ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/107964, December 2016*

Signature based Authentication Scheme for Vehicle Ad-hoc Network

A. Aravind* and W. R. Helen

School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India;
aravind.3215@gmail.com, helen@cse.sastra.edu

Abstract

Objectives: To embed security inVehicle Ad-Hoc Network(VANET). **Methods**: Anonymous authentication is achieved using group signature. The current authentication scheme involves a long delay while searching for a particular certificate in the Certificate Revocation List (CRL) and the message security is not ensured. Hence the scheme will not meet the requirement of security in VANETs. **Findings**: In the proposed scheme, a general authentication scheme is constructed for Vehicular Ad-hoc Network (VANETs) to overcome the aforementioned problem. Road Side Unit (RSA) serves the purpose of allocating the generated public key to the vehicles who come within their communication range. HMAC is deployed to replace the time consuming CRL and the security of the message is ensured using cryptographic algorithm. **Application**: Vehicle to Vehicle, Vehicle to Road Side Unit.

Keywords: Certificate Revocation List, Hash Message Authentication Code, Mutual Authentication, Vehicle Ad-hoc Network

1. Introduction

The world is developing with a lot of intra communications, ad-hoc network and Internet. VANET's has made a large attractive attention from academia, industry and etc. Depending on the characteristics of Vehicle ad-hoc network, we need to improve driver's experience, message dissemination and passenger safety. VANET network is formed by combining all the vehicles through a wireless channel. Vehicle communications include vehicle to vehicle communication and vehicle to Road side Unit communication. VANET is different from the MANET by the following reasons like: VANET network is dynamic in nature, dense and sparse and radio communication range is limited. Apparently, widely varying mobility characteristics of mobile or vehicular nodes are expected to have a significant impact on the performance. VANET has characteristics like high node mobility and unbounded network size. VANET nature will create various types of attacks like node mobility of the victim is high, duplicate information and system is flooded. Various types of threats occur in VANET. Threats like node resources is consumed, broadcast tampering, reply attack and ID disclosure. Various requirements are needed for the security purposes. Requirements like message authentication, data integrity, non-repudiation, accountability, access control and privacy protection. VANET network needed to be made available in the real time application. If there is any delay in the transmission of the message, then the message is meaningless. Non-repudiation will identify the attacker. Accountability will provide facility for the entity identification in the communication. Information of the driver needs to be preserved from the unauthorized person. This type of information is achieved using temporary keys. All the keys will be stored in the vehicle. Key is reloaded ever time when the official checkup starts. In[1]

**Author for correspondence*

they talked about how to secure the communication among the vehicles using group. Main problem in the VANET is that message is tampered or duplicate message is sent from an unauthorized user. To overcome this problem, a general framework is constructed for securing the message transmission based on the group signature algorithm. Framework starts the process by generating public keys for the group. When a new member joins the group, the corresponding group public key is given to the new member also apart from the existing members. Message is signed by member using secret key and group manager in the group will determine the identity of the group members. When the message is sent from a sender, it's identity is checked by using access control list. If the message identity is not in the list, then the message is dropped. Firewall will block any unwanted message sent from a sender. Message signature is verified by using public key of the group members and authorization for the member is checked after the group is generated. In [2] they have suggested a general searching technique for reducing the delay while searching for a certificate in the Searching for a particular certificate in the Certificate Revocation List produces delay. In order to overcome this problem, a new searching technique is implemented. There are different phases in the framework. The framework works as follows: In the first phase, Trusted Authority will choose a random number and computes its public key. Secret key and its corresponding pseudo identity is chosen for the vehicle. In the message authentication phase, message is made secure using public key and secret key. Road side unit will verify the message by checking the certificate. If the certificate is valid, message is signed with a public key. In the revocation phase, secret key will update the certificate and signature of the road side unit in the message and the message is broadcast to all the vehicles. When the vehicles receive this message, they will verify the signature and certificate of the Road side unit. If the signature and certificate is valid, corresponding message is secured. The main advantage in this paper is various levels of security is improved and message loss ratio is reduced. The only disadvantage is that communication overhead is increased. In [3] they has established a general scheme for distributive cross layer. Main problem is that the security of the message is not ensured. To overcome this problem, a distributed broadcast function is implemented to give the highest priority based on their message services. Message service is classified into three levels of classes. Class one is given to emergency warning message. Class second is given to long range emergency notification message. Class third is given to periodic beacon message. Message priority will be always given to class one. One hop multi cycle broadcast is suitable for emergency warning message and multi hop one cycle broadcast is suitable for long range notification message. Counter is maintained. Depending on the message priority the velocity and position is calculated. Message is broadcast continuously. The main advantage is notification of the message is given to all the vehicles based on the message priority obtained. The disadvantage is that repetition of broadcast messages. A new scheme has been introduced for batch authentication[4]. The two major issues considered in VANET are privacy and communications among the vehicle need to be secured. To solve this issue, a general anonymous scheme was introduced. This scheme will authenticate various requests from various vehicles at the same time. Authentication of the vehicles is achieved by using pseudonyms. Illegal vehicle is removed by calculating hash message communication code and security of the message is ensured using batch authentication. Our scheme has better performance than previous scheme. Communication overhead is reduced. In [5] they have established a new scheme for VANET to be secured. Securing the VANET is an important condition to meet the requirement of the authentication. Some common aspect of communication is identified and threat model is removed. Finally, proposed scheme achieves robustness. Based on the result obtained from the existing scheme, solution will be applied to VANET because it gives a different nature to the vehicle ad-hoc network. A good example is digital signature which is the most suitable technique against their high overhead. Only advantage is message delivery ratio is reduced. Only disadvantage is overhead is increased. In has made an analysis on the game theory to identify the passengers or drivers for maintaining the privacy of drivers[6]. Generally, there are p players in the game model. Based on the strategy chosen from the user the player will play the games. The strategies are proof function, maximum like hood function, etc.

In proof function cost of the attack is determined, attack power is increased and cost of the implementing the user strategies are determined. Probability distribution is used to distribute the strategies to all the users. Maximum like hood function is used to find the probability in which the strategies are high. Maximum like hood estimation is used to find the minimum probability of the strategies. There are also two defensive strategies. Anonymous technique is used for hiding the user identity. Cloaking technique is used for user privacy. In [7,8] they have discussed how to secure the information for safety and traffic related application. The proposed protocol has three phases like registration phase, mutual authentication phase and central authority tracking phase. In the registration phase all the vehicles and the road side unit will register with the trusted authority. Secret key is calculated and their corresponding identity is sent to the trusted authority. All the identities are stored in the database. Trusted authority generates certificate for both the road side unit and vehicle. In the mutual authentication phase road side unit will initiate the authentication process by establishing a pair wise key between the road side unit and the vehicle. Road side unit will generate its private key, public key and sends this information to their corresponding vehicle. On receiving the information vehicle will valid the pair wise key. If key is validated then they will produce an encrypted certificate of the road side unit. In the central authority tracking phase each certificate that is generated during the mutual authentication phase is unique central authority will look into database to find the real identity of the vehicle.

2. Proposed System

A general authentication scheme for Vehicle ad-hoc network (Figure 1) underneath the semi-consider ver-

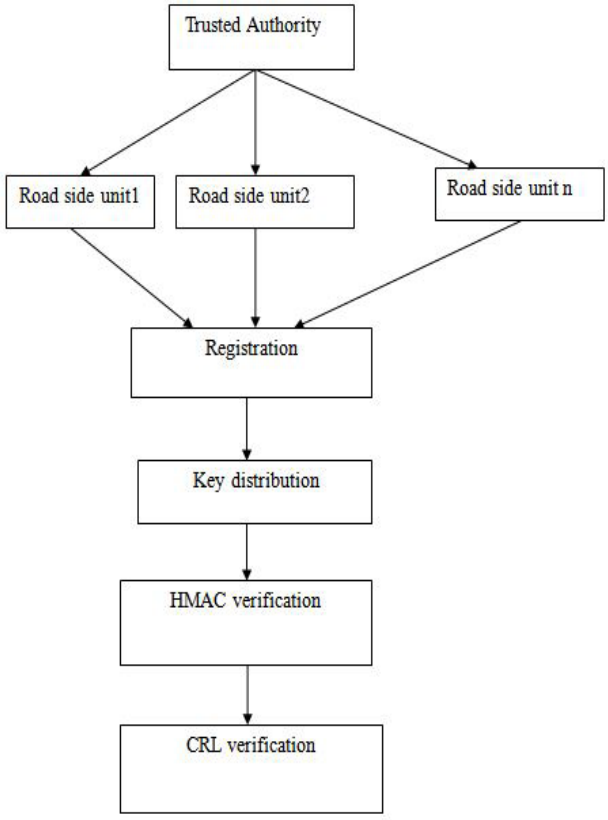

Figure 1. Proposed Architecture for VANET.

sion of Road side unit is proposed by collectively using the techniques of allotted management. HMAC value along with the organized key which is generated using hash-key algorithm, can update the time-eating CRL checking and make certain that message content is ensured. Authentication performance can be made better by using cooperative authentication. The proposed scheme includes trusted authority, constant road side unit at the road aspect, and mobile on board unit prepared in vehicle. Trusted authority is relied on management middle of the community. It affords registration and certification for vehicle and road side unit. It additionally divides an entire domain into small domain, in which a group key is generated for every domain and signature is issued for every domain. Road side unit control and talk with vehicles through their message exchange. They act as bridge between trusted authority and vehicles. Road side unit connects trusted authority using wired channel and vehicle by a WI-FI channel. In this scheme road side unit is made as semi-trust because they may reveal original information to an attacker. Road side unit generates a key, issues them to the vehicle and the vehicle is validated by their corresponding signature when the vehicle enters their respective domain. It consists of following manner: machine initiation, certificates issuing, secret key distribution, etc. Finally, message authentication will reduce message verification and extend the message velocity. In order to overcome the security leakage done by compromised RSU, a technique is contributed. Every vehicle gets individual credential information from TA during registration phase. Using the individual secret information, challenge response protocol is carried out in the case suspicious about way in which they act which is imposed by attacker vehicle. It is assumed that attacker is launching false event generation attack. In this attack, for instance attacker is reporting false information about vehicle traffic in which attacker lies about vehicle density in specific area. But originally there exists less number of vehicles in that area. This attack can be detected by the neighbors of the attacker vehicle. Once the suspicious activity is observed, vehicle's individual credential is verified through challenge response protocol. Attacker and compromised RSU can be detected easily during this process as attacker is unaware of individual credential of any vehicle.

2.1 Registration and Secure Group Key Distribution

Initially Trusted Authority computes its public key, private key, hash function as the system parameter. Trusted Authority divides the entire domain in to sub domains, each domain includes road side unit and Vehicles. In each domain, Trusted Authority generate public key and parameters. Trusted Authority transmits the public key parameters and public keys to all Road side unit in each domain. Vehicle enters a new domain to register at the RSU for preventing illegal vehicles from joining the domain. After the registration phase private and public key is given to the vehicle. In the certificate issuing phase one random number is chosen as private key and its corresponding public key will be calculated. Once the certificate is calculated it is issued to the road side unit and vehicle. Trusted Authority will create the signature and delivers the public key and certificate to the road side unit and the vehicle.

2.2 HMAC Verification

For improving the authentication efficiency Hash message authentication code checking is done before CRL checking. Message source is authenticated by verifying the HMAC value and the security of messages is achieved using a cryptographic key hash function. During the registration phase group seed will be calculated for all vehicles. All the valid vehicles will generate group key along with the group seeds. On receiving the group key each vehicle will attach hash message authentication code value, signature will be generated by using the group key. On receiving the message, message legitimacy is verified using HMAC in order to avoid overhead in the communication and storage. Message sender will not be known to the users and message signature will be created. On receiving the message digest value is calculated and sent along with the message from the sender. When the receiver receives the message it will verify the message digest value. If it is valid then it is considered as valid user.

2.3 CRL Verification

After the Hash message code verification Certificate Revocation List verification will be performed. Source and content of the message validity need to be checked so the receiver need to verify them. Invalid vehicles will be removed by checking in the certificate before authentication, however, it takes too much time to check one particular certificate in the CRL. On receiving the message from various revoked vehicles it will take time to verify all the source messages. Due to this reason delay is introduced during the CRL searching, hence greatly reduces system performance.

2.4 Security against RSU

In order to overcome the security leakage done by compromised RSU a technique is contributed. Every vehicle gets individual credential information from TA during registration phase. Using the individual secret information challenge response protocol is carried out in the case suspicious behavior imposed by attacker vehicle. It is assumed that attacker is launching false event generation attack. In this attack, for instance attacker is reporting false information about vehicle traffic in which attacker lies about vehicle density in specific area. But originally there exists less number of vehicles in that area. This attack can be detected by the neighbors of the attacker vehicle. Once the suspicious activity is observed, vehicle's individual credential is verified through challenge response protocol. Attacker and compromised RSU can be detected easily during this process as attacker is unaware of individual credential of any vehicle.

3. Performance and Result

This section focuses on the performance metrics and how the vehicles network is formed. The simulation work is done in Network Simulator version 2(NS-2). In the given graph as shown in the Figure 2, when the number of attackers increase, message delay is also increased, that is indicated by the red line in the existing system. Due to the searching of a certificate in the CRL. In the proposed system delay is decreased as indicated by the green line. Number of attackers increases Control packets also increased in Existing (CRL) scheme and proposed scheme the control packets are equal in the Figure 3.

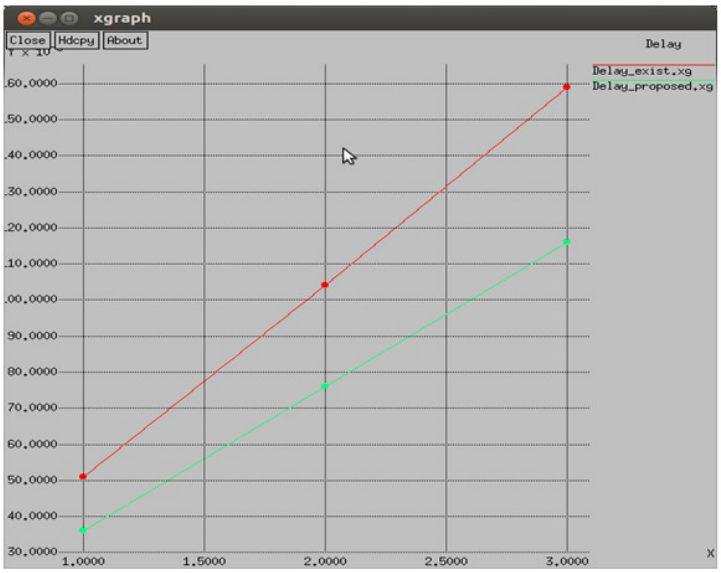

Figure 2. Performance delay.

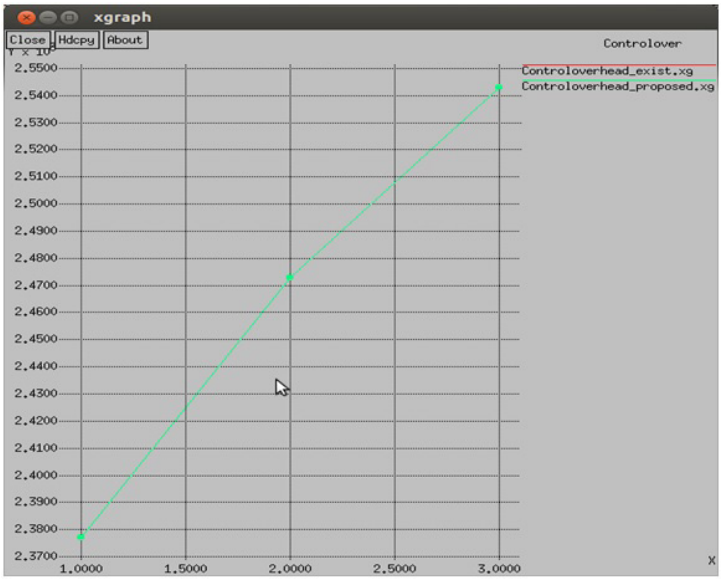

Figure 3. Control overhead.

4. Conclusion

The existing system involves a delay while searching for a particular certificate in the CRL and the security of the message is not ensured. A new signature authentication scheme is proposed using allocated management technique, HMAC and so on. The entire domain is split into a number of sub domains. RSU will broadcast the message to their respective vehicles. Hash Message Authentication code is deployed to replace the long checking CRL for reducing the delay and message security is ensured by using cryptographic algorithm. Using HMAC, delay is reduced and the performance is increased. Message content is secured by deploying cryptographic algorithms to vehicle ad-hoc network. Finally, the outcome will be more effective in terms of authentication speed and satisfy the security requirements of the VANET.

5. Acknowledgement

The authors wish to express their sincere thanks to the Department of Science & Technology, New Delhi, India (Project ID: SR/FST/ETI-371/2014) and SASTRA University, Thanjavur, India for extending the infrastructural support to carry out this work.

6. References

1. Guo J, Baugh JP, Wang S. A group signature based secure and privacy-preserving vehicular communication framework. Proceeding Mobile Network Vehicle Environment, Anchorage, AK, USA; 2007 May. p. 103–8.
2. Wasef A, Shen X. EMAP: Expedite Message Authentication Protocol for vehicular ad hoc networks. IEEE Transactions on Mobile Computing. 2013 Jan; 12(1):78–89.
3. Sun Y, Lu R, Lin X, Shen X, Su J. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Transactions on Vehicular Technology. 2010 Sep; 59(7):3589–603.
4. Zhang L, Wu Q, Solanas A, Domingo-Ferrer J. A scalable robust authentication protocol for secure vehicular communications. IEEE Transactions on Vehicular Technology. 2010 May; 59(4):1606–17.
5. Raya M, Hubaux JP. Securing vehicular ad hoc networks. Journal of Computer Security. 2007 Jan; 15(1):39–68.

6. Lee SB, Pan G, Park JS, Gerla M, Lu S. Secure incentives for commercial ad dissemination in vehicular networks. Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing USA; 2007. p. 150–9.
7. Zhang C, Lu R, Lin X, Ho PH, Shen X. An efficient identity based batch verification scheme for vehicular sensor networks. IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2008 Proceedings; 2008. p. 816–24.
8. Malik A, Pandey B. Performance analysis of various data collection schemes used in VANET. Indian Journal of Science and Technology. 2015 Jul; 8(15):1–8.