Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/140112

An Improved Trust and Certificate Aided Secure Communication (TCASC) Scheme for Cluster-based VANET

P. S. Abi[1,*], *M. Devi* [2] *and V. Rhymend Uthariaraj* [3]

[1] Dept. of Information and Communication Engineering, Anna University, Chennai, Tamil Nadu, India.
[2] Dept. of Electronics and Communication Engineering, University College of Engineering, Arni, Tamil Nadu, India
[3] Ramanujan Computing Centre, Anna University, Chennai, Tamil Nadu, India.

Received: 2 May 2019, Revised: 2 Jul 2019, Accepted: 10 Jul. 2019
Published online: 1 Jan. 2020

Abstract: VANET helps in preventing critical circumstances like traffic congestion, unobserved interferences, and accidents. VANET security is vital as their presence relates to dangerous, life-threatening conditions. To certify secure communication between vehicles in VANET, each message should be secured and checked continuously. However, current works are unable to notice the node compromise and message dropping attacks. Furthermore, they encompass a vast communication overhead. Hence the core objective of this research work is to develop a guaranteed communication scheme for VANET, which precisely detects compromised nodes with low-complexity, interruption, and overhead. In this paper, a Trust and Certificate Aided Secure Communication (TCASC) Scheme for VANET proposed and the vehicles in VANET grouped into clusters, and their Cluster Head (CH) are preferred based on the trust degree. The respective cluster head sends only the messages from validated members. Then security is certified by employing message validation and certificate revocation mechanisms. Simulation results proved that the proposed scheme attains increased detection accuracy and delivery ratio with reduced communication overhead.

Keywords: VANET, Trust, Cluster, Certificate, Communication

1 Introduction

VANETs have grown out of the need to support the growing number of wireless devices such as Global Positioning System (GPS) and mobiles that can now use in vehicles. VANET [1] is capable of performing smart inter-vehicle communication, thus achieving the safety of road traffic [1]. A VANET consists of two kinds of nodes: (i) mobile On-Board Unit (OBU) which consists of a network module, a centralized processing unit as well as a warning unit. (ii) Static Road Side Unit (RSU), which placed in specific locations which are centralized, such as an intersection point or junction of the roads [2]. In VANET, a network is formed between every two moving vehicles and also between a moving vehicle and the Road Side Unit (RSU). The vehicles connect to the RSU through Internet and connect with other vehicles through a mesh network [3]. Some of the applications of VANET include traffic congestion alarm, collision warning message, and lane change warning message [4]. Some of the issues of VANET are related to security, network management, congestion and collision Control, power control, etc. VANET is time critical where a safety-related message should be delivered within a short period. Hence message and entity authentication should be performed within that short time. In VANET, even authenticated nodes can perform malicious activities that can disturb the network activities. The attacks that can compromise the security are mainly targeted towards the transmitted message between the vehicles in the network [5].

1.1 Motivation of the Work

To ensure secure communication between vehicles in VANET, every message must be secured and monitored continuously.

Some of the components that need to be associated with the message are:

[*] Corresponding author e-mail: abipsphd@yahoo.com

1. Authentication: To assure security during communication, each message should be authenticated. So, while transmitting a message, the sending node encrypts the message with a private key and with the related certificates. The receiver looks for the key and validates the certificate, and then the message is accessed.
2. Availability: VANET is a real-time technology, and hence, the vehicles need to be available, and also perform in a quick manner. If the availability of the vehicles is not updated appropriately, then the message created may end up being disastrous.
3. Non-Repudiation: This feature enables the detection of the attacker even after some time of the occurrence of the attack.
4. Privacy: The driver details should be maintained private and secured from unwanted observers.
5. Integrity: Safeguarding the integrity of every message is very critical to avoid the attacks.
(vi) Confidentiality: To maintain the details of the driver as private information, it is necessary to encrypt all the messages. This prevents the outsiders from determining any details of the drivers [6].

This paper concentrates on authentication, privacy, and non-repudiation factors. Existing studies are unable to detect the node compromise and message dropping attacks. Moreover, they involve huge communication overhead. Hence the primary focus of this research work is to develop a secure communication scheme for VANET which accurately detects compromised nodes with reduced complexity, delay, and overhead.

2 Related Work

The suggested Privacy Preserving REvocation Mechanism (PPREM) [7] for VANETs. PPREM uses fast certification revocation checking method through a one-way accumulator. It fulfills the security, as well as privacy, needs such that the eavesdroppers are not able to get any information even after attacking the RSU. However, in this technique, the vehicles have to get the witness of the certificate before status validation.

In the scalable and effective trust-based framework for vehicular ad-hoc networks technique, experience-based and role-based trust factors are used to check the trust level between the vehicles [8]. The trust level is examined in a distributive and collaborative manner while the messages are being transmitted. It enhances the reliability of the data and system efficiency by identifying the compromised data. Based on the simulation results, it is seen that the proposed technique works appropriately in VANETs.

In the novel architecture for authentication and secure communication in VANET, the primary server is a central unit and is responsible for handling the entire system [9]. The server functionalities are further divided between several local servers depending on the location of presence. This enhances the response time. The database used for the storage purpose is distributive, and this minimizes the response time of the local servers and enhances the throughput. The proposed technique is suitable for effective communication in VANET.

In this paper, a message batch verification mechanism is proposed based on the Bloom Filter. This bloom filter is capable of validating several messages and handover authentication proficiently for numerous communications which include several vehicles. A group key is updated in the vehicle by this verification mechanism through the bloom filter. This minimizes the group rekeying overhead caused at the RSU when the number of vehicles in the VANET is more significant [11].

The authors proposed a secure broadcasting architecture for VANET in [12]. It consists of different layers, namely anonymity, credibility, encryption/decryption, relay vehicle selection, and transmission layer. It also consists of three different operating modes: transmission, receiving, and retransmission, which operate by utilizing secure broadcasting layers.

A privacy preservation technique which consists of a trusted authority (TA) [13]. The TA maintains privacy credentials to the vehicles and the information secured from the RSUs. When the vehicle starts the journey, it sends a request to the nearby RSU, connected to the TA. On receiving the request, the TA creates a false identity to the vehicle, which makes the vehicle anonymous. Once the identity created, the communication between the specified vehicle and other vehicles or RSU, cannot be known by any other nodes. This paper develops a trust- and certificate-aided secure communication scheme for VANET.

3 Trust and Certificate Aided Secure Communication (TCASC) Scheme

In our previous work [14], a trust-based security and power control technique for VANET proposed. In this work, the trust degree of each node estimated in terms of collaboration trust, behavioral trust, and reference trust values. As an extension to this work, this paper proposes a Trust and Certificate Aided Secure Communication (TCASC) scheme for VANET.

The block diagram of the proposed scheme represented in Fig. 1. At first, the vehicles formed into different clusters, and their cluster heads (CH) are chosen from the trusty nodes. i.e., the node with the highest trust degree and shortest distance [15] selected as a cluster head.

Only the messages trusted by all the cluster members transmitted by the corresponding cluster head by checking the aggregated trustworthiness of the message. This way, fake message or falsely injected messages ignored by the CH. For secure transmission of messages, symmetric cryptography is applied in which encryption/decryption is performed.

The certificates and their details are broadcast to the Road Side Units (RSU) by CA, which in turn transmit to each CH in its range. Each sender and receiver is authenticated by verifying the certificates. The nodes whose trust value is lower than the minimum trust level are added into the Certificate Revocation List (CRL) [16]. The CRL information is maintained at the CA. The CA accumulates the set of revoked identities into a single value. The accumulator is updated at CA by adding and removing revoked nodes, and it is reflected by each CH holding a copy of it [17].

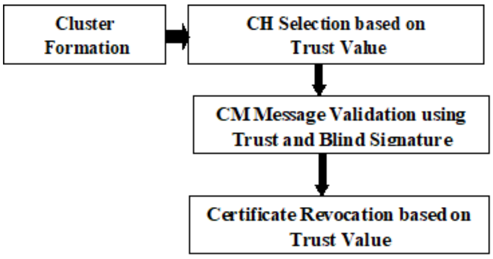
Cluster Formation
CH Selection based on Trust Value
CM Message Validation using Trust and Blind Signature
Certificate Revocation based on Trust Value

Fig. 1: Block diagram of TCASC

3.1 Cluster formation and CH selection

In VANET, initially the vehicles are grouped into clusters, and then for each cluster, a Cluster Head (CH) is elected. The CHs are selected based on the shortest distance between other cluster members and the trust value. All the vehicles within each other's transmission range to form a cluster. The CH selection algorithm is presented below.

3.1.1 Algorithm-Cluster Head Selection

Notations	Definition
$D_{i,j}$	Distance between a cluster member, i and it's neighbor, j
$TV_{i,j}$	Trust value of j as estimated by i
C_k	kth Cluster
CM_i	ith cluster member
CM_i^{add}	Address of CM_i
CM_i^{id}	ID of CM_i
CH	Cluster Head
NE_j	Neighbour list of CM_j
W_i	Weighted sum of CM_i
$Min(W)$	Minimum value of W
NE_i^{tot}	number of neighbors of CM_i

```
1. For each $CM_i$ of $C_k$
2. $CM_i$ broadcasts ($CM_i^{add}$, $CM_i^{id}$) to $CM_j$, $j \neq i$
3. $CM_i$ creates NE$_i$
4. $CM_i$ estimates $D_{i,j}$
5. $CM_i$ estimates $TV_{i,j}$
6. $CM_i$ computes $W_i$ (NE$_i^{tot}$, $D_{i,j}$, $TV_{i,j}$) using the following equation
```

$$W_i = \frac{(\alpha.NE_i^{tot} + \beta.TV_{ij})}{D_{ij}}$$

```
7. End for
8. For each $CM_i$ of $C_k$
9. If $W_i = \min(W)$, then
10. Select $CM_i$ as the CH
11. End if
12. End for
```

Once the clusters are formed, each cluster member has information of all its neighbors and hence creates a neighbor list. Based on the information stored in the neighbor list, each member node estimates the distance between itself and other vehicles, $D_{i,j}$, and also the $TV_{i,j}$. Then each member estimates the weighted sum based on the number of neighbors, $D_{i,j}$ and the $TV_{i,j}$. The member vehicle with the minimum weighted sum, i.e., with shortest distance w.r.t other members and higher trust value is selected as the CH. When a new vehicle joins a cluster, it receives a message from the CH which includes the CH ID and neighbor ID. The CH has centralized access to all its cluster members [18–20].

3.2 Cluster Message Validation

The transmission of a message between members of a cluster as well as between members of different clusters is strictly controlled by the involved cluster heads. The cluster message validation algorithm is presented below.

3.2.1 Algorithm-Cluster Message Validation

Notations	Definition
M	Message
C^S	Source cluster
C^D	Destination cluster
CM_i^S	Cluster member of the source cluster
CM_i^D	Cluster member of the destination Cluster
CM_j	Cluster members
CH^S	Source Cluster Head
CH^D	Destination Cluster Head
T_{op}	Trust opinion from each cluster member
TV_{agg}	aggregated trust value
TV_{pre}	pre-defined trust value
PBSig	Proxy Blind Signature
L	Lock
pb	public key

```
If $CM_i^S$ want to transmit $M$ to $CM_i^D$, then
    $CM_i^S$ broadcasts $M$ to $CM_j$
End if
$CM_j$ forwards $T_{op}$(M) to CH$^S$
$CH^S$ collects $T_{op}$(M) from CM$_j$ and determine $TV_{agg}(M)$
If $TV_{agg}(M) > TV_{pre}$, then
    $M$ is valid
Else
    $M$ is the fake or false injected message
    $CH^S$ discards $M$
End if
$CH^S$ estimate PBSig as
PBSig($L_{pb}[M, TV_{agg}(M)]$)
$CH^S$ forwards PBSig towards $CH^D$
If$CH^D$ receives PBSig then
    $CH^D$ unlocks PBSig and access M
    $CH^D$ forwards $M$ to $CM_i^D$
End if
```

When a vehicle belonging to a cluster intends to transmit a message M to a destination which lies in a different cluster, then the sender node initially broadcasts its M to its cluster members. On receiving M, the cluster members provide its T_{op} w.r.t M and forward it to CH. The CH collects T_{op} from all its members and aggregates it, to determine the TV_{agg} If TVagg $> TV_{pre}$, then M is considered as valid. Otherwise, M is considered as the fake or falsely injected message and is discarded by CH. For secure transmission of the valid M across clusters, the M, along with the TV_{agg} is locked using a public key and transmitted using proxy blind signature. The M has information related to recipient CH ID and its corresponding recipient cluster member ID. Only the recipient CH and cluster member are capable of unlocking the public key and accessing the M.

Thus, the transmission of messages in VANET is maintained with high security to ensure that no message gets compromised, thus assuring network safety.

3.3 Certificate Revocation Scheme

To ensure the validity of each vehicle in the cluster, the certificate revocation scheme is employed. For each vehicle in the cluster, a certificate is created, and it is broadcast. Then based on its validity, the certificate is either accepted or revoked.

The certificate is an X.509 PKI-based digital certificate which contains a public key and an identity and is signed by a certificate authority.

The structure of an X.509 digital certificate is as follows:
Certificate

- –Version Number
- –Serial Number
- –Signature Algorithm ID
- –Issuer Name
- –Validity period
  - –Not Before
  - –Not After
- –Subject name
- –Subject Public Key Info
  - –Public Key Algorithm
  - –Subject Public Key
- –Issuer Unique Identifier (optional)
- –Subject Unique Identifier (optional)
- –Extensions (optional)

Then the vehicles with the revoked certificates are considered to be compromised and then handled cautiously. In this scheme; certificate Authority (CA), Road Side Unit, Onboard unit, and free repositories are the main components. Here multiple existences of CAs is assumed which are responsible for distributing and revoking the certificates of the vehicles.

The certificate revocation scheme is described in the following algorithm.

3.3.1 Algorithm–Certificate Revocation

Notations	Definition
CA	Ccertificate Authority
RSU	Road Side Unit
OBU	On Board Unit
MR	Mobile Repository
CH	Cluster Head
CM_j	Cluster member
CA_cert_k	Certificate of vehicle k
$ID_{k(i)}$	ith pseudonym for kth OBU
$PK_{k(i)}$	ith public key for kth OBU
α	number of pseudonym l oaded in each OBU
TV	Trust value
TV_{th}	Threshold Trust value
$Ac(R)$	Accumulator value of the nodes details in CA
TS	Timestamp
CRL	Certificate Revocation List
W_j	non membership witness for vehicle j
w_j	membership witness
$g(u_j)$	group element
c_j	certificate of vehicle j
s	publicly known group element

```
For each $CM_j$ of cluster
    CA generates the certificate using below
        $$CA\_cert_k = \{(cert_{k(i)}(ID_{k(i)}, PK_{k(i)}), sig_{CA}(ID_{k(i)}||PK_{k(i)}))||1 \leq i \leq \alpha\}$$
    CA uploads CA_cert into the database of $CM_j$
    CA broadcast CA_cert to RSU
    CH verifies CA_cert
    If CA_cert is valid
        CH creates Ac(R) based on the TV.
        If TV $> TV_{th}$, then
```

```
$CM_j$ is valid
Else
$CM_j$ is added to CRL
End if
If Ac(R) is not cached, then
Ac(R) is downloaded from a repository
Else
If TS is expired, then Ac(R) is updated
End if
End if
$W_j$ is estimated using equation below $W_j = (w_j.u_j)$
If $u_j \neq 0$, then
$W_j$ is considered to be valid
Determine $W_{j(cj+s)}$ as
If $W_{j(cj+s)} =$ Ac(R). g($u_j$), then
CA_cert is considered to be valid
Else
CA_cert is added into CRL
End if
End if
```

Initially, CA generates the certificate for each CM of one cluster. The certificate contains the details of certificate id and *i*th public key for *k*th OBU, signed by the CA. The corresponding certificate is then broadcast to the RSU. After verifying the certificate, the CH creates accumulator value of the nodes Ac(R) based on their trust value. Then the CMs with lesser trust values are added in the CRL. The Ac(R) is updated whenever its timestamp expires. The non-membership witnesses nodes then verifies the certificate. Invalid certificates are then added to CRL. The updated list of the revoked nodes in CA is also transmitted to the CH, and then CH is accordingly updated.

Thus, each vehicle in VANET is monitored cluster-wise for security reasons and handled effectively.

4 Result and Discussion

The proposed TCASC scheme is simulated in NS2. In this simulation, 73 vehicles are deployed in the area of size 2500 meter x 700-meter square region. As TCASC deals with the certification revocation, it is compared with Privacy Preserving REvocation Mechanism (PPREM). Though PPREM provides privacy preservation, it is unable to detect compromised nodes, and involve high increased delay, overhead, and collision.

The performance metrics packet delivery ratio, throughput, average energy consumption, communication overhead, and miss detection ratio are measured. To measure the volume of affected communications, the throughput and packet delivery ratio metrics are considered. For analyzing the energy efficiency of the techniques, the average energy consumption metric is considered. To measure the overhead in message exchanges, the communication overhead metric is considered. For analyzing the detection accuracy, the miss detection ratio metric is considered. Fig. 2 shows the simulation topology used for the VANET scenario.

Table 1: Simulation Parameter of proposed TCASC scheme

Total vehicles	73
Size of the Area	2500 × 700 m
MAC Protocol	IEEE 802.11
Traffic Model	Constant Bit Rate
Propagation Model	Two Ray Ground
Antenna Model	Omni Antenna
Initial Energy	7.0 Joules
Tx Power	0.5 watts
Rx Power	0.3 watts
Range	250, 300, 350 and 400 m
Malicious nodes	1, 2, 3, 4, 5 and 6

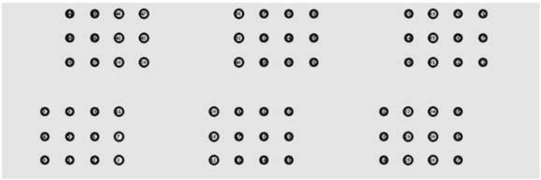

Fig. 2: Simulation topology for the VANET scenario

The simulation parameters are presented in Table 1.

4.1 Effect of Varying Malicious nodes

To analyze the impact of attack density, the number of malicious nodes launching false injection attack and node capturing attack varies from 1 to 6.

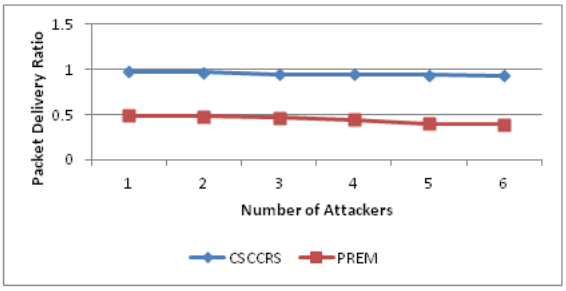

Fig. 3: Packet delivery ratio for varying malicious nodes

Fig. 3 shows that the packet delivery ratio occurred for TCASC and PPREM. The increase in attackers decreases the delivery ratio, as there is more drop due to the attacks. As seen from the figure, the delivery ratio of TCASC decreased from 0.97 to 0.93, and the delivery ratio of PPREM decreases from 0.48 to 0.39. Since TCASC handles the false injection and misbehaving attacks in addition to the forging attacks, TCASC has 53% higher delivery ratio when compared to PPREM technique.

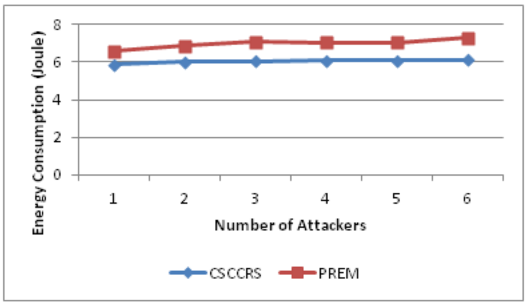

Fig. 4: Energy consumption for varying malicious nodes

Fig. 4 shows the average energy consumption measured for TCASC and PPREM. The increase in attackers increases energy consumption, as there are more authentication and validations to be performed. As refeseen from the figure, the energy consumption of TCASC increases from 5.8 to 6.11, and the energy consumption of PPREM increases from 6.5 to 7.2. Since TCASC involves CH for validations, it has 163 lesser energy consumption than PPREM technique.

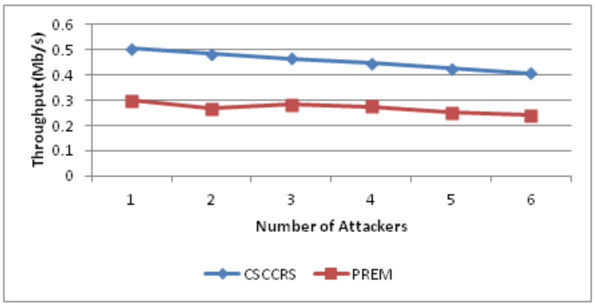

Fig. 5: Throughput for varying malicious nodes

Fig. 5 shows the throughput measured for TCASC and PPREM. The increase in attackers decreases the throughput, as there are more drops due to the attacks. As seen from the figure, the throughput of TCASC decreases from 0.5 to 0.4 Mb/s, and the throughput of PPREM decrease from 0.29 to 0.23 Mb/s. Since TCASC handles the false injection and misbehaving attacks in addition to the forging attacks, it obtains 40% higher throughput when compared to PPREM technique.

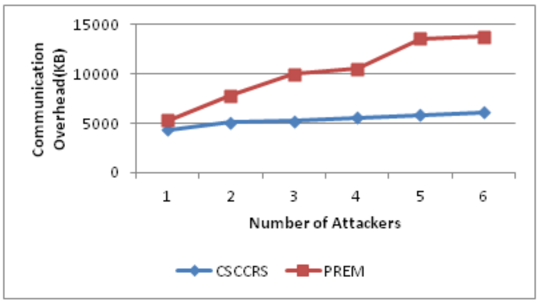

Fig. 6: Communication overhead for varying malicious nodes

Fig. 6 shows the communication overhead measured for TCASC and PPREM. The increase in attackers increases the overhead, as message exchanges between the nodes. As seen from the figure, the overhead of TCASC increases from 221 to 312KB, and the overhead of PPREM increase from 271 to 706KB. Since TCASC involves CH for validations, it has 43% lesser overhead than PPREM technique.

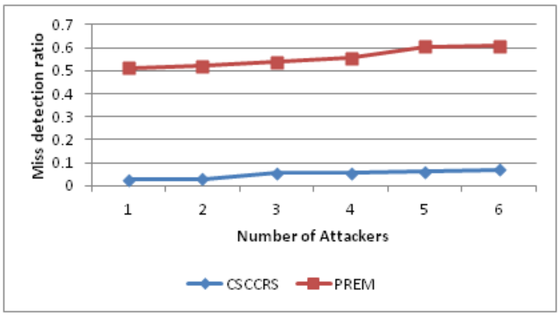

Fig. 7: Miss detection ratio measured for different attackers

Fig. 7 shows the miss detection ratio of TCASC and PPREM. The increase in attackers increases the miss detection ratio. However, the miss detection ratio of TCASC is 91% lesser than PPREM.

4.2 Effect of Different Transmission Ranges

To analyze the impact of transmission size, the transmission range is varied from 250 to 400m, having 2 attackers.

Fig. 8 shows that the delivery ratio occurred for TCASC and PPREM. The increase in transmission range slightly decreases the delivery ratio when PPREM is considered. As seen from the figure, the delivery ratio of PPREM decreases from 0.46 to 0.39. Since TCASC handles the false injection and misbehaving attacks in addition to the forging attacks, it has a 55% higher delivery ratio when compared to PPREM technique.

Fig. 9 shows the average energy consumption measured for TCASC and PPREM. The increase in transmission range decreases energy consumption since less transmitting power is needed. As referred to the figure, the energy consumption of TCASC decreases from

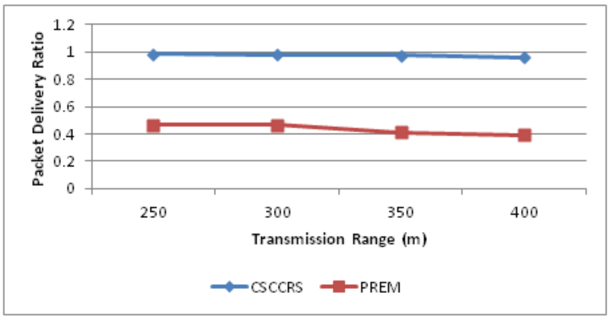

Fig. 8: Packet delivery ratio measured for different ranges

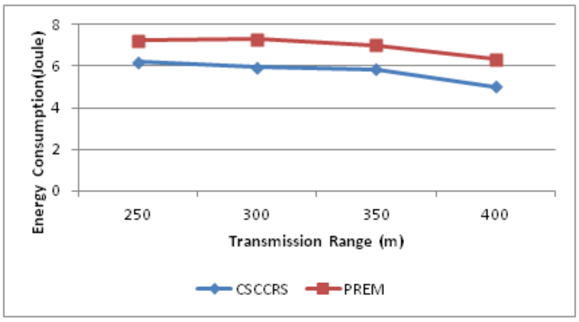

Fig. 9: Energy consumption measured for different ranges

6.2 to 5.0 joules, and the energy consumption of PPREM decrease from 7.2 to 6.3 Joules. Since TCASC involves CH for validations, it has 17% lesser energy consumption than PPREM technique

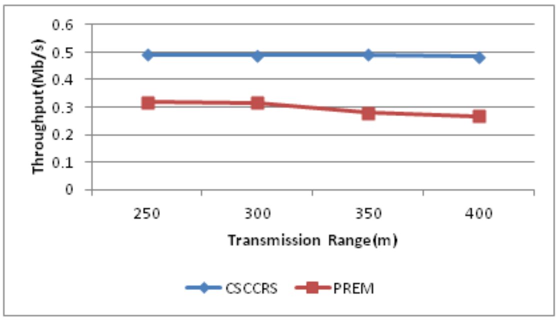

Fig. 10: Throughput measured for different ranges

Fig. 10 shows the throughput measured for TCASC and PPREM. The increase in transmission range slightly decreases the throughput, when PREM is considered. As seen from the figure, the throughput of PPREM decreases from 0.31 to 0.26 Mb/s. Since TCASC handles the false injection and misbehaving attacks in addition to the forging attacks, it has 40% higher throughput than PPREM technique.

Fig. 11 shows the communication overhead measured for TCASC and PPREM. The increase in transmission range increases the overhead. As seen from the figure, the overhead of TCASC increases from 6085 to 9075, and the overhead of PPREM increases from 6293 to 12816 packets. Since TCASC involves CH for validations, it has 17% lesser overhead than PPREM technique.

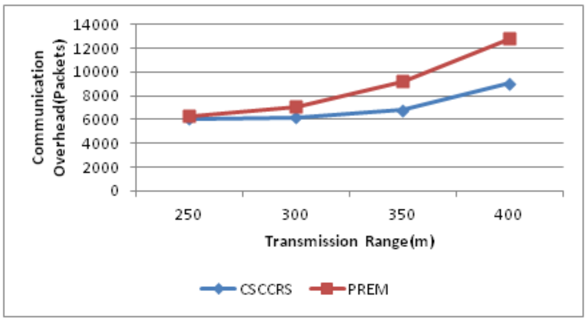

Fig. 11: Communication overhead measured for different ranges

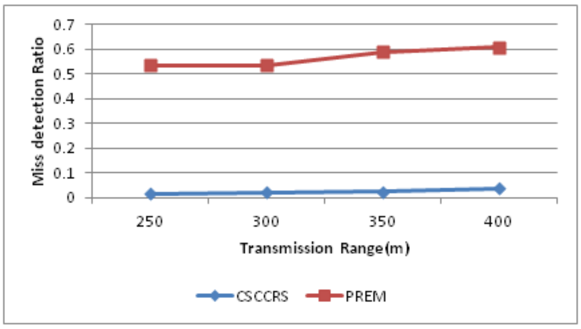

Fig. 12: Miss detection ratio measured for different ranges

Fig. 12 shows the miss detection ratio of TCASC and PPREM. The increase in range increases the miss detection ratio as more number of nodes are involved in the trust validation process. However, the miss detection ratio of TCASC is 95% lesser than PPREM.

5 Conclusion

In this paper, a Trust and Certificate Aided Secure Communication Scheme for VANET are developed. This technique is performed in three phases. In the initial phase, clusters are formed in VANET, and cluster head is selected for each cluster. In the next phase, whenever a cluster member intends to transmit a message; it is broadcast to all the other cluster members. Based on the trust opinions of other cluster members, the cluster head determines the overall trust value of the message and validates it. Then it is transmitted using proxy blind signature. In the final phase, the CA monitors all the vehicles in the cluster and creates a certificate for it. The certificate information is then broadcast to RSU and CH. Based on the trust value, members are validated, and cluster members with lower trust value are revoked and included in the CRL. These details are updated in the CA and then broadcast to RSU and also updated in CH. Thus, whenever any member of VANET needs to determine some details of any other cluster member, it can receive the details from the CH. By simulation results, it has been proved that TCASC reduces the energy consumption, communication overhead, and miss detection ratio when compared to the existing PPREM protocol.

References

[1] S. Aishwar, S. Akash, S. Akshay, S. Sanke and A. Deepa, Conditional Privacy preservation and secure communication in VANETS, *International Journal of Advanced Research in Computer Engineering & Technology, (IJARCET)*, **5**(1) (2016).

[2] K. Jagpreet and M. Priyanka, Secure Communication in Multi-Lane Environment in VANETs, **4**(5), 15–25 (2010).

[3] G.J. Archanaa and R. Venittaraj, A Secure Communication for Clustered RSU in VANETs, *International Journal of Innovative Research in Science, Engineering and Technology*, **3**(3) (2014).

[4] S. Ghassan, A.H. Wafaa, Al-Salih and R. Suresh, Security Analysis of Vehicular Ad Hoc Networks (VANET), *Second International Conference on Network Applications, Protocols and Services*, **5**(6), 100–120 (2010).

[5] M.H. Shruthi and V. Shashidhar, Secure Communication in VANETS using privacy preserving technique, *International Journal of Research In Science & Engineering*, **1**(2) (2010).

[6] D. Ameneh and G.R. Akbar, An advanced security scheme based on clustering and key distribution in vehicular adhoc networks, *Computers and Electrical Engineering*, **3**(4) (2013)

[7] G. Carlos, L. Jose, E. Oscar, M.D. Jorge and A. Juanjo, PPREM: Privacy Preserving REvocation Mechanism for Vehicular Ad Hoc Networks, *Computer Standards & Interfaces*, **36**, 513–523 (2014).

[8] Z. Jie, C. Chen and C. Robin, A Scalable and Effective Trust-Based Framework for Vehicular Ad-Hoc Networks, *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, **1**(4), 3–15 (2012).

[9] D. Bhagyashree, R.V. Dharaskar and V.M. Thakare, A Novel Architecture for Authentication and Secure Communication in VANET, *International Journal of Engineering Trends and Technology (IJETT)*, **4**(5) (2013).

[10] K. Su-Hyun and L. Im-Yeong, A Secure and Efficient Vehicle-to-Vehicle Communication Scheme using Bloom Filter in VANETs, *International Journal of Security and Its Applications*, **8**(2), 9–24 (2014).

[11] M. Devi and V. Rhymend Uthariaraj, Collaborative trustbased security and power control techniques for VANET, *International Journal of Mobile Network Design and Innovation*, **2**, 65–72 (2018).

[12] J. Muhammad, M. Arif Khan, R. Sabih Ur and A.Z. Tanveer, Secure Communication in VANET Broadcasting, *EAI Endorsed Transactions on Security and Safety*, **7**(1) (2018).

[13] A. Janani, S. Anbin, G. Dheepak, Secure Communication and Privacy Protection Using VANET, *IOSR Journal of Engineering*, **8**(8) (2018).

[14] S. Sudhakar and S. Chenthur Pandian, Hybrid cluster-based geographical routing protocol to mitigate malicious nodes in mobile ad hoc network, *International Journal of Ad Hoc and Ubiquitous Computing*, 21(4), (2016)

[15] C. BrijilalRuban and B. Paramasivan, Cluster-Based Secure Communication and Certificate Revocation Scheme for VANET, *The Computer Journal*, **62**(2), 63–275 (2019).

[16] C. Xiaolu and H. Baohua, A Center-Based Secure and Stable Clustering Algorithm for VANETs on Highways, *Wireless Communications and Mobile Computing*, **1**(2) (2019).

[17] A. Mehmood, A. Khanan, A.H.H.M. Mohamed, S. Mahfooz, H. Song and S. Abdullah, ANTSC: An Intelligent Naïve Bayesian Probabilistic Estimation Practice for Traffic Flow to Form Stable Clustering in VANET, *IEEE Access*, **6**, 4452–4461 (2017).

[18] S. Arul Thileeban, C. Sathiya Narayan, J. Bhuvana and V. Balasubramanian, PKI Model Optimisation in VANET with Clustering and Polling, *International Conference on Innovations in Bio-Inspired Computing and Applications*, 321–329 (2018).

[19] S. Sudhakar and S. Chenthur Pandian, Secure Packet Encryption and Key Exchange System in Mobile Ad hoc Network, *Journal of Computer Science*, **6**, 908–912 (2012).

[20] S. Sudhakar and S. Chenthur Pandian, Trustworthy Position-Based Routing to Mitigate against the Malicious Attacks to Signifies Secured Data Packet using Geographic Routing Protocol in MANET, *WSEAS Transactions on Communications*, **12**(11), 584 (2013).

P. S. Abi received B.Tech. (IT) from Thiruvalluvar College of Engineering and Technology, Vandavasi in the year 2006, and M.E.(CSE) from Anna University of Technology, Coimbatore in the year 2010. He has presented a paper in various National level conferences and International Journals.

M. Devi received the B.E.(EIE) from University of Madras in the year 2004 and obtaining M.E.(AE) from Anna University in the year 2006. She has completed her Research program in the field of Ad–Hoc Network in the Department of Information and Communication Engineering of Anna University Chennai. To her credit, she has presented and published many papers in various National & International level conferences and International Journals. Currently, she is serving as Teaching Fellow in the department of ECE of the University College of Engineering Arni.

V. Rhymend Uthariaraj is currently working as a Professor, Ramanujan Computing Centre, Anna University, Chennai,2017. His research interests include Computer Networks, Network Security, Pervasive Computing, and Wireless Networks. He is serving as an editorial member and reviewer of several international reputed journals. He has authored many research articles/books related to Computer Networks, Network Security, Pervasive Computing, Wireless Networks.