Majlesi Journal of Electrical Engineering
Vol. 18, No. 1, March 2024

Fast and Efficient Distance based External Wormhole Detection and Prevention System (FEDEWDPS)

Prathap Kumar Ravula[1], Srilakshmi Uppalapati[2], Ganesh Reddy Karri[3]
1- VFSTR Deemed to by University, Guntur, India.
Email: rpk_cse@vignan.ac.in (Corresponding author)
2- Koneru Lakshmaiah Education Foundation, Hyderabad, India.
Email: druppalapati2019@gmail.com
3- VIT-AP University, Guntur, India.
Email: ganesh.reddy@vitap.ac.in

ABSTRACT:
In terms of applications and research, VANET (Vehicular Ad-hoc Networks) communication is becoming more popular. Existing VANET communication protocols try to improve network performance but fail to consider security issues. Attackers exploit the vulnerabilities of VANET communication protocols. Providing security to the VANET is still a challenging task because of the vehicles' mobility and their short communication range. Based on our study, we found that wormhole attacks are the most common type of attack on VANET communication. The existing security solutions are inadequate to prevent or detect external wormhole attacks on VANET communication because these solutions do not consider important parameters such as vehicle mobility, neighboring ratio, and node mobility to detect the wormhole attack. To address external wormhole attacks in VANETs, we propose a two-level fast and efficient distance-based external wormhole detection and prevention system in this paper. In our proposed solution, we consider the vehicles' mobility, geographical location, and distance parameters to identify and isolate external wormhole attacker nodes. For effective monitoring of wormhole attacks, we use a dynamic threshold value for suspecting external wormhole attack links and then use the hop count metric to detect and prevent it. We used SUMO with NS2 simulators to compare our proposed system with existing works, and our simulations show that our proposed security solution outperforms existing works in terms of throughput, PDR, and jitter in a wormhole attack VANET environment.

KEYWORDS: VANET, FEDEWPS, Wormhole Attack, Vehicles Mobility.

1. INTRODUCTION

In the current traffic scenario, the admission of malicious vehicles is lowering the security of VANET. The VANET system aids in intelligent traffic control and demands the use of more advanced resources such as telemetric boxes, OBUs, and so on, as VANET packets contain vital information that an adversary must not be able to receive or alter in any way. In addition to increased responsibilities, drivers should have access to real-time traffic information [12].

Vehicle mobility encompasses automobiles, trains,bicycles, motorcycles, and other types of road vehicles [12]. In VANET, the movement of cars is controlled bythe streets, their ways, the traffic lights, and the road signs. The block size is determined by the streets, and the size of a junction affects the frequency with which vehicles slow down or stop. Managing the flow of motion with the addition of traffic lights and stop signs in predetermined locations contributes to the realism of a mobility model. The term "traffic interdependence" refers to the way nearby vehicles influence each other. If the speed increases, it will be controlled so that the location can be adjusted. Vehicle speeds are affected by speed limits [12].

VANETs are networks that comprise vehicles and roadside access points [18]. During the driving process,

Paper type: Research paper
https://doi.org/10.30486/mjee.2024.1977301.1053
Received: 27 October 2023; revised: 26 November 2023; accepted: 7 January 2024; published: 1 March 2024
How to cite this paper: P. K. Ravula1, S. Uppalapati, G. R. Karri, **"Fast and Efficient Distance based External Wormhole Detection and Prevention System (FEDEWDPS)"**, *Majlesi Journal of Electrical Engineering*, Vol. 18, No. 1, pp. 265-282, 2024.

information is shared between vehicles using accesspoints. As a result of its size, VANET has become a dynamic space for research, standardization, and growth, contributing to improvements in vehicle and road safety, traffic efficiency, and driving and riding convenience and comfort.

Each vehicle that is part of VANET serves the purpose of a wireless router or vehicle. It is equipped with sensors that connect to the computer and provide information about the vehicle's dimensions (speed and distance), lane location, and relative vehicle speed. An inter-vehicle communication system establishes a local area network to facilitate information exchange with other vehicles in the vicinity. This allows for changing lanes, receiving congestion warnings, rollover warnings, coupling and decoupling warnings, and communicating with inert vehicles. Because communication involves driver credentials, anything that poses a risk to the network also poses a risk to driver safety.

The intelligent vehicles that make up the vehicular network each have their own onboard units (OBUs), in addition to roadside units. There are two different modes of communication that can take place in a VANET: V2V and V2R. (V2I). The limited transmission range of VANET vehicles necessitates the use of multi-hop communication in order to properly route messages as shown in Fig. 1. In order to transport data over multiple hops, you need other nodes. Both the security of vehicle ad-hoc networks and their routing present significant challenges. The vehicular network needs to be guarded against attacks from both inside and outside the system [13].

As a wireless network, VANET is susceptible to all of the security risks associated with wireless networks. A security mechanism should check to make sure that transmissions originate from a trustworthy source and are not altered while they are in transit. Since deadlines for safety-related apps are more stringent, VANET has chosen to prioritize their development [34]. Because the network is ad hoc, any node can join or leave at any time, and there is no earlier trust connection between any of the nodes, so it is vulnerable to attacks such as the Sybil attack, the denial-of-service attack, the forging attack, the illusion attack [18], and the wormhole attack.

1.1. External Wormhole Attacks

External wormhole attacks are the most dangerous threat in VANETs. Typically, two or more malicious Vehicles initiate an attack. Vehicles are connected by a secret channel known as a tunnel which is used to perform four tunnel types of malicious activities: packet encapsulation, out-of-band transmission, high power transmission, and packet relay.

In Fig. 2, we see an external wormhole opened up to the outside world by hostile vehicles. There are two hostile vehicles, M1 and M2, that are operating outside the system and communicating with each other using a private channel. Any data packets received by vehicle M1 from cars within its coverage area (vehicles 1, 3, 4, 5, 6, 7, and 8) can be tunneled to vehicle M2 via an out-of-band channel, and from vehicle M2 those data packets can be broadcast to any cars within vehicle M2's communication range (such as vehicles 2; 12; 13;15; 16; 17). Vehicles 1 and 2 both fall within the coverage areas of both M1 and M2, and as a result they both think they are neighbors even though they are thousands of kilometers apart.

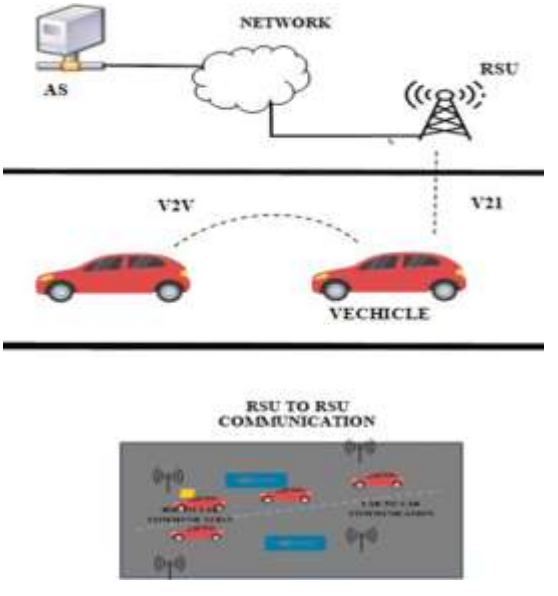

Fig. 1. VANET Architecture.

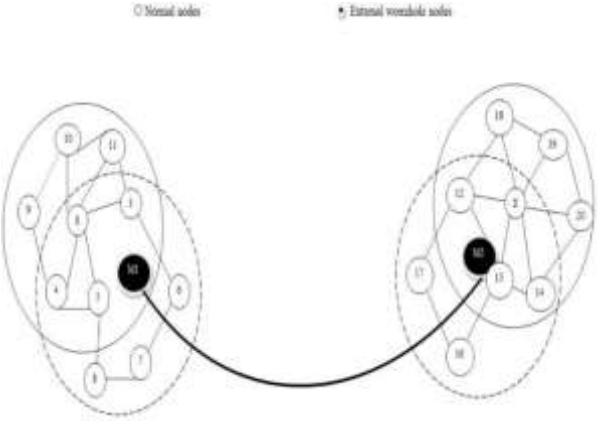

Fig. 2. The external wormhole formed due to maliciousvehicles.

Wormhole attacks are the most dangerous type of attack because their network coverage is very high when compared with normal vehicle radio ranges. We should have the robust collaborative monitoring techniques required to detect and isolate whole attacks before they are exploited [21]. However the existing mechanism is inadequate to address the wormhole attacks and security mechanisms of other wireless networks like ad- hoc, sensors, and IoT are not fit to the VANET [33]due to high mobility which is discussed in the literature. This problem led to high false positives and false negatives in the result, moreover, highly dynamic links between the vehicles led to failure [25] of identifying wormhole attacks. In this paper, our objective is to detect and prevent the wormhole attackin more challenging network VANET.

1.2. Objectives of our Proposed Work

For that we have set the following objectives:

1. Identify the accurate neighboring vehicles using dynamic threshold values that reduce the number of wormhole links to verifywhich leads to effective utilization of VANET resources such as computing and network resources.
2. Based on the dynamic threshold we suspect the malicious wormhole links and these links are further process to detect the wormhole.
3. In the detection of wormhole attacks, we use distance, vehicle mobility and hop_count parameters in the highly dynamic environment.
4. Any vehicle pair is detected as wormhole attack then the link will be removed in the active path VANET .

The rest of the paper is discussed as follows: in section 2, we discussed and compared the existing security mechanisms, the proposed intrusion detection system isexplained in section 3, results and analysis are discussed in section 4, and finally, we conclude this paper in section 5.

2. LITERATURE REVIEW

Wormhole attack is a type of security threat in VANET (Vehicular Ad-Hoc Networks) where attackers create a tunnel between two distant locations in the network, allowing them to intercept and manipulate the communication between vehicles. The following are some of the techniques used for wormhole attack detection and prevention in VANET:

Wormhole attack is a type of security threat in VANET (Vehicular Ad-Hoc Networks) where attackers create a tunnel between two distant locations in the network, allowing them to intercept and manipulate the communication between vehicles. The following are some of the techniques used for wormhole attack detection and prevention in VANET:

Geographical-Based Techniques: This technique uses the geographic location of vehicles to detect wormhole attacks. The technique assumes that the distance between two vehicles is proportional to the time taken for the signal to travel between them. If two vehicles are detected to be communicating with each other but their distance is greater than the maximum transmission range, then it is an indication of a wormhole attack.

Cryptographic-Based Techniques: This technique uses cryptographic mechanisms such as digital signatures and hash

functions to detect and prevent wormhole attacks. The technique involves the use of time- stamping or sequence numbers to detect the replay attacks and prevent the attackers from creating a new tunnel between two distant locations.
Network-Based Techniques: This technique uses network topology and routing information to detect wormhole attacks. The technique involves the use of hop-count, path delay, and neighbor information to identify suspicious nodes in the network.

Behavioral/Trust-Based Techniques: This technique uses the behavior of nodes to detect wormhole attacks. The technique involves the monitoring of the nodes' behavior to detect changes in the communication pattern or sudden changes in the number of packets sent and received.
Sharma et al. [1] proposed a dynamic trust-based approach for detecting and preventing wormhole attacks in VANETs. In this paper, the authors proposed a dynamic trust-based approach to detect and prevent wormhole attacks in VANETs. They used a combination of distance, velocity, and direction of the nodes to calculate trust values, which were used to detect and isolate malicious nodes.

Zardari et al. (2022) [2] proposed a lightweight wormhole detection and prevention scheme for MANETs. This paper proposed a lightweight wormhole detection and prevention scheme for MANETs. The authors used a distance-based approach to detect wormholes and proposed a scheme to prevent the wormhole attack by creating virtual paths.
Mani G. et al. (2020) [3] proposed a robust wormhole detection and prevention system for VANETs. This paper proposed a robust wormhole detection and prevention system for VANETs. The authors used a combination of distance-based and trust-based approaches to detect and isolate malicious nodes. They also proposed a new technique to prevent wormhole attacks by using a trusted anchor node.

Adhikari et al. (2020) [4] proposed a hybrid approach for detecting and preventing wormhole attacks in VANETs": In this paper, the authors proposed a hybrid approach for detecting and preventing wormhole attacks in VANETs. They used a combination of time-based and trust-based methods to detect and isolate malicious nodes. They also proposed a scheme to prevent wormhole attacks by using a virtual network infrastructure.

Akwirry et al. (2022) [5] proposed a novel wormhole detection technique in VANETs based on trust management. This paper proposes a trust management-based wormhole detection technique in VANETs. The proposed technique uses the trust level of neighboring vehicles to detect the presence of a wormhole. The study shows that the proposed technique is effective in detecting wormholes and outperforms existing techniques in terms of detection accuracy.

Rullo et al. (2019) [6] proposed a lightweight physical-based wormhole detection technique in VANETs. This study proposes a lightweight physical-based wormhole detection technique in VANETs. The proposed technique uses the time of flight of radio signals to detect the presence of a wormhole. The authors show that the proposed technique is effective in detecting wormholes and has low computational overhead.

Ali et al. (2022) [7] proposed a wormhole attack detection and prevention in VANETs using machine learning Techniques. This paper proposes a wormhole attack detection and prevention technique in VANETs using machine learning techniques. The proposed technique uses machine learning algorithms to analyze network traffic patterns and detect anomalies that indicate the presence of a wormhole. The study shows that the proposed technique is effective in detecting wormholes and has low false positive rates.

Ercan et al. (2022) [8] proposed a distributed wormhole detection technique in VANETs Using ant colony optimization. This study proposes a distributed wormhole detection technique in VANETs using ant colony optimization. The proposed technique uses the pheromone trails of virtual ants to detect the presence of a wormhole. The authors show that the proposed technique is effective in detecting wormholes attacks.

Masoud et al. [9] proposed wormhole attack solution in this research utilizing a variety of machine learning classification algorithms. In the MANET, they employed node attributes, particularly node speed, to extract features. They contain 3997 examples (normal 3781 and malicious 216) that include both normal and malicious models. The accuracy of the KNN, SVM, DT, LDA, NB, and CNN methods is 97.1 percent, 98.2 percent, 98.9 percent, 95.2 percent, 94.7 percent, and 96.4 percent, respectively, according to the classification findings. The accuracy of the DT approach, according to studies, is 98.9 %which is higher than the other approaches. SVM, KNN, CNN, LDA, and NB, in order of relevance, imply high accuracy.

Kuldeep et al. [10] proposed the presence of a malicious node in the network was detected utilizing a Trust based technique in this paper. In addition, by increasing the network's control overhead that node was deleted using a security technique to increase network performance using network metrics. The observer nodes will be used to evaluate this technique. AODV, Secure-AODV, and Trust-AODV will be used to evaluate all network measures. When compared to AODV and Secure-AODV, Trust-AODV produces better outcomes. The NS2 simulation results show that the suggested paradigm considerably improves network performance.

SreeDivya et al. [11] proposed that Black hole and wormhole attacks do significant damage to the data broadcasting zone, resulting in data drops or collapses. A unique CVL-HKH-BO method is suggested to address these issues. As a result, the recommended method of hybrid krill herd and bat optimization is based on the fitness function to detect and

prevent attacks. The proposed method can detect 99.15 percent of attacks and cause minimal packet loss. It lowers the amount of energy used by nodes in the VANET. As a result, the suggested technique's performance is compared to that of several current methods. As a result, the comparative result proved the efficacy of planned inquiry.

Gaurav et al. [12] proposed the IPS Scheme is used to identify and prevent Black hole and Wormhole attacks in VANET. Swarm optimization is used to apply the IPS algorithm to the RSU to recognize the harmful behaviors of an attacker vehicle. Performance indicators are used to assess the effectiveness of prior IDS and prospective IPS. When compared to a typical VANET scenario, the suggested security technique improves performance by around 90%. The NS-2 network simulator was used for the simulation.

Ankit et al. [13] proposed a safe AODV routing system to detect and identify the black hole attack. The suggested approach is a tweaked version of the original AODV routing system, with RREQ and RREP packet protocols improved. Different network metrics are used to show the suggested technique on an NS-2.33 simulator. The suggested technique has an average throughput of 77.79 for various malicious nodes, compared to 29.74 for the present AODV routing protocol. Similarly, the suggested technique has an average PDR of 75.28, compared to 33.11 for the conventional AODV routing protocol. The proposed strategy outperforms existing methods in terms of reliability.

Parma Nand et al. [14] proposed the influence of a wormhole attack is examined when it comes to throughput, PDR, and E2E delay. A method for detecting and preventing wormhole attacks in VANET over a real map with various vehicle densities is also proposed, based on the multipath concept, to construct an intelligent transportation system. The SUMO-0.32.0 and NS-2.35 simulator was used to run the simulation.

Vasiliy et al. [15] proposed the Swarm algorithm of Artificial Intelligence is used in this research to detect black hole and wormhole attacks. The trust concept is used in this method, which is based on IWD (Intelligent Water Drops). NS-3 network simulator is used to carry out the simulation. Throughput, packet delivery, and delay time are among the network performance metrics examined. With the inclusion of IDS in the created swarm algorithm, throughput increased by 20%, the share of delivered packets increased by 30%, and the delay time fell by 40%.

Ting-Hui et al. [16] proposed the wormhole attack is identified in this research using the QTS algorithm. The simulation findings show that the QTS technique effectively decreases the number of logic gates required to combine rules and that it performs well across a wide variety of node densities and transmission ranges. The QTS Algorithm demonstrates how to identify wormhole attacks using a combination of MA and logic operations. True negatives, False negatives, True positives, and False Positives all have a 100% detection rate that is unaffected by the number of nodes.

U. Srilakshmi et al. [17] ACO (Ant Colony Optimization) protocols for WSN have been proposed. It does not solve the network process's negative impact. As a result, we recommended a new SD-ACO method with QoS parameters. It optimizes the routing paths, allowing for secure data transmission and the recognition of malicious nodes.The results of a simulation using the NS2 are to validate the effectiveness of our method.

Ratnasih et al. [18] proposed the performance of the reactive routing protocol in a VANET with a wormhole attack. The throughput increases in lockstep with the initial power change, while the latency decreases rapidly. When the node density is altered, the highest delay value is 0.122 ns for 10 nodes and the highest throughput value is 0.215 Mbps for 8 nodes.

Prathap et al. [19] Proposed VANET Security Requirements, such as identification and authentication, privacy, routing, availability, and secrecy in attacks like Sybil, DDOS, blackhole, and wormhole, and challenges such as time constraints, network scale, and high mobility.

Basant Subba et al. [23] To solve challenges such as dynamic network topology, communication overhead, and scalability to increased vehicle density, developed a novel clustering algorithm, CH election technique, and game theory-based IDS framework for VANET. Finally, the proposed clustering strategy preserves the IDS framework's stability, ensuring that it scales effectively over networks with growing vehicle concentrations.

Kumar et al. [24] advocated addressing malicious attacks that compromise network security, and it is critical to recognize and avoid those attacks. A black hole attack can be detected using a Secure Routing Protocol. To validate the source and destination nodes, cryptography function-based encryption and decryption are incorporated for increased security. Different network factors s are illustrated on an NS-2.33 simulator. The suggested technique has an average throughput of 77.79 for varied malicious nodes, compared to 29.74 for the present AODV routing protocol. Similarly, the suggested technique has an average PDR of 75.28, In the AODV routing protocol, it is 33.11.

Shivaprasad et al. [27] Audio-video files would be exchanged in the created network as a result of data transmission among different automobiles. Because this network is designed for transitory communication, these multimedia messages should be transferred in a fraction of a second. Cars engaging in this communication must be trustworthy, or else other vehicles in the network will be misled by an intruder. In an ad-hoc network, blockchain induces high-end communication. It also improves the overall security of the network as a whole. In this research, we offer a blockchain-based security system for vehicular communication that securely and efficiently handles this communication. The proposed system's performance will be evaluated using characteristics such as end-to-end delay, reliability, and packet

delivery ratio.

Heena et al. [29] proposed a better security method for VANET that is capable of dealing with attacks such as DoS, Sybil, and Replay. The suggested study uses the Enhanced K-Mean method to construct clusters for various attacks, as well as a hybrid strategy that employs a Support Vector Machine (SVM) and Feed- forward backpropagation to verify the classifier's accuracy. In terms of throughput, jitter, and PDR, the results demonstrate a significant improvement.

Gaurav et al. [30] suggested an IPS strategy for protecting Vehicle to RSU (V-RSU) communication in the VANET against malicious (Black hole) and Wormhole attacks. Vehicles in the planned IPS scheme receive traffic data while traveling down a highway and then share data after they leave the RSU service area. The proposed security system's major purpose is to effectively manage automobiles in the presence of an intruder. The suggested IPS method with PSO performs better in the presence of both attackers in the VANET, according to simulation results. Performance metrics are used to assess the performance of prior IDS, Attackers, and prospective IPS. The key benefit of implementing IPS protection in RSUs is that once an attacker is found, their individual information may be readily relayed to all RSUs for subsequent alerts regarding dangerous network activity. After all, this data is sent to prevent harmful cars from entering the area. Intruders are detected and useful traffic packets are lost with the suggested IPS security with PSO. Vehicle mobility is improved by minimizing displacement.

Shahjahan et al. [31] proposed an attack on the Blackhole and Wormhole. The wormhole attack in VANET's multi-hop communication is detected using a machine-learning method in this paper. We developed a VANET scenario using the NS-3.24.1 simulator using the AODV routing protocol, which uses the overall mobility traces provided by the SUMO-0.32.0 simulator to represent the wormhole assault. The peculiarity of this study effort is that it uses machine learning to make a vehicle ad-hoc network free of wormhole assault utilizing the proposed detection and prevention technique. The proposed machine learning models' performance is compared to previous research. As a result, it is obvious that our suggested approach, which employs machine learning, is a potent tool for detecting wormhole assaults in VANETs. To counter the wormhole attack in VANET, a solution based on packet leasing and cryptographic measures is implemented. The k-NN model in an earlier research paper (Singh et al., 2019) has a detection accuracy of 99 percent for wormhole attacks, however, due to correct data normalization, the k-NN model in our study effort has a detection accuracy of 99.196 percent for wormhole attacks in VANET.

Arun et al. [32] Examine the impact and harmful actions of a few of the most common assaults, as well as some security measures against some of the most serious attacks in the VANET. The attacker's goal is to change the actual route or offer misleading information about the route to the sender, and some attackers are just flooding undesired packets to use network resources. The study also discusses several routing options because data routing is critical for delivering traffic information to leading vehicles.

In this section, we explain the two-level wormhole attack detection and prevention system, we also call it as Fast and Efficient Distance based external Wormhole Detection And Prevention System (FEDEWDPS), which addresses the issues like mobility and training and testing with lightweight approaches for wormhole attacks which are still exist in existing mechanism. The majority of existing security solutions in the literature are for MANET, and these solutions fail to produce good results in VANET due to mobility differences between VANET and MANET. Machine learning and AI-based solutions are proposed to detect blackhole and wormhole attacks; however, the mobility of the vehicles is not considered to classify the attack, leading to high numbers of false positives and negatives. Blockchain technology is used to address VANET attacks, but these techniques failed due to the wormhole nature; in this case, the hop_count is not modified, but a wormhole still exists. Based on our review of the literature, we found that current VANET security solutions are insufficient to prevent wormhole attacks.

The table 1 presents the comparison study of various methods proposed by different authors for detecting and preventing wormhole attacks in vehicular ad hoc networks (VANETs). The focus is mainly on wormhole attacks, most of the methods face limitations in terms of high computational overhead, high false positives and false negatives due to high speed mobility vehicles, vulnerability to internal attackers, and a single point of failure. Some methods also require feature extraction and classification algorithms, which add more computational overhead. Furthermore, some methods are limited to detecting only specific types of attacks, such as black hole attacks or misleading information attacks, while others fail to handle high dynamic topology and scalability issues. Finally, some methods are based on machine learning techniques or swarm optimization algorithms, which also add more computational overhead. In our proposed work, we consider both network and geographical based methodologies to prevent external wormhole attacks.

Table 1. Summary of Literature Review and Narrative Description.

Author	Method Name	Attacks Detected/Prevented	Limitations
Sharma et al. [1]	Dynamic Trust-based Approach for Wormhole Detection	Wormhole attacks	High computational overhead Fail to handle high-speed mobility vehicles lead to more false positives and false negatives Internal attackers vulnerability exist
Zardari et al. [2]	Lightweight Wormhole Detection and Prevention Scheme	Wormhole attacks	High false positives and negatives due to node vehicles speed Internal wormhole attacks exist
Mani G. et al. [3]	Robust Wormhole Detection and Prevention System	Wormhole attacks	Requires a trusted node for prevention Vulnerable to single point of failure Inefficient for high dynamic topology Internal wormhole attacks exist
Adhikari et al. [4]	Hybrid Approach for Wormhole Detection and Prevention	Wormhole attacks	Vulnerable to single point of failure Inefficient for high dynamic topology Internal wormhole attacks exist
Akwirry et al. [5]	Trust Management-Based Wormhole Detection	Wormhole attacks	Vulnerable to single point of failure New vehicles still have chance to perform wormhole attacks with their trust Internal wormholeattacks exist
Rullo et al. [6]	Lightweight Physical-based Wormhole Detection	Wormhole attacks	Fail to handle high speed mobility vehicles lead to more false positives and false negatives Internal attackers vulnerability exist
Ali et al. [7]	Wormhole Attack Detection and Prevention using ML Techniques	Wormhole attacks	High computational overhead Fail to handle high speed mobility vehicles lead to more false positives and false negatives
Ercan al. [8]	Distributed Wormhole Detection using Ant Colony Optimization	Wormhole attacks	Fail to handle high speed mobility vehicles lead to more false positives and false negatives Internal attackers vulnerability exist
Masoudet al. [9]	Machine Learning-Based Wormhole Detection	Wormhole attacks	Requires feature extraction and classification algorithms lead to more computational overhead
Kuldeep et al. [10]	Trust-Based Technique for Malicious Node Detection	Malicious nodes	Fail to handle high speed mobility vehicles lead to more false positives and false negatives Internal attackers vulnerability exist
SreeDivya et al. [11]	Hybrid Krill Herd and Bat Optimization-Based Wormhole Detection	Black hole and wormhole attacks	Fail to handle high speed mobility vehicles lead to more false positives and false negatives Internal attackers vulnerability exist
Gaurav et al. [12]	IPS Scheme for Black Hole and Wormhole Attack Prevention	Black hole and wormhole attacks	Requires a swarm optimization algorithm and performance indicators which need more computational overhead
Ankit et al. [13]	Safe AODV	Black hole attack	Limited to black hole attack
Parma Nand et al. [14]	Multipath concept-based	Wormhole attack	High computational overhead Fail to handle high speed mobility vehicles lead to more false positives and false

Vasiliy et al. [15]	Swarm algorithm	Black hole and wormhole attacks	High computational overhead Fail to handle high speed mobility vehicles lead to more false positives and false negatives Internal attackers vulnerability exist
Ting-Huiet al. [16]	QTS Algorithm	Wormhole attack	High computational overhead Fail to handle high speed mobility vehicles lead to more false positives and false
U.Srilaks -hmi et al. [17]	SD-ACO	Malicious nodes	Negative impact on network process
Ratnasih et al. [18]	Reactive Routing	Wormhole attack	Fail to handle high speed mobility vehicles lead to more false positives and false
Prathap et al. [19]	VANET Security Requirements	Sybil, DDOS, black hole, and wormhole attacks	Time constraints, network scalability low detection rate for high mobility
Prathap et al. [20]	AODV and DSR	Black hole and wormhole attacks	High computational overhead Fail to handle high speed mobility vehicles lead to more false positives and false
Basant Subba et al. [23]	Clustering algorithm and IDS framework	Malicious attacks	High computational overhead Fail to handle high speed mobility vehicles lead to more false positives and false negatives Internal attackers vulnerability exist
Kumar et al. [28]	Secure Routing Protocol	Black hole attack	Not able to detect the wormhole attacks
Shivapras ad et al. [27]	Blockchain-based	Intruder attacks	High computational overhead High storage overhead
Heena et al. [29]	Enhanced K-Mean method, SVM, and Feed-forward backpropagation	DoS, Sybil, and Replay	not able to detect the wormhole attacks
Gaurav et al. [30]	IPS strategy with PSO	Black hole and Wormhole	High computational overhead Fail to handle high speed mobility vehicles lead to more false positives and false negatives Internal attackers vulnerability exist
Shahjaha n et al. [31]	Machine learning and cryptographic measures	Wormhole	High computational overhead Fail to handle high speed mobility vehicles lead to more false positives and false negatives
Arun et al. [32]	Various routing options and security measures	Misleading information about the route, flooding undesired packets, and actual route changes	High computational overhead Fail to handle high speed mobility vehicles lead to more false positives and false negatives Internal attackers vulnerability exist

3. FAST AND EFFICIENT DISTANCE BASED EXTERNAL WORMHOLE DETECTION AND PREVENTION SYSTEM (FEDEWDPS)

In our detection and prevention system, first we find the number of neighboring vehicles for a minimum of x seconds with the help of the relative speed of a vehicle. Secondly, use this neighboring node information to suspect the wormhole attack links. For that, we use the dynamic threshold value defined by ARIMA which is explained in 3.1 section, and finally, apply the distance measures to detect the wormhole attacks, followed by preventing the wormhole attacks from

the active paths which is explained in 3.2 section.

3.1. Vehicle Speed, Distance and Neighboring Vehicles Threshold Value Calculation

3.1.1. Vehicle speed and distance

Distance between two vehicles V1 AND V2 WITH AVERAGE SPEED S1 AND S2

V1= lon_v1, lat_v1
V2= lon_v2, lat_v2
l1= c1∗ (lat_v2− lat_v1)
l2= c1∗ (lon_v2− lon_v1) ∗ COS (lat_v1/c2),

There are c1 miles in one degree of latitude and c2 miles in one degree of longitude [22]. One degree of latitude is equivalent to c1 miles and one degree of longitude is equal to c2 miles, where c1 and c2 are constants with values of 69.1 and 57.3, respectively.

td= (c2 − c1) ∗c3

where td instantaneous travel time in seconds, c3 value is86400seconds

dv1,2= $\sqrt{l_1^2 + l_2^2}$ *c4

where dv1,2is vehicles distance in meters, and c3 is a constant value 1609.344 to convert miles into meters

Sv1,2= (dv1,2/td)∗ c5

Where Sv1,2 speed between two vehicles v1 and v2 and c5 is a constant value 3.6 to convert km/h to m/s.

3.1.2. ARIMA model to set the dynamic Neighboring vehicles threshold value (xt)

In VANET, the number of neighboring vehicles varies with respect to time. If we set the fixed threshold value to monitor the number of neighboring vehicles, it leads to overfitting and underfitting problems. As a result, we have more false positives and false negatives. To overcome these, we use Autoregressive Integrated Moving Average (ARIMA) time series model for predicting number of neighbors of a vehicle also called as dynamic neighboring vehicles threshold value. The ARIMA models have a general notation of ARIMA, and the parameters p (the number of time lags in the autoregressive model), d (the number of times past values have been subtracted from the data), and q (the number of times the moving average has been applied) the vehicle is considered a suspected wormhole attacker; otherwise, the vehicle has legitimate behavior. Internal and external wormhole detections are performed on all vehicle pairs that share a neighbor are all positive integers (p, d, q) [27]. The standard notation for ARIMA models that include seasonal components is ARIMA (p, d, q) (P, D, Q) m, where m is the number of periods that comprise each season and P, D, Q are the autoregressive, differencing, and moving average terms that are unique to the seasonal component of the ARIMA model.

$x_t = f_1 x_{t-1} + f_2 x_{t-2} + \ldots + f_{p+d} x_{t-p-d} + d + u_t + a_1 u_{t-1} + a_2 u_{t-2} + \ldots + a_q u_{t-q}$

Where x_t is the number of neighboring vehicles predicted value at time t and u_{t-q} is the prediction error at time t, f_1 and f_2 are the coefficients of previous iterations, p and q are integers that are often referred to as autoregressive and moving average polynomials.

3.2. Identifying Suspected Wormhole Attacks using number of Neighbors' in VANET

Because wormholes affect a small number of vehicles in comparison to the entire network, it is pointless to examine every vehicle in search of wormholes. Wormholes will maliciously increase the network's connectivity, leading to an apparent increase in the total number of neighbors. In our proposed work, we identify nodes with more neighbors than is typical (neighboring vehicles threshold value). VANET vehicles should use the neighboring vehicle threshold value to compare the number of neighbors to that of other vehicles to identify the wormhole attackers in the network. The following is an outline of the steps that need to be taken:

The neighboring vehicles (nv) in the VANET will be familiar with the vehicles that are immediately adjacent to them. First, nv finds all the neighboring nodes using the distance parameter. Then, disregard the neighboring vehicles, whose relative speed is more than double that of nv. After excluding the neighboring vehicles, they then find the neighbors of neighbors after excluding the over-speed neighbor nodes from the neighboring set. The average number of neighbors for each vehicle is then computed. Compare the average neighbors of a vehicle with the neighboring vehicles

threshold value. If a vehicle's average neighbors are more than or equal to the neighboring vehicle's threshold value (xt) then with the suspected vehicles. However, wormhole detections are only performed on vehicle pairs that they claim are direct neighbors. The entire procedure is explained in Algorithm 1.

Algorithm 1: Identifying Vehicles Neighboring Ratio to detect the suspected vehicles in ANETSuspected vehicles are identified by the vehicles neighbor ratio threshold

Input: VANET with V vehicles and neighbor vehicles set NV, vehicle mobility M, and neighboring vehicles threshold value xt

Output: Suspected vehicles that are part of wormhole communication links.

v_i= lon_v_i, lat_v_i

v_j= lon_v_j, lat_v_j

li= 69.1 ∗ (lat_v_j− lat_v_i)

lj= 69.1 ∗ (lon_v_j− lon_v_i) ∗ COS (lat_vi/57.3)

td= $(c_2 - c_1) * 86400$

$d_{vi,j}=\sqrt{l_i^2 + l_j^2} * 1609.344$

$s_{i,j}= (d_{v1,2}/t_d) * 3.6$

1 for each vehicle vi in V and ith vehicle neighbor set Nvi in NV do

2 Let nvi = |Nvi | (the number of neighboring vehicles of vi) at time ti.

3 Nvi = Nvi + {vi}

4 for each node vj∈Nvi do

5 nvj = |Nvj | (the number of neighboring vehicles of vj)

6 for each node vk∈Nvj do

7 vj= lon_vj, lat_vj

8 vk= lon_vk, lat_vk

9 l1= 69.1 ∗ (lat_vk−lat_vj)

10 l2= 69.1 ∗ (lon_vk−lon_vj) ∗ COS lat_vj/57.3),11

td= (ti – ti-1) ∗ 86400

12 dv(i,j)= $\sqrt{l_i^2 + l_j^2}$ * 1609.344

13 sv(j,k)= (dv(j,k)/td)∗ 3.6

14 if((vr$_j$)/2>=$d_{v(j,k)}$or ($s_{v(j,k)}$ <2*vs$_j$or 2* vs$_k$)) //vr$_j$& vs vehicle radio range& speed

15 if(i==j)

16 in$_i$= Ix$_i$ + 1 //in$_i$ is the selected including neighboring vehicles at v_i

17 Nv$_i$'= Nv$_i$' U v_k

18 else if(v_j∈Nv$_i$')

19 in$_j$ = in$_j$ + 1

20 in = in + in$_j$

21 nv$_i$ = in$_i$

22 Average number of neighboring vehicles of v_i's (nv'$_i$) = (in)/(nv$_i$) ;

23 Calculate vi's neighboring vehicles r_i = (nv$_i$/nv'$_i$);

24 if r_i>x_t then

25 Add v_i to suspected vehicles set S_V;

26 for each vehicle v_i∈ S_V do

27 for each vehicle vj∈ SV do

28 Detection of the wormhole paths using Algorithm

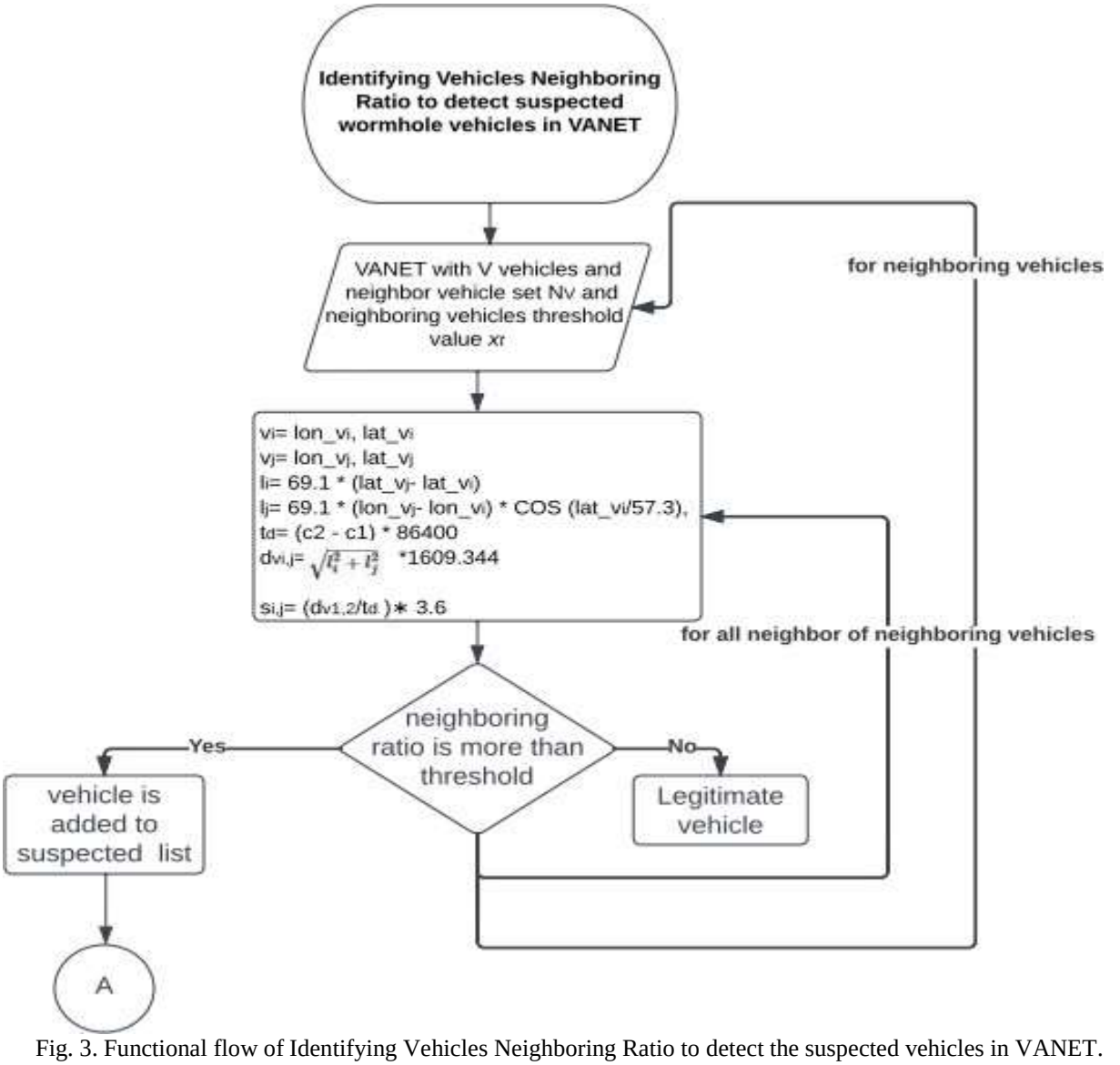

Fig. 3. Functional flow of Identifying Vehicles Neighboring Ratio to detect the suspected vehicles in VANET.

3.3. External Wormhole Detection and Prevention

In wormhole detection and prevention, Algorithm 1provides the initial input for the process. When vehiclesupdate their location information, the monitoring vehicles calculate the distance between suspected vehicles. If the distance between these vehicles is greater than the threshold value, they are treated as external wormhole nodes. The monitoring node removes these external wormhole vehicles from active paths and updates the routing tables. If the location information of the vehicles is not updated, the monitoring node uses neighborhood information to estimate the distance between thesuspected wormhole attack vehicles. If the estimated distance is greater than the one hop count, these vehicles are considered external wormhole attackers. The monitoring node then removes the external wormhole attack vehicles from the active route and updates the routing table, as outlined in Algorithm 2.

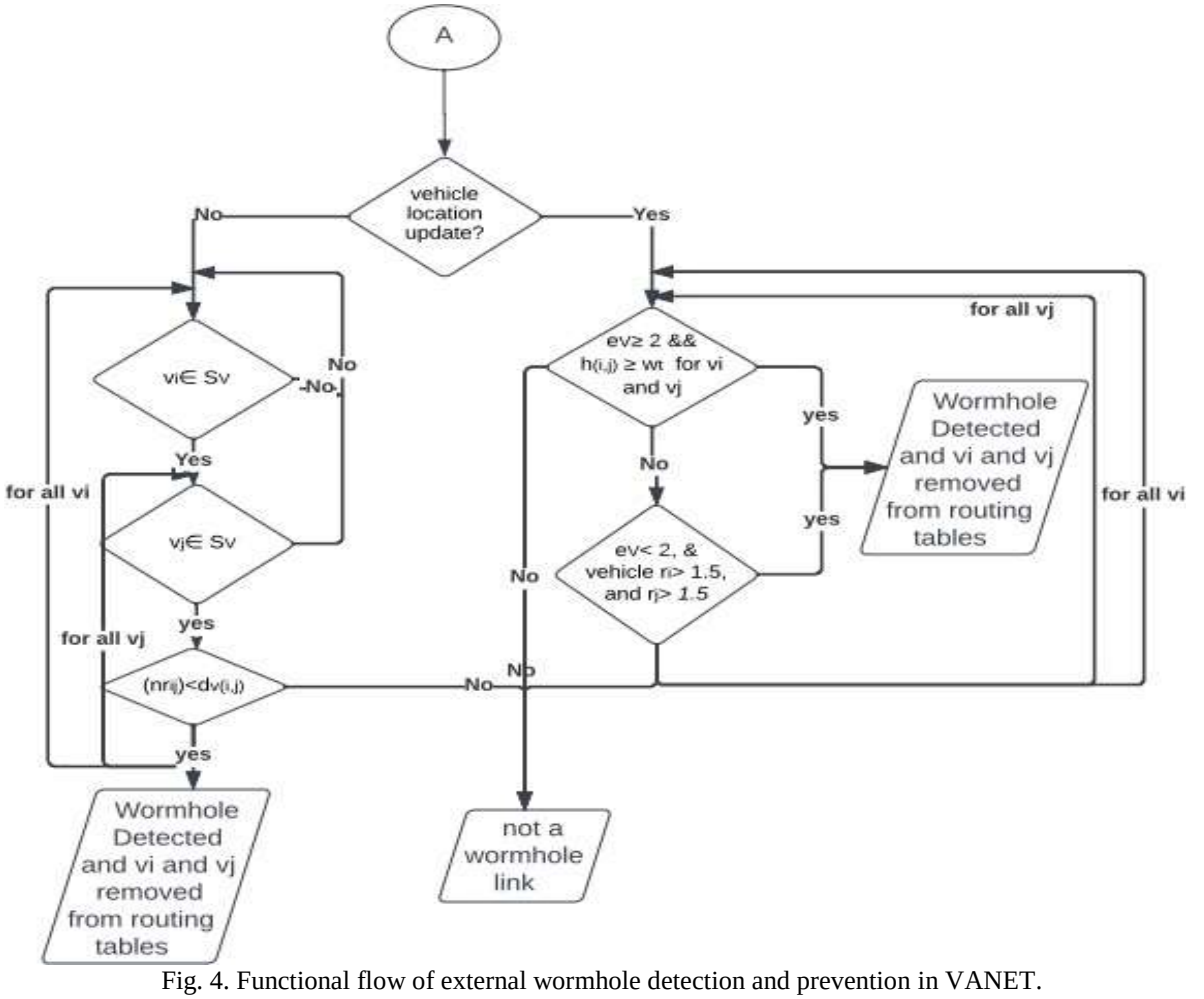

Fig. 4. Functional flow of external wormhole detection and prevention in VANET.

Example Scenario:

Wormhole attack detections in the mentioned suspicious vehicles, this information obtained from algorithm 1, here we have considered direct neighbor vehicle pairs. The primary premise of detecting external wormholes is to compare the hop counts between exclusive neighbor vehicles. Algorithm 2, presents the detection and prevention of wormhole attacks in all the phases. In Fig.2, owing to the wormhole attack tunnel formed between M1 and M2, thus vehicle v1's neighbor set is Nv1={v2, v3, v4, v5, v9, v10, v11, v12, v14, v15, v16, v17}.

Based on the foregoing observation, we may choose a vehicle from a neighbor vehicle pair whose exclusive neighbor number is greater than 2 and define additional linkages between its exclusive neighbors.

Neighbors should skip the neighbors of the other vehicle, then check whether the hop counts of these new links are bigger than the wormhole threshold to see if external wormholes exist. We'll take vehicle v1 from the neighbor vehicle pair v1 and v2 as an example, and define that the link between vehicle v1's exclusive neighbor set {v9, v10, v11, v15, v16} (shaded area in Fig.2) should bypass vehicle v2's neighbor set {v1, v3, v4, v5, v6, v7, v8, v12, v14, v15, v18, v19, v20}. (The non-shaded part in Fig.2). Once the hop count between these new links reaches the wormhole threshold, such as the new link from vehicle v9 to v15, it is considered that external wormholes exist between vehicle v1 and vehicle v2. Then, vehicle v1 and v2 eliminate each other from their neighbor tables and notify their neighbors about the removed neighbor vehicles. There isn't a wormhole if there isn't a wormhole.

Similarly, the neighbor set of vehicles v2 is Nv2={v1, v3, v4, v5, v6, v7, v8, v12, v14, v15, v18, v19, v20}. Then there's the common neighbor of vehicle pair v1 and v2, which is Nv1.Nv2 stands for v3, v4, v5, v12, v14, and v15. The exclusive use of vehicle v1 as shown in Fig.2. We may assume that the hop-count between any two vehicles is maximum which equals to less than or equal to two, and vehicle v1's exclusive neighbor set v9, v10, v11, v16, v17 is one; however, v9, v11, v12, and v16, v17 are far away, and the true hop between them is considerably bigger than one.

4. RESULT ANALYSIS

NS2 has the capability to simulate both wired and wireless network functions and standards and offers support for TCP, routing, and multicast protocols. The code for NS2 is written in C++ and TCL, which define the core mechanisms of simulation objects and start scheduler events, respectively. Table 2 provides a list of parameters for a network simulation that evaluates the performance of a vehicular communication system under specific conditions. The simulation involves 200 vehicles within a network area of 5km x 5km, with 10 to 20 wormhole attacks. The vehicles follow a waypoint-based mobility pattern, and have a communication range of 500m with a data rate of 1Mbps using the IEEE 802.11p communication protocol, which is designed for vehicular networks. To prevent congestion, the simulation uses a Random Early Detection (RED) queue, and the total simulation time is 1000 seconds. The study focuses on the implementation and evaluation of wormhole attacks in a vehicular communication system. These attacks involve malicious nodes creating a tunnel through the network to intercept or modify network traffic. In this study, the attacker receives packets from the source vehicles and forwards them to the other end of the wormhole tunnel. The attacker can drop, reorder, inject malicious packets, or increase the queuing delay of each packet. The study compares the proposed FEDEWDPS with other existing approaches such as dynamic trust-based approach, ACO, ML-based, and physical location-based approaches.

Table 2: Simulation Parameters.

Network Parameters	**Values**
Number of vehicles in the network	200
Number of RSUs	10
Number of wormhole attacks	10 to 20
Size of the network area	5km x 5km
Mobility pattern of the vehicles	Random Waypoint
Communication range of the vehicles	500m
Data rate of communication between the vehicles	1Mbps
Type of communication protocol used	IEEE 802.11p
Queue	RED
Simulation time	100s

Jitter is the variation in the delay of received packets, and it is an important metric in measuring the quality of a network connection. In a wormhole attack scenario, the attacker creates a tunnel between two distant points in the network, allowing them to intercept and modify packets as they pass through. The jitter values shown in Fig.5 represent the variation in packet delay in five different scenarios: FEDEWDPS, dynamic trust-base approach, ACO, ML based and physical location-based.

- Dynamic Trust-based approach: The jitter values are much higher in this scenario, ranging from 0.06 ms to 2.8 ms. This is likely due to the computational overhead of dynamic trust maintenance, which introduces significant delays in the network.
- ACO: The jitter values of ACO scenario, ranging from 0.5 to 0.9. Ant Colony Optimization (ACO) is an algorithm that can be used to optimize parameters in a network, but it may also introduce delays as it searches for the optimal solution.
- ML-based approach: The jitter ML-based scenario, ranging from 0.05 ms to 0.95 ms. ML-based algorithms (ACO) require both testing and training to introduce delays as they search for the optimal solution.
- Physical Location approach: The jitter value is of physical location-based approach, ranging from 0.03 ms to 0.98 ms. This approach required more computational power and location information exchange among the vehicles leading to more control overhead and all possible paths need to be tested which introduces additional delays in the communications.
- FEDEWDPS: The jitter values in this scenario are much lower than in the previous two scenarios, ranging from 0.00068 ms to 0.2 ms. IDS (Intrusion Detection System) is a security mechanism that can detect and prevent attacks in a network, and the two-level IDS is more effective in maintaining a stable network connection. As a result, The dynamic trust-based, ACO, ML-based and physical location-based approaches introduce significant delays, while effective IDS can help maintain a stable network connection.

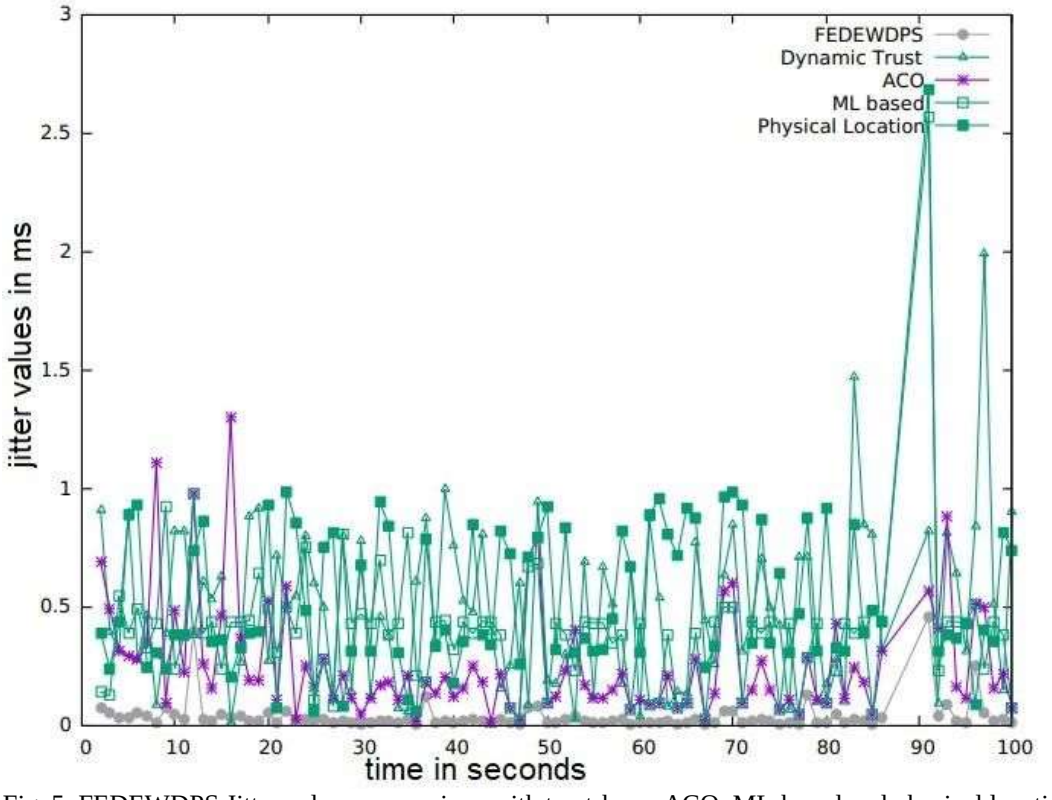

Fig. 5. FEDEWDPS Jitter values comparison with trust-base, ACO, ML-based and physical location-based.

The packet delivery ratio (PDR) is a measure of the ratio of the number of packets successfully delivered to the destination to the total number of packets sent by the source. In a wormhole attack scenario, the PDR is affected by the presence of the attacker, which may drop or modify packets, causing a reduction in the PDR.

Based on the results, we can see that the Packet Delivery Ratio (PDR) in the scenario shown in Fig. 6, FEDEWDPS is 89%, indicating that almost all the packets sent by the source were successfully delivered to the destination in the hostile environment. The PDR for dynamic trust, ACO, ML-based, and physical location based is at low PDR 32%, 42%, 48% and 38% respectively. This indicates that these methods were not effective in detecting and preventing the wormhole attack when compared with our proposed FEDEWDPS which as 89% for high-speed (160 kmph) mobility vehicles.

Throughput in a network refers to the amount of data that can be transmitted over a given period. In the context of a wormhole attack, the throughput measures the efficiency of data transmission in the network despite the attack. The results show the throughput values for different scenarios, namely FEDEWDPS, dynamic trust, ACO, ML based, and physical location-based approaches.

From Fig. 7, we can see that our proposed FEDEWDPS has the highest throughput values in all simulation test cases in the hostile environment. The dynamic trust, ACO, ML-based, and physical location-based have low or less than 6000 bytes/sec throughput values in most of the time, indicating that these methods are not effective in mitigating the wormhole attack. The FEDEWDPS has high throughput values when compared with exiting dynamic trust, ACO, ML-based, and physical location-based. Thus, our proposed FEDEWDPS is effective in mitigating the wormhole attack and shows the best performance in the hostile network.

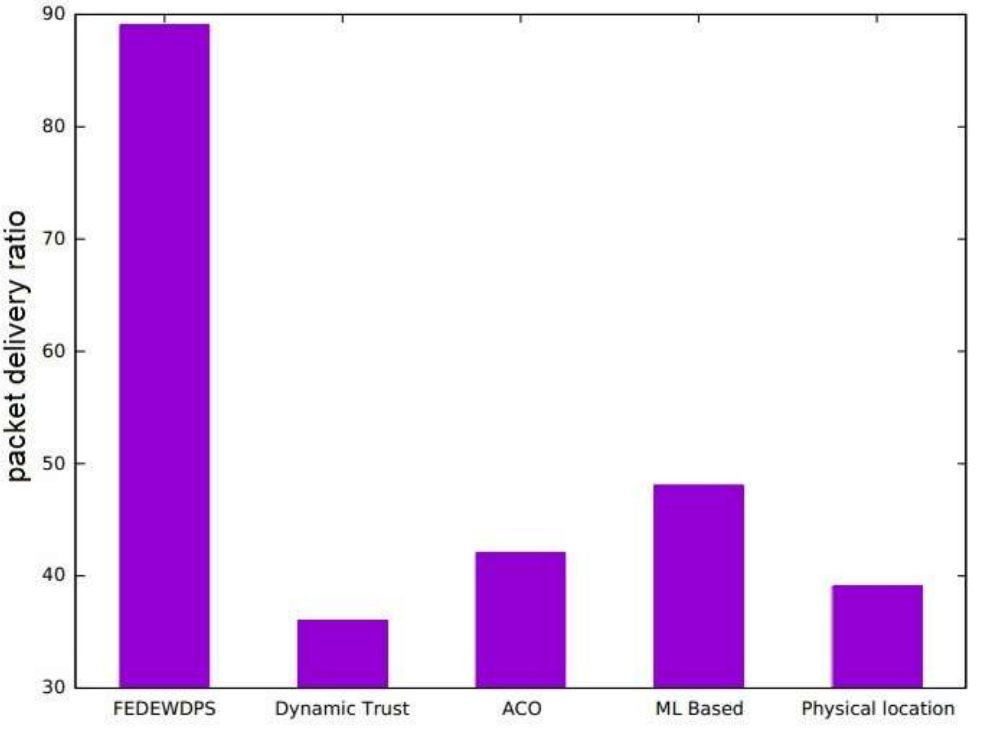

Fig. 6 FEDEWDPS PDR values comparison with trust-base, ACO, ML-based and physical location-based approaches.

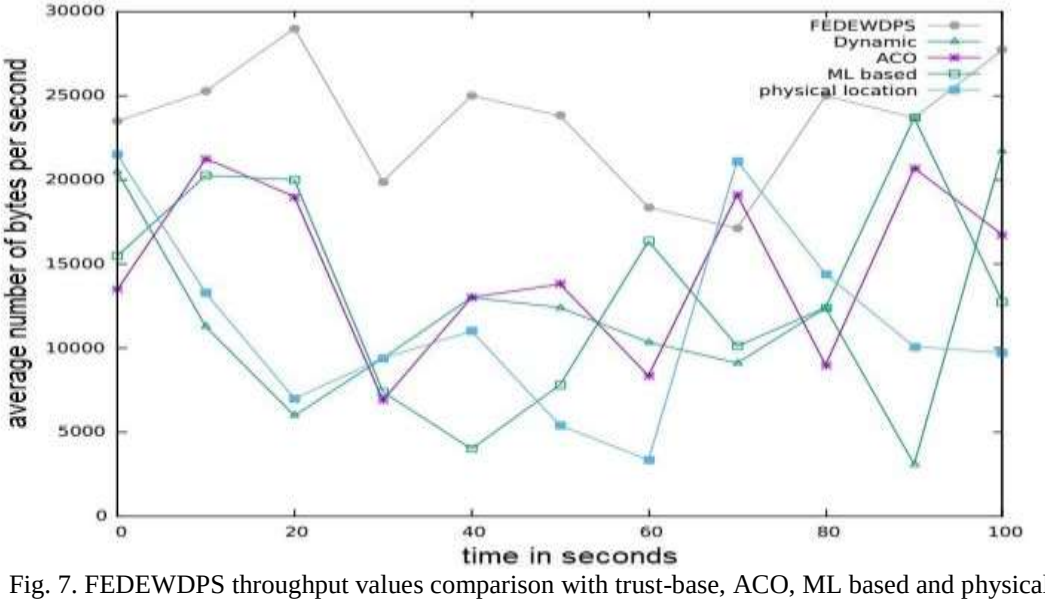

Fig. 7. FEDEWDPS throughput values comparison with trust-base, ACO, ML based and physical location based approaches.

False positive is an alert generated by an intrusion detection system (IDS) that incorrectly identifies normal traffic asan attack. In the case of a wormhole attack, false positives occur when legitimate packets passing through the network are flagged as malicious by the IDS.

The results provided in the fig. 8, the number of false positives generated by five different approaches such as FEDEWDPS , trust-base, ACO, ML based and physical location based approaches, when detecting the external wormhole attacks. The false positive rate is shown for each technique at different time intervals.

At the beginning of the experiment, all existing approaches have zero false positives, which are expected

since there was no wormhole attack present in the network. However, as the wormhole attacks began to propagate through the network, the false positive rates for each technique increased.

Based on comparison results, it appears that the FEDEWDPS generated the least false positives overall, with a maximum false positive rate of 10.4% at the end of the experiment. On the other hand, the physical location, ACO and ML based approaches generated higher false positive rates, with the dynamic trust Cryptosystem technique generating the most false positives of the three.

False negatives refer to instances where the system fails to detect an attack when an attack has actually occurred. We have compared the effectiveness of detecting wormhole attacks of FEDEWDPS, ACO, ML-based, and physical location-based approaches in Fig. 9. We have observed that the number of false negatives of our proposed FEDEWDPS only 12% even when the vehicle speed is very high which less when compared with the ACO, ML-based, physical location-based approaches.

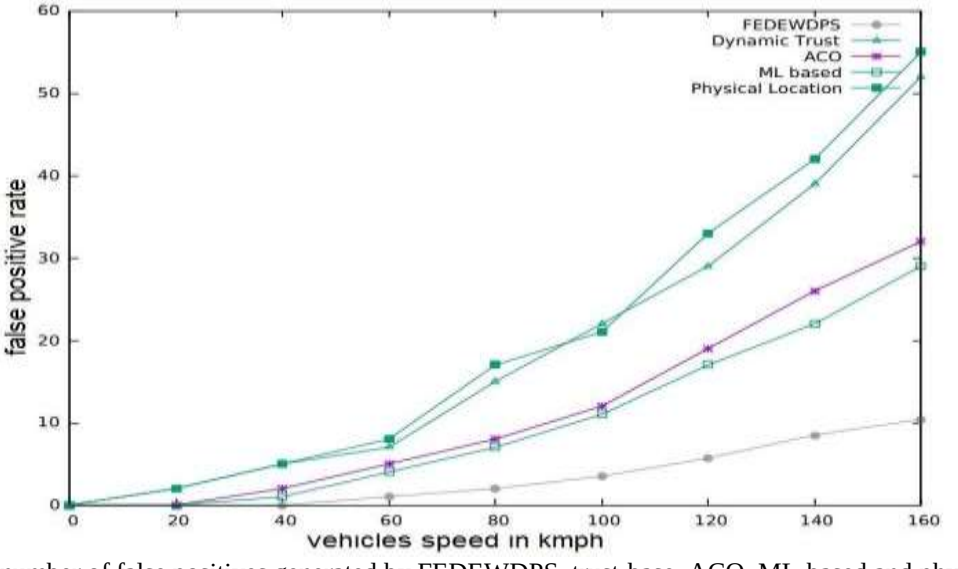

Fig. 8. The number of false positives generated by FEDEWDPS, trust-base, ACO, ML-based and physical location-based approaches.

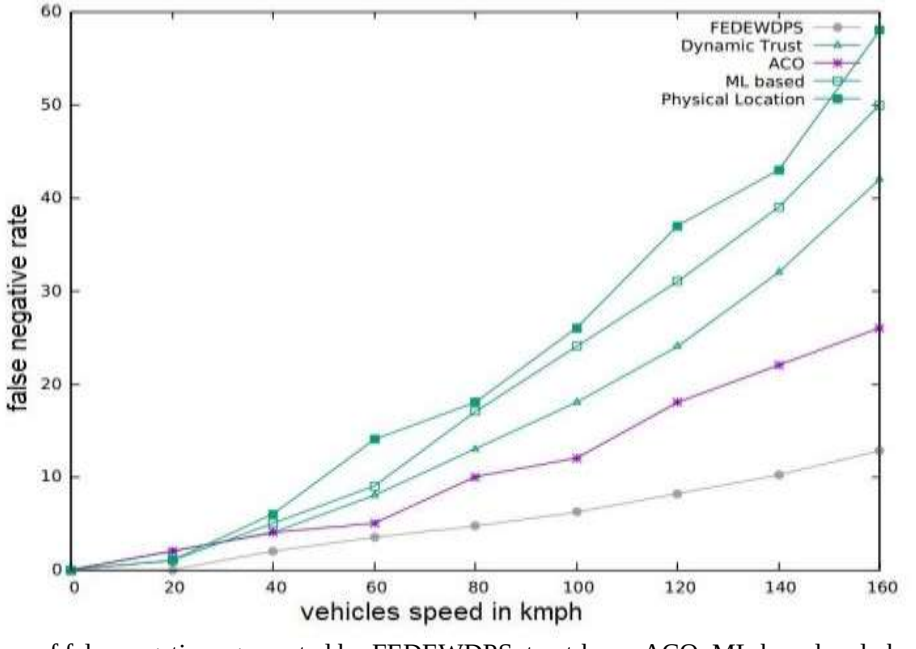

Fig. 9. The number of false negatives generated by FEDEWDPS, trust-base, ACO, ML-based and physical location-based approaches.

5. CONCLUSION

In this paper, we proposed a Fast and Efficient Distance-based External Wormhole Detection and Prevention System (FEDEWDPS) for detecting and preventing external wormhole attacks in Vehicular Ad-hoc Networks (VANETs). Existing VANET security solutions do not address this specific type of attack. Our proposed system uses vehicles themselves to act as monitors in a two-level approach for wormhole detection and prevention. At the first level, we use a dynamic threshold value based on the neighboring vehicle ratio using the ARIMA model to suspect a wormhole attack. If any vehicle covers more than this threshold value, it is considered a potential wormhole attack. This method is efficient because it does not verify remaining links for wormhole attacks, thereby conserving resources. At the next level, we verify the distance between the suspected nodes and their corresponding distances to detect and isolate the wormhole attacks. We analyzed the performance of our proposed FEDEWDPS and found that it has better throughput, packet delivery ratio (PDR), and jitter, with fewer false positives and negatives compared to existing methods such as ACO, ML-based, dynamic trust-based, and physical location-based approaches in a hostile environment.

Data Availability. Data underlying the results presented in this paper are available from the corresponding author upon reasonable request.

Funding. There is no funding for this work.

Conflicts of interest. The authors declare no conflict of interest.

Ethics. The authors declare that the present research work has fulfilled all relevant ethical guidelines required by COPE.

REFERENCES

[1] Sharma N, Sharma, M., & Sharma, D. P, **"A trust based scheme for spotting malicious node of wormhole in dynamic source routing protocol"**, *In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)* (I-SMAC), pp. 1232- 1237, IEEE, October ,2020.

[2] Zardari, Zulfiqar Ali, **"A lightweight technique for detection and prevention of wormhole attack in MANET",** *EAI Endorsed Transactions on Scalable Information Systems*, 2021.

[3] Mani G, **"Reliable Wormhole Detection System Based Secure Routing and Authentication for Environmental Monitoring",** *Journal of Green Engineering* 10 , 734-749, 2020.

[4] Adhikary, Kaushik, **"Hybrid algorithm to detect DDoS attacks in VANETs",** *Wireless Personal Communications* , 114 , 3613-3634, 2020.

[5] Akwirry, Brian, et al. **"A Multi-Tier Trust-Based Security Mechanism for Vehicular Ad-Hoc Network Communications.",** *Sensors* 22.21, 8285 , 2022.

[6] Rullo, Antonino, **"Optimal placement of securityresources for the Internet of Things",** *The Internet of Things for Smart Urban Eco systems* , 95-124, 2019.

[7] Ali Shahjahan, Parma Nand, and Shailesh Tiwari , **"Detection of wormhole attack in vehicular ad-hoc network over real map using machine learning approach with preventive scheme",** *Journal of Information Technology Management* , Vol. 14, no. *Security and Resource Management challenges forInternet of Things* , pp. 159-179, 2022.

[8] Secil Ercan, Marwane Ayaida, and Nadhir Messai, **"Misbehavior detection for position falsification attacks in VANETs using machine learning",***IEEE Access*, Vol. 10 , pages:1893-1904, 2021.

[9] Masoud Abdan and Seyed Amin Hosseini Seno, **"Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad-Hoc Network (MANET)",** *Wireless Communications and MobileComputing*, pp. 1-12, 2022.

[10] Kuldeep Narayan Tripathi, S. C. Sharma**, "A trust- based model (TBM) to detect rogue nodes in vehicular ad hoc networks (VANETS)"**, *Int J Syst Assur Eng Management,* 11(2), pp. 426–440, 2019.

[11] N. SreeDivya, VeeramalluBobba, Ramesh Vatambeti, **"An Adaptive Cluster based Vehicular Routing Protocol for Secure Communication",** *WirelessPersonal Communications*, 127, 1717–1736, 2021.

[12] Gaurav Soni, Arjun Rajput, **"An IPS Approach to Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET"**,*Contemporary Issues in Communication, Cloud and Big Data Analytics*, Vol. 281, pp. 57–65, 2020.

[13] Ankit Kumar a, Vijayakumar Varadarajan, **"Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm ",** *Microprocessors and Microsystems*, Vol. 80, 103352, 2021.

[14] Parma Nand and Shailesh Tiwari, **"Impact of wormholeattack on AODV routing protocol in vehicular ad-hocnetwork over real map with detection and preventionapproach ", Int**. *J. Vehicle Information and Communication Systems*, Vol. 5,

No. 3, pp. 354-373, 2020.
[15] Vasiliy Krundyshev, **"Artificial swarm algorithm for VANET protection against routing attacks ",** IEEE, 2018.
[16] P. Kaur, D. Kaur, and R. Mahajan, **"Simulation based comparative study of routing protocols under wormhole attack in manet,"** *Wireless Personal Communications*, vol. 96, pp. 47–63, 2017.
[17] Ting-Hui Chu, Shu-Yu Kuo, Yao-HsinChou , "**Using Quantum-inspired Tabu Search Algorithm with Logic Operation and Moving Average Indicator for Wormhole Attack Detection in a WSN"**, *Journal of Internet Technology*, Vol. 20, 2019.
[18] Kaur, Sanjay Batish& Arvind Kakaria, "**An Approachto Detect the Wormhole Attack in Vehicular Ad hoc Networks ",** *IJSSAN*, 2012
[19] Ratnasih , **"Performance Analysis of Reactive RoutingProtocol on VANET with Wormhole Attack Schemeaper",** *JURNAL INFOTEL*, 2018.
[20] Ravula Prathap Kumar, MunisamyShanmugam , **"A Detailed Case Study on VANET Security Requirements, Attacks and Challenges",** *Advances in Modelling and Analysis* B, Vol. 62, No. 2-4,December , pp. 48-52, 2019.
[21] R. PrathapKumar , D. Murli Krishna Reddy ,G.Parimala,S. Deva Kuma, **"IMPACTS OF WORMHOLE AND BLACK HOLE ATTACKS IN VANETS",** *Design Engineering*, ISSN: 0011-9342, Issue: 7, pp. 2128- 2146,2021.
[22] Xiao Luo, Yanru Chen, Miao Li, Qian Luo, Kang Xue, Shijia Liu, Liangyin Chen. **"CREDND: A Novel SecureNeighbor Discovery Algorithm for Wormhole Attack"** , *IEEE Access*, 2019.
[23] Basant Subba, Santosh Biswas , Sushanta Karmakar "**A game theory based multi layered intrusion detection framework for VANET"**, E*lsevier* , pp. 12-28, 2018.
[24] Ankit Kumar, Vijayakumar, **"Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm ",**, *Elsevier*, pp. 0141-9331, 2021.
[25] Muhammad Arifa, Guojun Wanga**,"A survey on security attacks in VANETs: Communication, applications and challenges",** ,*Elsevier*, 2214-2096, 2019.
[26] Ratnasih , Doan Perdana **"Performance Analysis of Reactive Routing Protocol on VANET with Wormhole Attack Schemeaper",** *JURNAL INFOTEL*, ISSN: 2085-3688, 2018.
[27] Shivaprasad More, Rahul Ganpatrao Son kamble, Uday Kumar Naik, Shraddha Phansalkar**, "Secured Communication in Vehicular Ad hoc Networks (VANETs) using Block chain"** ICCRDA, 2020.
[28] *Ankit Kumar, Madhavi Sinha* **"Design and development of new framework for detection and mitigation of wormhole and blackhole attacks in VANET",** *Journal of Statistics and Management Systems*, ISSN: 0972-0510, 2019.
[29] Heena Khanna, Manmohan Sharma, **"An Improved Security Algorithm for VANET using Machine Learning",** *Journal of Positive School Psychology*Vol.6, No.3, pp. 7743 – 7756, 2022.
[30] Gaurav Soni, Kamlesh Chandravanshi, **"An IPS Approach to Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET",** 2021.
[31] Shahjahan Ali, Parma Nand, Shailesh Tiwari**, "Detection of Wormhole Attack in Vehicular Ad-hoc Network over Real Map using Machine Learning Approach with Preventive Scheme",** *Journal of Information Technology Management*, 2008-5893, 2021.
[32] Arun Singh Kaurav, Sushama Rani Dutta, "**Detection and prevention from different attacks in VANET: A Survey",** *Journal of Physics: Conference Series*, 2021.
[33] Krishna K, V., & Reddy K, G. , **"VANETVulnerabilities Classification and Countermeasures: A Review ",** *Majlesi Journal of Electrical Engineering* , *16*(3) , 63-83, 2022.
[34] Hajiee, M., Fartash, M., & Osati Eraghi, , "**Trust-based Routing Optimization using Learning Automata in Wireless Sensor Network",** *Majlesi Journal of Electrical Engineering*, *15*(4), 87-98, 2021.