Review

AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks

Maria Hanif [1], Humaira Ashraf [1], Zakia Jalil [1], Noor Zaman Jhanjhi [2,*], Mamoona Humayun [3], Saqib Saeed [4] and Abdullah M. Almuhaideb [5]

[1] Department of Computer and Software Engineering, International Islamic University, Islamabad 44000, Pakistan; maria.mscs1078@iiu.edu.pk (M.H.); humaira.ashraf@iiu.edu.pk (H.A.); zakia.jalil@iiu.edu.pk (Z.J.)

[2] School of Computer Science, SCS Taylor's University, Subang Jaya 47500, Malaysia

[3] College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia; mahumayun@ju.edu.sa

[4] SAUDI ARAMCO Cybersecurity Chair, Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; sbsaed@iau.edu.sa

[5] SAUDI ARAMCO Cybersecurity Chair, Department of Networks and Communications, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; amalmuhaideb@iau.edu.sa

* Correspondence: noorzaman.jhanjhi@taylors.edu.my

Abstract: The popularity of wireless sensor networks for establishing different communication systems is increasing daily. A wireless network consists of sensors prone to various security threats. These sensor nodes make a wireless network vulnerable to denial-of-service attacks. One of them is a wormhole attack that uses a low latency link between two malicious sensor nodes and affects the routing paths of the entire network. This attack is brutal as it is resistant to many cryptographic schemes and hard to observe within the network. This paper provides a comprehensive review of the literature on the subject of the detection and mitigation of wormhole attacks in wireless sensor networks. The existing surveys are also explored to find gaps in the literature. Several existing schemes based on different methods are also evaluated critically in terms of throughput, detection rate, low energy consumption, packet delivery ratio, and end-to-end delay. As artificial intelligence and machine learning have massive potential for the efficient management of sensor networks, this paper provides AI- and ML-based schemes as optimal solutions for the identified state-of-the-art problems in wormhole attack detection. As per the author's knowledge, this is the first in-depth review of AI- and ML-based techniques in wireless sensor networks for wormhole attack detection. Finally, our paper explored the open research challenges for detecting and mitigating wormhole attacks in wireless networks.

Keywords: wormhole attacks; WSNs; detection techniques

1. Introduction

Several types of distributed denial-of-service (DDoS) attacks are currently being launched against wireless sensor networks. The sinkhole, black hole, grey hole, wormhole, Sybil, and clone assaults are examples of these attacks. The wormhole attack in WSN includes more than one malicious node, establishing an active path between them over long ranges. These malicious nodes then affect the routing algorithm. Wormhole attacks can be categorised into three types, i.e., open wormhole, half wormhole, and closed wormhole.

The continuous development of wireless communication tends to increase in WSN implementation [1]. WSN is self-organised and consists of a self-organised network con-

sisting of devices called sensor nodes [2]. Sensor nodes are low-cost and low-power devices [3]. These nodes can gather information, and processing-band sensors can collect information and their processes include preprocessing [4]. Sensor nodes are used to transmit data all over the network. They can act as routers that forward neighbours' data to the base station, the gateway to transferring data to remote servers [5]. WSN has a wide range of applications due to its dynamic structure and high-quality data transfer. WSN uses include environmental monitoring, smart homes, and healthcare [6]. Moreover, WSNs are implemented for military, urban, and industrial purposes [7]. In the military, WSNs are used for surveillance, combat monitoring, and intruder detection. In healthcare, WSNs are used for patient monitoring and home assisting systems. In their environment applications, WSNs are used for water, air monitoring, and emergency alerting systems [8].

Due to their dynamic infrastructure and multiple functionalities, WSNs are easy to deploy. However, due to their limited capabilities and low-cost, low-power sensor nodes, they are vulnerable to DOS attacks [9,10]. These security risks are becoming more prevalent daily, causing disruptions throughout the network by changing data, disclosing confidential information, providing access to illegitimate users, or allowing illegal access [11]. These DOS attacks include wormholes, black holes, jamming, and clone attacks. The wormhole attack is the most severe attack against WSNs. The attacker can attack the network without disrupting the integrity of the communication in the network topology [12]. It is the most challenging attack to counter because the attacker can secretly launch an attack on only two malicious nodes and make a tunnel between them to forward data [13]. The attacker can send data, control traffic, modify data, and manipulate information as a legitimate system [14]. Due to their nature as a challenge difficult to combat, it is difficult to detect wormhole attacks [15]. Further research has been conducted to detect wormhole attacks and prevent them from manipulating WSNs.

Wormhole nodes make a fake path shorter than the actual path within the network. This path disturbs the routing topology, which works according to the distance between the nodes. A wormhole path consists of two nodes and a tunnel between them. The first malicious node receives data packets from one location and sends them to the second malicious node, which is at a distant location. The second malicious node then sends these data packets locally. A wormhole attack can quickly be built by an attacker without having any knowledge about the network and without even disturbing any nodes of the network. Therefore, a wormhole attack is severe. This attack has different modes. Figure 1 depicts the types of wormhole attacks. In hidden modes, packet encapsulation and packet relay are included. In packet encapsulation, each data packet is sent through legal paths only. When one wormhole node receives a data packet, it encapsulates the packet to stop the increasing hop count. This packet remains basic in its actual form due to the second node of the wormhole tunnel. In packet relay mode, a wormhole attack can be launched using one node only. This malicious node relays packets of far-located nodes to make them neighbours. This is their neighbour node, which means that other nodes can send data packets to that node. In participation modes, high-power transmission and out-of-band are included. In high-power transmission, a single malicious node with a high transmission capability attracts the data packets to follow its path. In the out-of-band mode, two malicious nodes make an out-of-band channel with high bandwidth to create a wormhole tunnel between them. Figure 2 demonstrates the wormhole attack in WSN.
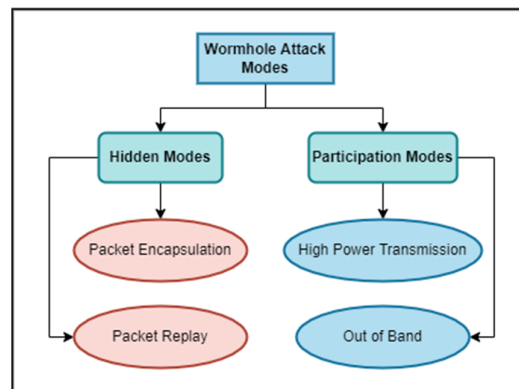
Figure 1. Classification of wormhole attacks based on hidden and participating nodes.

Mohit et al., reviewed different techniques for the detection of wormhole attacks, a significantly dangerous attack affecting the mission of the network [16]. Alomar et al., focused on the security of wormhole detection techniques in WSNs by compromising their energy efficiency [17]. Goyal et al., reviewed schemes for recognizing a wormhole attack in IoT networks [18]. Farjamnia et al., provided a review of several techniques for the recognition and avoidance of wormhole attacks in WSNs [19].
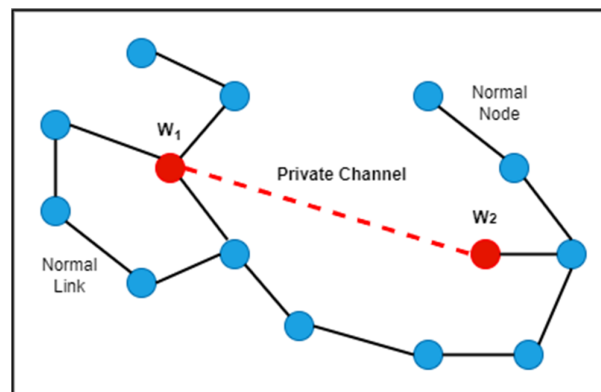
Figure 2. External wormhole attack with high power transmission.

Table 1 presents a summary of the existing surveys of wormhole detection schemes. The main focus of the existing surveys is stated in the brief. The difference between the existing surveys and this paper is also presented.

According to Table 1, it is clear that there are several gaps in the existing surveys. The surveys are not presented systematically and do not provide detailed and comprehensive critical and comparative analyses. The listed surveys do not include the latest techniques such as artificial intelligence-based schemes and machine learning schemes for mitigating wormhole attacks. Therefore, we present this systematic literature review to fill the gaps in the existing surveys by contributing to the field. This study provides state-of-the-art approaches and the most recent schemes for mitigating wormhole attacks in WSNs.

Table 1. Summary of surveys of wormhole detection techniques.

Year	Main Focus of Survey	Major Contributions	Enhancements in Our Paper
2020	Survey wormhole attack detection and prevention techniques in WSN	Mohit et al. [16] reviewed schemes such as WGDD, RTT, Packet leaches, AOMDV, ANN, and high-power transmission. The advantages and disadvantages of these schemes are listed along with the author's remarks about the schemes. However, a performance analysis based on quality assessment was not included.	Our survey presents a detailed performance analysis, including critical analysis and results comparison, and identified the gaps in all existing schemes.
2018	Detection and prevention analysis of wormhole attacks in wireless sensor networks	Kumar et al. [17] presented a comparative analysis of several techniques, including reputation-based routing, Packet leaches, Beacon nodes, LITEWORP, and algorithms using active nodes. However, the study did not include the strengths and limitations of the existing schemes.	Our survey presents a detailed critical analysis and comparative analysis of the schemes and identified gaps.
2018	Review intrusion detection of wormhole attacks in IoT	Goyal et al. [18] compared several existing techniques, including the use of the hound packet, distributed detection algorithm, modified AODV, node connectivity, Merkle tree, and AODV protocol for recognising and preventing wormhole attacks, including the constraints of all the schemes. However, strengths were not specified.	Our survey presents a comprehensive comparative analysis of all existing schemes and detailed critical analysis.
2019	Review techniques used against wormhole attacks on wireless sensor networks	Farjamnia et al. [19] presented a review of the existing models (including AOVD with different sizes, ADT, T-AOVD, AOMDV, and DV-Hop with different sizes). The advantages and disadvantages of the models were specified.	Our survey presents a detailed literature review along with a solution to identify gaps in the existing schemes.
2020	Schemes to detect wormholes in WSNs	Umashankar et al. [20] presented a detailed review of the literature on wormhole attack detection. However, the latest schemes were not included. The advantages and disadvantages of the existing schemes were not specified.	Our survey presents all the latest schemes, including AI- and ML-based schemes, and a detailed critical analysis of all existing schemes.
2019	Survey the detection and prevention of wormhole attacks in mobile ad hoc networks	Anju et.al. [21] presented several existing schemes of wormhole recognition, including AODV, RTT, Neighbour Discovery, and Hop count. However, the strengths of the schemes were not specified, and the presented survey was not systematic.	Our survey presents all existing schemes in detail and identifies a better technique. Moreover, challenges are specified for future research.
2018	Survey approaches and measures in detecting wormhole attacks in WSNs	Diksha et al. [22] presented a literature review on different location time, cluster-base, public key encapsulation, moving average indicator, hop count, and RTT-based approaches. However, it is not a systematic survey and not all the pros and cons of the schemes were elaborated in detail.	Our survey presents a detailed literature review of existing techniques along with a comprehensive critical analysis. It also includes AI- and ML-based schemes.
2018	Techniques and challenges in detecting wormhole attacks in WSNs	Padmarpriya et al. [23] presented challenges in WSN concerning the limited bandwidth, time, power management, design constraints, and security. The schemes of wormhole recognition were presented on a category basis. However, there was neither a critical analysis of schemes nor a quality assessment of research articles.	Our survey presents a comprehensive critical analysis of all existing schemes. Moreover, research gaps and challenges are identified.

The use of WSNs has been increasing day by day in the field of medical and military [24]. Eal et al., conducted an extensive survey that provides a deep insight into different WSNS applications in the real world and the nature of the security needed for those WSNs [25]. This SLR aims to identify gaps in the research on the detection and prevention of wormhole attacks in WSNs. To identify gaps in the research, the research papers of the last four years—sourced from three databases, i.e., IEEE, Springer, and Elsevier, were systematically searched. All strings with three synonyms were searched for, and seven papers were selected for each string. Newspapers, theses and white works were not included. Repeated papers in all strings were excluded. The articles were then filtered out based on title and abstraction. This SLR reviews all the schemes for recognizing and avoiding wormhole attacks in WSNs. All the techniques were deeply studied based on set objectives. This work provides a comprehensive critical analysis of the existing methods.

After the critical analysis of all techniques, this SLR presents a detailed performance analysis of all wormhole mitigation schemes, followed by a section presenting the identified challenges. Finally, this SLR concludes that many researchers have presented different techniques based on different objectives. Several methods are evaluated based on detection accuracy, performance, additional hardware used, packet delivery ratio, and energy consumption. Figure 3 presents the organization of the paper.
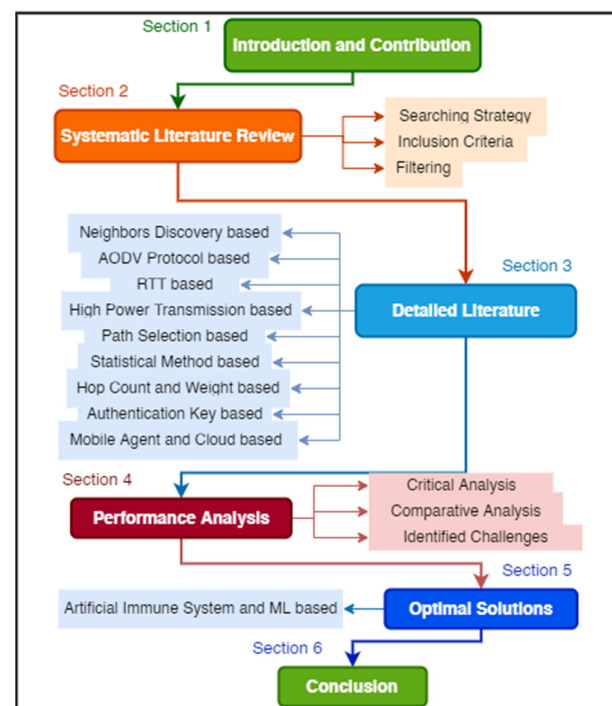
Figure 3. Paper organization.

The main contributions of our work are as follows:

1. A detailed review is performed to analyse the problems in state-of-the-art techniques for wormhole attack detection.
2. In this paper, AI and ML techniques are proposed as the optimal solution to the state-of-the-art problems in wormhole detection in wireless sensor networks.
3. The open research challenges are identified, and the literature addressing them is listed.

This paper is organized as follows: Section 2 provides a systematic literature review; Section 3 provides detailed literature, and Section 4 provides performance analysis. The

performance analysis is divided into subsections based on the critical analysis, comparative analysis, and identified challenges. Section 5 discusses the optimal solutions, followed by the last section, Section 6, which provides conclusions. Table 2 represents the acronyms used in this paper and their definitions.

Table 2. Notations and their definitions.

Acronyms	Definition	Acronyms	Definition	Acronyms	Definition
AODV	Advance On-Demand Distance Vector	FPR	False Positive Rate	PSO	Particle Swarm Optimization
AOMDV	Advance On-Demand Modified Distance Vector	HCBS	Heterogeneous Cluster-Based Secure Protocol	PDR	Packet Delivery Ratio
AD-PSO	Advance Distance Particle Swarm Optimization	HKP-HD	Hybrid Key Pre-Distribution	P	Performance
ANN	Artificial Neural Network	IPS	Intrusion Prevention System	PC	Poor Connectivity
ACI	Augmented Concentration Index	KNN	K Nearest Neighbour	PLR	Packet Loss Ratio
CREDND	Creating Credible Discovery using Neighbour Discovery	LEC	Less Energy Consumption	RTT	Round Trip Time
DOS	Denial-Of-Service	LR	Fewer Resources	RPL	Routing Protocol for Low Power and Lossy Networks
DA	Detection Accuracy	LC	Less Complexity	RSSI	Received Signal Strength Indicator
DR	Detection Rate	LITEWORP	Light Weight Countermeasure for Wormhole Detection	RHE2WADI	RSSI and Hop Count-based Energy-Efficient Wormhole Attack Detection in IoT
DT	Decision Tree	LSTM	Long Short-Term Memory	SLR	Systematic Literature Review
DV-HOP	Distance Vector–Hop	LDA	Linear Discriminant Analysis	S	Speed
DRFOIDL-ID	Delta Rule First Order Iterative Deep Learning-Intrusion Detection	LITS	Location Information and Time Synchronization	SVM	Support Vector Machine
DELPHI	Delay Per Hour Indicator	MANET	Mobile Ad Hoc Network	SWAN	Statistical Wormhole Apprehension Using Neighbours
DMK	Dynamic Matrix Key	MDD	Mean Detection Delay	VCL	Visiting Centre Local
ETS	Energy Trust System	MAXIS	Maximum Independent Sets	WSN	Wireless Sensor Network
EPSMAW	Energy Preserving Secure Measure Against Wormhole	MAPS	Mobile Agent Packet Structure	WLAN	Wide Local Area Network
EIGRP	Enhanced Interior Gateway Routing Protocol	NB	Naïve Bayes	CNN	Convolutional Neural Network
EFM	Encapsulation and Fragmentation of Message	NIAPC	Neighbourhood Information and Alternate Path Calculation	FFNN	Feed Forward Neural Network
EDAK	Efficient Dynamic Authentication and Key Management	NSI	Neighbour Similarity Index	WCA	Weighted Cluster Algorithm

2. Systematic Literature Review

The research literature presented in this paper is reviewed systematically. First, a searching protocol was developed according to which the systematic searches were conducted. These searchers were led using the development of strings according to the identified research question. Afterwards, a search strategy was made to categorise all the searches according to the search journals. Moreover, research articles were included according to their inclusion criteria and filtered according to their title, abstract, and objectives.

2.1. Searching Protocol

A searching protocol was designed according to which papers published over four years (2018, 2019, 2020, and 2021) were selected for searching. In addition, three synonyms of each keyword and four databases (IEEE, Springer, Elsevier, and Science Direct) were used for searching. Only seven papers were selected against each string. Figure 4 presents the search strategies.
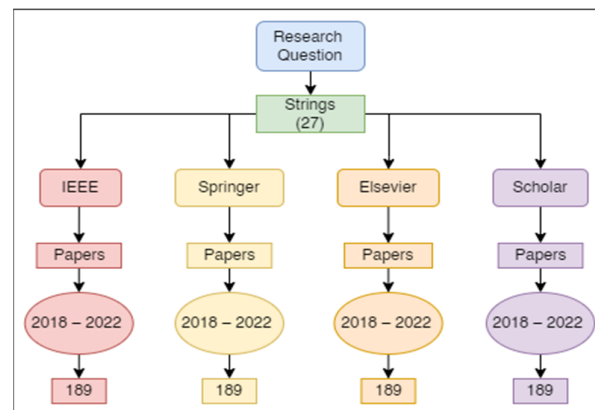
Figure 4. Search strategy using various databases.

2.2. String Development

The strings were developed by using three synonyms of each keyword.

Research Question: Which methods provide the detection of wormhole attacks in WSNs?

2.3. Inclusion Criteria

An inclusion criterion was made according to which all papers from journals were included. No white papers were included. Those papers which are not yet published are not included.

2.4. Filtering

In the filtering phase, the first stage was title-based filtering, as shown in Figure 5. All papers which were not relevant to the topic of the problem were excluded from all the selected databases.

Figure 5. Screening for research articles selection in order to deduce the research objectives.

In the second part, abstract-based filtering was conducted. All the papers in which the abstracts were irrelevant to the problem were excluded from all the selected databases. In the third part of the filtering, objective-based filtering was conducted, as shown in Figure 5.

All the papers were filtered according to their objectives, and a table was produced which shows papers categorised by their objectives.

After the title and abstract-based clustering, the objectives of the research papers were identified and categorised into clusters. Table 3 shows this objective-based screening. The categories of objectives were as follows: detection rate (DR), packet delivery ratio (PDR), low energy consumption (LEC), no additional hardware (NAH), detection accuracy (DA), false positive rate (FPR), mean detection delay (MDD), end-to-end delay (EED)fewer resources (LR), less complex (LC), speed (S) and poor connectivity (PC).

Table 3. Objective-based screening.

Ref.	DR	PDR	LEC	NAH	DA	P	FPR	MDD	EED	LR	LC	S	PC
[26]	-	✓	-	-	✓	-	✓	-	-	-	-	-	-
[27]	-	-	✓	-	✓	-	-	-	-	-	-	-	-
[28]	✓	-	-	✓	-	-	-	-	-	-	-	-	-
[29]	✓	✓	✓	-	-	-	-	-	✓	-	-	-	-
[30]	-	-	-	-	✓	-	✓	-	-	-	-	-	-
[31]	✓	-	-	-	-	-	-	-	-	-	-	-	-
[32]	-	-	-	-	✓	-	-	-	-	-	-	-	-
[33]	-	-	-	-	-	-	-	-	-	-	-	-	-
[34]	✓	-	-	-	-	-	-	-	-	-	-	-	-
[35]	✓	-	-	-	-	-	-	✓	-	-	✓	-	-
[36]	-	-	-	-	✓	-	-	-	-	-	-	-	-
[37]	-	-	✓	✓	✓	-	-	-	-	-	-	-	-

[38]	-	-	✓	-	-	-	-	-	-	-	-	-	-
[39]	-	-	-	-	✓	-	✓	✓	-	-	-	-	-
[40]	-	-	-	-	-	-	-	-	✓	-	-	✓	-
[41]	-	-	-	-	-	-	-	-	-	-	-	-	✓
[42]	✓	✓	-	-	-	-	-	-	-	-	-	-	-
[43]	-	-	✓	-	-	-	-	-	✓	-	-	-	-
[44]	-	-	-	-	-	-	✓	-	-	-	✓	-	-
[45]	-	-	✓	-	-	-	-	-	-	-	✓	✓	-
[46]	-	-	-	-	-	-	-	-	-	✓	-	-	-
[47]	-	-	✓	-	-	-	-	-	-	-	-	-	-
[48]	-	✓	-	-	-	✓	-	✓	-	-	-	-	-
[49]	-	-	-	✓	-	-	-	-	-	-	-	-	-
[50]	✓	-	-	-	-	-	-	-	-	-	-	-	-
[51]	-	✓	-	-	-	-	-	-	-	-	-	-	-
[52]	-	✓	-	-	-	-	-	-	-	-	-	-	-
[53]	-	✓	-	-	-	-	-	-	✓	-	-	-	-
[54]	✓	-	-	-	-	-	-	-	-	-	-	-	-
[55]	✓	-	-	-	-	-	-	-	-	-	-	-	-
[56]	-	-	-	✓	-	-	-	-	-	-	-	-	-
[57]	-	-	✓	-	-	-	-	-	-	-	-	-	-
[58]	-	✓	-	-	-	-	-	-	-	-	-	-	-
[59]	-	-	-	-	✓	-	-	-	-	-	-	-	-
[60]	-	✓	-	-	-	-	-	-	✓	-	-	-	-
[61]	-	-	-	-	✓	-	-	-	-	-	-	-	-
[62]	✓	-	-	-	-	-	-	✓	-	-	-	-	-
[63]	-	✓	-	-	-	-	-	-	✓	-	-	-	-
[64]	-	-	✓	-	✓	-	-	-	✓	-	-	-	-
[65]	-	-	-	-	-	-	-	-	-	-	✓	-	-
[66]	✓	-	-	-	-	-	-	-	-	-	-	-	-
[67]	✓	✓	-	-	-	-	-	-	✓	-	-	-	-
[68]	-	-	✓	-	✓	-	-	-	-	-	-	-	-
[69]	-	-	-	-	✓	-	-	-	✓	-	-	-	-
[70]	-	-	-	-	-	✓	-	-	-	-	-	-	-
[71]	-	-	-	-	-	✓	-	-	-	-	-	-	-
[72]	-	-	-	-	-	✓	-	-	-	-	-	-	-
[73]	-	-	-	-	-	✓	-	-	-	-	-	-	-
[74]	-	-	-	-	-	✓	-	-	-	-	-	✓	-
[75]	-	-	✓	-	-	-	-	-	-	-	-	-	-

3. Detailed Literature

The main aim of all the papers was to recognize and prevent wormhole attacks in wireless sensor networks.

3.1. Artificial Immune Systems and Machine Learning-Based Systems

The research of Ref. [26] presented an artificial immune system with fuzzy logic for mitigating wormhole attacks with high FPR and PDR and less PLR. The system was designed by modifications to the AODV protocol with fuzzy logic to develop an immune system. The results were simulated using the NS2 simulator. The delivery ratio of the AODV protocols decreases with a high increase in the number of connections. In the process of finding the right path, the shortest path can be lost due to network traffic.

The research of Ref. [27] presented a hybrid RPL protocol for mitigating wormhole attacks with high DA and using less computation power. It uses a support vector machine, a supervised machine learning algorithm for detecting intruders. RPL is a complex protocol that increases the network's control packets, resulting in overhead and increased energy consumption.

The research of Ref. [28] presented an ANN approach for wormhole mitigation. It uses the connectivity information of sensor nodes as a distance measure for hop counts. The simulations of the proposed approach were conducted on 500 nodes using MATLAB. The ANN's training and testing results show that this approach can detect wormholes with a high detection accuracy—up to 97%—and without using any additional hardware.

The research of Ref. [29] presented a deep learning approach for wormhole mitigation. It uses RTT and LSTM for the detection process. It also uses the Whale optimization algorithm with fitness rate modification to select the optimized path. The analysis of the scheme was conducted using Python. The results show that this optimised LSTM approach provides a high detection accuracy and PDR. It also consumes less energy and provides less E2E delay.

The research of Ref. [30] presented a wormhole mitigation approach named Delta Rule First Order Iteration Deep Neural Learning Intrusion Detection (DRFOIDL-ID). It uses a deep neural network for the detection of intruders and removes them by the isolation process. The DRFOIDL-ID was compared with the energy trust system (ETS) and RPL-based system. The results showed that DRFOIDL-ID provides a high detection accuracy and less FPR and PLR.

The research of Ref. [31] presented a machine learning-based approach for wormhole mitigation in MANET. It uses KNN, SVM, DT, LDA, NB, and CNN for the classification of malicious nodes from the extracted features of the collected data of the nodes. The simulations of all the methods were conducted in MATLAB 2019b. The results showed that the decision tree (DT) provides high detection accuracy: of up to 98.9%.

The research of Ref. [32] presented a novel intrusion detection system that uses fuzzy logic with a feed-forward neural network. The fuzzy rules are used to train the neural network, and the neural network's performance was evaluated through simulation. The results were compared with simple machine learning techniques, which showed that this novel approach provides a detection accuracy of up to 98.8%.

The research of Ref. [33] presented an unsupervised learning-based scheme that uses a weighted clustering algorithm for wormhole attack detection. It is an energy-efficient scheme that makes clusters of networks and collects data on the base station without any intervention in the network's activity. These data are then classified using SVM and MLP (multilayer perceptron). The results of this approach showed an accuracy of up to 90%, but in a real-time system, it showed an accuracy of up to 75%.

The research of Ref. [34] presented a supervised machine learning-based scheme which detects wormhole attacks in VANET over an accurate map. It uses the random forest and K-nearest neighbour classifiers for malicious node detection. This paper also proposed a packet leash and cryptographic concept-based scheme to prevent wormhole attacks. The simulation results showed that the proposed scheme for detection provides a detection accuracy of up to 99.1%.

The research of Ref. [35] presented a supervised machine learning-based scheme which uses the naïve Bayes classifier with EC-BRTT (enhanced code-based round trip time) for malicious node detection. The simulation of the presented technique showed effective results in terms of communication overhead, data delay, and attack detection.

The research of Ref. [36] presented a supervised-based machine learning algorithm for intrusion detection. It uses decision tree algorithms named C4.5 and CART to identify network patterns. The results of the proposed approach were compared in terms of different network parameters, such as accuracy, number of nodes, number of training samples, and number of attackers. The results show that C4.5 attained a higher accuracy

(70%) than the CART classifier. Figure 6 shows the classification of AI-based schemes for wormhole detection in WSNs.
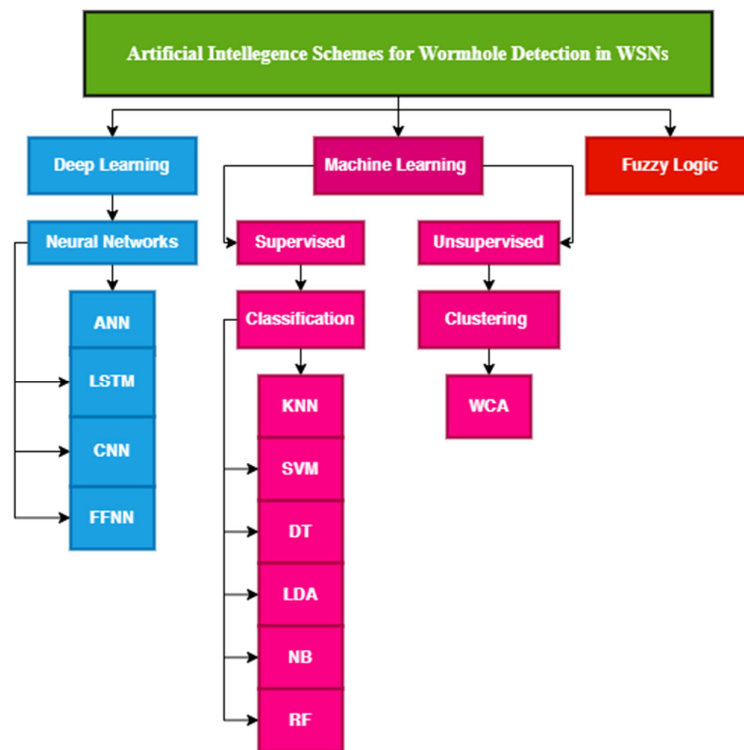

Figure 6. Classification of AI- and ML-based wormhole detection schemes.

3.2. Neighbor Discovery-Based Systems

The research of Ref. [37] presented a less energy-consuming technique, using no additional hardware and providing higher detection accuracy. A localized protocol for creating credible discovery (CREDND) is proposed. It recognizes wormholes outside—as well as inside—the network. The presented scheme, CREDND, was compared with the accuracy of the already existing SECUND and SEINE techniques, which also use local monitoring and hop difference. CREDND did not work well with dynamic changes in the communication range of nodes.

The research of Ref. [38] presented an energy-friendly trust-based technique with reduced overhead on network traffic. A trust-based mechanism is used to detect wormhole and grey hole attacks in IoT networks. It uses the routing protocol for low power and lossy networks (RPL) as a routing protocol for IoT networks. It computes direct and indirect trust based on the properties of nodes and the opinions of neighbour nodes, respectively.

The research of Ref. [39] presented a technique that provides a lower false positive rate, shorter mean detection delay, and higher detection accuracy. A decentralised statistical scheme detects wormholes in MANETs using an NS3 simulator. It uses already existing statistical wormhole apprehension using the neighbors (SWAN) algorithm with some modifications. A decentralised statistical technique showed a loss of control and costlier operations.

The research of Ref. [40] presented an MLAMAN technique that detects wormhole attacks in dynamic tunnel lengths and changes nodes' speed. It detects intruders by calculating hop difference and using the AODV protocol in three levels, i.e., packet level, neighbour level, and membership level, for the authentication of intermediate nodes. The results of the MLAMAN protocol were simulated using an NS2 simulator. This protocol

provides an accuracy of 100% in a static network and an accuracy of 98% in a dynamic network. The delivery ratio of the AODV protocols decreases with a high increase in the number of connections. In the process of finding the right path, the shortest path can be lost due to network traffic. The AODV protocol does not provide scalability, load balancing, or congestion control.

The research of Ref. [41] presented a detection scheme in 3D networks for wormhole detection by using only the connectivity information of the node. The proposed maximum independent sets (MAXIS) use a greedy algorithm. The proposed technique can be easily implemented. The detection rate was calculated for several node densities. The results showed that the proposed technique can provide an accuracy of 90%. The greedy algorithm fails to find an optimal solution.

The research of Ref. [42] proposed a scheme—named neighbourhood information and alternate path calculation (NIAPC), which provides high accuracy, PDR, and throughput. The presented scheme is based on the AODV protocol. The simulation was conducted for 100 nodes, showing a high detection accuracy without specific storage requirements.

The research of Ref. [43] presented a scheme—named energy preserving secure measure against wormhole (EPSMAW)—which provides low end-to-end delay, less energy consumption, and traffic overhead. The presented scheme uses the AODV routing protocol and is based on neighbour and connectivity information. The simulations were conducted for 150 nodes, showing high throughput and a lower false positive rate.

The research of Ref. [44] presented a software-defined network-based approach for wormhole detection. It uses information regarding neighbour similarity. The simulations of the presented approach were conducted on 100 and 1000 nodes, which were implemented using Python. The K-means clustering was applied after computing the neighbour similarity index (NSI) and augmented concentration index (ACI) values. The results showed that SWAN can detect wormholes with less communication overhead and low FPR and FNR.

3.3. AODV Protocol-Based Systems

The research of Ref. [45] presented an improved AODV protocol technique that is less complex and consumes less energy. An ad-hoc on-demand distance vector (AODV) protocol detects and prevents blackhole and wormhole attacks. Several denial-of-service attacks are also compared. The delivery ratio of AODV protocols decreases with a high increase in the number of connections. In the process of finding the right path, the shortest path can be lost due to network traffic.

The research of Ref. [46] presented a confirmation system for detecting wormhole attacks using a honeypot. It creates trees attacked by wormholes and honeypots in order to make a decision. It used the AODV protocol and resilient ethernet protocol to search for the wormholes of a tree. The system was simulated for 50–200 nodes. This proposed system provides accurate results in different network sizes. It provides scalability and a reduction in the production of false alarms. The delivery ratio of the AODV protocols decreases with a high increase in the number of connections. In the process of finding the right path, the shortest path can be lost due to network traffic.

The research of Ref. [47] presented a review of the performance of wormhole attacks in three different protocols: AODV, OSLR, and ZRP (a hybrid protocol IARP and IERP). The results were simulated using the qualnet 5.0 simulator (Scalable Network Technologies, Inc., Los Angeles, CA, USA). The results were evaluated based on end-to-end delay, throughput, and energy consumption. The results showed that AODV and ZRP are better than OSLR. ZRP has more throughput than the other two protocols. The delivery ratio of AODV protocols decreases with a high increase in the number of connections. In the process of finding the right path, the shortest path can be lost due to network traffic.

The research of Ref. [48] presented a lightweight scheme for wormhole mitigation in MANET. The sender nodes collect all reply packets and their sequence numbers and

compare them with the calculated average sequence number to detect intruders. This lightweight scheme is compared with the AODV in the NS2 Simulator. The results showed that the proposed mechanism provides high throughput, high PDR, less routing overhead, and average delay.

3.4. RTT-Based Systems

The research of Ref. [49] presented an RTT-based technique that uses clock synchronisation and does not require additional hardware. A round-trip time (RTT) centred mechanism was proposed in order to recognise dynamic wormhole attacks. It detects the wormhole attack by comparing the actual and expected RTT of the nodes. The performance of the mechanism was simulated using the NS2 simulator. The results were improved regarding packet delivery ratio, average energy consumption, throughput, routing overhead, and jitter. The RTT is inhibited due to network traffic. If a server requests an increase, it results in increased RTT and affects the efficiency of the RTT. The RTT also increases when a node experiences network congestion due to the network traffic slowing down the connection. The increased distance between the nodes increases the RTT.

The research of Ref. [50] proposed a new protocol for the detection of wormhole attacks in wireless mesh networks, providing high detection rates. The proposed protocol used the round-trip time (RTT) method in conjunction with the propagation time. The simulations of four different scenarios with different numbers of nodes were performed on NS3 simulators to test the effectiveness of the proposed protocol. The RTT was inhibited due to network traffic. If a server requests an increase, it results in increased RTT and affects the efficiency of the RTT. The RTT also increases when a node experiences network congestion due to network traffic slowing down the connection. The increased distance between nodes increases the RTT. Table 4 briefly presents a summary of methodologies of wormhole detection schemes.

Table 4. Summary of methodologies of wormhole detection schemes.

	Ref.	Scheme	Methodology
Neighbours discovery based	[37]	CREDND (creating a credible neighbour discovery) protocol	This scheme uses a neighbour ration threshold to evaluate which nodes should be checked. After this, an external wormhole is recognized by hop count as external malicious nodes acting in hidden mode and using the out-of-band channel. In the last step, an internal wormhole is recognized by authentication packets as internal malicious nodes act as normal nodes and use packet encapsulation.
	[38]	Trust-based scheme	This lightweight trust-based scheme computes direct trust (DT) by considering the node properties and indirect trust (IT) and by considering the opinions of neighbour nodes. Every node keeps track of its neighbours and checks that they work according to the RPL network rules. The sum of DT and IT is calculated, and the decision is made based on TT (total trust).
	[39]	Decentralized statistical scheme	This scheme uses two parameters, i.e., the number of new neighbours and the number of old neighbours. The SWAN algorithm is used for detecting the number of neighbours. The decision rule is used with a sliding window to make the decision.
	[40]	MLAMAN scheme	This scheme works by changing tunnel lengths and the speed networks of the nodes. The malicious node is recognized by using hop-difference and AODV protocol. It detects intruders at the packet, neighbour, and membership levels.
	[41]	MaxIS scheme	The proposed method uses a greedy algorithm to search for intruders in maximum independent sets with forbidden sub-structures.
	[42]	NIAPC scheme	This scheme uses the AODV protocol and neighbourhood information to detect malicious nodes. It finds an alternate path for secure communication all over the network.
	[43]	ESPMAW scheme	This scheme uses the AODV routing protocol, neighbour, and connectivity information to find intruders in the system.

	[44]	SDN-based scheme (SWANS)	This scheme uses the information of neighbour similarity for the detection of wormholes in software-defined networks.
AODV protocol-based schemes	[45]	Wormhole recognition using AODV	The sender sends an RREQ (route request packet) to the receiver node in the AODV network. The sender calculates the average sequence numbers of all the receiver nodes. The receiver sends an RREP (route reply packet) to the sender, who compares the sequence number of the receiver with the already calculated average and decides whether the path is attacked.
	[46]	Confirmation system using honeypot	This method uses a honeypot for creating trees. The AODV and resilient ethernet protocol searches these trees for wormhole node detection.
	[47]	AODV based scheme	AODV, OSLR, and ZRP are used to detect malicious nodes in the wireless sensor network.
	[48]	Lightweight scheme (AODV)	In this scheme, the sender nodes collect all reply packets along with their sequence numbers and compare them with the calculated average sequence number to detect intruders.
RTT based	[49]	RTT-centred wormhole recognition	The AODV protocol is used in the route discovery phase. The sender sends an RREQ and saves the TREQ. The receiver sends the RREP back to the sender. The RTT is calculated as the difference between the TREP and TREQ. The path is considered a wormhole attack if the RTT exceeds the threshold limit.
	[50]	RTT centred scheme	This scheme uses RTT in conjunction with propagation time. The sender sends an RREQ packet and receives an RREP packet. The sender then calculates the RTT and propagation time to decide whether the route is attacked or attacked-free.
	[51]	EIRGP and RTT-based scheme	This scheme uses the EIGRP protocol and round-trip time for the detection of intruders.
	[52]	Trust-based scheme	This scheme uses RTT and AODV protocols for detecting malicious nodes.
High-power transmission based	[53]	Energy model by using AODV and hop count	Hop count is used to computing the distance between sender and receiver. Every node consists of a routing table and the next-hop of all nodes. The AODV routing protocol and high-power transmission are used to build a wormhole path. The malicious nodes send data packets with high energy levels, resulting in nodes draining. The system shows the normal nodes in green and the negative nodes in red.
	[54]	RPL-based scheme	The RPL routing protocol is used with the RSSI value to detect malicious nodes in the network.
Path selection	[55]	3PATw scheme	This scheme applied 3PAT to recognize the blackhole in each communication in the network. Once it recognized the black hole, the modified transmission radius based (TRB) is applied to recognize the wormhole.
	[56]	Spanning trees scheme	This scheme selects a rode node for the spanning tree. The Breadth-First Search (BFS) algorithm is applied to detect wormhole nodes in the tree.
	[57]	AD-PSO scheme	First of all, K paths are selected. The sender sends a detection packet (DP) containing RTT and hops count information. The receiver generates a feedback packet (FP). The DP and FP are compared to find wormhole nodes. Once it detects the malicious node, PSO is used to find the optimal attacker-free path.
Statistical method based	[58]	Encapsulation and fragmentation of message (EFM) scheme	This scheme presents a data packet security process that encapsulates the message and adds extra four-bit information. The message is decapsulated at the receiver's end. The technique divides the message into small pieces and sends all pieces through different parts to the destination.
	[59]	Intrusion prevention system	This scheme presents an intrusion prevention system (IPS) which detects malicious nodes and broadcasts their credentials all over the network so that no more nodes connect with those malicious nodes.
	[60]	HCBS protocol-based scheme	This scheme detects malicious nodes in clusters by using the heterogeneous cluster-based secure directing convention (HCBS) protocol.
Hop count and Weight-based	[61]	LITS scheme	This scheme uses a verification process of two replayable control messages and time synchronization to detect malicious nodes.
	[62]	WDV-hop scheme	This scheme first detects suspicious nodes by using hop count, calculates localization error for them, and drops the malicious nodes.
	[63]	Delay per hour indication (DELPHI)-based scheme	This scheme uses DELPHI (delay per hop indication) approach with some broadcasting modification by computing threshold values to detect intruders.

		[64]	RHE2WADI scheme using RSSI value	This scheme uses received signal strength indicator (RSSI) values and hop count to detect malicious nodes in the IoT network.
Authentication	Key-based	[65]	EDAK scheme	This scheme uses a dynamic matrix key process to store all the local information of the nodes so that legal nodes can be identified. It performs encryption and decryption along with two hash functions.
		[66]	HKP-HD scheme	This scheme uses key generation and its pre-distribution to reduce the chance of attacker nodes.
		[67]	Elliptic curve cryptography scheme	This scheme uses elliptic curve cryptography with the AODV protocol for wormhole attack-free networks.
Mobile agent and Cloud-based		[68]	Visiting centre local-based scheme	This scheme introduces a mobile agent in the network which is responsible for distinguishing malicious nodes from normal nodes.
		[69]	Cross-layer verification scheme	This scheme presents a cross-layer verification framework (CLVF) to find intruders in the system.

The research of Ref. [51] presented a scheme based on the EIGRP protocol, which provides high throughput and less packet delivery ratio. It used round trip time for the detection of intruders. The scheme is simple, and simulations show improved results in terms of performance. The research of Ref. [52] presented a hybrid trust-based scheme that provides AODV protocol with RTT for the detection of wormhole nodes. This scheme provides high Packet delivery ratio.

3.5. High-Power transmission-based Systems

The research of Ref. [53] presented a high-power transmission technique with a high packet delivery ratio and less end-to-end delay for recognising wormholes in mobile ad-hoc networks (MANETs). MANETs use WLAN technology for communication. The proposed technique uses the ad-hoc on-demand distance vector (AODV) protocol to detect wormholes by high-power transmission using the energy model ns2 simulator. The delivery ratio of AODV protocols decreases with a high increase in the number of connections. In the process of finding the right path, the shortest path can be lost due to network traffic.

The research of Ref. [54] presented a detection scheme for wormhole attacks that provides an effective detection rate. It uses the RPL protocol and RSSI values to detect intruder nodes. The experiments were simulated on Contiki OS with a Cooja simulator for the different nodes, i.e., 8, 16, and 24. The results provide a successful true positive detection rate of 90%.

3.6. Path Selection-Based Systems

The research of Ref. [55] presented the 3PAT wormhole technique for detecting wormhole attacks, which provides results with a high packet delivery ratio and detection rate. It combines existing transmission radius-based and 3PAT blackhole algorithms with slight modifications. The RTT is inhibited due to network traffic. If a server requests an increase, it results in increased RTT and affects the efficiency of the RTT. The RTT also increases when a node experiences network congestion due to network traffic slowing down the connection. The increased distance between nodes increases the RTT.

The research of Ref. [56] presented a spanning trees technique for detecting wormhole attacks which use no additional hardware and provides higher detection accuracy. This technique used the breadth-first search algorithm to select the roots of trees. It used only the network's connectivity information. It is a cost-effective technique without any traffic overhead. All the traffic flows towards a single path, which sometimes restricts more direct paths.

The research of Ref. [57] presented an optimal AD-PSO scheme for recognising and preventing wormhole attacks in WSNs with less energy consumption and an effective network lifetime. The proposed technique used the ad-hoc on-demand multipath distance vector (AOMDV) for wormhole path detection and particle swarm optimization

(PSO) for optimal path selection. The results were compared with trust- and energy-based routing protocols (TESRP) regarding the energy consumption and network lifetime. The delivery ratio of AODV protocols decreases with a high increase in the number of connections. In the process of finding the right path, the shortest path can be lost due to network traffic.

3.7. Statistical Method-Based Systems

The research of Ref. [58] presented a scheme that uses the encapsulation and fragmentation of message (EFM) techniques to secure data packets. This technique encapsulates the message and adds extra four-bit information to it. The message is decapsulated at the receiver's end. The technique divides the message into small pieces and sends all the pieces through different parts to the destination. In this case, more data loss can be avoided when there is a wormhole attack in the network. The simulations were conducted for 10 nodes which showed the average packet delivery ratio.

The research of Ref. [59] presented an intrusion prevention system (IPS) scheme which detects malicious nodes and broadcasts their credentials all over the network so that no more nodes connect with those malicious nodes. This scheme causes unnecessary communications among nodes, resulting in high costs and increased traffic overhead.

The research of Ref. [60] presented a trust-based scheme for wormhole mitigation in ad-hoc WSN. It detects malicious nodes in clusters using the heterogeneous cluster-based secure directing convention (HCBS) protocol. The simulations of the presented approach—named TSDAMN—were conducted in the MANsim testing system, which showed high throughput, limited E2E delay, less PLR, and high PDR.

3.8. Hop Count and Weight-Based Methods

The research of Ref. [61] presented a scheme named Location information and time synchronisation (LITS), which detects suspicious nodes using increased delay information. The suspicious nodes are passed through a verification process of two replayable control messages and time synchronization.

The research of Ref. [62] presented a detection scheme—named WDV-hop-based localisation—which provides a high detection rate. The scheme first detects suspicious nodes, then calculates their localisation errors, and drops the malicious nodes.

The research of Ref. [63] presented a wormhole mitigation approach that provides high throughput and PDR. It uses the DELPHI (delay per hop indication) approach with some broadcasting modification by computing the threshold values. The simulations of this scheme were conducted in the NS2 simulator. The results showed that the proposed scheme provides less packet loss, less jitter, and average E2E delay.

The research of Ref. [64] presented a hybrid approach for wormhole mitigation named RSSI and hop count-based energy efficient wormhole attack detection system for IoT network (RHE2WADI). It uses received signal strength indicator (RSSI) values and hop count to detect malicious nodes in the IoT network. The simulations were conducted in a Cooja simulator. The results showed that it provides a high detection accuracy of up to 95%, less overhead, less energy consumption, and less delay.

3.9. Authentication Key-Based Systems

The research of Ref. [65] presented a scheme—named efficient dynamic authentication and key (EDAK) management—which generates dynamic keys for messages to be transmitted from the source to the destination. The dynamic matrix key DMK process stores the local information of all the nodes so that legal nodes can be identified. The EDAK performs encryption and decryption, along with two hash functions. The scheme is flexible and scalable to large networks. It causes less traffic overhead.

The research of Ref. [66] presented a hybrid key pre-distribution scheme (HKP-HD) scheme, which reduces the chances of sensor nodes being attacked.

The research of Ref. [67] presented an elliptic curve cryptography scheme for wormhole mitigation. It uses the AODV protocol. The simulations were conducted on 250 nodes in the NS2 simulator. The results showed that the presented crypto scheme provides high throughput, high PDR, less E2E delay, and less routing overhead.

3.10. Mobile Agent and Cloud-Based Systems

The research of Ref. [68] presented a scheme named visiting centre local (VCL), which is based on mobile agent packet structure (MAPS). This scheme introduces a mobile agent in the sensor network which is responsible for distinguishing malicious nodes from normal nodes. The simulations for 200 nodes are done in the Sinalgo simulator, and the results show an improved packet delivery ratio, less energy consumption, and enhanced network lifetime.

The research of Ref. [69] presented a scheme—named cross-layer verification framework (CLVF)—which provides high detection accuracy, minor end-to-end delay, and high throughput. The simulations were conducted for 250 nodes, and the results were compared with the existing LBIDS technique. The results were better than the existing techniques.

4. Performance Analysis

4.1. Critical Analysis

Table 5 summarises the critical analysis of all the schemes for recognising and avoiding wormhole attacks. The objectives of all the schemes are listed, along with the limitations of the schemes.

The research of Ref. [37] presented the creating credible discovery (CREDND) scheme, which uses neighbour information. It uses no additional hardware. It detects wormhole attacks at a high rate and consumes less energy; however, this scheme does not work well in networks with changing communication ranges of nodes. A high-power transmission technique was presented [53], providing a high packet delivery ratio and less end-to-end delay. However, this scheme uses the AODV protocol, which provides no scalability [70].

The research of Refs. [49–52] presented RTT-based techniques which provide a high detection rate. The limitation of these schemes is that the RTT increases with the increase in distance between nodes. The local area network traffic also affects the RTT.

The research of Refs. [38,54] presented RPL protocol-based schemes. The presented schemes are complex, as RPL increases control packets in the network resulting in traffic overhead [71].

The research of Ref. [45] presented an improved AODV protocol that consumes less energy. It is a less complex scheme. However, it provides no congestion control [70].

The research article of Ref. [41] presented a forbidden substructure technique that uses a greedy algorithm; however, sometimes, it fails to find an optimal solution.

The research of Ref. [46] proposed a tree-based model with a honeypot which uses very few resources. However, no protection is provided against misconfiguration, so it is easy to create loops.

The research of Ref. [39] presented a decentralised statistical technique that provides high detection accuracy and a false-positive rate. This scheme provides less mean detection delay; however, there is a loss of control regarding the traffic overhead and costlier operations affect the performance.

The research of Ref. [56] presented a spanning tree technique, which uses no additional hardware and provides high detection accuracy; however, it restricts more direct paths as all data flow towards only a single path.

The research of Ref. [57] presented an AD-PSO technique, which consumes less energy and provides an effective network lifetime. This is an optimal scheme but does not provide load balancing [70].

The research of Ref. [40] is a modified AODV scheme that uses multi-hop count analysis. It provides the maximum moving speed of nodes; however, there is a loss of energy in the multi-hop count analysis.

The research of Ref. [26] proposed an artificial immune-based scheme using fuzzy logic, which provides high PDR, high FPR, and less PLR. However, this scheme provides less stability in the network due to fuzzy logic [72].

The research of Ref. [27] presented an SVM-based scheme with an RPL protocol which provides high detection accuracy and requires less computation power; however, the computational complexity of the SVM is high [73].

The research of Ref. [42] presented a NIAPC scheme using AODV, which provides high detection accuracy, PDR, and throughput.

Table 5. Summary of critical analysis of wormhole detection schemes.

	Detection Algorithm	Effort Year	Technique	Performance Metrics	Shortcoming
Neighbours discovery-based	[37]	2019	CREDND (creating a credible neighbour discovery) Protocol	No additional hardware, less energy consumption, detection accuracy	It cannot work well with dynamic changing in the communication range of nodes [37]
	[38]	2018	Trust-based scheme	Low energy consumption	RPL is a complex protocol that increases the network's control packets, resulting in overhead and increased energy consumption [71]
	[39]	2018	Decentralized statistical scheme	Detection accuracy, false-positive rate, mean detection delay	Loss of control, costlier operations
	[40]	2019	MLAMAN scheme	Tunnel length, the maximum moving speed of nodes	Loss of energy in multi-hop count analysis
	[41]	2019	MaxIS scheme	Poor connectivity	The greedy algorithm fails to find an optimal solution
	[42]	2019	NIAPC scheme	High detection accuracy, PDR, and throughput, no specific storage requirement	The FNR for a short-distance wormhole is high [42]
	[43]	2019	ESPMAW scheme	High throughput, less E2E delay, less energy consumption, and traffic overhead	It cannot detect wormholes for shorter tunnel lengths [43]
	[44]	2021	SDN-based scheme (SWANS)	Less communication overhead, less FNR	The FPR is low [44]
AODV protocol-based schemes	[45]	2018	Wormhole recognition using AODV	Low energy consumption, less complex	No scalability, no congestion control, no load balancing [70]
	[46]	2018	Confirmation system using honeypot	Fewer resources	No protection against misconfiguration (easy to create loops)
	[47]	2018	AODV based scheme	High detection accuracy	Low throughput [47]
	[48]	2021	Lightweight scheme (AODV)	High throughput, high PDR, less routing overhead	The end-to-end delay is average [48]
RTT-based	[49]	2018	RTT-centred wormhole recognition	No additional hardware and clock synchronization	Increases with the increase in distance between nodes, LAN traffic affects the functionality of RTT
	[50]	2020	RTT centred scheme	Detection rate	Increases with the increase in distance between nodes, LAN traffic affects the functionality of RTT
	[51]	2018	EIRGP- and RTT-based scheme	High throughput, less PDR	It cannot find malicious nodes effectively [51]

Category	Ref	Year	Scheme	Advantages	Disadvantages
	[52]	2019	Trust-based scheme	High PDR, no additional hardware	The throughput rate is low [52]
High-power transmission-based	[53]	2019	Energy model by using AODV and hop count	High packet delivery ratio, less end-to-end delay	No scalability, no congestion control, no load balancing [70]
	[54]	2019	RPL-based scheme	Detection rate	RPL is a complex protocol that increases the control packets in the network which results in overhead and increased energy consumption [71].
Path selection	[55]	2018	3PATw scheme	Detection rate, packet delivery ratio	Increases with the increase in distance between nodes, LAN traffic affects the functionality of RTT
	[56]	2018	Spanning trees scheme	No additional hardware, high detection accuracy	Restricts more direct paths as all data flow towards only a single path
	[57]	2020	AD-PSO scheme	Less energy consumption, effective network lifetime	No scalability, no congestion control, no load balancing [70]
Statistical method-based	[58]	2019	Encapsulation and fragmentation of message (EFM) scheme	Less PLR	The packet delivery ratio is average [58]
	[59]	2020	Intrusion prevention system	High detection accuracy	The traffic overhead is increased and the computation cost is high [70]
	[60]	2021	HCBS protocol-based scheme	High throughput, high PDR, less PLR, less E2E delay	Cluster head selection increase computational complexity [60]
Hop count and Weight-based	[61]	2018	LITS scheme	High detection accuracy, reduced localization error	It requires clock synchronization, which increases the computation cost [61]
	[62]	2018	WDV-hop scheme	High detection accuracy	The packet delay is increased and the complexity is high [62]
	[63]	2021	Delay per hour indication (DELPHI)-based scheme	High throughput, PDR, less PLR, less Jitter	The end-to-end delay is average [63]
	[64]	2021	RHE2WADI scheme using RSSI value	High detection accuracy, less traffic overhead, less energy consumption	The end-to-end delay is average [64]
Authentication Key-based	[65]	2019	EDAK scheme	Less traffic overhead, scalable to large networks	There is no data integrity [65]
	[66]	2018	HKP-HD scheme	High detection accuracy, less chance of attack	It does not apply to highly mobile networks [66]
	[67]	2021	Elliptic curve cryptography scheme	High throughput, high PDR, less E2E delay, less routing overhead	No scalability, no congestion control, no load balancing [70]
Mobile agent and Cloud-based	[68]	2018	Visiting centre local-based scheme	High detection accuracy, less energy consumption, enhanced network lifetime	Security in the transaction context is medium [68]
	[69]	2019	Cross-layer verification scheme	High detection accuracy, high throughput, less E2E delay	It cannot be applied to multicast routing protocols; the performance rate of the network degrades with time

The scheme has no specific storage requirement; however, the false negative rate for the short-distance wormhole is high.

The research of Ref. [43] presented an ESPMAW scheme using AODV, which provides high throughput, less E2E delay, and traffic overhead. This scheme consumes less energy. However, it cannot detect wormholes for shorter tunnel lengths. The research of

Ref. [51] presented an EIRGP- and RTT-based scheme, which provides high throughput and less PDR; however, it cannot find malicious nodes effectively. The study of Ref. [52] presented a trust-based scheme using RTT and AODV, which provides high PDR. This scheme uses no additional hardware; however, the throughput rate is low. The research [58] proposed the encapsulation and fragmentation of message (EFM) scheme, which provides less PLR; however, the packet delivery ratio is average. The research of Ref. [59] presented an intrusion prevention system which provides high detection accuracy; however, the traffic overhead is increased, and the computation cost is high. The research of Ref. [61] presented a LITS scheme that provides high detection accuracy and reduced localization error; however, it requires clock synchronisation, increasing the computation cost.

The research of Ref. [62] presented a WDV-hop scheme that provides high detection accuracy; however, the packet delay is increased, and the complexity is high. The research of Ref. [65] presented an EDAK scheme which provides less traffic overhead. This scheme is scalable to large networks; however, there is no data integrity. The research of Ref. [66] presented an HKP-HD scheme which provides high detection accuracy. This scheme has less of a chance of attack; however, it is not applicable for the highly mobile network. The research of Ref. [32] presented a PPKP scheme which provides secure communication; however, it can only be applied initially. The research of Ref. [68] presented a visiting centre local-based scheme which provides high detection accuracy and less energy consumption. It provides an enhanced network lifetime; however, the security in the transaction context is only medium [64]. The research of Ref. [69] presented a cross-layer verification scheme that provides high detection accuracy and high throughput. This scheme experiences less E2E delay. However, it cannot be applied to multicast routing protocols. The performance rate of the network degrades with time.

The research of Ref. [44] presented a SWANS scheme which provides less communication overhead, less FPR, and less FNR.

The research of Ref. [28] presented an ANN-based approach with a hop count which provides high detection accuracy. This scheme uses no additional hardware; it only uses connectivity information. However, the computational complexity of the neural network is high [74].

The research of Ref. [63] presented a delay per hour indication (DELPHI) scheme which provides high throughput, PDR, and less PLR. This scheme provides less jitter; however, the end-to-end delay is average. The research of Ref. [60] presented an elliptic curve cryptography scheme using AODV which provides high throughput, high PDR, and less E2E delay. It provides less routing overhead, although provides no scalability, no congestion control, and no-load balancing [70].

The research of Ref. [29] presented an LSTM scheme using RTT, providing high detection accuracy, high PDR, and less energy consumption. It provides less E2E delay; however, the computational complexity of the neural network is high [74]. The research of Ref. [60] presented an HCBS protocol-based scheme which provides high throughput, high PDR, and less PLR. This scheme provides less E2E delay; however, the cluster head selection increases the computational complexity [75]. The research of Ref. [48] presented an AODV-based scheme which provides high throughput, high PDR, and less routing overhead, although the end-to-end delay is average. The research of Ref. [30] presented a DRFOIDL-ID scheme using RPL, which provides high detection accuracy, less FPR, and PLR; however, the computational complexity of the neural network is high. The research of Ref. [31] tested the ML supervised learning methods KNN, SVM, DT, LDA, NB, and CNN for wormhole detection in which DT provides high detection accuracy; however, CNN has high computational complexity. The research of Ref. [72] presented the RHE2WADI scheme using RSSI value, which provides high detection accuracy, less traffic overhead, and less energy consumption; however, the end-to-end delay is average.

4.2. Comparative Analysis

Table 6 presents a summary of the comparative analysis of the performance matrices of all the schemes of wormhole recognition and avoidance. All the schemes are evaluated and compared in this table based on the performance matrices.

Table 6. A comparison of the performance matrices wormhole detection schemes.

Scheme	DR	EC	TO	NL	T	FPR	MDD	PDR	PLR
Artificial immune system with fuzzy logic [26]	High	-	-	-	-	High	-	High	Low
SVM-based scheme [27]	High	-	-	-	-	-	-	-	-
ANN with hop count [28]	High	-	-	-	-	-	-	-	-
LSTM with RTT [29]	High	Low	-	-	-	-	Low	High	-
DRFOIDL-ID using RPL [30]	High	-	-	-	-	Low	-	Low	Low
ML-based scheme [31]	High	-	-	-	-	-	-	-	-
Fuzzy Logic based scheme [32]	High	-	-	-	High	-	-	High	-
WCA [33]	-	Low	Low	-	High	-	Low	-	-
KNN and RF [34]	-	-	Low	-	-	Low	-	-	-
EC-BRTT [35]	High	-	-	-	-	-	-	-	-
CART [36]	High	-	Low	-	-	-	-	-	-
CREDND [37]	High	Low	-	-	-	-	-	-	-
Trust-based scheme [38]	-	Low	-	-	-	-	-	-	-
Decentralized statistical scheme [39]	High	-	-	-	-	Low	Low	-	-
MLAMAN [40]	High	-	-	-	-	-	-	-	-
MaxIS [41]	Avg	-	-	-	-	-	-	-	-
NIAPC [42]	High	-	-	-	High	-	-	High	-
ESPMAW [43]	-	Low	Low	-	High	-	Low	-	-
SDN- SWANS [44]	-	-	Low	-	-	Low	-	-	-
AODV [45]	-	Low	-	-	-	-	-	-	-
Confirmation system using honeypot [46]	High	-	-	-	-	-	-	-	-
AODV based [47]	High	-	-	-	-	-	High	-	-
Lightweight AODV [48]	-	-	Low	-	High	-	-	High	-
RTT-centred scheme [49]	High	-	-	-	-	-	-	-	-
RTT-based scheme [50]	High	-	-	-	-	-	-	-	-
EIRGP with RTT [51]	-	-	-	-	High	-	-	Low	-
Trust-based scheme [52]	-	-	-	-	-	-	-	High	-
Energy model with AODV [53]	-	-	-	-	-	-	Low	High	-
RPL-based scheme [54]	High	-	-	-	-	-	-	-	-
3PATw [55]	High	-	-	-	-	-	-	High	-
Spanning trees [56]	High	-	-	-	-	-	-	-	-
AD-PSO [57]	-	Low	-	High	-	-	-	-	-
EFM [58]	-	-	-	-	-	-	-	-	Low
Statistical scheme [59]	High	-	-	-	-	-	-	-	-
HCBS protocol [60]	-	-	-	-	High	-	Low	High	Low
LITS [61]	High	-	-	-	-	-	-	-	-
WDV-hop [62]	High	-	-	-	-	-	-	-	-
DELPHI [63]	-	-	-	-	High	-	-	High	Low
RHE2WADI with RSSI [64]	High	Low	Low	-	-	-	-	-	-
EDAK [65]	-	-	Low	-	-	-	-	-	-
HKP-HD [66]	High	-	-	-	-	-	-	-	-
Elliptic curve cryptography [67]	-	-	Low	-	High	-	Low	High	-
Visiting Centre Local-based [68]	High	Low	Low	-	-	-	-	-	-
Cross-layer verification [69]	High	-	-	-	High	-	Low	-	-

4.3. Identified Challenges

This section presents the issues and challenges of all schemes of recognition and the avoidance of wormhole attacks listed in Table 7. It briefly states the limitations of all the schemes. These are the open research areas in which work can be conducted in the future to overcome the issues and challenges addressed by the schemes.

Table 7. Identified challenges of wormhole detection schemes.

Category	Challenges
Neighbour discovery-based schemes [37–44]	It is difficult to work well in different communication ranges and dynamically changing WSNs. The dependency on the neighbour node should not be high. In addition, the energy consumption is high, which shortens the network lifetime.
AODV-based schemes [45–48]	It is difficult to provide scalability, load balancing, and congestion control in working with the AODV protocol. The shortest path may be lost due to traffic overhead. The delivery ratio of the AODV protocol decreases with a high increase in the number of connections. Therefore, it is difficult to work with it in complex conditions. It also cannot be implemented in a network with many nodes.
RTT-based schemes [49–52]	The RTT stops when there is an increase in network traffic. It also increases with the increase in distance between nodes. It is difficult to work with RTT in a complex network as the increase in server requests increases, affecting RTT's efficiency.
RPL-based schemes [38,54]	It is difficult to work in the RPL network as it is a complex protocol that generates a large number of control packets resulting in high energy consumption. The network overhead increase with an increased number of data packets.

4.3.1. Need to Work with Constantly Shifting Ranges

When the nodes in WSNs are changing their positions continuously, and the network uses various communication ranges, the communication becomes difficult because each node depends on neighbours' information, making it vulnerable to several attacks. Therefore, it is difficult for it to work well in different communication ranges and dynamically changing WSNs because the dependency on the neighbour node should not be high [37]. The delivery ratio of AODV protocols decreases with a high increase in the number of connections. Therefore, it is difficult to work with it in complex conditions [45].

4.3.2. Need for Scalability and Load Balancing

The AODV protocol is well known for routing. However, it does not assure the proper working of the network in cases of increased network size. It also does not provide load balancing and congestion control. When the network traffic increases, there is a high chance of the loss of the shortest path in the AODV protocol [53]. The AODV protocol which is used for routing does not provide scalability in the network. It cannot be implemented in-network with a large number of nodes [46]. The AODV protocol used for routing does not provide congestion control in the network [40,57]. The RPL routing protocol increases network overhead with more data packets [38]. Working in complex conditions with a decentralised scheme is difficult as it experiences control loss and costlier operations [39]. In the spanning tree scheme, all the traffic flows towards a single path instead of more direct paths [56].

4.3.3. Need for High-Rate Transmission over Long Distance

The RTT scheme is often used to reduce several security threats; however, there are several limitations of the RTT. It does not work at a high rate of data packet transmission. It stops when there is an increase in network traffic. It also increases with the increase in distance between nodes [49]. Large-scale networks slow down the connection when a node experiences network congestion due to network traffic [55]. In a complex network, it increases with the increase in server requests, which affects the efficiency of RTT [50]. Recognising wormhole attacks is difficult with a greedy algorithm as it fails to find the

optimal path for routing [41]. It is difficult for it to work in the RPL network as it is a complex protocol that generates many control packets, resulting in high energy consumption [54]. The statistical method-based schemes also provide computational complexity, resulting in high computation costs and network overhead [58–60].

5. Optimal Solutions

The previous section specifies several state-of-the-art problems such as no scalability, load balancing, congestion control, communication overhead, data integrity issues, high energy consumption, time delay, average PDR, and PLR, less FPR, low transmission rate, and low detection rate.

AI- and ML-Based Schemes as Optimal Solutions to State-of-the-Art Problems

Artificial intelligence- and ML-based schemes can be used to solve all the identified state-of-the-art problems [26–36]. The first challenge, as mentioned in Table 7, is neighbour-based discovery schemes. Although these schemes provide a detection accuracy of up to 90%, they are not energy efficient. In addition, they do not detect shorter tunnel wormholes in some cases. To overcome the problem, an unsupervised learning-based scheme that uses a weighted clustering algorithm [33] can be used. This provides less energy consumption with 90% detection accuracy. This scheme then uses a support vector machine and machine layer perceptron, which improves the results in terms of throughput and packet delivery ratio.

The second challenge, as mentioned in Table 7, is AODV-based schemes. Although the AODV protocol does not provide scalability, load balancing, and congestion control, an artificial immune system uses fuzzy logic with AODV [26] to provide a high detection accuracy of up to 98%. This highly scalable method provides high FPR and PDR, and less PLR. It also overcomes the problems of load balancing and congestion control. Another machine learning approach [34] used the AODV protocol with supervised KNN and random forest classifiers. This novel approach provides high PDR and high detection accuracy of up to 98.6%. In addition, it provides less PLR and JitterSum. It uses the packet leash cryptographic technique to prevent wormholes, which overcomes the state-of-the-art problems of AODV-based schemes.

The third challenge, as mentioned in Table 7, is RTT-based schemes. Although RTT does not work well in increased network traffic, EC-BRTT [35] used a supervised machine learning classifier named the naïve Bayes classifier with RTT. This scheme provides very efficient results regarding detection accuracy, time delay, throughput, PDR, energy consumption, and network lifetime. The milestone of this machine learning scheme is the reduced communication overhead, which overcomes the state-of-the-art problem of RTT-based schemes. Another deep learning approach that uses RTT with LSTM [27] provides high detection accuracy with high PDR. LSTM is a deep neural network that works very well in complex conditions. This scheme's latency rate and packet loss ratio are also very low. It uses a whale optimisation algorithm with a fitness rate to find the optimal routing path for data packet transmission. This optimal solution also consumes less energy and less end-to-end delay.

The fourth challenge, as mentioned in Table 7, is RPL-based schemes. A Delta Rule First Order Iteration Deep Neural Learning Intrusion Detection (DRFOIDL-ID) [30] has been presented and compared with RPL-based schemes. This deep learning outperforms RPL-based schemes in all terms, including attack detection rate (ADR), attack detection time (ADT), false alarm rate (FAR), and packet loss rate (PLR). The ADR of DRFOID-ID is 92%; this is 80% in the existing RPL-based mechanism. The ADT of DRFOID-ID is 13 ms; this is 20 ms in the existing RPL-based mechanism. The FAR of DRFOID-ID is 8%; this is 20% in the existing RPL-based mechanism. The PLR of DRFOID-ID is 2 PPS (packets per second); this is 5 PPS in the existing RPL-based mechanism. In addition, the neural network works well with increased data transmission rates and complex network situations.

All of the above analysis shows that AI- and ML-based techniques are better than the state-of-the-art techniques in terms of detection accuracy, PDR, FPR, PLR, energy consumption, and transmission rate. Figure 7 compares the detection accuracies of AI- and ML-based schemes, neighbours discovery-based schemes, AODV-based schemes, and RTT-based schemes. AI- and ML-based schemes achieve higher detection accuracy than the other categories.
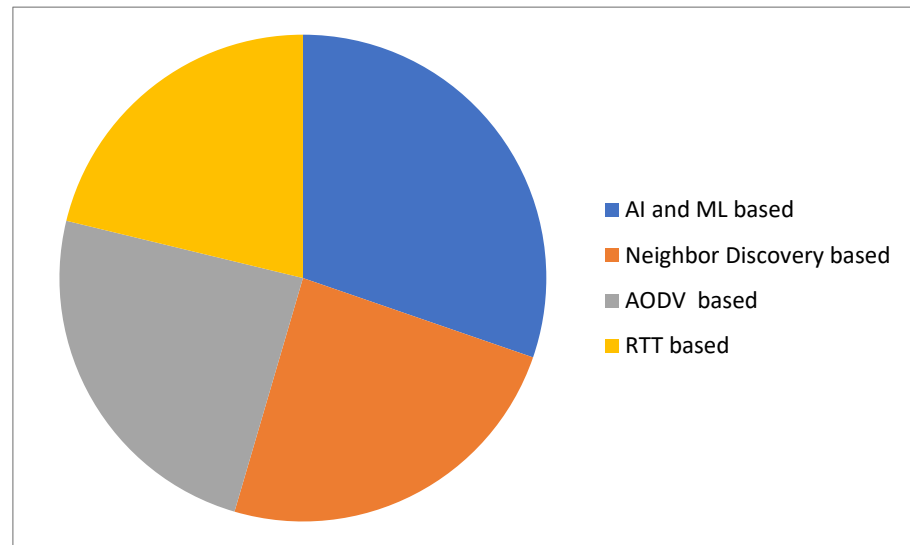

Figure 7. Analysis of the accuracy of AI- and ML-based schemes in comparison to other schemes.

6. Conclusions

Several schemes are reviewed in this paper in which some detect wormhole attacks and others provide the avoidance of wormhole attacks. These schemes include AI- and ML-based, neighbours discovery- and path selection-based schemes, statistical method- and AODV-based, RTT and hop count, cloud, and mobile agent-based schemes. The paper presents an SLR reviewing all of these schemes using extensive critical and comparative analysis. The schemes were evaluated based on detection accuracy, network lifetime, energy consumption, complexity, packet delivery ratio, packet loss ratio, and delay. The gaps in the literature were identified, which shows the future scope of work in detecting and avoiding wormhole attacks. Researchers have recently attempted to apply artificial intelligence systems to identify wormhole attacks, with rather promising detection results. The comparison shows that AI- and ML-based schemes for wormhole detection provide more favourable results than state-of-the-art techniques.

Author Contributions: Conceptualization, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A.; methodology, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A.; validation, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A.; formal analysis, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A.; investigation, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A. resources, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A. data curation, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A. writing—original draft preparation, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A. writing—review and editing, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A. visualization, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A. funding acquisition, M.H. (Maria Hanif), H.A., Z.J., N.Z.J., M.H. (Mamoona Humayun), S.S. and A.M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Saudi Aramco Cybersecurity Chair, Imam Abdulrahman Bin Faisal University, Saudi Arabia.

References

1. Adil, M.; Almaiah, M.A.; Omar Alsayed, A.; Almomani, O. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. *Sensors* **2020**, *20*, 2311.
2. Elsayed, W.; Elhoseny, M.; Sabbeh, S.; Riad, A. Self-maintenance model for wireless sensor networks. *Comput. Electr. Eng.* **2018**, *70*, 799–812.
3. Sah, D.K.; Amgoth, T. Renewable energy harvesting schemes in wireless sensor networks: A survey. *Inf. Fusion* **2020**, *63*, 223–247.
4. Sampoornam, K.P.; Saranya, S.; Mohanapriya, G.K.; Devi, P.S.; Dhaarani, S. Analysis of LEACH Routing Protocol in Wireless Sensor Network with Wormhole Attack. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021; pp. 147–152.
5. Shahraki, A.; Taherkordi, A.; Haugen, Ø.; Eliassen, F. Clustering objectives in wireless sensor networks: A survey and research direction analysis. *Comput. Netw.* **2020**, *180*, 107376.
6. Numan, M.; Subhan, F.; Khan, W.Z.; Hakak, S.; Haider, S.; Reddy, G.T.; Alazab, M. A systematic review on clone node detection in static wireless sensor networks. *IEEE Access* **2020**, *8*, 65450–65461.
7. Kandris, D.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications of wireless sensor networks: An up-to-date survey. *Appl. Syst. Innov.* **2020**, *3*, 14.
8. Ali, A.; Ming, Y.; Chakraborty, S.; Iram, S. A comprehensive survey on real-time applications of WSN. *Future Internet* **2017**, *9*, 77.
9. Premkumar, M.; Sundararajan, T.V.P. DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. *Microprocess. Microsyst.* **2020**, *79*, 103278.
10. Liu, Y.; Ma, M.; Liu, X.; Xiong, N.N.; Liu, A.; Zhu, Y. Design and analysis of probing route to defense sinkhole attacks for Internet of Things security. *IEEE Trans. Netw. Sci. Eng.* **2018**, *7*, 356–372.
11. Yousefpoor, M.S.; Yousefpoor, E.; Barati, H.; Barati, A.; Movaghar, A.; Hosseinzadeh, M. Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. *J. Netw. Comput. Appl.* **2021**, *190*, 103118.
12. Ahutu, O.R.; El-Ocla, H. Centralized routing protocol for detecting wormhole attacks in wireless sensor networks. *IEEE Access* **2020**, *8*, 63270–63282.
13. Sankara Narayanan, S.; Murugaboopathi, G. Modified secure AODV protocol to prevent wormhole attacks in MANET. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e5017.
14. Alenezi, F.A.; Song, S.; Choi, B.Y. WAND: Wormhole Attack Analysis using the Neighbor Discovery for Software-defined Heterogeneous Internet of Things. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
15. Siddiqui, M.N.; Malik, K.R.; Malik, T.S. Performance Analysis of Blackhole and Wormhole Attack in MANET-Based IoT. In Proceedings of the 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2), Islamabad, Pakistan, 20–21 May 2021; pp. 1–8.
16. Verma, M.K.; Dwivedi, R.K. A Survey on Wormhole Attack Detection and Prevention Techniques in Wireless Sensor Networks. In Proceedings of the 2020 International Conference on Electrical and Electronics Engineering (ICE3), Gorakhpur, India, 14–15 February 2020; pp. 326–331.
17. Dwivedi, R.K.; Sharma, P.; Kumar, R. Detection and prevention analysis of wormhole attack in wireless sensor network. In Proceedings of the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 11–12 January 2018; pp. 727–732.
18. Goyal, M.; Dutta, M. Intrusion Detection of Wormhole Attack in IoT: A Review. In Proceedings of the 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), Kottayam, India, 21–22 December 2018; pp. 1–5.
19. Farjamnia, G.; Gasimov, Y.; Kazimov, C. Review of the techniques against the wormhole attacks on wireless sensor networks. *Wirel. Pers. Commun.* **2019**, *105*, 1561–1584.
20. Ghugar, U.; Pradhan, J. Survey of wormhole attack in wireless sensor networks. *Comput. Sci. Inf. Technol.* **2020**, *2*, 33–42.
21. Kumar, S.S. Abridgement and Prevention of Wormhole Attack in Mobile Ad Hoc Networks using Coordinator Node. Ph.D. Thesis, Vels University, Chennai, India, 7 February 2020. Available online: http://hdl.handle.net/10603/274578 (accessed on 28 May 2022).

22. Giri, D.; Borah, S.; Pradhan, R. Approaches and measures to detect wormhole attack in wireless sensor networks: A survey. In *Advances in Communication 2018, Devices, and Networking*; Springer: Singapore, 2018; pp. 855–864.

23. Padmapriya, S.D.; Jeyalaksshmi, S.S.; Kamalakkannan, S. A Survey: Techniques and Challenges to Detect Wormhole Attack in Wireless Sensor Network. *J. Appl. Sci. Comput.* **2018**, *5*, 2120–2126.

24. Liu, Y.; Dong, M.; Ota, K.; Liu, A. ActiveTrust: Secure and trustable routing in wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2013–2027.

25. Memon, S.K.; Nishar, K.; Hanafi Ahmad Hijazi, M.; Chowdhry, B.S.; Sodhro, A.H.; Pirbhulal, S.; Rodrigues, J.J.P.C. A survey on 802.11 MAC protocols industrial standards, architecture elements for providing QoS guarantee, supporting emergency traffic, and security : Future directions. *J. Ind. Inf. Integr.* **2021**, *4*, 100225.

26. Jamali, S.; Fotohi, R. Defending against Wormhole Attack in MANET Using an Artificial Immune System. *New Rev. Inf. Netw.* **2016**, *21*, 79–100.

27. Jhanjhi, N.Z.; Brohi, S.N.; Malik, N.A.; Humayun, M. Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning. In Proceedings of the 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 13–15 October 2020; pp. 1–6.

28. Singh, M.M.; Dutta, N.; Singh, T.R.; Nandi, U. A Technique to Detect Wormhole Attack in Wireless Sensor Network Using Artificial Neural Network. In *Evolutionary Computing and Mobile Sustainable Networks*; Springer: Singapore, 2021; pp. 297–307.

29. Pawar, M.V.; Anuradha, J. Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. *Int. J. Pervasive Comput. Commun.* **2021**, *ahead of print*. https://doi.org/10.1108/IJPCC-10-2020-0162.

30. KP, K.S. Delta Ruled First Order Iterative Deep Neural Learning for Sybil and Wormhole Attacks Detection in Healthcare Wireless Sensor Network. *Preprint* **2021**. https://doi.org/10.21203/rs.3.rs-512769/v1.

31. Abdan, M.; Seno, S.A.H. Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad-Hoc Network (MANET). *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 2375702. https://doi.org/10.1155/2022/2375702.

32. Ezhilarasi, M.; Gnanaprasanambikai, L.; Kousalya, A.; Shanmugapriya, M. A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks. *Soft Comput.* **2022**, 1–12. https://doi.org/10.1007/s00500-022-06915-1.

33. Gulganwa, P.; Jain, S. EES-WCA: Energy-efficient and secure weighted clustering for WSN using machine learning approach. *Int. J. Inf. Technol.* **2022**, *14*, 135–144.

34. Ali, S.; Nand, P.; Tiwari, S. Detection of Wormhole Attack in Vehicular Ad-hoc Network over Real Map using Machine Learning Approach with Preventive Scheme. *J. Inf. Technol. Manag.* **2022**, *14*, 159–179.

35. Lakshmi Narayanan, K.; Santhana Krishnan, R.; Golden Julie, E.; Harold Robinson, Y.; Shanmuganathan, V. Machine learning-based detection and a novel EC-BRTT algorithm-based prevention of DoS attacks in wireless sensor networks. *Wirel. Pers. Commun.* **2021**, 1–25. https://doi.org/10.1007/s11277-021-08277-7.

36. Gite, P.; Chouhan, K.; Krishna, K.M.; Nayak, C.K.; Soni, M.; Shrivastava, A. ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4. 5 and CART classifiers. *Mater. Today Proc.* **2021**, *in press*. https://doi.org/10.1016/j.matpr.2021.07.378.

37. Luo, X.; Chen, Y.; Li, M.; Luo, Q.; Xue, K.; Liu, S.; Chen, L. CREDND: A novel secure neighbor discovery algorithm for wormhole attack. *IEEE Access* **2019**, *7*, 18194–18205.

38. Mehta, R.; Parmar, M.M. Trust-based mechanism for Securing IoT Routing Protocol RPL against Wormhole & Grayhole Attacks. In Proceedings of the 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 6–8 April 2018; pp. 1–6.

39. As'adi, H.; Keshavarz-Haddad, A.; Jamshidi, A. A New Statistical Method for Wormhole Attack Detection in MANETs. In Proceedings of the 2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Tehran, Iran, 28–29 August 2018; pp. 1–6.

40. Vo, T.T.; Luong, N.T.; Hoang, D. MLAMAN: A novel multi-level authentication model and protocol for preventing wormhole attacks in mobile ad hoc networks. *Wirel. Netw.* **2019**, *25*, 4115–4132.

41. Bai, S.; Liu, Y.; Li, Z.; Bai, X. Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures. *Comput. Netw.* **2019**, *150*, 190–200.

42. Patel, M.; Aggarwal, A.; Chaubey, N. Detection of Wormhole Attack in Static Wireless Sensor Networks. In *Advances in Computer Communication and Computational Sciences*; Springer: Singapore, 2019; Volume 760, pp. 463–471. https://doi.org/10.1007/978-981-13-0344-9_39.

43. Aliady, W.A.; Al-Ahmadi, S.A. Energy preserving secure measure against wormhole attack in wireless sensor networks. *IEEE Access* **2019**, *7*, 84132–84141.

44. Alenezi, F.A.; Song, S.; Choi, B.Y. SWANS: SDN-based Wormhole Analysis using the Neighbor Similarity for a Mobile ad hoc network (MANET). In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 17–21 May 2021; pp. 653–657.

45. Kaur, T.; Kumar, R. Mitigation of blackhole attacks and wormhole attacks in wireless sensor networks using aodv protocol. In Proceedings of the 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–15 August 2018; pp. 288–292.

46. Tiruvakadu, D.S.K.; Pallapa, V. Confirmation of wormhole attack in MANETs using honeypot. *Comput. Secur.* **2018**, *76*, 32–49.

47. Govindasamy, J.; Punniakody, S. A comparative study of reactive, proactive, and hybrid routing protocol in wireless sensor networks under wormhole attack. *J. Electr. Syst. Inf. Technol.* **2018**, *5*, 735–744.

48. Zardari, Z.A.; Memon, K.A.; Shah, R.A.; Dehraj, S.; Ahmed, I. A lightweight technique for detection and prevention of wormhole attacks in MANET. *EAI Endorsed Trans. Scalable Inf. Syst.* **2021**, *8*, e2.

49. Kori, S.; Krishnamurthy, G.N.; Sidnal, N. RTT Centered Automatic and Dynamic Wormhole Attack Discovery in Sensor Network. In Proceedings of the 2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Msyuru, India, 14–15 December 2018; pp. 1684–1690.

50. Roy, A.K.; Khan, A.K. RTT-based wormhole detection for wireless mesh networks. *Int. J. Inf. Technol.* **2020**, *12*, 1–8.

51. Karthigadevi, K.; Balamurali, S.; Venkatesulu, M. Wormhole attack detection and prevention using EIGRP protocol based on round trip time. *J. Cyber Secure. Mobil.* **2018**, *7*, 215–228.

52. Kori, S.; Krishnamurthy, G.N.; Sidnal, N. Distributed Wormhole Attack Mitigation Technique in WSNs. *Int. J. Comput. Netw. Inf. Secure* **2019**, *11*, 20–27.

53. Gayathri, S.; Seetharaman, R.; Subramanian, L.H.; Premkumar, S.; Viswanathan, S.; Chandru, S. Wormhole Attack Detection using Energy Model in MANETs. In Proceedings of the 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 21–23 August 2019; pp. 264–268.

54. Deshmukh-Bhosale, S.; Sonavane, S.S. A real-time intrusion detection system for wormhole attack in the RPL-based Internet of Things. *Procedia Manuf.* **2019**, *32*, 840–847.

55. Thanuja, R.; Ram, E.S.; Umamakeswari, A. A linear-time approach to detect wormhole tunnels in mobile Adhoc networks using 3PAT and transmission radius (3PAT w). In Proceedings of the 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2018; pp. 837–843.

56. Harsányi, K.; Kiss, A.; Szirányi, T. Wormhole detection in wireless sensor networks using spanning trees. In Proceedings of the 2018 IEEE International Conference on Future IoT Technologies (Future IoT), Eger, Hungary, 18–19 January 2018; pp. 1–6.

57. Tamilarasi, N.; Santhi, S.G. Detection of Wormhole Attack and Secure Path Selection in Wireless Sensor Network. *Wirel. Pers. Commun.* **2020**, *114*, 329–345.

58. Scholar, M.T.; Yadav, B. Predication and Root Selection of Worm Hole Attack in WSN. *Int. J. Sci. Res. Eng. Trends* **2019**, *5*, 1937–1944.

59. Scholar, M.T.; Kant, R.; Sen, A.D. Collaborative Decision for Wormhole Attack Prevention in WSN. *Int. J. Sci. Res. Eng. Trends* **2020**, 6, 212.

60. Chatla, A.B. Trust-Based Secure Network For Detection Of Attacks (Wormhole And Black Hole) Due To Malicious Nodes In Ad Hoc Wireless Sensor Network. *Turk. J. Comput. Math. Educ. TURCOMAT* **2021**, *12*, 2763–2769.

61. Bhushan, B.; Sahoo, G. Detection and defense mechanisms against wormhole attacks in wireless sensor networks. In Proceedings of the 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall), Dehradun India, 15–16 September 2017; pp. 1–5. https://doi.org/10.1109/ICACCAF.2017.8344730.

62. Li, J.; Wang, D.; Wang, Y. Security DV-hop localization algorithm against wormhole attack in wireless sensor network. *IET Wirel. Sens. Syst.* **2018**, *8*, 68–75.

63. Kaur, P.; Kaur, D. Performance Evaluation of the Proposed Wormhole Detection Scheme with Existing Schemes. *Wirel. Pers. Commun.* **2021**, *119*, 1–11.

64. Bhosale, S.A.; Sonavane, S.S. Wormhole Attack Detection System for IoT Network: A Hybrid Approach. *Wirel. Pers. Commun.* **2021**, *124*, 1081–1108.

65. Athmani, S.; Bilami, A.; Boubiche, D.E. EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs. *Futur. Gener. Comput. Syst.* **2019**, *92*, 789–799.

66. Ahlawat, P.; Dave, M. An attack resistant key predistribution scheme for wireless sensor networks. *J. King Saud Univ. Comput. Inf. Sci.* **2021**, *33*, 268–280.

67. Shukla, M.; Joshi, B.K.; Singh, U. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. *Wirel. Pers. Commun.* **2021**, *121*, 1–24.

68. Patel, M.A.; Patel, M.M. Wormhole Attack Detection in Wireless Sensor Network. In Proceedings of the International Conference on Inventive Research in Computing Applications, ICIRCA, Coimbatore, India, 11–12 July 2018; pp. 269–274. https://doi.org/10.1109/ICIRCA.2018.8597366

69. Jagadeesan, S.; Parthasarathy, V. Design and implement a cross-layer verification framework (CLVF) for detecting and preventing black hole and wormhole attack in wireless ad-hoc networks for cloud environment. *Clust. Comput.* **2019**, *22*, 299–310.

70. Chezhiyan, D.U. Measurement-based analysis of reactive protocols in manet. *Int. J. Wired Wirel. Commun.* **2013**, *1*, 60562730. Available online: https://api.semanticscholar.org/CorpusID:60562730 (accessed on 28 May 2022).

71. Sobral, J.V.; Rodrigues, J.J.; Rabêlo, R.A.; Al-Muhtadi, J.; Korotaev, V. Routing protocols for low power and lossy networks in internet of things applications. *Sensors* **2019**, *19*, 2144.

72. Kambalimath, S.; Deka, P.C. A basic review of fuzzy logic applications in hydrology and water resources. *Appl. Water Sci.* **2020**, *10*, 1–14.

73. Gupta, D.; Gupta, U. On robust asymmetric Lagrangian ν-twin support vector regression using pinball loss function. *Appl. Soft. Comput.* **2021**, *102*, 107099.

74. Yap, K.Y.; Sarimuthu, C.R.; Lim, J.M.Y. Artificial Intelligence Based MPPT Techniques for Solar Power System: A review. *J. Mod. Power Syst. Clean Energy* **2020**, *8*, 1043–1059.

75. Purkar, S.V.; Deshpande, R.S. A review on energy-efficient clustering protocols of heterogeneous wireless sensor network. *Int. J. Eng. Technol.* **2017**, *9*, 2514–2527.