ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

Security in Vehicular Ad-hoc Network

Yogita A. More [1], Nilima P. Patil [2]

P.G. Student, Department of Computer Engineering, SSBTs College of Engineering, Bambhory, Jalgaon, India[1]

Assistant Professor, Department of Computer Engineering, SSBTs College of Engineering, Bambhory, Jalgaon, India[2]

ABSTRACT: The automobile manufactures uses wireless communication and networking into vehicles to increase safety and efficiency on road transmission. Vehicular ad hoc network (VANAT) is subset of mobile ad hoc network. Vehicular Communication requires vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) with security to improve road safety. VANETs security is essential because badly designed VANET is exposed to network attacks and danger to the security of drivers. The VANET is to provide road safety information among the nodes hence the frequently exchange of such type of data on the network clearly signifies the role of security. Encryption and description of modified SHA-256 is use to provide security to network packets. Network packets contain information or message. The messages which are transferred between nodes or vehicular is secure.

KEYWORDS: VANET, MANET, OBU, RSU.

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) have recently attracted extensive attentions as a promising approach to enhancing road safety, as well as improving driving experience. By using a Dedicated Short-Range Communications (DSRC) technique, vehicles equipped with wireless On-Board Units (OBUs) communicate with other. VANET use fixed infrastructure, e.g., Road-Side Units (RSUs), located at critical points of the road. Therefore, two basic communications in VANET are Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications [12]. Once VANETs become available, numerous safe, commercial and convenient services deployed through a variety of vehicular applications. These applications mostly rely on vehicles OBUs to broadcast outgoing messages and validate incoming ones. The broadcast packets contain information about position, current time, speed, direction, driving status etc. For example, by frequently broadcasting and receiving packets, drivers are better aware of obstacles and collision scenarios. They act early to avoid any possible damage. Assign a new route in case of a traffic accident in the existing route.

However, before implementing these attractive applications, particularly safety-related ones, must address and solve VANET-related security issues. To secure vehicular networks, an authentication scheme is indispensable to ensure messages are sent by authentic vehicles and not altered during transmissions. Otherwise, an attacker can easily change the normal function of VANETs by injecting bogus messages. Therefore, vehicles should broadcast each message with a digital signature.

There are several requirements to achieve security in VANETs [10]. Security attributes are as follows.

AUTHENTICATION: In vehicular communication, it is very important to authenticate the sender of message to prevent alteration.

CONFIDENTIALITY: It is important the privacy of each entity must be protected. Directional antennas and encrypted data should be used to provide confidentiality.

INTEGRITY: Instances for all messages must be protected from the damages done by the intruder by altering the message content, so information should be secured. Data integrity is the assurance the data received by nodes, RSUs and is the same [11]. As what has been generated during the exchanges of the message. In order to protect the integrity of the message and digital signature which is integrated with password access are used.

AVAILABILITY: Availability means insure the network resources must be available to legitimate user. Non-Reputation: Non-reputation means, able to induce the ability to identify the attacker even after its occurrence. Ensures sending and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

receiving parties cannot deny ever sending and receiving the message. In certain fields, non-repudiation is called auditability.

II. RELATED WORK

In [3], to tackle the aforementioned problems, including security, efficiency, and scalability problems, proposed an anonymous batch authentication and key agreement (ABAKA) scheme to build a secure environment for value-added services in VANETs. To avoid bottleneck problems, ABAKA is inspired by the concept of batch verification to simultaneously authenticate multiple requests sent from different vehicles using elliptic curve cryptography (ECC), which is adopted by the Trial-Use standard. Meanwhile, multiple session keys for different vehicles also be negotiated at the same time. To the best of knowledge, it is study provides batch authenticated and key agreements for value added applications in VANETs. In [2], proposed algorithm is based private key encryption. That encryption private key is used to make communication between nodes. Security measures guarantees the transmission of information or data are authentic. Authentic data is accessible only by authorized parties. The proposed algorithm provides authentication, security increase throughput and reduce delay. In [1], proposed robust detection mechanism against sybil attack. In propose approach node keeps a record of it's neighbor nodes. Record is exchange groups of its neighboring nodes periodically. Record performs the intersection of these groups. If some nodes observe they have similar neighbors for duration of time. Similar nodes are identified as sybil nodes. It is simple and efficient approach. In [4], proposed TESLA (Timed Efficient Stream Loss-Tolerant Authentication) is used as an authentication method for distributing secret keys to all OBUs in multicast and broadcast network communications with minimum delay. It is used as an authentication method for multicast and broadcast network communications. TESLA uses symmetric key cryptography for broadcast authentication. TESLA solved the problems of distributing secret keys to all OBUs in multicast and broadcast network communications with minimum delay. PKI is not the only option to confirm user authentication in VANET system. There is a completely different technique called TESLA which provides an efficient alternative to signatures. In [5], provides a way by which message authenticity is improved by combining two schemes digital signatures and attribute based cryptographic schemes. proposed system provide a comparison of various attribute based cryptographic schemes for message authentication is done on the basis of dynamicity i.e. whether the attributes are dynamic in nature or not. Computation overhead is more in case of IBE and KP-ABE schemes where as overhead incurred in case of CP-ABE is minimum. Both the KP-ABE and CP-ABE schemes provide collusion security. KP-ABE scheme suffers from the key abuse attack where as CP-ABE scheme do not have any affect of attack. It concludes CP-ABE is better technique as compared to IBE and KP-ABE. In [6], proposed a new algorithm to enhance the security mechanism of AODV (Ad hoc On Demand protocol. It enhances AODV protocol detect and takle a particular category of network attack such as black hole attack. The proposed algorithm maintains the look-up table. Look-up table stores the PREP sequence. The sequence is arranged in ascending order using POP and PUSH operation. A header H-node attached to each message which received from different nodes and assign priority to PRREP message. It is considered in that order by source node. It is calculate based on sequence number. The very high destination sequence number is discarding the RREP. The proposed algorithm increases the security of black hole attack. In [7], proposed p-secure approach. P-secure approach is used for detection of DoS attacks before the confirmation time. Proposed approach improves road safety, transport and efficient also reduce the impact of transport on the environment. It is a attack detection algorithm that is applied for detecting DoS attack. The P-secure approach improving safety in VANET, also reduction in processing delay's. In [8], observe that signature flooding can be mitigated by broadcast authentication schemes whose overheads match the entropy of the broadcast messages. Approach in the context of VANETs and propose two flooding-resilient broadcast authentication schemes, SelAuth and FastAuth for different VANET applications. Schemes are based on digital signatures thus providing non-repudiation. To the best of knowledge, prior work on lightweight broadcast authentication either lacks the non-repudiation property or fails to operate efficiently in dynamic VANET environments. In [9], proposed trusted opportunistic forwarding model in VANET, it incorporates trust mechanism into OR and to enhance the security of routing and protect the network from malicious attack. Opportunistic routing mainly focus on two factors that are cost and security.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

III. PROPOSED ALGORITHM

A. Modified SHA-256 Encryption Algorithm

Aim of the proposed algorithm is to maximize the delivery ratio, minimize packet drop, minimize end to end delay and providing security to network packet by minimizing the shifting and increasing rounding of SHA-256 algorithm [13]. The proposed algorithm is consists of main steps.

- Initialize the hash value H_1- H_8.
- Padding of message, the length of the padded message should be multiple of 512-bits.Keeping track of previously used paths.
- Parsed into 512-bit message blocks M_0,M_1,.....,M_N.
- Initialize registers a, b, c, d, e, f, g, h with intermediate hash values.
- Apply compression function to update registers.
- Process 32-bit words and generates 32-bit word as output.
- Compute intermediate hash values.
- Display encrypted message.

In modified SHA-256 Encryption algorithm first padding n number of blocks . Pad the message in the usual way: suppose the length of message M, in bits, is l. Append the bit 1 at the end of message then zero bits and then length become 512-bit padded message. Second parse the message into n 512-bit blocks M_0,M_1,.....,M_N. Use the big-endian convention throughout, so within each 32-bit word, the left-most bit is stored in the most significant bit position. Initialize registers a, b, c, d, e, f, g, h with the $(i = 1)^{st}$ intermediate hash value. The initial hash value when i = 1. Register value give input to the compression function. Apply the modified SHA-256 compression function of encryption to update registers a, b,..., h. Apply compression function from 0 to 69. Function generate 256 bits encryption message. Compute Ch(e, f, g), Maj(a, b, c), $\sum_0(a)$, $\sum_1(e)$ and W_j .Compute the i^{th} intermediate hash value $H^{(i)}$. Initialize new hash vales to hash $H^{(i)}$. Six logical functions are used in Modified SHA-256 of encryption algorithm. Each of these functions operates on 32-bit words and produces a 32-bit word as output. Expanded message blocks W0, W, … , W(69) are computed via the modified SHA-256 message schedule.

.

B. Modified SHA-256 Decryption Algorithm

The proposed algorithm is consists of main steps.

- Initialize the hash value H_1- H_8.
- Padding of message, the length of the padded message should be multiple of 512-bits.Keeping track of previously used paths.
- Parsed into 512-bit message blocks M_0,M_1,.....,M_N.
- Initialize registers a, b, c, d, e, f, g, h with intermediate hash values.
- Apply reverse compression function to update registers.
- Process 32-bit words and generates 32-bit word as output.
- Compute intermediate hash values.
- Display decrypted message.

In modified SHA-256 decryption algorithm use same steps of modified SHA-256 encryption algorithm only apply the reverse compression function 69 to 0. By using reverse function of modified SHA-256 decryption algorithm compute decrypted message.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

IV. SIMULATION RESULTS

Experimental results consist of the values of End-to-End delay, Delivery ratio and number of Packets Drops with respect to proposed system as well as existing system. Figure 1 shows the difference of end-to-end delay between existing and proposed system. The result shows the average end-to-end delay of 10 experiments of 50 nodes, 100 nodes, 150 nodes and 200 nodes. The average end-to-end delay of 50-200 is calculated by using end to end equation. The end to end delay is measures in micro second. Figure 2 shows the difference of delivery ratio between existing nodes, 150 nodes and 200 nodes. The average delivery ratio is calculated by using equation of delivery ratio. The delivery ratio is measure in percentage. Figure 3 shows the difference of packet drop between existing and proposed system. The result shows the average packet drop result of 10 experiments of 50 nodes, 100 nodes, 150 nodes and 200 nodes. The packet drop is calculated by using equation of packet drop.

Experimental results show the difference between existing and proposed system. Results shows the propose system is better than existing. If number of nodes is increases 50-200 then increases the end-to-end delay and packet drop. But comparing both proposed system and existing system, in propose system decreases the end-to-end delay, packet drop and increases the delivery ratio. The proposed system proves that modified SHA-256 algorithm is secure algorithm.

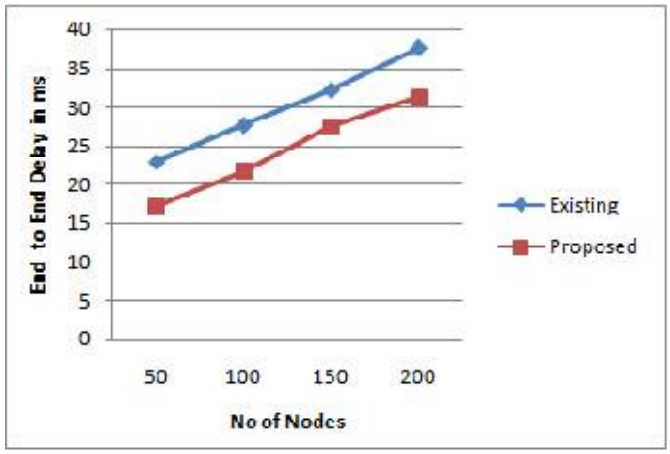

Fig.1. End to end Delay

In figure 1 sows the result of end to end delay. If number of nodes increases by 50 to 200 then end to end delay of proposed and existing system increases. If compare the both system existing and proposed, in proposed system decreases end to end delay. So proposed system prove the modified SHA-256 algorithm is secure.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

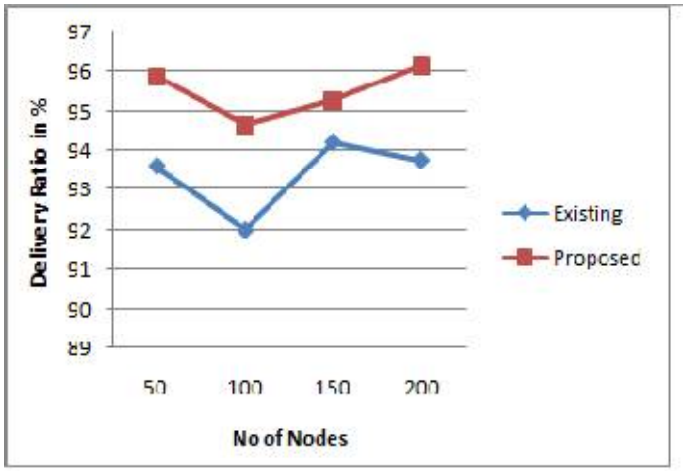

Fig. 2. Delivery Ratio

In figure 2 sows the result of delivery ratio of 10 experiment of 50 to 200 nodes. Result sows that the proposed system is better than existing because if compare the results of both existing and proposed system, the proposed system is prove that modified SHA-256 algorithm is based.

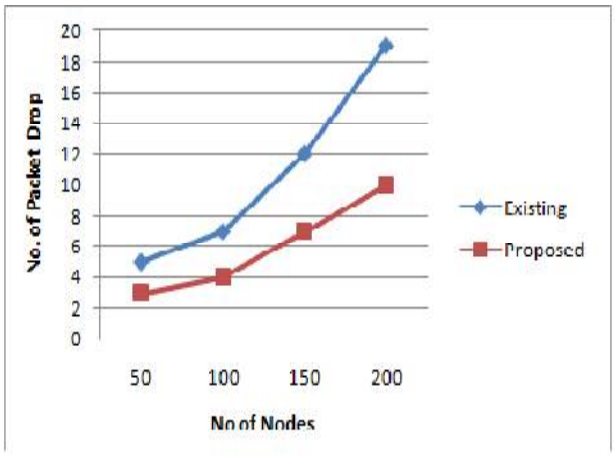

Fig.3. Packet Drop

In figure 3 shows the average result of packet drop. In proposed system the packet drop is decreases as compare to existing system. So proposed system is prove that the modified SHA-256 algorithm is secure.

V. CONCLUSION AND FUTURE WORK

Vehicular Ad-hoc networks (VANETs) is continuously self-configuring infrastructure less network. Each device in VANETs is free to move independently in any direction. Therefore change it's links to other devices frequently. The main issue in VANETs is security. The proposed system to prevent or mitigate the standard security goals. Security measures guarantees that the transmission of data or information is authentic. The encryption and decryption of modified SHA-256 algorithms provide security to network packets or data. The proposed system can be applied to vehicular users in vehicular ad hoc network. The proposed system is evaluated using through NS-2 simulator tool and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

tcl file is generated using sumo and move tool. The main properties of VANET is high mobility, so proposed system leads to reduction in end-to-end delay, packet drop, increasing delivery ratio and improving safety in VANET.

The research work should be focused on the performances of data transmission in VANETs tested by applying more encryption and decryption algorithms to provide more security with increased throughput and reduced delay. And also increase security of message by applying different security protocols.

REFERENCES

1. Azita Soltanian Bojnord and HodaSoltanian Bojnord, 'A Secure Model for Prevention of Sybil Attack in Vehicular Ad Hoc Networks', IJCSNS International Journal of Computer Science and Network Security,Vol.17 No.1, pp. 30-34, January 2017.
2. Manpreet Kaur, Rajni and Parminder Singh,'An Encryption Algorithm to Evaluate Performance of V2V Communication in VANET', International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.2, pp. 15-21, June 2013.
3. Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien,'ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks', IEEE Transaction On Vehicular Technology, VOL. 60, NO. 1, pp. 248-262, January 2011.
4. K.Madhurima and P.Kalyani, 'Accelerate TESLA Protocol for VANETs', International Journal of Research and Computational Technology, Vol.6, Issue 2, pp. 1-7, September 2014.
5. Sandhya Kohli and Rakesh Dhiman, 'Secure Message Communication using Digital Signatures and Attribute Based Cryptographic Method in VANET', International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 591-594, December 2010.
6. Parul Tyagi and Deepak Dembla ,'Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)', Egyptian Informatics Journal, pp. 133-139, November 2016.
7. Reza Fotohi, Yaser Eblazadeh and Mohammad Seyyar Geshlag ,'A New Approach for Improvement Security against DoS Attacks in Vehicular Ad-hoc Network', (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 7, No. 7, pp. 10-15, November 2016.
8. Hsu-Chun Hsiao, Ahren Studer,Chen Chen and Adrian Perrig,'Flooding-Resilient Broadcast Authentication for VANETs', Security and Protection, pp. 193{204, September 2011.
9. Mayuri Pophali, Shraddha Mohod and T.S.Yengantiwa, 'Trust Based Opportunistic Routing Protocol for VANET Communication', International Journal Of Engineering And Computer Science, Vol.6, pp. 7408-7414, August 2014.
10. Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim, 'A Literature Survey on Security Challenges in VANETs', International Journal of Computer Theory and Engineering, Vol. 4, No. 6, pp. 1007, December 2012.
11. Ram Shringar Raw, Manish Kumar and Nanhay Singh, 'Security Challenges, Issues and their Solutions for VANET', International Journal of Network Security and Its Applications (IJNSA), Vol.5, No.5, pp. 95, September 2013.
12. Anup Dhamgaye and Nekita Chavhan, 'Survey on security challenges in VANET', IJCSN International Journal of Computer Science and Network, Vol. 2, Issue 1, pp. 88-96, 2013
13. Dilli Ravilla, Chandra Shekar Reddy Putta, 'Enhancing the Security of MANETs Using Hash Algorithms ', Eleventh International Multi-Conference on Information Processing, pp.196-206, 2015.