AUTHENTICATION AND SECURITY SCHEME AGAINST DOS ATTACK FOR VANET

Sonali Ghodke[1] and Rohini Bhosale[2]

[1]Post Graduate Student.Computer Engineering Department, Pillai's HOC College of Engineering & Technology, Rasayani, Panvel, Affiliated to Mumbai University, Maharashtra, India

[2]Assistant Professor. Computer Engineering Department, Pillai's HOC College of Engineering & Technology, Rasayani, Panvel, Affiliated to Mumbai University, Maharashtra, India

Abstract—

Nowadays Intelligent Transportation System (ITS) is becoming a very popular technology and its main component is known as VANET. To improve road safety and driving conditions, an unplanned network is formed by vehicles on the road spontaneously is called as Vehicular Ad-hoc Network (VANET). Every network is vulnerable to security attacks and VANET is no exception. Security is the key factor in VANET because it affects the life of people. This proposed mechanism focuses on the authentication scheme and also detects Denial of Service (DoS) attack. In this system the authenticity of the message is achieved by using digital signature and digital certificate with the capability of preventing malicious vehicles entering into the VANET system. As nodes can send any life critical information to each other, availability of the network needs to be maintained. This scheme is responsible for availability of the network by detecting DoS attack.

Keywords— Intelligent Transportation System(ITS), Vehicular Ad hoc Network(VANET), Denial of Service(DoS).

I. INTRODUCTION

The development of Intelligent Transportation System (ITS) has made a big step in recent years and shortly it has become very popular. The important application of (ITS) is called as VANET. To improve road safety and driving conditions, an unplanned network is formed by vehicles on the road spontaneously is called as Vehicular Ad-hoc Network (VANET). In VANET, driving safety is enhanced via inter-vehicle communication or communication with roadside units. Hence it is also called as a vehicular sensor network. The main aim of VANET technologies is to improve safety on roads by serving real-time traffic information such as vehicle collisions, road conditions, curve warnings, emergency breaking, traffic updates etc. To share this information vehicle establishes a network and can communicate with each other.

This communication is categorized into two types in VANET. The first type is the Vehicle to Vehicle (V2V) communication in which the moving vehicles can communicate with each other and the second type is the Vehicle to Road Side Unit (V2R) communication in which the moving vehicles can communicate with the RSU's which are located aside the roads. As it is a wireless communication, using the Dedicated Short Range Communications (DSRC) standard channel V2V and V2R communication can take place. Each vehicle is equipped with On-Board Unit (OBU) which is based on IEEE 802.11p radio technology. A special concern in VANET is a safety because it directly affects the life of the people. Figure 1 shows the communication in VANET.

As communication takes place in an open wireless channel, various security threats and attacks occur in VANET network and can disrupt the services provided. Hence it is important to focus on security requirement and security against attacks in VANET. Due to high mobility nature of

VANET network security becomes a key factor in it. To ensure the smooth functioning of intelligent transportation systems the information passing through a network must be secured and protected.

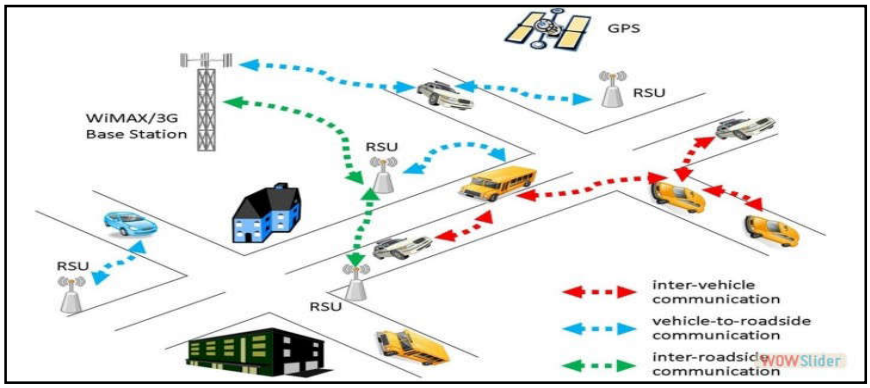

Figure 1: Communication in VANET

The first step to provide security in VANET is performed by providing authentication so that only authenticated nodes can communicate with each other. Authentication is a mechanism which helps to establish the proof of identities. An unauthorized access to a VANET communication may lead to a serious problem with respect to the life-critical messages exchanged between the nodes. In this paper first, we focus on the authentication scheme and also security mechanism against DoS attack for the secure communication in VANET. This paper proposes authentication scheme with the mechanism of detecting DoS attack in VANET. The Main contributions of this paper are as follows:

1) We propose a privacy-preserving authentication approach with the help of using DSA algorithm which is a variant on the ElGamal and Schnorr algorithms.
2) We introduce a scheme which helps to detect and mitigate DoS attack in VANET network by using flow monitoring algorithm. This will achieve the availability of the network for secure communication in VANET.

The rest of the paper is organized as follows. Section II presents related work. The preliminaries of the proposed work are explained in section III. In section IV our proposed approach is presented. Security analysis is explained in section V followed by performance analysis in section VI. Section VII concludes the paper.

II. RELATED WORK

Security in the network is a specific problem whether it is wired or wireless networks. Because of the high speed of the nodes in VANET network, dynamic topology and high mobility are the unique characteristics of VANET. Due to this, it becomes vulnerable to various kinds of security attacks. Many authentication techniques have been proposed by the researchers.

Among these existing techniques, Perrig et al. [1] represented a Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol, which uses symmetric keys instead of using asymmetric keys. Since the symmetric key systems are significantly faster than signatures, the Denial of Service (DoS) attack is averted in this system. But with the symmetric key, it is hard to achieve non-repudiation. The best way to provide nonrepudiation with authentication is a digital signature. TESLA++ can solve only one problem of TESLA (i.e) memory-based DoS, still, they suffer from scalability and non-repudiation. TESLA++ gives poor performance in multi-hop communication.

W. Shen et al. [2] represented Cooperative Message Authentication Protocol (CMAP) to find out the malicious information broadcasted by the malicious vehicles in the road transport system. In

this vehicles shares their location and various safety messages to avoid the collision in a cooperative way. Hence authentication of each message and vehicle is needed to be done. In this protocol, they have proposed three verifier's selection algorithm based on which authentication is to be done. The main limitation of this system is if there is no verifier available to verify the message, malicious message may be consumed by the vehicles.

X. Lin et al.[3] suggested a privacy-preserving authentication scheme based on group signature and identity (ID)-based signature (GSIS). In group signature security and privacy can be achieved without having the overhead of managing the huge number of certificates. Group signature is used to anonymously sign messages with the private key by senders and verified with the group public key by receivers, while identities of senders can only be recovered by authorities. With ID based management complexity can be further reduced.

Pandi Vijaykumar [4] proposed Dual Authentication And Key Management Technique For Secure Data Transmission in Vehicular Ad Ho Network in which for authentication they used two components hash code and fingerprint.

Usha Devi Gandhi [5] presented a request-response detection algorithm for detecting DoS attack in VANET. In this, the vehicles that wish to enter into a network will send a request to RSU. Each RSU is having its own database consisting of the information about the hop counts. If the hop counts and the RSU do not match then considered that node is malicious else allow the node to take part in the network communication.

Amarpreet Singh [6] presented a novel mechanism for detecting DoS attack in VANET by using enhanced attacked packet detection algorithm. In this algorithm DoS attack is being detected using timeslot which is basically based on average communication time of the node, Reza Fotohi [7] presented a new approach for improved security against DoS attack in VANET. In this technique, they proposed a P-secure algorithm to detect the DoS attack before the confirmation time which reduces the overhead delay and increases security.

Comparing with most of the existing authentication schemes, authentication overhead still remains a serious problem. DoS attack detection algorithm existing in the literature is having more overhead in terms of throughput, PDR, energy, and delay as compared with the existing system. Also, a technique to mitigate the DoS attack is not mentioned in the previous work. The proposed system supports the authentication with less authentication overhead and it also detects and mitigates the DoS attack.

III. PRELIMINARIES

This section describes security requirements, attack model and assumptions of our proposed approach.

A. Security Requirements:

In order to prevent various security attacks following security requirements must be fulfilled by any network.

Authentication: The basic requirement of our approach is authentication. It ensures that the origin of a message or document is correctly identified.

Non-repudiation: The sender vehicle cannot deny the transmission of the sent message. The proposed approach achieves this requirement by using a digital signature.

Confidentiality: The principle of confidentiality specifies that data are only read by authorized parties. The sender and intended recipient should be able to access the contents of the message.

Availability: It is a very important factor in VANET. Information or resources should be available to authorized parties at any functioning time.

B. Attack Model:

In this section, various types of attacks in a VANET environment are described. In VANET, communication takes place in an open wireless channel various security threats and attacks occur in VANET network and can disrupt the services provided. There are several attacks which can affect the performance of the operation in VANETs. Attacks can be classified as insider attack which is happened by internal authorized vehicle those are compromised and external attack which belongs to outsider vehicle that is not a part of the network. Based on threat to VANET security requirement, various attacks have been summarized in the below table,

Security Requirement	Attacks
Confidentiality	Eavesdropping, Traffic analysis
Integrity	Masquerading, Replay attack, Message tampering/alter
Availability	DoS, Jamming attack, Blackhole attack, Grayhole attack.
Authentication	Sybil attack, GPS spoofing attack, Node impersonation attack

Table 1: Attacks on Security Requirements in VANET

C. Assumptions:

The following assumptions are made in our approach which is very essential for secure VANET communication.

1) Each vehicle is equipped with OBU and some tamper-proof hardware.
2) TA is powerful then OBU and RSUs which is a trusted entity.
3) TAs public key is given to all vehicles and RSU.
4) TA has powerful firewalls and other protections that prevent them from being compromised [7]
5) Each vehicle is having its own private key which is given by the TA during the authentication time. RSU is also having its own private key.

IV. PROPOSED TECHNIQUE

Due to the open wireless channel of communication, various security threats and attacks occur in VANET network and disrupt the services provided. By considering this issue we have to provide strong authentication and better security approach for secure communication in VANET network. Hence we have proposed a system which consists of two parts as follow.

A. Authentication:

Authentication is a mechanism which helps to establish the proof of identities. It is the first step to provide security in VANET so that only authenticated nodes can communicate with each other. An unauthorized access to a VANET communication may lead to a serious problem with respect to the life-critical messages exchanged between the nodes. In the proposed system, authentication is done by using a digital signature. In this TA will form a cluster on the basis of location and energy of a node. Each cluster consists of one RSU which is fixed along the roadside. TA will generate some DSA parameter consisting keys and node id. Using this parameter authentication is takes place and certificate generates. Also for strong authentication digital signature will get generated by using RSU key and TA key and communication begins. V2V communication can take place by verifying the digital signature as well as digital certificates. Exchange of messages can take place by doing encryption and decryption using SHA algorithm. The following are the steps for authentication.

1. TA's public key is given to each vehicle and RSU at the time of registration.
2. For each node, TA will generate DSA parameter which consists of key and node id.
3. From DSA parameter RSU will extract the public and private key.
4. The TA maintains the list of private keys of all vehicles corresponding to its node id.
5. To create a certificate sends a certificate request to TA.
6. TA will generate the certificate and sends it to the node in an encrypted format.
7. After receiving the certificate from TA, using TA's public key it can be decrypted and self-signed by using the private key of the node.
8. For V2V communication exchange of messages can be done by sharing this digital certificate.

B. Security mechanism against of DoS attack

One of the major security requirement in VANET is the availability of the network.The unavailability of the network may result in DoS attack. To detect DoS attack flow monitoring algorithm is used in proposed mechanism.

The following are the steps for Flow monitoring algorithm

1. Set the counter s= 100 for flow
2. Set the repeat flow of counter s: loop
3. Set TTL for packet to live TTL= 100s
4. Use loss monitor to track the flow of packet at every hop count. Agent/Loss Monitor
5. Detect the node with ack packet.

By using the above two approach we can get the strong authentication and also resistance to DoS attack.

V. SECURITY ANALYSIS

This section analyzes the proposed approach with respect to the security requirements.

1. **Vehicles authentication:**

   TA will generate DSA parameter for each vehicle from which public, private key and node id is extracted. A self-signed certificate is then generated by the vehicles which are then signed by TA with its private key after verifying node id and nodes private key. Exchange of certificate between the nodes will start the communication. Hence strong authentication is provided by the proposed approach.
2. **Nonrepudiation:**

   After exchanging the digital certificate communication between the nodes will start in VANET network. TA which is the center head is only responsible to sign the certificate by using its private key. As we are using digital signature signer cannot claim they did not send a message.
3. **Resistance to DoS attack:**

   DoS attack can be launched by sending a stream of packets continuously in the network. With the help of flow monitoring algorithm, we have set the counter and timestamp for each packet. Hence in a given timestamp if the sender sends more packets that node will be considered as a compromised node.
4. **DoS Prevention:**

   If a malicious node is found in the network then it can be directly terminated from the network for future secure communication.

VI. PERFORMANCE ANALYSIS

In order to evaluate the performance of the proposed scheme with respect to the existing authentication scheme, we have chosen four parameters such as energy, packet delivery ratio, delay, and throughput. Simulation is done in NS2.35 simulator tool and parameters used in simulation are as shown in table below,

Channel Type	Wireless Channel
Mac type	802.11
Queue Type	Droptail / Priority Type
Interface Type	Phy / WirelessPhy
Antenna Type	Omni Antenna
Area Size	800 X 800
No of Nodes	50
Simulation Time	10 sec

TABLE 2: SIMULATION PARAMETER

A. Packet Delivery Ratio (PDR):

Packet Delivery Ratio can be defined as the ratio between the numbers of sent packets to the number of received packets. Figure 2 shows comparison based on packet delivery ratio of the existing system and proposed a system

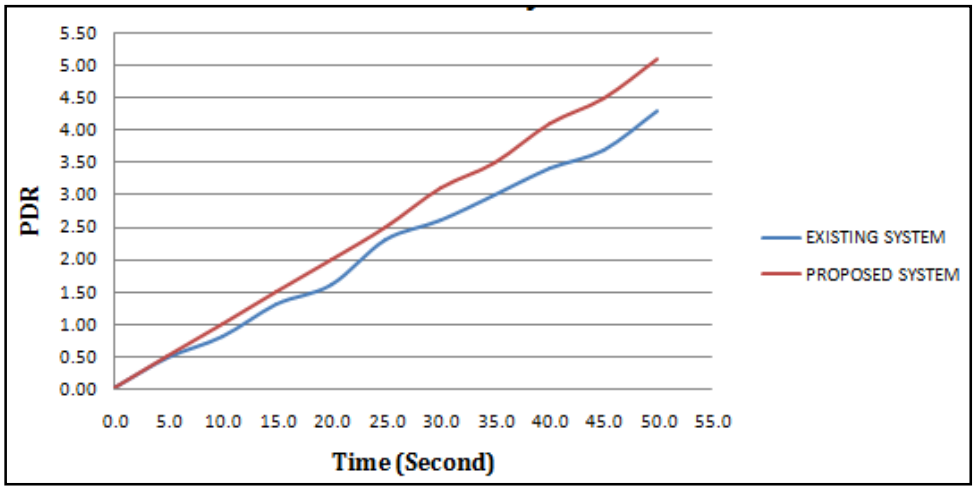

Figure 2: PDR vs. Time

B. Energy:

Energy represents the energy level of the nodes in the network. Each node is having an initial value that is the energy level of the node at the beginning of the simulation. A node cannot be able to receive or transmit the data if its energy level reaches to zero. Figure 3 shows comparison based on an energy of the existing system and proposed a system.

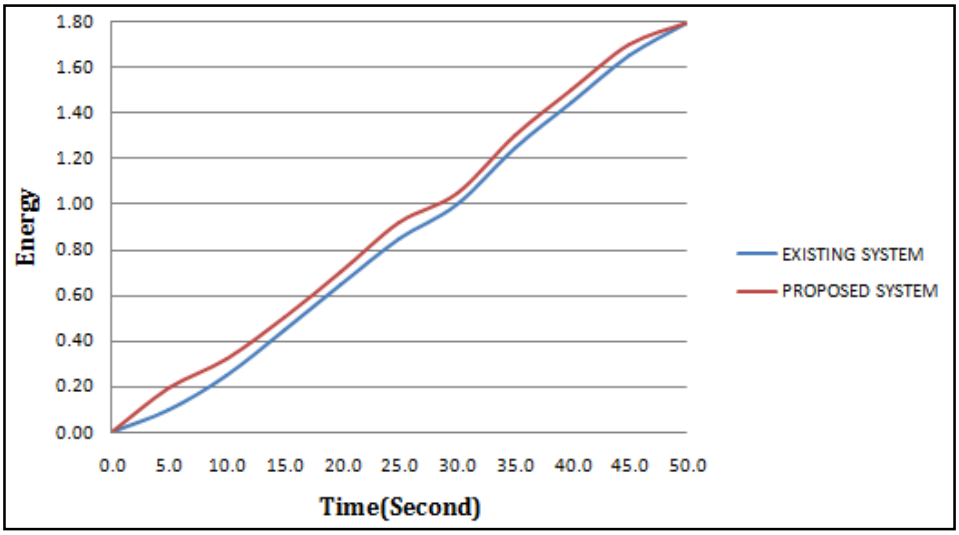

Figure 3: Energy vs. Time

C. Throughput

Throughput can be defined as the number of data packets successfully transmitted from source to destination in a unit time. Figure 4 shows comparison based on throughput of the existing system and proposed a system.

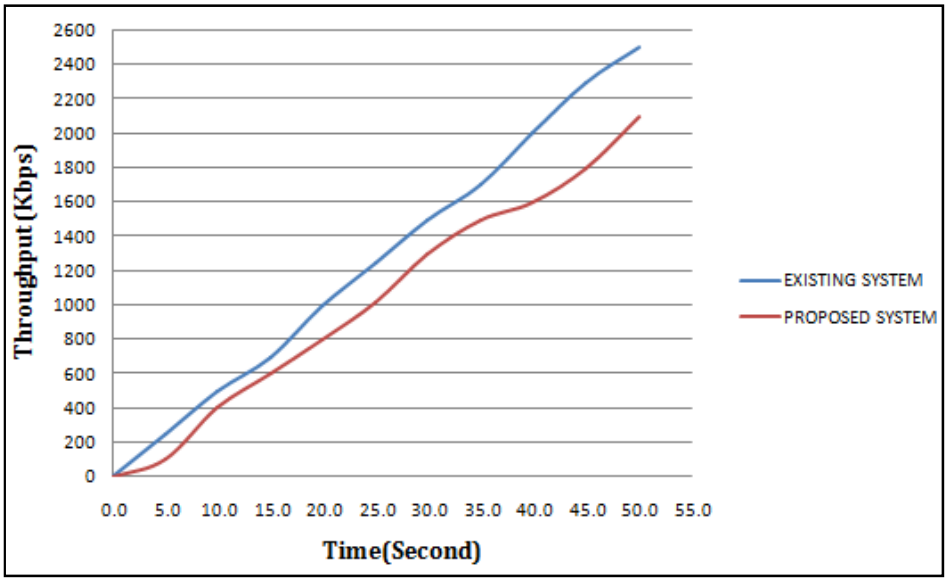

Figure 4: Throughput vs. Time

D. Delay

Delay is the difference between the time at which source node generated the packet and the time at which the destination node received the packet. Figure 5 shows comparison based on the delay of the existing system and proposed a system.

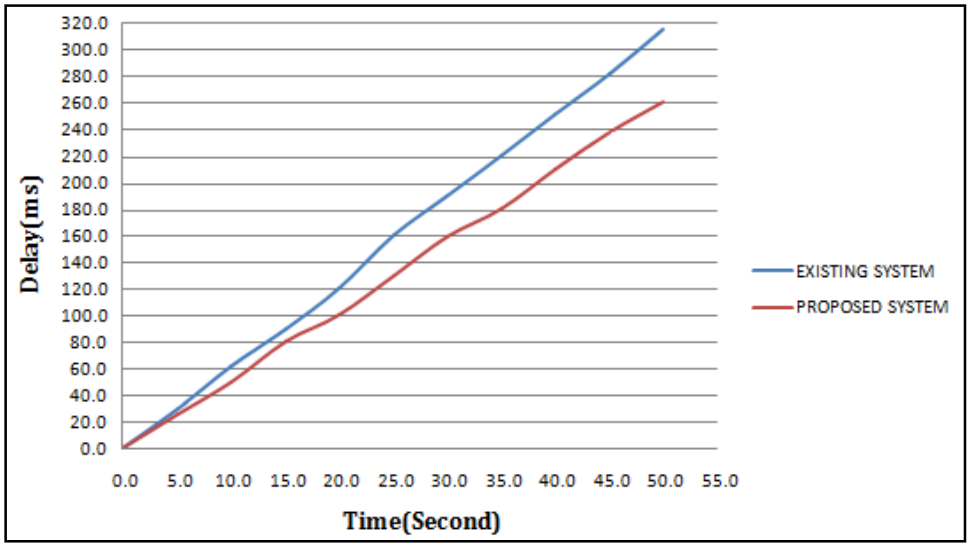

Figure 5: Delay vs. Time

VII. CONCLUSION

In the proposed system, strong authentication is provided by exchanging digital certificate to each other which is signed by TA. This will prevent unauthorized vehicles entering into the VANET network. It also provides a solution to a DoS attack which ensures the availability of the network for secure communication of the nodes. DoS attack is being detected by setting a threshold value and to calculate a number of packets sent by the sender to receiver at a given timestamp. Both authentication and security against DoS attack are achieved in the proposed system to make VANET more powerful and secure.

REFERENCES

[1] Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," RSA Crypto., vol. 5, no. 2, pp. 2–13, Aug. 2002.

[2] Lin et al." TSVC: Time efficient and secure vehicular communication with privacy-preserving" IEEE Trans. Vol.7 no.12 pp. 411-416, Dec 2008.

[3] Usha Devi Gandhi "Request response detection algorithm for detecting DoS attack in VANET" IEEE transaction ICROI T-978-1-4799, Feb 2014..

[4] Reza Fotohi "A New Approach for Improvement Security Against DoS attack in Vehicular Ad-Hoc Network " International journal of advanced computer science and application(IJACSA), Research Gate vol 7, no.7, 2016.

[5] Amarpreet Singh "A Novel Mechanism For Detecting DoS Attack In VANET By Using Enhanced Attacked Packet Detection Algorithm" IEEE Trans. 978-1-4673-8253-3, 2015.

[6] Karan Varma "Prevention of DoS attack in VANET" Springer Science, April 2013.

[7] P.Vijayakumar, M.Azees, A.Kannan, and L.Jegatha," Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks" IEEE Trans on intelligent trans.system, VOL. 17, NO. 4, APRIL 2016.

[8] K.Deepa Thilak,"DoS Attack on VANET Routing and possible defending solutions-A Survey," International Conference On Information Communication And Embedded System ICICES 2016

[9] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in Proc. IEEE INFOCOM, Anchorage, AK, USA, May 2007, pp. 103–108.

[10] Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," Vehicular Technology, IEEE transactions vol 56, no pp 3442-3456 ,2007.