C2MTCR: Cluster-Based Communication And Merkle Hash Tree Certificate Revocation Model For Vehicular Adhoc Networks

Jeevitha.R, Dr.N.Sudha Bhuvaneswari

Abstract: Vehicular Ad-hoc Networks (VANET) has been focused on driving safety, driving efficiency and entertainment in road networks. Vehicular networks are the subset of Mobile Ad-hoc Networks (MANET). Each and every vehicle is considered as a node. One node can directly communicate with another node within its transmission range. When the nodes communicate, there is a chance of malicious attackers to intrude and degrade the performance of the entire vehicular network. Malicious node detection is a vital security issue for safety-related applications. The malicious vehicle should be detected and revoked to the smooth functioning of the vehicular communication system. The malicious nodes are revoked to avoid flooding of any wrong message from these may lead to adverse effects like traffic jam and accidents. A defense technique such as certificate revocation is devised to eradicate and provide protection against the malicious nodes that behaves like a legitimate node. The revoked information of the non-legitimate node should be disseminated to the nodes in the vehicular network. In this paper, a new model for Certificate revocation scheme for VANET is proposed to overcome the flaws of Certificate Revocation List (CRL). Cluster-based communication and Merkle Hash Tree Certificate Revocation model (C2MTCR) is based on clustering and construction of Merkle Hash Tree to revoke the malicious certificates from the vehicular networks. The proposed work is simulated using Network Simulator (NS2) and Power BI tool and the results are compared with the existing works.

Index Terms: CA, CRL, C2MTCR, MHT, revocation, VANET.

1. INTRODUCTION

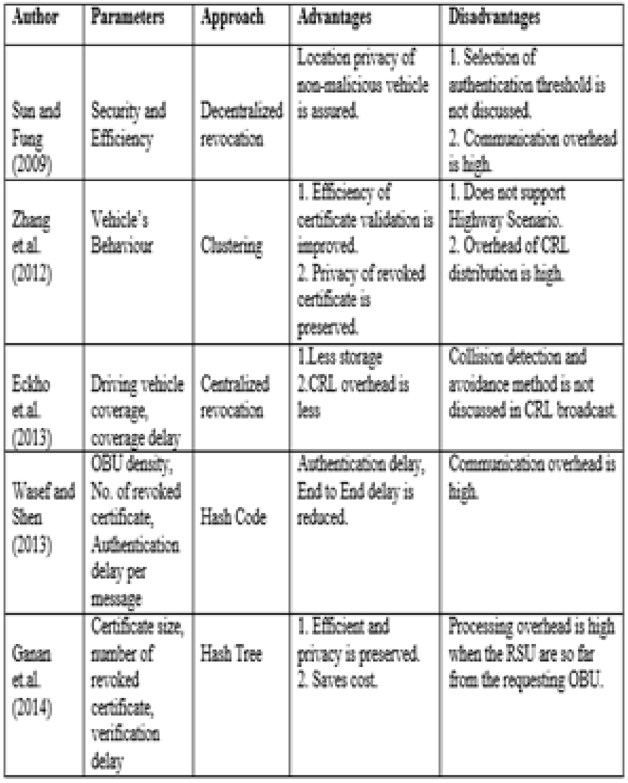
Vehicular Adhoc Networks are designed for the cars to communicate under roadside infrastructure. VANET is focused on the driving safety, driving efficiency and infotainment in road applications. One node can directly communicate with other node within its transmission range. When the nodes communicate, there is a chance of malicious attackers to intrude and degrade the performance of the entire vehicular network. So, the malicious nodes should be detected and evicted from the network. Evicting the misbehavior nodes from the vehicular network has four phases: misbehavior detection, reporting the misbehavior nodes, Certification revocation of malicious nodes and disseminating the revocation information [1]. Certificate revocation is a method of exempting the malicious vehicles from the network. The certificate revocation techniques are classified into two categories namely, Centralized and Decentralized. In centralized revocation technique, the Certificate Authority (CA) is responsible for revocation and it broadcast the certificate to Certificate Revocation List (CRL). The revoked vehicles ID will be present in the CRL. In decentralized technique, the revocation is done by the neighboring nodes of the malicious vehicle. The misbehavior activities of the vehicle are detected by forming clusters and the vehicle ID is revoked. It is reported to the Road Side Unit (RSU) or CA and other vehicles are warned. Decentralized methods are classified into Hash tree and group based. Under Hash tree, Revocation tree and Keyed Hash code can be used [3]. When CRL is used, the vehicles need to communicate with the CA each time to verify the status of the certificate. This paper follows the clustering based decentralized revocation technique and Merkle Hash Tree (MHT) is used to eradicate the flaws in the CRL.

2 RELATED WORKS

The work in [2], Cluster-Based Secure Communication and Certificate Revocation scheme for VANET (SCCR) was proposed. Secure communication is maintained between the nodes by using symmetric cryptographic approach. SCCR performs well when compared to SKCD, PPREM and VANET based secure and privacy-preserving Navigation (VSPN). Secure scheme based on Clustering and Key Distribution (SCKD) was proposed by Daeinabi et.al [16].This method uses clustering and key distribution. The overhead is reduced. Malicious vehicles are monitored and cluster head is chosen based on trust vehicles. In [17], Privacy Preserving REvocation Mechanism for Vehicular Ad Hoc Networks (PPREM) was proposed. PPREM enhances the certificate status checking process by replacing CRL with a fast revocation checking process. The security and privacy requirements of VANETs are preserved. It reduce the revocation cost. The paper summary of certificate revocation techniques in VANET and their pros and cons are discussed as follows.

- *Jeevitha.R is currently pursuing Ph.D. (Computer Science) in Dr.G.R.Damodaran College of Science.*
- *Dr.N.Sudha Bhuvaneswari is currently working as Associate Professor in Dr.G.R.Damodaran College of Science.*

TABLE 1
CERTIFICATE REVOCATION IN VANETS



Author	Parameters	Approach	Advantages	Disadvantages
Sun and Fung (2009)	Security and Efficiency	Decentralized revocation	Location privacy of non-malicious vehicle is assured.	1. Selection of authentication threshold is not discussed. 2. Communication overhead is high.
Zhang et.al. (2012)	Vehicle's Behaviour	Clustering	1. Efficiency of certificate validation is improved. 2. Privacy of revoked certificate is preserved.	1. Does not support Highway Scenario. 2. Overhead of CRL distribution is high.
Eckho et.al. (2013)	Driving vehicle coverage, coverage delay	Centralized revocation	1.Less storage 2.CRL overhead is less	Collision detection and avoidance method is not discussed in CRL broadcast.
Wasef and Shen (2013)	OBU density, No. of revoked certificate, Authentication delay per message	Hash Code	Authentication delay, End to End delay is reduced.	Communication overhead is high.
Ganan et.al. (2014)	Certificate size, number of revoked certificate, verification delay	Hash Tree	1. Efficient and privacy is preserved. 2. Saves cost.	Processing overhead is high when the RSU are so far from the requesting OBU.

3 PROPOSED MODEL FOR REVOCATION OF MALICIOUS NODES IN VANET

VANET security has two major critical issues namely authentication and privacy preservation. In this section, we present a model for revocation of malicious nodes in the authentication based Session Hijacking Attack (SHA).

Network model

Consider a Vehicular Network VN that has n vehicles, where each and every vehicle is equipped with On Board Unit i.e. {OBU1, OBU2......OBUn} to send and receive the message msg. Let V= {Vk, k ∈ {1, 2, 3 ...n}} be the set of vehicles in VN forming clusters. Road Side Unit is placed every 300 meters {RSU1, RSU2..........RSUn} for system initialization. Assume that there exist a Certificate Authority (CA). It is the trusted third party in Vehicular Cloud VC which has high level of computation performance. It is in charge of distributing the certificates to the vehicles in VN. Assume that vehicle is registered at CA. Each vehicle will be assigned unique session ID and its information will be copied and saved in VC in the form of Merkle Hash Tree (MHT). RSU acts as an intermediate entity between vehicles and CA. It can communicate with vehicle using wireless radio signals. Message authentication is done by public key cryptography. All the honest vehicles in VN share the same public key Pubk, while each vehicle V will have a unique private key Pvtk. The private key is known only to the vehicle itself. Pubk and Pvtk distribution is done by the CA. The keys are generated and assigned to the vehicles when the vehicles register at the CA. When a vehicle in VN broadcasts a Msg, a copy of Msg is sent to RSU. RSU needs to authenticate the received msg before sending them to other RSU or vehicles in VN.

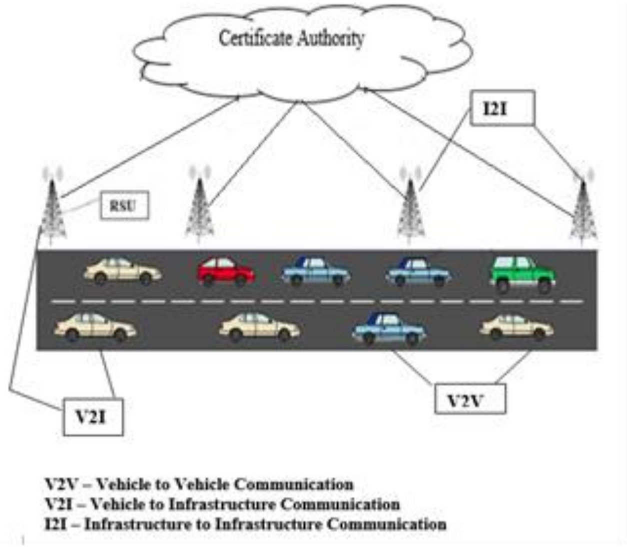

Certificate Authority
I2I
RSU
V2I
V2V
V2V – Vehicle to Vehicle Communication
V2I – Vehicle to Infrastructure Communication
I2I – Infrastructure to Infrastructure Communication

***Fig. 1**. Network Model*

Suppose if a malicious msg is received by an OBU in the vehicle v, it can report to the RSU. The RSU will report to the CA. The CA has the authority to revoke the malicious certificate and it makes it invalid. Finally, the malicious vehicle is isolated from the vehicular network and it is prevented from communicating with the legitimate vehicles. The parameters used in the model includes transmission range, distance, speed and trusted vehicles.

***Table 2**.*
Notations and meaning

Notation	Meaning
VN	Vehicular Network
V	A set of vehicle in VN
V_k	A vehicle in V
Msg	Message
CA	Certificate Authority
VC	Vehicular Cloud
Pub_k	Public key
Pvt_k	Private Key

Bilinear Pairing

The operations involved in the authentication of the schemes include bilinear pairing, hash-to-point, encryption, point addition and point multiplication [13]. Consider a bilinear map c: G1*G2 ->G3, where G1, G2, G3 are cyclic groups, G1=<m> and G2=<n> with same prime order p. It is a non-degradable bilinear map such that ê (m, n) ≠1 and for any a, b ∈Z and all m ∈ G1, n ∈ G2, ê (ma, nb) = ê (mn) ab. Since all are groups of prime order, it follows if m is a generator of G1 and n is a generator of G2, then e (m, n) is a generator of G3. The bilinear pairing c: G1*G2 ->G3 which can efficiently compute ê (m, n) for any m, n ∈ G1. If G1 = G2, then it is symmetric pairing. Otherwise it is asymmetric pairing [10].

Two cryptographic hash functions H1 and H2 are defined as follows:
$H1 :\{ 0, 1\}^{*} \rightarrow G1$
$H2: \{0, 1\}^{*} \times G1 \rightarrow Z^{*}p$
The private key is randomly chosen as $x \in Z^{*}p$ and public key is set as $Pubk=nx \in G2$. The system parameters are defined as SP= {p, e, c, H1, H2, Pubk}. These parameters are loaded into a vehicle while registering and it will be shared with all RSU and vehicles in the vehicular network. At the time of registration, each vehicle receives a unique session ID and a password for message signing and authentication from CA [11].
Phases involved in the proposed model are as follows:

1. Vehicular Cluster formation
2. Key generation and key assignment
3. Vehicle position and direction prediction
4. MHT construction
5. Identifying and updating the revocation information of malicious nodes.

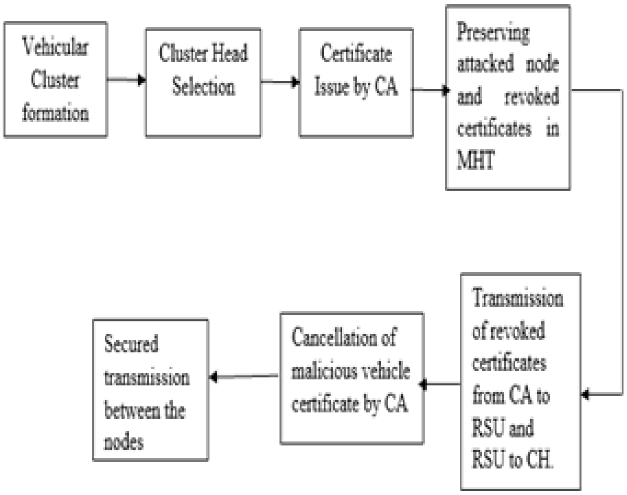

Vehicular Cluster formation
Cluster Head Selection
Certificate Issue by CA
Preserving attacked node and revoked certificates in MHT
Transmission of revoked certificates from CA to RSU and RSU to CH
Cancellation of malicious vehicle certificate by CA
Secured transmission between the nodes

Fig. 2. *Block diagram of proposed model*

Vehicular Cluster formation

Clustering is applied in VANET because of reduced delay and less overhead. They offer efficient resource consumption, solves scalability issues and load balance in wireless network. The communication in the cluster occurs between cluster member node to the cluster head and cluster head to another cluster head. Each cluster will have a cluster head that is selected or elected by the cluster nodes. The size of one cluster varies from other cluster and it mainly relies on the transmission range of the network and vehicle density [7]. Vehicle density is inversely proportional to the speed of the vehicle. If the vehicle speed is less, the density will be higher. If the density is high, the cluster size is big [12]. Initially, all the vehicles (nodes) form clusters and CH is selected based on the trust values.

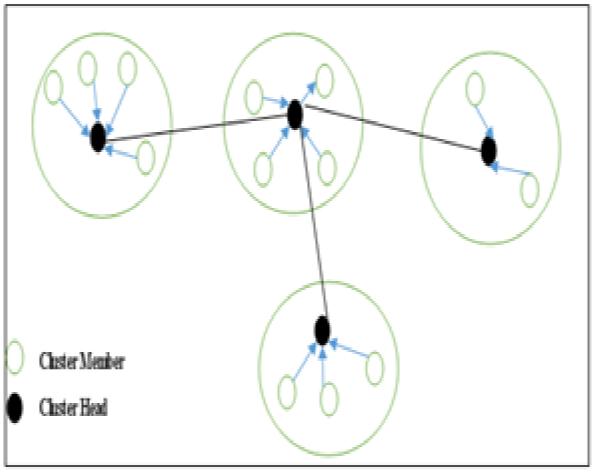


Fig. 3*. Cluster Member to CH and CH to CH communication [2]*

Key generation and key assignment

Vehicles are the clients in the network. Each vehicle possess an On-Board Unit (OBU) which is used as a navigation and communication platform. The transmission range is set to 300 meters. The vehicle stays connected mostly for two minutes. According to DSRC, safety messages are broadcasted every 100-300 ms to other vehicles. Certificate Authority (CA) is the trusted third party in the vehicular cloud that issues the digital certificate as well as the public-private key pairs. CA maintains the revoked certificates in MHT. The invalid certificates should not be used by any one. CA is responsible for updating the honest nodes and malicious nodes [8]. A Road Side Unit can be a physical device located at highways, urban areas, and intersections or on traffic lights. RSU is equipped with a network device to allow communication between the nodes as per DSRC standards. RSU can send, receive and forward the data to an OBU whenever the OBU enters the RSU communication range and it provides internet connection to the OBUs. RSU can also communicate with the other RSUs [2].

Vehicle position and direction prediction

It is important to predict the moving direction of vehicles as a result of the fast movement of vehicles and therefore the frequent change of topology in VANET. To do this, several researches are performed to seek out new ways to predict the speed and direction of moving vehicles. The moving direction of vehicles is set based on the road types, traffic signals and vehicle's destination path [6].

MHT construction

MHT is used for data synchronization and data verification. All leaf nodes are at same depth and non-leaf nodes is a hash of its child node. A hash function maps an input to a fixed output and this output is referred to as hash. The output is always unique for every input. For a binary Merkle tree, the complexity of search and traversal is O (n). The complexity of synchronization, searching, deletion and insertion operation is O (log n) [6].

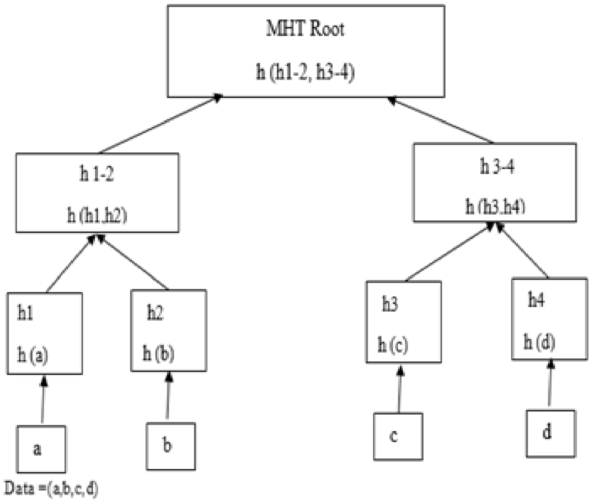


***Fig. 4**. Merkle Hash Tree*

Identifying and updating the revocation information of malicious nodes

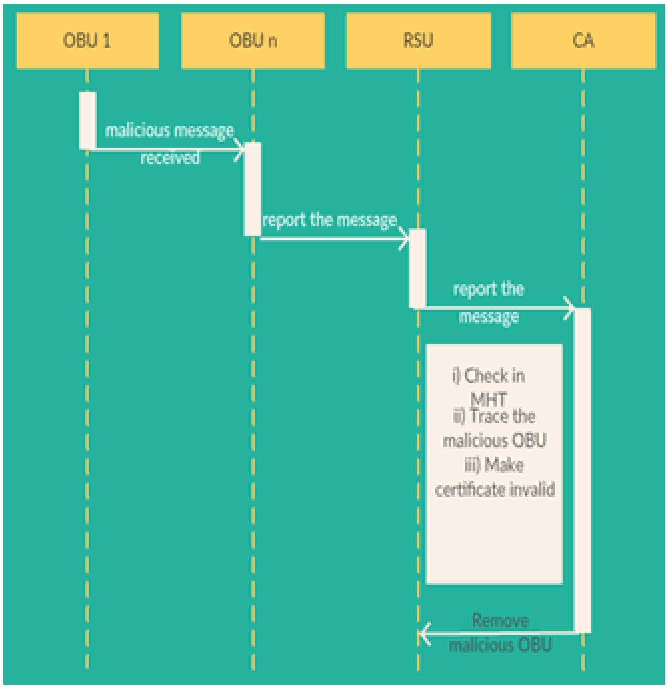


***Fig. 5**. Removing malicious node*

Once a malicious message is received by the vehicle OBU, it reports it to the nearest RSU. The RSU then forwards and sends the report to the CA. The CA checks in the MHT and it traces the malicious OBU. The certificate of the malicious vehicle is made invalid. The malicious vehicle should be revoked from the network. The revocation information should be broadcasted to other vehicles in the network so that the consequence of misbehaviour does not have an impact on time critical VANET system.

Trust model

The malicious certificates could destroy the honest nodes. The node that gets flaws along with its certificate is stored in CA in the form of MHT. The nodes with its trust value lesser than the least trust value (malicious node) are included in MHT. The behavior of vehicle is represented by the trust metric. Trust metric T is the continuous value in the interval [0, 0.1... 1]. Initially the vehicle have T=0.1 as the starting trust value. A vehicle with T=1 is considered to be honest vehicle. If the value of T is less than 0.5 i.e., T<0.5, then the node is considered to be malicious and if the value lies between 0.5-0.9, it is considered to be semi-honest vehicle. The vehicles with high trusted value monitors its neighboring nodes in the cluster. High trusted vehicles are given chance to vote about the neighboring nodes. The election message is sent to CA to revoke the certificate of the malicious node. CA verifies in MHT and revokes the certificate.

4 SPEED AND STORAGE CALCULATIONS

The proposed method has trusted vehicles, speed and vehicle density as parameters. Clustering based Merkle Hash Tree approach is used. Relative direction of vehicle is bidirectional. Absolute vehicle density is 10-250 vehicles per kilometer and Speed range is 60-120 km/hr. The data storage is derived based on the above mentioned factors.

Distance (d) is calculated as

$$d = \sqrt{(x2 - x1)2 + (y2 - y1)2} \text{ ------------------- (1)}$$

x1, x2 - Current position of the vehicle

y1, y2 – Position of vehicle from which the distance is calculated

Speed (S) = Distance/ Time

$$S = \frac{d}{t} \quad \text{--- (2)}$$

t- Time

In highway, the maximum speed of the vehicle is 120 km /hr. In urban area, the maximum vehicle speed is 60 km/hr.

Average vehicle speed (S) = Σ (Vehicle 1+ Vehicle 2+......+Vehicle n)/ Total no. of vehicles

$$= \Sigma \frac{V1 + V2 + \ldots\ldots + Vn}{n}$$

$$S = \Sigma \frac{V}{n}$$

To calculate the value of n,

Average Travel speed = Traffic flow/ Vehicle density

Traffic Flow = Number of vehicles / Time

Vehicle Density (VD) is the number of vehicles ‘m’ that occupy a road segment of length ‘l’.

$$VD = \frac{m}{l}$$

Number of vehicles in a region (n) = Vehicle Density * Area ---------(3)

$$n = \left(\frac{m}{l}\right) \cdot \pi r 2$$

Each vehicle stay in a region for certain time = (2* coverage radius (meters))/ Speed (m/s) -------------------------(4)

$$= \frac{2 \cdot CR}{S} (sec\,onds)$$

Let us consider the certificate size as ‘cs’ bytes.

For ‘n’ number of vehicles, size of data collected will be CS* n bytes-- (5)

$$DS = \frac{CS \cdot n}{\frac{2CR}{S}}$$

Total number of data stored in a second is calculated.

Substituting the value of ‘n’ from equation 3,

$$DS = \frac{CS \cdot \left(\frac{m}{l}\right) \cdot \pi r 2}{\frac{2 \cdot CR}{S}}$$

The above equation is simplified as follows:

$$DS = CS \cdot \left(\frac{m}{l}\right) \cdot \pi \cdot r \cdot \left(\frac{S}{2}\right)$$

5 SIMULATION SETUP

In this paper, we present simulation results conducted using Network Simulator 2 and Power BI, which is cloud based interactive data visualization tool. To measure the performance of our proposed model, we run using this tool to check its efficiency in removing malicious nodes from the network and cancelling the malicious nodes’ certificates and also the revocation time can be reduced.

Table 3.
SIMULATION PARAMETERS

Parameter	Values
Simulation Time	100 s
Transmission Range	300-1000m
Vehicle speed	60-120 km/h
Hello message size	100 bytes
Hello message interval	2 seconds
Vehicle density	10-250 vehicles/km

6 RESULTS AND DISCUSSIONS

The QOS parameters are measured using NS2. Total number of packets generated at the source node is 4718. Total number of packets received at the destination is 4277. 20 nodes are taken and two clusters are formed.

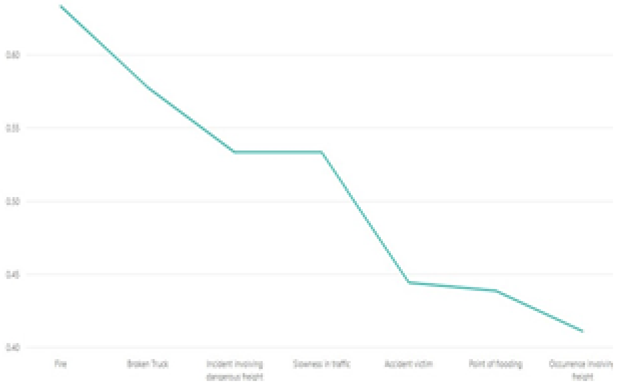


Fig. 6*. Probability of each occurrence*

The fig.6 shows the probability of each occurrence. For the proposed work, 20 nodes and 7 occurrences are considered. The average probability of each occurrence are as follows: Fire 0.63, Broken truck 0.58, Incident involving dangerous freight 0.53, Slowness in traffic 0.53, Accident victim 0.44, Point of flooding 0.44 and Occurrence involving freight 0.41.

Scenario 1: For honest nodes

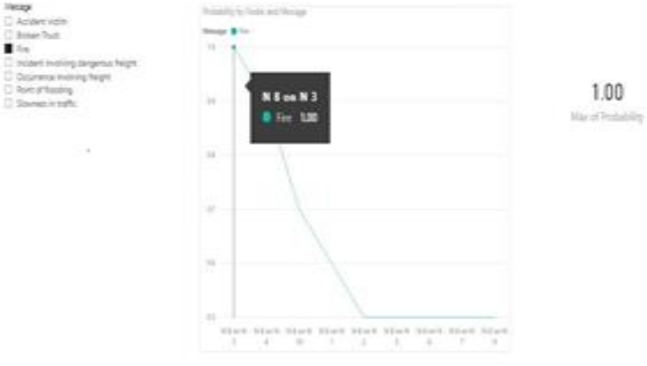


Fig. 7. *Maximum Probability for fire occurrence*

Probability for fire is 1. It denotes that the occurrence is true, overall probability of fire incident is 0.63.

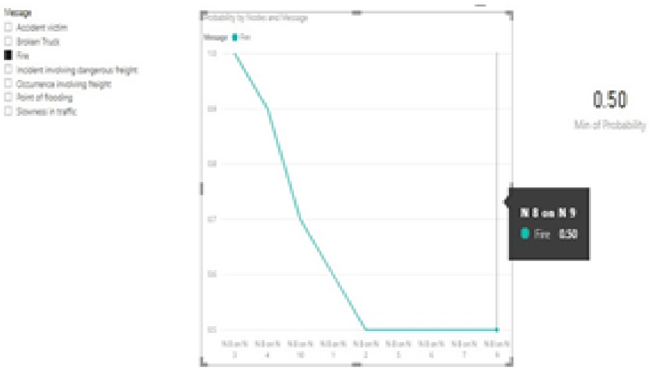


Fig. 8. Minimum Probability for fire occurrence

The minimum probability of fire is 0.50. The values are ranging from 0.50 to 1.00 which indicates it as honest node.

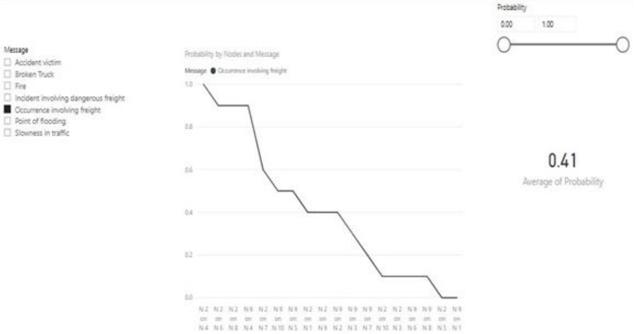


Fig. 9. *Probability of Occurrence Involving freight*

The average of probability of occurrence involving freight is 0.41.

Scenario 2: For malicious node whose certificate is to be revoked.

Maximum probability values are taken from the range of 0.50 to 1.00. The outcome of probability is 0.86. Out of 20 nodes, 5 nodes voted and elected this particular node passing the message as occurrence involving freight as trusted node.

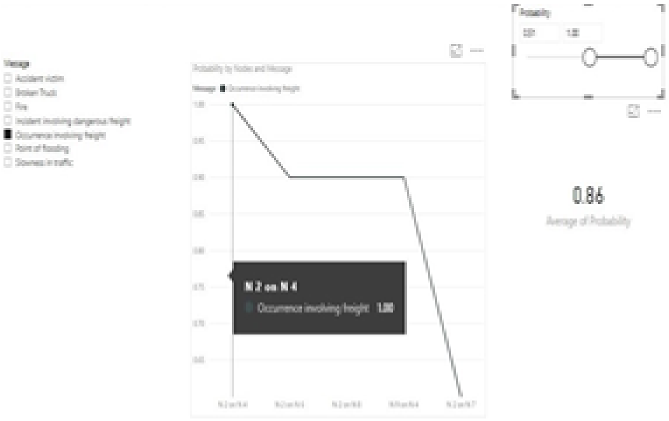


Fig. 10. *Maximum Probability values for occurrence of freight*

Minimum probability values are taken from the range of 0.0 to 0.50 where the outcome of probability is 0.24. 13 nodes voted or elected this particular node passing the message as Occurrence involving freight as malicious node. This fake message is passed by this node to other nodes is to increase congestion, drop packets, reroute and to disturb the trusted vehicular communication. This message is verified with the certificate authority through RSU to check whether it is fake message or not. If it is fake message, the certificate of that node will be revoked to improve the network performance.

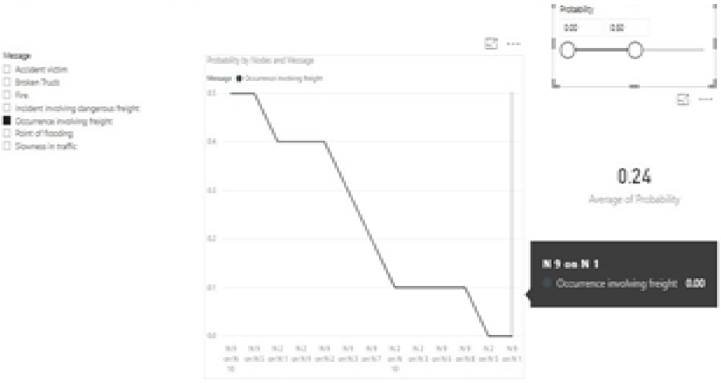


Fig. 11. *Minimum Probability values for occurrence of freight*

Trusted probability of Occurrence involving freight are treated as Malicious and the certificate of those nodes will be revoked. When comparing the voters of (Occurrence involving freight) node, the max voters (13 nodes) says it as malicious node with probability of 0.86 out of 1.00 Only 5 nodes with probability 0.24 out of 1.00 says it as trusted node, the certificate of these nodes will be made invalid.

The proposed work C2MTCR is compared with the existing work SCCR, SKCD and PPREM using NS2.

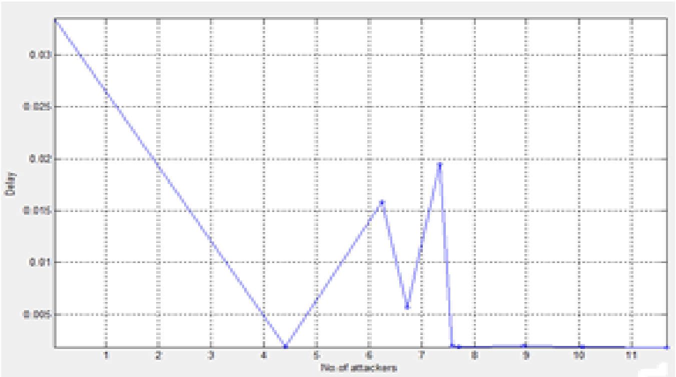


Fig. 12. *End-to-End delay for C2MTCR*

Delay time is the time taken for a packet to reach from source node to destination node. From the above result obtained, it can be inferred that delay time increases as the number of attackers increase.

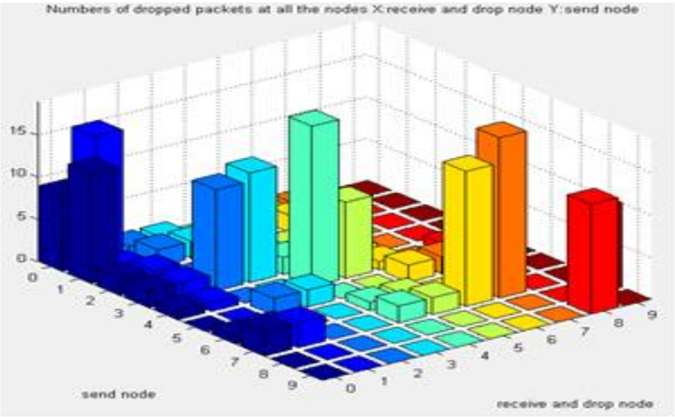


__Fig. 13.__ Packet drop for C2MTCR

Total number of packet drop for the proposed model is 162. As the number of attackers increase, there is a chance of packets to be dropped during the message transmission. C2MTCR has 34% fewer drop values and the packet delivery ratio is 91% when compared to SCCR, SKCD and PPREM.

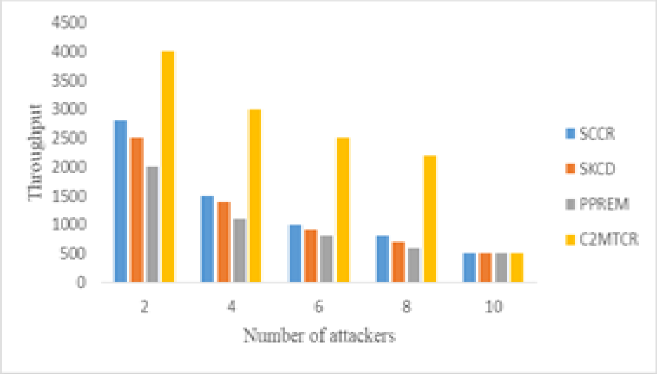


__Fig. 14.__ Number of attackers vs Throughput

As the number of attackers are less, throughput increases. Throughput decreases when the number of attackers are more. C2MTCR has good throughput compared to existing works.

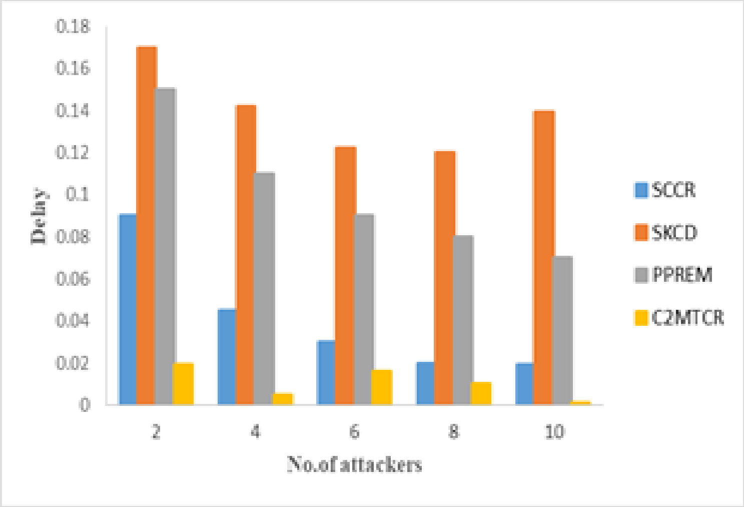


__Fig. 15__. Number of attackers vs End-to-End delay

As the number of attackers increase, the packet drops and the delay time increases to deliver the packet from source to destination node. From the above graph, C2MTCR shows less delay compared to the existing work.

7 CONCLUSION

In this paper, Cluster-based communication and Merkle Hash Tree Certificate Revocation model (C2MTCR) is proposed. It is based on clustering and construction of Merkle Hash Tree to revoke the malicious certificates from the vehicular networks. The proposed method checks the trust of the messages that are transmitted and they are analyzed using Power BI tool. From the above simulation results, the usage of C2MTCR reduces delay and message loss when compared to the existing methods SCCR, SKCD and PPREM. The distribution of revocation information is an open research problem for VANETs. In future, our proposed work will be implemented for sparse network.

REFERENCES

[1] Al Falasi, H. and Barka, E. (2011). Revocation in VANETs: A survey. International Conference on Innovations in Information Technology. pp.214-219.

[2] BrijilalRuban and B.Paramasivan. (2019). Cluster-based Secure Communication and Certificate Revocation Scheme for VANET. The Computer Journal. 62(2): 263–275.

[3] Dinesh Singh and Ranvijay. (2018). A state-of-art approach to misbehaviour detection and revocation in VANET: survey. International Journal of Ad Hoc and Ubiquitous Computing. 28 (2):77-93.

[4] Eckhoff, D., Dressler, F. and Sommer (2013). Smartrevoc: an efficient and privacy preserving revocation system using parked vehicles. 2013 IEEE 38th Conference on Local Computer Networks (LCN), IEEE, Sydney, NSW.pp.827–834.

[5] Ganan, C., Munoz, J.L., Esparza, O., Mata-Diaz, J. and Alins. EPA: an efficient and privacy-aware revocation mechanism for vehicular ad hoc networks. Pervasive and Mobile Computing. 21:75–91.

[6] C. Lyu, D. Gu, Y. Zeng and P. Mohapatra. PBA: Prediction-Based Authentication for Vehicle-to-Vehicle Communications. IEEE Transactions on Dependable and Secure Computing. 13(1): 71-83.

7] Marzak, B., Toumi, Talea, M. and Benlahmar (2015) Cluster head selection algorithm in vehicular Ad Hoc networks. 2015 International Conference on Cloud Technologies and Applications (CloudTech).

8] Muthumari.L, Sharmasthvali Y and Sivakumar S. (2018). Trust based malicious node detection and certificate revocation based on cluster head for MANET. International Journal of Pure and Applied Mathematics.119 (15):385- 390

9] Sun and Fang. (2009).Defense against misbehavior in anonymous vehicular ad hoc networks. Ad Hoc Networks. 7(8):1515-1525.

10] Tahani Gazdar, Abderrahim Benslimane, Abdelfettah Belghith and Abderrezak Rachedi. (2014).

[11] A secure cluster-based architecture for certificate management in vehicular networks", Security and Communication networks. 7: 665-683.

[12] Tao Jing, Yu Pei, Bowu Zhang, Chunqiang Hu, Yan Huo, Hui Li and Yanfei Lu. (2018). An efficient anonymous batch authentication scheme based on priority and cooperation for VANETs. EURASIP Journal on Wireless Communications and Networking. 5-13.

[13] Thamarai Selvan M, Maheshwari M and Roselin Mary. (2013). A Cluster-based Highway Vehicle Communication in VANET. International Journal of Computer Applications. 0975 – 8887.

[14] Tianhan Gao, Yanqiang Li, Nan Guo and Ilsun You. (2018). An anonymous access authentication for vehicular Adhoc networks under edge computing. International Journal of Distributed Sensor networks. 14 (2): 1-15.

[15] Wasef, A. and Shen, X. (2013). Emap: Expedite message authentication protocol for vehicular ad hoc networks. IEEE Transactions on Mobile Computing. 12(1): 78–89.

[16] Zhang, Q., Almulla, M., Ren, Y. and Boukerche. (2012). An efficient certificate revocation validation scheme with k-means clustering for vehicular ad hoc networks. 2012 IEEE Symposium on Computers and Communications (ISCC), IEEE, Cappadocia, Turkey. 000862–000867.

[17] Daeinabi, A. and Rahbar, A. G. (2014). An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks. Computers & Electrical Engineering, 40(2): 517–529.

[18] Ganan, C., Munoz, J. L., Esparza, O., Mata-Diaz, J., and Alins, J. (2014). PPREM: Privacy Preserving REvocation Mechanism for Vehicular Ad Hoc Networks. Computer Standards & Interfaces, 36(3): 513–523.