Indian Journal of Science and Technology, Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/106794, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Enhancing the Message Authentication Process in VANET under High Traffic Condition using the PBAS Approach

Nitish Kumar Bharti* and Manoj Sindhwani

Electronics and Communication Engineering (ECE),Lovely Professional University, Phagwara – 144411, Punjab, India; nkb4521@gmail.com, manoj.16133@lpu.co.in

Abstract

The significance and popularity of VANET is increasing nowadays because of their great contribution in improving traffic efficiency and safety. We present an authentication and verification scheme of the Vehicular Ad-hoc Networks VANET for the low as well as high traffic conditions. However, communication between two or more vehicles or with RSUs needs to be secure as well as authenticated. In this paper we will discuss the Elliptic Curve Cryptography Algorithm (ECC) approach which uses the vehicle ID, a random generated prime number and time stamp to encrypt the message in a secure manner. Our main focus is to reduce the authentication time; therefore we have used the proxy vehicle which is verified by both RSU and CA and they will do half of the authentication process and decrease the authentication time. In this paper we have taken the parameters of packet loss, delay and throughput and compared the proposed approach for the low traffic conditions and also for high traffic conditions. So the result shows that the proposed scheme provides high quality of message authentications in less time period on both the traffic conditions without affecting the overall security of VANET.

Keywords: Certificate Authority (CA), Elliptic Curve Cryptography (ECC), Proxy Based Authentication Scheme (PBAS), Road Side Unit (RSU)

1. Introduction

A Vehicular Ad-hoc Network is a part of MANET. Both VANET and MANET belong to the family of the Wireless Ad-hoc Network. Ad-hoc means connections which are free to move. VANET is decentralized network means there is no third party which can control the network movement like we see in the mobile phones that they are controlled by a central authority. Mainly ISM band are used to establish the connection and transfer the data from one network to another network. VANET has three things they are vehicles, roadside unit and certificate authority all these things play their role in making VANET. In VANET cryptographic[1] security method play a vital role in securing the information which are being transferred. There are various cryptographic techniques which are useful in hiding the data in the network like FPGA[2]. Nowadays a hybrid multilevel security scheme is used like color code based on DNA computing and ECC[3]. VANET[4] has very precise applications in the field of MANETs such as traffic updates, police vehicles, fire vehicles and also used to lowering the telecommunication cost by establishing free voice over IP system like Global talk, Skype between a different user of another network[5].

1.1 Characteristics of Vehicular Network

The vehicular network has some special behaviour and characteristics, which distinguishing them from other types of network. As compared to other networks vehicular network has unique and attractive features given as follows:

· **Unlimited Transmission Power:** In the ad-hoc devices power issues is the main constraint but in the case of this network nodes/vehicle provide continuous power to computing and communication devices.

*Author for correspondence

· **Computational Capacity Increases:** As the vehicle spent time in the network it gets familiar with the network and this lead to the increase in the computational capacity of the network.

· **Predictable Mobility:** In the Mobile Ad-hoc Network where hard to predict the vehicle mobility, vehicles has very predictable movements that are limited to roadways. Roadways information is often available from positioning systems and map-based technologies such as GPS[6,7].

· **High Mobility:** Vehicular networks operate extremely dynamic with their limited configurations.

· **Partitioned Network:** The movement of the nodes in VANET is fast so sometimes it is seen that there is a disconnection in the network because of the more partitioned between the vehicles. So certain distance is decided above which vehicle cannot go therefore by this way partitioned between vehicle is avoided.

· **Network Topology and Connectivity:** The vehicular network environment changes from place to place because the network is totally based on real time scenario. When the vehicle moves and changes their position constantly in the dynamic scenarios. Network topologies change frequently as the link between the nodes connect and disconnect are very often

2. Related Work

VANET is a network of the wireless moving vehicle which communicate among them self and also with the infrastructure to provide safe traffic condition. VANET works on the wireless ISM band[8] i.e. IEEE 802.11p. The OBU is installed on the vehicles which help in communicating with the RSU. Traffic has increased on the road in the last few years, due to the lack of services and facility the congestion on the road has increased. Some researchers have shown in their paper that VANET plays a great role in minimizing the accident, transfer of warning message, provide infotainment.

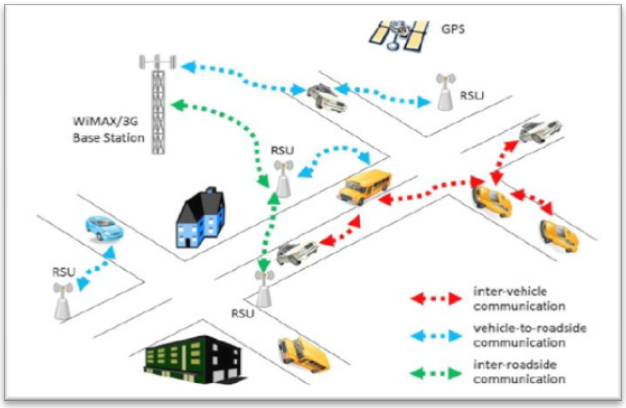

Figure 1. Architecture of VANET.

Security is an important factor in any of the communication network and CIA (Confidentiality, Integrity and Availability) play an important factor in VANET. Authentication is a vast process it deals with verifying the valid user and allows them to use the network safely. The main problem in authentication is the time which it takes at RSU for verification. There are many methods which can be used for the process. Security will secure the network all the time from the attacker so authentications play an initial role and it is very helpful in the security process. In[9] proposed various schemes for IEEE wireless Access point authentication and verification in VANET. The main contribution of their paper is to provide safety of verification of vehicular message and strategy for the road verification messages. A variation of Elliptic Curve Digital Signature Algorithm (ECDSA) is used in combination with the Identity-based (ID-based) signature and its current position information on a vehicle is utilized as the ID of the corresponding vehicle. This waives the need for a third-party public key certificate for message authentication in VANETs. To decimate the issue of the VANET, they have also used the double verification to cross check the security of messages.

Message authentication in-vehicle communication must be secure so[10] proposed the scheme called Elliptic Curve Digital Signature Algorithm ECDSA. The scheme works in the following ways; 1. Public and private keys are generated by the vehicle which is going to transfer the information i.e. source vehicle. 2. The public key is distributed throughout the network. 3. The secure hash algorithm is used to create the hash of the message to maintain the integrity of the message. 4. A high encryption method is used along with the private key of the sending vehicle and message is send to the destination node. 5. At the receiver side as the publically distributed key is used to decode the message sent by the sending node. 6. The destination vehicle generates the hash using the secure algorithm and compares it with the previously generated hash. The result of ECDSA algorithm is quite impressive because the key size generated by ECDSA[11] is less compared with RSA[12] and Diffie-Hellman[13].

In[14] proposed SOA i.e. Service Oriented Architecture. Vehicular Ad Hoc Network is mainly subpart of Mobile Ad Hoc Network. In this type of communication, vehicle

communicates among them and transfers the necessary information to other vehicles of a particular area; they communicate using wireless radio wave having high bandwidth. Now a day's popularity is gained by Vehicular Ad Hoc Network for their role in enhancing the safety and traffic efficiency, however, the communication among the vehicle node should be secure and authenticated. Message security is the great challenge in VANET SOA help in preventing the content of the message from the attacker. SOA has four steps they are, 1. Registration, in this registration of the vehicle is done. 2. Authentication, in this message, is send to RSU for verification of validity. 3. Privacy, in this data, is not leaked to the third party. 4. Updating, in this the whole data is updated in a given period of time. In this security is supported with the infrastructure which is well equipped with various security measures. SOA is complex because it combines many of the security aspects. Many of the services play their role in providing the best security. This type of idea may work well but problem comes when the complexity increases sometimes it may lead to the failure of the whole network.

In[15] proposed a scheme of group signature to improve the network security. In this method a group is chosen according to the nodes of that particular area and from that group, a Cluster Head (CH) has chosen the working of Cluster Head it to monitor the group and gather or send the information packet to all the nodes of that area. In group signature, the Cluster Head will contact with the RSU and all the necessary information of CH is verified by the RSU and then RSU will issue the signature or certificate to that verified vehicle. That generated certificate will act as a certificate for another vehicle of the area. This will increase the security of vehicle in network most of the vehicle are now authenticated by the RSU or by the group signature generated by the Cluster Head, to process the information in the safer way. One of the best approaches is ECDSA based authentication of the message in VANET. The operational approach is proposed for ECDSA scheme are:

- Source node as a vehicle generates an asymmetric private and public key.
- For all vehicles in VANET public key is shared in the network.
- Hash of the message is created by the source vehicle using secured hash algorithm.
- Generated hash message is encrypted by the private key and forward to the destination node.
- Destination vehicle decrypts the encrypted message using the public key and decryption results in a hash message.
- Similarly, destination vehicle node generates the hash message as same as source vehicle.

This approach provides the strong authentication policy for destination node because hash generates the unique message if the transmitted message is changed hash message would be changed.

3. Research Methodology

In the proposed approach we have compared the PBAS scheme for the traffic scenario of high traffic during rush hours with low traffic. In the whole process the proxy vehicle is chosen by the RSU of that area, proxy vehicle are those vehicle that spent most of the time in the area so that no time is wasted in again selecting the proxy vehicle. The vehicle registered ID is verified by RSU and CA after verification a UID is generated by the RSU and that UID is given to the proxy vehicle by encrypting the data. Some of the steps that are taken during authentication process and choosing the right proxy vehicle are given below:

- Initialization phase of vehicle. M = {ID, P, Ts}.
- M of the vehicle is encrypted with random seed and again encrypted with key of RSU. {e = E (M encrypted with seed), K}.
- Decrypting process is done at RSU by using the key.
- Verification is done by the RSU and CA.
- If request found genuine UID is provided to the proxy vehicle through secure medium.
- Now proxy vehicle can verify the message which is again checked by RSU.

Table 1. Notations

Component	Description
CA	Certificate Authority
p	Random Prime number
e	Encryption
d	Decryption
Ts	Timestamp
UID	Unique Identity
n	License/vehicle number
RSU	Road side Unit

Algorithm 1. Message authentication scheme in VANETs

1. Begin.
2. Vehicle input M = {Ts, N, P} (M = message Ts = time-stamp n = license/vehicle no. P = prime no.).
3. Perform encryption e = E (M, PURSU) (PURSU = public key of RSU).
4. Forward e to RSU.
5. RSU perform decryption d = D (e, PRRSU) (PRRSU = Private key of RSU).
6. Compare N with stored information in database.
7. If N is valid. Then,
8. Calculate MIRSU, generate UID.

(MIRSU = multiplicative inverse of Prime number calculate, P UID = Unique identifier).

9. Forward UID, MIRSU to user.

User computes MI U (MIU = calculate multiplicative inverse again at user side to compare).

If

10. MI RSU = MIU.

Then

11. Keep UID, determine maximum member of group (nodes under range of the RSU).
12. Compute group generator, assign group leader, vice leader (use cyclic group concept additive operation).
13. Generate member of group (use Euler totient).
14. Perform signing and verification.
15. End if.
16. Else.
17. Reject the request.
18. End if.
19. Else.
20. Reject the request, update CRL.
21. End.

4. Simulations and Results

Simulation of the VANET is done by using network simulator 2.35 version; we have analysed several network topologies to test the effectiveness and performance of the VANET. PBAS is used to reduce the load at RSU which will decrease the authentication time. We will see the parameters which are taken for generating the outcome. The VANET topology is shown is the Figure 2.

In the simulation, we have considered various parameters they are delay, throughput and packet loss.

In the proposed approach the proxy vehicle is chosen and due to which the work load at RSU is minimized and

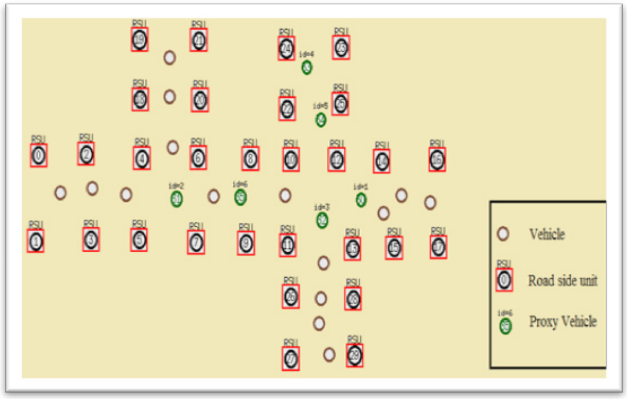

Figure 2. VANET network topology.

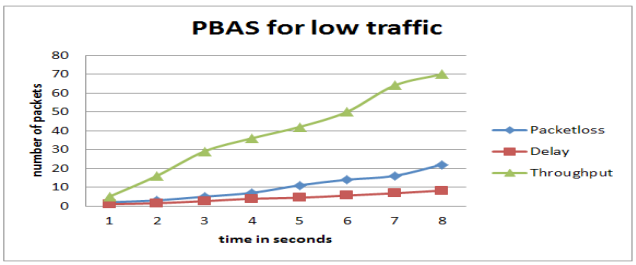

Figure 3. PBAS scheme for low traffic.

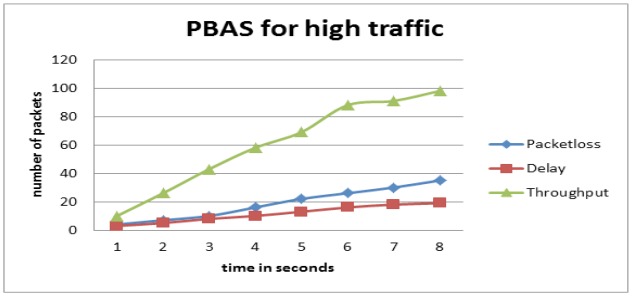

Figure 4. PBAS scheme for high traffic.

the time required for authentication is also minimized. The proposed approach is suitable for the low traffic because the packet loss and delay are low and the throughput of network is high.

The Figure 4 shows the result of the traffic during rush hours. The result is almost similar to the low traffic the throughput is high and the packet loss and delay are low therefore performance of our approach is stable for low as well as for high traffic.

5. Conclusion

The proposed scheme gives satisfactory results when the number of a vehicle approaching to RSU for authentica-

tion process is more. To authenticate the vehicle, vehicles provide its credentials to RSU or to valid proxy vehicle and credentials are verified, if it found genuine than access will be granted to the vehicle. In this mutual authentication along with PBAS based scheme has been proposed to provide a secure path for authentication and this will reduce delay, packet loss and all this lead to an increase in the throughput of the network. In this paper we have also analyses the traffic condition of vehicles during the low and high traffic. The result of message authentication is better than any other approaches used for authenticating the messages we have also used the ECDSA algorithm for the encryption and decryption of messages, using the proposed approach the overall security of the network increases.

6. References

1. Sasi SB, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015 Feb; 8(3). DOI: 10.17485/ijst/2015/v8i3/59585.
2. Thasneem Salim PT, Vigneswaran T. FPGA implementation of hiding information using cryptography. Indian Journal of Science and Technology. 2015 Aug; 8(18). DOI: 10.17485/ijst/2015/v8i19/76853.
3. Vijayakumar P, Indupriya S, Rajashree R. A hybrid multilevel security scheme using DNA computing based color code and elliptic curve cryptography. Indian Journal of Science and Technology. 2016 Mar; 9(10). DOI: 10.17485/ijst/2016/v9i10/88987.
4. Raya M, Hubaux JP. Vehicular Ad-hoc Networks. J Comput Security. 2007 Jan; 15(1):39–68.
5. Chim TW, Yiu SM, Hui LCK, Li VOK. VSPN: VANET-based Secure and Privacy-Preserving Navigation. IEEE Transactions on Computers. 2014 Feb; 63(2):510–24.
6. Huang JL, Yeh LY, Chien HY. ABAKA: An Anonymous Batch Authenticated and Key Agreement scheme for value-added services in Vehicular Ad-hoc Networks. IEEE Trans Vehicular Technology. 2011 Jan; 60(1):248–62.
7. Ganan C, Munoz JL, Esparza O, Mata-Diaz J, Alins J. PPREM: Privacy Preserving Revocation Mechanism for Vehicular Ad-hoc Networks. Computer Standards and Interfaces. 2014; 36(3):513–23.
8. Toor Y, et al. Vehicle Ad Hoc Networks: Applications and related technical issues. IEEE Communications Surveys and Tutorials. 2008; 10(3):74–88.
9. Biswas S, Misic J. A cross-layer approach to privacy-preserving authentication in wave-enabled vanets. IEEE Transactions on Vehicular Technology. 2013 Jun; 62(5):2182–92.
10. Manvi SS. Message authentication in Vehicular Ad-hoc Networks: ECDSA based approach. International Conference on Future Computer and Communication; 2009.
11. Chetan VS. Security framework for VANET for privacy preservation. IEEE Journal; 2013 Jul.
12. Sun Y, Lu R, Lin X, Shen X, Su J. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Transaction on Vehicular Technology. 2010; 59(1):3589–603.
13. Raya M, Papadimitratos P, Hubaux J. Securing vehicular communications. IEEE Wireless Communication. 2006; 13(1):8–15.
14. Lu R, Lin X, Zhu H, Ho PH, Shen X. ECPP: Efficient Conditional Privacy Preservation Protocol for secure vehicular communications. IEEE Infocom; 2008. p. 1229–37.
15. Mamun MSI. A multi-purpose group signature for vehicular network security. International Conference on Network-Based Information Systems; 2014 Sep.