A Survey on Identity Based Batch Verification Scheme for Privacy and Security in VANET

Pratabidya Mahapatra[1], A.Naveena[2]
[1]MTech, Dept. of ETM, GNITS, Hyderabad, India
[2]Assistant Professor, Dept. of ETM, GNITS, Hyderabad, India

---***---

Abstract - *Vehicular adhoc network is an emerging network which facilitates vehicular communication for the safety requirements. Each vehicle broadcasts messages to its neighboring vehicle as well as to the roadside units(RSUs). However this increases the concerns for security and privacy. To check the message validity at RSU, a batch verification of all signed messages is being performed by RSU, which is known as Identity-based batch verification(IBV). In this scheme, messages should be signed and verified by RSUs without revealing the real identity of vehicles. This scheme assures anonymous authentication, message integrity , privacy as well as traceability. So in this paper, we present a survey of all the existing IBV schemes.*

Key Words: **Anonymous identity, Authentication, Batch Verification, Privacy, Security, Vehicular adhoc Network**

1.INTRODUCTION

VANET provides a network where vehicles among the road communicate for driving safely. Vehicles are equipped with onboard unit(OBU),which communicates with other vehicles as well as roadside units(RSUs) located at street to increase the driving safety. So this communication refers Vehicles-to-Infrastructure (V2I) and Vehicle-to-Vehicle(V2V) communication. A trusted third party, known as Trusted Authority(TA), communicates with RSU by wired connection. TA is powered with sufficient storage and computational capability. So this network provides an efficient way to sense various physical signals to traffic distribution and collects various traffic information with more accuracy and low cost.

This communication is basically governed by Dedicated Short Range Communications(DSRC) protocol. Each vehicle periodically broadcasts about its present state to its nearest vehicle and RSUs in every 100-300 ms. RSU verifies the messages to check its validity and also sometimes manages the traffic situation locally. As privacy is another important aspect, the real identity of the driver is not disclosed throughout the communication. Therefore an anonymous communication is maintained. In the case of dispute the real identity of driver is revealed by TA.

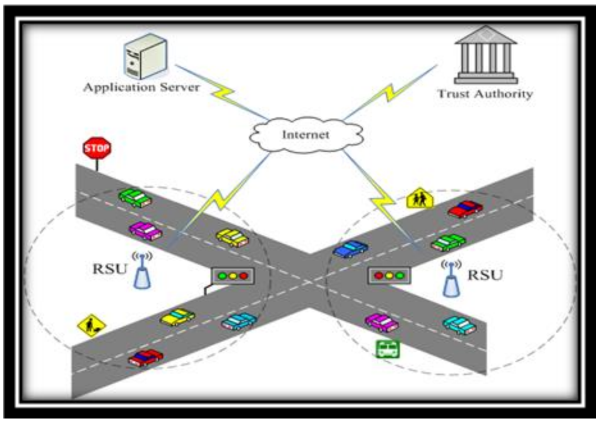

Fig -1: The network model

In order to increase the verification speed at RSUs, a bulk of messages is verified at the same time by RSU instead of verifying individually. This verification is known as Identity based Batch Verification(IBV). This drastically reduces the total verification delay. So this scheme should satisfy the following requirements in order to have security and privacy.

1.Message authentication: RSUs should be able to verify message, that is sent by legitimate vehicle without being modified.

2.Identity Privacy Preservation: The real identity of vehicle is kept anonymous from RSUs.

3.Traceability: The real identity of attacker should be retrieved by TA in the case of dispute.

2. LITERATURE SURVEY

2.1 An efficient Identity based batch verification scheme for Vehicular sensor network

In the conventional signature scheme, the received message are verified one by one. So this may fail to satisfy the stringent time requirement of the vehicular communication applications. In order to tackle the above mentioned problems and make VSNs suitable for the intelligent traffic systems, Zhang et al proposed a scheme[1] which states that multiple signatures can be verified at the same time instead of one after the other. This improves the signature verification speed. Different pseudo identities are created by tamperproof device in order to achieve conditional privacy . Then private keys are generated to sign the message. These signed messages are sent to RSUs by vehicles. In the case of dispute, the real identity of the adversary is revealed by TA.

This scheme reduces the verification time and the certificates are also not required for the verification. But the two weakness of this scheme are that it is prone to replay attack and it doesn't satisfy the property of non repudiation.

2.2 ABAKA: An anonymous batch authenticated and key agreement scheme for value-add services in vehicular ad hoc networks

This ABAKA [2] provides an batch authentication scheme for value-added messages. Here multiple messages are authenticated by one verification process and a session key is negotiated by each vehicle to have secure communication path. The tamperproof device generates pseudo identity with the help of a random point. Then private keys are generated with the help of generated IDs. In the verification process, it verifies all the messages sent by vehicle as well as compute session keys and broadcasts to vehicles. Vehicles check the freshness of messages and then generate session keys.

This scheme efficiently maintains privacy and confidentiality. Service provider also traces the real identity of vehicle as required. As RSU broadcasts the response message, it reduces the transmission overhead. But the disadvantage of this scheme is that it doesn't achieve signature non repudiation.

2.3 SPECS: Secure and privacy enhancing communications schemes for VANETs

SPECS [3] provides a secured communication in VANET by handling both "ad hoc messages " as well as "group messages". Whenever a vehicle meets a new RSU, it authenticates itself with TA via RSU. Then TA allows RSU to verify the vehicle signature with its pseudo identity. TA sends its master key and shared secret to the vehicle once in the session of communication. In order to send adhoc messages, vehicle has to sign the messages with its signing key and sends for verification. RSU verifies all the messages in batch mode and broadcasts notification message to the sender vehicles. In order to send group messages, a group is created with set of desired vehicles. A secret key is created for the group by TA and is sent to the members of the group.

The advantage of this scheme is that by sending group messages, vehicles can authenticate and communicate securely without the intervention of RSUs. But the disadvantage is that it is prone to impersonation attack, where adversary successfully assumes the identity of one of the legitimate vehicles in a group throughout the communication.

2.4 b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET

This b-SPECS is a secured scheme [5] which overcomes the weakness of SPECS as well as suffices the security and privacy requirements. This gives a software based solution without depending on tamperproof devices. In initial handshaking, vehicle sends encrypted real identity(RID) , password(PWD) and signature to TA. TA decrypts that RID,PWD and signature. Then TA chooses a shared secret, computes verification public key and selects random number. TA sends encrypted units to both RSU and OBU. RSU decrypts that unit to get verification public key and OBU decrypts to calculate the shared secret. In message signing phase, OBU calculates a random nonce then computes its anonymous IDs and private keys. Then it signs the message and sends to TA for batch verification.

The advantages of this scheme are that

1.It decreases its transmission overhead as OBU doesn't sign and encrypt the shared secret.

2.It satisfies a variety of security requirements and withstands the weaknesses of the impersonation attack.

The Disadvantage of this scheme is that TA should always be online. So it will be overloaded.

2.5 Towards a secure batch verification with group testing for VANET

This improved authentication scheme [4] is proposed with batch verification based on bilinear pairing to make VANET more secure, efficient and more suitable for practical use. In this scheme tamperproof device checks the real identity and password, generates the Anonymous Identities. With the help of this Anonymous Identities and timestamp ,it generates the signing key. With the help of these keys, messages will be signed by vehicle and sent to RSU. RSU first checks the freshness of the received message by the timestamp and proceeds for batch verification.

This scheme efficiently handles replay attack as it is considering the timestamp But it has some severe security flaws such as anti traceability attack, forgery attack and identity privacy violation.

2.6 Enhancing security and privacy for Identity based Batch Verification Scheme in VANETS

This scheme [6] overcomes the flaws of the IBV scheme proposed by Lee and Lai. First TA generates and preloads the system parameters. Next, the tamper proof device checks real identity and password entered by vehicle and generates the Anonymous Identities by using random numbers. With the help of this anonymous identities, message is being signed by OBU and sent to RSU. At RSU, message verification is done after checking the freshness of the received message.

This scheme efficiently handles forgery attack, anti traceability attack and identity privacy violation. But the disadvantage of this scheme is that it is vulnerable to invalid signature attack.

3. CONCLUSION

Security is one of the most important aspect of communication. The IBV scheme provides a more secured way in communication in VANET. Hence it can be regarded as a preferred choice in communication. In this paper, a survey of existing IBV scheme has been mentioned with its advantages and disadvantages. The proposed IBV scheme efficiently handles all security flaws but it is unable to handle some security issues like invalid message problem. The future work can be done to improve the IBV scheme by recognizing the invalid signatures.

REFERENCES

[1] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, “An efficient message authentication scheme for vehicular communications,” IEEE Transactions on Vehicular Technology, vol. 57, no. 6, pp. 3357-3368, 2008.

[2] J. L. Huang, L. Y. Yeh, and H. Y. Chien, “ABAKA:An anonymous batch authenticated and key agreement scheme for value-add services in vehicular ad hoc networks,” IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248-262, 2011.

[3] T. W. Chim, S. M. Yiu, Lucas C.K. Hui, and O. K. Li, “SPECS: Secure and privacy enhancing communications schemes for VANETs,” Ad Hoc Networks, vol. 9, no. 2, pp. 189-203, 2011.

[4] C. C. Lee and Y. M. Lai, “Toward a secure batch verification with group testing for VANET,” Wireless Networks, vol. 19, no. 6, pp. 1441-1449, 2013.

[5] S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, “b-SPECS+: Batch verification for secure pseudonymous authentication in VANET,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1860-1875, 2013.

[6] Shiang-Feng Tzeng, Shi-Jinn Horng, “Enhancing security and privacy scheme for identity based batch verification scheme in VANET,” IEEE Transaction on Vehicular technology, 2015.