RESEARCH ARTICLE OPEN ACCESS

Proxy Based Batch Authentication Scheme for Vehicular Ad Hoc Network

Godavari H. Kudlikar [1], Sunita S. Barve [2]
Department of Computer Science and Engineering
Savitribai Phule Pune University / MIT Academy of engineering, and Alandi (D)
Pune - India

ABSTRACT
Previously in vehicular ad-hoc network Public Key Infrastructure (PKI) scheme was used for authentication. this scheme was used as Vehicular Signature application for maintaining integrity of message and for verifying senders identity. Using this scheme lot of time was required for verification as RSU verifies received message one by one and was difficult for RSU to identify the vehicle. So proxy Based Batch Authentication is being proposed which reduces computational overhead of RSU using number of proxy vehicles which performs batch authentication of message and sends the result to RSU. Also an expedite key negotiation scheme is designed for transmitting very critical messages.

Keywords:- Vehicular ad-hoc network, Proxy vehicle, Proxy based authentication, privacy preservation, Key negotiation, Vehicular ad-hoc network.

I. INTRODUCTION

VANET has become a popular topic as it has a potential to offer road safety and good driving experience it also provides value-added services such as internet facilities, Wi-Fi, vehicles position, direction, speed etc. As communication in VANET is wireless there are certain security issues so certain attacks are possible. Such security attacks leads to bad user experience and create drastic consequences. So to make VANET secure is one of the key objective for designers.

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

In order to overcome with this above difficulty Zhang et al. in [22] introduced a scheme called efficient batch signature verification scheme for vehicular communication, in which multiple messages can be verified simultaneously. But it does not meet VANET authentication speed. A protocol named Dedicated Short Range Communications (DSRC) were RSU must verify around 2500-5000 message per sec if vehicle broadcasts messages after every 100-300ms which is the most challenging task for any current batch-based digital signature scheme.

Using this scheme the goal is to overcome with the above efficiency problem. So this paper is used to design and implement a Proxy Based Authentication Scheme (PBAS) were proxy vehicle plays vital role, here in this scheme multiple messages can be authenticated using verification function. In addition to this concept of batch key negotiations is being added where, RSU verifies messages simultaneously and broadcast single message to all vehicles in RSU range. Some of the design requirements of the proposed scheme are as follows:

- The scheme should meet authentication and message integrity requirement.
- It should be resistant to replay attack
- It should meet privacy preservation requirement.
- The scheme should verify processes even if small number of proxy vehicles has been compromised.

Remainder of paper explains as follows: Section II outlines literature survey. Section III describes proposed system along with process summary. In section IV mathematical model is being explained followed by conclusion made in section V.

II. RELATED WORK

An Raya et al. presented Public-Key Infrastructure (PKI) based scheme in which RSU verifies received messages one by one at any time which is difficult for predicting identity of vehicle. But it requires time for processing and are unable to satisfy some of the efficiency requirement, which leads to transmission overhead and computational complexity of RSUs if number of vehicles are increased for authentication. So Zhang et al. in [22] introduced an efficient batch signature verification scheme used for communication between vehicle and infrastructure communications in which an RSU can

verifies multiple signatures (near about 1600 messages per sec) at a time so that time required for verification can be significantly reduced. According to the Dedicated Short Range Communications (DSRC) protocol in [23], each vehicle should broadcasts a traffic safety message after every 100-300 ms such that RSU will verify 2500-5000 msg if number of vehicles are around 500. But problem with this IBV scheme is it suffers from replay attacks.

In vehicular communication messages can be authenticated using the Elliptic Curve Digital Signature Algorithm (ECDSA) were for each message one certificate is included. A major challenge is to reduce the consumption of resource in transmission and consumption. Although it provides better security, verify authenticity and non-repudiation but it does not overcome security attacks and also it contains most expensive operation like modular inversion, scalar multiplication operation. Some of the limitations of using this scheme are Message Delay and Message Loss Rate.

Chim et al. in [16] introduced a Secure and Privacy Enhancing Communications Scheme (SPECS), here in this scheme after batch authentication, a group of vehicles is formed and they communicate with one other securely without RSUs which is called as group communication protocol.
However, in [7], Shi-Jinn Horng et al. found that SPECS is susceptible to impersonation attacks, were a malicious vehicle can act as an real entity to broadcast false messages or even force vehicles belonging to other group to send fake messages securely among themselves.

To overcome this weakness of SPECS scheme Shi-Jinn Horng in [7] proposed b-SPECS+ scheme. This scheme satisfy a variety of security requirements and overcome the weaknesses under certain assumptions like TA is always online, the redundant TA should avoid being a bottleneck
or a single point of failure.

Shim et al. in [13] proposed a scheme called Conditional Privacy Preserving Authentication scheme, here in this scheme each message is mapped to pseudo identity and Trust Authority is responsible for regaining real identity. RSU verifies multiple received signatures thus reducing total verification time. Main goal is to use identity based signature (IBS) scheme under computational DiffeHellman (CDH) assumption. This scheme uses general hash functions instead of using MapToPoint function which is not efficient. And after that a secure conditional privacy-preserving authentication scheme (CPAS) is constructed for secure V2I communications using a pseudo-IBS. CPAS supports fastest batch verification process so it can verify 750 signatures in less than 300 ms.

Albert et al. in their work [5] introduced an protocol called expedite message authentication protocol(EMAP) which is alternative to CRL checking process and is done by using 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 and is the first solution to reduce authentication delay caused by CRL checking. 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. According to analysis, it is concluded that EMAP is demonstrated to be secure and efficient protocol.

III. PROPOSED WORK

Proposed system consist of proxy vehicles, RSUs were each proxy vehicle plays an vital role in authenticating multiple messages simultaneously using verification function. After verification of message done by proxy vehicles, results are sent to RSUs for verification of signature. Using this concept the computational overloads of RSUs can be reduced. This is done by mechanism designed for RSU to verify output given by different proxy vehicles using verification function so that RSU can evaluate the validity of different messages which is as shown in fig. 1.

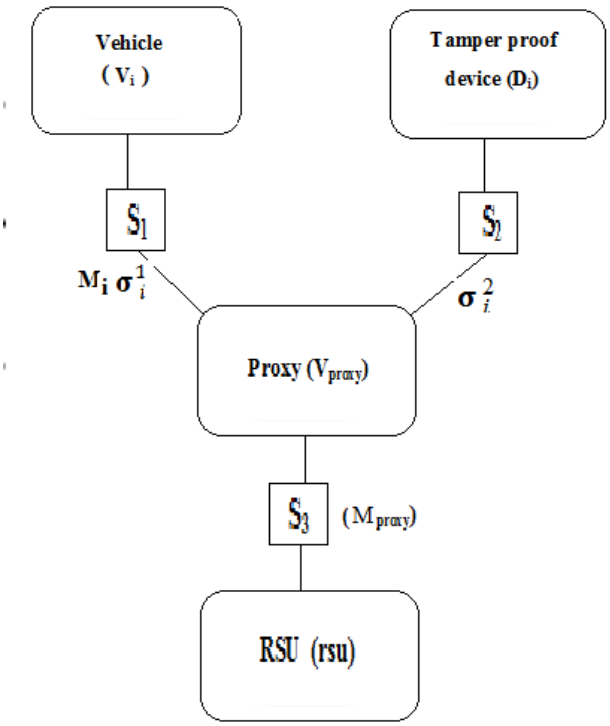

Fig. Proxy Based Authentication Scheme were S_1: Generation of Message and signature by V_i, S_2: D_i generating another signature, S_3: Batch verification Result by V_{proxy}

Following fig shows main characteristics features of the proposed PBAS scheme.

In this proposed Proxy Based Authentication scheme(PBAS) computational load of RSUs is reduced using cooperate communication amongst proxy vehicles, where each proxy vehicle verifies the signatures using a verification function and then it sends output to nearby RSU. After getting the results from proxy vehicle RSU verifies the output which results in consuming less computing resource by RSU. Cryptographic operations are performed for verification in an authentication scheme and these operations are executed using traditional authentication schemes by RSUs.

Process Summary

1) Generation of public and private keys for the system

This step is the fundamental step which initializes the system or execution environment
with the initial parameters required for authentication purposes and all the private and public parameters for the network elements and components are calculated separately. The network elements and components are then loaded with these parameters. Also for each Road Side Unit a tamper proof device is installed and initialized for further processing.

2) Generation of signatures for messages

In this step each vehicle, which is sending a message signs it with its pseudonym and corresponding private key identifier generated in the earlier process. The vehicle sends this message and its signature to a proxy vehicle for verification purpose.

3) Batch Verification using proxy vehicles

In this process, a set of dedicated proxy vehicles with respect to Road Side Unit are provided with the messages to perform a batch verification of the signatures. The proxy vehicle actually verified the messages with the help of bi-linear mapping within a set of messages received.

4) Verification of Outputs at Road Side Units

The Road Side Units are equipped with a set of procedural steps. These steps are carried out in series of tasks. There are in all three tasks. The first task ensures that message sender is a genuine proxy vehicle and that while forwarding the message was not modified. The second task checks whether the output submitted by the proxy vehicle is correct. The third task denotes the proxy vehicle if it fails to perform properly.

IV. MATHEMATICAL MODEL

The implementation of the paper comprises of multiple cryptographic techniques were each element and component carrying out these calculation are important. Below shows the arithmetic representation of the system. It includes execution routine that performs calculation based on following representation.

Here all the required public and private keys of system such as for vehicle, RSU, Tamperproof are generated using standard key generation algorithm such as SHA-1.

Some of the additional calculation required for implementation of system is as follows.

Notation	Description
II	Message Concatenation
$Master_j$	j^{th} private master keys where j={1, 2, 3}
Vec_i	i^{th} vehicle
$Publickey_i$	Public key of system, where k ={1,2,r}
$PriKey_i$	Private key of vehicle V_i
$PudoID_i$	Pseudo identity of vehicle V_i
$RealID_i$	Real identity of vehicle V_i
$RealID_r$	Real identity of RSU
M_i	Message from a Vehicle
H(.)	MapToPoint hash function
h(.)	A one-way hash function such as SHA-1

A. Pseudonym for identity of Vehicle:

Pseudonym key is generated by Vec_i which is used to achieve privacy preservation were r_i is different for different areas as shown below.

$$PudoID_i = (PudoID_i^1,\ PudoID_i^2)$$

a) $PudoID_i^1 = r_i P$

b) $PudoID_i^2 = RealID_i \oplus H(r_i Publickey_1)$

B. Signature for Vehicle's message:

Vec_i picks the pseudo identity key generated using above calculations from tamperproof device and signs the message M_i using the below formula.

$$\sigma_i^1 = PriKey_i^1 + h(M_i)\, PriKey_i^2$$

C. Signature for tamper proof device:

Tamper proof device generates its own signature using master key $Master_3$

$$\sigma_i^2 = (r_i + Master_3 + (h(M_i) + \sigma_i^1))\, Pubkey_r$$

D. Calculation for batch verification at proxy vehicle:

Before Batch verification Vec_i sends message containing $\{PudoID_i, M_i, \sigma_i^1, \sigma_i^2\}$ and then both L.H.S. and R.H.S are calculated.

$map(\sum_{i=1}^{n}\sigma , P) = map(\sum_{i=1}^{n} RealID , Pubkey)$

$map(\sum_{i=1}^{n} h(Msg_i)H(RealID_i^1 \| PID_i^2), Pubkey_2)$

Where,

map = bilinear mapping over additive cyclic group of prime order

If both the values are identical it means that identity of sender and message integrity are preserved.

E. Calculation of verification of output from proxy vehicles at RSUs:

In this phase RSU mainly focuses on three task using this below calculation. It checks identity of proxy vehicle, correctness of verification output send by proxy vehicle and revokes proxy vehicle if it finds any fake proxy in this system.

$$map(\prod_{i=1}^{n}\sigma_i^2, RealID_r) = map\{\prod_i^1[\sum_{i=1}^{n}(h(M_i)+\sigma_i^1)]PriKey_r^2, PriKey_r^1\}$$

V. CONCLUSION

Using PBAS overloads of RSUs can be reduced using proxy vehicles if the design requirement is satisfied, such that each proxy vehicle will authenticates multiple messages from the other vehicles and sends the generated result to RSU. PBAS should offers fault tolerance i.e. even if a small number of proxy vehicles are compromised in VANETs the scheme continue operating. Only assumption in designing this system is that vehicles are fully trusted under condition of efficient message delivery.

REFERENCES

[1] Chim T.W, Yiu, S.M, Hui Li, "VSPN: VANET-Based Secure and Privacy Preserving Navigation", Computers, IEEE Transactions on , vol.63, no.2, pp.510-524, Feb. 2014.

[2] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang and Hui Li, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks", in Vehicular Technology, IEEE Transactions on , vol.63, no.2, pp.907-919, Feb. 2014

[3] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, Alejandro Quintero "VANET security surveys", in Computer Communications, vol.44, pp 1–13, May 2014

[4] Lamba S; Sharma M., "An Efficient 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", in Mobile Computing, IEEE Transactions on , vol.12, no.1, pp.78-89, Jan. 2013

[6] Xiaodong Lin; Xu Li, "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks", in Vehicular 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 Verification for Secure Pseudonymous Authentication in VANET ", in Information 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", in IEEE 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 Traffic-Monitoring Systems" in Intelligent 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", in Vehicular Technology, IEEE Transactions on , vol.62, no.4, pp.1505-1518, May 2013

[11] Xiaojun Li; Liangmin Wang, "A Rapid Certification Protocol from Bilinear Pairings for Vehicular Ad Hoc Networks" in Trust, 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 Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks", in Vehicular 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", in Communications, 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 Efficient Distributed-Certificate-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 efficient identity-based batch verification scheme for vehicular sensor networks", in Proc. IEEE INFOCOM, pp. 246-250, 2008.