Secured Multi-Hop Clustering Protocol for Location-based Routing in VANETs

K. Sushma Eunice[1], I. Juvanna[2]
IT. HITS, Hindustan Institute of Technology and Science
Chennai, India

***Abstract*—In today's world, with the rise in the count of vehicles and lack of proper navigation, the congestion has become a major problem. In this scenario, VANETs play a very important part in improving the traffic condition and also in providing proper navigation. Improved navigation system reduces congestion thereby reducing the possibility of occurrence of accidents. In this research work, we have used a position-based routing protocol i.e., GPSR (Greedy Perimeter Stateless Routing Protocol) to effectively analyze the geographical position of the vehicles in the network and to provide updated navigation information. In this system, we have used a security mechanism to identify valid and invalid messages for secure V2V and V2I communications. This mechanism drops all the invalid messages thereby keeping the VANET secure. It also reduces the possibility of attacks on wireless communications in the VANET. This system has better safety features and network performance compared to other hybrid schemes via NS2 simulation.**

Keywords*—Vanet; tamper-proof device; location-based routing protocols; intelligent transportation system; gpsr algorithm; trusted authority; roadside unit; routing protocols

I. Introduction

Advancements in the automobile industry and rise in the economy standards have led to a significant upsurge in the number of vehicles. However, with the increased vehicle count, traffic congestion also rises. Increased traffic congestion may lead to frequent accidents. The major problem that exists in today's transportation system is congestion. Congestion needs to be handled well to prevent road accidents. Therefore, the need of the hour calls out for reliable experience in driving and improved safety for drivers. All these circumstances have paved a way for research in VANETs with the aim of improving the safety of the drivers through inter-vehicle communication (V2V) and communications between a vehicle and public infrastructure (V2I) [2]. The VANET architecture comprises of three main parts. The architecture of VANET is shown in Fig. 1.

A. System Architecture

- Trusted Authority (TA): The major role of trusted authority is to register every vehicle and to issue secret keys. Trusted authority acts as a trusted management center. The communication link between trusted authority and RSU is wired. The channel connecting the trusted authority and the RSU is very efficient. As it a strong wired network, it acts as a very good channel for proper transmission of data. TA acts as a central system, which issues secret keys and necessary parameters of the system. This information is needed for RSUs and vehicles to verify the authenticity of the messages. TA is responsible for delivering these keys to RSUs and vehicles through secure channels. It is also responsible for locating and finding the vehicles which have sent malicious messages to create problem in the network. In this process, it identifies the malicious message sender and helps to resolve the dispute.
- Road Side Unit (RSU): The RSU is placed along the roads and it serves as a link between the trusted authority and the vehicles (ordinary vehicles or edge computing vehicles) [3], [4]. Roadside units are stationary, and they help the vehicles to connect to different vehicles outside the network. RSU can authenticate the messages as well as it can assign the task to edge computing vehicles (ECV) [7]. Edge computing vehicles (ECVs) share the load of the RSUs by verifying the messages that are being transmitted. ECVs need to report to the RSU with the verification result within a stipulated time T. If the RSUs does not receive any response from ECV in the prescribed time, it simply assigns that verification task to other ECV.
- On-Board Unit (OBU): Vehicles is network is equipped with an OBU. OBU is responsible for inter-vehicle communication (V2V) and communication between vehicle and public infrastructure [3], [4]. As V2V and V2I communication are wireless, they are prone to more attacks. It is important to secure these wireless communications in order to stay out of the attacker's hands. Attackers always keep an eye on the weak wireless communications to take advantage at any point in time. Hence it is always important to provide enough security to the messages that are transmitted. Sender and receiver both need to be aware of fraudulent messages. Additionally, the vehicles will have a tamper-proof device (TPD) that stores the keys issued by the Trusted Authority (TA). Tamper-proof devices help to achieve physical level security [3].

The main objective of this system is to efficiently utilize the intelligent transportation system for secure communication and better navigation. This system analyses attacks on wireless communications i.e., V2V and V2I. The cars can no longer be considered as mechanical machines. They are loaded with software to make them intelligent systems rather than just being a mechanical machine. These intelligent systems are now used for secure communication with other

vehicles and to pave a way for the efficient and enhanced driving experience. It provides up-to-date routing information by using the GPSR protocol and also validates the messages being transmitted by using a security mechanism. It drops all the invalid messages by enhancing the security in VANET.

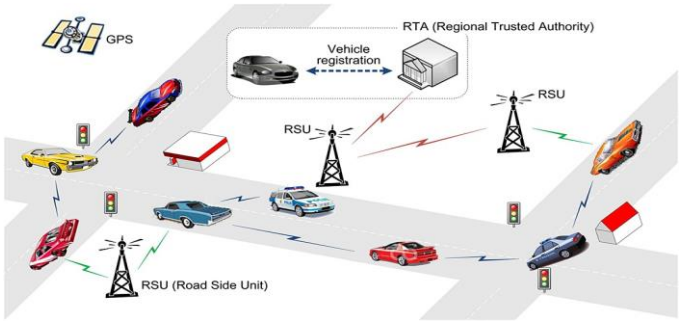

Fig. 1. The Architecture of VANET.

II. Related Works

J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, S. Gao and C.Liu [1] proposed a review on routing protocols. From this research work, we can infer the pros and cons of different routing protocols and can analyze efficient routing protocols. The key technology in vehicular ad-hoc networks is the routing protocols and this paper gives a clear picture of the importance of routing protocols.

Y. Xie, L. Wu, Y. Zhang and J. Shen [2] proposed a scheme for secure authentication with conditional privacy. This paper focuses on challenges that we come across while designing the authentication for VANETs to achieve security and preserving conditional privacy. From this work, we can be well prepared for all the issues that we come across while designing the authentication procedures in the vehicular ad-hoc network.

S. Jiang, X. Zhu, and L. Wang [3] proposed an efficient scheme based on HMAC. In this research work, the vehicles are managed by the RSUs in localized order. From this, we can make the RSUs deal with authentication of vehicles in its range to improve the efficiency of the system.

S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin and A.Hassan [4] proposed a paper on challenges, results, and status of VANETs. From this research work, we can infer various challenges that we face while dealing with VANETs. This provides an insight into the proper working of VANETS.

Y. Sun, R. Lu, X. Lin, X. Shen and J. Su [5] proposed a scheme on pseudonymous authentication with secure privacy preservation. From this research work, we can conclude that pseudonymous authentication scheme with good privacy protection provides very strong protection of privacy of the vehicles and it also does not let adversaries trace the vehicle even if the RSU gets compromised.

C.-C. Lee and Y.-M. Lai [6] proposed a batch verification scheme with group testing. In this research work, group testing is performed to lower the time taken and to boost the efficiency of the system. VANET being intelligent transportation system has a huge number of vehicles and hence transmits a huge number of messages. Authenticating these messages one by one is a time taking process, hence from this paper we have known that group testing can handle huge traffic which is proved to be efficient.

D. He, S. Zeadally, B. Xu and X. Huang [7] proposed an efficient scheme on preserving privacy in the authentication process. In this scheme, security and the problems that exist in preserving privacy are addressed. It takes care of both privacy protection and mutual authentication. It has relatively good performance in terms of computational cost and communicational cost. This scheme can be adapted to lower the communicational and computational cost.

V. Miller [8] proposed a paper on elliptic curves in cryptography. The author used the elliptic curve in cryptography for the first time to enhance security. From this research work, we can imply that we can use the elliptic curve in cryptography.

Jie Cui, Lu Wei, Jing Zhang, Yan Xu and Hong Zhong [9] proposed a paper on a message-authentication scheme using edge computing. This research work validates the messages being transmitted between different vehicles in the network. This system helps us to verify the messages exchanged in the network to keep the VANET secure.

Brad Karp and H. T. Kung [10] proposed a paper on GPSR protocol. It provides complete working of the protocol. This information can be used to adopt the GPSR protocol and to enhance it.

III. Identification of Valid and Invalid Messages

This system deals with the identification of valid and invalid messages in VANET. In this system, there are six different phases [9].

A. Initializing the System

Trusted authority is the central system which oversees issuing necessary parameters of the system and secret keys. These secret keys and system parameters are necessary for identifying each vehicle in the network. Trusted authority traces the vehicles based on these system parameters and keys that are stored in the vehicles. Trusted authority loads all the parameters of the system into the vehicle's TPD and the memory of RSU in advance. Trusted authority and RSU are connected via a wired network for transmission of data. The significant steps involved in this phase are as follows.

- Trusted authority (TA) uses two prime numbers and an elliptic curve E which is non-singular where it is defined as $y^2 = x^3 + ax + b \bmod q$.
- Trusted authority selects the system private key randomly and based on that it calculates the public key of the system.
- Trusted authority selects the roadside unit's private key and based on that it calculates the public key of the roadside unit (RSU).
- A trusted authority is responsible for assigning true-identity and password to all the vehicles. It loads all the vehicle's tamper-proof devices with the vehicle's real identity, password, and the system private key.

- A trusted authority is the sole in charge of producing all the public parameters of the system to all the vehicles and RSUs.

B. Generation of Vehicle's Signature and Pseudo-Identity

All the vehicle's need to produce the signature of the message before sending the message to ensure its authenticity. By producing the signature, the sender vehicle proves its authenticity. Tamper-proof device (TPD) issues pseudo identity, signature, and key for all the ordinary and edge computing vehicles.

- Every vehicle will have a TPD, which maintains the vehicle's real identity, password and the system's private key to connect to the system when it comes within the range of that system. The vehicle cross-checks its real identity and the password by matching its value with the values stored in the TPD by sending its value to the TPD.
- TPD hides the true identity of the vehicle from other vehicles and systems apart from the TA. TPD hides the true identity of the system by generating pseudo-identity which is calculated by using randomly selected number.
- Every vehicle needs a signature to ensure the authenticity of the message. The message's signature is calculated by combining the message M and time stamp T [9].

C. Election Strategy of Edge Computing Vehicle (ECV)

Edge computing vehicle (ECV) helps the RSU to authenticate the message signature as much as possible. ECV is elected based on two factors.

- Shortest distance to RSU
- Enough available computation power

Shortest distance to RSU can be calculated by using the distance membership function and enough available computational power can be calculated by using the available performance metric membership function [9]. All the above calculations can be performed using fuzzy logic.

$$DM(x) = 1,\ d(x) \leq (R/2) \quad (1)$$

$$DM(x) = (R - d(x))/(\frac{R}{2}) \text{ for } (R/2) < d(x) \leq R \quad (2)$$

$$DM(x) = 0,\ d(x) > R\ . \quad (3)$$

Where

DM(x) denotes the distance membership function.

R denotes maximum transmission range of RSU.

d(x) denotes space between the vehicle and the RSU

$$APM(x) = (MCL(x) - UCR(x))/(MCL(x)) \quad (4)$$

Where

APM(x) denotes the available computational power

MCL(x) denotes maximum computational load on the vehicle

UCR(x) denotes the used computational resource of the vehicle.

D. ECV Authenticates the Batch here, there are Two Phases.

- Phase determining the task: Here, the pseudo identity list is allocated to the edge computing vehicle (ECV) by RSU to authenticate the message. After allocating the list to ECV, RSU then updates ECV by sending a message to it.
- Batch authentication and Result feedback stage: ECV carries out the task of verifying the messages sent by RSU by using the preloaded key of RSU. ECV verifies the message and rejects the message if it is invalid and proceeds to the next step if the message is valid.

E. RSU Verifies the Authentication Result of ECV

Loss of packets and delay always exist in VANETs to some extent. So RSU shares its load with ECV to perform message authentication in an efficient way. RSU waits for the verification result from ECV for a prescribed amount of time and if it doesn't receive the message within that time, then it assigns the verification task to another ECV [9]. In this way, RSU lowers the delay in VANETs. Otherwise, if the RSU receives the verification result from ECV within time T, then it checks the result and proceeds to the next step if the message is valid else rejects the message.

F. Authenticating the Ordinary Vehicle's Messages

The ordinary vehicles don't have to verify the messages separately. It is taken over by ECVs and RSUs.

1) Drawbacks of this system: this system only verifies the valid and invalid messages that are being transmitted in the VANET. It does not address the routing issues to provide an enhanced driving experience to the users. The user needs to check for an alternative solution if he needs routing information.

IV. Secured Multi-HOP Clustering Protocol with Location-based Routing

The proposed system deals with the congestion issue in a very effective way. We are using the GPSR routing protocol which is very efficient among other position-based routing protocols. It provides better routing as it uses the buffer of the vehicles to provide an updated route to deal with the frequently changing network. In addition, we have integrated a mechanism to identify valid and invalid messages in the VANET.

A. Greedy Perimeter Stateless Routing Protocol (GPSR)

VANETs are considered as intelligent transportation systems. There are many protocols to provide proper routing in VANETs but position-based routing protocols are the efficient ones. In VANETs routing protocols play a very important role. A routing protocol is a key technology that determines the performance of vehicular communication like inter-vehicle communication (V2V) and communication between vehicle and public infrastructures (V2I). The major problem that exists in the VANET is the frequently changing network. The network comprises of various nodes which are

not stationary. Hence the network topology changes and the relation among the nodes becomes unstable. Focussing on the major problem that exists in most of the routing protocols, we have proposed an enhanced Greedy Perimeter Stateless Routing protocol (GPSR) which has better performance as it depends on the buffer of the nodes for routing.

Greedy perimeter stateless routing (GPSR) functions in two different ways.

- Greedy Forwarding
- Perimeter Forwarding

GPSR protocol uses greedy forwarding method or perimeter forwarding method to route the packet to the destination. GPSR packet stores five values, which help the start node to route the packet to the destination node without any mix-up. GPSR Packet is shown in Fig. 2.

GPSR packet consists of five different fields, where D denotes Destination.

Lp denotes the place where the data packet enters into the chosen mode (Eg: Perimeter mode).

Lf denotes the initial node it started within the face of the graph (planar).

e0 denotes the traversal of the first edge on the current face.

M denotes the mode of the packet: GREEDY MODE / PERIMETER MODE.

1) Greedy forwarding: In this mode, every node broadcasts its IP address and position (IP, (X, Y)) periodically. Every node maintains a table and stores the position of its one-hop neighbors [10]. With respect to the data maintained in the table, the packet is routed to its destination. As every node broadcasts its IP address and position information, all the nodes will have a piece of up-to-date information about all the routes. This reduces the delay in delivering the packets and paves a way for efficient routing. Congestion issue is also handled very efficiently as there is effective communication between the nodes. There are few cases where greedy forwarding fails and in such case, we go for perimeter forwarding. Greedy forwarding fails when a node that has the packet does not have any one-hop neighbor.

In the below figure there are 12 nodes where node S is a source node, node D is the destination node and all the other nodes are considered as intermediate nodes. Now lets assume that node S has a packet and it has to deliver the packet to the destination D. So node S checks its one-hop neighbor which is closest to the destination i.e., node C and routes the packet to its one-hop neighbor node C. Similarly node C using its table finds its one-hop neighbor which is nearest to the destination D and routes the packet to that node to reach the destined node. In this process, if a node come across a situation where it does not have anyone hop neighbor then greedy forwarding method fails and it switches to perimeter forwarding method.

Fig. 2. GPRS Packet.

From Fig. 3, the path that is obtained by following the greedy forwarding method to reach the destination node is S-C-L-N-P-D. This sequence is selected based on the information stored in the table that each node stores.

2) Perimeter forwarding: The network contains certain regions where the greedy path does not exist (i.e., absence of one hop neighbors), in such case GPSR uses perimeter forwarding method to recover from that situation. In the perimeter forwarding method, the right-hand rule is used to calculate the perimeters to transmit the data packet to the destined node.

Perimeter forwarding method follows the right-hand rule to route the data packet to the destined node [10]. From Fig. 4, we see that a packet is forwarded from start node S to end node D in the direction of arrows i.e., by following the right-hand rule.

B. Identification of Valid and Invalid Messages

This module verifies all the messages that are being transmitted between the vehicles and the RSU/TA. The verification process is conducted in the following way.

- All the vehicles are equipped with a tamper-proof device (TPD) which log the necessary vehicle information like vehicle true-identity, vehicle password and the private key of the system.
- Trusted authority generates all the necessary parameters that are required for identifying vehicles and the roadside units (RSUs).
- Trusted authority and the RSUs are connected via a wired network for secure and efficient communication. It uses an efficient protocol like Transport Layer Security (TLS) for secure communication.
- A trusted authority is the central system which controls RSUs and the vehicles in the VANET. It is responsible for taking necessary action like tracing the suspect vehicle in case of any dispute/accident.
- There are few vehicles which are elected as edge computing vehicles (ECVs) based on the closeness to RSU and available computational resource. These vehicles work as both producers and consumers. They take care of the work-load on RSU in verifying the messages thereby reducing the load on the RSU.
- The advantage of using ECVs is that it reduces the RSU's overhead thereby enhancing its efficiency.
- RSUs and ECVs identify valid and invalid messages. If any message is identified as invalid, it is rejected.
- Ordinary vehicles no longer need to authenticate the messages received. This task is done by RSUs and the ECVs.

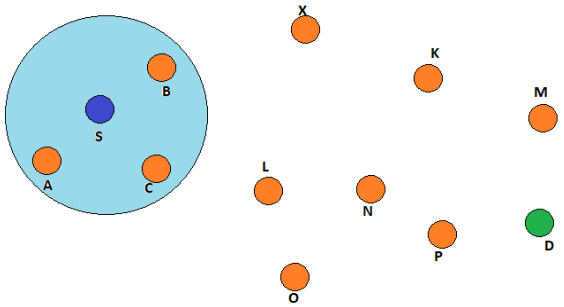

Fig. 3. Greedy Forwarding.

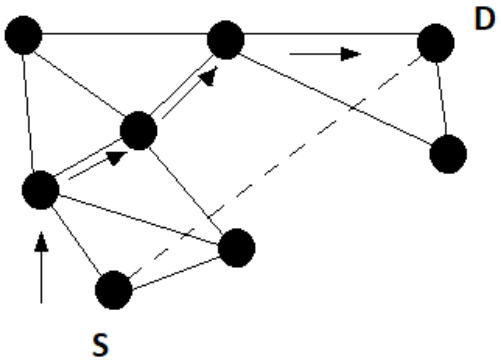

Fig. 4. Perimeter Forwarding.

So all the valid messages are forwarded to the intended vehicles and all the invalid messages are rejected thereby leaving no scope for malicious activities in the VANET.

V. Simulation and Analysis

The results of the simulation are shown here to illustrate the presentation and behavior of the algorithm used.

NS2 is used to show the nodes which represent the vehicles and the transmission of data between them. From Fig. 5, we see that eight nodes are used to represent eight cars moving on the road, four cars moving on the left side of the divider and the other four cars moving on the right side of the divider. The leftover nodes are used to mark the road corners.

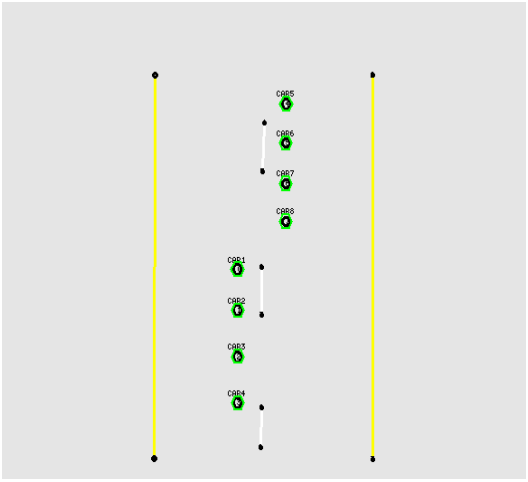

Fig. 5. Nodes Moving on the Road.

In Fig. 6, car 2 has stopped for some reason and broadcasted a message with its location and IP to update the nearby vehicles to change their route to avoid an accident. After receiving the message, the vehicles coming behind car 2 will change its route to avoid an accident. By communicating successfully and securely, vehicles can avoid accidents and can have a better and safe driving experience and navigation. By this, we can say that vehicles can no longer be considered as just mechanical machines. They have improved to a great extent contributing to the intelligent transportation system.

Energy is estimated based on the simulation results obtained using NS2. Fig. 7 depicts the energy. RSUs verify and validate the transmitted messages and hence the energy is calculated based on the count of messages transmitted to the count of messages validated by RSU.

Throughput is estimated based on the simulation results obtained. Fig. 8, depicts Throughput. Throughput is estimated by taking in to account, the quantity of data/messages transmitted with respect to time.

Packet delivery ratio is assessed by analyzing the obtained simulation results. Fig. 9, depicts packet Delivery Ration. Packet delivery ratio is analyzed by noting down the count of vehicles and distance covered.

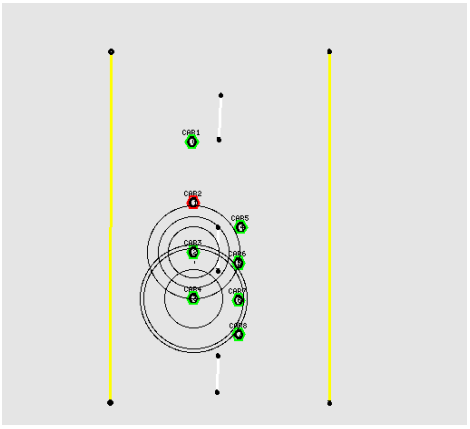

Fig. 6. Nodes Communicating with Each Other.

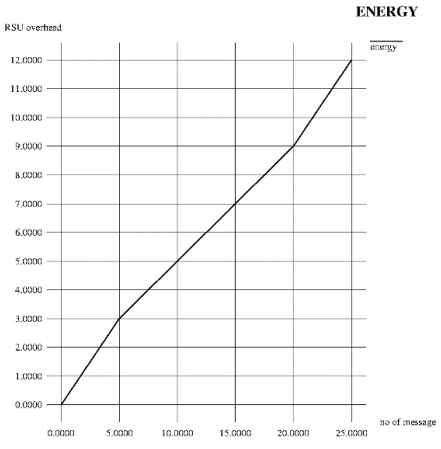

Fig. 7. The Relation between RSU Overhead and the Number of Messages Transmitted.

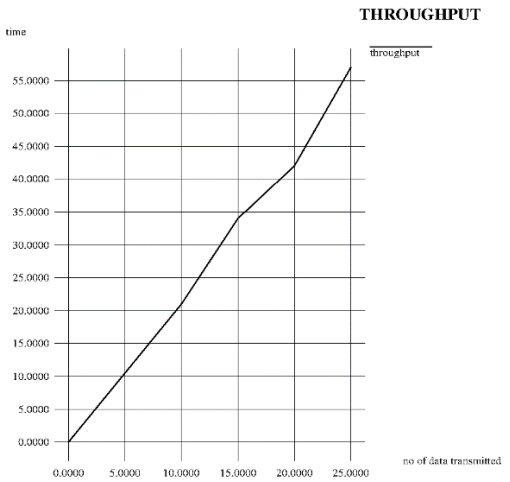

Fig. 8. Relationship between Time and the Amount of Data Transmitted.

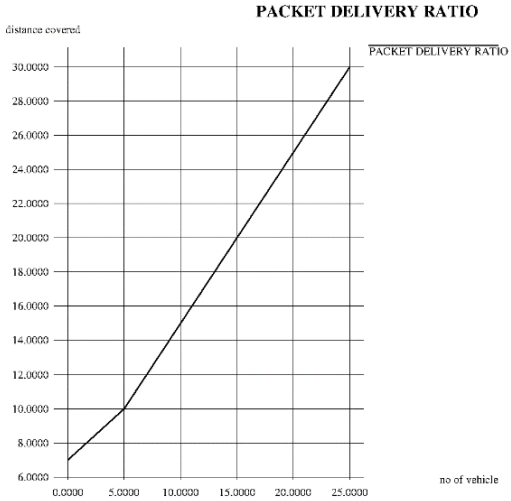

Fig. 9. Relationship between the Number of Vehicles and Distance Covered.

VI. Conclusion

From this study, we can conclude that congestion can be reduced and at the same time malicious messages can be avoided in the VANET thereby reducing the scope of attacks over the vehicular ad-hoc network (VANET). The throughput and the packet delivery ratio are enhanced with this system. The overhead on the RSU is also reduced by electing edge computing vehicle (ECV) which shares the load on the RSU by verifying the valid and invalid messages. Two-way behavior of ECV i.e., both as producer and consumer is beneficial for the RSU and at the same time for the ordinary vehicles in the VANET.

Acknowledgment

We are very grateful to each and everyone who guided us in each and every step and special thanks to the institution for providing the support.

References

[1] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing on the Internet of vehicles: A review," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 5, pp. 2339–2352, Oct. 2015.

[2] Y. Xie, L. Wu, Y. Zhang, and J. Shen, "Efficient and secure authentication scheme with conditional privacy-preserving for VANETs," Chin. J. Electron., vol. 25, no. 5, pp. 950–956, 2016.

[3] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," IEEE Trans. Intell. Transp. Syst., vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

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

[5] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

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

[7] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Trans. Inf. Forensics Security, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[8] V. Miller, "Use of elliptic curves in cryptography," in Proc. Adv. Cryptology—CRYPTO. New York, NY, USA: Springer, 1986, pp. 417–426.

[9] Jie Cui, Lu Wei, Jing Zhang, Yan Xu, and Hong Zhong, "An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks", IEEE Trans. Intell. Transp. Syst, pp. 1524-9050, Early Access.

[10] Brad Karp and H.T. Kung, "GPSR: greedy perimeter stateless routing in wireless networks", in Proc. 6th Annual Int. Conf. Mobile computing and networking, 2000, pp. 243-254.