. Here the encrypted message is represented by K raised by defining power e, followed by the remainder of divided result l, obtained as a product of two numbers that happened to be prime; in our case we have q and p. A ring signature is used here which enables us to specify possible signatures without actually revealing the composed signature.

The signature scheme introduced by David Pointcheval and Jacques Stern they [3] provide signature schemes when obtained value along with the hashed coefficients with message is compared with the key for better security. Thereby in this method one main advantage is that it increases the message complexity, security and memory usage. The main disadvantage is complex computation and exhaustion of memory units.

Ashwini M. Rathod and Archana C. [4] introduces A Secure Network Discovery Message Authentication in Wireless Sensor Network in this paper permits the transmission of messages over any number of nodes without affecting the threshold issues. But still messages are not transmitted in a secured way which is one major drawback.

Tao Han, Ning Zhang, Kaiming Liu *et al*. [5] examines the security of WiMAX and man-in-the-middle attacks in Wireless Metropolitan Area Network using Secure Initial Nenvork Entry Protocol (SINEP) based on DiffieHellman (DB) key to improve the quality of security, still there exist some issues while securing.

Hyeran Mun, Kyusuk Han and Kwangjo Kim[6] introduces Elliptic Curve Diffie Hellman (ECDH) with symmetric key cryptosystem, EAP-AKA based key authentication which reduces the threats of IMSI, SQN synchronization, additional bandwidth consumption, and man-in-the middle attack. It also provide mutual authentication between AAA server and UE for computational overhead.

Z. Shi, Z. Ji, Z. Gao, and L. Huang [7] introduces and explains how EAP-Archie is used here for ciphering and approving. Even though it overcomes the security defects in widespread enactment still it doesn't completely solve the defect from happening.

L. Huang, Y. Huang, and Z. Gao[8] deals with the EAP-TLS which permits the users to access the network in a secured way and demonstrates using test beds. However it does not test the performance of the protocol thoroughly.

J. Hong Kok Han, M. Yusoff Alias, and M. Goi Bok [9] depicts the Denial - of- Service(DOS) attack on WiMAX networks of the mobile and how this attack causes issues but it doesn't overcome the comprehensive secured service stages of the WiMAX network.

L. Maccari, M. Paoli, and R. Fantacci [10] this paper accords with the two main features, dynamic resources and mesh mode theory which admits the attack .The main drawback is that in wireless metropolitan area networks the allocation of resources is not fully done for all the networks which hinders the communication.

A. Authentication backing in Multihop WiMAX standards

The WiMAX standards almost equivalent to IEEE 802.16 p architect. It has an added feature.

- The distributed authentication mode is said to have lesser burden of BS as well as delay when compared to the centralized mode. The user can either opt for centralized or distributed authentication mode.

Similarly, the security architecture in the IEEE 802.16m has been altered in order to adapt to the advanced air interface network. The alterations are:

- The authentication supports only EAP - based.
- SAS has been always stable.
- TEKs are obtained at the MS and not at the BS
- Here key renewal system is implemented.

B. Security backing in Multihop LTE standards

In Multihop operations RN are added with extra features to eNB for backup. It has got the following features:

- The RN is made more secure by using the removable Universal Integrated Circuit Card (UICC)
- Switching encryption occurs only at AS level.
- USIM-INI is used for initial IP connectivity in an unsecured channel and USIM-RN communicates only via a secure channel.

C. Authentication hazard in LTE networks

There have been continuous researches on the WiMAX security of LTE networks. The concept is stated by Cao *et al*. The major categories are vulnerabilities in 1) access network; 2) IMS domain; 3) HeNB; and 4) MTC domain. However, due to the page limit, we only focused on the access network.

D. DoS attack during initial attachment

Initial stage attack in the UE is very critical in Dos. Here the UE cannot log into the home network. This is similar to the Dos attack in WiMAX networks during initial network entry. Here for a particular time limit the UE requests for access to eNB, and halts for the acknowledgement to be obtained. The acknowledgement by the eNB to UE consists of required bandwidth and interval regulation along with the preamble ID. When this ID fails to match with communicated random preamble the request is ignored and count exceeds the limit there by making the UE contradictive with home network which leads to DoS attack.

The CBTC system framework is composed five major parts, which is shown in Figure-3. The automatic Train subsystem is used to calculate travel time between two trains. The ATO subsystem used to calculate the distance and velocity value for the train. In CBTC framework duplex communication between station connector and train, this is shown in Figure-1. The location and velocity of the train are captured by the Zonal controller. Based on the location and speed the zone controller emits the movement authority signal to each system in the train. The automatic protection system derives the protection point.

3. PROPOSED METHODOLOGY

This proposed session deals with explicitly secured and potent source anonymous message authentication scheme (SAMA). The authentication of SAMA is done by unitary comparison rather than individually attesting of signatures. In general there exists an ambiguity set (AS) where the sender's secured message is not related to the fellow senders, thereby making it non-linkable to sender specific.

A. Interpretation

The blueprint of SAMA consists of:

Step 1: Provoke (m,Q_1,Q_2,….,Q_n): m is an given message and Q_1,Q_2,….,Q_n are public keys of AS S={A_1, A_2,….,A_n}, consider A_(t),to be the message sender, ranging between 1≤t≤n, using d_t as the private key it produces an unsigned message S(m).

Step 2: S(m) Verification :Here the unsigned message S(m) is spawned by confidential key of all members in AS, and verified whether it's been generated by the members of AS. Step 3: Sender Enigma: Considering n to be the overall count of AS members, the verification successfully determines the evident sender of the message to be the probability 1/n.

B. System architecture

The relevant node choice of an AS plays a predominant role in providing strong source privacy, considering the original node source to be hidden in the ambiguity set. The proposed idea debates on how the SAMA prohibits the rivalry from source message recording by AS analysis.

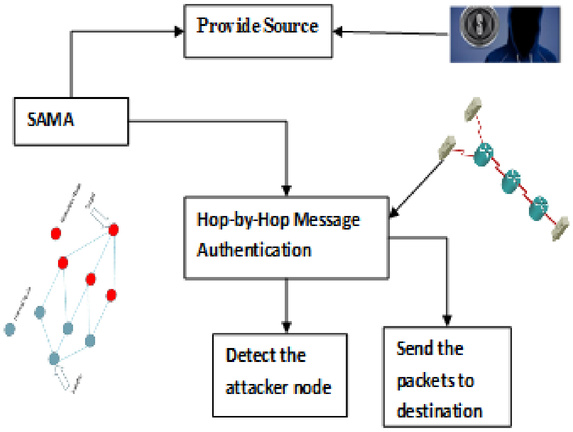

Provide Source
SAMA
Hop-by-Hop Message Authentication
Detect the attacker node
Send the packets to destination

Figure-1. System architecture.

During the message communication a private key is selected from the list of ambiguity sets by choice in authenticate server. These sets include it, together with some other nodes. The possibility of obtaining the original node or even the order of a previous hop could be figured by the attacker's node on receiving the message. Besides, when these attackers being incapable to traffic monitoring of the previous hops discriminating between the forwarder and the original node is impossible; At most care the AS selection should be made, thereby making the attackers inaccessible to the source message.

C. SAMA on Elliptic curves

1) SAMA signature generation

Considering message me to be communicated between sources to a destination node in a network by a sender (say Mike. The AS includes n members, M_1, M_2,…,M_n, for example, S= { M_1, M_2…M_n} be the message transmitted by sender Mike is Mt, between the range t, 1≤ t≤ n. Here the node Mi and its public key Qi are not discriminated. Therefore, we also have S={Q_1,Q_2,…,Q_n}.

2) Authentication generation scheme

When the message to be transmitted is missed the message sender Mike uses the private key dt, 1≤t≤N and performs three steps they are as follows:

Step 1: Consider an arbitrary coefficient and its corresponding ki value for each 1≤i≤n−1, i=t, and compute i from (ri, yi) =kiG.

Step 2: Choose a random $k_i \in Z_p$ and compute r_t from $(r_t, y_t) = k_t G - \sum_{i \neq t} r_i h_i Q_i$ such that for any, where $h_A \overset{1}{\leftarrow} h(m, r_1)$.

Step 3: Compute $s = k_t + \sum_{i \neq t} k_i + r_t d_t h_t \mod N$

In SAMA the message m is defined by:

$$S(m) = (m, S, r_1, y_1, \dots, r_n, y_n, s)$$

3) SAMA signature verification

For Nick's verification $(m, S, r_1, y_1, \dots, r_n, y_n, s)$, the public keys $Q_1, \dots, Q_n$. Should be known beforehand. Then he should check and verify the following steps:

Step 1: Checks that $Q_i \neq \mathcal{O}, i = 1, \dots, n,$ else it is arrival id

Step 2: Checks that $Q_i, i = 1, \dots, n$ lies on the curve

Step 3: Checks that $nQ_i = \mathcal{O}, i = 1, \dots, n$

Step 4: Verify that r_i, y_i, i=1,…,n, and s are values in[1,N−1].Else the signature is irrational.

Step 5: Calculate $h_i^1 \leftarrow h$ (m, r_i), where h is the same function used in the signature generation.

Step 6: Calculate. (X0, Y0)=sG - $\sum^{n}_{i=0} r_i \; h_i \; Q_i$. The signature becomes valid only if the first coordinate of $\sum_i (r_i \; y_i)$ equation ls x0 ,is valid.

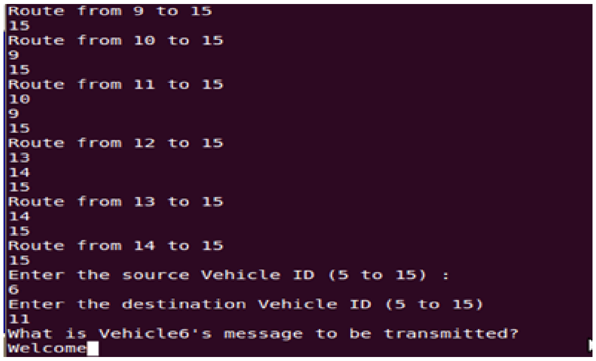
Use footnotes sparingly (or not at all) and place them at the bottom of the column on the page on which they are referenced. Use times 8-point type, single-spaced.

To help your readers, avoid using footnotes altogether and include necessary peripheral observations in the text (within parentheses, if you prefer, as in this sentence).

Number footnotes separately from reference numbers, and in superscripts. Do not put footnotes in the reference list. Use letters for table foot notes.

4. EXPERIMENTAL RESULTS AND DISCUSSIONS

Similar to WiMAX networks, the intruder can introduce a DoS attack during the random-access process, as the messages are in plain text. In our proposed scheme, the random-access the encryption of the request and acknowledgment message is performed by the use of a public key of AS. Hence, the messages exchanged during the random-access process are encrypted, and the DoS/Replay attack is avoided. Our proposed source-anonymous message authentication (SAMA) contributes absolute message sender anonymity.



```
Route from 9 to 15
15
Route from 10 to 15
9
15
Route from 11 to 15
10
9
15
Route from 12 to 15
13
14
15
Route from 13 to 15
14
15
Route from 14 to 15
15
Enter the source Vehicle ID (5 to 15) :
6
Enter the destination Vehicle ID (5 to 15)
11
What is Vehicle6's message to be transmitted?
Welcome
```

Figure-2. Vehicle's initial information.

Initially n number of source node is created and routed to each other. The source and the destination vehicle ID along with the message which has to be transmitted is entered which is shown in Figure-2. Here the source vehicle ID is given as 6 and destination vehicle ID is given as 11 and the message "Welcome" is entered.

Transmission of data in the VANET environment from source to destination is shown in Figure-3. The "welcome" message is transmitted from the source vehicle 6 to the destination vehicle 11. Here hop by hop data transmission takes places for the messages to reach the destination.

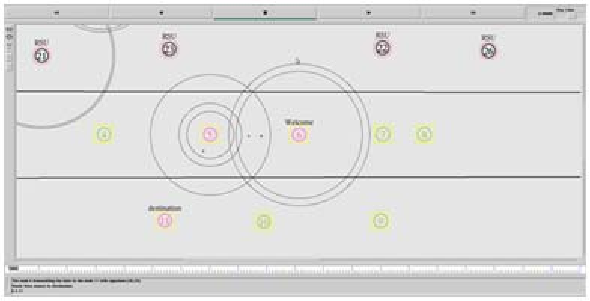


Figure-3. Data transmission.

The source vehicle generates a signature value (36, 29) for the source vehicle 6 which in turn is transmitted and verified at the destination vehicle 11, if both the generated signature matches, then the signature is valid which is shown in Figure-4.

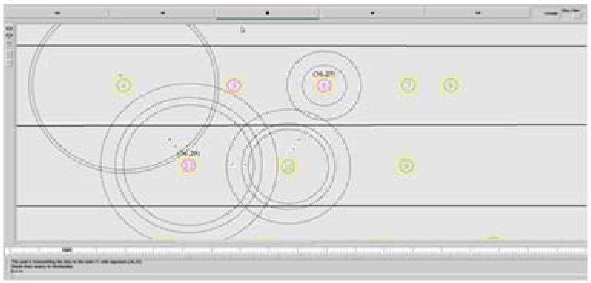


Figure-4. Signature verification.

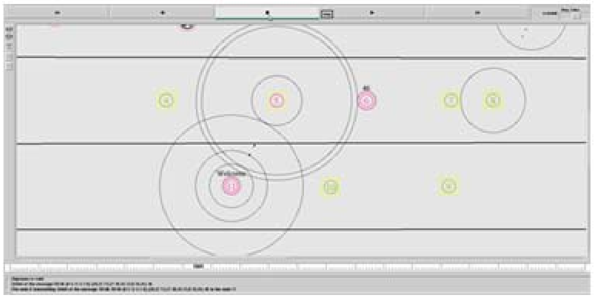


Figure-5. SAMA signature generation.

After the signature verification is done the SAMA signature value for the source vehicle 6 is generated as 46 for the corresponding message “Welcome” using the single equation which is discussed above is shown in Figure-5.

The generated SAMA Signature is then verified, if the same signature is obtained on the destination, vehicle as that of the source vehicle the corresponding message entered becomes valid which is shown in Figure-6.

A. Message transmission delay

The overall time taken by the packet to reach the destination inclusive of delay due to the queuing of data packets and while locating the routes. Here the data packets which reach the destination finally are only taken into count. The $MAF_m(y)$ is defined as : $MAF_m(y) = f(h(m), y) = \sum_{j=0}^{d_y} M_j y^j$. $MAF_m(y)$ is represented by its d_y+1 coefficients, where $p \in (2^{l-1}, 2^l)$ Thereby the overall length exist within the limit $l(d_y + 1)$. The overall length per message is calculated in our scheme by the following expression: $4l(n - 1) + n(\log_2 r)$. where r is the number of nodes.

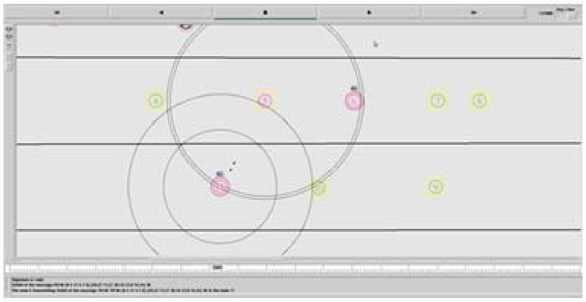


Figure-6. SAMA signature verification.

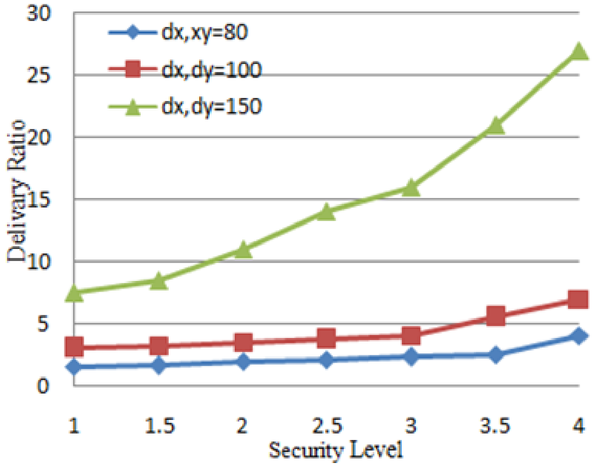


Figure-7. Message transmission delay.

B. Energy consumption

It’s the ratio between the energy spent by the node to the pioneer energy, measured in metrics. The simulation outcome provides us the initial and final energies. The calculated energy is the energy consumed by each node during the earlier stages. The final energy is the exhausted energy by all the nodes.

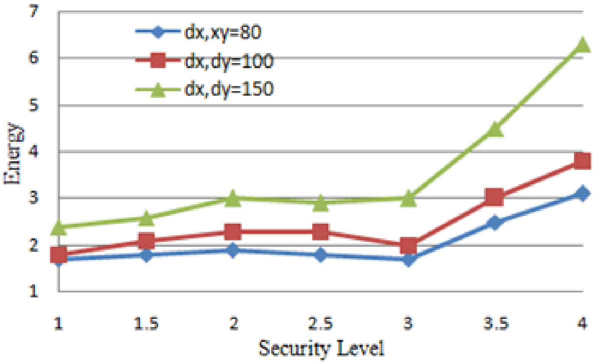


Figure-8. Energy consumption.

5. PERFORMANCE ANALYSIS

Here in this part assessment of our proposed verification scheme is done and shown in simulation demonstrations. The Energy consumption by the sensor node, Packet delivery ratio and delay is the parameters used to determine the achievement of the idea proposed. In our simulation tool NS2, the trace file is given as the input to the x graph which generates graph as the result. Through a public-key enciphering system, the authentication is conveyed mainly due to their high estimation aloft, the public-key-based encryption methods are generally taken into consideration but not preferred. However, our research demonstrates that this is not always true. In each AS there will be n number of nodes selected at random. On providing additional source security aid, even the corruption of one single message will be handled at secure rate. The source privacy can be achieved even for smaller values of n thereby elevating the system performance.

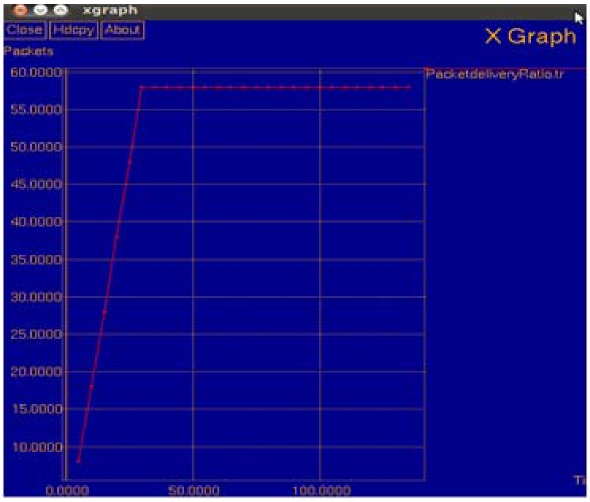


Figure-9. Packet delivery ratio.

The ratio of packets sent to the terminal is shown in the graph Figure-9. Here the ratio is calculated based on number of packets received and number of packets sent.

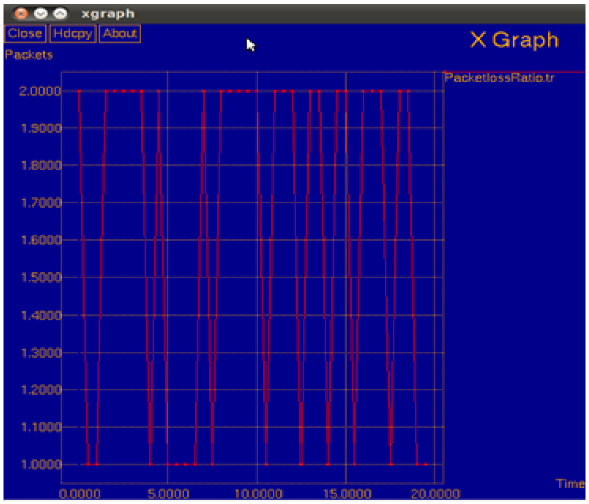


Figure-10. Packet failure ratio.

The graph shows the ratio of the packet failure when they are sent to destination is shown in the Figure-10.

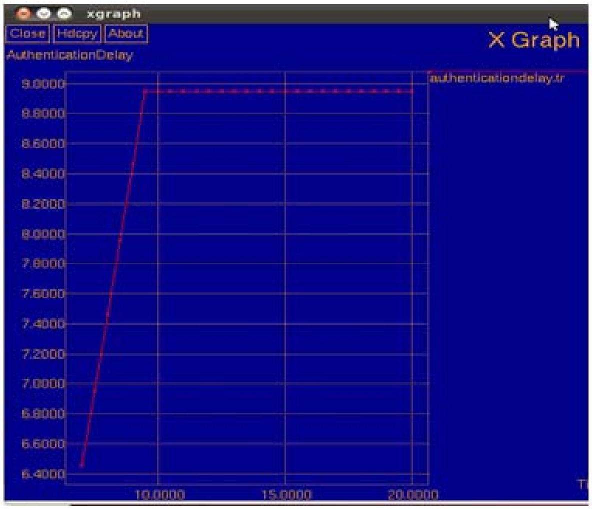


Figure-11. Authentication delay.

The average time to deliver the packets to the terminal is calculated based on the arrival time, send time and number of connections which is shown in the graph Figure-11.

6. CONCLUSIONS

The main perception of this paper deals with potent Source Anonymous Message Authentication (SAMA) providing hop by hop authentication and securing the source. The proposed design in the SAMA consists of three steps which allows authentication of SAMA by unitary comparison rather than individually attesting. The outcome of the simulation proves to be more productive than the polynomial-based approach relating computational and communication overhead thereby providing strong source security.

REFERENCES

[1] Perrig, R. Canetti, J. Tygar, and D. Song, “Efficient Authentication and Signing of Multicast Streams over Lossy Channels,” Proc. IEEE Symp. Security and Privacy May 2000.

[2] R.L. Rivest, A. Shamir, L. Adleman,”A method for obtaining digital signatures and public key cryptosystems,”in Commun. Of the ACM. Feb 1978, vol. 21.2, pp. 120-126.

[3] D. Pointcheval and J. Stern, “Security proofs for signature schemes,” in Advances in Cryptology - EUROCRYPT, Lecture Notes in Computer Science Volume 1070, pp. 387-398, 1996.

[4] Ashwini M. Rathod, Archana C. S,” Secure Network Discovery by Message Authentication in Wireless Sensor Network “,international Journal of Research in Engineering Technology and Management ISSN 2347-7539.

[5] Tao Han, Ning Zhang, Kaiming Liu et.al , "Analysis of mobile WiMAX Security :Vulnerabilities and Solutions," in Mobile Ad Hoc and Sensor Systems, 5th IEEE Int. Conf. ., 2008, pp. 828-833.

[6] H. Mun, K. Han, and K. Kim, "3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAPAKA," in roc. Wireless TeleCommun. Symp. 2009, pp. 1-8.

[7] Z. Shi, Z. Ji, Z. Gao and L. Huang, "Layered security approach in LTE and simulation," Proc. 3rd Int. Conf. Anti-Counterfeiting, Security, Identification Commun. pp. 171-173, 2009.

[8] L. Huang, Y. Huang, and Z. Gao, "Performance of authentication protocols in LTE environments," in Proc. Int. Conf. Comput. Intell. Security, 2009, pp. 293-297.

[9] J. Hong Kok Han, M. Yusoff Alias, and M. Goi Bok, "Potential denial of service attacks in IEEE802.16e-2005 networks," in Proc. 9th Int. Conf. Commun., Inf. Technol., 2009, pp. 1207-1212.

[10] L. Maccari, M. Paoli, and R. Fantacci, "Security analysis of IEEE802.16 communications," in Proc. IEEE Int. Conf. Commun. 2007, pp. 1160-1165.

[11] A. Veeramuthu, S. Meenakshi, and A. Kameshwaran, "A plug-in feature extraction and feature subset selection algorithm for classification of medicinal brain image data," Communications and Signal Processing (ICCSP), 3rd International Conference, pp.1545-1551, 2014.