Secure HMAC Authentication using DSDV in VANET

M. Malarmathi
Research Scholar
School of Computer Science and Engineering, Bharathidasan University, Trichy

Abstract— Vehicular Adhoc Network (VANET) is a part of MANET where the nodes pass on to vehicles. HMAC authentication scheme based on secretcryptography key technique for VANETs. Even though secretkey is extensively used in VANETs to realize unidentified verification, the presented schemes based on public key suffer from long computation delay in the certificate revocation list (CRL) checking and in the key verification method, significant to high message thrashing(lose). As a result, they cannot meet the requirement of verifying hundreds of messages per second in VANETs. In this scheme, first divide the precinct into several domains, in which roadside units (RSUs) are responsible for distributing group private keys and managing vehicles in a localized manner. Then, use a hash message authentication code (HMAC) to avoid time consuming CRL checking and to ensure the integrity of messages before batch group certification. HMAC may be used to simultaneously verify both the data integrity and the authentication of a message. As a final point, adopt cooperative message authentication among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden. The security and performance analysis show that scheme is more efficient in terms of authentication speed, while keeping conditional privacy in VANETs.

Key words: VANET, DSDV Routing Algorithm, HMAC (Hash Message Authentication Control) Algorithm

I. INTRODUCTION

A Vehicular Ad Hoc Network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. In VANETs, vehicles communicate with Each other, as well as with RSUs, through an open wireless channel, in which attackers can easily get users' private information, such as identity, tracing, etc., if they are not properly protected. A Vehicular Ad-Hoc Network or VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network[1]. VANET turns every participating vehicle into a wireless router or node, allowing vehicles approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As vehicles fall out of the signal range and drop out of the network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created. VANET is a subgroup of MANET where the nodes refer to vehicles. Since the movement of Vehicles is restricted by roads, traffic regulations we can deploy fixed infrastructure at critical locations. The primary goal of VANET is to provide road safety measures where information about vehicle's current speed, location coordinates are passed with or without the deployment of Infrastructure. Apart from safety measures, VANET also provides value added services like email, audio/video sharing etc.

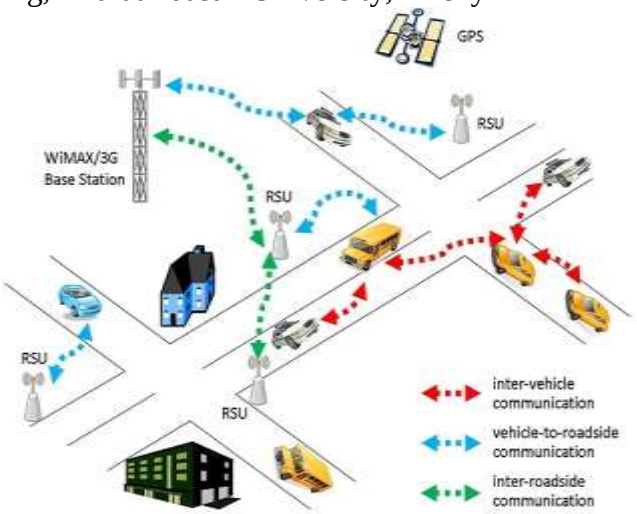

Fig. 1: Vehicular Ad Hoc Network

A. Communication Types

- Vehicle to Vehicle (V2V)
- Vehicle to Infrastructure (V2I)
- Vehicle to Roadside (V2R)

B. Hybrid Models

- Vehicle to Vehicle (V2V) & Vehicle to Infrastructure (V2I)
- Vehicle to Vehicle (V2V) & Vehicle to Roadside (V2R)

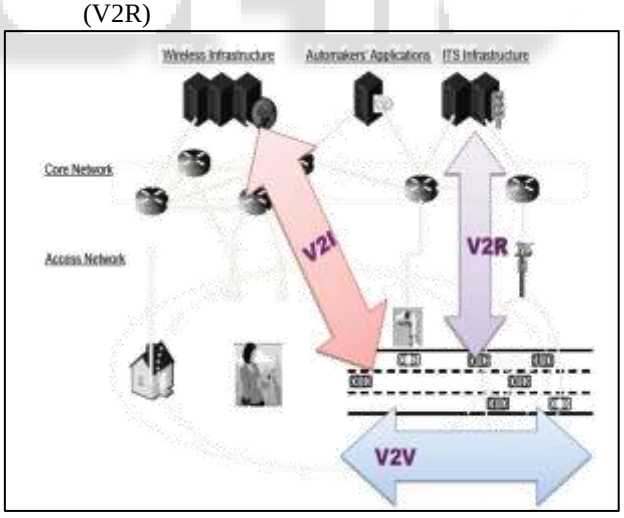

Fig. 2: Communication Types

1) Vehicle To Vehicle Communication (V2V)

Vehicle to Vehicle communication approach is most suited for short range vehicular networks. It is Fast and Reliable and provides real time safety. It does not need any roadside Infrastructure.

2) Vehicle To Infrastructure/Roadside Communication (V2I/V2R)

- Vehicle to Infrastructure provides solution to longer-range vehicular networks.

- It makes use of preexisting network infrastructure such as wireless access points (Road-Side Units, RSUs).
- Communications between vehicles and RSUs are supported by Vehicle-to-Infrastructure (V2I) protocol and Vehicle-to-Roadside (V2R) protocol.
- The Roadside infrastructure involves additional installation costs.
- The V2I infrastructure needs to leverage on its large area coverage and needs more feature enhancements for Vehicle Applications.

II. Routing Methodologies

In V2V communication, the collision warning messages are broadcast from vehicle to vehicle across multiple hops without the involvement of a roadside unit. In case of V2R the warning messages are first sent to a roadside unit, and then broadcast by the roadside unit to all vehicles in range. In V2R/V2V Hybrid Model, Vehicles which receive a warning message via V2V communication will send it to a roadside unit if they did not receive a warning message with the same event ID from roadside units.

With the massive development of wireless communications, ad hoc networking, and Internet of Things, vehicular ad hoc networks (VANETs) have attracted extensive attention and research efforts from academia, industry, and governments in recent years. In a general setting, [7] a VANET is composed of three components: onboard units (OBUs) equipped in mobile vehicles, fixed roadside units (RSUs), and a central trust authority (TA). Being aware of the traffic condition, such as vehicles' position, speed, direction, etc., VANETs are expected to improve the driving experience, traffic safety, and multimedia infotainment dissemination for drivers and passengers. In VANETs, vehicles communicate with each other, as well as with RSUs, through an open wireless channel, in which attackers can easily get users' private information, such as identity, tracing, preference, etc., if they are not properly protected. Another characteristic of VANETs is high-speed mobility, leading to limited communication time among RSUs and vehicles. As a result, we need to design an efficient authentication scheme with privacy preservation for VANETs.

In this paper, propose an efficient conditional privacy preserving authentication scheme for VANETs under the semi-trust model of RSU, by jointly using the techniques of distributed management, HMAC, batch group signature verification, and cooperative authentication. We first divide the precinct into several domains so that the system can run in a localized manner. Then, we calculate HMAC with the group key generated by the self-healing group-key generation algorithm, which can replace the time-consuming CRL checking and ensure the integrity of messages before batch verification. The security and performance analysis show

That the proposed scheme can achieve more efficient group signature based authentication while keeping conditional privacy for VANETs.

III. Overview of DSDV

This protocol is based on classical Bellman-Ford routing algorithm designed for MANETS. Each node maintains a list of all destinations and number of hops to each destination. Each entry is marked with a sequence number. It uses full dump or incremental update to reduce network traffic generated by rout updates. The broadcast of route updates is delayed by settling time. The only improvement made here is avoidance of routing loops in a mobile network of routers. With this improvement, routing information can always be readily available, regardless of whether the source node re-quires the information or not. DSDV solve the problem of routing loops and count to infinity by associating each route entry with a sequence number indicating its freshness. In DSDV, a sequence number is linked to a destination node, and usually is originated by that node (the owner). The only case that a non-owner node updates a sequence number of a route is when it detects a link break on that route. An owner node always uses even-numbers as sequence numbers, and a non-owner node always uses odd-numbers. With the addition of sequence numbers, routes for the same destination are selected based on the following rules: i) a route with a newer sequence number is preferred; ii) in the case that two routes have a same sequence number, the one with a better cost metric is preferred. [3] The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven. Each route update packet, in addition to the routing table information, also contains a unique sequence number as-signed by the transmitter. The route labeled with the highest (i.e. most recent) sequence number is used. If two routes have the same sequence number then the route with the best metric (i.e. shortest route) is used. Based on the past history, the stations estimate the settling time of routes. The stations delay the transmission of a routing update by settling time so as to eliminate those updates that would occur if a better route were found very soon. To damp the routing fluctuations due to unsynchronized nature of periodic updates, routing updates for a given destination can propagate along different paths at different rates. To prevent a node from announcing a routing path change for a given destination while another better update for that destination is still in route, DSDV requires node to wait a settling time before announcing a new route with higher metric for a destination.

IV. Related work

The idea of real-time navigation using VANET is not totally new. In this paper[6], this paper propose a new application—VANET based secure and privacy-preserving navigation (VSPN),which makes use of the collected data to provide navigation service to drivers. Based on the destination and the current location of the driver (the query), the system can automatically search for a route that yields minimum traveling delay in a distributed manner using the online information of the road condition. In addition of driving guidance, the navigation results can also be used for

other purposes. The drawback of this system the authentication process at vehicles can be even simpler because a vehicle only needs to check against the central server's signature on the processed result. However, such a centralized approach is not scalable, especially for large cities.

A similar scheme is proposed in a recent work [8].However, there are a number of differences between their scheme and ours. First, their scheme is of a small scale that covers a car park, while ours is large scale to cover the whole city and beyond. Second, in their scheme a car park is monitored by three RSUs that take up the roles of determining vehicle's location, searching for a vacant parking space, and providing navigation service to guide the vehicle to go from the car park entrance to the selected parking space. In our scheme, the road system in the city is monitored by a large number of RSUs that take up the navigation task in a distributed manner. Third, in terms of security functions, their scheme assumes RSUs to be fully trusted. This makes

Sense because the three RSUs are installed indoors and can be monitored by security guards. However, such an assumption is no longer valid in our outdoor setting. It is impossible to have security guards monitor all RSUs across the city. Thus, unlike their scheme, authentication of RSUs becomes a vital component in ours. Fourth, our scheme allows one's identity and navigation query to be delinked. This feature is only interesting for wide area navigation like ours.

J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in Proc. Mobile New. Veh.Environ. Anchorage, AK, USA, May 2007, pp. 103–108.[9]In this paper propose a novel group signature based security framework for vehicular communications. Compared to the traditional digital signature scheme, the new scheme achieves authenticity, data integrity, anonymity, and accountability at the same time. Furthermore, describe a scalable role-based access control approach for vehicular networks. Finally, present a probabilistic signature verification scheme that can efficiently detect the tampered messages or the messages from an unauthorized node. A group signature scheme allows members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer. Furthermore, it is not possible to decide whether two signatures have been issued by the same group member. However, there exists a designated group manager who can, in case of a later dispute, open signatures, i.e., reveal the identity of the signer.

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. [10] In this paper, propose an efficient pseudonymous authentication scheme with strong privacy preservation, named PASS, for vehicular communications. Unlike traditional pseudonymous authentication schemes, the size of Certificate Revocation List (CRL) in PASS is linear with the number of revoked vehicles and unrelated to how many pseudonymous certificates are held by the revoked vehicles. PASS supports Roadside Units aided distributed certificate service that allows the vehicles to update certificates on road, but the service overhead is almost unrelated to the number of the updated certificates. Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries cannot trace any vehicle even all Roadside Units have been compromised. Extensive simulations demonstrate that PASS outperforms previously reported ones in terms of the revocation cost and the certificate updating overhead.

L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.[11] A number of challenges such as efficient certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong dependence on tamper-proof devices arise in existing protocols for securing VANETs. The proposed a new privacy-preserving authentication protocol that efficiently addresses those challenges by considering the special features of vehicular mobility, road limitations and densely distributed RSUs in VANETs. In system, each RSU maintains an on-the-fly generated group within its communication range, in which vehicles can anonymously generate V2V messages, and verify anonymous V2V messages from other vehicles. Vehicles generating false/bogus messages can be traced by a third party. Our scheme has been shown to be robust, scalable and practical. Furthermore, it clearly outperforms state-of-the-art alternatives in the case of dense traffic.

Y. Hao, Y. Chen, C. Zhou, and S. Wei,"A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.[12] In this paper, propose a distributed key management framework based on group signature to provision privacy in vehicular ad hoc networks (VANETs). Distributed key management is expected to facilitate the revocation of malicious vehicles, maintenance of the system, and heterogeneous security policies, compared with the centralized key management assumed by the existing group signature schemes. In our framework, each road side unit (RSU) acts as the key distributor for the group, where a new issue incurred is that the semi-trust RSUs may be compromised. Thus, we develop security protocols for the scheme which are able to detect compromised RSUs and their colluding malicious vehicles. Moreover, address the issue of large computation overhead due to the group signature implementation. A practical cooperative message authentication protocol is thus proposed to alleviate the verification burden, where each vehicle just needs to verify a small amount of messages. Details of possible attacks and the corresponding solutions are discussed.

Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with protection against RSU compromise in group signature based VANETs," in Proc. IEEE GLOBECOM, New Orleans, LA, USA, Dec. 2008, pp. 1–5.[13] The SMART Highway project combines road construction with advanced technology and vehicle telecommunication. A Vehicular Ad hoc Network (VANET) is the core technology of the SMART Highway, whose transport operation is based on road vehicle. The VANET is

a next-generation networking technology that enables wireless communication between vehicles or between vehicles and a Road Side Unit (RSU). In the VANET system, a vehicle accident is likely to cause a serious disaster. Therefore, some information on safety is essential to serve as the key exchange protocol for communication between vehicles. However, the key exchange scheme of the general network proposed for a fast-moving communication environment is unsuitable for vehicles. In this paper, the initial communication from the RSU is passed only with group keys. Then the key value in the communication is updated when the vehicle itself uses Bloom filters to verify the proposed method. In the proposed VANET scheme, the distributed operations are focused on the RSU and more secure group communication can be achieved by minimizing the number of key exchanges. Accordingly, communication between multiple vehicles more efficient and secure key exchange at the vehicle certification by signcryption and vehicle certification method that uses a counting bloom filter for more efficient certification is proposed.

V. SECURITY REQUIREMENTS

We aim at designing a scheme to provide VANET-based navigation to satisfy the following security requirements:

A. Message Integrity and Authentication

A vehicle should be authenticated before it can issue a navigation query. On the other hand, an RSU (vehicle) is able to verify that a message is indeed sent and signed by a certain vehicle (RSU) without being modified by anyone.

B. Identity Privacy Preserving

The real identity of a vehicle should be kept anonymous from other vehicles as well as from RSUs and a third-party should not be able to reveal a vehicle's real identity by analyzing multiple messages sent by it.

C. Traceability

Although a vehicle's real identity should be hidden from other vehicles and RSUs, TA should have the ability to obtain a vehicle's real identity so that the vehicle can be charged for using the navigation service. Also TA has the role to maintain liability via nonrepudiation property of messages when accidents happen on the road.

D. Confidentiality

The content of a query and that of a navigation result should be kept confidential from eavesdroppers.

E. Unlinkability

Even if all RSUs and TA collude, they cannot link up a vehicle's query with its realidentity. Note that there can be other kinds of attacks such as distributed denial of service (DDoS) attacks in a VANET environment. However, there are already many existing techniques.

VI. PROPOSED WORK (HMAC-DSDV)

A. System Model

The system model of VANETs in this paper consists of a TA, fixed RSUs at the road side, and mobile OBUs equipped in vehicles, as shown in Fig.

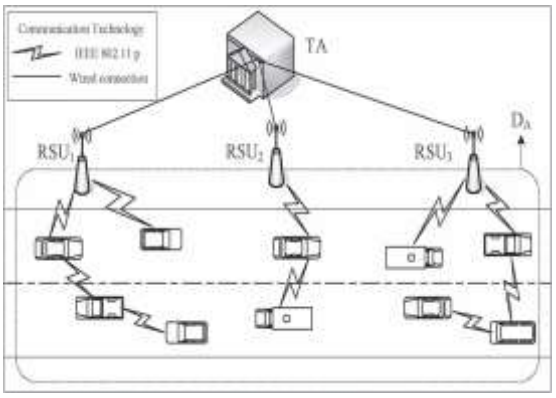

Fig. 4: System model of VANETs

- TA is a trusted management center of the network. It provides registration and certification for RSUs and OBUs when they join the network. It also divides the whole precinct into several domains, generates the group key and group signature materials for every domain, and then sends these materials to the RSUs in the domain. As usual, assume that TA is powerful enough in terms of communication, computation, and storage capability, and it is infeasible for any adversary to compromise.
- RSUs manage and communicate with vehicles in their communication range. They are bridges between TA and end users, which connect with TA by wire and OBUs by a wireless channel. In this paper, we assume RSU to be semi-trust, i.e., they can operate as expected but may reveal data to an adversary. RSUs are also responsible for issuing the group key materials and group signature related keys to validate OBUs when OBUs join the domain.
- OBUs periodically broadcast traffic-related status information containing its location, speed, and direction to improve the road environment, traffic safety, and multimedia infotainment dissemination for drivers and passengers. Each vehicle has a tamper-proof device (TPD) to store Security-related materials. Integrity by attaching a message authentication code (MAC) to the message, which is accomplished by a cryptographic keyed hash function. In this paper, use HMAC for two purposes: 1) ensuring the validity of senders' identities, since only valid users can generate correct HMACs; and 2) checking the integrity of messages before batch verification, thus achieving the efficiency of batch verification.

B. Advantages

The security is more efficient in terms of authentication speed, while keeping conditional privacy in VANETs.
The procedure can be understood by following algorithm:

- Step 1. Sends source and destination address to RSU.
- Step 2. RSU checks the vehicle information using HMAC algorithm.
- Step 3. Get shortest and traffic less path form RSU.
- Step 4. RSU checks the paths
- Step 5. If traffic or accident occurs in any routes at that time informs to the target vehicle.
- Step 6. Divert the target vehicle to another path using DSDV.

– Step 7. RSU sends alert message to nearby emergency services.
– Step 8. Target vehicle achieve its destination with secure path.

HMAC generates a Message Authentication Code by the following formula:

HMAC (M) = H [(K+opad) &H[(k+ipad) & M]]

M = Message
H [] = Underlying Hash function
K = Shared Secret Key
opad = 36hex, repeated as needed
ipad = 5Chex, repeated as needed
& = concatenation operation
+ = XOR operation

The HMAC (M) is then sent as any typical MAC(M) in a message transaction over insecure channels (See section 1). Again, any hash function can be used, but MD5 and SHA-1 seem to be most popular.

Here threshold is the average threshold time of the network. It varies from one network to another network. In our scenario value of threshold is the acknowledgement time of all the packets transmission.

VII. SIMULATION RESULTS

The proposed HMAC-DSDV routing protocol is simulated using NS2 simulator and compared to DH-DSRC routing algorithm. The aim of these simulation runs is to analyze the performance of the proposed HMAC-DSDV protocol and to compare its performance with the DH-DSRC. Performance is compared in terms of average throughput, average delay and average drop packets. Average dropped packets is the ratio for the packets not delivered to RSU and nodes (vehicles), throughputs is defined as the ratio of number of packets received to that of the number of packets sent and the end to end delay is the overall average delay experienced by a packet from the vehicle to that of the RSU or another vehicle.

There are 17 nodes placed randomly in the simulation environment use. Due to random dynamic topology, the source and destination are also selected randomly.

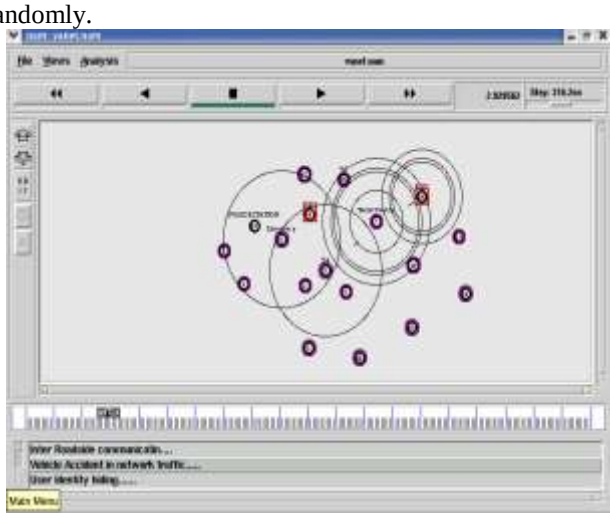

Fig. 1: Message Transmission

This figure 1 shows the transmission of packets using selected path and it shows the random network topologies.

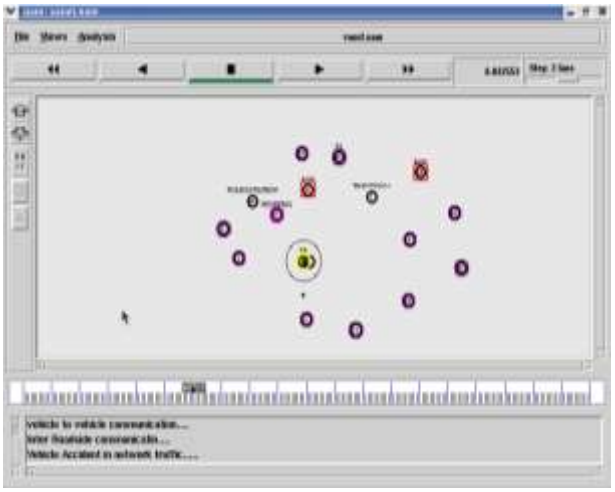

Fig. 2: Message Loss

This figure 2 depicts when the node energy level is low and after transmission of packets node wait for acknowledgement for the threshold phase of time. If packets not received acknowledgement with in threshold time that the time congestion is occurs in the transmission and the loss is start. The node transmit packets and waits for acknowledgement for the threshold period of time. If the acknowledgement not received with in threshold period then the node broadcast again to select alternate path or retransmit the packets and the node energy level is low means to select the another path. Due to this threshold period of time our proposed system detects and control congestion very fast than existing system.

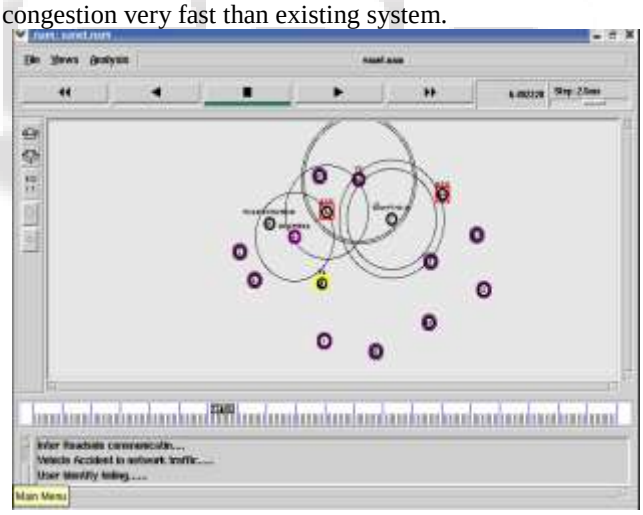

Fig. 3: Message Retransmit to Another Vehicle

This figure 3 depicts the node selects the another vehicle to retrieve destination information with power level is decrease and if packets not received acknowledgement with in threshold time then nodes select alternate path for retransmit packets. And therefore, the packet loss is decreases due to it detect congestion fast and packets retransmit through new path every time. When the congestion is occurs and decrease the node energy level. So, in our proposed system is reduced amount of congestion.

In this section we are viewing results of our proposed system and existing system by using some different performance parameters.

Various parameters used for analysis are described below:

A. Formulae:

1) Packet Loss Ratio (PLR):

It is the ratio of difference between the total number of generated packets and total number of received packets divided by the total number of generated packets.

PLR= (Generated packets- Received Packets)/ Generated packets (1)

2) Packet Delivery Ratio:

Packet delivery Fraction (PDF): It is the ratio of the amount of data packets delivered to the destination and total number of data packets sent by source.

PDF= (Received Packets / Packets Sent)*100 (2)

3) Average End to End Delay:

The interval time between sending by the source node and receiving by the destination node, which includes the processing time and queuing time.

EED=(Time packet received-Time packet sent) / Total no. of packets received (3)

B. Tables:

No. of vehicles	Generated messages	Received message	Message delivery ratio	message loss ratio	Average end to end delay
10	17477	5820	33.3009	0.666991	16.5604
20	23588	8915	37.7946	0.622054	14.4912
30	18681	9177	49.1248	0.508752	14.4734
40	18396	8918	48.4779	0.515221	13.7088

Table 1: Table showing performance analysis of existing system (DSRC)

No. of vehicles	**Generated message**	**Received message**	**Message delivery ratio**	**Message loss ratio**	**Average end to end delay**
10	1644	1634	99.3917	0.0060	1.6572
20	1392	1372	98.5632	0.0143	2.6635
30	873	863	98.8545	0.0115	2.2003
40	954	944	98.9517	0.0105	4.8575

Table 2: Table showing performance analysis of proposed system (HMAC-DSDV)

This table shows the performance analysis of Enhanced Power Coefficient and Hop Count-AODV Algorithm (EPHC – AODV) system on different quantity of nodes. This table depicts that value of all performance parameters shows changeable behavior with the increases number of nodes except packet delivery, average end- to- end delay. And packet loss is decreases with the quantity of nodes.

In this section we also show the comparison analysis between existing and proposed system through graphs using different parameters on different quantity of nodes. And these graphs shows results or performance of our proposed system are better than existing system.

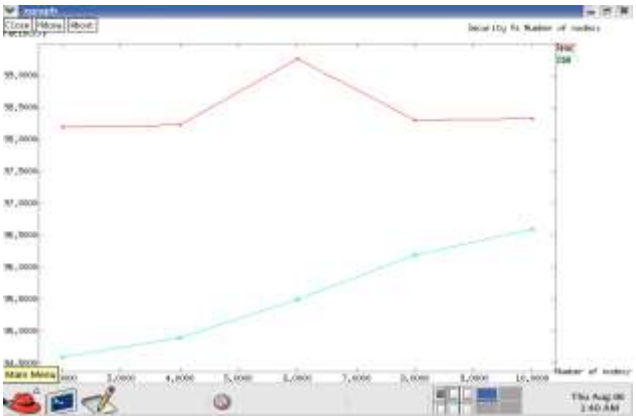

Fig. 4: Comparison of Security in Proposed System and Existing System

The Figure 4 depicts comparison of Packet delivery ratio. The proposed work is to increase the Packet delivery ratio. The nodes are waiting for acknowledgement in threshold phase of time .If the Acknowledgement not received with in threshold phase means congestion is occurs so to select the alternative path or retransmit the packets and when the node energy is low to select the different path. Because the node energy is very important in packet transmission. When the node energy level is low the node doesn't transfer the packet. While in existing system are not use power coefficient and the hop to find the node energy level in the packet transmission. So the existing system detects the congestion very slow. This show our system is more efficient to control congestion than existing system.

Figure 5 depicts comparison of Packet loss ratio. The Packet loss ratio is decreases in our proposed work. The nodes are waiting for acknowledgement for threshold period of time if the Acknowledgement not received with in threshold period which shows congestion so to control congestion the node broadcast again to select alternate path or retransmit the packets. So it detects congestion fast and control congestion effectively when the node energy is decrease to select the different path.

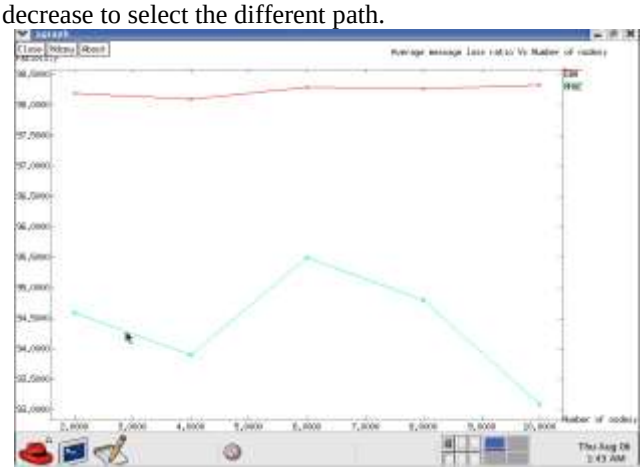

Fig. 5: Comparison of Packets Loss Ratio In Proposed System and Existing System

Many packets are loss in waiting for acknowledgement long time and when the node energy level is low to increase packets loss. While in existing system are not use power coefficient and the hop to find the node energy level in the packet transmission. So existing system is detects and control the traffic very slow. This shows our

system is more effective to control congestion than existing system.

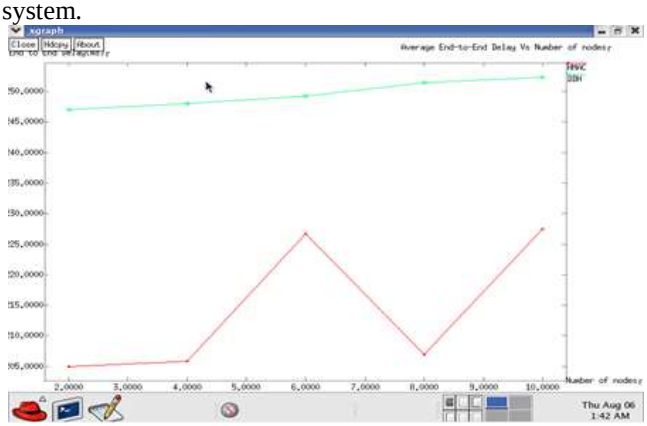

Fig. 6: Comparison of Average End To End Delay In Proposed System And Existing System

Figure 6 depicts comparison of average end to end delay. In our proposed work is to decrease the average end to end delay. Because in this network nodes are waiting for acknowledgement for threshold phase of time, if the Acknowledgement not received with in threshold period that the time congestion is occur. To control the congestion means the node again to select alternate path or retransmit the packets. And when the node energy is low to select the different path. Because the node energy is very important in packet transmission. When the node energy level is low the node doesn't transfer the packet.

So it detects congestion fast and control congestion effectively. While in existing system are not use power coefficient and the hop count to find the node energy level in the packet transmission. So existing system is detects and control the congestion very slow. This shows our system is more effective to control congestion than existing system.

VIII. Conclusion

The proposed an efficient privacy-preserving group signature based authentication scheme for VANETs. The techniques of distributed management, HMAC, batch group signature verification, and cooperative authentication to achieve the design goal. First, divide the whole network into several domains, which allows localized management. HMAC is used in our scheme to replace the time-consuming CRL checking and to ensure the integrity of messages before batch verification, reducing the number of invalid messages in the batch. Cooperative authentication to improve the efficiency of scheme. By employing the given methods, our scheme can meet the requirement of verifying 600 messages per second. The security and performance analysis show that our scheme can achieve efficient group signature based authentication while keeping conditional privacy for VANETs.

In the future work the congestion control schemes are to design a scheme which will allot time slots for beacons and emergency messages. Even if the vehicle density increases and the channel gets exhausted easily, this scheme will allow vehicles to broadcast messages by dynamically partitioning the beacon interval and increasing the transmission duration of messages. So, with the help of this scheme vehicles will be allowed to broadcast emergency messages without the expense of beacons, which are also equally important in vehicular communications.

IX. References

[1] 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. IEEE INFOCOM, Phoenix, AZ, USA, Apr. 2008, pp. 246–250.

[2] 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.

[3] J. Guo, J. P. Baugh, and S. Wang "A group signature based secure and privacy-preserving vehicular communication framework," in Proc. Mobile Netw. Veh.Environ., Anchorage, AK, USA, May 2007, pp. 103–108.

[4] Akshai Aggarwal1, Savita Gandhi, NirbhayChaubey "Performance analysis of AODV,DSDV AND DSR in MANETS" International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, November 2011.

[5] T.W. Chim, S.M. Yiu, and L.C.K. Hui " VSPN: VANET-Based Secureand Privacy-Preserving Navigation" IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 2, FEBRUARY 2014.

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh.Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[7] A.Wasef and X. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," in Proc. IEEE ICC, Cape Town, South Africa, May 2010, pp. 1–5.

[8] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

[9] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANETBasedSmart Parking Scheme for Large Parking Lots," Proc. IEEEINFOCOM '09, pp. 1413-1421, Apr. 2009.

[10] J. Guo, J. P. Baugh, and S. Wang,"A group signature based secure and privacy-preserving vehicular communication framework," in Proc. Mobile Netw. Veh.Environ. Anchorage, AK, USA, May 2007, pp. 103–108.

[11] 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.

[12] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

[13] Y. Hao, Y. Chen, C. Zhou, and S. Wei,"A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.

[14] Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with protection against RSU compromise in group signature based VANETs," in Proc. IEEE GLOBECOM, New Orleans, LA, USA, Dec. 2008, pp. 1–5.

[15] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3357–3368, Nov. 2008.
[16] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in Proc. 8th ACM Int. Symp. MobiHoc, Montreal, QC, Canada, Sep. 2007, pp. 150–159.
[17] M. Raya and J.-P.Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, Jan. 2007.
[18] K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 62, no. 2, pp. 536–551, Feb. 2013.
[19] A.Wasef and X. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 78–89, Jan. 2013.
[20] S. Jiang, X. Zhu, and L. Wang, "A conditional privacy scheme based on anonymized batch authentication in vehicular ad hoc networks," in Proc. IEEE WCNC, Shanghai, China, Apr. 2013, pp. 2375–2380.
[21] Y. Hao, Y. Chen, C. Zhou, and S. Wei, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.
[22] R. Dutta, S. Mukhopadhyay, and M. Collier, "Computationally secure self-healing key distribution with revocation in wireless ad hoc networks," Ad Hoc Netw., vol. 8, no. 6, pp. 597–613, Aug. 2010.
[23] S. Frankel, R. Glenn, and S. Kelly, The AES-CBC cipher algorithm and its use with IPsec, RFC 3602, Sep. 2003.
[24] D. Eastlake and P. Jones, US secure hash algorithm 1 (SHA1), RFC 3174, Sep. 2001.
[25] X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacy preserving authentication based on group signature for VANETs," presented at the IEEE Global Telecommunications Conf., Atlanta, GA, USA, Dec. 2013, Paper WN-23.
[26] K. A. Shim, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1874–1883, May 2012.
[27] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "AKABA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 60, no. 1, pp. 248–262, Jan. 2011.

