Reduction of the Authentication Time using ECC and PBAS Approach in VANET

Nitish Kumar Bharti and Manoj Sindhwani*

Department of Electronics and Communication Engineering, Lovely Professional University, Jalandhar -144411, Punjab, India; nkb4521@gmail.com, manoj.16133@lpu.co.in

Abstract

VANET is subpart of MANET and the significance and popularity of VANET are increasing now a day because of their great contribution to improving traffic efficiency and safety. However, communication between two or more vehicles or with RSUs needs to be secured as well as authenticated. We have focused on to reduce the authentication time, that's why we used the proxy vehicle which is verified by both RSU and CA; proxy vehicle will do half of the authentication process and reduce the authentication time. The simulation results show that proposed approach minimizes the authentication time, delay, packet loss due to the collision of the packet in the network and also increase the overall throughput of the network. In this paper, we also discussed the Elliptic Curve Cryptography algorithm (ECC) approach which uses the vehicle ID, a randomly generated prime number and time stamp to encrypt the message in a secure manner. As a result the whole VANET network will be secured and faster in handling the congestion during peak hours.

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

1. Introduction

The Vehicular Ad-Hoc Network will be the best solutions for the traffic problem now a day's, as the number of accidents on the road is increasing rapidly in the last few years. VANET will surely minimize the challenge of road safety to a great extent. VANET is the efficient way of preventing accidents because it provides a platform for wireless radio network where vehicular nodes communicate among themselves and transfer the real scenario information of that area, which plays their role in developing a safe environment for driving. VANET has various parameters which make it a user-friendly, effortless and reliable network. The wireless network is completely mobile, it requires few infrastructures, help the applications in a random, dynamic along with multi-hop topology. VANET is a subpart of MANET but they have some characteristics which are different such as a frequent change in topology, limited bandwidth and energy is limited. Many times the cause of the accident is a lack of information about that area like traffic information, construction of roads, blockage of highway etc. So VANET provides this type of information to vehicles of another area by communicating using wireless radio wave of high bandwidth. Now a day's popularity is gained by vehicular



Figure 1. VANET architecture.

*Author for correspondence

ad hoc network for their role in enhancing the safety and traffic efficiency, however, the communication among the vehicle node must be secure and authenticated.

Therefore, security must have to play an important part in any of the networks to secure the information and also to run the network smoothly. VANET architecture is shown in Figure 1.

In VANET, the communication is mainly between two or more moving nodes called Vehicles to Vehicle (V2V), Vehicle to Infrastructure (V2I) and vice versa (I2V). The network topology of the network keep on changing in a frequent interval of time due to the high mobility of nodes, therefore, chances of an attacker to eavesdrop the information among the vehicle increases in an open source area. Due to the openness and high mobility of nodes in the network, malicious vehicles can join the network and broadcast false information message that could result in the collapse or problem in the network. On one hand, a vehicle needs to be authenticated while; it's private data like location and identity information must be kept secret and prevented from misuse. It is predicted that any insignificant behaviour of users such as changing the original information and various attacks on the important messages could be serious to other drivers. Furthermore, for any network conditional privacy preservation is an important aspect which must be achieved. The private information, including the maker, model, driver bio-data, speed, position, license plate and VIN of the vehicle, the route to be followed by the driver must be protected, while the authority may check the data of communicating user, this means non-repudiation of data must be achieved. Security plays an important role in any of the communication networks. We have discussed some of the paper which will give a brief idea about various authentication security and privacy scheme in VANETs.

1.1 Public Key Infrastructure (PKI) in VANET

This section will focus on the thing needed to secure the Vehicular Ad-Hoc Network against various attacks and threat. Any communication must be aimed to create a network that consists all these things they are authentication, authorization and accounting for providing a security in VANET. Communication to Road Side Unit (RSU) is important for VANET because vehicles need to go through the authentication process themselves to the nearest RSU for getting the verified certificates from CAs which helps in making a secure connection. In addition, the non-repudiation property which enables one of the important properties known as accountability of user actions is not provided by the symmetric cryptography. So, the use of public key cryptography is a safer and suitable option for deploying VANET security.

This signifies the demand of a Vehicular PKI (VPKI) where the Certificates Authorities (CAs) will provide a secure and certified private/public key pairs to the vehicle. If the CAs is from different area or region, they need to verify and cross check again by the CAs of that particular area before providing certificates to the new user. The advantages of using a Public Key Infrastructure in VANET security are having some challenging problems, especially, certificate revocation. The distribution of certificate revocation lists, which have the updated agreement of certificates is the best way to discard certificates (CRLs). There are many loopholes in this approach. First, due to the increase in the population of the vehicle, the size of CRL is maximized.

Second, a short lifetime period of certificates may create a vulnerable window. Last but not least, in the first years of deployment, there will be no noticeable of infrastructure.

1.2 Authentication

Authenticating the beginning of message packet is the fundamental security functions in VANET. The impersonation and changing the traffic condition, vulnerabilities property is counter by inherent integrity and authentication. The authorization level of the vehicles is also controlled through authentication. Various asymmetric techniques are used to authenticate vehicles to each other, vehicles will sign each message which they send with their own private key and attach the necessary certificates. Thus, when receiver vehicle receives the message, it compares the key used to sign the message and once this step is done correctly, it verifies the message. To minimize the security overhead, a common approach used are Elliptic Curve Cryptography (ECC) RSA and Diffie-Hillman, but the size of the key in (ECC) is less than Diffie-Hellman and RSA, therefore (ECC) is most compact and safe cryptographic mechanism.

1.3 Privacy

Privacy is also an important part of security system which must be achieved. Since the data which are

being exchanged in the network is important. So in this method, the message is encrypted and decrypted using the public and private key so the message cannot be modified by other users who are present in the network. There are various schemes in the literature that deal with the issue of conditional privacy preserving, security and authentication in VANET. Two most popular schemes can be broadly divided into two categories; 1. Group signature based schemes, 2. Pseudonymous authentication based scheme. Anonymous Public Key Infrastructure (PKI) based certificates are used by pseudonymous-based authentication schemes to check the messages signed by the associated unknown private keys.

These unknown certificates are related to some pseudo identity that is used to hide the actual identity of a vehicle. Security of network will focus on distributing various private keys and certificates. A vehicle chooses any of the private keys from the storage of keys to sign the message. By using unknown certificate, a receiver is able to cross-check and verifies the signature¹. This certificate hides and preserves the real identity of the sender as well as a receiver and achieves user privacy. The certification authority distributes the certificates and keeps the mapping, identity of certificates. Integrity of messages can be achieved by using hash chain to reduce the CRL size. The proxy re-signature technique is used to improve the certificates^{2.3}. Identity-based batch verification schemes can be used to decrease the authentication period. TPD is used to generate associated private keys and random pseudo identity-based certificates⁴. A scheme of conditional privacy preserving which generates less time pseudonym keys between RSUs and OBUs but the problem with this scheme is the assumption of more deployment of RSUs, otherwise no certificate will be updated⁵.

Group signature-based approaches are facing problem in group management and computations issues. Another problem is the requirement of fully trusted certification authorities and in some cases RSUs as well. The main idea behind the group signature-based authentication is to hide the real identity of group members which consist of communicating vehicles. Identity-based signature group signature and privacy preserving authentication scheme will also help in making the network secure^{6.7.} The concept of the group signature scheme is that the group member signs the message with the private keys which are communicating vehicles and is verified with the group public key[§]. RSUs uses Identity-based signature scheme to sign and authorize every message they produce to reduce signature overhead also CRL size of group signatures will also be reduced^{2.10}.

The disadvantage is that the computational cost increases because for each pairing calculation are required. A hybrid scheme is proposed by¹¹ which have the combined features of pseudonym-based approaches and group signature based approaches. This scheme is computationally not feasible as it needs to check if a message is from a revoked vehicle. Other vehicles and neighboring vehicle, verify the vehicle entering the group as a group member by verifying anonymous messages between Vehicle to Vehicle (V2V). In this scheme, the presence of numerous RSUs is there, these RSU shares the system loads so that there is no downfall in the performance. However, a very large number of RSUs deployments are required in the scheme that is the dark side of this scheme. Revocation issues, communication and long CRL12 computation are problems for Pseudonym-based approaches. For better solution VANET provides safety on roads, traffic management and providing a facility for driver and passengers. The topology of this network is changing rapidly so various malicious and security attack creates aproblem in practical implementation. Therefore, we need a high and secure authentication approach which can minimize the malicious attack and robust the network. One of the best approaches is ECDSA13 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. Requirement for VANET safety and security are message non-repudiation, authenticity, entity authentication, message confidentiality, integrity, access control, anonymity, privacy, availability and liability identification^{14–17}.

2. Research Methodology

Now we will discuss the flow diagram of proposed authentication scheme. The main aim is to reduce the authentication time during the authentication process when the traffic is high during the peak hours of the day. Authentication is an important process which a vehicle must have to undergo for using the network so that the network is secure. We will use the Elliptic Curve Cryptography along with the Vehicle ID and by making the combination of various random prime numbers which will act like as seed for encrypting the message of the vehicle the encryption is done by the public key and message is sent to the RSU. The RSU decrypt the message and verify the identity of the vehicle by using the data registered with CA and after verification, RSU will send the certificate to the vehicle by using a secure medium. After the first process registered a vehicle will act like a proxy RSU for the nearby vehicle.

If the quantity of the vehicle increases the RSU will make a more proxy vehicle that will provide authentication to the vehicle during rush hours, by this the load at RSU will be minimized. Since the load is minimized the collision of the packet in a network will be less therefore packet-loss and delay will decrease, so the throughput of overall network increases. Delay increases in the authentication of the message at RSU due to the increase in the number of the vehicle at the RSU of that coverage area. So proxy based authentication scheme is used which is also known as PBAS¹². Now we will discuss how the proxy vehicle helps in minimizing the workload of RSUs. In PBAS the proxy vehicle is used for authenticating the message of the nearby vehicles and that verified message are again sent to the nearest RSU of that area for cross verification and authentication permission, since most of the things are verified by the registered and secure proxy vehicle the authentication process at the upper level fasten up.

In proposed scheme we have modified the PBAS scheme, the proxy vehicle is chosen by the RSU of that area, the vehicle that spent most of their time on the network has the higher chance of becoming the proxy vehicle, so no time is wasted again in selecting the proxy vehicle. The vehicle registration is verified by RSU and CA. After verification the 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 the authentication process and for choosing the right proxy vehicle are given below:

- Initialization phase of the 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}.
- The 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.

The Figure 2 will give the brief idea how the proxy vehicle will execute the authentication process.



Figure 2. Proxy vehicle signature verification.

Figure 3 will show the flow diagram of proposed scheme.

Table 1 will give the detail of notations.

Component	Description
СА	Certificate Authority
р	Random Prime number
e	Encryption
d	Decryption
Ts	Timestamp
UID	Unique Identity
n	License / vehicle number
RSU	Roadside Unit



Figure 3. Flow diagram of proposed scheme.

Algorithm 1. Message authentication scheme in VANET

1. Begin

2. Vehicle input M = {Ts, N, P} (M = message, Ts = timestamp, N = license/vehicle no., P = prime no).

- **3.** Perform encryption e = E (M, Pu RSU). (Pu RSU = public key of RSU).
- 4. Forward e to RSU.

5. RSU perform decryption d = D (e, Pr RSU) (Pr RSU = Private key of RSU).

- 6. Compare N with stored information in database.
- 7. If N is valid.
- 8. Calculate MIRSU, generate UID.

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

9. Forward UID, MIRSU to user.

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

10. If 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 Eulertotient).

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.

3. Simulation and Results

Simulation of the VANET is done by using network simulator 2.35 versions. We have analysis of 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 discuss the parameters which are taken for generating the outcome. The VANET topology is shown is the Figure 4 and the network parameter are shown in Table 2.



Figure 4. Simulation topology.

We have taken traffic scenario of the metropolitan city where the numbers of the vehicles are high in an area, also a 1500 m \times 100 m bidirectional road with two lanes in each direction. Vehicle speeds vary from 80 km/h and sometimes reduced to 5 km/h. An RSU is installed at the roadside, whereas different numbers of OBUs are mounted with moving vehicles on the road.

Simulation Parameter	Simulation Information
Channel	Wireless Channel
Propagation Model	Two-Ray Ground Propagation
Antenna type	Omni-directional
Routing Protocol	AODV
Number of Nodes	38
Number of Sending Nodes	38
Number of Receiving Nodes	35
Simulation time	7.524 seconds

Table 2. Simulation parameters

In the simulation, we have considered various parameters. The parameter consists of delay, throughput, packet loss and routing overhead.

As the authentication time is minimized by using proposed scheme, the authentication process of messages has fastened up. Due to this, the delay in message delivery is less. Figure 5 shows that the delay of packet delivery using PBAS technique is 75% less as compared to and direct approach. This means that the time taken in the authentication process is less in PBAS approach.



Figure 5. Comparision of delay between PBAS and direct approach.

The congestion in the network decreases due to the division of workload at RSU by proxy vehicle, the packet

delivery ratio increases because the packet drop and expiry rate in the network are minimized, which lead to the increase in the throughput. The Figure 6 compares both the scheme and the throughput using PBAS approach is 64% higher than the direct approach technique.





Figure 6. Comparision of throughput between PBAS and direct approach.

Figure 7. Comparision of packet-loss between PBAS and direct approach.

Packet loss mainly occurs when the transmitted packet fails to reach the destination. The packet delivery ratio is high using proposed approach because throughput is high therefore the packet loss is minimized.

Figure 7 shows the comparison of PBAS and direct approach technique. In the PBAS technique, we use the

ID for verification of valid nodes and those nodes will provide the shortest and safe path for transmission of packets between vehicular nodes. So packet loss due to congestion and any other means decreases by 84% in the network by using PBAS technique instead of using the direct approach technique.

In the proposed approach the proxy vehicle spent their most of the time in their area. So there is less movement of vehicular nodes outside a particular area, therefore, the routing overhead is minimized. The Figure 8 compares both the techniques and the result shows the new routing overhead using PBAS approach is 82% less than the direct approach.



Figure 8. Comparision of routing overhead between PBAS and direct approach.

4. Conclusion

The Vehicular Ad-Hoc Network is the type of network in which multiple vehicles join or leave the network at the same time. Due to such configuration of the network, it is very difficult to maintain privacy or isolate security attacks in the network. To maintain privacy in the network, the vehicle needs to authenticate with the RSU and RSU will provide channel access to the vehicle. In the proposed work, secure authentication mechanism has been provided which can authenticate the vehicle in the minimum time. The proposed scheme gives satisfactory results when the number of a vehicle approaching to RSU for authentication process is more. During rush hours, RSU divide the authentication process with the valid proxy vehicle, by doing this load at RSU is reduced and the process of authentication is fastened. To authenticate the vehicle, vehicles provide its necessary certificates to RSU or to the valid proxy vehicle and these certificates 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. In future we will implement PBAS and security scheme using high clustering approach which can help the metropolitan area traffic for reducing the authentication time and increasing the throughput and security of overall network.

5. References

- 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):1–7.
- Sasi SB, Sivanandam N, Emeritus. A survey on cryptography using Optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015 Feb; 8(3):1–6.
- Parthasarathy MB, Srinivasan B. Increased security in image cryptography using wavelet transforms. Indian Journal of Science and Technology. 2015 Jun; 8(12):1–8.
- Amalarethinam DIG, Geetha JS, Mani K. Analysis and enhancement of speed in public key cryptography using message encoding algorithm. Indian Journal of Science and Technology. 2015 Jul; 8(16):1–7.
- Salim PTT, Vigneswaran T. FPGA implementation of hiding information using cryptography. Indian Journal of Science and Technology. 2015 Aug; 8(18):1–7.
- Raya M, Papadimitratos P, Hubaux PY. Securing vehicular communications. IEEE Wireless Communications. 2006; 13(5):8–15.
- Sun Y, Lu R, Lin X, Shen XS. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Transaction on Vehicular Technology. 2010; 59(1):3589–603.
- Zhang C, Lin, Lu R, Ho PH. An efficient message authentication scheme for vehicular communications. IEEE Transactions on Vehicular Technology. 2008; 57(6):3357– 68.
- Lin X, Lu R, Zhang C, Zhu H, Ho PH, Shen X. Security in Vehicular Ad Hoc Networks. IEEE Communication Magazine. 2008; 46(4):88–95.
- Lin X, Sun X, Ho PH, Shen X. A secure and privacy-preserving protocol for vehicular communications. IEEE Transaction on Vehicular Technology. 2007; 56(6):3442–56.
- Chaum D, van Heyst E. Group signatures. Processing of Advances in Cryptology – Eurocrypt.1991; 547:257–65.

- 12. Wasef A, Lu R, Lin X, Shen X. Complementing public key infrastructure to secure Vehicular Ad Hoc Networks security and privacy in emerging wireless networks. IEEE Wireless Communication. 2010 Oct; 17(5):22–8.
- Zhang C, Ho P, Tapolcai J. On batch verification with group testing for vehicular communications. Wireless Network. 2011; 17(8):1851–65.
- 14. Wasef A, Jiang Y, Shen X. DCS: An efficient Distributed Certificate-Service scheme for vehicular networks. IEEE Transactions. Vehicular Technology. 2010; 59(2):533–49.
- Hubaux JP, Capkun S, Luo H. The security and privacy of smart vehicles. IEEE Security and Privacy Magazine. 2004; 2(3):49–55.
- Raya M, Hubaux JP. Securing Vehicular Ad hoc Networks. Journal of Computer Security. 2007; 15(1):39–68.
- Yiliang L, et al. Message authentication using proxy vehicles in Vehicular Ad Hoc Networks. IEEE Transactions. 2015; 64(8):3697–710.