ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

Secure Message Authentication in VANET

[1] Vanashri G. Bhelawe, [2] Manoj M. Dongre
[1][2]Department of Electronics and Communication,
Ramrao Adik Institute of Technology, Nerul, Navi Mumbai

***Abstract*— As the use of modern technology has been used to a great extent in almost every section of engineering and almost every part of the day to day life, the advancencement in the automobile industries will help to gain more popularity and advantages while driving. Vehicular Adhoc network (VANET) is the new modified enhancement for vehicles which not only enhance the features of vehicle but also take care of the security, integrity issues face by the vehicle users. The proposed scheme will eliminate the undesirable activities of the malicious users to maintain the integrity of messages. The proposed method uses the token evidence method to eliminate the malicious activities. As number of road side units also affects the performance of VANET, we will increase their numbers according to traffic to get better result.**

***Keywords*—Trusted authority, Attacks in VANET, Authentication, Safety in VANET, End to End Delay, malicious attacks, Road side units.**

I. INTRODUCTION

As the wireless technology has become the integral part of our daily life, everyone has the availability of wireless network anywhere, anytime. VANET that is vehicular adhoc network deals with the facility that has been provided to vehicular adhoc network to enjoy the uninterrupted wireless network. To avail this facility the car manufacturing industries and telecommunication industries are coming together and enhancing the vehicle to equip it with the wireless technology. In this type of network the vehicles acts as a wireless router or wireless nodes with some specified range along with some road side infrastructure called as road side units forms a huge wireless network.

Such huge wireless networks containing cars with the communicating equipments and road side unit forms a network called vehicular adhoc network that is VANET. Different protocols have been used in VANET. In this network vehicles can also be able to communicate with each other through inter vehicular communication. Vehicular Adhoc network use Dedicated Short Range Communications (DSRC) technique to communicate with road side infrastructure.

Such vehicles are called as intelligent vehicles as they have on board units, which helps in establishing the wireless communication with other vehicles as well as other road side units. Such vehicular adhoc network facilitates vehicle users with enormous applications such as traffic warnings, accident warnings, sharing messages and any important data, etc. With the help of this, vehicle users also can ensure their safety while driving. In case of some emergency users can get alert about it, which can enable the vehicle users to act accordingly and can avoid such accidents. The VANET enables the vehicle and road side units

In the proposed paper, Section I is the introduction of the VANET technology and basics about the topic, in section II related work has been written from literature survey of the related topics. Design Methodology has been discussed in later in section III. The proposed method which uses Evidence Token Mechanism has been explained in section IV and the simulation and result has been described and shown in section V. The topic is concluded in the section VI.

II. LITERATURE SURVEY

To improve the purpose of the proposed method some schemes has been studied. Some of Which are based on traditional public key infrastructure (PKI) [6], [8] Method. Efficient protocol proposed by Zang et. al. [2] which was based on batch signature techniques to reduce message verification overhead. But unfortunately this system is vulnerable to DoS attacks. Fast symmetric cryptography also can be used but VANET is so dynamic in nature so this makes it challenging to apply. Proposed scheme is very efficient to this dynamic nature of VANET as it minimizes delay by transmitting and receiving messages to and from the user without involvement of any trusted authority.

III. DESIGN METHODOLOGY

Let there be 'n' number of vehicles communicating in the given range with other vehicles and with the road side units. Let 'r' be the range upto which a vehicle can communicate. Whenever any vehicle comes in the range of trusted authority, initially checking of authentication of the respective vehicle user undergo

All Rights Reserved © 2017 IJERECE

ISSN (Online) : 2394-6849
International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

verification. Once trusted authority done with the process of authentication check, the vehicle gets registered with the trusted authority. This registration allows the vehicle user to communicate further with other vehicles and with the road side infrastructure efficiently and securely.

Secure Cooperative Authentication Scheme:
This part concerns with the method to eliminate the malicious behavior of some vehicles. As in the network there may be a situation where some selfish users also present and disturbs the cooperative authentication. Such users can become a threat to the VANET security. For such user if any vehicle fails to generate the correct authentication key to the authorities, it will get less message authentication. Due to which they cannot take part in the communication process. As we are considering that the environment is highly dynamic that means as we are considering vehicles moving at a high speed on the busy roads or on the highways, the network stability is more concerned here in such case. Propagation delay for this process must be very small to provide uninterrupted service.

Non-cooperation Case:
This case concerned with vehicular adhoc network where vehicles will not cooperate for message authentications. Here when messages have been sent to the other vehicles. If the user has unique identity of its own but does not take part in the cooperative communication. In such vehicular adhoc networks if any users doesn't take part in the cooperative communication technique, in that case the when public messages are to be send to all then such users will not be able to receive that messages. This can led to the disturbance for the cooperative authentication process. We will not be able to get the desired outcome.

Cooperation Case:
This case is for the vehicles of cooperative case. When vehicles cooperate with the authentication process the communication becomes more convenient. The cooperative method for vehicles in VANET is given as follows:
On the basis of number of messages received vehicle authenticates randomly chosen signatures to communicate with the sender, road side unit or with other vehicles. Using such signatures they send messages back to the recipient that is to the proper destination. Corresponding user generates an integrated signature for the concern message and then sends the message with respective signature altogether with the indexes of the original messages they have to convey to other vehicles comes in the range of trusted authority. The vehicle user is then authenticates the other users integrated signatures. The vehicle users authenticates the signatures that should not been covered by the integrated signatures.

As given in above stages the vehicles will authenticate one signature per message. This type of method increases the computations overhead per message.
If the computation overhead is not reduced within two steps then more than one signature per message needs to be authenticated by trusted authority.

IV.EVIDENCE TOKEN MECHANISM

To achieve the secure authentication here we are introducing the method namely evidence-token mechanism. Evidence Token mechanism works on the principle that the vehicle must balance the timing allotted to them to give maximum throughput, so that utilize the given time slot wisely and economically. In this the time slots are to be given to each vehicle, so that it will communicate in a given time.

The Trusted authority will be responsible for the time allocation and its maintenance. The tokens are allotted by trusted authority to the vehicle users when any user passes by its coverage area and evidences from the users are also collected by trusted authority via the road side units. If TA finds the evidences are real then it will issue token to the vehicles according to their past history of authentication efforts.

The evidences used for vehicles are used only once and are not repeated. In order to verify the identity of users the trusted authority will generate the tokens and also distribute them among the users.

Initially we will consider how secure cooperative authentication can be done. To achieve this kind of communication securely the need of elimination of malicious users is necessary. Such malicious users can be caught by trusted authority while checking the authentication of vehicles. In such checking if any of the user fails to give their real authentication to trusted authority then such users are identified as malicious user as they try to break the secure communication also can becomes the threat to secure communication process. Such malicious nodes are also try to steal the data and also try to duplicate the data transferred during vehicle to vehicle communication.

Also it has been seen that if the vehicle users shows the authentication then it can get more message authentication by authority. In case if the vehicle fails to do so, the vehicle gets less authentication. As VANET is highly dynamic environments the pseudonym needs to assign to the vehicles for security reasons. To eliminate the selfish behavior of malicious

All Rights Reserved © 2017 IJERECE

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 4, Issue 4, April 2017

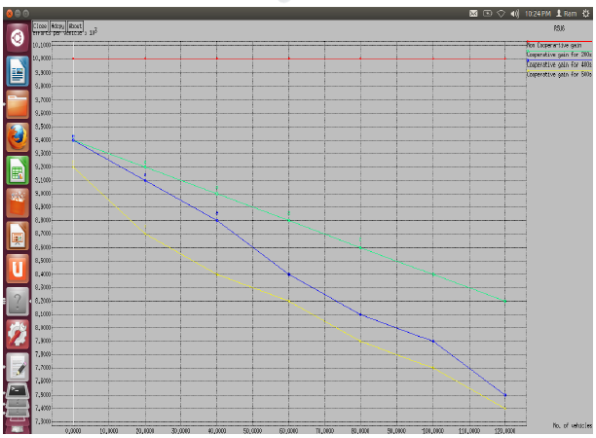
users we will use this secure method of cooperative authentication scheme.

To overcome the defects in the communication, we will use evidence token scheme and signocryption scheme based on identity. The proposed scheme of secure cooperative authentication in vehicle to vehicle communication gives the secure environment to the vehicles. As we have use extra proof regarding the identity of user to check that the messages sent by them are original or not for the authentication process.

IV.SIMULATION RESULT

In this paper, the performance of network parameters such as Throughput ratio and cooperative gain of both the proposed method and existing method are plotted in the graph. In our proposed method, the performance of these parameters are similar to existing method till certain point of transmission time and when the transmission time increases the proposed method overcomes the existing method.

To get the desired simulation result we consider various number of vehicles in area say around 8 to10 km. Let us consider that vehicle user can communicate within the range of transmission of around 500m into its surrounding environment. The vehicles we consider here are equipped with the on board units which are useful. Certain numbers of road side units have been setup at a distance of 1kms apart. After this setup we will study the performance and accordingly evaluate the required outcomes by taking the group of road side units consisting of four RSUs, 6 RSUs, and 10 RSUs. We have considered here the case of six road side units that is 6 RSUs for evaluation.



Cooperative gain for 6 RSUs

Table 1
Cooperative gain for 6 RSUs

No. of vehicles	Non cooperative gain (%)	Cooperative gain (%)		
		200s	400s	500s
20	100	94	93	90
40	100	91	87	83
100	100	88	85	75
120	100	84	72	68

The gain for the given setup is cooperative gain as while packet transmission we will consider malicious users also for security purpose. Whereas in non cooperative case, packets are sent as much as users are available in the network results in 100% gain. This non cooperative case the security is not considered. On the other hand in later case, the cooperative case, and the transmission of packets done only after security check. In this if any vehicle is found to be malicious, the packet from such users gets dropped and no information exchange done with that user.

V.CONCLUSION

The result confirms that the proposed scheme can achieve the message authentication securely as well as effectively. Whereas the cooperative gain in the simulation results shows that the proposed scheme can reduces the computational overhead on vehicle users for authenticating signatures and allow the users to communicate directly which led to reduction of time delay. This facilitates the Trusted Authority to keep track of malicious activities efficiently and eliminates the external and internal attacks by such malicious users. The cooperative gain has been calculated and improves by using different values of token time allotted to each of the vehicle user. Here in output graph cooperative gain for 200sec, 400sec and 500 sec has been calculated by using 8 and 10 road side unit. The trusted authority and road side infrastructure collectively gives specific time period to the vehicle users. By this procedure the vehicle users can be controlled by the road side infrastructure. The simulation results shows that the computational overhead has been reduced to some extent. Thus we can achieve secure communication within the vehicular adhoc network. Also malicious users can be eliminated significantly and cooperative communication can be achieved

All Rights Reserved © 2017 IJERECE

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

REFERNCES

[1] Xiaodong Lin, Senior Member, IEEE, and Xu Li "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks" IEEE Transactions on Vehicular Technology, vol. xx, no. xx, March 2013.

[2] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," In Proc. of the 27th IEEE nternational Conference on Computer Communications pp. 246?50, Phoenix, Arizona, USA, 2008.

[3] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442?456, NOVEMBER 2007.

[4] X. Liang, R. Lu, X. Lin, and X. Shen, "PPC: Privacy-preserving chatting in vehicular peer-to-peer networks," In Proc. of the 72nd IEEE Vehicular Technology Conference (VTC2010-Fall), pp. 1-5, Ottawa, Canada, 2010.

[5] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007.

[6] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs,"IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp.616?29, 2011.

[7] U.S. Department of Transportation, "National highway traffic safety administration," In Veh. Safety Commun.Project, Final Report. Appendix H: WAVE/DSRC Security, Apr. 2006.

[8] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," IEEE Transaction on Wireless Communications, vol. 7, no. 12, DECEMBER 2008.

[9] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An Efficient RSUaided Message Authentication Scheme in Vehicular Communication Networks," In Proc. of IEEE International Conference on Communications (ICC), Beijing, China, May 2008.

[10] X. Lin, "Secure and Privacy-Preserving Vehicular Communications," PhD Thesis, University of Waterloo, Canada. 2008.

[11] J. Freudiger, M. H. Manshaei, J. P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in Proc. of ACM Conference on Computer and Communications Security, 2009, pp. 324–337.

[12] W. Susilo, F. Zhang, and Y. Mu, "Identity-based strong designated verifier signature schemes," in Proc. of the 9th Australasian Conference on Information Security and Privacy (ACISP), Sydney, Australia, pp. 313–324, 2004.

[13] M. Slavik and I. Mahgoub, Stochastic broadcast for VANET, in Proc. 7th IEEE CCNC, Las Vegas, NV, Jan. 2010, pp. 15.

[14] Y. Bi, L. Cai, X. Shen, and H. Zhao, A cross layer broadcast protocol for multihop emergency message dissemination in inter-vehicle communication, in Proc. IEEE ICC, May 2010, pp. 15.

[15]N. Mariyasagayam, H. Menouar, and M. Lenardi, An adaptive forwarding mechanism for data dissemination in vehicular networks, in Proc. IEEE VNC, Tokyo, Japan, Oct.
2009, pp. 15.

[16]A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," J. Commun. Netw., vol. 11, no. 6, pp. 574–588, 2009.

[17] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux Antonio Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," VANET'07, 10 September, (2007).

[18] P. Golle, D. Greene and J. Staddon, Detecting and correcting malicious data in VANETs, in: Proceedings of VANET'04, 2004, pp. 29–37.

[19] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, M. Raya "Architecture for Secure and Private Vehicular Communications'' in Telecommunications, ITS, vol.5, no.6, pp.1-6, June/July 2007.

All Rights Reserved © 2017 IJERECE

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

[20] L.Butty , T.Holczer, I.Vajda,"On the effectiveness of changing pseudonyms to provide location privacy in VANETs"In Proc.of Privacy in Ad hoc and Sensor Networks (ESAS 2007).

All Rights Reserved © 2017 IJERECE