New Cluster based Secure Certificate Revocation Scheme for Vehicular Ad-Hoc Networks

G. Spica Sujeetha[1], V. Anitha[2]
[1]*PG Scholar, Department of Wireless and Mobile Communication, GNITS Shaikpet, Hyderabad, India.*
[2]*Assistant Professor, Department of Electronics and Telematics Engineering, GNITS, Shaikpet, Hyderabad, India.*

Abstract- In wireless as well as networking communications technologies, VANETs have been developed as a result of the advances in the past few centuries. The traffic safety and efficiency can be improved by the usage of the VANET. A wireless communication device termed by means of an on board unit (OBU) is involved by each vehicle that functions using the IEEE 802.11p standard for wireless communication in VANETs. Two kinds of communication models are involved in VANETs. One is vehicle-to-vehicle (V2V) and the other is vehicle-to-infrastructure (V2I) communications. The major necessity in VANETs is to provide safety of transmitted messages. By means of proxy vehicles, ID-MAP, a new identity-based verification method without bilinear pairings to challenge its problems and have an effective method is achieved well and proposed in the earlier. But In ID-MAP scheme, they don't concentrate on malicious nodes behavior and revocation process. So we propose new cluster based secure certificate revocation scheme (NCSCR). In our method, check and avoid the malicious node behavior using revocation process. The performance of proposed method is efficient while compared to existing methods ID-MAP, PBAS.

Keywords- VANET, vehicles, proxy vehicles, authentication, privacy preserving, ID-MAP, NCSCR.

I. INTRODUCTION

In wireless as well as networking communications expertise [1-3], VANETs have been developed as a result of the advances in the past few centuries. The traffic safety and efficiency can be improved by the usage of the VANET. An on board unit (OBU) is a wireless communication device as well as a dedicated short range communication (DSRC), which is a wireless communication protocol is involved by each vehicle that functions using the IEEE 802.11p standard in VANETs intended for wireless communication and employed in vehicle-to-vehicle (V2V) as well as vehicle-to-infrastructure (V2I) communications.

The communication controlling links, changing, deleting and replay of messages can be easily done by the adversary due to the mode of wireless communication. Therefore, some of the severe threats for VANETs are imitation, transformation, replay and man in the middle attacks. Traffic chaos or accidents are caused by the abovementioned threats [4], [5]. Hence, the major necessity in VANETs is to provide safety of transmitted messages. Since serious threats for drivers may be caused by the leakage of their identities and mischievous objects might trace their messages as well as traveling roads for crimes, therefore, the secrecy of the vehicle's identity need to be attained [6]. In instance of any misbehaviour, mischievous vehicles ought to be found and punished, since unrestricted privacy preservation is undesirable for VANETs [7], [8].

Certain verification methods named as Public Key Infrastructure-based (PKI-based) [4], [6] have been presented for satisfying safety as well as confidentiality complications in VANETs. The vehicles must store a huge amount of key pairs as well as their equivalent certificates which are necessary for transmitting with the messages, as these methods are inefficient. Several methods like privacy preserving identity-based authentication methods [8]–[15] are suggested to report certificate managing in PKI-built authentication methods. For instance, assume this situation: In a RSU coverage area, when 500 vehicles are present, by the requirement of DSRC protocol since every vehicle transmits its message regarding traffic safety for every 100-300 milliseconds, RSU must authenticate around 2500-5000 signatures in a second. An exciting authentication procedure by means of proxy vehicles on behalf of vehicular systems named by way of PBAS has been suggested by Liu et al. [16] for overcoming this complication. Using distributed calculating, a huge amount of signatures can be verified instantly by RSUs which are assisted by proxy vehicles in PBAS. Compared to earlier effective authentication methods grounded on batch authentication process at RSUs, the time which is necessary for verifying 3000 signatures is reduced by 88% was claimed by Liu et al. [16] in their scheme.

II. LITERATURE SURVEY

Architecture with robust security that is resistive to these threats is presented and a potential safety and secrecy threat for VANETs has been introduced in 2006 by Raya et al. [4]. For achieving authentication, integrity and privacy for each transmission, PKI has been modified in such a way that several key sets as well as their equivalent certificates have been preinstalled into vehicles where each pair is utilized. In Raya et al.'s method [4], in case of any disputes, for keeping key pairs and their certificates, a huge storing space should be allocated for each vehicle, and for checking their validity and tracing them, a huge storing space to record vehicles 'certificates must be allocated for the trusted

authority. The issues of Raya et al.'s efficiency and large storage space method [4] is upgraded by a novel verification method by provisional unidentified documentations delivered with RSUs which is proposed by Lu et al. [8] in 2008. For an effective method in the RSUs as well as for having huge storing space for vehicles, the idea of mix-zones is proposed by Freudiger et al. [17] owing to the extensive communications of vehicles by RSUs for obtaining Unidentified documentations. A distributed key concerning a vehicle as well as an RSU to recommend an effective verification method has been made with a key agreement protocol exploited by message authentication codes which is presented by Zhang et al. [18] in 2008. In order to fulfil the necessity for confidentiality, a huge amount of key pairs in addition to their documentations are preserved by a large storage space is essential for each method.

The certificate managing issues of earlier methods [5], [9], [17], [18] is addressed by an identity-centered cryptography [19] in designing authentication methods for VANETs is presented by Zhang et al. [10] in 2008. The verification cost at RSUs [10] is reduced by an identity-based signature method using batch authentication. Additionally, the conditional privacy preserving is satisfied by their method. Nevertheless, to fulfill the privacy requirement, binary search and bloom filter approaches, a novel identity-centered verification method by twofold distributed confidences has been proposed by Chim et al. [11] in 2011, since the method offered by Zhang et al. [10] is affected by impression, anti-controllability as well as secrecy irreverent attacks. The method presented by Zhang et al. [10] and their method is compared regarding communication overhead as well as message authentication and found efficient using a feature of 45%.

Additionally, Lee and Lai [11] upgraded their method to a secure identity-based authentication method in 2013, since they presented that Zhang et al.'s method is open for the repetition attack as well as doesn't have non-repudiation property although holding the effectiveness of Zhang et al.'s method. Horng et al. [12] upgraded the message signing stage of their method in such a manner that it may come across the requirements of safety as well as confidentiality of Chim et al.' [10] method which is unresisting to impression attack in 2013. For proposing an effective conditional privacy preservative authentication method using batch verification, an efficient identity-based signature has been presented by Shim [13] in 2012. False acceptance of invalid batching signatures and security errors are some of the security weaknesses in Shim's [13] method which is explained by Liu et al. An upgraded modification method by the signing algorithm is proposed by Zhang et al. [14] in 2014 by representing that Lee and Lie's authentication [11] method doesn't have non-repudiation and is susceptible to impersonation attack. Moreover, a new effective authentication method is proposed by Bayat et al. [15] in 2015 that tried to resolve their safety liability and an impersonation attack for Lee and Lie's authentication method [11]. Regrettably, Bayat et al.'s method [15] and Zhang et al.'s method [14] remain susceptible towards the variation attack. The computational overheads at RSUs is improved by a new proxy-based authentication method for VANETs which is presented by Liu et al. [16] in 2015 and presented that it consumes an excessive benefit in authentication of vehicles' initials whenever several vehicles stay in an RSU coverage areas. To fulfill confidentiality as well as safety necessities of VANETs, the author presented ID-MAP in [20]. Resistant to variation and impersonation attacks is assured by verifying unforgeability of the fundamental signature method compared to adaptively selected-message as well as individuality attack in ECDLP in the unsystematic oracle exemplary in this course. A new identity-based authentication method deprived of bilinear combinations is suggested by proxy vehicles, ID-MAP, for blocking the previous problems and consumes an additional effective method.

III. PROPOSED FRAMEWORK

To identify the validity documentation of the safe transmission of messages which happen through the usage of symmetric cryptography method, a cluster-based secure communication as well as certificate cancellation method is used in order to enhance the vehicles identity where the encryption as well as the decryption of certificates might take place.

In NCSCR scheme, there are three participants.

Trusted Authority (TA): The generation of structure factors, principal public key, secret key, and participants' secret key, preloading them to vehicles, and tracing the vehicles from their virtual characteristics is performed by a confidential third party called as TA in case of any misconduct.

The RSUs: Communication with the vehicles (proxy vehicles), checking the received messages validity from vehicles (proxy vehicles), as well as sending them towards the traffic control center can be achieved by the RSUs which are at roadsides.

Vehicles: Using tamper-proof devices OBUs, they are supplied and interact with one another's in addition to RSUs.

The major seven phases in this scheme:

i) **Setup:** The loading of system parameters into vehicles' tamper proof devices as well as RSUs, are generated by TA in this phase.

ii) **Anonymous identity generation:** On receiving a registered pseudo identity, each vehicle hides its actual identity and generates its equivalent secret key in this phase.

iii) **Clustering process:** Based on distance between nodes, the nodes (vehicles) remain collected into different clusters as well as the CH (cluster head) must remain chosen in this stage.

iv) **Certificate authority:** For revoking and distribution of certificates which belongs to the vehicles, this phase remains responsible. The particulars of the certificates are transmitted towards the intermediate nodes usually recognized as RSU by

the TA. Each and every CH receives its broadcasted detail that is located inside its range.

v) **Message generation:** Every vehicle selects a message and transmits the calculated message towards the proxy vehicle by a timestamp t in this stage.

vi) **Verification of messages by proxy vehicles:** The integrity and received messages identity of sender is verified by using a proxy vehicle in this part. The related-CH transfers the messages trusted by the complete participants of the cluster and therefore the trustworthiness of whole messages is validated.

vii) **Verification of proxy vehicles' output by RSUs:** False outcomes and revoke mischievous proxy vehicles are detected by the results acquired from proxy vehicles and verify an RSU in this stage. The revoked node from the cluster is picked and to preserve this attacked (revoked) node in CRL (certificate revocation list), the principles must be followed. The certificates of the nodes which are considered as malicious or malicious will be added into CRL.

3.1 Cluster head selection

In order to isolate the framework into various node clusters and to deal with the data broadcast through the communicating nodes, clustering is used. A cluster is referred as a group of nodes. From the group of cluster, the CH is selected.

Since limited resources of energy are offered, for effective communication the overall, CHs are interconnected to each other. Communication between the cluster nodes is established by the CH in cluster-based architecture. Various clusters are formed by grouping of vehicles and from the reliable nodes, CH must be chosen. The CH is selected by a means at which the node is at minimum distance from the remaining nodes. The selection of CH from the cluster members is represented in Figure 2. Furthermore, the determination of CH includes the following steps.

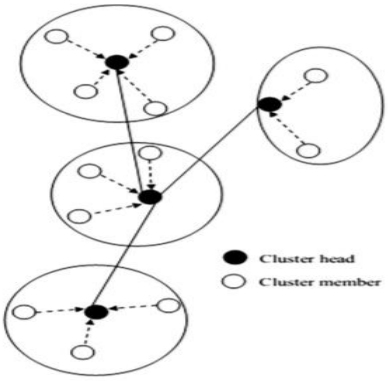

Fig.1: Cluster head selection

The attacked nodes by its certificates may sometimes be revoked by a TA earlier to their conclusion periods. The accumulator assures that a documentation is not over-ridden its period of validity and sequentially verifies non-membership witness as well as witness nodes. Every unit of the network will have the ability in using this collected amount towards validating the validity of a delivered certificate if they acquire connecting non-membership evidence. Rather than directing, the TA towards entire nodes in the cluster, it delivers this valid certificate towards the CH.

At this point, the preservation of the measurement of an collected group of witness nodes (active nodes) is done by every CH that works similar to MR (mobile repositories) and the measurement of revoked nodes ids is achieved. The CH will be requested if some information about its certificate is needed by some of the cluster members. The transmission of messages is obtained securely by the usage of symmetric cryptography method, if it recognizes valid certificate after attaining the information from CH, wherever the encryption as well as decryption of certificates might take place. The block diagram of our proposed scheme is represented in Figure 2.

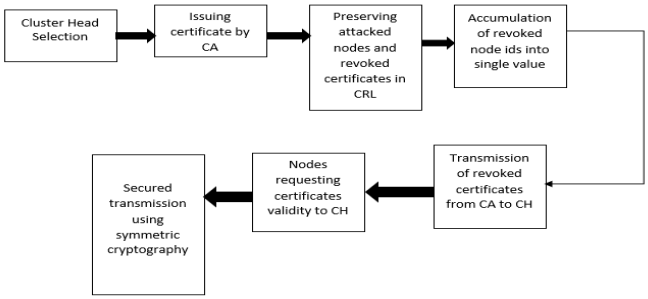

Fig.2: Block diagram of proposed scheme

3.2 Issuing certificates by TA

The things behind this task are given below:

Certification authorities

Generating the collection of certificates is the responsibility of the TA's. Distributing the revocation information and permitting it for accessing the remaining entities is also the responsibility of the TA. By the overall entities of the network, the TA must be entirely assumed to be trusted, therefore it need to be agreed that the attacker should not trade off.

Road-side units

According to the clusters intermediate node, the RSU will operate. By the support of TA, The RSU receives the details of the certificates and is communicated to each CH which suits its range. The TA is managed entirely by RSUs which remain the constant entities. Since the RSUs are placed on the establishment side which doesn't experience the loss of links, they have the capacity to obtain the TA at any time. The RSU is cancelled by TA when TA is considered.

Process of revoking the certificates using CRL

The nodes may be destroyed by the entrance of the malicious certificates, when TA distributes the certificates to the nodes. The

CRL remains a list which stores the documentations of the node that is failed.

IV. RESULT AND DISCUSSION

By means of the simulator NS2, the proposed NCSCR is considered. In this simulation, around 24 nodes are allocated.

Parameter	Value
Application Traffic	CBR
Transmission rate	1000 bytes/0.1ms
Radio range	250m
Packet size	1000 bytes
Maximum speed	25m/s
Simulation time	9000ms
Number of nodes	24
Area	1500x1500
Routing protocol	AODV
Queue	Queue/DSRC
Routing method	NCSCR, ID-MAP, PBAS

Table1: Simulation table

Simulation values as well as parameters of our proposed method are presented in Table 1. In the region of 1500 m × 1500 m, the nodes are unsystematically positioned and in the field of radio range as 250m. 100 J is the early energy of nodes utilized in this replication.

In the Table1, shows that the parameters of system that are utilized in our simulations. We make use of Application Traffic as CBR (Constant Bit Rate) it could be supported to control the traffic in network, Routing Protocol as AODV and it is used for routing level in network, Routing Methods are NCSCR, ID-MAP, and PBAS in our simulation, and this routing approached are used efficiently to perform the outcomes of network. Then, the rate of transmission is 1000 bytes/0.1ms by taking into the consideration of the Packet size as 1000 bytes and with a Maximum speed 25m/s and the total Simulation time is 9000 msec.

4.1 Evaluation results

In this section, we utilize key distribution through TA and provide the authentication to all vehicles based on routing method. According to the computation overhead, communication overhead, average message delay, average message loss ratio, average message delay speed, and average message loss speed, we present experimental results of the algorithm which are introduced below.

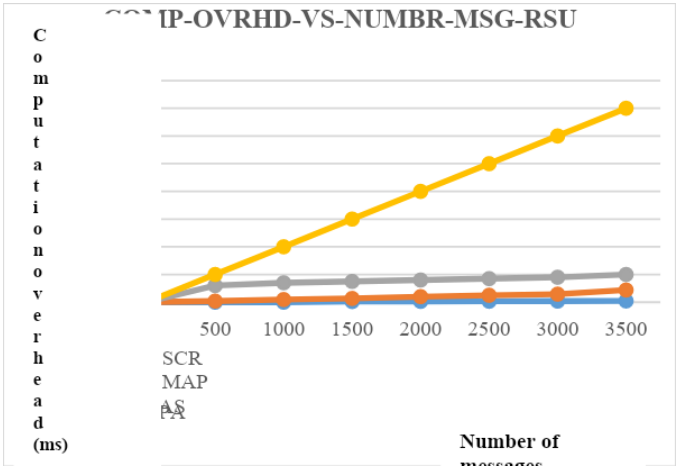

Fig.3: Computation overhead

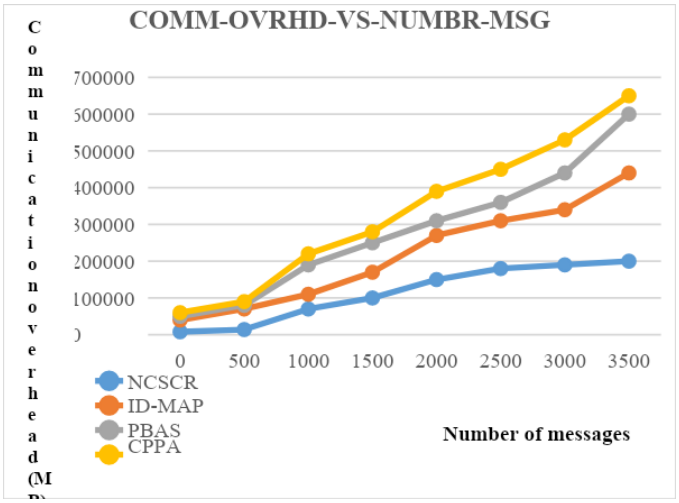

Fig.4: Communication overhead

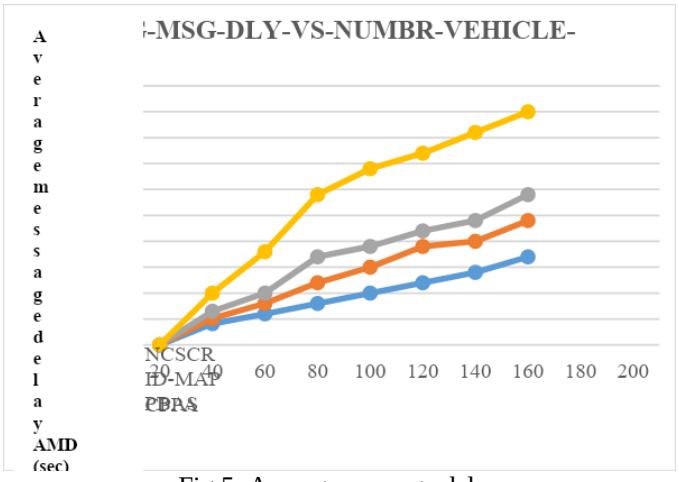

Fig.5: Average message delay

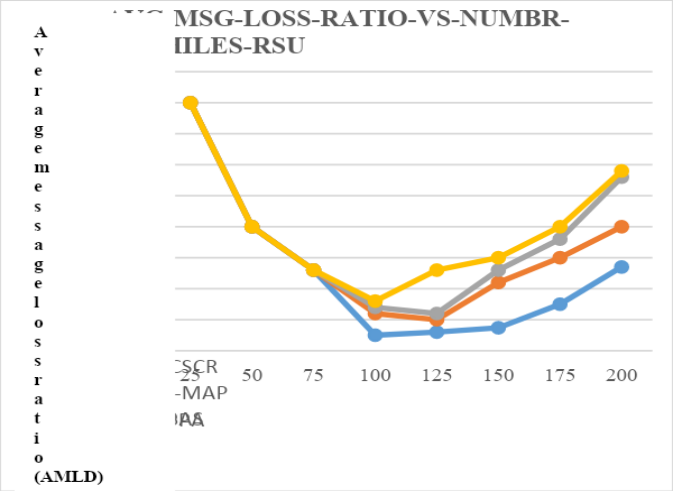

Fig.6: Average message loss ratio

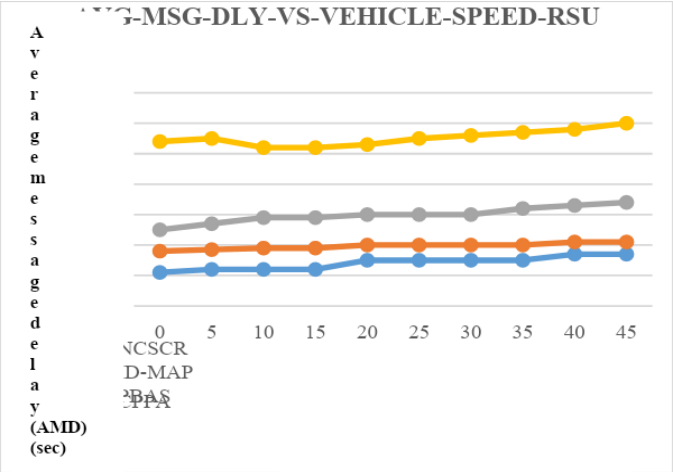

Fig.7: Average message delay speed

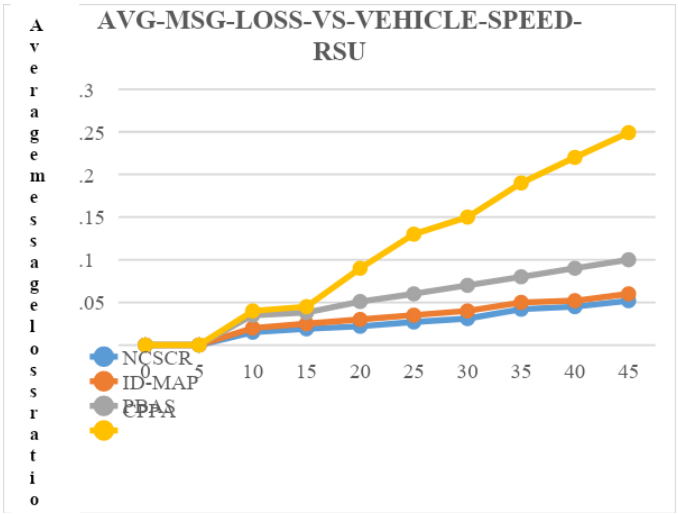

Fig.8: Average message loss speed

In fig 3, this graph would be showing and representing computation overhead. It shows a number of messages versus overhead. Here, in NCSCR, ID-MAP and PBAS, the verification of maximum number of messages is done by an RSU per second. Fig 4 graph would show and represent Communication overhead. Fig 4 is showing and representing the communication overhead. It shows a number of messages versus overhead. Therefore, when the earlier effective and secure verification methods are compared, NCSCR consumes an improved communication overhead next to RSUs as presented in Fig. 4. In figure 5, shows number of vehicles versus average message delay. The time occupied for transmitting the messages from vehicles towards an RSU and the average message delay comparison is shown in Figure 5. The average message loss ratio comparison, the amount of dropped messages and the total amount of messages recovered ratio using an RSU is shown in Figure 6. With regard to the vehicle's average speed, the average message delay comparison of anticipated method and the existing schemes is shown in Figure 7. In terms of average speed of vehicles, the comparison of average message loss ratio of our suggested method NS-SCR, ID-MAP, PBAS is shown in figure 8.

V. CONCLUSION

For VANET, an NCSCR authentication method has remained proposed in this paper. Therefore, the secure communication among the vehicles is maintained with certificate revocation method by the implementation of cryptography scheme. The entire non-terminated certificates of the attacked nodes are revoked by TA and the certificates of the attacked node might not fail. All the particulars about the active nodes as well as the attacked nodes are stored by CH, which is received by TA. The CH is requested to share the particulars regarding the validity of the documentations using the entire cluster members. The trustworthiness of the nodes is validated by the proposed method and similarly verifies whether the node is authenticated or not. The existing method performance is paralleled by the simulation outcomes of NCSCR approach. On reducing the key size for every single iteration of routing is concentrated as future work. Therefore, in order to transfer a message that is produced in the course of an event, a smaller amount of information is necessary. The computation interval as well as communication overhead can therefore be decreased by keeping the same security standard. With regard to computation error as well as duration of average link, this effort may be prolonged in accepting robustness of the algorithm.

VI. REFERENCES

[1]. S. Zeadally, R. Hun, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217–241, 2012.

[2]. M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, "Detecting misbehaviors in VANET with integrated root-cause analysis," Ad Hoc Networks, vol. 8, no. 7, pp. 778–790, 2010.

[3]. Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 74–88, 2008.
[4]. D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681–2691, 2015.
[5]. M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," IEEE Wireless Communications, vol. 13, no. 5, pp. 8–15, 2006.
[6]. J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," IET Communications, vol. 4, no. 7, pp. 894–903, 2010.
[7]. J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security Privacy, vol. 2, no. 3, pp. 49–55, 2004.
[8]. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.
[9]. R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. of the 27th Int. Conf. on the Computer Communications- IEEE INFOCOM 2008. Phoenix, AZ, USA: IEEE, 13-18 April 2008, pp. 1903–1911.
[10]. 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 Int. Conf. on Computer Communications-IEEE INFOCOM 2008. Phoenix, AZ, USA: IEEE, 13-18 April 2008, pp. 816–824.
[11]. T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," Ad Hoc Networks, vol. 9, no. 2, pp. 189–203, 2011.
[12]. C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," Wireless Network, vol. 19, no. 6, pp. 1441–1449, 2013.
[13]. 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.
[14]. K.-A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1874–1883, 2012.
[15]. J. Zhang, M. Xu, and L. Liu, "On the security of a secure batch verification with group testing for VANET," International Journal of Network Security, vol. 16, no. 5, pp. 355–362, 2014.
[16]. Y. Liu, L. Wang, and H.-H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 64, no. 8, pp. 3697–3710, 2015.
[17]. J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J.-P.Hubaux, "Mix-zones for location privacy in vehicular networks," in Proc. of the 1st Int. ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS). Vancouver, BC, Canada: ACM, 14 August 2007, pp. 1–7.
[18]. C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. of IEEE Int. Conf. on Communications (ICC 2008). Beijing, China: IEEE, 30 May 2008, pp. 1451–1457.
[19]. A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. of 4th Annual Int. Cryptology Conf. on Advances in Cryptology- CRYPTO 1984. Santa Barbara, CA, USA: Springer-Verlag, Berlin, 19-22 August 1985, pp. 47–53.
[20]. M. R. Asaar, M. Salmasizadeh, W. Susilo and A. Majidi, "A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5409-5423, June 2018.