Privacy-Preserving and Secure Communication using an Adaptive Signature Misbehavior Detection Framework in VANET

C.M.T.Karthigeyan[1], C.Satheesh Pandian[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering , Bargur (An Autonoumus Institution Affiliated to Anna University, Chennai) Krishnagiri, Tamilnadu, India.

[2]Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering , Bodinayakanur,Theni District, Tamilnadu, India.

Abstract

Vehicular Ad-hoc Network (VANET) is a wireless communication between vehicle to vehicle and vehicle to roadside infrastructure. The major issue of VANET is the high mobility of vehicles using wireless technology. Most of the existing solutions for data privacy in VANETs could not provide a comprehensive scheme to meet the Quality of Service (QoS) parameters. Also, existing works could not provide reliable communication, and the security storm issue has not been fully resolved. The attacker changes the transmitted information easily, captures the sensor nodes, performs its tasks, and reduces the sensor network's ability. These attacker nodes act as genuine nodes in the network and cause damage to the network. The Adaptive Certificate Signature Misbehavior Detection (ACSMD) framework is proposed for the dissemination of correct information. The proposed countermeasures are proven to detect and block internal attackers from sharing false warning messages. A lightweight authentication algorithm is introduced to provide robust authentication between contacting nodes. The Dynamic Freeway Routing Protocol (DFRP) is introduced to search the communication routing vehicle to the destination node. In this proposed method, ACSMD provides better security in the VANET environment and identifies the malicious or attacker (Node Impersonation Attack, Sybil Attack, and Distributed Denial Of Service (DDOS) Attack, and replica attacks) node. The results and analysis of the proposed ACSMD model over the standard protocols are presented using simulations.

Keywords: - Quality of Service, Sybil Attack, VANET security, Cryptography, lightweight authentication.

I. Introduction

An advanced tool for creating a temporary base in a network that uses high-speed trains as VANET nodes is essential. VANETs interface with each other and convert shared vehicles from 100-300 MTS to remote switches or nodes to allow the network to have a wide range. Different vehicles participate, and the vehicle interfaces are made into a portable system with each other so that the range of the car's falling flag and drop organization is organized. VANET belongs to the classification of remote ad hoc networks. In VANET, a node can be a vehicle or a Roadside Unit (RSU). They can talk to each other by allowing remote connections to a particular range. VANET is widespread and has recently become well known. The structure is presented in figure 1. The main contrast is that the mobile router in the assembly system is a car or truck. Several different uses are rising depending on the vehicle's response.

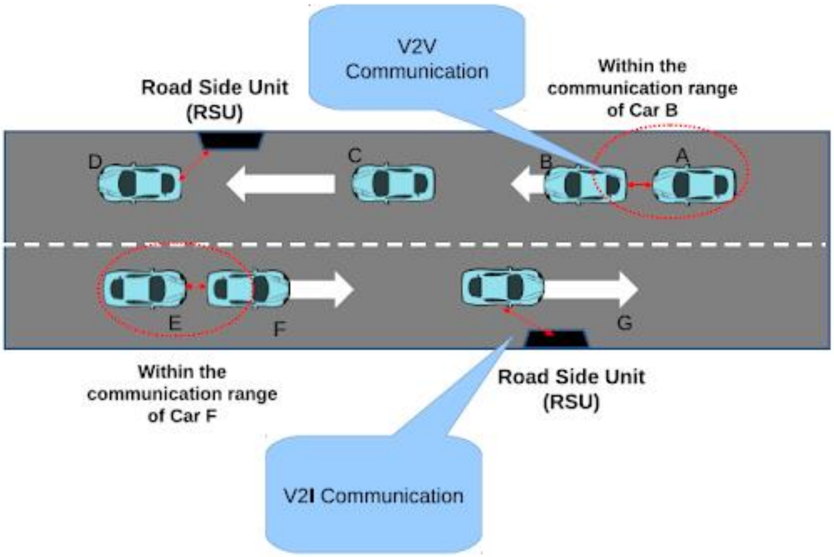

Figure 1. VENET architecture

Some safe products also reflect the significant problem. The subject of the information is to use the information within most of the time opportunities at the Qualification Center. Confirmation is an explicit requirement of VANET that the data source must be checked to ensure the authenticity of the information given. Wired system applications and VANET applications share various warranty prerequisites, but VANET applications usually have a gradual and rigorous need to verify their wired system. A specific level of the unnamed is usually required to ensure the driver's safety, and the validation model needs to ensure that this secret is maintained. It is the reason that needs to be confirmed for the purpose and is not known in most cases of the use of ID cable systems in existing gatherings. Authorized personnel must be allowed to remove unclear preconditions in the obligation-related example of legal inspections. Security prerequisites are set for VANET, and countless attacks are considered to be negotiating over them. Detailed conversations in this area clarify what they can do and their potential outcomes under these attacks. Invaders typically generate clients with different system glitches and troubles. The invaders are stationed according to the instructions of natural and positive action.

a. Node Impersonation Attack

The malicious or attacker vehicle node stands between two authentication vehicles. The attacker node (A) sends a repeated communication request between V1 and V2. That two-nodes V1 and V2 are assumed to directly communicate wrongly. The attack process is presented in figure 2. This type of attack is also called an Invisible Node attack.

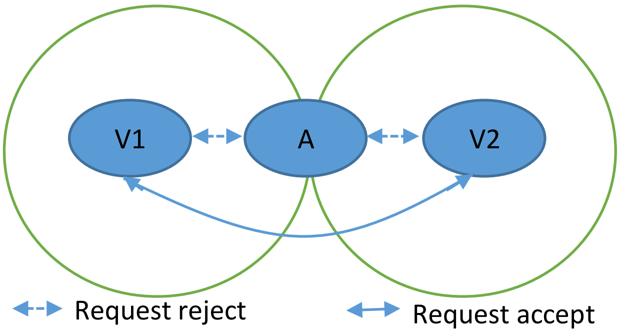

Figure 2 node impersonation attack

b. Sybil attack

The attacker vehicle node sends multiple messages with different IDs from other vehicles. They used to send multiple messages with different ids from the same location. The authentication vehicle thinks that these messages come from a different source, so the collision occurs and is enforced to take another route.

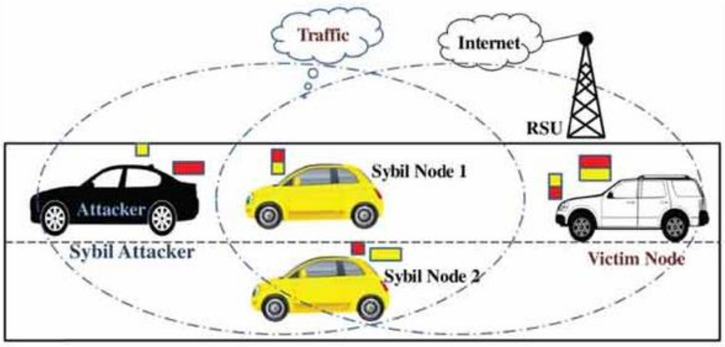

Figure 3 Sybil attack

The Sybil attacker creates more ids request to the victim node to create the traffic and change the communication route. The process of the Sybil attack is shown in above figure 3.

c. Distributed Denial Of Service (DDOS) attack

DDoS attacks are more vital than DOS attacks because it is a decentralized method. Here, the attacker uses different time slots to send messages and uses different locations to launch attacks.

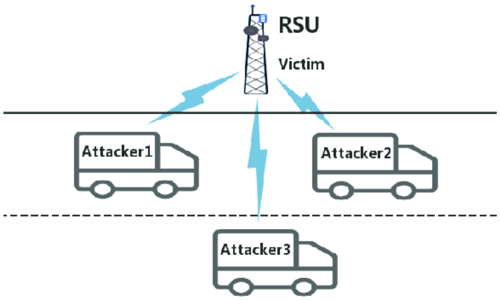

Figure 4 DDOS attack launching V2I (vehicle to infrastructure)

The nature of the message may change from vehicle to vehicle creating a network using these time slots that are not available to the communication vehicle. The vehicle to infrastructure DDOS attack process is presented in figure 4.

d. False injection attack

It has legal authority; malicious vehicles can send messages and data to other vehicles irrespective of their being an illusion or illegal. They may also modify other laws messages or data from the relay node that receives and processes the transmitted neighbors.

II. Related work

In this section, earlier methods of VANET security and attack analysis techniques are presented. The VANET security state model using a Homogeneous Continuous-Time Markov Chain (HCTMC) method was presented [1]. The HCTMC is stubborn as a function of transmitted data, dynamics vehicle channel randomness, and security strength values built into the transmission delay of the current context in VANET. First, a summary of the details of the VANET structure and the Software-Defined Networking (SDN) controller layer and infrastructure is given. Second, in describing different wireless communications, SDN-VANET applications such as Visitor Noise Ratio (VNR) [2] and VANET Internet check some parameters and compare the concentration of SDN-VANET applicable. Existing systems do not verify the Confidentiality, Integrity, and Availability (CIA) of the underworld [3] simultaneous services. Therefore, the method is presented in [4], which uses end-to-end verification in VANET to solve evasion intrusion for security in VANET. While guaranteeing the privacy of the vehicle, it is difficult to define whether the communication sent by the vehicle is trustworthy. A conditional trust management approach [5], block chain-based trust management model [5], combined with a conditional privacy-preserving announcement scheme, are suggested in VANET.

To study Road Condition Monitoring (RCoM) methods [6], the major powers helped cloud servers create timely and accurate real-time road condition responses in emergencies. They must be borrowed and supervised. In ref [7], Cascade Connection Trust Emergency Message Distribution (TCEMD) effectively employs entity-oriented trust values for data-oriented reliability evaluation. It has been proposed to use a vehicle and roadside unit (restricted stock unit), traceability and security access authentication scheme between the distributed Internets, a vehicle system framework for intelligent vehicle-to-vehicle communication [8]. On the other hand, that solution allows the vehicle to use the anonymity of renamed Vehicle-to-Vehicle (V2V), and vehicle-to-Information (V2I) communications in an incomplete reliable environment.

A Trust-Based Distributed Authentication (TDA) approach relies on global trusts servers and vehicle activities to avoid collision attacks [9]. It can ensure the safety of communication with the vehicle in two-car workshops in the network. In addition, the Channel State Routing Protocol (CSRP) offers improved communication reliability between vehicles. It has a mode privacy protection that needs to meet proper communication in VANET and a lightweight authentication protocol with the hash function and XOR operation. Using the protocol BAN to achieve security goals [10] shows the logic of informal security analysis It is used to verify the security of the protocol. The results show that privacy can be simulated and guaranteed under attack.

The resources for holding restricted stocks have been exhausted, and It is no longer a legal vehicle to provide services[11]. Since the vehicle's power is related to the possibility of a very successful attacker, the arrival and departure of vehicles of that model depends on the M / M / N queuing system. It shows how an attacker can adaptively select different attack strategies to attack different traffic environments. In ref [12], the author uses the Convolutional Neural Network (CNN) for Effective anomaly detection. This method takes the sparse properties of space-time and the VANET traffic to the account. It extracts the Mahalanobis distance which uses the neural network architecture convolution to estimate the flow matrix loss function.

In ref [13], the functionality of Multi-Generation Mixing (MGM) is implemented by incorporating an architecture that exercises the SDN concept to increase the reliability of in-vehicle networks and the security of data transmission with Network Coding (NC). Protocols are designed based on MGM-NC for encoding and decoding data. In ref [14], the author proposed a new biologically inspired spider monkey approach for time synchronization technology for large-scale VANET to improve time-synchronized packet transmission to minimize energy consumption. The proposed technology is based on a heuristic stimulus derived from the natural spider monkey behavior framework approach. [15] The author proposes security authentication and key management methods in that article. The edge computing infrastructure and new in-vehicle ad hoc network system models use a more traditional VANET structure in our design to provide sufficient computing and storage capabilities.

[16] Automatically they register, update, and unlock user public keys; an efficient Decentralized Key Management Mechanism (DB-KMM) approach is used to blockchain and VANET. At the same time, lightweight mutual authentication and key agreement protocol based on the binary polynomial has also been proposed. This secures real-time traffic data aggregation method is [17] a cloud of vehicles in VANET. After the validity of the vehicle, a signature is confirmed by the proposed method, and the original business data is recovered from the signature. For an effective multi-key secure outsourcing computing scheme [18], MSOC-free use is the first FHE to propose public keys in the settings of two non-collusion servers, namely Clouds and Cryptographic Service Providers (CSPs).

2.1 Problem Statement

❖ Security and privacy are important factors and major issues that need to be addressed when deploying in-vehicle communication systems. Most researchers do not consider secure communications.

❖ The existing methods could not achieve high performance; there is low throughput performance, Packet Delivery Ratio (PDR), high time complexity performance, high packet loss, and it is difficult to find the attacks.

III. Implementation of the proposed method

Roadside Unit (RSU) Communicates with a trusted authority via short-range wireless communication between the roadside unit and the vehicle via the Internet backbone network. Therefore, the RSU detects a malicious vehicle within that range, and it can be notified of other entities misbehaving of the vehicle. The proposed Adaptive Certificate Signature Misbehavior Detection (ACSMD) framework is implemented to verify the communication node certificate signature and identify the malicious node. The trusted authorities are responsible for registering and embedding public security parameters and public keys for the vehicle's On-Board unit (OBU).

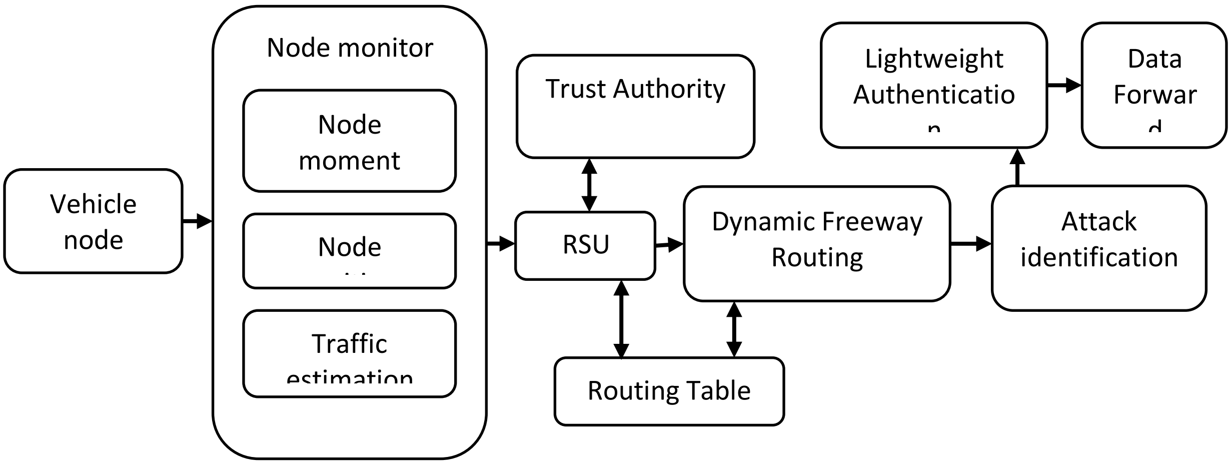

Figure 5. Proposed method block diagram

To trace the vehicle location and estimate each node’s speed of movement, communication channel behavior and the block diagram are presented in figure 5. Network of trust factor control at the source of the data packets will help to promote the time control mechanism. Dynamic Freeway Routing Protocol (DFRP) avoids the routing overhead and identifies the shortest communication multi-paths between communication nodes. The lightweight authentication method used to evaluate the reliability of the vehicle channels should ensure the secure transmission of data over a secure communication channel. Node Impersonation Attack, Sybil Attack, DDOS attack, and replica attacks are identified using this proposed method.

These attacks have different behavior in the VANET environment. The node impersonation attack can communicate between two nodes and update their signature key, when two nodes request data transfer. The Sybil attack sends request messages continuously from different vehicle id. When traffic accrues, it will search for another route for communication. First, verify each node signature key from the RSU trust authority node and allow communication. In this trust, the authority verifies the vehicle information that whether they have a unique id or not. In the proposed protocol, the transfer node receives an acknowledgment from the receiver and verifies that the two keys are the same. If keys do not match, the node is removed from the network. This authentication method verifies each vehicle node packet and network and identifies the authentication type attacks (Sybil and node impersonation attacks). The RSU monitors each node's position, moving average speed, and traffic estimation that helps avoid the collision and identifies the Sybil attack node. When the node generates multiple requests with different ids, the RSU verifies each vehicle node distance and matches the position of the update to the routing table. The registered base station (BS) database analyzes each vehicle node identification information to identify DDOS attack node information. The base station is responsible for checking the authentication to improve the security performance.

3.1 Coefficient Node Selection for a trust model

This trust model coefficient node selection algorithm collects the vehicular node IDs, timestamps, and current locations and compares their initial information at registration. The adjacent node selection depends on the ratio of the Correlational coefficients. The correlation method is used to verify each transmission packet that whether they are sent repeatedly to avoid redundant data. It will execute node selection, when the node transmits the data packet. Each vehicle node digitally signs to RSU and locally broadcasts its claim ID and geographic vehicle node location (g (i, j)). Each neighbor sends (with probability p) the claim to a set of g > 1 pseudo-randomly selected network locations. By checking the path, "hello," packets are routed with the opportunity to ensure the reliability of the transmission. However, the information is sent undetected. Therefore, the coefficient ratio model is designed to select adjacent nodes. The calculated safety nodes for these coefficient values depend on the security entropy value. In this belief, the neighboring vehicle node is in contact with each vehicle node, which has an equal coefficient value of the two nodes. It is difficult to compare the two pairs of node correlation values and random neighbor node selection information. Reliability is the probability of successfully delivering a message to its intended destination before the message's lifetime expires.

The two-node values depend on the node location and the range of personal data transfer. Correlational coefficient-based node selection is followed in equation 1.

Node coefficient ($C_{i,j}$) = $\frac{1}{n-1}\sum_{i=0}^{n-1}\left(\frac{SN_i-\overline{SN}}{T_{sn}}\right)\left(\frac{DN_i-\overline{DN}}{T_{Dn}}\right)$ ---- (1)

From equation 1$C_{i,j}$ is the Correlational value of Source Node (SN) and destination node (DN) with entropy (T). Now, the problem is to select "SNi," the neighbor of the node. The "SN_i" depends on each adjacent attraction to the overall adjacent SN quality value in each direction.

$C_{i,j}(pkt) = \frac{1}{n-1}\sum_{i=0}^{n-1}\left(\frac{SN(pkt(i))-\overline{SN}(pkt\,(i))}{data_{pkt}}\right)$ --- (2)

The above equation is used to calculate the optimal node selection problem which minimizes redundant and replica data from the vehicular network. The source node on moving different locations is used to evaluate the average location of node based on $\overline{SN}$ which is a vehicle moving direction possibility point.

The source node moves to different locations to evaluate the vehicle node's average location based on $\overline{SN}$ (a vehicle moving direction possibility point). The node moves the vehicle's moving speed to take T_{sn}.

The two pairs of node correlational coefficient values.

Correlationalþ (i, j) = $2 - \frac{cov(\alpha(i,j),\alpha 1(i,j))}{\sqrt{F(i,j)}}$ --- (3)

þ (i, j) represents the correlation coefficient value of I and j nodes with the mutual information (transmission node point) $\alpha(i,j)$ and the communication joint function $F(i,j)$. The $F(i,j)$ (RSU to vehicle) communication point, the vehicle are signed from RSU.

Algorithm steps:

Step 1: To analyze the degree of node angle and number of connection edges in terms of equation 1 which is as follows

$SN_i = \sum_j C_{i,j}$ + þ (i, j) --- (4)

Step 2: To evaluate the outgoing (massage transmission vehicle) (SN_i^{out}) and incoming (message receiver node) SN_i^{in} node getaway edge and the node ID, timestamp. Then the total trust value to calculate the combination of in and out node edges is performed in equation 6.

SN_i^{out}=$\sum_j n_{i,j} \cdot g(i,j)$ --- (5)

SN_i^{in}=$\sum_j n_{i,j} \cdot g(i,j)$ --- (6)

$SN_i^{tot} = SN_i^{in} + SN_i^{out}$ --- (7)

Step 3: Ni =Ni+1 (msg, τ) to get the information

$SN_i = þ(ID, \tau, g(i,j))$ // vehicle id, timestamp (τ), location g (I, j)

Where the Ni is the neighbor vehicle node

Step 4: to initiate the trust evaluation compared to base station register and each node correlated coefficient value þ (i, j) using equation 2 to avoid the replication vehicle node.

Step 5: Each node checks the coefficient þ (i, j) value and that value is compared to the threshold value (taken based on success rate followed by parameter packet rate, transmission rage and time) for node selection. If the vehicle node coefficient value is lower than the threshold, the node will be removed from the network.

Communication channel sensing operations form a correlation node selection architecture optimized to reduce malicious vehicle node links. The neighbor with the larger Correlational coefficient ratio value is selected as the next adjacent node. Any node information which is not in the base register, that node will not be allowed to the network.

3.2 Dynamic Freeway Routing Protocol for Route Discovery

A Dynamic Freeway Routing Protocol is implemented where a node (source) needs a path to another node (target) which initiates a flood-based route discovery process. The target is used to transfer the nearest neighbor information irrespective of its authentication and it is also called freeway forwarding. Each vehicle node in the Dynamic Freeway Routing Protocol knows its current physical location and a neighbor RSU or vehicle node information location is to avoid node replication attacks. Knowledge of the location of a node provides better routing and knowledge of the target.

Neighboring vehicle nodes help achieve more accurate forwarding decisions without the interference of topology information. The source of the vehicle is submerged in an RREQ packet on the network. The RREQ packet is a hop list that propagates through the network (vehicle to RSU and each other vehicle), containing a collection of a path request packet. A node knows that the RREQ packet received to the destination vehicle node responds with RREP along the reverse direction of the collection route with RREQ.

Algorithm steps:

Input: RREQ message in selective or source nodes SN_i

For each connection j, k in SN_{i+n}

If source node send RREQ message to destination

$SN_i \rightarrow \sum_{j,k}^{DN} \mathrm{RREQ}\ (DN\ (\mathrm{j,k}))$

Else

$\sum_{fwd}^{RREQ} = \forall_{j,k}(t) \leftarrow \delta_{j,k}(t)$

End if

- $fwd = \forall_{j,k};$ // forward broadcast message of another available node with a t time stamp. $\delta_{j,k}(t) =$ failure node if RREQ does not reach the information sent to neighbor vehicle node.

If $J_{avai} + k_{avai} < 2$

$DSR_{\partial} = SN_{in}$

- $SN_i \leftarrow$RRES (j, k) // each node checks the response message and verifies the location. The available multi-route from the source vehicle node to the destination vehicle node path add to the DSR (Dynamic Source Routing) table.

Else

Route $(R_\gamma) = SN_{in}$" Max_{th}

$R_\gamma = max\left(2, \frac{\min\left(R_\gamma(j_\alpha)\right) | R_\gamma(k_\alpha)}{2^{SN(i-1)}}\right)$

//, where the route was infinity sent to other $R_\gamma(j_\alpha)$ which is an available sender route and $R_\gamma(k_\alpha)$, is an available receiver route

$2^{SN(i-1)}$ is the RSU node total number of available routes

$\min\left(R_\gamma(j_\alpha)\right)|R_\gamma(k_\alpha)$ Minimum length route available between sending and receiving nodes.

```
        $R_{sum} = R_\gamma(j_\alpha) + R_\gamma(k_\alpha)$
        If $R_{sum}$ =0 and $R_\gamma$ "$SN_{in}$" 3
                DSR = $\left(\frac{\max(R_j,R_k)}{Th\_DSR[Route]} XSN_{in}\right)$
        End if
    End if
End for
```

This process helps to check the number of connections and vehicle nodes to establish the communication channel. The source vehicle node forwards the RREQ message to the destination vehicle. If the request reaches the RREP from the destination vehicle, that means that the message is successfully replayed to the source vehicle. If the RREQ message fails, then $\forall_{j,k}(t)$ authenticates the neighbor vehicle to the RSU node sequence time (t) interval. $J_{avai} + k_{avai}$ is an available multi-path route that identifies the network. R_{sum} is the sum of the two routes, the shortest path to calculate the destination vehicle node. It means that a source can receive several corresponding RREP messages on a common, different route to a destination vehicle. The Dynamic Freeway Routing Protocol of the (e.g., shortest) path chooses one and keeps it in the other path's cache. If the selected route is disconnected from speeding up route discovery, the cached route can avoid the traffic.

3.3 Lightweight Authentication

Digital signatures provide authenticity and integrity. Privacy prevents vehicle tracking by issuing short-term identifiers called roadside infrastructure to avoid the Sybil attack, DDOS and replica packet attack, and false injection attack. Moreover, aggregate signatures cannot validate all signatures together, which benefits from reduced computational authentication time. To provide the security solution and privacy preservation scheme, one can think about the traditional symmetric and asymmetric cryptography techniques.

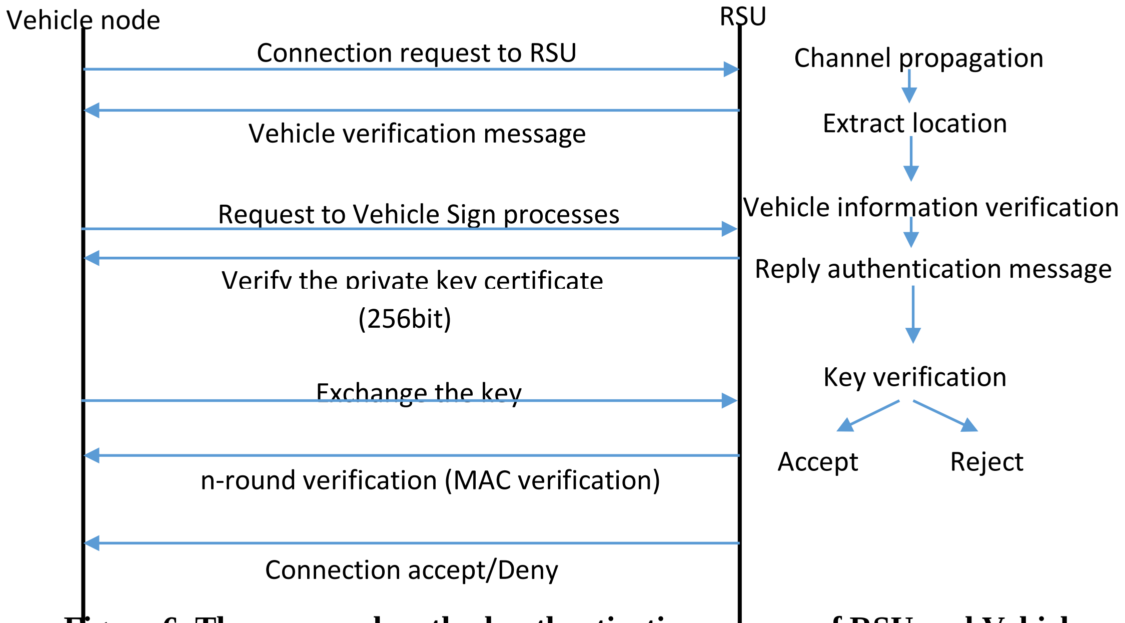
Vehicle node
RSU
Connection request to RSU
Vehicle verification message
Request to Vehicle Sign processes
Verify the private key certificate
(256bit)
Exchange the key
n-round verification (MAC verification)
Connection accept/Deny
Channel propagation
Extract location
Vehicle information verification
Reply authentication message
Key verification
Accept
Reject

Figure 6. The proposed method authentication process of RSU and Vehicle

A gateway that chooses to authenticate the vehicle's nodes during the mutual authentication phase is selected at vehicle node selection. Also, the key part of the session key securely exchanged with vehicle (v_i) and between RSU (r_j) is managed by secure key negotiation. The authentication phase is executed in 4 messages handshakes. After the user selects the desired vehicular node, the node delegates the vehicle authentication process to the gateway to verify the node's identity. After validating that identity, a trust relationship is established between the RSU and the vehicle node.

Our proposed lightweight authentication protocol using a k n-round-pass with 256bit sent authentication message to all neighbor vehicles (number of vehicle in VANET environment) and then establish the connection. The n-round verification process initially verifies the vehicle node location and information of the vehicular node. Next round verification is done for private key certification of the vehicle and finally the vehicle node MAC address with register database is validated. The process of authentication is presented in figure 6. The parameters t and p are bound with the maximum length (max) of a message.

(1) The vehicle node initiates a request by sending a request message to the RSU node, then the node in the message (2) delegates the vehicle message to the gateway to authenticate the requesting node (both vehicle and RSU node already registered with the gateway in node selection). If authentication passes the gateway, it returns a message to RSU (r_j), (3) authenticating both the vehicle and the RSU node. Finally, in the message (4), the RSU authenticates the vehicle node and communicates exchange information.

3.4 Authentication procedure:

Key Generation: The key generation involves the computation of (private key, public key) pairs. First, an RSU ring element is chosen $a \in R_q$ (R_q-request) with a prime number $n \in \delta$ n number of round authentication. Then, select s and $e \in \delta$ where e is the error value and δ random integer. Based on this, the public key is computed as$k = a_s + n(\delta)$. Which is defined as by k=as+b, where s refers to the secret key.

It can run the proposed encryption method key generation algorithm registration machine to enter the system parameters. It outputs a public / private key pair.

Vehicle Sign processes: H is the collision-resistant hash function H: {0, 1}$\rightarrow R_q$. m is the message. To sign a RSU, select vehicle $v \in R_q$ from uniform distribution over R_q. Choose $e \in \delta$ and compute$r_j = (v + H(m)).s + n(\delta)$. Return the signature ((v, u) on m).

Verification: On input the public key k = (a, b) the signed message (m, (v, u)) and H (m), Output 1 if$(v, u) \in R_q * R_q$and the condition $[-a.u + b.v] mod\, n == -b.H(m) mod\, n$ is established, Otherwise output 0.

Establish Connection: Receive messages sent fromr_j. First, check the time freshness of the received message m_t. If the time difference between the sent time t and the current time of V is within the allowed timespan, the RSU continues the authentication with $r_j(n) \rightarrow v_i$. Otherwise, the session is terminated, and a rejection message $r_j$is sent.

3.5 Process of VANET communication and attack detection

The Adaptive certificate signature misbehavior detection (ACSMD) method is proposed to verify the location information of each node. This proposed method makes RSU a two-way initial phase to authenticate all vehicle nodes. RSU verifies each vehicle node information using N-Round Pass Lightweight Authorization to establish a communication link. In this process, each node key certificate, MAC, location and private keys are to be verified. After that, each node's operating direction, speed, and data packets are to be monitored and check for any malicious node and protect it from the attacker in the network. When the malicious node can try to communicate the RSU, The RSU checks the MAC, public key, location, and node information (ID, timestamp, other) and then verifies the authorized or unauthorized vehicle.

Step 1: To initiate the network model and select the vehicular nodes (v_i) in the VANET environment.

Step 2: Verify each node information $v_i = \{ID, \tau, g(i,j)\}$ with the registered database (Base station) help of the RSU node. If the resulting factor is more than 1 means, it is deemed to be registered in vehicle register, otherwise it is rejected and moved to sign process.

- Then, the RSU node verifies the ID of another equal vehicle node and executes the lightweight authentication process to check the attacker or malicious vehicle.
- The correlation node selection process traces each node information and a data packet to avoid false packets or messages in the VANET environment.

Step 3: The vehicular requester node sends the request message (m) to the vehicular source node via RSU. The RSU node traces the requested vehicle node location and traffic rate based on a vehicle moving speed.

- When the number of requests is received from the same location, check node information and remove the vehicle on the network. If the node is authorized, the routing method executes the available search route and checks the traffic conjunction, this process avoids collision.

Step 4: After the route is established, source vehicle transmits the message (m, (v, u)) to encrypt using a public key and transmit to the destination vehicle node. If any malicious user can access the message, RSU executes an authentication process to avoid the attacker.

- The node monitoring process checks the packet transmission speed and timestamp values. If any packet receives a delay, the routing method traces the node location, then transmits the message to another available route.
- When the RSU node receives the number of requests, it checks the request node location, other information and neighbor node information to identify the DDOS node and replica request.

IV. RESULT AND DISCUSSION

This experimental analysis analyzes the vehicular wireless sensor network's operation and performance with the proposed method. RSU is an access point that has been supporting V2I communication and magnifying V2V connectivity communication. In this method, NS-2 has been implemented using common network simulation tools. This tool has been used in the field of wireless sensor networks. The simulation time is 500 seconds, and the time during the simulation process varies, and statistics are collected.

Table 1 proposed method simulation parameters

Parameters	Value
The dimension of the network	X-axis 500 and Y-axis 500
Simulation Tool	NS2
Propagation	Two Ray Ground
Access control	802_11
Node connectivity	Multi-hop and centralized
Simulation time	500sec
Number of nodes	100nodes(Malicious node-5)
Communication	RSU-Vehicle/Vehicle-RSU
Data size	250MB
Packet size	512kbps
Number of packets	500packets

Table 1 shows the proposed method’s simulation parameters. VANET node movements are confined to a 500m x 500m area with a 3-second pause. In this proposed Adaptive Certificate Signature Misbehavior Detection (ACSMD) method, simulation results are evaluated based on QoS parameters such as Packet Delivery Ratio (PDR), throughput (TH), End-to-End Delay, and detection ratio (DR). Furthermore, it is compared to existing method like a Homogeneous Continuous-Time Markov Chain (HCTMC).

$$Packet\ Delivery\ Ratio\ (PDR) = \frac{Total\ number\ received\ packets}{Total\ number\ sent\ packets} * 100 \qquad ---- (8)$$

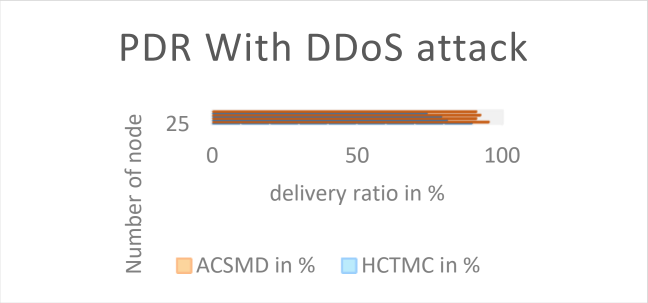

Figure 7(a) comparison analysis of PDR with DDoS attack

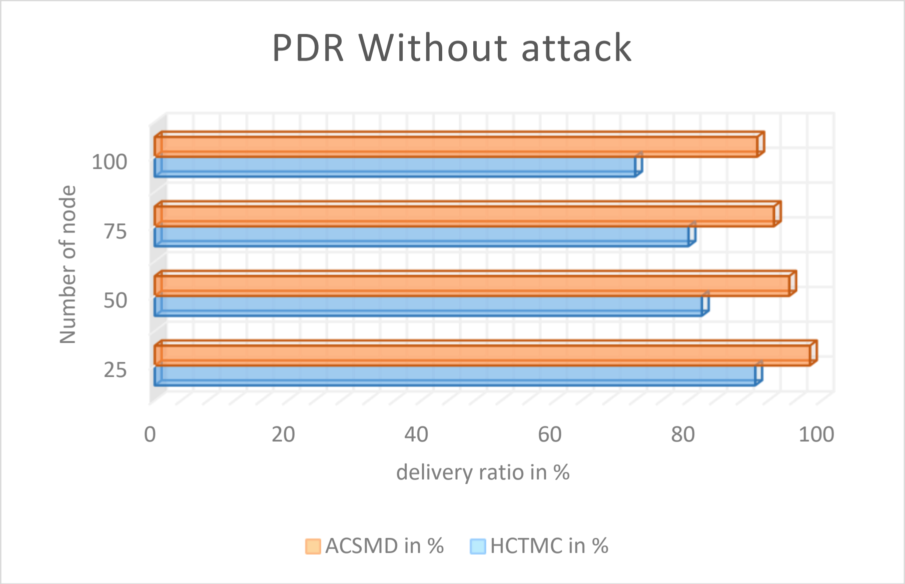

Figure 7(b) comparison analysis of PDR without attack

Figure 7 (a) depicts the comparison analysis of the average Packet Delivery Ratio (PDR) of the existing and proposed method ACSMD with a DDoS attack, and figure 7(b) shows the depiction without attack PDR value. The proposed ACSMD algorithm has a 90.6% average packet delivery performance without attack and a 91% of delivery ratio with the attack. Similarly, the existing method HCTMC has 74% data delivery ratio with the attack in the network.

$$Throughput = \frac{Number\ of\ recevied\ packetsX\ packetsize}{Simulation\ time} \qquad \text{---- (9)}$$

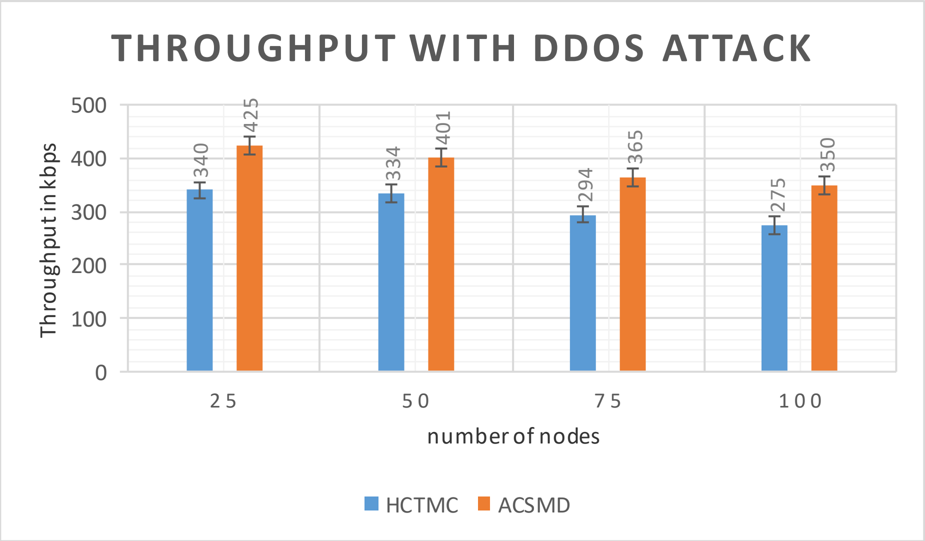

Figure 8 (a) comparison analysis of throughput with DDoS attack

Figure 8 (a) shows a comparison analysis of throughput with the DDoS attack. The existing method HCTMC and the proposed ACSMD method‘s comparison are given with attack and without attack.

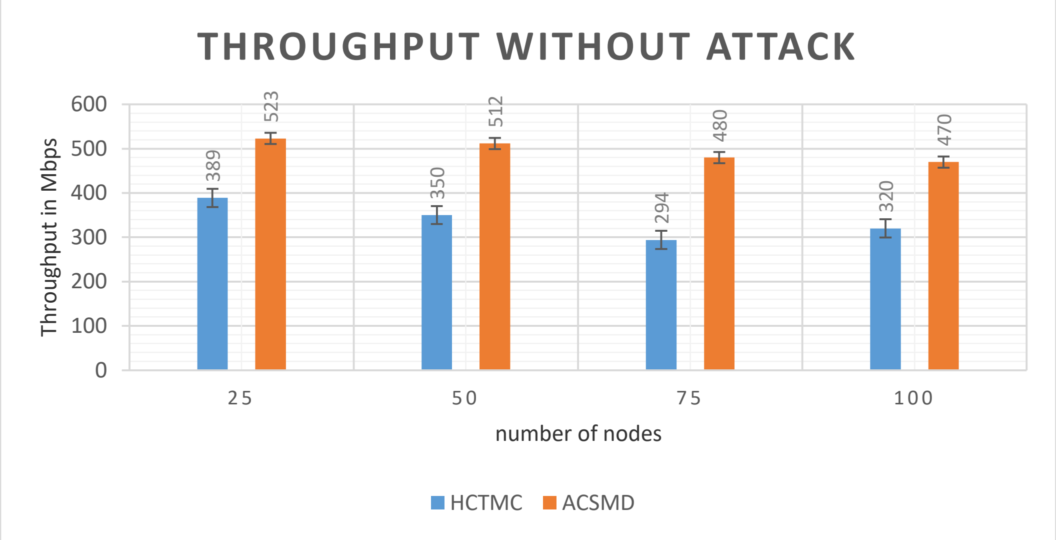

Figure 8(b) comparison analysis of throughput without attack

Figure 8 (b) defines the comparison analysis of throughput without attack. The proposed ACSMD method provides 470kbps for 100 nodes, and the existing method HCTMC has provided less throughput 260kbps.

The data exchange between the vehicles located at a different terrain causes a high end to delay. The source node successfully responds to the service ahead of time, and the data is referred to as end-to-end delay. It can be accepted from the trace file packets by the sender and the receiver generated by the difference time between packets.

$End\ to\ end\ delay\ =\ Received\ time - Send\ time$ --------- (10)

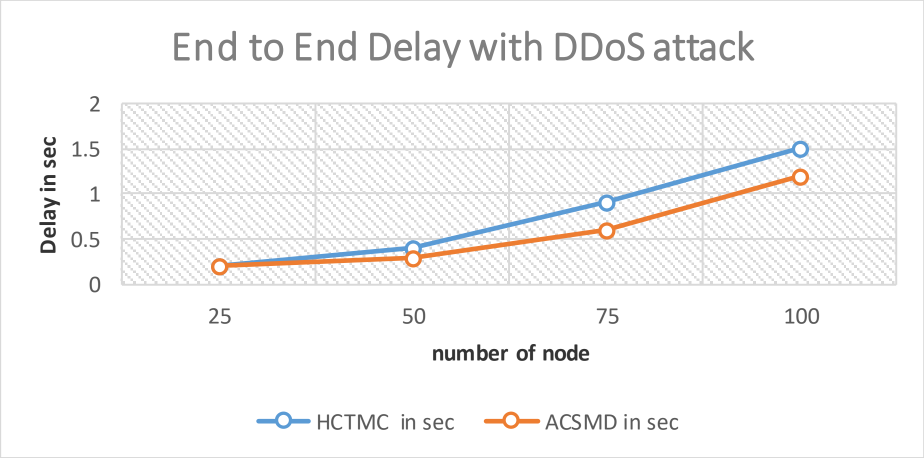

Figure 9(a) comparison analysis of End-to-End Delay with DDoS attack

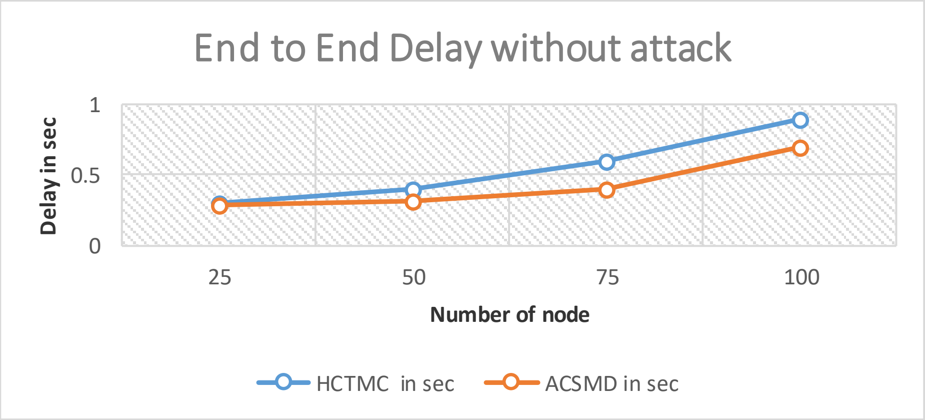

Figure 9(b) Analysis of End-to-End Delay without attack

Figures 9 (a) and (b) represent an attack without attack delay analysis. The proposed ACSMD method provides an average of 0.7sec for 100 nodes less time delay performance without attack. Similarly, HCTMC provide a 0.9sec average time delay for 100 nodes without attack. This comparison is shown in the figure. This analysis shows that the proposed ACSMD method provides less time delay than HCTMC.

In this attack, detection accuracy is to evaluate the number of attack nodes present in the network. Thus, accuracy can be defined as the percentage of error-free information received by the receiving node. Attack detection accuracy can be calculated using the following equation.

Attack Detection accuracy = $\frac{TPAD}{TPAD+FPAD} * 100$ ----- (11)

Let us assume that TPAD represents the true positive attack detection based on correctly identified attacks, and FPAD represents the false positive attacks detection based on incorrectly identified attacks.

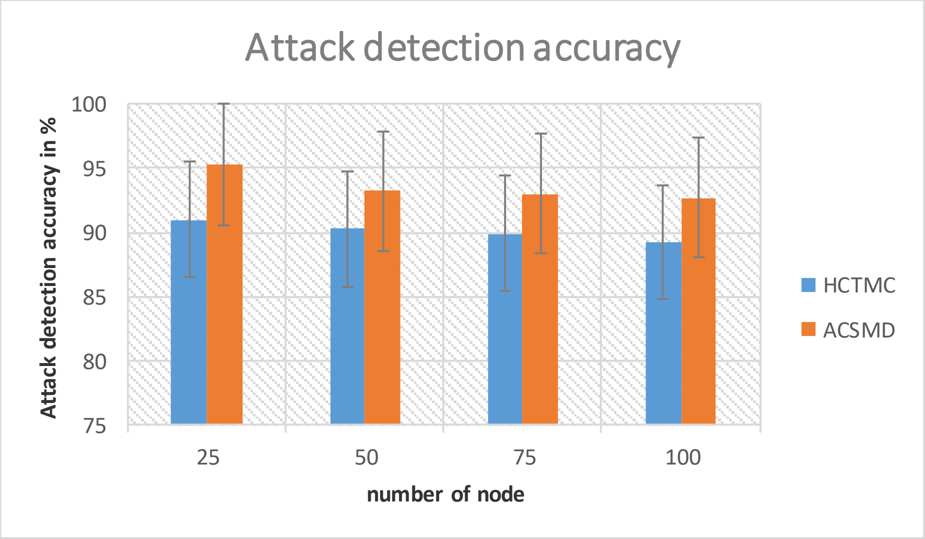

Figure 10. Attack detection accuracy

The attack detection accuracy analysis is shown in figure 10. Although the system improves its detection accuracy in all respects, the proposed ACSMD method has low detection accuracy compared to the existing HCTMC method.

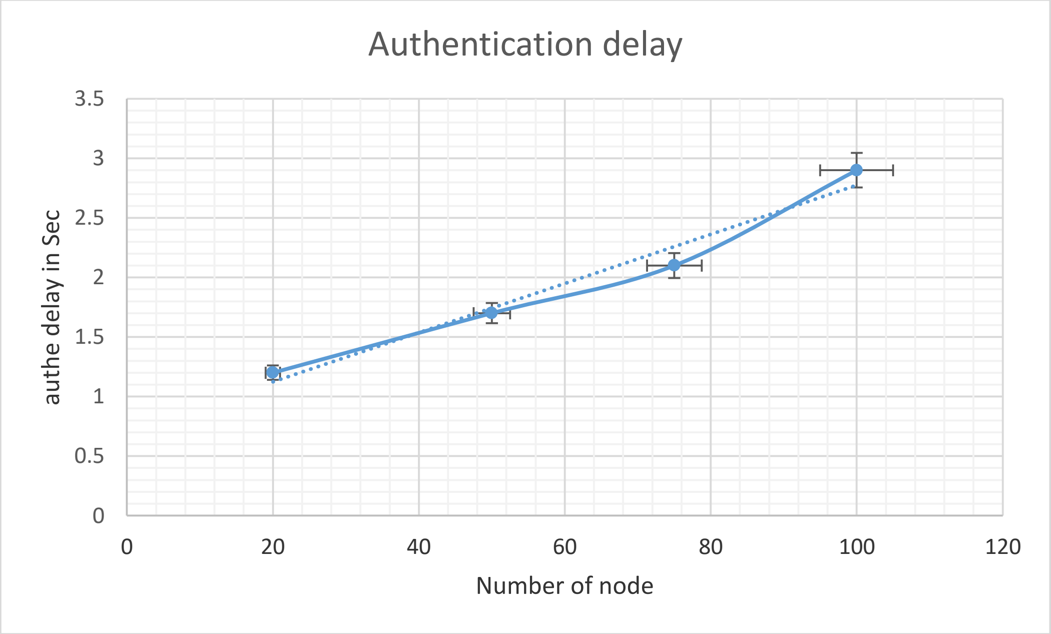

Figure 11 Authentication delay

The analysis of authentication delay is presented in figure 11. This proposed method uses a lightweight n-round pass with a 256bit key authentication process for each vehicle node (less than 1.2 sec for 20 nodes). The above figure shows the different number of vehicle node authentication results in seconds and proves that the proposed method has taken less authentication time.

Packet loss rate= $\frac{Number\ of\ sent\ packets - Number\ of\ received\ packet}{number\ of\ sent\ packets} * 100$ --- (12)

The above equation using calculate the packet loss rate performance.

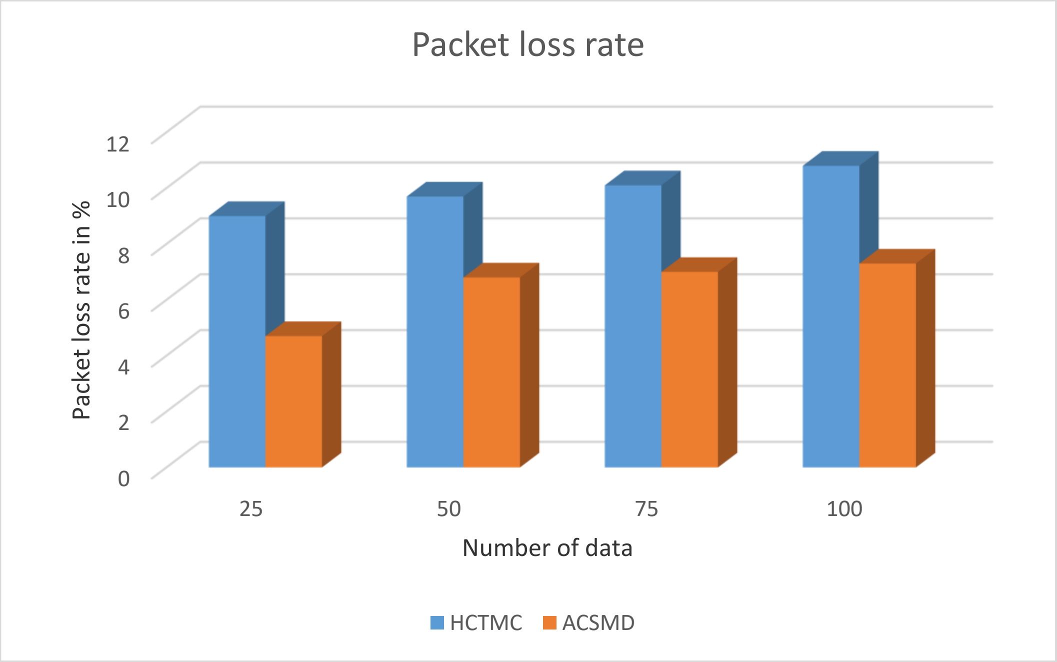

Figure 12 Analysis of Packet loss rate performance

Figure 12 describes the packet loss rate performance in percentage. The proposed ACSMD algorithm packet loss rate performance result is 7.3%; similarly, the existing HCTMC algorithm packet loss rate performance is 10.8%. The proposed algorithm gives low packet loss results compared with other existing algorithms.

v. Conclusion

Vehicular Ad-hoc Network (VANET) is subjected to various attacks due to their use and deployment environment. The main purpose of this work is to provide good protection against Sybil attacks, DDOS attacks, node localization attacks and node Impersonation Attacks. Various attack methods have been proposed in the existing works. The Dynamic Freeway Routing Protocol for Route Discovery provides multi-path communication when the source changes dynamically. It has low detection accuracy when the number of attacks increases. These issues have been addressed in the proposed work by enhancing the existing distributed detection methods using ACSMD. Correlative coefficient value is used to evaluate the node correlation trust value used for node selection and neighbor node authentication in this proposed method. The proposed methods are evaluated using the performance metrics such as packet delivery ratio, throughput, and attack detection ratios respectively.

Reference

[1]. J. Wang, H. Chen and Z. Sun, "Context-Aware Quantification for VANET Security: A Markov Chain-Based Scheme," IEEE Access, vol. 8, pp. 173618-173626, 2020, doi: 10.1109/ACCESS.2020.3017557.

[2]. O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani and H. Alsariera, "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET," in IEEE Access, vol. 8, pp. 91028-91047, 2020, doi: 10.1109/ACCESS.2020.2992580.

[3]. G. Kumar, R. Saha, M. K. Rai and T. Kim, "Multidimensional Security Provision for Secure Communication in Vehicular Ad Hoc Networks Using Hierarchical Structure and End-to-End Authentication," in IEEE Access, vol. 6, pp. 46558-46567, 2018, doi: 10.1109/ACCESS.2018.2866759.

[4]. S. A. Alfadhli, S. Lu, K. Chen and M. Sebai, "MFSPV: A Multi-Factor Secured and Lightweight Privacy-Preserving Authentication Scheme for VANETs," in IEEE Access, vol. 8, pp. 142858-142874, 2020, doi: 10.1109/ACCESS.2020.3014038.

[5]. X. Liu, H. Huang, F. Xiao and Z. Ma, "A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4101-4112, May 2020, doi: 10.1109/JIOT.2019.2957421.

[6]. Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin and H. Wang, "Privacy-Preserving Cloud-Based Road Condition Monitoring With Source Authentication in VANETs," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1779-1790, July 2019, doi: 10.1109/TIFS.2018.2885277.

[7]. Z. Liu et al., "TCEMD: A Trust Cascading-Based Emergency Message Dissemination Model in VANETs," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4028-4048, May 2020, doi: 10.1109/JIOT.2019.2957520.

[8]. D. Zheng, C. Jing, R. Guo, S. Gao and L. Wang, "A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs," in IEEE Access, vol. 7, pp. 117716-117726, 2019, doi: 10.1109/ACCESS.2019.2936575.

[9]. M. R. Tolba, "Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs," in IEEE Access, vol. 6, pp. 62747-62755, 2018, doi: 10.1109/ACCESS.2018.2875906.

[10]. X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar and N. Kumar, "A Lightweight Privacy-Preserving Authentication Protocol for VANETs," in IEEE Systems Journal, vol. 14, no. 3, pp. 3547-3557, Sept. 2020, doi: 10.1109/JSYST.2020.2991168.

[11]. Yang, J. Weng, N. Cheng, J. Ni, X. Lin and X. Shen, "DeQoS Attack: Degrading Quality of Service in VANETs and Its Mitigation," in IEEE Transactions on Vehicular Technology, vol. 68, no. 5, pp. 4834-4845, May 2019, doi: 10.1109/TVT.2019.2905522.

[12]. L. Nie, Y. Wu, H. Wang and y. li, "Anomaly Detection Based on Spatio-Temporal and Sparse Features of Network Traffic in VANETs," in IEEE Access, vol. 7, pp. 177954-177964, 2019, doi: 10.1109/ACCESS.2019.2958068.

[13]. J. Bhatia, P. Kakadia, M. Bhavsar and S. Tanwar, "SDN-Enabled Network Coding-Based Secure Data Dissemination in VANET Environment," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6078-6087, July 2020, doi: 10.1109/JIOT.2019.2956964.

[14]. C. Iwendi, M. Uddin, J. A. Ansere, P. Nkurunziza, J. H. Anajemba and A. K. Bashir, "On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique," in IEEE Access, vol. 6, pp. 47258-47267, 2018, doi: 10.1109/ACCESS.2018.2864111.

[15]. H. Tan and I. Chung, "Secure Authentication and Key Management With Blockchain in VANETs," in IEEE Access, vol. 8, pp. 2482-2498, 2020, doi: 10.1109/ACCESS.2019.2962387.

[16]. Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu and W. He, "An Efficient Decentralized Key Management Mechanism for VANET With Blockchain," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5836-5849, June 2020, doi: 10.1109/TVT.2020.2972923.

[17]. J. Shen, D. Liu, X. Chen, J. Li, N. Kumar and P. Vijayakumar, "Secure Real-Time Traffic Data Aggregation With Batch Verification for Vehicular Cloud in VANETs," in IEEE Transactions on Vehicular Technology, vol. 69, no. 1, pp. 807-817, Jan. 2020, doi: 10.1109/TVT.2019.2946935.

[18]. J. Zhou, Z. Cao, Z. Qin, X. Dong and K. Ren, "LPPA: Lightweight Privacy-Preserving Authentication From Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 420-434, 2020, doi: 10.1109/TIFS.2019.2923156.