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.
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, ..., OBU{n}} to send and receive the message msg. Let \( V = \{ V_k, k \in \{1, 2, 3, ..., n\} \} \) be the set of vehicles in VN forming clusters. Road Side Unit is placed every 300 meters \{RSU1, RSU2, ..., RSU{n}\} 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.

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

<table>
<thead>
<tr>
<th>Notation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>VN</td>
<td>Vehicular Network</td>
</tr>
<tr>
<td>V</td>
<td>A set of vehicle in VN</td>
</tr>
<tr>
<td>V_k</td>
<td>A vehicle in V</td>
</tr>
<tr>
<td>Msg</td>
<td>Message</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>VC</td>
<td>Vehicular Cloud</td>
</tr>
<tr>
<td>Pub_k</td>
<td>Public key</td>
</tr>
<tr>
<td>Pvt_k</td>
<td>Private Key</td>
</tr>
</tbody>
</table>

### 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 \( c : G_1 \times G_2 \rightarrow G_3 \), where \( G_1, G_2, G_3 \) are cyclic groups, \( G_1 = \langle m \rangle \) and \( G_2 = \langle n \rangle \) with same prime order \( p \). It is a non-degradable bilinear map such that \( \hat{e}(m, n) \neq 1 \) and for any \( a, b \in \mathbb{Z} \) and all \( m \in G_1, n \in G_2, \hat{e}(ma, nb) = \hat{e}(mn) \) ab. Since all are groups of prime order, it follows if \( m \) is a generator of \( G_1 \) and \( n \) is a generator of \( G_2 \), then \( e(m, n) \) is a generator of \( G_3 \). The bilinear pairing \( c : G_1 \times G_2 \rightarrow G_3 \) which can efficiently compute \( \hat{e}(m, n) \) for any \( m, n \in G_1 \). If \( G_1 = G_2 \), then it is symmetric pairing. Otherwise it is asymmetric pairing [10].
Two cryptographic hash functions H1 and H2 are defined as follows:

\[ H1: \{0, 1\}^* \rightarrow G1 \]
\[ H2: \{0, 1\}^* \times G1 \rightarrow \mathbb{Z}_p \]

The private key is randomly chosen as \( x \in \mathbb{Z}_p \) and public key is set as \( \text{Pubk} = nx \in G2 \). The system parameters are defined as \( \text{SP} = \{p, e, c, H1, H2, \text{Pubk}\} \). 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**
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.

**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].
Identifying and updating the revocation information of malicious nodes

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

\[ d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \]  

\[ \text{Speed (S)} = \frac{d}{t} \]

\[ t\text{- Time} \]

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 \( S = \frac{\sum (\text{Vehicle } 1 + \text{Vehicle } 2 + \ldots + \text{Vehicle } n)}{\text{Total no. of vehicles}} \)

To calculate the value of n,

\[ VD = \frac{m}{l} \]

\[ \text{Number of vehicles in a region (n) = Vehicle Density} \times \text{Area} \]

---

(1)

(2)

(3)
Each vehicle stay in a region for certain time = \( \frac{(2 \times \text{coverage radius (meters)})}{\text{Speed (m/s)}} \) - (4)

Let us consider the certificate size as ‘cs’ bytes.
For ‘n’ number of vehicles, size of data collected will be \( CS \times n \) bytes - (5)

Total number of data stored in a second is calculated.
Substituting the value of ‘n’ from equation 3,

The above equation is simplified as follows:

\[ DS = CS \times \left( \frac{m}{l} \right) \times \pi \times r \times \left( \frac{S}{2} \right) \]

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time</td>
<td>100 s</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>300-1000m</td>
</tr>
<tr>
<td>Vehicle speed</td>
<td>60-120 km/h</td>
</tr>
<tr>
<td>Hello message size</td>
<td>100 bytes</td>
</tr>
<tr>
<td>Hello message interval</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Vehicle density</td>
<td>10-250 vehicles/km</td>
</tr>
</tbody>
</table>

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.

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](image)

Probability for fire is 1. It denotes that the occurrence is true, overall probability of fire incident is 0.63.
The minimum probability of fire occurrence is 0.50. The values are ranging from 0.50 to 1.00 which indicates it as an honest node.

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 a trusted node.

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

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 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.

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.

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 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.

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.

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 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.

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.

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 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.

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.

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 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.
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


