Sigma J Eng Nat Sci, Vol. 44, No. 2, pp. 983–993, April, 2026

Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2026.2020

Research Article

Investigating the effectiveness of IS-DOS prevention mechanisms for mitigating DOS attacks in VANET

Harsh Pratap SINGH[1], Nagendra SINGH[2,*], Sai Kiran Naik BANOTH[3], Vedika PATIL[4], Neha ARYA[5], Neeraj SHRIVASTAVA[6]

[1]Department of Computer Science Engineering, Medicaps University, Indore, 453331, India
[2]Department of Electrical Engineering, Trinity College of Engineering & Technology, Karimnagar, 505001, India
[3]Technical Lead at Fannie Mae, 20005, USA
[4]Department of Computer Engineering, KC College of Engineering and Management Studies and Research, Thane, 400603, India
[5]Department of Electronic and Instrumentation, Shri Govindram Seksaria, Institute of Technology and Science, Indore, 452003, India
[6]Department of Electrical Engineering, Medicaps University, Indore, 45333, India

ARTICLE INFO

Article history
Received: 10 February 2025
Revised: 13 April 2025
Accepted: 15 June 2025

Keywords:
Vehicular Networks; Mobile Ad-hoc Network; Routing Load; Black Hole; Security Threat; Ad Hoc On-Demand Distance Vector; IS-DoS (Improved Security in Denial of Service).

ABSTRACT

Ensuring secure and reliable communication in vehicular networks, a type of mobile ad hoc network is a major challenge due to the frequently changing topology. The dynamic nature of VANETs, where nodes can frequently join or leave the network, can lead to insecure communication and link disconnections caused by obstructions such as buildings, tunnels, bridges, and fossils. Disconnections can cause packet loss and negatively impact network performance. It is often difficult to determine the reason behind packet loss, whether it is due to node detection or security threats. VANETs are vulnerable to various attacks, including denial-of-service, black hole, and greyhole attacks. This study focuses on mitigating DoS flooding attacks to enhance network safety and efficiency of VANET communication. In this work, we propose a novel intrusion detection algorithm IS-DOS, which may help effectively identify and prevent DOS flooding attacks by leveraging the traffic pattern analysis with the AODV routing protocol framework. To evaluate the effectiveness of the proposed approach, use network simulator NS 2.34 for the conventional DOS, QRT-DOS and our proposed model IS-DOS. The quantitative performance metrics such as packet delivery ratio, throughput, end-to end delay, and routing overhead were analyzed under various network conditions. The simulation results demonstrated that IS-DOS improves the packet delivery ratio by 15% and throughput by 12% compared to existing DOS and QRT-DOS mitigation approach. Moreover, IS-DoS diminishes average packet delay by 20% and drops routing overhead by 18%, signifying enhanced network efficiency and resilience. These findings recommend that IS-DoS not solitary mitigates flooding attacks more effectually than prior approaches but also sustains network stability in the existence of high mobility and recurrent topology changes. The novelty of this work deceits in its adaptive detection mechanism tailored for VANET surroundings, which develop beyond existing solutions by suggesting real-time, low-overhead attack anticipation without

***Corresponding author.**
*E-mail address: ernsingh007@gmail.com

This paper was recommended for publication in revised form by Editor-in-Chief Ahmet Selim Dalkilic

Published by Yıldız Technical University Press, İstanbul, Turkey

compromising normal network operations. This research contributes to improving the security and reliability of vehicular communications, which is indispensable for the prevalent adoption of intelligent transportation systems.

Cite this article as: Singh HP, Singh N, Banoth SKN, Patil V, Arya N, Shrivastava N. Investigating the effectiveness of IS-DOS prevention mechanisms for mitigating DOS attacks in vanet. Sigma J Eng Nat Sci 2026;44(2):983–993.

INTRODUCTION

The growing global demand for transportation, fueled by rapid urbanization and population growth, has spurred the advancement of intelligent and secure vehicular communication systems [1]. These systems rely on communication tools and internet services and can be based on dynamic wireless networks, static wired networks, or hybrid networks. While static infrastructure networks present many challenges, such as cell sites, access points, and physical and digital cables, wireless networks are easier to establish and maintain [2,3]. Vehicular Ad Hoc Networks (VANETs) ... have emerged as a pivotal component in modern Intelligent Transportation Systems (ITS). Contributing significantly to road safety, traffic management, and infotainment services. Additionally, they allow for seamless integration with the Intelligent Transport System and testing of the latest developments in smart car networks [4].

These advancements are expected to revolutionize the driving experience and characteristics and improve the safety of vehicles on highways and in cities. However, the open literature extensively explores. A critical challenge remains unresolved: maintaining secure and reliable communication under conditions of high mobility and frequent topological changes [5,6].

In order to ensure the safety of VANET communications, previous research has proposed various techniques based on the measures of cryptography and trust such as digital certificates, Public Key Infrastructure (PKI), and trust models [7-9]. Whereas these techniques are providing some degree of security, they are often ineffective in high speed scenarios, or when the adversaries are involved, and immediate trust checking along with low latency reaction is necessary. One of the major unexplored issues on this area is how the network can be exploited by Distributed Denial of Service (DoS) attacks, especially the flooding-based DoS attacks, which interfere with the network performance due to overloading of routing protocols. Such attacks can severely disrupt service, result in delays and loss of packets particularly in the busy urban environment. Moreover, as VANET connections are temporary, even now it is not easy to differentiate malicious behavior and usual disconnection [10,11].

This work suggests IS-DoS (Intelligent Suppression of DoS Flooding Attacks), a novel security approach created especially for dynamic vehicle situations, to fill these shortcomings. By employing behavior-based traffic pattern analysis to identify and prevent DoS flooding attacks instead of just cryptographic techniques, the suggested methodology improves VANET's security. Its capacity to function in real-time, adjust to changing network conditions, and reduce detection overhead is what makes it innovative. Additionally, this work presents an RSU-based addition that makes it possible for roadside units to efficiently monitor and react to unusual traffic patterns. We use the suggested IS-DoS method over the AODV routing protocol and test it with the NS-2.34 simulator. The algorithm is evaluated in comparison to the baseline. Using performance indicators including throughput, end-to-end latency, routing overhead, and packet delivery ratio (PDR), DoS and QRT-DoS techniques.

In summary, the novelty of this study lies in its development of a lightweight, real-time DoS mitigation strategy tailored for VANET environments. Unlike conventional cryptographic defenses, IS-DoS provides a proactive and scalable approach that improves both security and network efficiency under high-mobility conditions. Section II of the article presents a comprehensive review of related work on improving the safety and efficiency of VANETs. Section III describes our proposed algorithm for detecting DoS flood attacks in VANETs. Section IV presents the experiment setup and analysis of the results, while the conclusions of the proposed work are mentioned in Section V.

RELATED WORK

A method for detecting DDoS attacks that makes use of big data technology is presented in Article [1]. It uses Apache Spark to process massive amounts of traffic and HDFS to store important suspicious info [2]. We employ a micro-batch data processing methodology to enable real-time traffic gathering [3], and we analyse the acquired traffic using a Random Forest (RF) classifier. The NSL-KDD and UNSW-NB15 datasets were used to validate the suggested method, which produced remarkable detection accuracies of 99.95% and 98.75%, respectively [4].

To enable robust broadcasting on VANETs, a unique method for choosing multipoint relay (MPR) schemes is proposed in [5, 6]. It is an optimisation of the relay selection technique that utilises a weak 2-hop set of MPR nodes by considering each 2-hop node multiple times. The Fuzzy Cluster Management System forms vehicle clusters on VANETs based on two fuzzy models of FCMS1 and FCMS2. Article [7] introduces FCMS1 that takes into consideration the input characteristics in the form of vehicle centrality,

security, cluster affiliation, and relative speed in predicting the likelihood of vehicle remaining within a cluster.

The authors of [8] present a multivariate stream analysis method of detecting and evaluating the DDoS attacks on VANETs. To achieve more accuracy in making a detection, the technique considers the traffic in different time periods and conditions, and applies specific rules to the different traffic types. Article [9] presents ID-MAP, a special identity authentication method that exploits proxy vehicles and encrypting messages using elliptic curve that operates under the random oracle model to achieve message authenticity and to avoid forgery[10].

Article [11] introduces a non-parametric statistical method of detecting low-rate DDoS attacks in intelligent transportation systems. This method beat two parametric models in terms of average detection delay and false alarm rate when tested with the Simulation of Urban Mobility tool [12]. In [13], a Quick Response Table (QRT)-based secure routing strategy that logs route data and highlights unknown anomalies is described. According to the simulation data QRT can improve throughput, packet delivery

Table 1. Comparison table of existing literature

Article/Reference number	Technique/approach	Key results/findings	Comparison with proposed work
[1]	DoS attack prevention using general VANET routing security	Proposed heuristic method for general DoS prevention	Lacks big data scalability or ML accuracy used in proposed method
[2]	Apache Spark-based DDoS detection	Real-time mitigation architecture using Spark	Similar big data tech but lacks comparative ML evaluation
[4]	Distributed NIDS using RF classifier	Accuracy: 99.95% (NSL-KDD), 98.75% (UNSW)	Comparable to proposed method; confirms efficacy of RF on same datasets
[5,6]	IEEE 802.11p DoS detection, Secure auth	Real-time relay strategy for VANETs	Different layer focus (MAC/ authentication); does not include big data or ML models
[8]	Trust framework (TEAM)	Uses multivariate stream analysis	Focused on trust, not suitable for scalable DDoS
[9,10]	Fuzzy cluster-based MPR with trust/security	Improves clustering efficiency and relay trust	Complementary to our traffic-level detection but not core to DDoS prevention
[11]	Statistical low-rate DDoS detection	Reduced false positives, better avg. detection time	Doesn't scale to high-speed traffic as in Spark+RF architecture
[13]	Anonymous auth + privacy	Improved security + low overhead	Auth-layer focus; doesn't handle DDoS on transport/network layers
[17,18]	P-Secure proactive DoS detection	Improved delay, throughput	Suitable for DoS but lacks real-time big data handling or accuracy benchmarks
[22]	IDoS-CC (intelligent DDoS + congestion control)	Real-time congestion-aware DDoS detection	Comparable but lacks ML accuracy and dataset validation
[23]	Puzzle-based co-auth	Prevents DoS via pseudonym attack resistance	Authentication-level focus only
[24]	Fuzzy logic + fog-based 5G VANET detection	Effective at edge-layer DDoS detection	Similar but doesn't benchmark with standard datasets
[26]	ML-MDS using SVM, DT, etc.	Accuracy improved across classifiers	Proposed RF model performs better and is validated with two datasets
[27]	ML in SDN-WISE IoT	Reliable for SDN-based DDoS detection	Limited to SDN-IoT; doesn't address VANET big-data challenges
[29]	ML-based intrusion detection with RF	Multi-level IDS improved detection	Similar ML basis but proposed method uses big data + real datasets
[31]	Hybrid LogitBoost prediction model	Improved DDoS resilience	Uses hybrid model but lacks real-time big data validation
[35]	Real-time multi-stage IDS	Low false alarm rate, multi-stage detection	Aligns with proposed goal but lacks performance metrics on benchmark datasets

rate (PDR) and reduce routing load and delay in mitigating DoS attacks[14,15].

Article [16] recommends the use of an anonymous authentication procedure that allows tracking the entry of entities and ensures privacy to prevent the introduction of hostile vehicles. Article [17,18] presents the P-Secure method of proactive DoS attack detection that reduces the processing overhead in the system and enhances its network performance. Simulation results show that P-Secure is more effective in packet delivery ratio, delay, and data transfer rate compared to OBU-based VANET models.

Article [19] emphasises the necessity of strong management techniques to guarantee safe VANET connectivity. In [20], we introduce a node reliability strategy and local route redesign procedures to handle route creation collisions. To prevent serious accidents, a crash prevention protocol for vehicular networks is put forth in [21]. It consists of intelligent, roadside, and sensor devices.

The goal of the IDoS-CC strategy put forth in [22] is to identify DoS attacks and manage congestion. To prevent DoS attacks that target pseudonymous authentication, Article [23] proposes a co-authentication method that uses a hash puzzle system. For 5G-enabled smart cities, [24] proposes a fog-based DDoS detection method, based on fuzzy logic, to distinguish between malicious and genuine communication.

To solve scalability issues in SDNs, a lightweight framework for DoS detection and mitigation were presented in [25]. Using the UNSW_NB-15 dataset, Article [26] looks at the ML-MDS model by sorting vehicular traffic with methods like logistic regression, decision trees, SVMs, and neural networks. In [27], a machine learning-based technique in the SDN-WISE IoT controller uses a specialized testing environment to identify DDoS attacks. Article [28] adds to the research by proposing a way to find low-rate and hidden DDoS attacks through communication between the SDN controller and the system that helps to reduce the attacks.

Article [29] presents a machine learning-based multilevel intrusion detection system that uses random forest for feature selection and quick correlation-based filtering. Article [30] uses the K-Means and C5.0 algorithms to investigate anomaly identification in VANETs. To improve vehicular infrastructure resistance against DDoS assaults, Article [31] suggests predictive risk evaluation using a hybrid Logit-Boost model. Article [32] presents a trust-based approach for dynamic pseudonym modifications.

To prevent impersonation, Article [33] offers a safe, effective conditional privacy-preserving authentication scheme that uses hash functions and bilinear pair cryptography. Article [34] employs random forests, and posterior detection approaches to enhance the precision of intrusion detection [35]. Lastly, a real-time multi-stage intrusion detection system (IDS) with low false-alarm rates and automatic intrusion detection capabilities for intelligent transportation systems is described in [36]. Table 1 shows a deep comarisions of the existing works.

Proposed Algorithm

This work used an IS-DoS Prevention Mechanisms approach to tackling the issue of DoS flooding attacks in vehicular networks to explore desirable flooding schemes. The objective of the proposed mechanism is to ensure secure information sharing among vehicles while addressing challenges such as delivering data correctly, selecting appropriate nodes or vehicles to transmit data to the destination, and maintaining communication among vehicles [21]. In order to achieve this, Road Side Units (RSUs) are deployed at every terminal to monitor traffic conditions and identify any misbehavior or malicious activity in the network. The approach operates in two modes: Vehicle-RSU (V to RSU) and Vehicle-Vehicle (V to V) communication [22]. The RSU acts as a communication hub between vehicles and can detect malicious nodes or vehicles, decreasing their trust value and preventing them from secure communication within the network [23].

Working steps of the proposed algorithm

The suggested approach's algorithmic steps are explained in this section. It provides a series of easy-to-follow guidelines for putting the strategy into practice and reducing DoS flooding attacks in vehicle networks. Algorithm 1 describes a protocol for secure communication in a vehicular network using road site monitoring units. It includes steps for registration, authorization, and route packet transmission while considering the range of the monitoring units.

Algorithm 1: Algorithm for authorisation and communication in vehicular networks

Input: Cr: Number of cars in the network
RSUi: Road Site Monitoring Units
DOS: Denial of Service Attack in network
CMUi: Attack control and monitoring unit ∈ RSUi
Ψ: Radio range of RSUi is 15 Km
Rp: AODV (Ad hoc On-Demand Distance Vector)
lr: Vehicle location
sr: Vehicle speed

Output: Received packet, PDR, throughput, routing overhead, delay, DOS packet detection

```
Step 1:
Ci wants to communicate with Cj
If RSUi.authorize(Ci):
Step 2:
Ci.broadcast(Rp)
    Step 3:
      If not RSUi.is_in_range(Cj):
        RSUi.broadcast_to_neighbors(RSUi.RSUj, Rp)
    Step 4:
      If RSUi.RSUj.find(Cj):
        If RSUi.RSUj.check_db(Cj):
          Step 5:
            If RSUi.RSUj.authorize(Cj):
              RSUi.RSUj.send_packet(Cj, Rp)
            Else:
              RSUi.send_feedback(Ci, "Cj is not authorized.")
```

```
            Else:
              RSUi.send_feedback(Ci, "Cj is not registered.")
            Else:
              RSUi.send_feedback(Ci, "Cj is not in range.")
          Else If RSUi.check_db(Cj):
            Step 6:
              If RSUi.authorize(Cj):
                RSUi.send_packet(Cj, Rp)
              Else:
                RSUi.send_feedback(Ci, "Cj is not authorized.")
        Else:
          RSUi.send_feedback(Ci, "Cj is not registered.")
      Else:
        RSUi.send_registration_message(Ci)
        Ci.register_to_itself()
        Ci.authorize_for_future_communication()
```

Algorithm 2 is designed to monitor real-time communications systems and detect abnormal behaviour. It analyses the communication data, decreases trust value and blocks communication if abnormal behaviour is detected.

Algorithm 2: Detecting Abnormal Behavior in Real-Time Communications SystemInputs

```
Cr: number of cars in the network
Ci: a specific car in the network
Cj: Another specific car in the network
l1: initial location of Ci
l2: destination location of Ci
Ψ: radio range of RSUi
RSUi: Road Site Monitoring Unit
CMUi: Attack control and monitoring unit
Outputs
location: real-time location of Ci
speed: speed of Ci
communication_data: communication data of Ci
behavior: behavior of Ci and Cj (normal or abnormal)
temporary_block_authorization: authorization temporary block if Ci or Cj is untrusted.
Step 1:
RSUi_sense() {
track_locations(Cr)
}
Step 2:
while (Ci travels from location l1 to l2 and Ψ is under RSUi) {
capture_data(Ci) {
location = get_location(Ci)
speed = get_speed(Ci)
communication_data = get _communication_data(Ci)
}
}
Step 3:
if (Ci communicates with Cj through RSUi) {
CMUi_on()
monitor_behavior(Ci, Cj)
}
Step 4:
if (data_not_normal(Ci) or data_not_normal(Cj)) {
behavior = analyze_behavior(Ci, Cj)
if (behavior == "abnormal") {
decrease_trust_value(Ci)
decrease_trust_value(Cj)
block_communication(Ci, Cj)
untrusted_detected()
temporary_block_authorization()
}
} else {
normal_behavior_monitored()
assist_ci_cj()
handover_communication(Ci, Cj)
}
Else {
Ci_only_travels_using_RSUi_guidelines()
provide_service_to_Ci()
}
```

Attacker Detection

Figure 1 shows the flow of security approach for detecting DoS attacks in VANETs. Detecting unwanted activity in the network is crucial for identifying malicious nodes that flood the network with false information packets and continuously drop legitimate data packets.

DOS Attack Prevention Scheme Flowchart

Figure 2 illustrates the proposed approach for identifying malicious vehicles or nodes and protecting the network against DoS attacks. When CMU messages are received, the approach blocks the malicious vehicles from selecting secure nodes for transmitting data packets and enhances the network's reliability [24-27].

EXPERIMENTAL SETUP AND RESULTS ANALYSIS

This section involves the analysis of designing and implementing experiments to test hypotheses and draw meaningful conclusions about the performance of the proposed algorithm. This process is crucial in validating the effectiveness and efficiency of the new proposed technologies.

Simulation Setup

We used the network simulator NS-2.34 to compare the suggested method with earlier studies in order to assess its quality. Data packets were routed via the AODV protocol in the simulation. Since DoS attacks have the potential to seriously hinder data packet transmission, the simulation was centered on identifying them in VANETs. The simulation was set up with 30 wireless sensor nodes/devices randomly deployed in an 1100 x 1100-meter simulation area. The physical medium used was wireless, and the nodes were allowed to move randomly during the simulation.

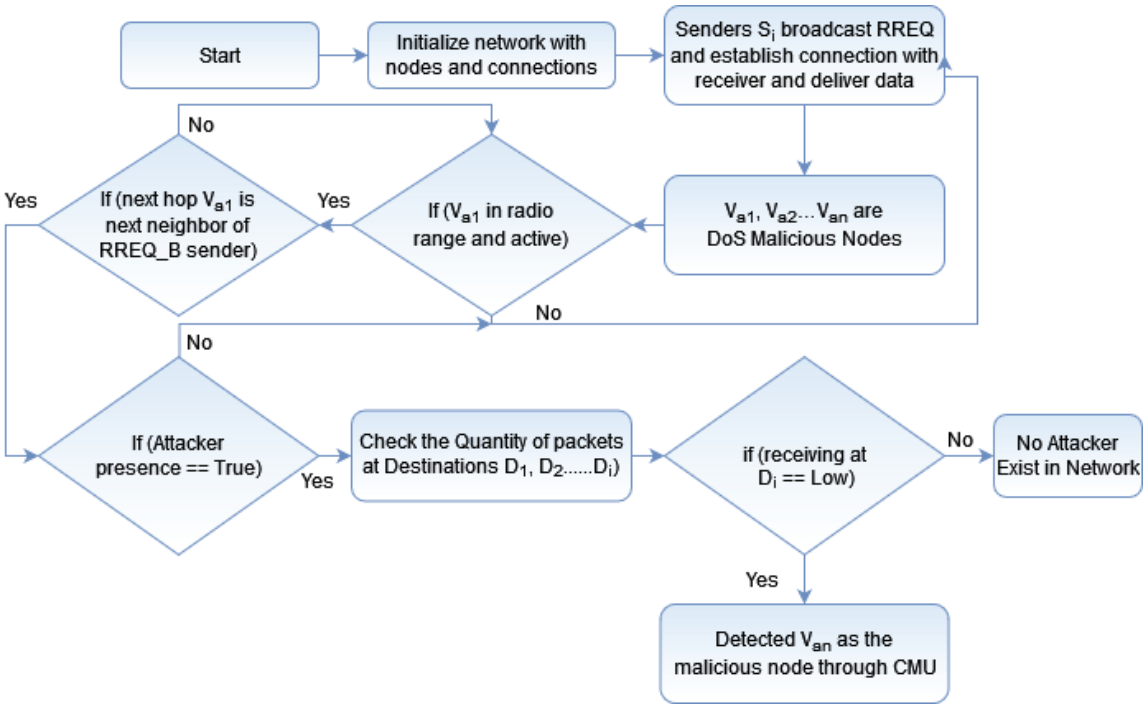

Figure 1. Attacker Detection.

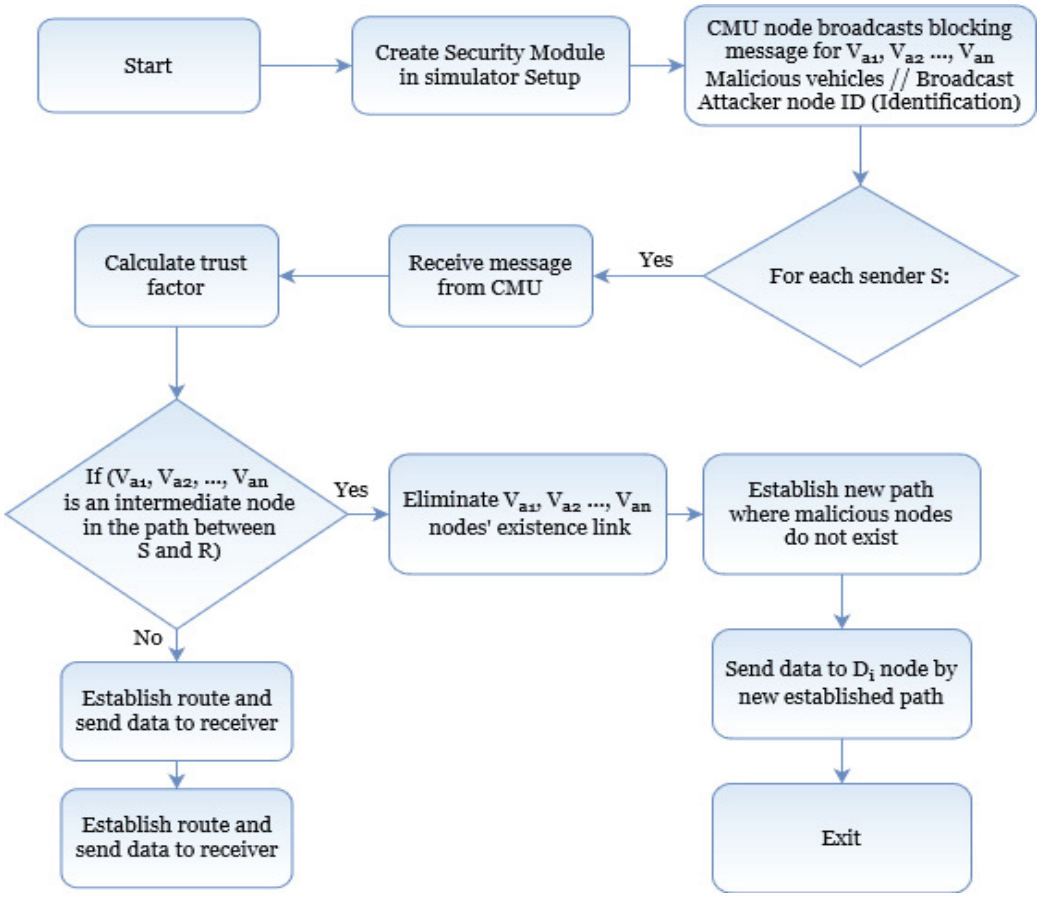

Figure 2. Prevention scheme.

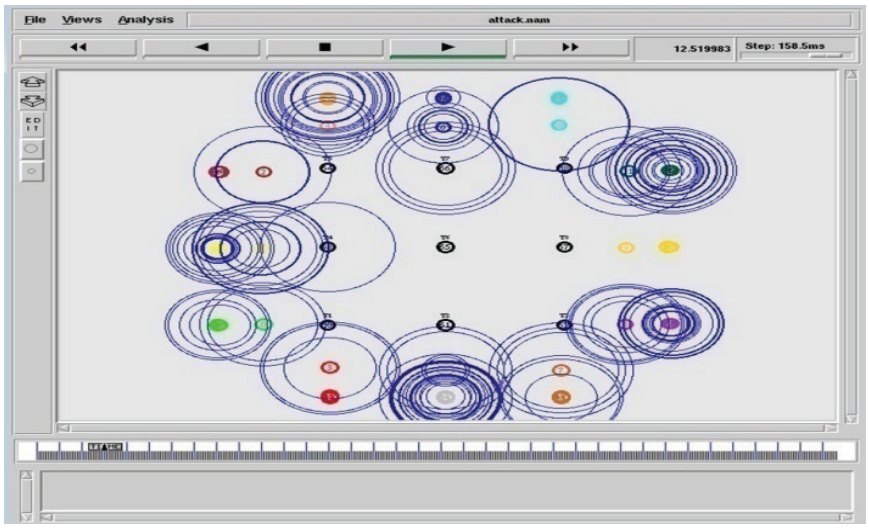

Figure 3. Dos attack prevention simulation result.

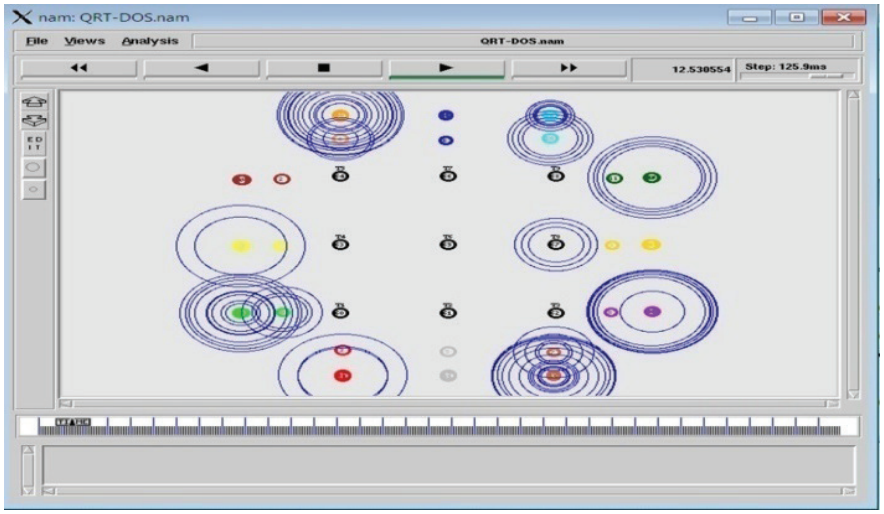

Figure 4. QRT-Dos attack prevention simulation result.

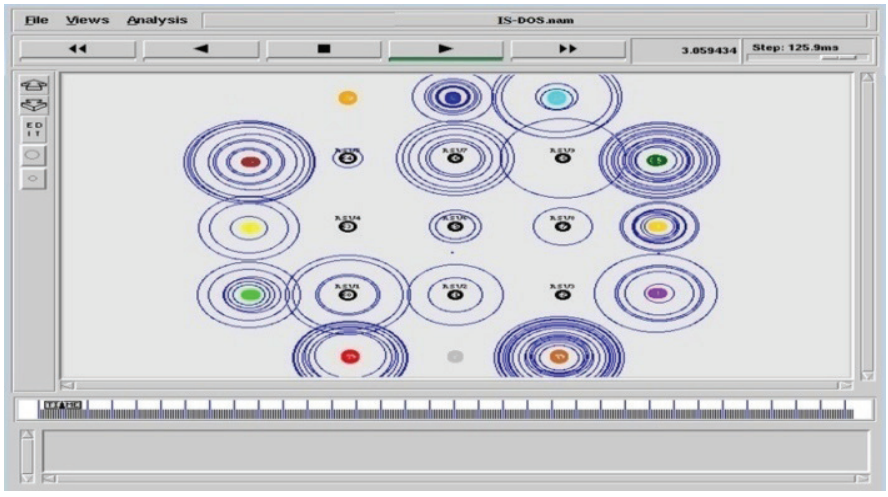

Figure 5. IS-Dos attack prevention simulation result.

The simulation results for the Dos attack prevention system are displayed in Figure 3. We simulated 300 iterations, and the queue length was set to 50. We used MAC 802.11p as the MAC layer and simulated Denial-of-Service (DoS) flooding as the attack type. We used two prevention mechanisms, QRT-DoS and IS-DoS, to prevent DoS attacks. Two different forms of traffic were used in the simulation: file transfer protocol and constant bit rate. The propagation radio model used was Two Ray Ground, and the data rate was set randomly. The QRT-Dos attack prevention system is displayed in Figure 4, and the IS-Dos attack prevention system is displayed in Figure 5.

Here it is clearly seen that the IS-Doc prevention system showing better performance compared to Dos and QRT-Dos. In the result analysis section 4.2 presented a complete comparative analysis is given between Dos, QRT-Dos and IS-Dos.

RESULTS AND DISCUSSION

The analysis involved performance evaluation of different prevention techniques.

Table 2. Simulation parameters for WSN DoS attack prevention

Parameters	Configuration Value
Simulation Area	1100 x 1100 meters
Network Type	Wireless Sensor Network (WSN)
Nodes/Devices	30
Material	Wireless
Movement of Node	Random
Number of Iteration	300
Length of Queue	50
MAC Layer	MAC 802.11p
Type of Attack	DoS flooding
Type of Prevention	QRT-DoS, IS-DoS
Type of Traffic	Constant Bit Rate, File Transfer Protocol
Propagation Radio Model	Two Ray Ground
Rate	Random

Packet Sends Analysis

Figure 6 displays the packet send analysis results for the suggested method. The analysis revealed that the proposed approach with the QRT-DoS prevention mechanism resulted in fewer packets being sent than the IS-DoS prevention mechanism when a DoS flooding attack was present in the VANET. Figure 6 illustrates how the suggested IS-DOS technique works to improve performance by preventing attacker flooding in the VANET. The different simulation parameters for preventing WSN DoS attacks are displayed in Table 2.

Analysis of Packet Receive

The impact of DoS flooding attacks on packet receive analysis is shown in Figure 7. The DoS attacker is very harmful forthe network because those vehicles that are in the range of attackersandthusattackers are directly or indirectly flooded flooding with fake message to all nearby nodes in the network. The fake packets are flooded by attacker node/s and the attacker is actually flooded with unwanted packets and drops in whole data packets. In the presence of DoS flooding attacks in VANET, the packet receive analysis with QRT-Dos was lower than that of the Improved Security (IS-dos) Approach. The attacker dropped data in the network but the proposed IS-DOS is stopping its malicious activities.

Throughput Analysis

The effects of the DoS flooding attack on the network's throughput were analyzed, and the results are presented in Figure 8. It is observed that the output of the QRT prevention mechanism is lower compared to the Improved Security (IS) approach when a DoS flooding attack is present in the vehicular network

Packet Drop Analysis

Figure 9 illustrates how DoS flooding attacks affect the AODV routing protocol's packet drop analysis. In the VANET, packet drop happens as a result of increased network traffic. The findings indicate that when DoS attacks

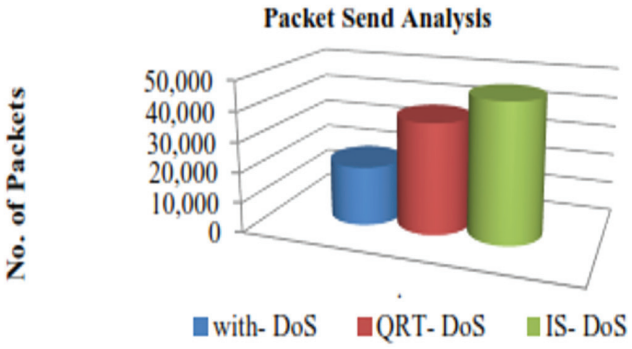

Figure 6. Packet send analysis using AODV protocol in VANET.

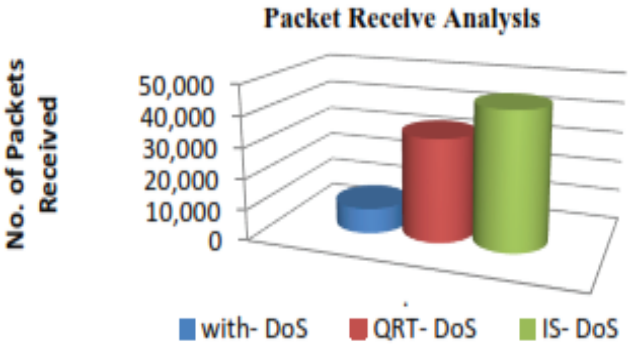

Figure 7. Packet Receive Analysis using AODV protocol in VANET.

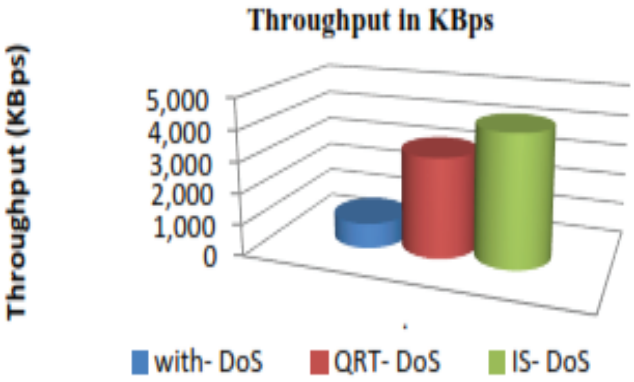

Figure 8. Throughput Analysis using AODV protocol in VANET.

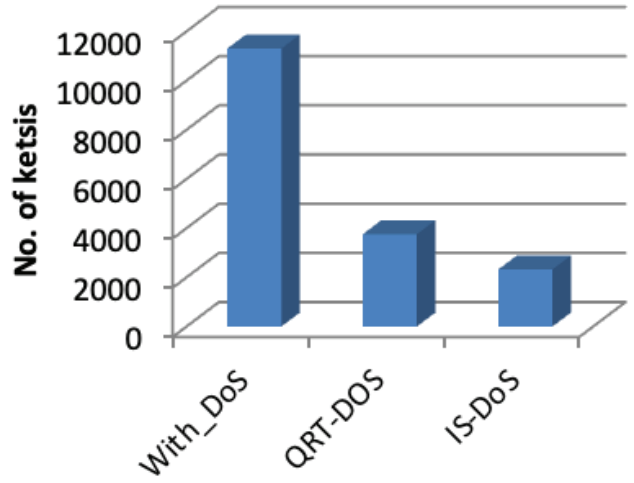

Figure 9. Packet drop analysis between proposed and existing techniques.

are present in the vehicular network, the packet drop analysis using QRT is higher than the Improved Security Approach.

Packet Delivery Ratio Analysis

The packet delivery ratio is an important metric that indicates the number of packets successfully delivered to their destination nodes compared to the total number of packets transmitted in the network. A higher packet delivery ratio shows better network performance. The impact of the DoS flooding attack on the packet delivery ratio in VANET is shown in Figure 10. It has been observed from figure, Figure 10 that the packet delivery ratio analysis with QRT is lower than the Improved Security (IS) Approach in the presence of a DoS flooding attack in the vehicular network. This means that the IS approach is more effective in preventing the impact of DoS attacks on the packet delivery ratio in VANET.

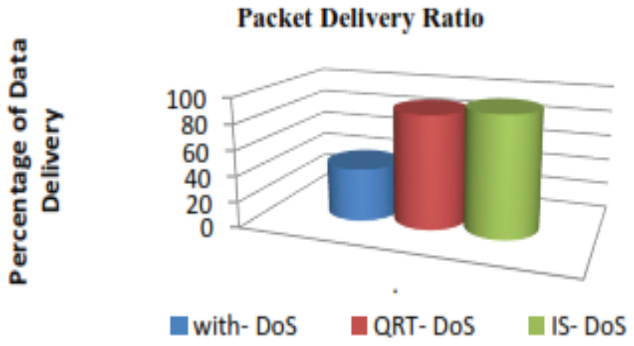

Figure 10. Packet Delivery Ratio analysis using AODV protocol in VANET.

Routing Load Analysis

Figure 11 illustrates the impact of DoS flooding attacks on routing load analysis. The routing load should be minimized to improve network performance, as it leads to delays. It has been observed that QRT results in a higher routing load than the Improved Security (IS) approach in the presence of DoS flooding attacks in vehicular networks.

Denial-of-Service Packets

This performance metric measures the packet loss due to the Denial-of-Service (DoS) attack in the VANET. Figure 11 displays the impact of DoS packets on VANET. The

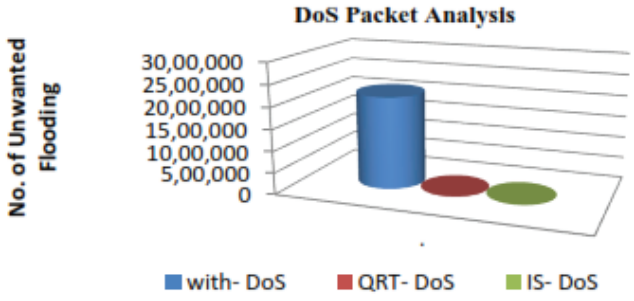

Figure 11. Denial of Service Packets using AODV protocol in VANET.

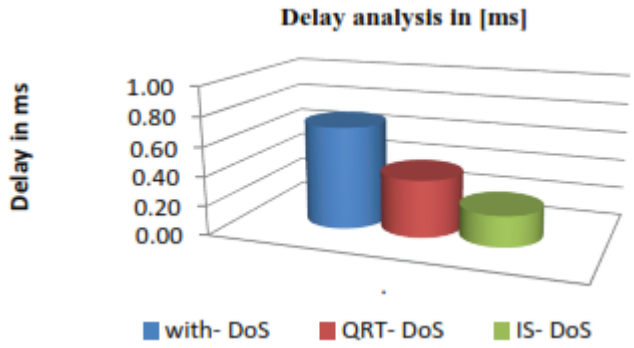

Figure 12. Delay analysis using AODV protocol in VANET.

results indicate that unwanted packet flooding is lower in the Improved Security (IS) approach than in the QRT-DoS approach.

Delay Analysis [ms]

This parameter shows the delay analysis due to a denial-of-service attack in VANET. Figure 12 shows the delay analysis, and it has been observed that the delay is very low in the Improved Security (IS) Approach compared to the QRT-DoS approach.

CONCLUSION

The Improved Security (IS) Approach is used for increasing security and improving the Vehicular network performance. Suppose abnormal behaviour of any vehicle is detected in the network. In that case, that vehicle's trust value is decreased and marked as untrusted by the control and monitoring unit (CMU) in its table. The following results were observed after implementing the IS Approach: (i) the Packet Delivery Ratio of the IS approach is nearly 5% more than the existing QRT approach; (ii) the throughput of the IS approach is about 1000 KBps more than the existing QRT approach; (iii) packet Drop Analysis of the IS approach is about 1400 packets less than the existing QRT approach. Other measuring parameters like packet send and receive analysis, routing load analysis, denial of service packets, and delay analysis also show better results with the IS approach.

Following future enhancements required for the improvement of the robustness, efficiency, and effectiveness of the IS-DOS prevention mechanisms:-

- Exploring advanced machine learning techniques that help improve efficiency, like improved deep learning techniques.
- In future studies, include 5G/ 6G enhanced high bandwidth communication technologies that help to reduce the latency and improve the efficiency of the VANET system.
- In the future, hybrid security systems may be implemented, like cryptographic-based methods.

AUTHORSHIP CONTRIBUTIONS

Authors equally contributed to this work.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

STATEMENT ON THE USE OF ARTIFICIAL INTELLIGENCE

Artificial intelligence was not used in the preparation of the article.

REFERENCES

[1] Verma K, Hasbullah H, Kumar A. Prevention of DoS attacks in VANET. Wirel Pers Commun 2013;73:95-126. [CrossRef]

[2] Haydari A, Yilmaz Y. Real-time detection and mitigation of DDoS attacks in intelligent transportation systems. In: Proceedings of the 21st International Conference on Intelligent Transportation Systems (ITSC); 2018. p. 157-163. [CrossRef]

[3] Singh D, Ranvijay, Yadav RS. A state-of-art approach to misbehaviour detection and revocation in VANET: Survey. Int J Ad Hoc Ubiquitous Comput 2018;28:77-93. [CrossRef]

[4] Gao Y, Wu H, Song B, Jin Y, Luo X, Zeng X. A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network. IEEE Access 2019;7:154560-154571. [CrossRef]

[5] Lyamin N, Vinel A, Jonsson M, Loo J. Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks. IEEE Commun Lett 2013;18:110-113. [CrossRef]

[6] Asaar MR, Salmasizadeh M, Susilo W, Majidi A. A secure and efficient authentication technique for vehicular ad-hoc networks. IEEE Trans Veh Technol 2018;67:5409-5423. [CrossRef]

[7] Ahmad F, Franqueira VN, Adnane A. TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks. IEEE Access 2018;6:28643-28660. [CrossRef]

[8] Usha M, Ramakrishnan B. Robust MPR: A novel algorithm for secure and efficient data transmission in VANET. Wirel Pers Commun 2020;110:355-380. [CrossRef]

[9] Bylykbashi K, Elmazi D, Matsuo K, Ikeda M, Barolli L. Effect of security and trustworthiness for a fuzzy cluster management system in VANETs. Cogn Syst Res 2019;55:153-163. [CrossRef]

[10] Kolandaisamy R, Md Noor R, Ahmedy I, Ahmad I, Reza Z'aba M, Imran M, et al. A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks. Wirel Commun Mob Comput 2018;2018:2874509. [CrossRef]

[11] Waraich PS, Batra N. Prevention of denial of service attack over vehicle ad hoc networks using quick response table. In: Proceedings of the 4th International Conference on Signal Processing, Computing and Control (ISPCC); 2017. p. 586-591. [CrossRef]
[12] Azees M, Vijayakumar P, Deboarh LJ. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Trans Intell Transp Syst 2017;18:2467-2476. [CrossRef]
[13] G R, C GK, Singh N, Patil VR. Autonomous forecasting of traffic in cellular networks based on long-short term memory recurrent neural network. Cybern Syst 2023;56:33-45. [CrossRef]
[14] Singh HP, Sheetlani J, Salimath N, Gopal KM. Design and implementation of an algorithm for mitigating the congestion in mobile ad hoc network. Int J Emerg Technol 2019;10:472-479.
[15] Singh HP, Singh R. Prevention mechanism of black hole and jamming attack in mobile ad-hoc network. J Harmon Res Eng 2020;8:1-7. [CrossRef]
[16] Krishna K, Vamshi, Reddy KG. VANET vulnerabilities classification and countermeasures: A review. Majlesi J Electr Eng 2022;16:63-83.
[17] Shahid KA. Secure trust-based blockchain architecture to prevent attacks in VANET. Sensors 2019;19:49-54. [CrossRef]
[18] Poongodi M. Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics. IEEE Access 2019;7:158481-158491. [CrossRef]
[19] Bashir RR, Saeed Y, Ali A, Algarni AD, Muthanna A, Hijjawi M, et al. 2cap: A novel curve crash avoidance protocol to handle curve crashes in vehicular ad-hoc network. IEEE Access 2024;12:60601-60619. [CrossRef]
[20] Gopi R. Intelligent DoS attack detection with congestion control technique for VANETs. Comput Mater Contin 2022;72(1). [CrossRef]
[21] Shiek Aalam S, Sivakumar M, Anjali Devi S, Teja PVS, Singh N. Emerging trends in vehicular communication and routing for intelligent transportation systems. In: Bhatia J, Tanwar S, Rodrigues JJPC, Kumhar M, editors. Deep Learning Based Solutions for Vehicular Adhoc Networks. Studies in Computational Intelligence, Vol. 1207. Singapore: Springer; 2025. [CrossRef]
[22] Gaurav A. DDoS attack detection in vehicular ad-hoc network (VANET) for 5G networks. In: Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions; 2022. p. 263-278. [CrossRef]
[23] Singh N, Singh HP, Mishra A, Khare A, Swarnkar M, Almas SK. Blockchain cloud computing: Comparative study on DDoS, MITM and SQL injection attack. In: Proceedings of the IEEE International Conference on Big Data & Machine Learning (ICBDML); 2024; Bhopal, India. p. 73-78. [CrossRef]
[24] Nayak RP. MLMDS: Machine learning based misbehavior detection system for cognitive software-defined multimedia VANETs in smart cities. Multimed Tools Appl 2023;82(3):3931-3951. [CrossRef]
[25] Bhayo J, Shah SA, Hameed S, Ahmed A, Nasir J, Draheim D. Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. Eng Appl Artif Intell 2023;123:1-17. [CrossRef]
[26] Singh HP, Patel H, Singh N, Rane P, Soni S. DLAR: Deep learning-based adaptive routing strategies for vehicular ad-hoc networks (VANETs). In: Bhatia J, Tanwar S, Rodrigues JJPC, Kumhar M, editors. Deep Learning Based Solutions for Vehicular Adhoc Networks. Studies in Computational Intelligence, Vol. 1207. Singapore: Springer; 2025. [CrossRef]
[27] Ali WA. Intrusion detection system for vehicular ad hoc network attacks based on machine learning techniques. Inf Secur J A Glob Perspect 2024;33(6):128-139. [CrossRef]
[28] Singh N, Suhane P, Singh HP, Rane P, Shukla D. Traffic prediction and modeling in vehicular ad hoc networks. In: Bhatia J, Tanwar S, Rodrigues JJPC, Kumhar M, editors. Deep Learning Based Solutions for Vehicular Adhoc Networks. Studies in Computational Intelligence, Vol. 1207. Singapore: Springer; 2025. [CrossRef]
[29] Verma A, Saha R. IPREVIR: Fortifying vehicular networks against denial of service attacks. IEEE Access 2024;12:48301-48320. [CrossRef]
[30] Memon I, Shaikh RA, Shaikh H. Dynamic pseudonyms trust-based model to protect attack scenario for internet of vehicle ad-hoc networks. Multimed Tools Appl 2024;83:13395-13426. [CrossRef]
[31] Al-Shareeda MA. SE-CPPA: A secure and efficient conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. Sensors 2021;21:1-22. [CrossRef]
[32] Bangui H, Ge M, Buhnova B. A hybrid machine learning model for intrusion detection in VANET. Computing 2022;104(3):503-531. [CrossRef]
[33] Khan IA. An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles. IEEE Trans Intell Transp Syst 2021;13(12):25469-25478. [CrossRef]
[34] Shah AS, Karabulut MA. Optimization of drones communication by using meta-heuristic optimization algorithms. Sigma J Eng Nat Sci 2022;40(1):108-117. [CrossRef]
[35] Kemal E. Cross-layer design in wireless AD HOC and sensor networks. Sigma 2010;28:66-73.
[36] Tonbul E, Takan MA, Büyükköse GT, Erginel N. Modeling open vehicle routing problem with real life costs and solving via hybrid civilized genetic algorithm. Sigma J Eng Nat Sci 2024;42(3):714-730. [CrossRef]