International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Design and Develop a Trust Based Scheme for Sybil Attacker Detection and Prevention in VANETs

Ashish Chourey[1], Sitesh Kumar Sinha[2], Banshi Lal Patidar[3]

[1]Research Scholar, Department of Computer Science & Engineering, Rabindranath Tagore University, Bhopal, India
[2]Professor, Department of Computer Science & Engineering, Rabindranath Tagore University, Bhopal, India
[3]Project Manager, Department of Food Civil Supplies and Consumer Protection, Govt. of Madhya Pradesh Bhopal, India

Abstract
Intelligent transportation systems (ITS) are not complete without the incorporation of vehicular ad hoc networks (VANETs), which are a crucial component that enables vehicles and infrastructure to communicate in a secure and efficient manner. Nevertheless, VANETs are extremely vulnerable to Sybil attacks. In Sybil attack hostile nodes create multiple identities in order to disrupt network operations, influence traffic flow, or drop data packets in network. This study aims to provide a trust-based detection system to safeguard VANETs against Sybil assaults. In this paper, proposed a Direct and Indirect Trust System (DITS) approach, which calculate the direct and indirect trust of vehicles. he Sybil attacker stolen the identities of other vehicles and start to drop the traffic information in the network. The performance of proposed DITS approach is compared with CLS scheme in different vehicles density scenarios and the DITS is showing better result. The DITS approach average packets receiving is 3% more due to less delay and overhead in network. Extensive simulations have demonstrated the system's effectiveness in detecting Sybil assaults with high accuracy and low false-positive rates. The proposed DITS approach is scalable, resilient to dynamic network topologies, and contributes to enhanced security and reliability in VANET environments.

Keywords: DITS, ITS, Routing, Sybil Attacker, VANET.

1. Introduction

The goal of vehicular ad hoc networks, also known as VANETs, is to make it possible for automobiles to frequently share data in order to facilitate applications related to route planning, road safety, and e-commerce [1][2][3]. The security of the network is an essential component for each of these applications. The traditional approach to network security involves the utilization of a key management system, which not only ensures the integrity of data but also authenticates users of the network [4][5]. It is our opinion that this solution addresses the wrong problem, in addition to the fact that it poses concerns regarding privacy and is not feasible for a VANET. Large-scale VANETs cannot guarantee that nodes, once honest, will remain uncorrupted in the future [6][7].Security from attacks is the major

issue in vehicular communication. The attackers are very harmful and the aim of the attackers is to drop the traffic information or consumes available resources for traffic status forwarding [8][9][10]. Vehicles are able to share information with one another and with the infrastructure that is located along the roadside thanks to these types of communication, which in turn improves road safety, increases traffic efficiency, and enables a variety of services to be provided. The overview of all modes of communication are explain properly in [3][11][12]. In the figure 1, Vehicle to Vehicle (V-V), Vehicle to RSU (V-RSU) and RSU to RSU (RSU-RSU) communication is mentioned. If the vehicles are only communicating with other vehicles means the communication is the V-V communication. Furthermore, an on-board unit enables wireless connection. Moreover, it incorporates an electronic license plate (ELP) that displays the vehicle's distinctive number [12][13].The primary objective of VANET is to ensure the safety and comfort of passengers while assisting drivers by predicting potential risks on the road. Every car outfitted with a VANET device will function as a node inside the ad hoc network, capable of receiving and transmitting messages across the wireless network [14][15].

Collision warnings, road signal arms, and real-time traffic visualization will provide the motorist with crucial resources to determine the optimal route to events or congested places [16][17]. VANET is differentiated from MANET by distinct properties, including significant mobility constrained by road topology, an initially low market penetration rate, an unlimited network size, and infrastructure support. Given the aforementioned characteristics, it is clear that traditional VANET routing protocols have challenges in identifying reliable routing paths within VANET environments [18][19]. There are many routing protocols in VANET but problem is all are vulnerable from attacks and not able to detect the attacker presence in network[20] [21]. For certain applications, data from the single-hop broadcast zone surrounding a vehicle is adequate. Safety applications frequently depend on one-hop transmissions because too stringent real-time requirements. Nonetheless, other applications, especially those aimed at traffic optimization, require the distribution of information across broader regions. In these multihop settings, contention for available wireless bandwidth is a concern. As a result, various suggestions have been developed for effective multihop information dissemination methods.

A Sybil attacker node in a vehicular ad-hoc network (VANET) is responsible for creating many phony identities or nodes within the network in order to carry out a Sybil assault of the network [22][23][24][25]. It is possible for a malicious node to utilize these phony identities in order to control the behaviour of the network, disrupt communication, or drop traffic information in place of forward to other vehicles and infrastructure unit. The mechanism behind a Sybil attack in a VANET.

1. **The fabrication of identities**

Using stolen credentials or generating bogus node IDs, the attacker generates many phony identities in order to gain access to the network.

2. **The Participation of Networks**

At the same time as they are actively participating in the network, these phony identities are sending or relaying data to other cars or infrastructure.

1.1 Challenges and Security Implications in VANET

The inherent properties of VANETs complicate the implementation of security measures for secure communications in V-V and V-RSU contexts. In the subsequent part, we shall examine many challenges encountered by VANETs [20][26][27]. The few major challenges and security impacts are: -

- **Network Scale:** VANETs may encompass a substantial quantity of vehicles, thereby affecting their

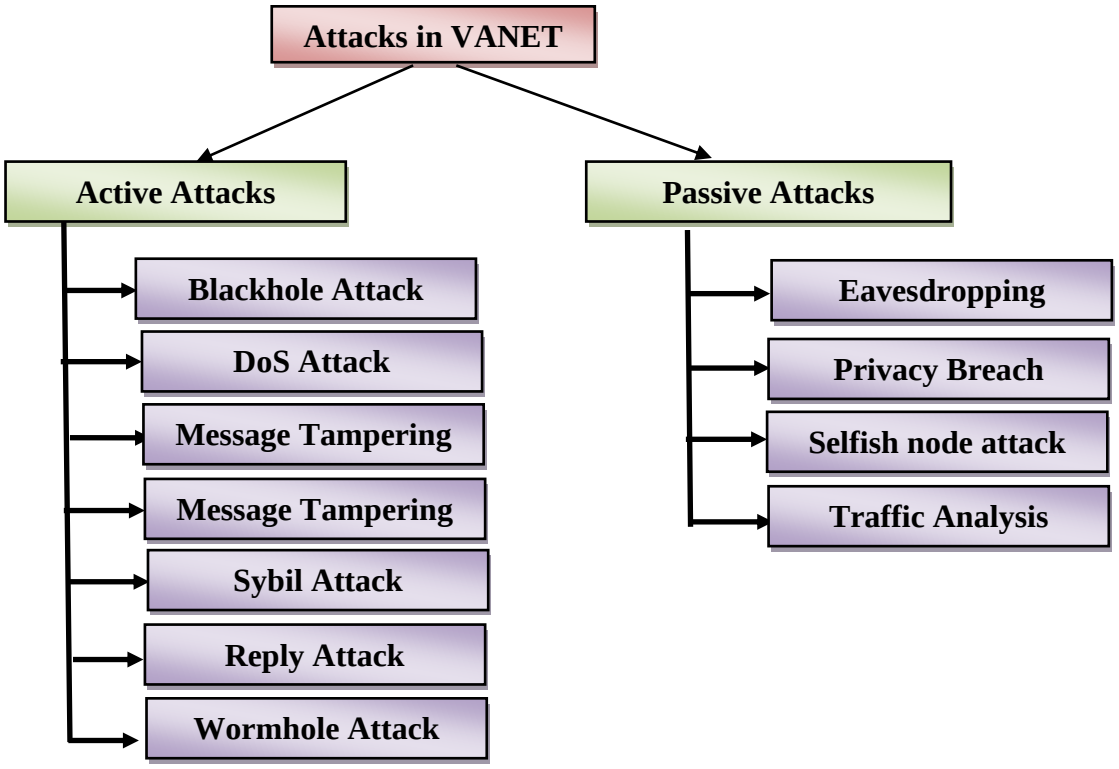
performance in the absence of a dependable and confidential process for distributing cryptographic keys to all participants. Consequently, before to implementing VANETs, perform a comprehensive analysis to ascertain the system's scalability in response to fluctuations in the number of communicating vehicles.

- **Network Volatility:** Due to the transient nature of communications between vehicles, a connection may be established briefly before being severed as a result of acceleration. Consequently, the likelihood of sustaining long-lived contexts in VANETs is minimal; implementing security measures reliant on identity verification proves challenging.
- **Heterogeneity:** VANETs depend on vehicles capable of managing diverse applications. Consequently, the functions executed by their apparatus, including GPS systems that ascertain the vehicle's position and speed, require verification. These applications must employ secure methodologies without undermining network efficiency or scalability.

2. Types of Attacks in VANET

Malicious behavior in Vehicular Ad-hoc Networks (VANETs) encompasses a wide range of attacks aimed at exploiting network vulnerabilities, compromising security, or endangering users [28][29]. These behaviors disrupt the system's confidentiality, integrity, and availability, directly affecting its safety-critical nature. In Vehicular Ad-hoc Networks (VANETs), attacks can be broadly classified as active or passive based on their nature and purpose [28][30].Here's an overview of attacker types mentioned in figure 1.

Figure 1: Types of Attacks in VANET



2.1 Active Attacks

Active attacks involve actions intended to disrupt the network's operations, compromise its integrity, or manipulate its data [31] [32]. The attacker actively participates in the network with malicious intent.Characteristics of active attacks are:

- Disruptive and overt.
- May modify, inject, or block data.
- Aimed at damaging the network, stealing data, or misleading participants.

2.2 Passive Attacks

Passive attacks aim to gather information from the network without directly affecting its operations [34][35]. The attacker remains undetected while eavesdropping or monitoring communications [31].The passive attackers are [31]:

1. **Eavesdropping:** Intercepting communications between vehicles or infrastructure to extract sensitive data.
2. **Privacy Breach:** Tracking vehicle locations or driver identities over time, violating user privacy.
3. **Selfish Node Attack:** The selfish node attack role is to flooding the unwanted information in the network and try to consume the resources required for communication [26].
4. **Traffic Analysis:** Observing communication patterns to infer movement, routines, or other private details.

2.3 Comparison of Active and passive Attacks in VANET

Sybil attacks present a significant threat to VANETs, affecting safety, reliability, and privacy. Mitigating this threat necessitates an amalgamation of cryptographic methodologies, behavioural analysis, and trust-centric procedures [33][34]. Ongoing study and collaboration are crucial for establishing strong defences against this advanced attack. The difference in active and passive attacks are mentioned in table1.

Table 1:Comparison Between Active and Passive Attacks

Aspect	Active Attack	Passive Attack
Visibility	Overt and noticeable	Covert and undetectable
Impact on Operations	Disruptive	Non-disruptive
Objective	Destroy or manipulate the network	Steal or gather information
Detection	Intrusion Detection Systems (IDS), anomaly detection	Encryption and pseudonym techniques
Prevention	Authentication, trust management	Data encryption, privacy-preserving protocols
Reaction	Alert and isolate malicious nodes	Reduce privacy risks proactively
Examples	DoS, Sybil, Replay, Wormhole attack	Eavesdropping, Traffic Analysis

3. Literature Survey

The previous work provides researchers with the inspiration to innovate in the field of attack and securi-

ty. Table 2 lists the research proposals from various researchers, along with their limitations and potential enhancements to improve routing performance [35]-[45].

Table 2: Previous work of researchers

Reference No.	Work done Proposed	Performance Evaluated	Limitations	Enhancement Possible
[35]	Proposed a fake node detection and prevention method for secure vehicular communication. In this approach, genuine vehicles give rewards, and fake vehicles are punished and given penalties.	Evaluated only fake node detection.	No other performance metrics mentioned for evaluates performance. Not compare the performance with another research.	Possible to create a fake and genuine vehicles information table for disable fake identities.
[36]	Proposed an approach that is using Decision Tree (DT), Logistic Regression (LR) K-Nearest Neighbor, Support Vector Machine (SVM), (K-NN), Naive Bayes (NB) and are applied to the dataset for attacker pattern and classification.	Evaluated the false positive ratio, balance factor, hard voting and soft voting analysis.	Difference in fake nodes and attacker is not mentioned, Hard voting and soft voting depend on malicious action of attacker infection. But infection information is missing.	Possible to maintain the fake identification record with vehicles for immediate block attacker presence. Also work on information dropping minimization.
[37]	Proposed an extreme learning machine (ELM) designated as SYDVELM. The SyDVELM mechanism generates an anomalous mobility pattern for vehicular nodes through the utilization of irregular characteristics. This enables us to contrast the actual mobility of	Evaluated the cross-entropy loss and accuracy in different time interval. Attacker loss analysis is not mentioned.	Sybil attacker active percentage in network is not clearly explained.	Possible to define some rule for the attacker malicious action. The rules are depending on any performance metrics like packets percentage ratio.

	a vehicle node with the erroneous displacement patterns of a Sybil node.			
[38]	Proposed a security scheme against DDoS attacker. The attacker detection is based on the header format, that is different in presence of attacker in network.	Evaluated the throughput, delay, drop percentage, SDN ratio, DDoS flooding.	Why attacker Flooding information is startedfrom 450 seconds. Difference in normal and attacker flooding sequence is not mentioned in cased of data dropping and vehicle out of range in network.	Possible to fixed the limited flooding by threshold and deny the extra flooding above threshold happed in network. Only allow repeated flooding for same node during retransmission.
[39]	Proposed a security scheme against blackhole attack in 6G environment. Proposed scheme detected the attacker by high sequence number and using 6G for traffic information delivery.	Evaluated the throughput, data dropping, Packet Delivery Ratio (PDR) and delay.	The sequence number method is the common method of attacker detection. Except 6G no novelty in approach. 6G data rate is mentioned but proper utilization is not possible in light traffic density.	Possible to use the high data rate for long distance traffic management or for forwarding and emergency service on roads.
[40]	Proposed a priority-based scheme for improve QoS. Use k-hop method with time required for connection establishment. Use the concept of clustering for filter the inputs and improve routing performance.	Evaluated Packet delivery ratio and packet loss ratio in 150meters and 300meters transmission rang in perority-1 and priority2. Evaluated end to end delay in priority-1 and priority-2.	Location information of vehicles is not mentioned in any analysis. Cluster head and cluster members information is missing.	Possible to use location-based protocol for maintain location information with multipath approach.

4. Problem Statement

The Vehicular Ad hoc Network (VANET) is particularly vulnerable due to its dynamic topology and distributed management, which is facilitated by multiple roadside units (RSUs) or multiple ITS. To overcome the network vulnerability, i.e., security and reliability needs, the well-defensive system, which provides the network, is more promising to users. In this paper, This behaviour can result in potential accidents, a loss of faith in the system, and violations of privacy rules. The development of strong techniques that can detect, prevent, and mitigate Sybil assaults while simultaneously maintaining the scalability and privacy of VANETs is a significant task.

- It is possible that authority figures and drivers will lose faith in the dependability of the VANET system.
- The use of false identities distorts routing and decision-making, which in turn results in the dissemination of false information.
- False information about traffic or emergency notifications posted on the road may cause accidents or traffic congestion.
- Using false identities, Sybil attackers are able to listen during communications or track vehicles for further surveillance.

5. Proposed Direct Trust and Indirect Trust Scheme for Sybil Attacker in VANET

Vehicular ad hoc network is a collection of vehicles to form network for exchanging message from one to another based-on radio zone. The network is a semi-ad hoc network where some devices are movable and some are fixed, in this network base station (BTS) or road side unit (RSU) is fixed device and treated as central controller of network, which play an important role such as monitor vehicle activity, sends control signal and monitor real time traffic condition of the network.

5.1 Indirect Trust Calculation:

The calculation of indirect trust of any vehicle is calculated by their past behavior such as packet forwarding ratio, delay time, drop ratio, number of unauthorized message. Base station is responsible to calculate the indirect trust of any vehicle and their weight for final trust calculation is assign as 30%. The following formula helps to calculate indirect trust of any vehicle.

$$\boldsymbol{PFR_v} = \frac{\sum_{i=1}^{n} \boldsymbol{Forward_i}}{\sum_{i=1}^{n} \boldsymbol{Received_i}} \quad \text{.....(1)}$$

Where

$\boldsymbol{PFR_v}$: Packet forwarding ratio of vehicle v at i^{th} time

$$\boldsymbol{T_t = L/B} \quad \text{.....(2)}$$

$$\boldsymbol{TD_p = T_t + T_p + T_q + T_{proc}} \quad \text{.....(3)}$$

Where

B is bandwidth in bps and L is size of data in bit.

$\boldsymbol{TD_p}$: Total delay of packet from source to receiver node, $\boldsymbol{T_t}$ is transmission time delay, $\boldsymbol{T_p}$ is propagation delay, $\boldsymbol{T_q}$is queuing delay and $\boldsymbol{T_{proc}}$ is processing delay.

$$\boldsymbol{Drop_r} = \frac{\sum_{i=1}^{n} \boldsymbol{Drop_i}}{\sum_{i=1}^{n} \boldsymbol{Received_i}} \quad \text{.....(4)}$$

Where,

$\boldsymbol{Drop_r}$: Drop ratio, $\boldsymbol{Drop_i}$is number of data drop

Number of unauthorized message

$$Un_{msg} = (TG_{msg} - AFH_{msg}) \text{.....(5)}$$

$$I_{dt} = \frac{PFR_v - Drop_r}{PFR_v}, \begin{cases} if\ PFR_v > Drop_r, increase\ turst \\ PFR_v < Drop_r,\ decrease\ trust \\ PFR_v = Drop_r, No\ change \end{cases} \text{.....(6)}$$

If $TD_p > avg(TD_p)$&Un_{msg} $found$ than no need to calculate indirect trust it simply I_{dt} = 0 assign.

Where,

I_{dt}: Indirect trust of vehicle i, Un_{msg}:unauthorized message, $TG_{msg}$is total different types of message generated by network, $AFH_{msg}$is actual header format of network protocol

5.2 Direct Trust Calculation:

Direct trust is calculated during real time bases while network in execution mode, in this criteria any of the vehicle behave like identity spoofing than it's treated as Sybil attacker vehicle. To detection that type of attack is critical because it's behave as legitimated node and capture the data of other node. In our proposed direct indirect trust system (DITS) calculate the direct trust with their real time behavior such as packet forwarding ratio, mapping ratio of MAC address to IP address, data drop, movement of vehicle, individual participation ratio in network. These parameter associate to calculate direct trust of node and takes 70% of weight for final trust calculation, in the below following formula is used to calculate direct and final trust. In the equation (7) and (8) for vehicle final velocity = v and displacement = s calculation.

$$v_i = u_i + a_i t \text{ .....(7)}$$

$$s_i = u_i t + \frac{1}{2} a_i t^2 \text{ .....(8)}$$

$$\mathbf{Avg}(s_n) = \frac{\sum_{i=1}^{n} u_n t + \frac{1}{2} a_i t^2}{Y_n} \text{.....(9)}$$

Where u_i: initial velocity of vehicle i, v_i: final velocity of vehicle i, a_i: acceleration of vehicle i and t: time, $\mathbf{Avg}(s_n)$: average displacement of vehicle n.

$$A_{map} = \frac{No\ of\ IP_t}{MAC\ address} \text{.....(10)}$$

Where

A_{map}: MAC to IP address mapping ratio, no of IP_t: number of IP address assign to vehicle at time t, MAC address: unique MAC address.

$$IP_i = \frac{No\ of\ packet\ in\ Y_i}{Total\ No\ of\ packet\ flood\ in\ network} \text{.....(11)}$$

$$AVG(P) = \frac{Y_n}{Total\ No\ of\ packet\ flood\ in\ network} \text{.....(12)}$$

Where

$(IP_{per})_i$: Individual participation ratio of vehicle i, $AVG(P)$: average participation ratio of Vehicle, Y_n: number of vehicles in network.

$$DT_i = \frac{s_i + IP_i}{\mathbf{Avg}(s_n) + AVG(P)}, \begin{cases} if\ DT_i > 1, untrusted \\ DT_i = 0,\ not\ participated \\ DT_i < 1,\ assume\ as\ trusted \end{cases} \text{.....(13)}$$

Where

DT_i: direct trusted

Total Trust Calculation:

The sybil attacker is detected by combining of direct and indirect trust, which depends on trust value if final trust (FT) is greater than 0.5, $\boldsymbol{A_{map}}$ = 1 and $\boldsymbol{Un_{msg}}$ = 0 is means vehicle is trusted and increase the trust value by given equation (14), otherwise node set as un-trusted if FT ≤ 0.5 or $\boldsymbol{A_{map}}$> 1 and $\boldsymbol{Un_{msg}}$> 0, The total trust of vehicle is calculated by equation (14),

$$\boldsymbol{FT_i = w1 * DT_i + w2 * I_{dt(i)}} \text{.....(14)}$$

Where

$\boldsymbol{FT_i}$: Final trust of vehicle I, weight vector (w1, w2), w1: 0.7 and w2 = 0.3, w1 + w2 = 1. All the formula used to detect the sybil attacker node in vehicular communication.

The roadside unit is also responsible for forwarding the location information to other RSUs and legitimate vehicles. If the vehicle is deemed malicious, the RSU immediately blocks the attacker node, does not respond to the attacker vehicle, and does not allow it to enter the VANET network. RSU also monitors vehicle-to-vehicle communication to check for adherence to network protocol rules; if not, it flags the vehicle as malicious and blocks it. The RSU device incorporates a trust-based system, which aids in accurately identifying a Sybil attacker node and enhancing vehicular communication security.

6. Simulation Parameters

The simulation parameters used for the simulation of Sybil attacker, previous CLS approach and proposed DITS scheme is mentioned in table 3. The attacker's aim is to drop the number of data packets transferred by the sender to the receiver. There is only one attacker in the network. There are multiple attackers present in the network. Not only evaluate the performance of the proposed DITS scheme in a single node density scenario, but also create different node density scenarios within the network. Consider the radio range to be 550 meters and use a random waypoint mobility model in the simulation. Table 4 mentions the remaining parameters.

Table 3: Simulation Parameters

Parameter	Value
Simulator	NS-2
MAC Protocol	IEEE 802.11a
Routing Protocol	AODV
Attack Type	Sybil
Security Type	CLS, DITS
Network Size (m3)	1100 X 1100 m^2
Mobility Model	Random Way Point
Number of Nodes	25, 50, 100, 150
Speed of Nodes (m/s)	Random
Communication Ranges (m)	550m
Simulation Time (s)	200

7 Result Analysis

In this section mention the result analysis of CLS and DITS.

7.1 Packets Receiving Analysis

In the VANET, the dissemination of traffic information among vehicles is crucial, as most vehicles ultimately determine their routes based on the information they receive.

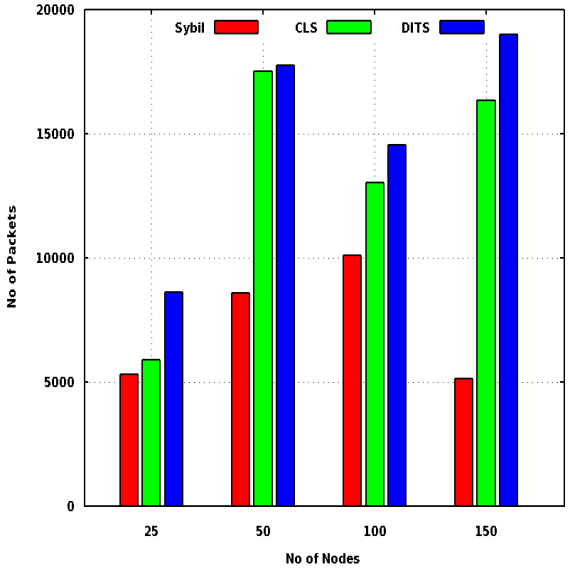


Figure 2 Packets Receiving Analysis

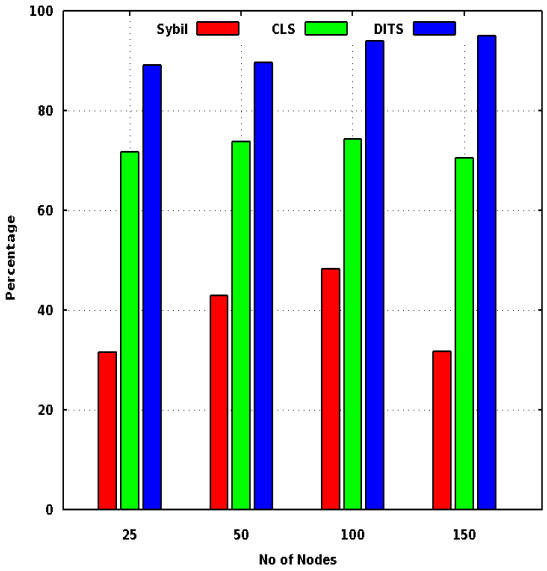


Figure 3 Data Receiving Percentage Analysis

If the network drops data packets and fails to properly receive traffic information, it necessitates retransmitting the information. When the Sybil attacker was present, the majority of the dropped data packets and traffic mismanagement incidents occurred on the roads. In figure 2, compare the packet receiving performance between the CLS and DITS schemes in VANET. In all vehicle scenarios, DITS receives more packets than CTS. The trust-based scheme is not only improving the routing performance but also completely disabling the Sybil attacker's malicious activities in the network.

7.2 Percentage of Data Receiving

The packet's receiving percentage is the ratio of packets received and packets sent in the network. In the presence of a Sybil attacker, if the data packets dropped in the network and traffic information was not

forwarded properly, it means to transmit the traffic information again in the network. In the presence of. In this figure 3, compare the packets receiving percentage performance between the CLS and DITS scheme in VANET. In all vehicle scenarios, the packet receiving percentage of DITS is higher than that of CTS. This is really surprising that the packets receiving percentage is about 10% more (minimum) in all the scenarios. The trust-based scheme is not only improving the routing performance but also improving the routing performance of the network and providing the attacker-free environment in the network.

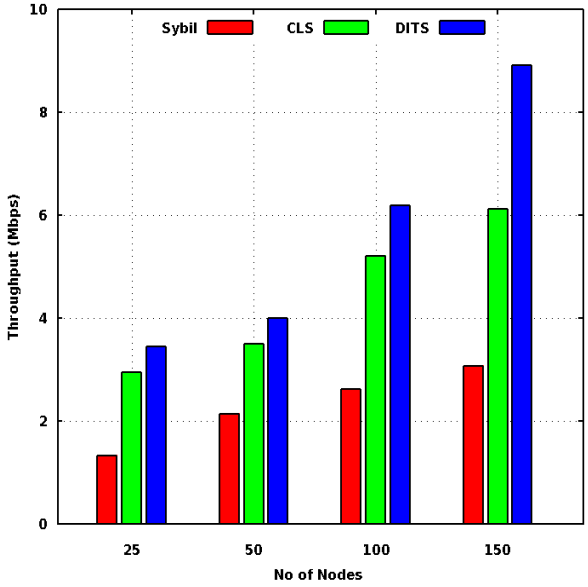
7.3 Throughput Analysis

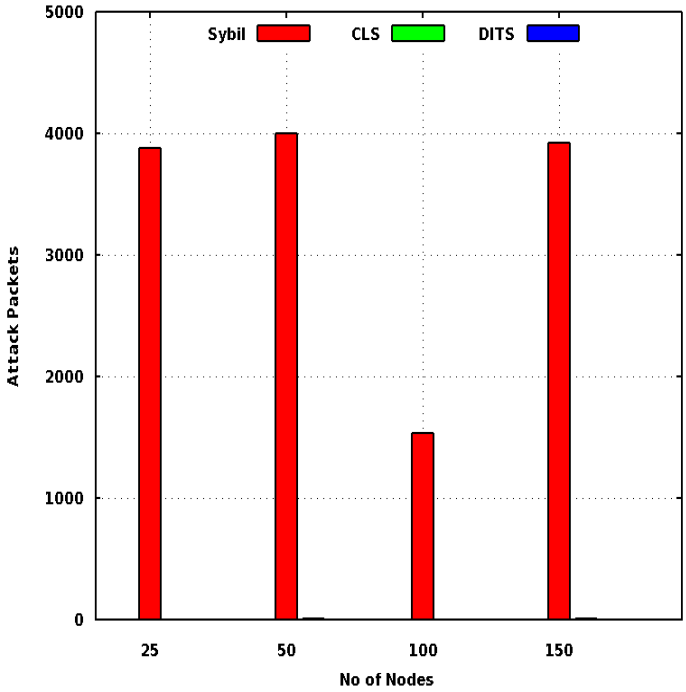
In throughput performance measure the how much megabits per second (Mbps) received at destination in sybil attacker module, CLS module and proposed DITS module. In a network, the source is the generator, and the destination is the final accepter. In the figure 4, measure the throughput performance of CLS and DITS, and the performance of DITS is better because there are fewer packet drops in the network. In the proposed DITS approach, the sender establishes a reliable link and controls data readmission. In the DITS, the maximum throughput performance exceeds 8.5 Mbps, whereas the CLS only achieves a performance of 6 Mbps for a capacity of 150 vehicles. In all other scenarios, the performance of the proposed approach is superior. The network can also facilitate the proper forwarding of traffic information and enable quick responses from vehicles.

7.4 Packets Infected by Sybil Attack

Sybil attacker vehicles are stealing the identities of other vehicles and dropping all the traffic information packets in the network. The source or trailing vehicles forward the request for traffic information, and the destination or leading vehicles accept the traffic information to make further decisions on the roads. The source vehicle normally establishes the connection for traffic information forwarding. In the figure 5, only the information packets dropping due to the presence of the attacker are mentioned, and negligible packets also dropped by the attacker in the presence of the CLS approach. Meanwhile, the CTS approach is secure but not fully secure. The attacker infection or dropping percentage in the presence of DITS is zero percent in the network, i.e., equivalent to the normal vehicular communication.

Figure 4: Throughput AnalysisFigure 5: Packets Infection Analysis





7.5 Rouitng Overhead Performance Analysis

Routing overhead means lots of extra packets flooding in the network for connection establishment, warning related to congestion, collision, and acknowledgement retransmission, etc. The overhead is definitely more noticeable in the presence of an attacker because of the retransmission of data in the network. Figure 6 shows the overhead performance of CLS and DITS in 25, 50, 100, and 150 vehicles. The proposed trust-based approach is very reliable, and attacker infection is almost zero in the network. We measured the overhead of the proposed scheme in 150 vehicles and found it to be no more than 2.4 in the network, while we measured the CLS performance at 3.20 in the same vehicles. High overhead indicates increased link breakage and unsatisfactory packet reception. In the presence of DITS, the overhead is normal and indicates improved packet forwarding of traffic information in the network.

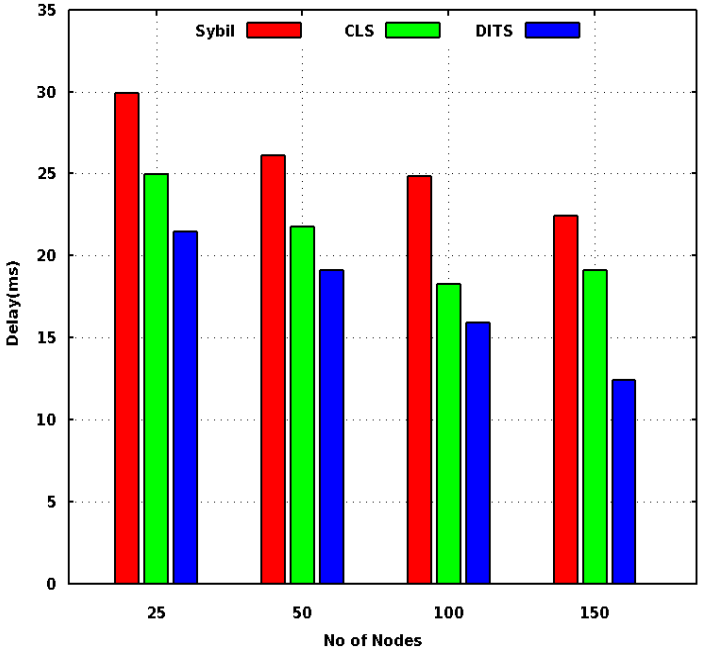


Figure 6: Routing Overhead Analysis

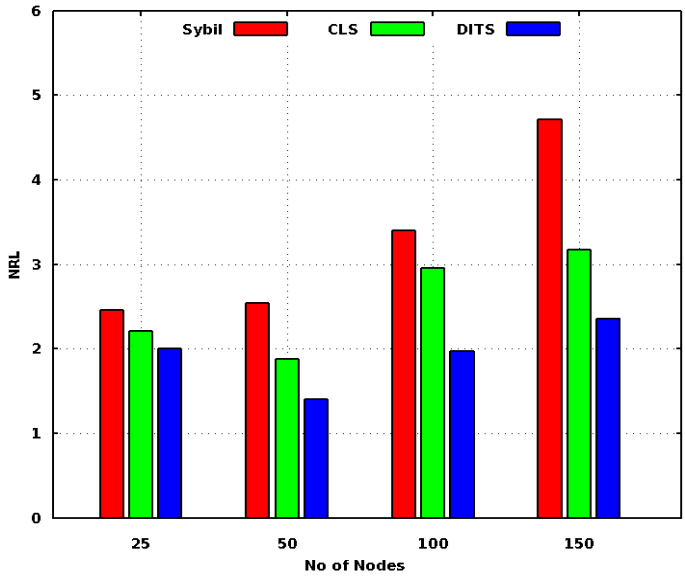


Figure 7 Delay Analysis

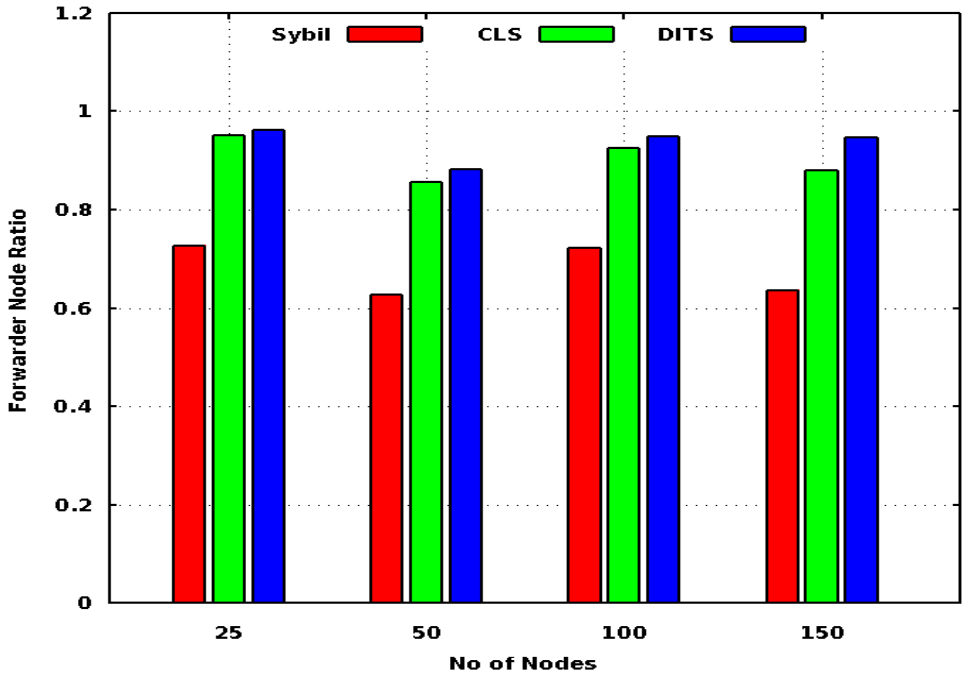
7.6 Delay Performance Analysis

The delay performance metrics evaluate the extra time the receiver takes during traffic information forwarding. The delay is undoubtedly caused by a Sybil attacker, particularly when large packets drop data in the network. The slow movement of vehicles on the roads contributes to the delay caused by heavy traffic. The same applies to heavy packet traffic, which causes a delay in communication between the sender and the receiver. The figure 7 shows the delay performance of CLS and DITS for 25, 50, 100, and 150 vehicles. The delay of the proposed scheme is not more than 12.4 ms in the network, which is measured in 150 vehicles density, but the CLS performance is measured at 19.10 ms in 150 vehicles. The delay is more than 5.50 ms. The high delay indicates that the network is experiencing heavy traffic and that an attacker is continuously dropping packets. The delay in the presence of DITS is normal because there are fewer link breakages, which leads to a gradual decrease in the network delay.

7.7 Forwarder Node Ratio

The sender node sends the data, and the receiver node accepts it in the network. Forwarding the same data to other nodes or destinations makes the intermediate node more responsive. The forwarder node possesses a limited buffer space for storing data packets. In this figure 8, measure the forwarding node ratio performance in different vehicle densities. The performance of DITS is improving, and vehicles are forwarding a significant number of packets to others in order to transfer valuable traffic information. If the sender sends data frequently, then intermediate vehicles will forward it to other vehicles. In a density of 150 vehicles, the data forwarding of DITS is 1.2% higher than that of CLS. When a Sybil attacker is present, only few vehicles forwarding the data and because of that data loss increases significantly.

Figure 8 Forwarder Node Ratio Analysis



.

8. Conclusion and Future Work

Vehicular Ad hoc Network (VANET) is not perfectly implemented in many countries due to the absence of advanced infrastructure. This type of transport system is very effective to control the traffic on roads or handle the traffic on many busy roads. In VANET, Intelligent Transport System (ITS) and RSUs playing the important role in vehicles communication. The direct trust calculation is completely based on the queue delay, processing capability and forwarding nodes. While indirect trust based on previous performance of nodes or vehicles. Using trust metrics that are generated from behavior analysis and past interactions, the proposed DITS method is able to discern between legitimate and malicious nodes in an efficient manner. The packet dropping is minimum and DITS is showing 3% improvement in packets receiving (measuring only packets receiving). The packet's receiving percentage (ratio of received and send) is 15% more as compared to previous CLS approach. While the overhead and delay are also showing 5% decrement in performance. The performance of DITS and CLS is evaluated in different vehicles density scenario and in all setup, DITS is showing better performance. The Sybil attacker infection is zero in presence of DITS approach in VANET. The findings of the simulation demonstrate the robustness of the approach, with excellent detection accuracy and improve proper traffic status information forwarding in network. By placing an emphasis on scalability and adaptability. The DITS demonstrates that it is well-suited for deployments in the actual world of VANETs, thereby paving the way for vehicular communication systems that are inherently more secure and dependable.

The ITS or RSUs both are required identity in VANET for attacker detection. Attacker detection on multiple layers is very complex. So, in future , it may be possible to concentrate on integrating the scheme with more sophisticated cryptographic approaches and investigating its performance in ITS systems that are more complicated and multi-layered.

References

1. PavithraT, Nagabhushana B.S , "A Survey on Security in VANETs," IEEE Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020, pp. 881-889
2. Soujanya B K and Azam F, "Ensuring Security and Privacy in VANET: A Comprehensive Survey of Authentication Approaches," Wiley, Journal of Computer Networks and Communications, 2024 pp. 1-32.
3. Chandravanshi K, Soni G., Mishra K., Jain G., Mishra, D.K., Tesfay, "Warning Message Broadcasting Through RSU for Real Road Map Profile in VANET," Conference paper, Data Science and Big Data Analytics (IDBA 2023), 17 March 2024, pp 365–376.
4. [Azees M., Vijayakumar P., DeborahL. J., "Comprehensive Survey On Security Services in Vehicular Ad-Hoc Networks," IET Intelligent Transport System, 10 (6), pp. 379–388, 2016.
5. Jiang D., Delgrossi L., "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in Proceeding of IEEE Vehicular Technology Conference (VTC Spring), May 2008, pp. 2036–2040.
6. Memon I., "A Secure and Efficient Communication Scheme with Authenticated key Establishment Protocol for Road Networks," Wireless Personal Communications, 2015, 85, pp. 1167-1191.
7. Hu H., Lu R., Zhang Z., Shao. J, "REPLACE: A Reliable Trust-based Platoon Service Recommendation Scheme in VANET", IEEE Transactions on Vehicular Technology , 2017, 66 (2) , pp.1786 - 1797.
8. Soni G., Chandravanshi K., JhariyaM. K., Rajput A., "An IPS Approach to Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET, First International Conference on Communication, Cloud, and Big Data (CCB), 2020, pp.1-8.
9. Quyoom A., Mir A.A., Sarwar A. "Security Attacks and Challenges of VANETs : A Literature Survey," Journal of Multimedia Information System 7(1), 2020, pp. 45-54.
10. Dutta A., SamaniegoL. M., Campoverde M. Tropea, F.D. Rango, "A Comprehensive Review of Recent Developments in VANET for Traffic, Safety & Remote Monitoring Applications," Journal of Network and Systems Management, Vol.32 (73), 2024, pp.1-37.
11. Hartenstein H., LanerteauxK. P "A Tutorial on Vehicular Ad Hoc Networks," IEEE Communication Magazine, 2008, pp. 164-171.
12. Bhoi S.K, Khilar P.M., "Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS Services," International conference on Communication and Signal Processing, 2013, pp.1170-1174.
13. Marvy B. Mansour, Cherif Salama, Hoda K. Mohamed, Sherif A. Hammad, "VANET Security and Privacy – An Overview," International Journal of Network Security & Its Applications (IJNSA), pp. 13-34, 2018, 10(2),
14. Soni G., Chandrawanshi K., "A Multipath Location based Hybrid DMR Protocol in MANET," IEEE 3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE), pp. 1-6,2020.
15. Kamboj S. Mann K. S., Kaur S., "An Optimized Multiple Malicious Node Detection method for detection of security attacks in VANETs," 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST), Mohali, India, 2021, pp. 152-157.
16. Soni G., Chandravanshi K,Kaurav A.S., Dutta S.R., "A Bandwidth-Efficient and Quick Response Traffic Congestion Control QoS Approach for VANET in 6G," Springer Conference on Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, 2022, 385, pp. 1-9.

17. Chandravanshi K., Soni G., Mishra, D.K., "Design and Analysis of an Energy-Efficient Load Balancing and Bandwidth Aware Adaptive Multipath N-Channel Routing Approach in MANET," IEEE Access, 10, 2022, pp. 110003 – 110025.
18. Nadia T.,Mourad M., Hamouma M., Hamoudi.K."A Survey on Vehicular Ad-hoc Networks Routing Protocols: Classification and Challenges," Journal of Digital Information Management, 2019, 17(4), pp. 227–244.
19. Slama A., Lengliz I., "Survey on Secure Routing In VANETs," International Journal of Network Security & Its Applications (IJNSA) Vol. 11(3), May 2019.
20. Mokhtar B., Azab M., Survey on Security Issues in Vehicular Ad Hoc Networks," Alexandria Engineering Journal, 2015, 54(4), pp.1115-1126.
21. Samara G., Al-Salihy W.A., Sures R., "Security analysis of vehicular Ad Hoc Networks (VANET)," IEEE Second International Conference on Network Applications, Protocols and Services, 2010, pp. 55–60.
22. Zhang Z., Lai Y., Chen Y., Wei J., Wang Y., "Detection Method to Eliminate Sybil attacks in Vehicular Ad-hoc Networks, Ad Hoc Networks, 2023, 141(15), pp.1-10.
23. Sultana R, Grover J, Meenakshi Tripathi, Manhar Singh Sachdev, Sparsh Taneja, "Detecting Sybil Attacks in VANET: Exploring Feature Diversity and Deep Learning Algorithms with Insights into Sybil Node Associations," Journal of Network and Systems Management, Volume 32 (3), May 2024.
24. Mangla C., Rani S., Herencsar N., "Misbehavior Detection Framework for Cooperative Intelligent Transport Systems ISA Transaction, Vol.132 pp. 52-60, 2023.
25. Yu B., Xu C.Z., Xiao, B., "Detecting Sybil attacks in VANETs," Journal of Parallel and Distributed Computing, Vol.73(6), pp.746-756, 2013.
26. Soni G., Chandrawanshi K., "A Novel Defence Scheme Against Selfish Node Attack in MANET," International Journal on Computational Sciences & Applications (IJCSA), 2013, 3 (3), pp. 51-63.
27. Verma R, Soni G., Sahu S, Chandrawanshi K., "Security Issues, and Requirements, Challenges," Blockchain Technology for IoE: Security and Privacy Perspectives, CRC Press, pp.21-40, 2023.
28. KauravA. S., DuttaS. R, "Detection and Prevention from Different Attacks in VANET: A Survey," Journal of Physics: Conference Series, 2021, 2040 (1), pp. 1-10.
29. MejriM. N., Othman J.B., Hamdi M., "Survey on VANET Security Challenges and Possible Cryptographic Solutions," Vehicular Communication., 2014, 1 (2), pp. 53–66.
30. Engoulou R.G., Bellaïche M., Pierre S., Quintero A., "VANET Security Surveys," Computer Communications, Vol .44(15), pp. 1-13, 2013.
31. Sakiz F., Sen S.,"A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV," Ad Hoc Networks, 2017, 61, pp. 33-50.
32. Nandy T., Noor R.M., Kolandaisamy R., IdrisM.Y.I., Bhattacharyya, S. "A Review of Security Attacks and Intrusion Detection in the Vehicular Networks," Journal of King Saud University - Computer and Information Sciences, 2024, 36(2), pp. 1-22, 2024.
33. Zhu Y.,Zeng J., Weng F., Han D., Yang Y., Li X., Zhang Y., "Sybil Attacks Detection and Traceability Mechanism Based on Beacon Packets in Connected Automobile Vehicles," Sensors, 2024, 24(7), pp1-26.

34. MathurS. M., Gupta R., "Identity Spoofing Sybil Attack Protective Measures using Physical & Logical Address Mapping for the VANET (ISPLM)," International Journal of Intelligent Systems and Applications in Engineering (IJISAE),2014, 12(19) pp.638-646.
35. Masood S., Saeed Y., Ali A., Jamil H., SameeN. A., Alamro H.,, Ali MuthannaM. S., A. Khakimov "Detecting and Preventing False Nodes and Messages in Vehicular Ad-Hoc Networking (VANET)," IEEE Access, 2023, Vol. 11, pp. 93920-93934.
36. Azam S., Bibi M., Riaz R., Rizvi S.S., Kwon S.J., "Collaborative Learning Based Sybil Attack Detection in Vehicular AD-HOC Networks (VANETS)," Sensors, MDPI, 22(18)2022, pp. 1-17..
37. Carlos H. O. O. Quevedo, Ana M. B. C. Quevedo, Gustavo A. Campos, Rafael L. Gomes, Joaquim Celestino, Ahmed Serhrouchn, "An Intelligent Mechanism for Sybil Attacks Detection in VANETs", IEEE International Conference on Communications (ICC), 2020.
38. Kaurav A.K, Srinivas K., "A Comprehensive Verification of the Header Format and Bandwidth Utilization to Detect Distributed Denial of Service Attack in Vehicular Ad hoc Network International Journal of Electrical and Computer Engineering (IJECE), 2014,14 (6), pp. 6538-5550.
39. Soni G., Chandravanshi K., "A Novel Privacy-Preserving and Denser Traffic Management System in 6G-VANET Routing Against Blackhole Attack," Sustainable Communication Networks and Application, 2022, pp. 649-663.
40. Nisara K., Mu'azubA. A.,. Lawalc I.A., Khand S., Memon S., "Reliable Priority Based QoS Real-Time Traffic Routing in VANET: Open Issues & Parameter," IEEE 14th International Conference on Application of Information and Communication Technologies (AICT), 2020.