# Survey on authentication scheme for VANET

[1]Sharon.S, [2]Venkatesh.V
[1]PG Scholar, [2]Assistant Professor
[1]Embedded Systems,
[1]SASTRA University, Thanjavur, India

*Abstract :* Vehicular Ad hoc Network (VANET) is the network of vehicles that are moving at high speed are made to communicate with each other for different purpose particularly for providing road safety. It is also an emerging technology which facilitates the communication between Vehicle to Vehicle (V2V) and Vehicle to Road Side Unit (V2R) for providing traffic safety to vehicle and provide convenience in driving the vehicle. Each vehicle monitors traffic related information and send it to the nearby vehicle and RSU for making the journey safe. It also sends warning and alert message to avoid accidents on the road. Security and privacy is an important aspect required for VANET communication. Even a small change in the data and delay in transmission can cause catastrophic effects it may even lead to loss of life. Efficient and flexible authentication scheme is required for preventing the data. Validation process is carried out for identifying the anonymous accessing of the data which can be done by signing and verification of messages. In this paper various authentication scheme that provides secure communications and its performance are discussed.

***IndexTerms*** **- Vehicular Ad hoc Networks, Privacy, Security, Authentication, Anonymous, Batch verification, Pseudonym, Wireless Sensor Networks.**

## I. INTRODUCTION

Vehicular Ad hoc Network (VANET) have been attracted in the recent decades towards extensive research efforts from government side, academics and industry. It plays an important role in traffic safety management. It monitors and sends traffic related information as well as alert messages to prevent from accidents and saving life. An infrastructure called Road Side Unit (RSU) is fixed along road side for monitoring the traffic related events and broadcast these events to On Board Unit (OBU) fixed in the vehicle. OBU are equipped with Tamper Proof Device (TPD) which provides additional security and it is very difficult to hack. The data that are to be transmitted are traffic signal, lane change warning, location, vehicle identification number, dangerous road features, crash alert and incident occurred such as accident, road block etc. Based on this information other vehicle can change its routes for travelling and avoids congestion of traffic Messages. Trusted Authority (TA) is reliable for every person it has enough calculation and storage capability. It communicates with the RSU through the secured fixed channel example internet.

Dedicated Short Range Communication (DSCR) are utilized for reliable exchange of data between vehicles and RSU.It provides the communication range of 100-300 ms. VANET predicts the chance for accidents and send warning notification to driver of the vehicle and so accidents can be avoided .In case of road block or accident occurred if the information is transmitted the driver can take alternate travelling route which in turn will save time ,avoid traffic jam and it will save fuel . In an emergency vehicle is travelling on heavy Traffic road if this Information is transmitted it will notify all other vehicles to provide way for the emergency vehicle .Crash alerts can be predicted and accidents can be avoided by sending alert messages.

Security and privacy are important issue regarding data transmission in VANET. Hence integrity of the message should be preserved. In VANET security is the important for exchange of data. Performance requirement for VANET in security system is crucial .Two major reasons are high mobility speed of the vehicle and real time analysis of data. Purpose of the attack is to create problem for users to access some information. There are variety of attacks such as Replay attack, Forgery attack, Impersonation Attack, Masquerade and Denial of service attacks etc.,. Since highly sensitive data are transmitted in VANET it should be secured. Invalid or unauthorized user should be identified initially and blocked. Authentication scheme based on Identity, Pseudonym, Public key infrastructure and hashing scheme that achieves the security requirements such as message authentication, privacy preservation, traceability, non-repudiation, unlink ability and replay resistance are given. Objective is to provide secure communication where transmitted message should reach the destination without any modification and at the correct time without delay even if small change and delay can cause tremendous effects. Various authentication achieving this security factors are discussed.

## II. RELATED WORKS

### 2.1Identity based scheme

Nai-Wei et al. (2016) proposed the scheme adopts Identity based signature on Elliptic Curve Cryptography for providing secure authentication for vehicle to RSU communication. This scheme is time consuming .It do not use paring and map to point operation for vehicular sensor networks.ID based signature simplifies Certificate revocation problem by using the identity of the signer as public key and Signers private keys are generated by Public Key Generator (PKG).There is no need for verifier to store all public keys and signers certificate. PKG sends the public parameters and Hash function requires only string parameters. For registration user sends the ID to the PKG. Signature for the message of ID is calculated as signing process and verification can be done as the batch verification. Future work will be using light weight scheme for authentication.

### 2.2Anonymous based authentication scheme

Jiun-Long Huang et al. (2011) proposed the scheme that can be used for value added services, reduces transmission overhead and provides efficient validation process in which multiple message request can be verified with one operation and negotiation of session keys are initiated. Elliptic Curve Cryptography ECC requires smaller keys and is used for reducing delay in verification and transmission overhead. Vehicle has to perform initialization for loading the system parameters .Each vehicle has a Tamper Proof Device in which data stored cannot be obtained anonymously. Tamper Proof Device (TPD) is involved in the generation of pseudo identity and private key. For accessing the service given by service provider (SP) authentication procedure and key agreement are processing is done by the SP for checking the validity of the vehicle that is requested and in negotiating a session keys. During mutual authentication validity of the SP is checked. Batch based verification is adopted. Future work will be on adopting predictive routing for increased efficiency and provide non-repudiation.

**2.3Batch verification scheme**

Shiang-Feng Tzeng et al. (2015) proposed the scheme provides security to random oracle model. This scheme reduces delay in computation and transmission overhead. It requires constant no of pairing and point of multiplication. Multiple messages are verified at the same time. TA generates system parameters for each vehicle and RSU. Each vehicle enters the Real Identity RID and password PWD to its Tamper Proof device. If they matches it generates anonymous identity and signing key. Messages are signed using the key and they are broadcasted. RSU receives the messages and multiple messages are verified. Disadvantage is that unauthorized signature cannot be identified in batch verification. Future work will be on identifying illegal signatures.

**2.4Identity and batch verification based scheme**

Debiao He et al. (2015) proposed the scheme that provides ID based authentication for V2V and V2I communication. This scheme has lower computation and communication cost .It provides conditional privacy without bilinear paring operation. System parameters are generated by Trusted Authority (TA). They are preloaded into each vehicles tamper proof device (TPD) which is done by TA and they are send to all RSU. Anonymous identity and digital signature for the message are generated by TPD and send to RSU. During verification process Validity of the message is checked by Verifier it may be a RSU or Vehicle .In this multiple messages are verified in batches. It supports mutual authentication and privacy preservation. It provides increased performance compared all other conditional privacy preservation schemes. Future work will be making the scheme to withstand to all attacks.

**2.5Pseudonym based scheme**

Shi-Jinn Horng et al. (2013) proposed the Pseudonym based authentication scheme that overcomes the disadvantages of specs and provides software based result without involving the Tamper proof Device in the process. In this system the transmission overhead is decreased and withstand the impersonate attacks. Vehicle signs the RSU using password and real identity. Encrypted real identity (RID), Password (PWD) and signature are sent by the vehicle to Trusted Authority. When they are received TA decrypts the encrypted text and obtain RID, PWD and signature is verified using public key .Pseudo identities and key for signing is generated by the vehicle. RSU verifies the signature using public key and verification done in batches if the pseudo identities do not match the stored one they are rejected. Disadvantage is TA is needed to be online always and so it is overloaded. Future work is to avoid compromise of RSU.

**2.6Group based scheme**

T.W. Chim et al. (2011) proposed the scheme that provides secured communication for group messages. Whenever a vehicle sees a new RSU, it validates itself with TA through RSU. TA allows the Signature of vehicle and its pseudo identity to be verified by RSU. Master key and shared secret key of the vehicle are sent to TA .Vehicle uses signing key for the signing of the messages. After that they are send for verification, all the messages are verified by RSU in the batch process. And the notification messages are sent to vehicle. Secret key is created and sent to all the members of the group for verification. Advantage of this scheme is that it provides secured authentication without the interference of RSU. Future work is to overcome the impersonate attacks.

**2.7Hashing based scheme**

Bidi Ying et al. (2013) proposed authentication scheme for privacy preservation to broadcast messages. The functionality of Message Authentication Code (MAC) and operations of hashing are used for authenticating the messages in VANET communication. During vehicle registration Trusted Authority register and authenticate the vehicle. Pair of Public, private anonymous key and anonymous certificates are assigned by TA. For authenticating the data that are to be transmitted is done using anonymous certificates. Two level hash chains that are high level hash chain and low level hash chains are used for avoiding the message loss. This scheme can be used for supporting emergency and routine messages. It provides conditional privacy and anonymity is preserved .Disadvantage is that it has message latency .Future work will be on eliminating the latency of message and message loss with increase in vehicles.

**2.8Multilevel based scheme**

T.W. Chim et al. (2012) proposed several level authentication protocol is used for transmitting messages for providing driving safety to the vehicles. This scheme eliminates the dependence of Tamper Proof Device and reduces the verification delay It uses tamper proof device in the process but the master secret that are preloaded into TPD is removed. To increase the level of security master secret can be updated whenever they are required. Messages that are sent to the vehicles can be classified as regular and urgent messages. Regular message are validated by neighbouring vehicles by using Hash-based Message Authentication Code (HMAC) and urgent messages are validated by means of a conditional privacy-preserving authentication scheme with the help of nearby RSU. Disadvantage is delay in the verification process .Future work will be on group communication can be used for making it easier.

**2.9Public key Infrastructure based scheme**

Pandi Vijayakumar et.al. (2016) proposed the Dual authentication key management that provides the higher level of security in communication to prevent the entering of unauthorized vehicle into the VANET .This scheme provides efficient computation for secure data transmission and with one broadcast from Trusted Authority (TA) it can be updated. User are classified by trusted authority as primary, secondary, and unauthorized users. In this group keys are distributed to the group of users and can be update when user join or leave the operation. Dual mode authentication is carried out .To avoid malicious user from using the secret key finger print is integrated into the hash code. Registration process can be carried either through online or offline for submitting the details of vehicle and driver. This is called Vehicle Authentication Process (VAP) .After completion of dual authentication process Authentication Code is generated which is used for sending and receiving the data. Future work will be on finding new method to preserve the privacy of the vehicles location from intruders.

## III. CONCLUSION

Vehicular Ad hoc Network has become the most interesting field for intelligent transportation systems because of transmitting the safety related information. Security and privacy is required for communication between Vehicle and RSU. Authentication is one of the important security features for VANETs that should be addressed. Hence, various authentication schemes such as Identity, Pseudonym, Public key infrastructure and hashing based are proposed. In this paper, a survey on different authentication techniques with its own security features are discussed. From the discussion it can concluded that by incorporation of lightweight Advanced Encryption Standard (AES) algorithm by reducing the number of rounds and key size it becomes low power consuming and compact. Then the authentication process will be efficient and secure against attacks. It is reliable and provides additional security for communication.

## REFERENCES

**[1]** Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhmmad Khurram Khan. 2015 .Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET from IEEE Transactions on Vehicular Technology ,vol.pp,no.99 .

**[2]** Bidi Ying, DimitriosMakrakis,HusseinT.Mouftah.2013.Privacy preserving broadcast message authentication protocol for VANETs from Journal of Network and Computer Applications ,(36 )1352–1364.

**[3]** T.W. Chim , S.M. Yiu , Lucas C.K. Hui , Victor O.K. Li .2012. MLAS: Multiple level authentication scheme for VANETs from Ad Hoc Networks ,(10) 1445–1456.

**[4]** Bidi Ying,DimitriosMakrakis , HusseinT.Mouftah 2013. Privacy preserving broadcast message authentication protocol for VANETs from Journal of Network and Computer Applications (36) 1352–1364.

**[5]** Debiao He, Sherali Zeadally, Baowen Xu, *Member, IEEE*, and Xinyi Huang. 2015. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks from IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 12.

**[6]** Pandi Vijayakumar, Maria Azees, Arputharaj Kannan, and Lazarus Jegatha Deborah.2016. Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks from IEEE Transactions on Intelligent Transportation systems, vol. 17, no. 4.

**[7]** Fei Wang, *Member, IEEE*, Yongjun Xu, *Member, IEEE*, Hanwen Zhang, *Member, IEEE*,Yujun Zhang, *Member, IEEE*, and Liehuang Zhu, *Member, IEEE.2016.* 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET from IEEE Transactions on vehicular technology, vol. 65, no. 2.