AI-Based Wormhole Attack Detection Techniques

Subjects: Computer Science, Artificial Intelligence

Contributor: Maria Hanif, Humaira Ashraf, Zakia Jalil, Noor Zaman Jhanjhi, Mamoona Humayun, Saqib Saeed, Abdullah M. Almuhaideb

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.

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 consisting 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].

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.

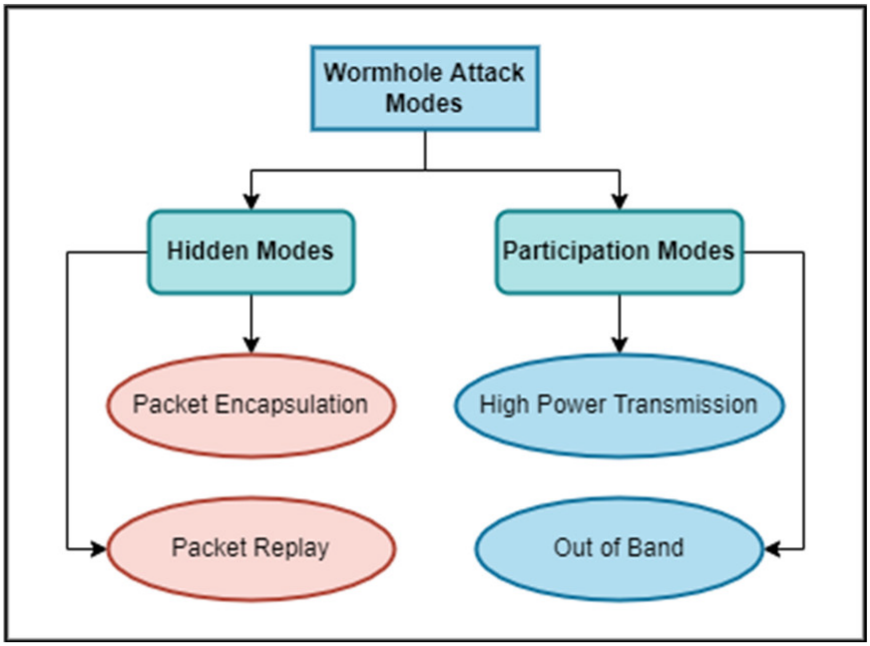

Figure 1. Classification of wormhole attacks based on hidden and participating nodes.

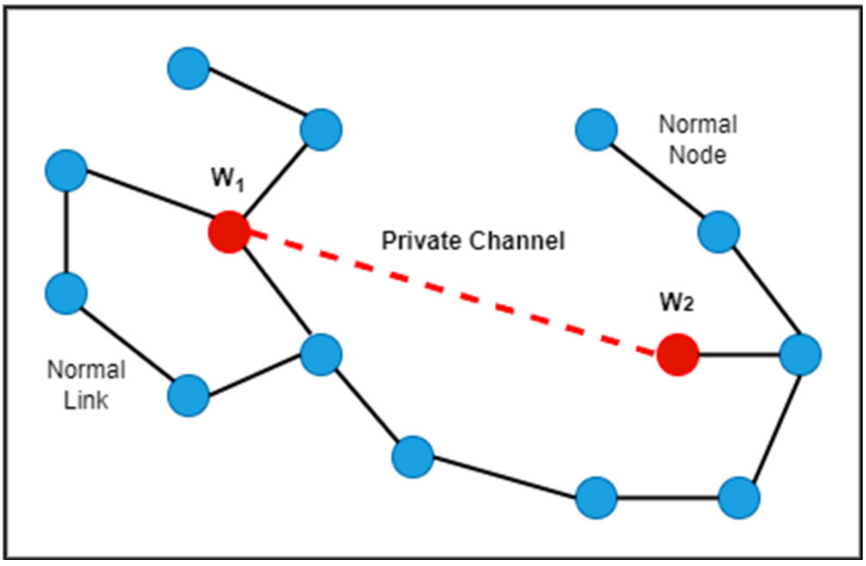

Figure 2. External wormhole attack with high power transmission.

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.

Table 1. Summary of surveys of wormhole detection techniques.

Year	Main Focus of Survey	Major Contributions	Enhancements in this research
2020	Survey wormhole attack detection and prevention techniques in WSN	Mohit et al. [12] 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.	This research presents a detailed performance analysis, including critical analysis and results comparison, and identified the gaps in all existing schemes.

Year	Main Focus of Survey	Major Contributions	Enhancements in this research
2018	Detection and prevention analysis of wormhole attacks in wireless sensor networks	Kumar et al. [13] presented a comparative analysis of several techniques, including reputation-based routing, Packet leashes, Beacon nodes, LITEWORP, and algorithms using active nodes. However, the study did not include the strengths and limitations of the existing schemes.	This research 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. [14] 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.	This research 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. [15] 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.	This research 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. [16] 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.	This research 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. [17] 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.	This research 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. [18] 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.	This research 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. [19] 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.	This research presents a comprehensive critical analysis of all existing schemes. Moreover, research gaps and challenges are identified.

2. Artificial Immune Systems and Machine Learning-Based Systems

The research of Ref. [20] 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. [21] 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. [22] 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. [23] 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. [24] 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. [25] 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. [26] 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. [27] 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. [28] 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. [29] 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. [30] 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 3** shows the classification of AI-based schemes for wormhole detection in WSNs.

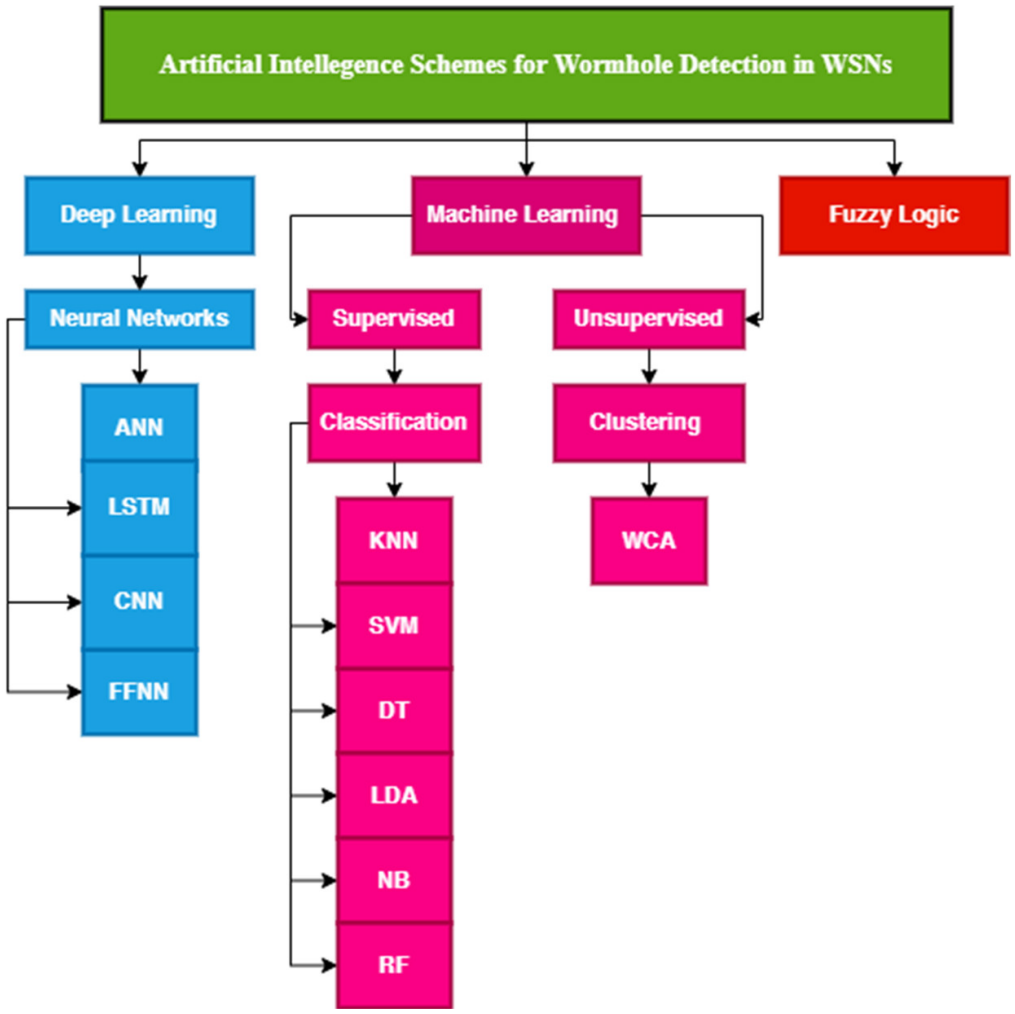

Figure 3. Classification of AI- and ML-based wormhole detection schemes.

3. Neighbor Discovery-Based Systems

The research of Ref. [31] 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. [32] 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. [33] 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. [34] 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. [35] 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. [36] 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. [37] 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. [38] 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.

4. AODV Protocol-Based Systems

The research of Ref. [39] 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. [40] 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. [41] 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. [42] 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.

5. RTT-Based Systems

The research of Ref. [43] 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. [44] 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 2** briefly presents a summary of methodologies of wormhole detection schemes.

Table 2. Summary of methodologies of wormhole detection schemes.

	Ref.	Scheme	Methodology
Neighbours discovery based	[31]	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.
	[32]	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).
	[33]	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.
	[34]	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.
	[35]	MaxIS scheme	The proposed method uses a greedy algorithm to search for intruders in maximum independent sets with forbidden sub-structures.
	[36]	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.
	[37]	ESPMAW scheme	This scheme uses the AODV routing protocol, neighbour, and connectivity information to find intruders in the system.
	[38]	SDN-based scheme (SWANS)	This scheme uses the information of neighbour similarity for the detection of wormholes in software-defined networks.

	Ref.	Scheme	Methodology
AODV protocol-based schemes	[39]	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.
	[40]	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.
	[41]	AODV based scheme	AODV, OSLR, and ZRP are used to detect malicious nodes in the wireless sensor network.
	[42]	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	[43]	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.
	[44]	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.
	[45]	EIRGP and RTT-based scheme	This scheme uses the EIGRP protocol and round-trip time for the detection of intruders.
	[46]	Trust-based scheme	This scheme uses RTT and AODV protocols for detecting malicious nodes.
High-power transmission based	[47]	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.
	[48]	RPL-based scheme	The RPL routing protocol is used with the RSSI value to detect malicious nodes in the network.

	Ref.	Scheme	Methodology
Path selection	[49]	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.
	[50]	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.
	[51]	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	[52]	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.
	[53]	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.
	[54]	HCBS protocol-based scheme	This scheme detects malicious nodes in clusters by using the heterogeneous cluster-based secure directing convention (HCBS) protocol.
	[55]	LITS scheme	This scheme uses a verification process of two replayable control messages and time synchronization to detect malicious nodes.
Hop count and Weight-based	[56]	WDV-hop scheme	This scheme first detects suspicious nodes by using hop count, calculates localization error for them, and drops the malicious nodes.
	[57]	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.
	[58]	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.

	Ref.	Scheme	Methodology
Authentication Key-based	[59]	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.
	[60]	HKP-HD scheme	This scheme uses key generation and its pre-distribution to reduce the chance of attacker nodes.
	[61]	Elliptic curve cryptography scheme	This scheme uses elliptic curve cryptography with the AODV protocol for wormhole attack-free networks.
Mobile agent and Cloud-based	[62]	Visiting centre local-based scheme	This scheme introduces a mobile agent in the network which is responsible for distinguishing malicious nodes from normal nodes.
	[63]	Cross-layer verification scheme	This scheme presents a cross-layer verification framework (CLVF) to find intruders in the system.

The research of Ref. [45] 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. [46] 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.

6. High-Power Transmission-Based Systems

The research of Ref. [47] 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. [48] 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%.

7. Path Selection-Based Systems

The research of Ref. [49] 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. [50] 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. [51] 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.

8. Statistical Method-Based Systems

The research of Ref. [52] 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. [53] 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. [54] 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.

9. Hop Count and Weight-Based Methods

The research of Ref. [55] 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. [56] 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. [57] 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. [58] 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.

10. Authentication Key-Based Systems

The research of Ref. [59] 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. [60] presented a hybrid key pre-distribution scheme (HKP-HD) scheme, which reduces the chances of sensor nodes being attacked.

The research of Ref. [61] 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.

11. Mobile Agent and Cloud-Based Systems

The research of Ref. [62] 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. [63] 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.

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. 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.
13. 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.
14. 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.
15. 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.
16. Ghugar, U.; Pradhan, J. Survey of wormhole attack in wireless sensor networks. Comput. Sci. Inf. Technol. 2020, 2, 33–42.
17. 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).

18. 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.
19. 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.
20. Jamali, S.; Fotohi, R. Defending against Wormhole Attack in MANET Using an Artificial Immune System. New Rev. Inf. Netw. 2016, 21, 79–100.
21. 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.
22. 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.
23. 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.
24. KP, K.S. Delta Ruled First Order Iterative Deep Neural Learning for Sybil and Wormhole Attacks Detection in Healthcare Wireless Sensor Network. Preprint 2021.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.
33. 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.
34. 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.
35. 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.
36. 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.
37. Aliady, W.A.; Al-Ahmadi, S.A. Energy preserving secure measure against wormhole attack in wireless sensor networks. IEEE Access 2019, 7, 84132–84141.
38. 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.
39. 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.

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

41. 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.

42. 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.

43. 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.

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

45. 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.

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

47. 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.

48. 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.

49. 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.

50. 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.

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

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

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

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

59. 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.

60. 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.

61. 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.

62. 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.

63. 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.