Asian Journal of Information Technology 15 (11): 1637-1644, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

Secure Group Authentication Technique for VANET

A. Punitha and J. Martin Leo Manickam
Department Electronics and Communication Engineering,
St. Joseph's College of Engineering, Chennai, India

Abstract: Vehicular Ad-hoc Network (VANET) is a network where vehicles within the network can communicate with each other using the help of the road side equipment. There are wide applications using VANET and hence has emerged as an important technology in the automobile industry. Since, VANET is very helpful in providing the real time traffic information to the vehicle users, offering notification related to the post crash, street hassle handling and traffic vigilance ability, it is widely used and in good demand. But, VANETs are prone to several threats due to its security related challenges like reduced tolerance for error, very high mobility, etc and high rate of attacks like eavesdropping, impersonating, session hijacking on the vehicular network. Hence, safety is a high priority in VANET. In this study, we develop a group authentication mechanism to securely form a group of vehicle that can communicate with each other efficiently.

Key words: VANET, error, communication, hijacking, technology

INTRODUCTION

VANET: Vehicular Ad-hoc Network (VANET) is a promising technology that employs wireless communication networks to facilitate vehicles to communicate with one another and with a fixed infrastructure such as Road Side Units (RSU) (Priya and Karuppanan, 2011). VANETs have attracted a lot of attentions due to their interesting and promising functionalities including vehicular safety, traffic congestion avoidance and location based services (Hao *et al*., 2011). Vehicle-to-vehicle and vehicle-to infrastructure communications improve vehicle's perception from the surrounding environment (Jeon *et al*., 2013).

Intelligent vehicle is evolving with various types of services to provide convenience of life by integrating with home network, telemetric and intelligent robot, thanks to development of convergence technology. Smart vehicles have embedded computers, Global Positioning System (GPS), short-range wireless network interfaces and potentially wireless access to the internet. With these equipments, vehicles can communicate with each other (V2V: Vehicle-to-Vehicle) or with Road Side Units (RSU) which are connected to the internet (V2I: Vehicle-to-Infrastructure) (Feiri *et al*., 2015).

Issues in VANET: The VANETs face a lot of issues due to its features like rapidly changing network topology, unbounded network size, High mobility, etc. Some of the challenges faced are network management, congestion and collision control, environmental impact, MAC design, security, data consistency liability and key distribution. VANETs are also subjected to various attacks such as impersonate, session hijacking, identity revealing, location tracking, repudiation, eavesdropping, denial of service, routing attacks like black hole attack, worm hole attack and gray hole attack. Hence, authentication is very important in VANET to maintain security and privacy.

Authentication in VANET (need for authentication and issues): Authentication is the verification of a user identity prior to granting access to the network. It can be considered as the first line of defense against intruders. Authentication is the cornerstone service, since other services depend on the authentication of communication entities. Authentication supports privacy protection by ensuring that entities verify and validate one another before disclosing any secret information (Wang and Zhang, 2012).

There are different methods are used to authenticate in VANET such as node level authentication, group level authentication, unicast authentication, multicast authentication and broadcast authentication:

Previous research and proposed solution: In our previous research (Chaurasia and Verma, 2011), a secure geographical path routing with location verification

Corresponding Author: A. Punitha, Department of Electronics and Communication Engineering, St. Joseph's College of Engineering, Chennai, India

technique in VANET was proposed. The technique encodes the geographical locations of nodes using geographic hashes. Data packets are transmitted securely over the communication channel through private and public keys of a node. The next hop is carefully chosen by geographic routing. The proposed technique uses two step location verification schemes. In the first step when data is transmitted from the source to its next hop, the packet is verified through reliability checks. In the next step, its location is validated by distance bounding scheme. As an extension to this work, we propose to design a secure group authentication technique for VANET.

Literature review: Priya and Karuppanan (2011) have proposed a Secure Privacy and distributed group authentication for VANET. This GAP protocol is designed for VANET to endow with security services such as authentication, traceability and anonymity preservation. Group signature and batch verification of the protocol significantly reduce the message delay when compared with its counterparts. Multiple RSUs in the case of a high node density help for successful delivery of certificates. The proposed protocol also scales well when the number of messages have increased and improves the service rate. For future work, the protocol can be tested with different batch verification time slots and can also be tested using a roadway traffic simulation such as MOBISIM tool.

Hao *et al.* (2011) has proposed a distributed key management framework with cooperative message authentication in VANETs. In this study, a novel distributed key management scheme based on the short group signature to provision privacy in the VANETs is proposed. The distributed key management is further enhanced with a cooperative message authentication protocol to alleviate the heavy computation overhead. The challenging issue that semi-trust RSUs may be compromised and compromised RSUs may even collude with malicious vehicles is investigated. A security protocol to prevent compromised RSUs and malicious vehicles from attacking is designed. This design guarantees that RSUs distribute keys fairly and provide some mechanisms to detect compromised RSUs and malicious vehicles.

Zhu *et al.* (2013) have proposed a distributed pseudonym management scheme in VANETs. In this study, a secure and efficient pseudonym management scheme for vehicular ad hoc networks is proposed. The scheme not only maintains the property of conditional privacy preservation but also provides the advantages in security against authority forge attacks and better robustness. In the scheme, a pseudonym is coproduced by V and PCA to avoid the deception of either party. A blind signature method is used to achieve the separation of issuance and tracking. Based on the improved share generation scheme of the RSA keys, the distributed tracking protocol is proposed to avoid a single point of failure. By searching for the optimal number of messages with a pseudonym certificate, the efficient pseudonym authentication mechanism is given to reduce communication overhead. By uniting the pseudonym issuance protocol and the tracking protocol, malicious vehicles are revoked easily. The communication cost and computation cost in our scheme are lower. As a result, our proposed scheme is suitable for anonymous communication with tracking requirements in VANETs, since it provides security, robustness and efficiency.

Feiri *et al.* (2015) have presented a technique that performs Pre-distribution of certificates for pseudonymous broadcast authentication in VANET. In this study, a new technique that combines certificate omission and certificate pre-distribution is proposed. This technique significantly reduces cryptographic packet loss caused by pseudonym changes while driving. Moreover, the introduction of certificate pre-distribution is possible without requiring deep changes to existing architectures for certificate management in vehicular communication.

Chaurasia and Verma (2011) have proposed infrastructure based authentication in VANETs. In this study, a mutual authentication technique for RSU and vehicle is proposed. The scheme preserves the privacy of the vehicle. The RSU is used as a mediator for authentication of both the RSU and the requesting vehicle. Since, the CTA is responsible for verifying credentials, the load of the RSU is drastically reduced. The technique has only one request reply message exchange. This reduces the bandwidth requirement and the total communication delay in the authentication process. However, many vehicles enter an RSU region together and request may cause substantial communication delay. The RSUs can reduce this message flow. However, this would increase the certificate storage requirements at the RSUs inordinately. Message flow and storage can be simultaneously reduced by issuing certificates with different validity periods in accordance to vehicle's speed and current traffic state.

Proposed secure group authentication for VANET

Overview: In this study, we propose to design secure group authentication techniques for VANET. In this technique, vehicles perform group signing and verification (Priya and Karuppanan, 2011). Then, they perform co-operative message authentication (Hao *et al.*, 2011). It consists of verifier selection process and

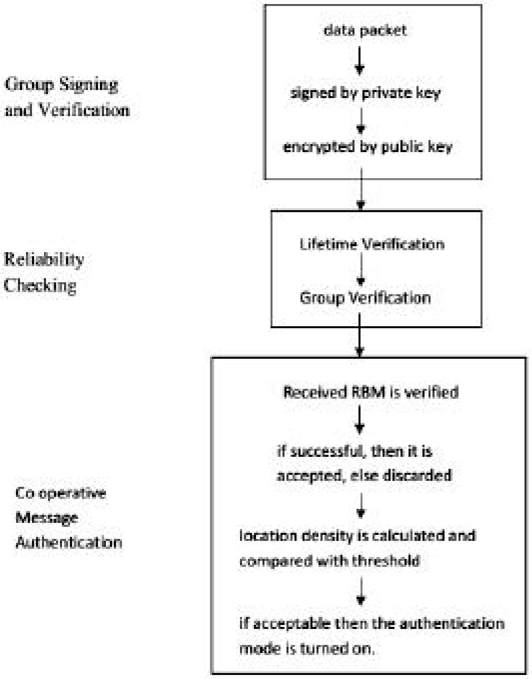
Group Signing and Verification
data packet
signed by private key
encrypted by public key
Reliability Checking
Lifetime Verification
Group Verification
Co operative Message Authentication
Received RBM is verified
if successful, then it is accepted, else discarded
location density is calculated and compared with threshold
if acceptable then the authentication mode is turned on.

Fig. 1: Block diagram

co-operative authentication process. In verifier selection process, the verifier nodes are selected according to the geographic information obtained in study 1. After performing the reliability checks and location verification given in study-1, the verifiers detect the suspected messages. Then the warning message is transmitted using co-operative authentication messages (CAM) (Hao *et al*., 2011) (Fig. 1).

MATERIALS AND METHODS

Group signing and verification technique: Every vehicle in the group creates a public key, $\text{key}_{\text{public}}$ and a private key, $\text{key}_{\text{private}}$ and is used in the transmission of the message, M. The message, M is signed using the $\text{key}_{\text{private}}$ and then encrypted using $\text{key}_{\text{public}}$ and finally transmitted. On reception of the message, M, it is decrypted using these keys.

Geographic hashing is used to encode the geographic position of the vehicle transmitting the message. Geographic hashes are a group of tokens which consists of secret information related to the vehicle position and it is maintained by each vehicle within the group. The information related to the vehicle position is disclosed only to the vehicles within the group, within its communication range.

In this study, the geographic hashes are generated using the modular arithmetic and a beacon message is broadcasted to let the neighboring vehicle know about the position information. Beacon is used by every vehicle in the group. The beacon format is shown in Fig. 2.

Node ID	Location	Graphic hashes of neighboring nodes	Public key	Random nonce

Fig. 2: Beacon format

The beacon consists of five fields. The ‘Node ID’ field indicates the id of the particular vehicle. Every vehicle has unique id associated with itself. The ‘Location’ field in the beacon indicates the current location of the vehicle within the group. The ‘geographic hashes of neighboring nodes’ is determined by the vehicle, based on the Eq. 1. The public key is the key generated randomly by the vehicle.

The selection of the verifier is done by the use of beacon message. When the beacon message is broadcasted by all the vehicles in the group. The vehicle that receives all or maximum number of beacon message in the group within the predefined time interval is selected as the verifier.

Data transmission mechanism: Assume S and D as source and destination vehicles respectively. Let R_S be the random nonce generated by the source and consider vn_i, vn_{i+1}, $vn_{i+2...}$ vn_{i+n} as a set of forwarding or intermediate nodes between source and destination. Let that L_{vni} denotes the location list of node vn_i.

The data packet to be transmitted is created by the source vehicle. It constructs the data packet by including destination ID (D), location list (L_S), random nonce generated by S and the message. The entire data packet is encrypted using public key Kpu_s of source. Finally, the message is digitally signed with private key Kpr_s of source:

$$S \xrightarrow{\text{Data packet}} vn_i$$
$$\text{Data packet}\left(\left\{D, R_S, L_S, \text{Message}\right\}_{puK_S}\right)_{prK_S} \tag{1}$$

When an intermediate vehicle receives the data packet, it performs reliability check. If the reliability check is completed successfully, then the data packet is transmitted to the next vehicle along the path towards the destination (vn_{i+1}) determined by geographical routing and a positive reply is transmitted back to the previous hop. If (Reliability checks are successful) then:

$$vn_i \xrightarrow{\text{Data packet}} vn_{i+1}\text{Data packet:}$$
$$\left(\left\{D, R_S, L_S, \text{Location}, \text{Message}\right\}_{puK_S}\right)_{prK_S} \tag{2}$$

Positive reply:

$$\left(\left\{R_S, prK_{vni}\left(R_S\right), \left\langle \begin{matrix} puK_{vni+1}, P_{vni+1}, \text{Location} \\ \left(P_{vni+1}\right), H_G\left(P_{vni+1}, P\right) \end{matrix} \right\rangle\right\}\right)_{prK_{vni}} \tag{3}$$

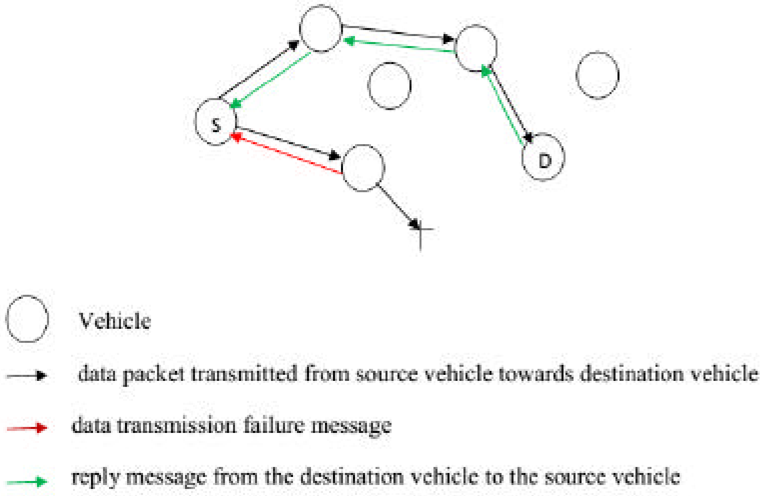
S
D
Vehicle
data packet transmitted from source vehicle towards destination vehicle
data transmission failure message
reply message from the destination vehicle to the source vehicle

Fig. 3: Group signing by all the vehicles in the group

If the reliability check fails, then the data packet is dropped and this information is transmitted to the source vehicle. When, the data packet is received at the destination vehicle, it tested for validity of message by checking digital signatures. If the received data packet is valid then the destination vehicle replies to the source vehicle.

$$vn_{k-1} \xleftarrow{\text{Recursive REPLY}} D$$

$$\text{Recursive reply: } \left(\begin{Bmatrix} L_D, R_S, \text{neighbor ID,} \\ \text{position information} \end{Bmatrix}\right)_{prK_D} \tag{4}$$

As soon as receiving recursive reply message, the source (S) authenticates public keys by the side of routing path. This is accomplished by verifying the obtained key value in the recursive reply message as (Fig. 3).

Reliability checking mechanism: The reliability of the messages is checked by verifying the signature. The signature can be tested by the pairing method. This verification process must be done at high speed due to the fact that the vehicles within the group keep sending out the messages to the group. So, we use batch verification method for checking the reliability of the messages.

Batch verification process: When a message is received from a vehicle in the group, the validity of the lifetime of the message is checked. The lifetime is checked by pairing with each member of the group. For instance, if there are 10 vehicles in the group, then 9 pairing operations will be performed with the broadcasting vehicle. If the lifetime gets expired before the pairing operation is completed then the message is rejected by the group. After the lifetime is verified, next the entire is group is verified (Priya and Karuppanan, 2011). It is explained in Algorithm 1:

Algorithm 1:

```
Assume max R as the maximum acceptable transmission range of a vehicle
within the group
Presume the maximum velocity of a vehicle as Vmax
Let $vn_i$ be the VANET vehicle and $d_{vni}$ be the data packet forwarded by this
vehicle $vn_i$, where i = 1,2… n
Assume S and D denote source and destination vehicles, respectively
$vn_i$ transmits $d_{vni}$ to $vn_{i+1}$ towards D
When $vn_{i+1}$ receives $d_{vni}$, it enters into phase-1
If (Timestamp ($d_{vni}$)≤existing time window) then
    If (Transmission range ($d_{vni}$)≤$max_R$ ) then
    If (Velocity ($d_{vni}$)≤ Vmax ) then
    The packet is digitally signed by vehicle $vn_{i+1}$
    The packet is forwarded to next vehicle selected by geographic routing
    Positive Reply is transmitted back to the forwarded vehicle
    Else
    The Packet is discarded
    Negati            ve reply is transmitted back to the forwarded vehicle
    End if
    Else
    The Packet is discarded
    Negative reply is transmitted back to the forwarded vehicle
    End if
Else
    The Packet is discarded
    Negative reply is transmitted back to the forwarded vehicle
End if
```

If message lifetime verification and group verification are successful, then the broadcasted message can be considered as reliable.

Co-operative message authentication technique: Co-operative Message Authentication mechanism consists of verifier selection process and co-operative authentication process. In verifier selection process, the verifier nodes are selected according to the geographic information. After performing the reliability checks and location verification, the verifiers detect the suspected messages. Verifiers are decided in a distributed manner by vehicles themselves according to their locations regarding to the sender. A cartesian coordinate is set up for each sender at the sending time and the location of the sender is its origin. Co-operative Authentication Technique is described in Algorithm 2.

Algorithm 2:

- When a RBM is received by any vehicle, it immediately updates the neighboring nodes and estimates the RSD
- This vehicle determines if it is the verifier node by measuring the distance between the itself and the surrounding nodes present in the neighboring list
- If the vehicle verifies that it is the verifier then it inserts the RBM in the process queue and ensures that it will be processed within the predefined verification period
- If the vehicle is proved to be a non verifier, then RBM is stored in the buffer
- If the vehicle receives a CAM and if the RBM is still present in the buffer then the RBM is converted into CRBM, removed from the buffer and inserted in the process queue.
- In order to avoid overloading the verifier, at least one verifier is maintained at each side of the sender so that the verification is guaranteed
- The messages: CRBM and RBM in the process queue are then verified message by message in the queue by enough number of vehicles to ensure safety
- If the message is determined to be valid, then it is accepted and used by the vehicles
- If the message is determined to be invalid, then if it is a CRBM message then it is dropped and if it is RBM message it is dropped and all the neighboring nodes are informed about it
- After the message is determined to be normal, the vehicle calculates the location density within the communication range using the location details present in the RBM
- If the calculated location density is greater than the predefined threshold value, then the cooperative authentication mode within the vehicle group is turned on by setting the A Mode flag

Overall algorithm:

- A group of vehicles is formed using the beacon message such that the group consists of vehicles which are within each other's communication range
- Data packet consisting of a beacon message is transmitted by every vehicle to other vehicles after signing and encrypting it
- Only the group members can access the data packet, since only the members have the public and private key information
- Thus the vehicle group is verified for safety
- The message is also checked for reliability by verifying the lifetime v alidity and the group validity
- If the message lifetime and group is verified and successful, then it is accepted, else it is discarded
- The validation of the group and message is confirmed for ensuring the privacy in the VANET
- The RBM is broadcasted by the RSU. When any vehicle receives RBM, it checks if it is verifier
- According to the vehicle status, the message is either sent to the process queue or buffer
- All the message in the queue is verified for the validity
- Using the location details of the valid message, the location density is estimated and compared with the threshold
- If the location density is greater than threshold then group is authenticated

Simulation

Simulation parameters: We use NS2 [ ] to simulate our proposed Secure Group Authentication (SGA) protocol. We use the IEEE 802.11 for VANET as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, the packet sending rate is varied 50 Kb. The area size is 2500×700 m^2 region for 20 sec simulation time. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in Table 1.

Performance metrics: We evaluate performance of the new protocol mainly according to the following parameters. We compare the CMA protocol with our proposed SGA protocol.

Table 1: Simulation parameters

Parameters	Values
No. of nodes	82
Area	12500×700
MAC	802.11
Simulation time	20 sec
Traffic source	CBR
Rate	50Kb
Propagation	Two Ray Ground
Antenna	OmniAntenna
Attackers	1,2,3,4,5 and 6
Mobile speed	5,10,15,20 and 25 m sec^{-1}

Average packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Throughput: The throughput is the amount of data that can be sent from the sources to the destination.

Packet Drop: It is the number of packets dropped during the data transmission

RESULTS AND DISCUSSION

The simulation results are presented in the next study.

Based on Attackers: In our first experiment we are varying the number of attackers as 1-6. Figure 4-8 show the results of delay, delivery ratio, packet drop, throughput and Overhead by varying the attackers from 1 to 6 for the CBR traffic in SGA and CMA protocols. When comparing the performance of the two protocols, we infer that SGA outperforms CMA by 36% in terms of delay, 49% in terms of delivery ratio, 84% in terms of packet drop, 50% in terms of throughput and 71% in terms of Overhead.

Based on Speed: In our second experiment we vary the vehicle speed as 5, 10, 15, 20 and 25 m sec^1. Figure 9-13 show the results of delay, delivery ratio, packet drop, throughput and Overhead by varying the speed from 5-25 m sec^{-1} for the CBR traffic in SGA and CMA protocols. When comparing the performance of the two protocols, we infer that SGA outperforms CMA by 41% in terms of delay, 45% in terms of delivery ratio, 91% in terms of packet drop, 52% in terms of throughput and 75% in terms of overhead.

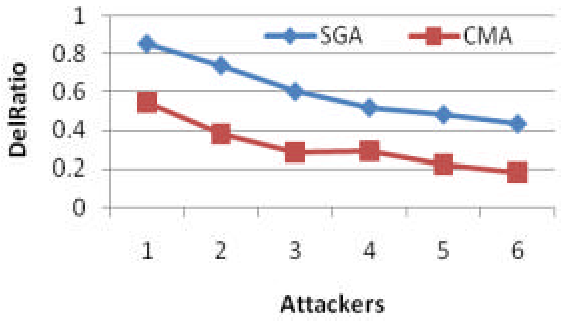

Fig. 4: Attackers vs delay

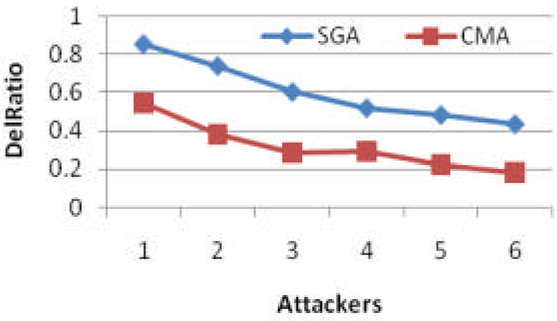

Fig. 5: Attackers vs delivery ratio

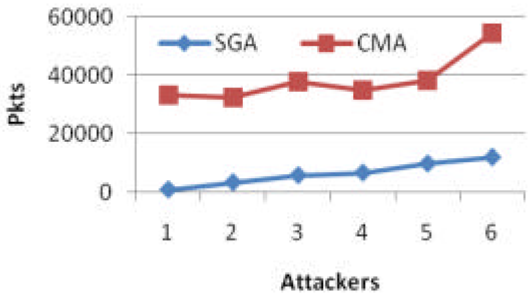

Fig. 6: Attakers vs drop

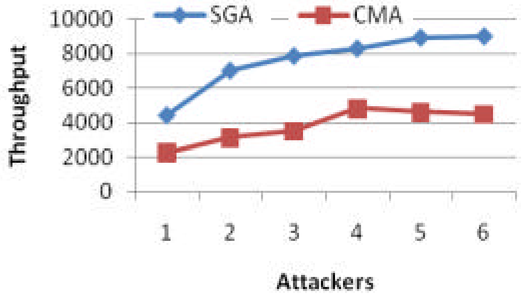

Fig. 7: Attackers vs throughput

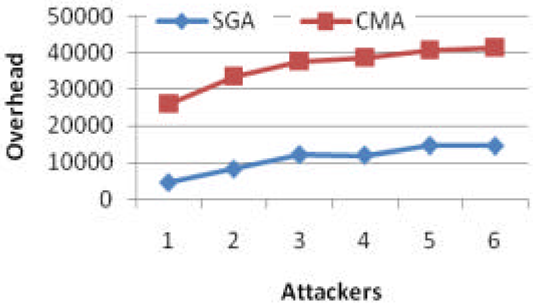

Fig. 8: Attackers vs overhead

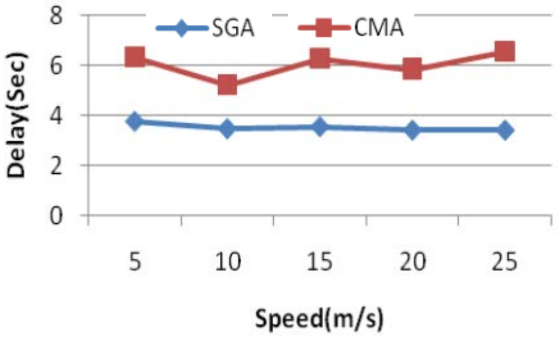

Fig. 9: Speed vs delay

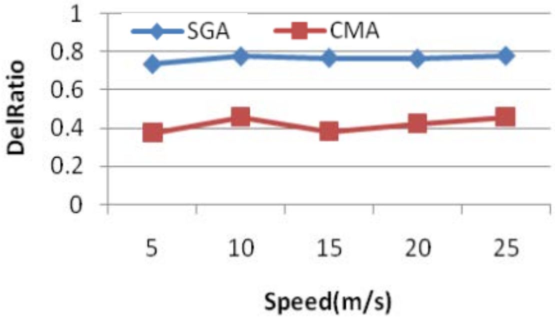

Fig. 10: Speed vs delivery ratio

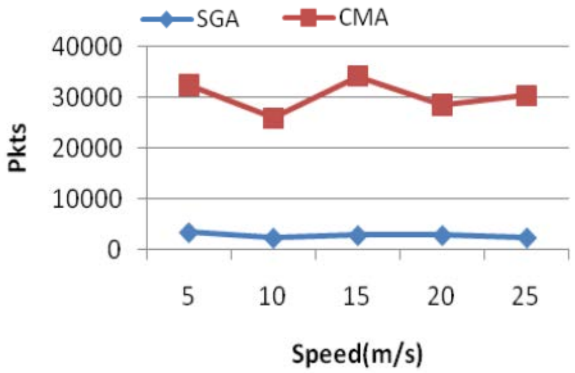

Fig. 11: Speed vs drop

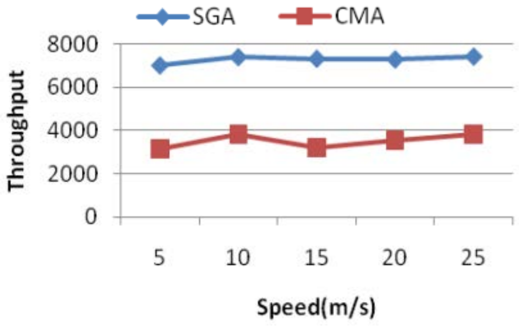

Fig. 12: Speed vs throughput

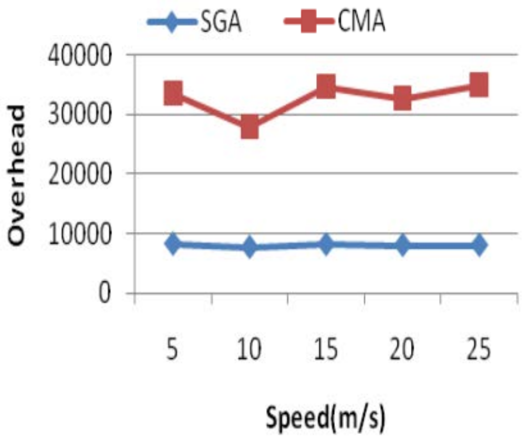

Fig. 13: Speed vs overhead

CONCLUSION

In this study, we propose a group authentication technique for VANET. This mechanism occurs in three phases. In the first phase, a group is formed which consists of several vehicles within each other's communication range using beacon message. In the second phase, the data message is checked for reliability by testing the lifetime and group validity.

When a vehicle receives the RBM from the RSU, the third phase, the co-operative message authentication is performed. Thus, through these phases, the group of vehicles gets authenticated and hence can ensure complete safety and privacy for the communication between the vehicles within the group.

REFERENCES

Chaurasia, B.K. and S. Verma, 2011. Infrastructure based authentication in VANETs. Int. J. Multimedia Ubiquitous Eng., 6: 41-54.

Feiri, M., R. Pielage, J. Petit, N. Zannone and F. Kargl, 2015. Pre-distribution of certificates for pseudonymous broadcast authentication in VANET. Proceedings of the 2015 IEEE 81st Conference on Vehicular Technology (VTC Spring), May 11-14, 2015, IEEE, Glasgow, Scotland, pp: 1-5.

Hao, Y., Y. Cheng, C. Zhou and W. Song, 2011. A distributed key management framework with cooperative message authentication in VANETs. Sel. Areas Commun. IEEE. J., 29: 616-629.

Jeon, Y.B., K.H. Lee, D.S. Park and C.S. Jeong, 2013. An efficient cluster authentication scheme based on vanet environment in m2m application. Int. J. Distrib. Sens. Netw., Vol. 2013.

Priya, K. and K. Karuppanan, 2011. Secure privacy and distributed group authentication for VANET. Proceedings of the 2011 International Conference on Recent Trends in Information Technology (ICRTIT), June 3-5, 2011, IEEE, Chennai, India, ISBN: 978-1-4577-0588-5, pp: 301-306.

Wang, H. and Y. Zhang, 2012. On the security of an anonymous batch authenticated and key agreement scheme for value-added services in VANETs. Procedia Eng., 29: 1735-1739.

Zhu, X., Y. Lu, B. Zhang and Z. Hou, 2013. A distributed pseudonym management scheme in VANETs. Int. J. Distrib. Sens. Netw., Vol. 2013.