ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Survey on Various Security Schemes in Vehicular Ad hoc Network

Godavari H. Kudlikar, Uma Nagaraj

M.E Student, Dept. of Computer., MIT Academy of Engineering., Pune University, India

Professor & Head, Dept. of Computer Engineering, MIT Academy of Engineering., Pune University, India

ABSTRACT: In vehicular ad-hoc networks for authentication Public Key Infrastructure (PKI) was used as Vehicular Signature application. PKI is used to verify the integrity of messages and the identity of message senders. Road Side Unit (RSU) verifies received messages one after another, it may not be able to be predicted and known by RSU i.e. from which vehicle message is being sent. In order to reduce the computational overhead of RSUs, we propose a Proxy Based Authentication Scheme (PBAS) using distributed computing. In PBAS, proxy vehicles are used to authenticate multiple messages with a verification function at the same time, so that RSU can independently verify the outputs given by each proxy vehicles within its range. We also design an expedite key negotiation scheme for transmitting sensitive messages.

KEYWORDS: Vehicular ad-hoc network; Proxy vehicle; Proxy based authentication scheme; Key negotiation; Privacy preservation; Vehicular ad-hoc network.

I. INTRODUCTION

Vehicular ad hoc network (VANET) has becomes increasingly popular concept in many countries. It is an important element of the Intelligent Transportation Systems (ITSs). In a typical VANET, each vehicle is assumed to have an on-board unit (OBU) and road-side units (RSU) installed along the roads. A trusted authority (TA) and some other application servers are installed in the backend. Communication between OBUs and RSUs is done using Dedicated Short Range Communications (DSRC) protocol using wireless channel. RSUs, TA, and the application servers communicate with each other using a secure fixed network such as the Internet.

VANET offers better driving experience and road safety, as well as many other value-added services. The basic application of a VANET is to allow arbitrary vehicles to broadcast safety messages, message contains information like vehicular speed, turning direction, traffic accident information to other nearby vehicles. This type of communication is called as vehicle2vehicle or V2V communications and communication between vehicle and RSUs is known as vehicle2infrastructure or V2I communications. VANET can also be called as a sensor network because useful information about road conditions from vehicles can be collected by the traffic control center or some other central servers.

Many forms of attacks against VANETs have risen recently that attempt to compromise the security of such networks. Security issue [3] [4] is critical in VANETs because many different forms of attacks [3] against VANETs may emerge due to the use of wireless devices in VANET communications. Such security attacks on VANETs may lead to drastic results such as the loss of lives or loss of revenue for those value-added services. Therefore the key objective of designer is to make VANET secure.

II. RELATED WORK

There are some security schemes which have been proposed in this literature as an effort to ensure that all information exchanged in VANETs is authenticated and thus can be fully trusted.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A. Public-Key Infrastructure (PKI) based scheme

Public-Key Infrastructure (PKI) based scheme is used for vehicular signature applications [1], where an RSU verifies received messages one after another. Vehicles forward messages at any time, it may not be able to be predicted and known by RSU. And this PKI-based scheme are time-consuming processes and may not satisfy the computational efficiency requirement under dynamic traffic patterns, and due to this computational complexity and transmission overhead of RSUs increases as the number of vehicles are increased for authentication.

Zhang et al. in [7] published and introduced an efficient batch signature verification scheme for the communications between vehicles and RSUs in which an RSU can verify multiple received signatures at the same time such that the total time required for verification can be significantly reduced. In their proposed scheme it is seen that an RSU can simultaneously verify about 1600 messages per second, which is not bad but still not fast enough to meet the requirement of VANET authentication speed.

According to the Dedicated Short Range Communication (DSRC) protocol in [8] [9], each vehicle broadcasts a traffic safety message after every 100-300ms. This implies that an RSU must verify around 2500-5000 messages per second if we consider number of vehicles to be around 500 vehicles within the coverage of an RSU. This is considered to be a great challenge for any current batch-based digital signature scheme mentioned in the literature [10] [11] [12] [13].

B. Elliptic Curve Digital Signature Algorithm (ECDSA)

In vehicular communication messages can be authenticated using the Elliptic Curve Digital Signature Algorithm (ECDSA) were each message includes one certificate. A major challenge is to find a way to reduce the consumption of resource in computation and transmission. As such ECDSA provides better security, verify authenticity, non-repudiation but still it does not facets to security attack. Another problem with using ECDSA is that it uses most expensive operation such as scalar multiplication or elliptic curve point multiplication [9]. Expensive operation includes modular inversion operation, scalar multiplication operation scalar multiplication operations. In fact the most time consuming operation in ECDSA is the elliptic curve scalar multiplication operation.

Some of the limitations of using this scheme are

- Message Delay
- Message Loss Rate

C. Identity-based Batch signature Verification (IBV) scheme

For verifying signature in VANETs Batch verification offers an efficient. Zhang et al. [7] introduced an Identity-based Batch signature Verification (IBV) scheme for communication between vehicle and RSUs called vehicular-to-infrastructure (V2I) communications, working is based on identity-based encryption algorithms [17] [18] which was proposed by Boneh et al. In this scheme an RSU can verify multiple received signatures simultaneously at the same time such that the time required for computation can be significantly reduced. For verification process the certificates are not required, due to this the transmission overhead can be reduced. Conditional privacy preservation can be achieved using pseudo identities, and Trust Authority (TA) is capable of tracing a real identity of vehicle from its pseudo identity.

In [19], Zhang et al. enhancement of IBV scheme is being done by adopting a group testing technique. The main objective of using this group testing is to find invalid signatures with a minimal batch verification workload

Limitation of using this scheme is

- IBV may suffer from replay attacks.

D. Anonymous Batch Authenticated and Key Agreement (ABAKA)

Huang et al. in [10] proposed an Anonymous Batch Authenticated and Key Agreement (ABAKA) scheme, this scheme is proposed for different value added services. Messages sent from different vehicle are authenticated and session keys are established at the same time. The security of the ABAKA scheme is determined based on ECDSA. If we compare basic ECDSA scheme with ABAKA scheme, relatively short signatures are adopted by the ABAKA scheme thus it reduces the computational and transmission overheads of RSUs.

In the future work to gain more efficiency some of the features of VANETs such as mobility model,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

preditable routing to be considered to design novel scheme.

E. Secure and Privacy Enhancing Communications Scheme (SPECS)

Chim et al. in [20] introduced a Secure and Privacy Enhancing Communications Scheme (SPECS), here in this scheme after batch authentication any vehicle can form a group with the other vehicles and can communicate with one another securely without RSUs. It is the first scheme to propose group communication protocol to allow vehicles to securely communicate with other vehicles in a group after authentication.

However, in [11], Shi-Jinn Horng et al. found out that SPECS does not works properly to impersonation attacks, and a malicious vehicle can act as an real entity vehicle to broadcast fake messages or even force another group member to send fake messages securely among themselves.

limitation of SPECS scheme is

- Impersonation Attacks

To overcome this weakness of SPECS scheme Shi-Jinn Horng in [11] proposed b-SPECS+ scheme. It satisfy a variety of security requirements and withstand the weaknesses of the impersonation attack under certain assumptions like TA is always online, the redundant TA should avoid being a bottleneck or a single point of failure. Network model for this scheme is as shown in fig

In future some of the challenges of VANET such as insider attacks can be addressed to avoid packet collisions between RSU and all vehicles within its range.

F. Conditional Privacy Preserving Authentication Scheme

Shim et al. in [12] proposed a scheme, here in this scheme pseudo identity based signatures is used for secure vehicle-to-infrastructure communications in VANET. Conditional privacy preservation is achieved were each message is mapped to distinct pseudo-identity, Trust authority is responsible for retrieving real identity of a vehicle from pseudo-identity. RSU verifies multiple received signatures thus reducing total verification time.

Main contribution in this paper is identity based signature (IBS) scheme under computational DiffeHellman (CDH) assumption. This scheme uses general hash functions, instead of using an inefficient special function known as the MapToPoint function. And after that a secure conditional privacy-preserving authentication scheme (CPAS) is constructed for secure V2I communications using a pseudo-IBS scheme to keep a balance between privacy and traceability achieving anonymous authentication, traceability, message integrity and unlink-ability. CPAS scheme supports the fastest batch verification process at the RSUs, such that the time for verifying 750 signatures simultaneously at the same time is less than 300 ms.

Future scope of this paper will extend the challenges to V2V communication and conduct more performance evaluation on message delay and message loss ratio in V2V communication. Also the evaluation of CPAS on a large-scale VANET testbeds with varying vehicle mobility models can be conducted.

In future some of the challenges of VANET such as insider attacks can be addressed to avoid packet collisions between RSU and all vehicles within its range.

G. Conditional Privacy Preserving Authentication Scheme

Shim et al. in [12] proposed a scheme, here in this scheme pseudo identity based signatures is used for secure vehicle-to-infrastructure communications in VANET. Conditional privacy preservation is achieved were each message is mapped to distinct pseudo-identity, Trust authority is responsible for retrieving real identity of a vehicle from pseudo-identity. RSU verifies multiple received signatures thus reducing total verification time.

Main contribution in this paper is identity based signature (IBS) scheme under computational DiffeHellman (CDH) assumption. This scheme uses general hash functions, instead of using an inefficient special function known as the MapToPoint function. And after that a secure conditional privacy-preserving authentication scheme (CPAS) is constructed for secure V2I communications using a pseudo-IBS scheme to keep a balance between privacy and traceability achieving anonymous authentication, traceability, message integrity and unlink-ability. CPAS scheme supports the fastest batch

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

verification process at the RSUs, such that the time for verifying 750 signatures simultaneously at the same time is less than 300 ms.

Future scope of this paper will extend the challenges to V2V communication and conduct more performance evaluation on message delay and message loss ratio in V2V communication. Also the evaluation of CPAS on a large-scale VANET testbeds with varying vehicle mobility models can be conducted.

H. Expedite Message Authentication Protocol (EMAP)

In order to ensure reliable operation of VANETs and to increase the amount of information gained from the received messages which are authenticated, job of OBU is to regularly check the revocation status of all the received certificates in a timely manner. By doing this, authentic delay is caused due to checking the Certificate Revocation List(CRL) for each received certificate. So Albert et al. in their work [5] introduced an protocol called expedite message authentication protocol (EMAP) which replaces the CRL checking process. This is done by an efficient revocation checking process using a fast and secure HMAC (Hash Message Authentication Code) function. Advantage of using this protocol is that it is not only suitable for VANETs but it can be applied to any network employing a PKI system. The is an alternative to CLR checking and is the first solution to reduce the authentication delay resulting from CRL checking in VANETs.

Working of this protocol is that the revocation check process is done using a keyed Hash Message Authentication Code i.e. HMAC, here in this process key used in calculating the HMAC is shared only between non-revoked On-Board Units (OBUs). Additional feature of EMAP is that it uses a novel probabilistic key distribution, where a secret key is shared securely and updated by non-revoked OBUs. Advantage of using this protocol is that it can significantly decrease the message loss ratio caused due to the message verification delay as compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation, it is concluded that EMAP is demonstrated to be secure and efficient protocol.

III. PROPOSED SYSTEM

Some security schemes such as Public key infrastructure (PKI) have been proposed for vehicular signature applications [1] to ensure information exchanged is authenticated and fully trusted. Here message sent by Road Side Unit(RSU) is verified one after another. These scheme are time consuming and fails to satisfy computational efficiency.

To overcome this problem Zhang et al. [22] introduced an efficient batch signature verification scheme for communication, in this scheme multiple messages can be verified simultaneously. But it does not meet VANET authentication speed. According to the Dedicated Short Range Communications (DSRC) protocol [8] [9], RSU must verify around 2500-5000 message per sec if vehicle broadcasts messages after every 100-300ms which is a great challenge for any current batch-based digital signature scheme.

In order to tackle the above mentioned efficiency problem of the existing authentication schemes we propose a Proxy Based Authentication Scheme (PBAS) for this purpose.

Proposed system consist of vehicles, proxy vehicles, RSUs were each proxy vehicle plays an important role in authenticating multiple messages simultaneously using verification function at the same time. After verification of message done by proxy vehicles, results are sent to RSUs for verification of signature. Using this concept the time-consuming centralized computing loads at RSUs can be reduced. This is done by a systematic and independent mechanism designed for RSUs to verify the output of the verification function given from different proxy vehicles, by which an RSU can evaluate the validity levels of different messages given by proxy vehicle in the same way as done in separate verification schemes as shown in fig. 1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

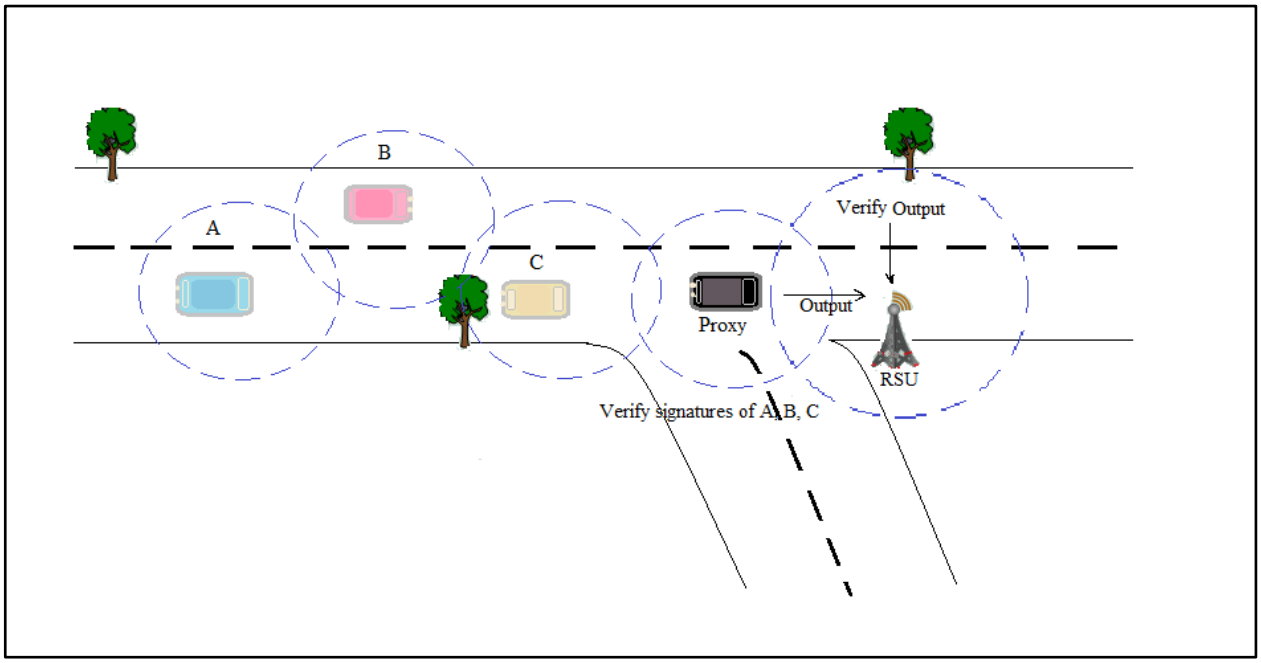

Fig. 1. General Scenario of PBAS

In this proposed Proxy Based Authentication scheme(PBAS) computational load of RSUs is reduced via the cooperation amongst proxy vehicles, where each proxy vehicle verifies the signatures of vehicle A, B, and C with a verification function, and then it sends its output to nearby RSU. After getting the results of proxy vehicles RSU verifies the output, thus consuming less computing resource. Here verification functions perform cryptographic operations in an authentication scheme, and these operations are executed using traditional authentication schemes by RSUs.

In addition to this, concept of batch key negotiations can also be added in the proposed scheme where, RSU can complete the batch process of vehicle's key negotiations by broadcasting a single message to all vehicles in RSU range.

Some of the design requirements of the proposed PBAS are as follows:

1. The scheme should meet the computational efficiency requirements of VANETs.
2. The scheme should meet the security requirements of VANET, such as message integrity and authentication, privacy preservation.
3. The scheme should verify process even if small number of proxy vehicles have been compromised.

IV. CONCLUSION

In PBAS burden of RSUs is reduced if we use vehicles computational capacity, where the proxy vehicles can authenticate multiple messages from the other vehicles. PBAS also provides RSUs with a systematic and independent mechanism to verify the messages from the proxy vehicles. PBAS offers fault tolerance i.e. even if a small number of proxy vehicles are compromised in VANETs the scheme continue operating. Moreover, we analyzed and compared the performance of PBAS with the other authentication schemes in terms of their computation and transmission overheads. We also used simulations to verify the efficiency of PBAS in realistic environments, showing that PBAS is a promising security scheme for efficient VANET authentication. We focused on cryptography algorithm under an assumption that any vehicle having completed system initialization can act as a proxy vehicle. However, it is important to make sure that these vehicles are fully trusted to serve for the others under the condition of efficient message delivery.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

REFERENCES

1. Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN: VANET-Based Secure and Privacy Preserving Navigation," inComputers, IEEE Transactions on, vol.63, no.2, pp.510-524, Feb. 2014
2. Xiaoyan Zhu; Shunrong Jiang; Liangmin Wang; Hui Li, "E_cient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks," inVehicular Technology, IEEE Transactions on, vol.63, no.2, pp.907-919, Feb. 2014
3. Richard Gilles Engoulou, Martine Bellache, Samuel Pierre, Alejandro Quintero VANET security surveys, in Computer Communications, vol.44, pp 113, May 2014
4. Lamba S; Sharma M., "An E_cient Elliptic Curve Digital Signature Algorithm (ECDSA)," in Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on , vol., no., pp.179-183, 21-23 Dec. 2013
5. Wasef, A.; Xuemin Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks," inMobile Computing, IEEE Transactions on, vol.12, no.1, pp.78-89, Jan. 2013
6. Xiaodong Lin; Xu Li, "Achieving E_cient Cooperative Message Authentication in Vehicular Ad Hoc Networks," inVehicular Technology, IEEE Transactions on, vol.62, no.7, pp.3339-3348, Sept. 2013
7. Shi-Jinn Horng; Shiang-Feng Tzeng; Yi Pan; Pingzhi Fan; Xian Wang; Tianrui Li; Khan, M.K., "b-SPECS+: Batch Veri_cation for Secure Pseudonymous Authentication in VANET," inInformation Forensics and Security, IEEE Transactions on, vol.8, no.11, pp.1860-1875, Nov. 2013
8. IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," inIEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006), vol., no., pp.1-289, April 26 2013
9. Rongxing Lu; Xiaodong Lin; Zhiguo Shi; Shen, X.S., "A Lightweight Conditional Privacy Preservation Protocol for Vehicular Tra_c-Monitoring Systems," inIntelligent Systems, IEEE, vol.28, no.3, pp.62-65, May-June 2013
10. Dietzel, S.; Petit, J.; Heijenk, G.; Kargl, F., "Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols," inVehicular Technology, IEEE Transactions on, vol.62, no.4, pp.1505-1518, May 2013
11. Xiaojun Li; Liangmin Wang, "A Rapid Certi_cation Protocol from Bilinear Pairings for Vehicular Ad Hoc Networks," inTrust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, vol., no., pp.890-895, 25-27 June 2012
12. Rongxing Lu; Xiaodong Li; Luan, T.H.; Xiaohui Liang; Xuemin Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," in Vehicular Technology, IEEE Transactions on, vol.61, no.1, pp.86-96, Jan. 2012
13. Kyung-Ah Shim, "CPAS: An E_cient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks," inVehicular Technology, IEEE Transactions on, vol.61, no.4, pp.1874-1883, May 2012
14. Jiun-Long Huang; Lo-Yao Yeh; Hung-Yu Chien, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks," in Vehicular Technology, IEEE Transactions on, vol.60, no.1, pp.248-262, Jan. 2011
15. Lingbo Wei; Jianwei Liu; Tingge Zhu, "On a Group Signature Scheme Supporting Batch Verification for Vehicular Networks," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on , vol., no., pp.436-440, 4-6 Nov. 2011
16. T. W. Chim, S. M. Yiu, C. K. Hui, and O. K. Li, SPECS: Secure and privacy enhancing communications schemes for VANETs, Ad Hoc Networks, vol.9, Issue.2, pp.189-203, Mar. 2011.
17. Isaac, J.T.; Zeadally, S.; Camara, J.S., "Security attacks and solutions for vehicular ad hoc networks," inCommunications, IET, vol.4, no.7, pp.894-903, April 30 2010
18. Yipin Sun; Rongxing Lu; Xiaodong Lin; Xuemin Shen; Jinshu Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," in Vehicular Technology, IEEE Transactions on, vol.59, no.7, pp.3589-3603, Sept. 2010
19. Ghassan Samara, Wafaa A. H. Al-Salihy, R. Sures., Security analysis of vehicular ad hoc networks (VANET), in IEEE Conf. Network Applications Protocols and Services (NETAPPS), pp.55-60, 2010.
20. Wasef, A.; Rongxing Lu; Xiaodong Lin; Xuemin Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]," in Wireless Communications, IEEE , vol.17, no.5, pp.22-28, October 2010
21. Wasef, A.; Yixin Jiang; Xuemin Shen, "DCS: An E_cient Distributed-Certi_cate-Service Scheme for Vehicular Networks," in Vehicular Technology, IEEE Transactions on , vol.59, no.2, pp.533-549, Feb. 2010
22. C. Zhang; R. Lu; X. Lin; P. Ho; X. Shen., An e_cient identity-based batch veri_cation scheme for vehicular sensor networks, in Proc. IEEE INFOCOM, pp. 246-250, 2008.
23. Dedicated Short Range Communications (DSRC), [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

BIOGRAPHY

Godavari Hanmareddy Kudlikar is a Graduate Student in the Computer Engineering Department, College of MIT Academy Of Engineering, Pune University. She is pursuing her Master (ME) degree from MITAOE, Alandi(D), Pune, State Maharashtra, India. Her research interest is in VANET.