Review Article

Chitvan Gupta, Laxman Singh*, and Rajdev Tiwari

Wormhole attack detection techniques in ad-hoc network: A systematic review

https://doi.org/10.1515/comp-2022-0245
received February 2, 2022; accepted June 5, 2022

Abstract: Mobile ad hoc networks (MANETs) are considered as decentralized networks, which can communicate without pre-existing infrastructure. Owning to utilization of open medium access and dynamically changing network topology, MANETs are vulnerable to different types of attacks such as blackhole attack, gray hole attack, Sybil attack, rushing attack, jellyfish attack, wormhole attack (WHA), byzantine attack, selfishness attack, and network partition attack. Out of these, worm hole attack is the most common and severe attack that substantially undermines the performance of the network and disrupts the most routing protocols. In the past two decades, numerous researchers have explored the number of techniques to detect and mitigate the effect of WHAs to ensure the safe operation of wireless networks. Hence, in this article, we mainly focus on the WHAs and present the different state of art methods, which have been employed in previous years to discern WHA in wireless networks. The existing WHA detection techniques are lacking due to usage of additional hardware, higher delay, and consumption of higher energy. Round trip time (RTT) based detection methods are showing better results as they do not require additional hardware. Machine learning (ML) techniques can also be applied to ad-hoc network for anomaly detection and has a great influence in future; therefore, ML techniques are also analyzed for WHA detection in this article. SVM technique is mostly used by the researchers for outstanding results. It has been analyzed that hybrid approach which uses the traditional detection technique and ML technique are showing better results for WHA detection. Finally, we have identified the areas where further research can be focused so that we can apply the WHA detection methods for larger topological area for more flexibility and accurate results.

Keywords: mobile ad-hoc network, artificial immune system, round trip time, machine learning, supervized learning

1 Introduction

In the past years, significant advancement has been taken place in the field of wireless network, which includes emerging number of different movable handheld devices such as laptops, smart phones, and Internet of Things (IoT) based devices [1,2]. Wireless communication has become an integral part of our lives due to availability of Wi-Fi access points in public places such as restaurants, bus stands, railway stations, hotels, and even in small shops where people can use these access points for surfing internet [3,4]. In ad-hoc networks, wireless devices can communicate with each other and share information via infrastructure less network. The nodes in ad-hoc network are responsible for discovering neighbor nodes to create a dynamic network for the transmission of data from source to destination. The nodes move to and fro in the network and communicate with other nodes in an arbitrary manner that cause the change in network topology in a random as well as in an unpredictable manner [5,6]. Nodes in ad-hoc network are capable of data collection, data storage, and processing and forwarding of information. Mobile nodes work in a self-organizing manner and create a dynamic topology in ad-hoc network. The property of nodes to detect the presence of other nodes makes the network reliable and can share the information securely. For instance, in battlefield, the video can be shared among the soldiers so that they can become aware of current situation in the battlefield [7]. In regard to disaster management, ad-hoc network plays an important role in disaster relief operations [8]. Wireless network IEEE 802.11 uses basic service set (BSS), which consist of access point and includes all the stations associated with it [9], while

* **Corresponding author: Laxman Singh,** Department of Electronics and Comm., Noida Institute of Engineering & Technology, Greater Noida, U.P., India, e-mail: laxman.mehlawat2@gmail.com
Chitvan Gupta: Department of Computer Science & Engineering, Dr. A.P.J. Abdul Kalam Technical University, Lucknow, U.P., India; G.L. Bajaj Institute of Technology and Management, Greater Noida, India, e-mail: chitvangupta@gmail.com
Rajdev Tiwari: CEEKH Edunix Pvt. Ltd., Noida, Uttar Pradesh, India, e-mail: drrajdevtiwari@gmail.com

ad-hoc network architecture uses IEEE 802.11 independent BSS (IBSS) as illustrated in Figure 1. Hence, there is no requirement of access point in ad-hoc network and the nodes can communicate in a distributed peer to peer manner. The least requirement of IBSS-based network is that nodes should lie within the radio range of each other.

Ad-hoc network has great potential to work as infrastructure less network for numerous critical applications due to low cost and easy deployment [10]. Ad hoc networks are also called as "on the fly" network or spontaneous network. For short range of communication, it provides effective solutions in some complex situations such as disaster management, weather monitoring, battlefield, sensing environment, and rescue operations [11–13]. There are different types of networks, which we encounter in our day-to-day life activities such as vehicular ad-hoc network, smart phone ad-hoc network, sensor network, smart home lightening network, robotic ad-hoc network, hospital ad-hoc network, and IEEE 802.15.3 wireless PAN are few of them. Other applications can be enumerated as mobile conferencing, e-health, Bluetooth, wireless fidelity IEEE 802.11, and data acquisition operations [14–17]. In mobile ad-hoc network, majority of the nodes are mobile nodes, where some of the nodes are treated as fixed wireless access point and the rest as relay nodes for transmitting information to remote nodes temporarily [18]. Every node in ad-hoc network has wireless interface for communication through radio frequency. There is no central administration to control the network. Therefore, ad-hoc network is a non-collapsed network because of additional facility for some nodes to leave and enter the network at any point of time as per the requirement [19]. Ad-hoc network is also called as multi-hop network due to the capability of nodes to behave as router owning to their limited transmission range in the network [20]. Every node in the network should be willing to forward the packets to the destination point without any interruption.

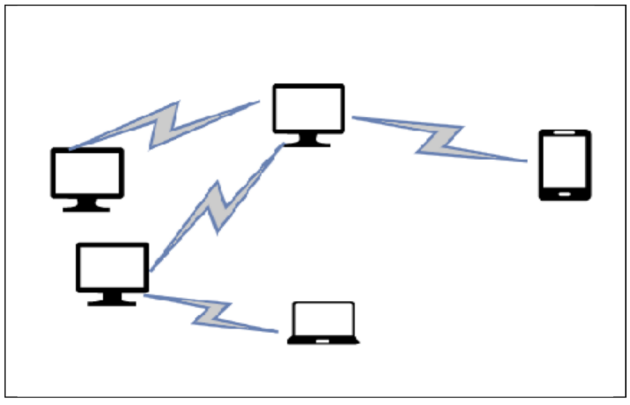

Figure 1: Ad-hoc network architecture using independent BSS.

In recent years, various new machine learning (ML) approaches and other hybrid conventional methods have been explored by researchers to address the issues related to detection of wormhole attack (WHA) in ad-hoc networks. Hence, we conduct a systematic literature review (SLR) with the prime aim of making the readers familiar about the advantages and limitations of latest ML techniques. The present study also focuses on exploring the associated challenges of the developed methods with regards to the detection of WHAs. Besides, we also emphasized on potential solutions highlighting future research directions for the early detection of WHA.

Hence, the presented SLR may provide a great help to the readers and research community while selecting any suitable approach to develop an efficient method for the detection of WHA. In this study, we present a review of various traditional and ML methods and their usage for the detection and classification of WHA. To achieve this, the present review article includes the following segments.

1.1 Exploration criteria

Through this SLR, we tend to identify various studies contributing to wormhole attack detection (WHAD) using traditional and ML techniques. In the present SLR, we tried to answer the following questions:

- Which traditional techniques exist to detect WHA?
- Which ML techniques are currently used to detect WHA?
- Which data resources are used for the detection of WHA?
- What are the advantages and limitations of the recently developed ML techniques?

We searched several electronic databases, including springer link, Science Direct (Elsevier) (http://www.sciencedirect.com), IEEE Xplore (http://www.ieeexplore.ieee.org), and PubMed (https://www.ncbi.nlm.nih.gov/pubmed/). During the search, the articles were chosen based on the "Title of an article," "abstract," and "Keywords" such as "Wormhole," "Detection," "Attacks in Ad-hoc network," and "ML" for inclusion or exclusion in the study. In cases where the paper title was found insufficient to decide whether the paper ought to be included or excluded in the SLR, we thoroughly studied the abstract along with the title of the research paper. Figure 2 presents the inclusion steps that indicates the systematic approach to include or exclude the articles in this study.

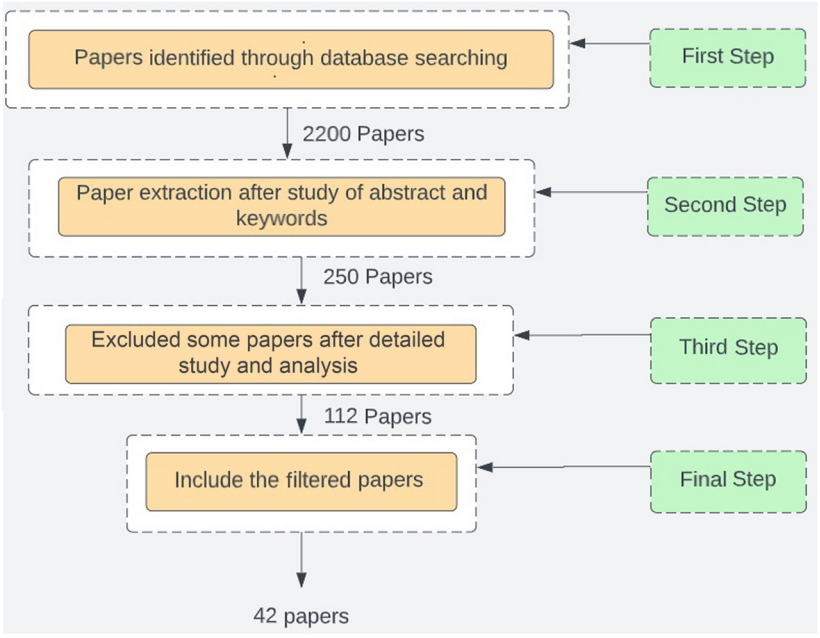

Figure 2: Paper inclusion steps.

Initially, about 250 relevant papers were extracted from large number of documents. We evaluated all relevant studies, but included only those which satisfied the following criteria:

- Studies focusing on WHA detection only
- Performance of techniques used such as detection rate and packet delivery rate
- A ML technique used for detection
- Articles must be full papers (not abstracts only)
- Published work between 2011 and 2021.

Based on the above criterion, only 42 studies (47%) were included, while the remaining 70 studies were excluded as they did not match the inclusion criteria. During the search, significant articles pertaining to computational intelligence were found. The journal name, publisher, and the number of articles published in the journal are listed in Table 1 and Figure 5.

This study includes 24 traditional methods and 18 ML-based methods for WHAD from 2011 to 2021. This review enables us to find what challenges need to be addressed and which parameter can be used to improve the performance of WHA detection approach. Our review is executed by following research queries such as:

- What traditional WHA detection methods exist so far?
- Which methods are most popular and widely used for WHA?
- What ML-based current state of art methods are used for WHA detection?
- What are the parameters used to evaluate the performance measure of WHA detection methods?

Further, the rest of the article is organized as follows: Section 2 lists out the various constraints in ad-hoc network, while Section 3 contains types and classification of attacks on ad-hoc network. In Section 4, we discussed the WHA and its severity on ad-hoc networks. Performance metrics to measure the performance of approach for WHA detection are elaborated in Section 5. Section 6 focusses on the classification of WHAD methods based on time, topology, neighbor, location, artificial intelligence, and ML. Various studies are analyzed in Section 7, whereas Section 8 explores various ML-based approaches used for WHA detection. Section 9 elaborated the result and discussion based on literature review. Further, advantages and issues in ML techniques are listed in Sections 10 and 11, respectively. Finally, we have found the research gap and suggested the possible solution to the problem, which are given in Section 12. Section 13 concludes the article.

2 Constraints in ad-hoc network

Some of the challenges which limits the normal operation of ad-hoc network are dynamic topology, self-organization, limited battery power of nodes, mobility, and changes in

Table 1: Published papers in relevant field

Elsevier	IEEE	Miscellaneous (PubMed)	Springer
Pervasive and Mobile Computing (1)	IEEE Transactions on Mobile Computing (1)	Sensors (2)	Networks and Communications (1)
Journal of Information Security and Applications, Elsevier (1)	Computer Networks (1)	Journal of Network and Computer Applications (1)	Wireless Network (1)
Computers & Security, Elsevier (1)	IEEE Access (4)	International Journal of Distributed Sensor Networks (Hindawi) (3)	Wireless Personal Communication (3)
Procedia Computer Science (2)	IEEE transaction on parallel and distributive computing (1)	Journal of Computer and System Sciences (1)	The Journal of Supercomputing (1)
Engineering Science and Technology, an International Journal (1)	10th ICCCNT Conference (1)	Geographic Wormhole Detection in Wireless Sensor Networks (1)	Journal of Medical Systems (1)
		John Willey & Sons Ltd, Special Issue on Advances in Metaheuristic Optimization Algorithms (1)	Soft Computing (2)
		Journal of Cyber Security and Mobility (1)	International Conference on Advanced Information Networking and Applications, WAINA 2019 (1)
		New Review of Information Networking, (Taylor & Francis) (1)	
		Iranian Conference on Intelligent System (1)	
		Journal of Electrical and Computer Engineering (1)	
		Wireless Communication and Mobile Computing, Hindawi (2)	
		International Journal of Communication Networks and Information Security (1)	
		Computers, Materials & Continua Tech Science Press (2)	

link and security [21]. Figure 3 presents the block diagram representing the constraints in ad-hoc network.

2.1 Wireless link

Ad-hoc network is an autonomous system, wherein wireless link connects several nodes in network without any physical connection. In the wired network, user needs to pass the firewalls and gateways, while in the ad-hoc network, there is no need of such types of protection walls due to the usage of wireless link [22,23]. Therefore, each node communicates with each other using radio waves effectively. The nodes can instantly move from a network as per the requirement, resulting in the unauthorized access that might affect the network by destroying the data or sending virus messages in the network. The

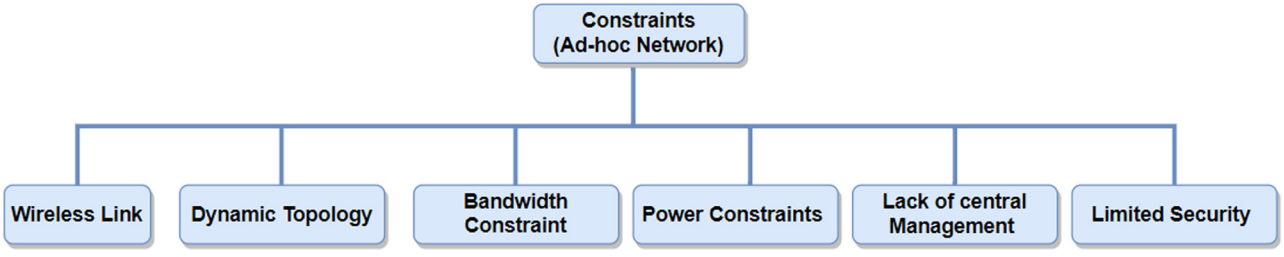

Figure 3: Block diagram representing the constraints in ad-hoc network.

wireless links are less secure owing to higher flexibility and open space, therefore, are unreliable and more prone to interference and high traffic jam [24].

2.2 Dynamic topology

Ad-hoc network is a collection of dynamic nodes, which, in general, exhibits highly dynamic characteristics. The wireless links in ad-hoc network usually have a relatively high bit error rate, making it difficult to conduct controlled, repeatable experiments with routing and other protocol in such dynamic environment. To address this problem, Lin et al. [25] developed a switch that connects multiple unaltered hosts according to the controllable dynamic topology with a controlled bit error rate on the links. Owing to the dynamic network topology, the network may vary rapidly in an unpredictable manner, therefore, routing tables need to be updated in case of proactive routing [26]. Whereas, in reactive routing, the routes are discovered at the time of communication by using route request packet [27].

2.3 Bandwidth constraints

Available bandwidth in ad-hoc network poses a challenge due to shared and open wireless links. The wireless links are more susceptible to noise, interference, and signal attenuation effects [28]. There are bandwidth issues in ad-hoc network due to multiple connections as the bandwidth of a node is shared for different connections.

Preetha et al. [29] explained how multiple connections are formed in AODV routing protocol. To solve the bandwidth problem in AODV routing protocol, the bandwidth of intermediate nodes is calculated during route discovery phase. If the intermediate nodes are capable enough to withstand all the connections including new connections, only then the path is created, otherwise new path needs to be searched.

2.4 Power constraints

Ad-hoc network is a collection of thousands of nodes for collecting information and passing it to the concerned node leading to power consumption at nodes. Nodes in ad-hoc network may have a substantial power constraint in terms of limited battery power. Due to power constraints, some of the nodes used to drop the packets of other nodes lead a to rise in malicious attacks. Therefore, it is essential to save the nodes power to avoid ease dropping of packet at the affected nodes. Various power control algorithms have been proposed by different researchers and scientists for the same, based on node degree, location information, graph theory, and game theory approach [30,31]. For instance, Rulnick and Bambos [32] proposed local and global strategies for power saving in ad-hoc network. In local strategy, the network nodes are in power saving mode by reducing the energy requirement during the transmission. Local policies operate on MAC and physical layers of the network. Whereas in global strategy, the network lifetime is maximized by putting some node in sleeping state and connected nodes in active state [33]. Anand and Sasikala [34] suggested Intelligent routing AODV technique for reducing the energy consumption in ad-hoc network by calculating the distance of nodes. The distance was calculated by a process called received signal strength (RSS) indication. A node was selected for transmission from the nodes lying in the same region, while other nodes were deactivated for transmission, same is applied for the case of acknowledgement [34].

2.5 Lack of central management

Owing to the lack of centralized management, it is difficult to control and monitor the traffic at large scale. Lack of central management and dynamic property of network leads to security attacks and obstruct the trust management in ad-hoc networks [35]. Nodes in ad-hoc network works in cooperative manner but due to decentralization, some attacks can break the cooperative algorithms. To address the issues caused due to the lack of central management, Faisal et al. [36] proposed a scheme based on RSS, which was able to detect the unauthorized clone node with fake identification. RSS can locate the node with unique location. Nodes messaging from the same location, indicates that there is unauthorized clone node at that location.

2.6 Limited security

Other than above constraints, ad-hoc network is vulnerable to other attacks such as fabrication, modification, interception, impersonation, and eavesdropping. Wang

et al. [37] proposed a method for securing the network from eavesdropping using directional antenna. Kao and Marculescu [38] proposed to minimize eavesdropping by controlling transmission power. Ad-hoc network may lack in some security services such as availability of data, authentication of nodes, data confidentiality, integrity, and non-repudiation [39]. Seno et al. [40] introduced a cluster-based distributed certification authority and secure cluster-based routing protocol for securing ad-hoc network. Owing to flexibility of ad-hoc network, the nodes may leave or join the network. The nodes lying in radio range of network can automatically join the network as well as transfer the information to other nodes within the network. Ad-hoc network may easily get affected by attacks due to movement of nodes. Due to lack of secure boundaries, ad-hoc networks have higher probability of getting affected by attacks [41,42]. Aluvala et al. [43] proposed a novel technique for node authentication in ad-hoc network. While Kumar et al. [44] proposed the elliptic curve cryptography technique for authentication of nodes in ad-hoc network.

Based on the above constraints, there is need of efficient routing protocol as well as security measures to get stable and reliable operation of ad-hoc network. Certain protocols have been developed by researcher community to deal with the reduction in delay, packet drop ratio, latency, average throughput [45,46] but the complex parameters like energy consumption, reliability [47], and mobility [48] are still there.

3 Attacks on ad-hoc networks

Ad-hoc network should have the ability to handle all types of issues like topological changes and node malfunction issues that occur after applying network reconfiguration methods [49]. In case a node leaves the network and causes broken links, the affected nodes can request for new routing paths immediately for continuous transmission on network [50]. Disconnected links and complaints of nodes for new routing updates can cause issues of delay and traffic jam but network stays operational [51]. In addition to the issues stated above, the ad-hoc network performance might get affected due to the presence of several attacks also. Ad-hoc networks are susceptible to network attacks due to the following reasons [52–54]: (i) absence of central administration that can authenticate the nodes, (ii) multi-hop communication, (iii) dynamic and frequently changing topology, (iv) limited energy consumption, and (v) lack of secure routing protocols owing to low processing power of nodes. Due to above constraints, the ad-hoc network is unreliable, and its performance get affected by different attacks as illustrated in Figure 3.

3.1 Classification of attacks

As revealed in Figure 4, attacks in ad-hoc network can be substantially classified as: active attacks and passive attacks. In active attack [55], attackers try to demolish the content of message transmitted over the network, while in case of passive attacks [56], an attacker utilizes the information for malicious purpose without disrupting the usual operation of the network. Both types of attacks are described in considerable detail in the following section.

3.1.1 Active attacks

Active attacks are major attacks which affect the network by preventing the data transmission between the nodes [57]. In active attacks, the prowler creates malfunction activities like modifying, mingling, forging, fabricating, and dropping the data packets, which interrupts the normal functioning of the network. It can fail the entire

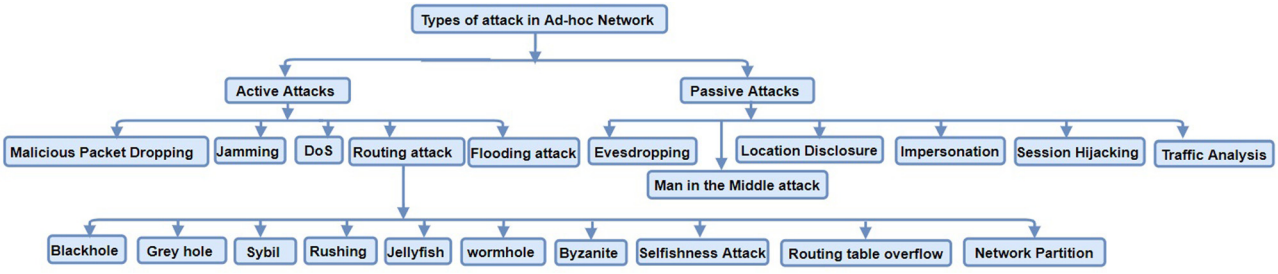

Figure 4: Types of attacks on Ad-hoc network.

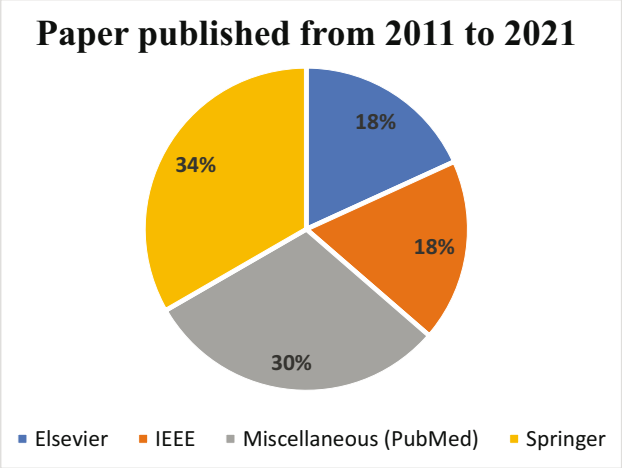

Figure 5: Paper published in relevant journals.

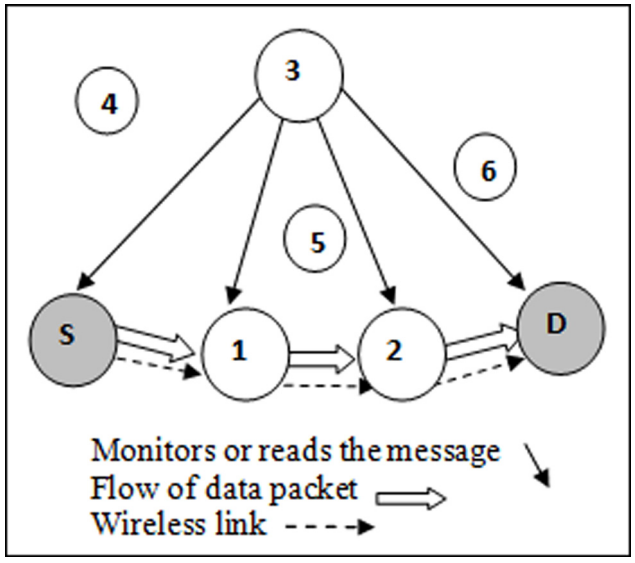

Figure 6: Passive attack in ad-hoc network.

network or degrade the performance of the network gradually [58]. Selfish nodes are the causes of active attacks and can be treated as malicious nodes later. Selfish nodes are the nodes that do not forward the packet to other nodes for their own benefit such as saving energy, whereas malicious nodes drop or modify the packets to interrupt the network performance [59]. Active attacks can be further categorized as: (i) malicious packet dropping; (ii) jamming the network; (iii) denial of service (DoS); (iv) routing attacks; and (v) flooding attacks [60]. Routing attacks are the major attacks that can harm the network by intruding routing information [61]. Blackhole attack [62–72], gray hole attack [73–75], Sybil attack [76,77], rushing attack [78], jellyfish attack [79], WHA [80,81], byzantine attack [82], selfishness attack [83], routing table overflow [84,85], and network partition [86] are some of the attacks which fall under the category of routing attack. These attacks impact the proper functioning of routing protocols by injecting fake information, altering data packets and dropping information of control packet during the discovery process of routing information [20]. These attacks are caused by the malicious nodes, which do not follow the set of protocols. However, some of the attacks like gray hole, rushing, and jellyfish attack follows the set of protocols yet disturbs the proper functioning of routing process [87–90].

3.1.2 Passive attack

Passive attacks do not disturb the network function directly. However, the intruder snoops the data floating in the network without altering it [91]. Figure 6 demonstrates the scenario of passive attack, where node 3 monitors the data transmitting in the network from source to destination.

It is difficult to discern the passive attacks as the proper operation of network does not get affected by passive attacks. Malicious nodes cause the passive attacks [92]. Applications of powerful encryption techniques can mitigate the number of passive attacks but at the cost of increased overhead [93,94]. Numerous attacks such as Eavesdropping, man in the middle attack, location disclosure, impersonation, session hijacking, and traffic analysis constitute the passive attacks [95,96].

4 WHA and its severity

Among the above discussed attacks, WHA is the most severe attack as per the literature [97,98]. It can greatly affect the confidentiality, availability, and overall security of the network. Consequences of WHA are listed below [99]:

- Destroying network topology and disturbing routing procedures
- Stumbling communication of nodes
- Dropping packets selectively
- Lead to traffic congestion
- Modification in data packets
- Changing sequence of packets
- Leakage of confidential information by monitoring and analyzing traffic
- Lead to DoS attack

Therefore, in subsequent sections, we shall primarily focus on the detection and prevention methods of WHA,

which is currently of prime concern for the research community as well as for the service providers.

Meghdadi et al. [100] analyzed the impact of WHA in the ad-hoc network and found it responsible for 32% data failure, leading to high security risk in wireless networks [101]. In shortest path routing, hop count was used as a metric for finding the shortest path.

As discussed earlier, the WHA are also known as replaying attack due to regenerating capability of packets in the network. Therefore, in the current and subsequent sections, we shall use the terms "wormhole attack" and "replaying attack" interchangeably. In replaying attack, any opponent node regenerates the packets for unauthorized illusion [101]. The malicious nodes create the illusion such that the two geographically remote nodes got directly connected and appear as neighbors even when being far away from each other [102]. The purpose of wormhole attack is to create man in the middle attack and drop the packets. A tunnel is created between two malicious nodes where one acts as a source node and the other acts as a destination node [103–105]. Tunnel may be the wired link or long-range high bandwidth wireless link that operates at different frequency bands. This tunnel is known as WHA. Wormhole nodes make illusion of shorter route in the network as compared to the original route [106,107]. It creates dilemma in the routing process by including fake nodes, which are not present in the routing table. Wormhole makes the malicious node attractive creating an easy path for other packets to go through. Actual routes are not discovered by the nodes due to WHA [108]. As we can see in Figure 7, the malicious nodes 4 and node 5 are distinct to each other and are connected through the tunnel. The malicious node 4 receives the data packets at one node and tunnels them to another malicious node 5. The route from node 4 to node 5 disturbs the routing process by making the tunnel. This tunnel has the lowest cost path from source S to destination D. Therefore, this tunnel path is selected for transmission and packets transmitting through this path are dropped by malicious node [109]. Wormhole links can be periodically turned on or off by the intruder, therefore possessing higher chances of destroying and affecting the routing protocols of the network [110].

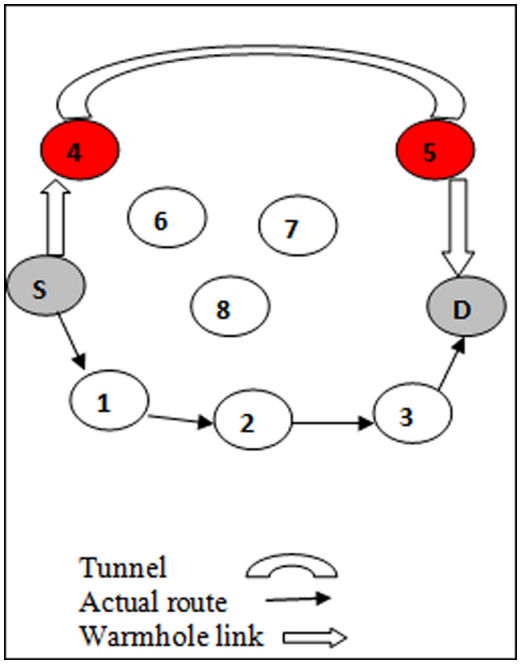

Figure 7: Tunnel between malicious nodes 4 and 5 due to wormhole attack.

4.1 Modes of WHA

There are two modes of WHA: (i) hidden mode (HM) and (ii) participation mode (PM). HM wormhole nodes are not visible to authenticated nodes as HM nodes do not deal with routing the packets [111]. HM wormhole attack merely targets the tunnel and forwards the packets to other malicious node without having entries in routing table. Whereas in participation mode, nodes are visible to authentic nodes as PM nodes participate in the routing process. PM node tunnels the packet to other PM nodes and can control the performance parameters of the network. A shortcut tunnel is created between two PM nodes or HM nodes either by in band (IB) or by out band (OB) channel [99] as illustrated in Figure 8. When wormhole nodes tunnel the packets through legitimated nodes, it is called as IB channel. P and Q malicious nodes tunnel the packets through authenticated nodes A and B, whereas in OB channel, two malicious nodes get connected using external link such as directional antenna or network cable [112].

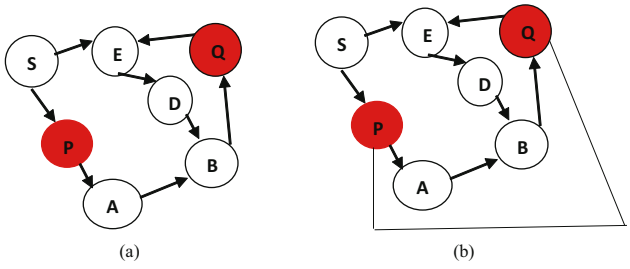

Figure 8: (a) In band channel and (b) out band channel.

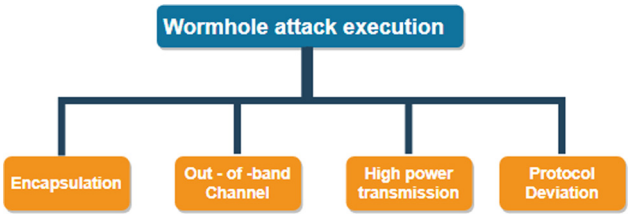

Figure 9: Wormhole attack execution.

4.2 Types of WHA based on the attack execution

WHA is a network layer attack that attacks the network without the knowledge of cryptography techniques. Therefore, it is difficult to detect WHA. There are number of ways to execute the WHA as shown in Figure 9. Encapsulation, out of bound channel, high power transmission, and protocol deviation are the major execution methods. In the encapsulation method, there are multiple nodes in the path of malicious node which might not be aware of suspicious nodes. In this technique, the packets are encapsulated and travel through the tunnel with less hop count [113]. The other packets also use the same link between the suspicious node [114]. In out of bound channel approach, the suspicious nodes are directly connected through the high bandwidth external wired or long-range wireless channel. It requires extra hardware and there is no need of encapsulation [112]. In high power transmission approach wormhole attack uses two suspicious nodes connected through high power transmission link. Suspicious nodes having high transmission capabilities and attracts more packets [115,116]. WHA are also created due to violation of network protocols to attract more packets. Attracting more packets are also known as rushing attacks [117,118].

4.3 Selection of detection features for WHA

In WHAD, extra resources are needed for recording detection features during the communication [119]. For instance, extra hardware is required for time and location feature. Location and data packet features need promiscuous mode, where all packets are monitored by all the nodes as well as by a controller node. The detection techniques, which use route reply and neighborhood features may not work properly due to high mobility [120]. In these techniques, congestion gets introduced due to extra data packets and neighborhood techniques. Imran et al. [121] listed features for detection of WHA as depicted in Figure 10.

4.3.1 Location

Based on the node's location in the network, network graph can be built for WHAD. A Global positioning system (GPS) device must be used with every node to track the locations to track their respective locations. In addition to collection of nearby node information, the GPS device reduces the cost and routing overhead of connected nodes. Relative location can also be gathered by directional antenna. Usage of GPS and antennas will cause increase in cost and battery consumption. Usage of location as a detection feature can increase false positive rate (FPR) owing to frequent change in mobile node positions. Lu et al. [122] designed a Pworm model for wormhole detection using key observation and localization-based system. It is well suited for reducing false alarm rate (FAR), scalability as well as time delay in terms of activation latency.

4.3.2 Time

In WHA, average round trip time (RTT) per hop is more than the RTT per hop for a route in normal situation in the network. Therefore, time can be a parameter for detecting WHA. For calculating time difference between two nodes, the nodes must be equipped with synchronized clock. Deployment of synchronized clock is expensive as well

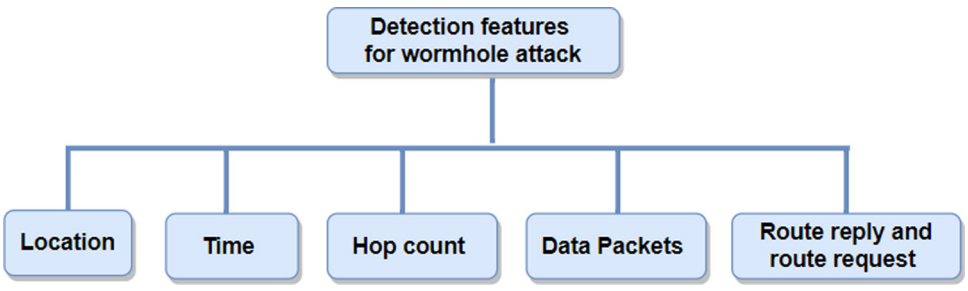

Figure 10: Detection features for wormhole attack.

as difficult. Usage of time as detection parameter may increase the FPR [123].

4.3.3 Hop count

Hop count decreases in case of WHA as the message travels through tunnel between the malicious nodes. Hop count is also a wormhole detection feature, while some technique uses hop count as a hybrid feature with time and location. Average time for single hop is calculated by dividing total hops by total distance [124].

4.3.4 Data packets

Nodes in the network can monitor their neighbor nodes whether they are dropping, forwarding, or modifying the received packets to the destination nodes or other nodes. There will be a trust value for every node. It is not easy to process each data packet in the neighborhood; however, the utilization of data packets as a feature is an efficient technique for large network with high mobility [125].

4.3.5 Route reply (RREP) and route request

RREP can also be used for detecting WHA. RREP message is unicast to the source node to transmit the route of the destination point. Route request (RREQ) messages are broadcasted by source node and can also be used for detection purpose. Most of the detection techniques use RREQ messages due to simple computation and fewer resources [126] (Table 2).

5 Performance metrics used for ad-hoc network

Performance of ad-hoc network can be assessed in terms of throughput, end-to-end delay, capacity, and packet delivery ratio. While designing the routing protocol, many issues related to parameters such as scalability, QoS support, security, and low power consumption needs to be considered [127]. To measure the effectiveness of wormhole detection techniques, various parameters viz., packet delivery rate, packet loss rate, average throughput, average end-to-end delay, and detection rate are usually considered, which can be defined as follows.

5.1 Packet delivery rate (PDR)

PDR represents the ability of the protocol to deliver data packets to the destination node in the presence of malicious nodes in the network. PDR is calculated by dividing total number of packets received at the destination by total number of packets sent by the source [128] as illustrated by equations (1) and (2).

$$\mathrm{PDR} = \frac{\sum \text{Received packets at destinations}}{\sum \text{Sent packets by sources}} \times 100\%, \quad (1)$$

$$\mathrm{PDR} = \frac{\sum_{k=1}^{n} X_{\mathrm{k}}}{\sum_{k=1}^{n} Y_{\mathrm{k}}} \times 100\%. \quad (2)$$

5.2 Packet loss rate (PLR)

PLR is caused by network congestion, it occurs when one or more packets of data travelling across the network fail to reach their destination. PLR is defined as the ratio of the total number of packets dropped during transmission to the total number of packets sent by the source.

$$\mathrm{PLR} = \frac{\sum \text{number of packet dropped}}{\sum \text{Sent packets by sources}} \times 100\%, \quad (3)$$

$$\mathrm{PLR} = \frac{\sum_{k=1}^{n} X_{\mathrm{k}}}{\sum_{k=1}^{n} Y_{\mathrm{k}}} \times 100\%. \quad (4)$$

Table 2: WHA detection features

Detection feature	Special hardware	Promiscuous mode	Mobility issue	Congestion	Routing delay	Expensive (memory, processing, and cost)
Time	Needed	—	—	—	—	More
Location	Needed	—	—	—	—	More
Data packet	—	Required	—	More	—	More
Route reply	—	Required	Yes	—	—	Less
Neighborhood	—	—	Yes	More	—	More
Hop count	—	—	—	—	Increases	Less

5.3 Average throughput

Average throughput is defined as the ratio of total size of packets received at the destination to the difference between stop and start time of the simulated network.

$$\text{Avg. throughput} = \frac{P_S}{T_{\text{start}} \sim T_{\text{stop}}}. \quad (5)$$

5.4 Average end-to-end delay (AED)

AED is the average delay between the transmitted packets and the received packets. AED includes all delays caused by data accusation, route discovery, propagation time, and data processing at intermediate nodes [105,151].

$$\text{AED} = \frac{\sum_1^N (T_{\text{Received}} - T_{\text{sent}})}{N}. \quad (6)$$

5.5 Detection rate

Detection rate (DR) defines the probability that wormhole nodes are successfully identified by the intrusion detection system. DR is expressed as the ratio of number of detected misbehaving nodes to the total number of actual misbehaving nodes

$$\text{Detection rate} = \frac{\text{Number of detected misbehaving node (NDMN)}}{\text{Total number of actual misbehaving nodes (NTMN)}}. \quad (7)$$

5.6 False negative rate (FNR)

FNR is defined as the number of malicious nodes that were not detected by the intrusion detection system. FNR is the ratio of undetected malicious node to total number of malicious nodes [128].

$$\text{False negative} = \frac{\text{Number of undetected malicious node (NUMN)}}{\text{Total number of malicious node (NTMN)}}. \quad (8)$$

5.7 FPR

FPR is defined as the number of legislative nodes that are detected as malicious nodes by intrusion detection system. It can be mathematically defined as the ratio of falsely detected malicious nodes to the normal behaving nodes. FPR is also termed as false accusation probability [128].

$$\text{False positive} = \frac{\text{Number of falsely detected malicious node (NFDMN)}}{\text{total number of normal enode (NTNN)}}. \quad (9)$$

5.8 True negative rate (TNR)

TNR is defined as the ratio of total number of detected normal nodes to the total number of normal nodes.

$$\text{True negative} = \frac{\text{Number of detected normal node (NDNN)}}{\text{Total number of Normal node (NTNN)}}. \quad (10)$$

5.9 True positive rate (TPR)

TPR defines the sensitivity of the model. It shows the proportion of nodes that are predicted as malicious, and these nodes are actual malicious (Table 3).

$$\text{True positive} = \frac{\text{Number of detected malicious node (NDMN)}}{\text{Total number of malicious node (NTMN)}}. \quad (11)$$

6 Classification of detection methods for WHA

Numerous authors have suggested various methods for the identification and classification of WHA. In WHA, the attacker node needs the cooperation of other nodes to become more energetic and stronger in comparison to the other nodes. To detect the attacker node, number of solutions have been proposed by the research community such as position or location based [129], Id validation based [130,131], and geographical distance based [132] methods. WHA cannot be detected using cryptography techniques alone due to possessing replaying and rerouting capability for the valid messages [133]. As depicted in Figure 11, the detection methods can be categorized into different classes based on the following parameters: time based; location based; neighbor based; hardware based; topology based; artificial immunity system based; and ML based.

6.1 Time-based method

In time-based method, delay is calculated using RTT and challenge response time. In RTT method, attack is detected based on delay calculation between the two devices. If delay is higher than the threshold, then alarm is generated to announce the attack [134]. Song et al. [1] introduced a statistical analysis method based on signal processing for the detection of WHA using time delay analysis. Chiu et al. [135] proposed DelPHI (delay per hop indicator) for WHAD, where transmission rate was kept fixed. In their study, multipath approach was used to discern the mean delay of all existing routes [55,138]. Van Tran et al. [136]

Table 3: Acronyms used in performance metrics

Acronym	Details	Acronym	Details
X	No. of packets received	NDMN	No. of detected malicious nodes
Y	No. of packets sent	NTMN	Total no. of malicious nodes
K	No. of source or destination nodes	NFDMN	No. of falsely detected malicious nodes
M	No. of nodes generating controlling packets	NTNN	Total no. of normal nodes
Ps	Size of packet	NUMN	No. of undetected malicious nodes
T start	Simulation start time	N control	No. of control packets
T stop	Simulation stop time		

suggested a RTT-based method for anomaly detection between two successive nodes. Jen et al. [137] proposed multipath hop count analysis method resulting in 100 % avoidance if RREP limit was less than or equal to 2.

6.2 Neighbor-based method

In neighbor-based method, graph theory concept is used for analyzing the neighborhood information to tackle the wormhole attack [139]. Every node has information of neighbor node as well as of their subsequent hop nodes [140]. Neighbor node information might change with time; therefore, neighbor discovery protocols are usually used to get the fresh routes. Malicious node may also get the updated information regarding neighbors from discovery protocol. Therefore, in WHA, malicious node may transmit a fake RREP message to source or jam the original RREP message. Wormhole can also increase the number of neighbor nodes over a threshold level. Lee and Suzuki [141] proposed a method for removal of wormhole link [141] called SWAT (self-healing mechanism from wormhole attack). This method tends to detect the WHA and has immense capability to recover the distorted routing structure effectively [142,143].

6.3 Location-based method

In location-based approach, sender and receiver exchange the location information of the nodes. To detect the WHA, the distance between the source and destination is inspected on the basis of hop count. This approach requires a GPS device connected to every node. However, the developed approach is not as accurate as needed due to incorrect location of devices due to infrastructure less network. Also, this method requires high computational time as well as power owing to integration of GPS with network nodes. This problem can be mitigated by grouping the number of nodes sharing the same location [55,144,145].

6.4 Hardware-based method

In hardware-based method, directional antenna, GPS, or special radio transceiver modules are utilized as the hardware devices, wherein some network protocols and software are employed to secure ad-hoc network from the WHA. Additional hardware increases the cost of overall network, which results in less accurate outcomes [146,147,182–185].

6.5 Topology-based method

In topology-based solution, the detection rate is low due to low density of nodes and poor connectivity. However, topology-based method is a feasible solution due to connectivity information being the sufficient condition and involvement of no extra hardware to accomplish the

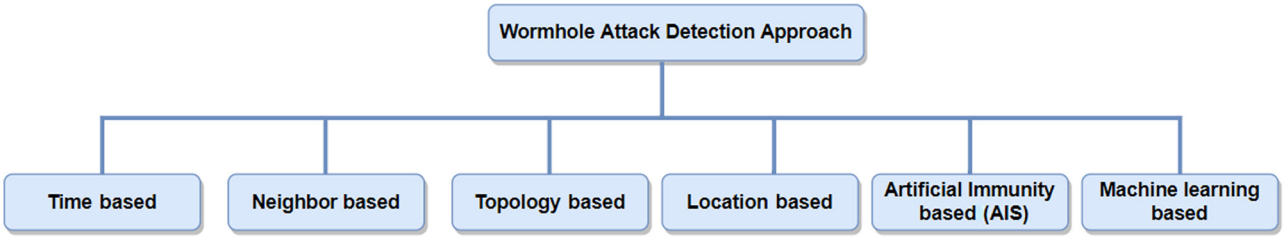

Figure 11: Classification of WHAD methods.

requisite task. WHA does not depend upon MAC layer due to being created on physical layer. This attack is also exempted from cryptography techniques, which makes it most dangerous security threats for ad-hoc networks [148].

6.6 Artificial immunity-based method

Artificial immunity-based detection system mimic the properties of human immunity system for self and non-self-discrimination [149]. This depiction is useful for ad-hoc network due to adoption of decentralized network. The concept of protection provided to the human body by the immune system is utilized for security enhancement in an ad-hoc network [128,150,151].

7 Literature review for WHAD

Routing attacks disrupt the functionality of routing mechanism. Therefore, in this section, we present the description, analysis, and scope of various methods and techniques, which have been reported in the literature so far for wormhole detection, in the form of various online sources such as ACM library, Springer library, Elsevier, Science directory, and IEEE Xplore Digital library. As has been stated earlier, numerous techniques have been developed by researchers for wormhole detection; however, each one of them have their own advantages, and disadvantages, which pose a constraint on their widespread use and applicability for real world problems. In this section, we also cover the performance comparison among different detection methods for wormhole attack stating their advantages, limitations, and detection rate.

For instance, Karlsson et al. [112] proposed a WHAD method called Traversal count and hop count analysis, which is based on RTT and hope count (HC) parameters. This method provides 75% detection rate with less overhead and FPs. Upadhyay and Chaurasia [153] developed a statistical approach for WHA detection using the following parameters such as average time delay, number of incoming packets, number of outgoing packets, and average route discovery time. There is high probability of WHA if the abrupt changes take place in the above parameters. Qazi et al. [154] proposed DSR routing method to ensure the network security from WHA in multi-rate environment using RREP and RREQ messages. Sundararajan et al. [127] presented a biological based artificial intrusion detection system (BAIDS), the performance of which was compared with hybrid negative selection algorithm, for anomaly detection. This system was claimed to yield satisfactory performance in terms of FAR and PDR, but suffered from high computational complexity due to insufficient routing information. Kim et al. [155] proposed a counterattack detection method using time stamp approach. In that method, authors used the time stamp to detect the anomaly. The proposed method does not seem to be promising as the intruders may easily fabricate time stamp of RREQ or RREP packet to elude the WHAD methods. Therefore, in general, two stage counterattack detection method is adopted. In the first stage, transmission time per hop is extracted from RREQ. If attacker fabricates the RREQ initial time to elude the detection scheme, it is detected in the next (i.e., in the second) stage. It is because the fabricated transmission time is shorter than the actual time. The problem of RREQ initial time fabrication was addressed by Karlson et al. [156], who proposed a Time Measurement Tampering in the Traversal Time and Hop Count Analysis (TTHCA for wormhole detection. In the proposed technique, they included hop count parameter in addition to Time stamp to resolve the issue. The limitation of this method is low FPR while using for the detection of time tampering attack. Despite being complex, it enhanced the security features. Giannetsos and Dimitriou [157] proposed Localized decentralized algorithm for countering (LDAC) WHA. It uses connectivity information to work for both static and mobile networks. This technique checks the connectivity graph for detection of malicious nodes and does not need any special hardware, GPS coordinates, clock synchronization, or some statistical methods. It utilizes only nodes ID in the network. Small initial time interval for partial neighborhood establishment is the only limitation of this method. Chen et al. [101] proposed a label-based DV hop localization method for the detection of WHA. Self-positioning nodes are employed as beacon nodes for assistance in distance vector hop localization. DV hop localization method works well when network has no packet loss and transmission radii is same for all the nodes in network. Sookhak et al. [158] used a key distribution technique and beacon packet for identifying the reliable neighbor in ad-hoc network. Lu et al. [122] designed a Pworm model for wormhole detection based on key observation and localization-based system. Pworm model reduces FAR, time delay in terms of activation, detection latency, and increases scalability. Ji et al. [159] proposed a distributed detection method for wireless network coding system (DAWN) to detect wormhole attack. This method monitors the change in the direction of packet's flow due to attack. This technique provides

TPR > 91% and FPR < 12.01%; however, the computational cost and overhead of this technique was high. Jamali and Fotohi [128] suggested an artificial immune system (AIS) for detecting WHAs. For instance, as a virus is detected in a human body, in the same way this concept could be used to detect the malicious nodes in the network. In AODV, as the source node gets the RREP message for RREQ, the sender immediately sends the message through that route without checking the security of the route, which may cause WHA. Therefore, by using AIS, the source node checks the security related parameters using antibodies (set of rules) for malicious antigens (unsecure routes). Amish et al. [119] proposed ad-hoc on-demand distance vector routing (AOMDV) protocol for wormhole detection. AOMDV calculates the multiple paths to the destination for the sake of link failure. It will select main path for communication on the time-based RTT approach. Proposed AOMDV approach has better throughput for a smaller number of nodes. Qazi et al. [160] developed a DSR routing method for securing network from WHA in multi-rate environment using RREP and RREQ messages. They achieved detection rate above 90% for both in-bound and out-bound tunnels. Tiruvakadu and Pallapa [161] used a WHA tree to confirm the presence of the attack. This tree was generated based on the presence of WHA symptoms. A honeypot is the center point, which aims at monitoring the WHA symptoms in network and developed a network analysis model for decision making. Sankara Narayanan and Murugaboopathi [162] proposed a modified AODV protocol to secure network from WHA. In [162], authors calculated the packet forward rate (PFR) and RTT of each node to detect the WHAs. It does not require any special hardware for this. Karthigadevi et al. [163] adopted EIGRP protocol and detected WHA based on RTT. From the results, we can infer that this method improves throughput and reduces end-to-end delay. Bai et al. [164] proposed a maximum independent set (MaxIS) wormhole detection for 3D network. It uses topology-based connectivity information. Luo et al. [165] proposed a neighbor discovery algorithm (CREDND) for WHA. It not only discovered internal WHA but external WHA also. External WHA were detected by counting hop difference between own exclusive neighbors, while internal WHA were detected by enabling the common neighbor nodes as witness to monitor the authentication packets, which are forwarded by malicious nodes. Aliady and Al-Ahmadi [166] presented an energy preserving secure measure technique against WHA based on network connectivity. In AODV protocol, the routes being discovered by RREP messages does not allow the packets to be forwarded immediately without checking the correctness of the route. Tamilarasi and Santhi [167] presented a method for wormhole detection and secure path selection. The path, which includes the wormhole nodes, is known as wormhole path. Therefore, this path needs to be identified for securing network from WHA. Multiple paths are generated from source node to destination using AOMDV protocol. Source nodes discern the WHA path using detection packet (DP) and feedback packet (FP) approach. Thereafter, the source node sends the data through optimal path after bypassing the WHA path. This method yields good results in terms of energy consumption and network lifetime. Singh et al. [168] proposed a method for wormhole detection using connectivity information and artificial neural network. They used the probability distribution for evaluating the detection rate. The research studies as mentioned above conducted the tests in simulation environment such as NS2, QualNet, and GloMoSim. The impact of WHA and efficiency of different detection and prevention algorithms are presented in Table 4. Abbreviations used in Table 4 are listed in Table 5.

8 Literature review on WHAD using ML

In present era, handling attacks in ad-hoc network has become more challenging owing to rise in complexity and large volume of the network with time. Most effective and simple approaches, which could be incorporated to cope with ad-hoc network attacks, are ML approaches. ML techniques have the capability to automatically learn the pattern from the complex network and develop the techniques and approaches to discern attack in the network. In this section, we have reviewed the numerous ML and deep learning techniques, which have been used for intrusion detection and classification of WHA in WSN. This section also covers the data collection methods and the set of features, which, in general, have been used most profoundly by researchers to ensure the network security. Numerous authors have proposed a number of solutions for wormhole detection using ML as listed in Table 6.

Xie et al. [170] proposed a hyper grid KNN based anomaly detection method. This is an improved KNN method. The proposed scheme has low computation and communication overhead, and it is able to handle training dataset with multi dimensions with DAR = 96% and FPR = 8%. Lie et al. [171] proposed an intrusion detection method using KNN classification. The proposed method has high detection rate 98.5% and low FAR 4.63%, with cut off value = 10. The prime focus of this article is Flooding

attack. For instance, in 2015, Titouna et al. [172] developed two-level sensor fusion-based outlier detection technique for wireless sensor network that was driven by the Bayes theorem. In this technique, the first level of detection was performed locally inside the sensor nodes, while the second level of detection was performed by a higher-level cluster head. This technique has one major advantage that it does not require any prior knowledge of data distribution provided that the cluster head has the fixed width. The developed method achieved the detection accuracy (DA) of more than 88% with FAR less than 17%, which seems to be quite satisfactory. Similarly, in 2016, Wazid and Das [173] proposed an effective algorithm based on K-means clustering for the detection of hybrid anomaly viz., black hole, misguiding, and WHAs in WSNs. The training dataset used in this algorithm comprises of various network parameters such as end-to-end delay, traffic behavior etc., to distinguish between normal and abnormal state of the network. K-means clustering algorithm achieved the detection rate of 98.6% with FPR of 1.2%. Subba et al. [174] proposed Vickrey–Clarke–Grove's scheme based on Bayesian game. This method is used to select the cluster leader in mobile ad hoc networks (MANETs) for multiple intrusion detection, which successfully reduced the congestion in the intrusion detection system and network power consumption. Feng et al. [175] suggested a new approach based on support vector data description (SVDD) technique for anomaly detection in wireless sensor network. In this technique, a sequential minimal optimization (SMO) algorithm was adopted to mitigate the computational complexity during training phase. SMO algorithm used second-order approximation to sort out the quadratic programming problem followed by the use of integrated square error to ease the process of decision making. On comparing the performance of both the methods (i.e., SVDD and SMO), SVDD was able to achieve better results in comparison to SMO in terms of reduced training time and testing time of 1.56 and 0.0012 s, respectively, with same accuracy for single hop data of node 4. Saeedi Emadi and Mazinani [176] used a density-based spatial clustering of application with noise (DBSCAN) algorithm for anomaly detection in WSN. In this algorithm, authors created different clusters based on the network data such as temperature, humidity, and voltage to detect the nodes as malicious nodes, which were supposed to have low density. The proposed algorithm obtained good results with the detection rate of 95.5% with 9 cluster heads.

Kavitha et al. [72] proposed an approach for identification and isolation of malicious node by using feature selection, optimization, and classification methods. The features are optimized using swarm optimization algorithm. These optimized features are classified using neural network. Proposed method achieves 98% PDR and 9.7 ms latency with 120.5 mJ energy consumption. Khan et al. [177] proposed SVM-based classification of malicious users in cognitive radio network. Proposed scheme provides reliable results and detection probability 1 with FAR probability = 0.4. Reddy and Thilagam [178] proposed a method for preventing DoS attack using Naïve Bayes classifier. The network node possesses 80% legislative traffic with this approach otherwise it is 0% in hostile environment. It uses RSA key (1,024 bits) for node authentication. One more algorithm named Optimized collaborative intrusion detection system (OCID) was developed by Elsaid and Albatati [179], which employed improved artificial bee colony (IABC) algorithm for optimization of weights in SVM reducing the classification error. The developed system had an average detection rate of 97.9% with FAR and standard deviation of 1.8 and 1%. Zhang et al. [180] presented an anomaly detection method using boosted decision tree (BDT) and neural network. The proposed method shows accurate results for anomaly detection. In ref. [182], SVM classification approach was used as an intrusion detection scheme to detect the different types of attacks in WSN like packet dropping, routing disruption, and resource consumption, achieving an accuracy of 92.8% for WHAs. WHA is considered under routing disruption due to being capable to deviate the packets from original route to wormhole tunnel. WHA was identified using NB and SGD algorithms by Prasad et al. [183]. The features, which were used to classify the anomaly, were determined based on network behavior and attained the accuracy of 93.06% based on them. The main limitation of the algorithm was that they assumed the dataset as a linear function, which might not work well for non-linear input dataset. Singh et al. [168] proposed KNN and SVM ML approach for wormhole detection in VANET. Four alarm types (TP, TN, FP, and FN) and accuracy are compared for both the approaches as shown in Table 6. The results are accurate and have low FAR. Sankaran et al. [181] introduced a reward-based learning technique for secure neighbor selection (SNS-RR), which involves three stages: (i) determination of node state, (ii) attribute analysis, and (iii) route selection. Nodes are classified based on their behavior. In their study, they used to monitor the multiple node attributes at regular intervals and classified them based on the behavior of their respective nodes. Suggested approach obtained the results with throughput, DR, and PDR of 132.21 kbps, 93.62%, and 0.87, respectively. In 2021, Tahboush and Agoyi [184] applied K-means clustering and RTT-based approach to recognize the WHA. They utilized NRT method to reduce the consumed energy in the network. Using the developed approach, authors were able to recognize in-band and

Table 4: Comparison of different detection methods for WHA

References	Techniques	Approaches (RTT/HC/DA/TS/NB/CB/LN/GB	Advantages	Limitations	Detection rate
Karlson et al. [112]	TTHCA	RTT and HC	Less overhead	Nodes in participation mode (PM) can alter the time measurement	75%
Upadhyay and Chaurasia [153]	SAA	DA	Lightweight	Route discovery time increases	Efficient
Qazi et al. [154]	Securing DSR from WHA in multi-rate ad-hoc network	RTT	Security against packet encapsulation wormhole, out of band wormhole, high power transmission wormhole, packet relay wormhole	Extra 18 bytes for data added to RREP message proposed for DSR can be extended for AODV	Efficient
Sundararajan et al. [127]	BAIDS	HNSA	Provides reliable information	Needs extra CPU cycle and memory, increases computational complexity, and limited to WHA only	High PDR and less FPR
Kim et al. [155]	Time stamp counterattack detection scheme	TS	Able to detect WHA as well as attacker's counterattack	Simulation was done for two malicious nodes only	DR = 96.3 % and FPR = 7.78%
Karlson Dimitriou [156]	TTHCA	TS, HC, and TTHCA	Enhanced TTHCA approach and enhanced security	More complex	Less FPR
Giannetsos and Dimitriou [157]	LDAC	NB and CB	Works in both static and dynamic network, efficient and lightweight, low cost and less overhead, and no special hardware	Requires small initial time interval for partial neighborhood establishment	DR = 100%
Barani et al. [149]	GAAIS	AIS	Does not require any special hardware	Needs three steps: training, detection, updating	92.57% DR, and 3 and 10 % FAR
Chen et al. [101]	DV-hop localization	Node localization	Localization error is reduced	Packet loss should not be there, transmission radii of nodes must be identical	DR = 95.6% and BSR = 50%
Sookhak et al. [158]	DWGRP	GB	No special hardware is required	Better results with low false detection rate	DR = 100% and low FDR
Lu et al. [122]	PWORM	Location key	Well suited for false alarm, scalability, and time delay, and both active and passive attacks are detected	Need to calculate MAC	For TH > 5%, FPR = 0 and for TH < 1%, FPR increases
Ji et al. [159]	DAWN	Location based	Does not rely on global synchronization, location information, and no need of hardware	Increases computational time and more overhead	Efficient TPR > 91% and FPR < 12.01%
Jamali and Fotohi [151]	AIS	AIS	Can be applied to AODV as well as to other protocols, no special hardware required, and no complex calculations	Mapping needs to be carried out between human body and ad-hoc network and training set required	Efficient
Amish et al. [119]	AOMDV	RTT	No special hardware is required	Need to calculate RTT for every route	Throughput = 72.56 bps

(*Continued*)

Table 4: *Continued*

References	Techniques	Approaches (RTT/HC/DA/TS/NB/CB/LN/GB	Advantages	Limitations	Detection rate
Kaur et al. [169]	RTT	RTT and DA	No special hardware is required such as GPS, and Clock synchronization	Yields a good result only for AODV	Efficient
Jamali and Fotohi [128]	AIS (DAWA)	Fuzzy logic AIS	Defensive technique	Required mapping between human body and ad-hoc network and requires training set	20% better defensive scheme as compared to COTA [122] and worm planar [123]
Qazi et al. [160]	M-Delphi	RTT	Does not require any special hardware, can have multi-rate transmission, and less overhead than Delphi	Need to add 18 bytes extra in packet	DR = 90% and FPR = 10%
Tiruvakadu et al. [161]	Honeypot	Location based	Achieves low FAR, no need of special hardware, uses attack tree, and eliminates the need of other details such as route info and no. of nodes	Node activities are monitored to create attack tree	Low FAR
Sankara Narayanan and Murugaboopathi [162]	MSAODV	RTT packet forwarded ratio	Packet loss, end- to-end delay, packet delivery ratio parameters are considered, and no special hardware is needed	Finds PFR and RTT for each node instead of entire network	Improved QoS
Karthigadevi et al. [163]	EIGRP protocol	RTT	Packet loss, end-to-end delay and packet delivery ratio parameters are considered. No special hardware is required	Pre-calculation of routes due to EIGRP	Improved DR, average throughput, PDR, and end-to-end delay
Bai et al. [164]	MaxIS	Topology based	Works with a poor connectivity even in a 3 D network structure and is light weighted	Node degree > 18	DR = 100%
Luo et al. [165]	CREDND	Hop difference and local monitoring	Used to detect external as well as internal WHA, no need of special hardware, no need of localization and synchronization, and saves node energy	Depends on neighbor ratio threshold (NRT), may not work with different communication range nodes	Improved accuracy and reduced energy consumption
Aliady and Al-Ahmadi [166]	EPSMA	NB	No additional cost, hardware, and synchronization is required	AODV routing protocol work for only 4 or less than 4 hop count tunnels	DR = 100%, HC < = 4, throughput = 147.7 Kbps
Tamilarasi and Santhi [167]	Secure path selection	RTT	Energy consumption is low with high network lifetime	Need to find DP and FP and uses AOMDV	Low energy consumption

Table 5: Abbreviations used in Table 4

Acronym	Details
TTHCA	Traversal time and hop count analysis
RTT	Round trip time
HC	Hop count
DA	Delay analysis
NB	Neighbor based
CB	Connectivity based
LN	Localization
GB	Geographical based
SAA	Statistical analysis approach
BAIDS	Biological based artificial intrusion detection system
HNSA	Hybrid negative selection algorithm
LDAC	Localized decentralized algorithm for countering WHA
DWGRP	Detection of WHA in geographic routing protocol
PWORM	Passive and real time wormhole detection scheme for WSN
DAWN	Distributed detection algorithm against WHA
M-Delphi	Multi-rate delay per hop indicator
GAAIS	Genetic algorithm AIS
MAODV	Modified secure AODV
Max-IS	Maximum independent set (MaxIS) based wormhole detection for 3D ad-hoc network using connectivity information
SGD-NB	Stochastic gradient descent (SGD) algorithm, Naïve Bayes (NB) algorithm for learning linear classifier
CREDND	Credible neighbor discovery
EPSMA	Energy preserving secure measures against WHA
HWAD	Hybrid WHAD

out-band WHA with throughput of 149.843 kbps for 150 nodes. The ML approaches, which have been used so far to detect WHAs and other kinds of anomalies in WSN, are listed in Table 6, along with the summary and performance measures.

Of the above ML techniques listed in Table 6, support SVM, KNN, and LR are the most prominent and widely used approaches which have been adopted on wider scale for anomaly detection in wireless ad-hoc networks. However, the ML and deep learning models are in its infant stage for the detection of wormhole and other types of attacks. Therefore, a lot of research is needed to explore the different aspects of ML techniques regarding anomaly detection. Abbreviations used in ML techniques are listed in Table 7.

9 Results and discussion

Systematic review on the WHA detection in wireless network from year 2013 to 2021 has been done based on various research papers on ML technique (MLT). From the literature review, it was found that most publications include the stages such as pre-processing, feature extraction, and selection of detection features. Finally, the classification stage is regarded as the heart of anomaly detection in WSN. In our review, there are usages of different MLTs as classifier for WHA detection.

Figure 12 indicates the rate of publication on MLT for WHA detection in the period from 2013 to 2021. Although anomaly detection is not a new research topic, it is clear from the graph that number of publications is varying slowly over the time and can be increased in the coming years. From the bar chart, it is shown that ML techniques have been widely used for anomaly detection. Year 2020 has the largest number of publications for WHA detection as per literature review.

Figure 13 presents the number of publications using certain MLT from year 2013 to 2021. It has been noticed that there is a significant diversity in the usage pattern of ML technique. Some of them have been extensively used such as SVM, while some of them have been less frequently used such as Naïve Bayes and neural network, and other techniques like DT, RF, and KNN have been less frequently used as shown in below graph.

SVM has been used in 7 papers, the range of DA is 92.8–97.9% whereas KNN has been used in 3 papers with a maximum accuracy of 98.5%. In the same way, decision tree has been used in 3 papers with more than 90% accuracy. Naive Bayes, K-means clustering and neural network has been used in 6 papers where Naïve Bayes has 88–93.12% accuracy, K-means clustering has 86% detection rate and neural network has 96–98.5% accuracy.

10 Advantages of MLTs

In the above section, performance analysis of various MLTs in terms of different performance measures such as accuracy, TPR, FPR, TNR etc., [190–199] have been discussed for WHA detection. About WHA and other kinds of malicious node detection, MLTs offer several advantages as follows:

(i) MLTs can yield more accurate, robust, and reliable results with low FPR.
(ii) Able to generate model even for noisy dataset. In Ad-hoc networks, the dataset is usually noisy owing to adoption of dynamic topology.

11 Issues in MLTs

As evident in the early part of this article, ML offers a wide range of applications. However, numerous issues need to

Table 6: ML techniques for detecting wormhole attack

Authors	ML techniques	Performance measures	Remarks
Xie et al. [170]	Hyper grid KNN-based anomaly detection	DAR: 96%	✓ Improved KNN
		FPR: 8%	✓ Low computation and communication overhead ✓ Able to handle training dataset with multi-dimensions ✓ Scalability is high
Lie et al. [171]	KNN classification	DR: 98.5% FAR: 4.63% with cut off value 10	✓Main focus is on Flooding attack
Titouna et al. [172]	Bayes theory and clustering	DAR > 88%	✓Two-level sensor fusion-based outlier detection technique
		FAR < 17%	✓Does not require prior knowledge of data distribution and cluster width needs to be fixed
Wazid et al. [173]	K-means clustering	DR: 8.6% FPR: 1.2%	✓Useful for hybrid attacks ✓Post-mining steps need to be performed to avoid mismatch in training
Subba et al. [174]	Vickrey–Clarke–Grove's scheme based on Bayesian game	High DR	✓Reduces congestion in the intrusion detection system ✓Reduces power consumption
Feng et al. [175]	SVDD and SMO	Training time: 1.56 s Testing time: 0.0012 s	✓Provide reduced computational complexity for training stage and decision-making stage. ✓Provides results for single hop data of node 4
Saeedi Emadi and Mazinani [176]	SVM and DBSCAN	DA: 95.5% with 9 clusters	✓Clusters were created based on the network data ✓Nodes with low density detected as malicious nodes
Zhang et al. [185]	BDT and& feed forward neural network	Accuracy > 90%	✓Fast method depends on a threshold level ✓Boosted classifier is used
Meddeb et al. [182]	SVM	SVM: Se: 0.85 Sp: 1.00 PPV: 1.00 NPV: 0.952	✓For WHAD, SVM classifier was used with 13 routing related features. ✓Employed data pre-processing to improve the precision and classification results
Prasad et al. [183]	NB	DR: 93.12% FAR: 5.3% Pe: 94% f-measure: 93.4%	✓NB algorithm: a probabilistic approach for classification that deals with high volume dataset. ✓ Used 21 features such as an input data.
	SGD	SGD: DR: 93.12% FAR: 5.3% Pe: 94% f-measure: 93.4% Acc: 93.08	✓Used SGD algorithm for learning the linear classifier under convex loss functions such as SVM and logistic regression (LR) ✓Produced more accurate results than NB algorithm
Singh et al. [186]	Classification and regression	SVM: TP: 0.9906 FP: 0.0014 KNN: TP: 0.9913 FP: 0.0087	✓KNN and SVM techniques are used to detect WHA in VANET ✓Used 4 alarm types
Kavitha et al. [72]	Swarm optimization algorithm and neural network	PDR: 98%	✓Features are optimized using PSO

(*Continued*)

Table 6: *Continued*

Authors	ML techniques	Performance measures	Remarks
		Latency: 9.7 ms	✓ Optimized features are classified using neural network
		Energy consumption: 120.5 mJ	✓ Results were obtained only for 10% malicious node
Khan et al. [177]	SVM-based classification of malicious users	Detection probability 1 with FAR probability 0.4	✓ Classifies legislative and malicious users
			✓ Obtains reliable results
Reddy and Thilagam [178]	NB classifier	Network nodes possess 80% legislative traffic	✓ RSA 1,024 bits used for node authentication
			✓ Focused on DoS attacks
Elsaid and Albatati [179]	Optimized weighted SVM	DR: 97.9 (avg.) Deviation: 0.9 FAR: 1.8 (avg.) SD: 1%	✓Developed OCID system ✓Uses IABC ✓ Optimization algorithm for optimizing the weight of SVM ✓ Helps to minimize the classification error
Zang et al. [180]	Multi-kernel extreme learning machine	DAR: 92.10% FPR: 2.37	✓ High detection rate ✓ Efficient learning speed
Sankaran et al. [181]	Classification approach	Throughput: 132.21 Kbps DR: 93.62% PDR: 0.87	✓ Used recurrent reward-based ML technique for secure neighbor selection (SNS-RR)
Tahboush and Agoyi [184]	K-means clustering	Throughput: 149.843 Kbps for 150 nodes	✓ Developed HWAD method, which involves K-means clustering and RTT-based approach to detect WHA. ✓ HWAD used NRT to lower the energy consumption in the network. ✓ Detected in-band as well as out-band WHA in the network
Abdan et al. [187]	KNN, SVM, DT, LDA, NB, and CNN methods	Accuracy of KNN: 97.1% SVM: 98.2% DT: 98.9% LDA: 95.2% NB: 94.7% CNN:96.4%,	✓ Used node properties for feature extraction such as speed of node ✓ Used 3,997 samples (3,781 normal nodes and 216 malicious nodes) ✓ DT method has highest accuracy
Shahid et al. [188]	ESWI technique	Detection rate: 99%	✓ Works for IoT based wireless network ✓ Simple and less complicated technique, therefore overhead and energy consumption is low ✓ Increased throughput
Alajlan [189]	Multistep detection	Higher true positive rate	✓ Uses three modules for WHA detection node validation process, fake link reduction process, and wormhole isolation.
		Lower false negative rate (0.015)	✓ Works for distributed environment

be addressed while working with MLTs such as need of large volume of data to provide adequate training to the model, and expensive resources. In case of ad-hoc networks, need of training data and input test data are more prominent. Proper labeling is to be done to the training dataset to yield more accurate results. In case of fault management and securing network, the numerous works rely upon the synthetic data that does not present the complexity of real-world problems. Real world data are more critical and challenging especially for ad-hoc networks. Therefore, academia and industry must put combined efforts to generate public repositories of reliable data. In addition, standard evaluation metrics are also required to compare and analyze the performance of different existing and new MLTs regarding network security. Choice of a specific ML model is also crucial; all methods

Table 7: Abbreviation used in ML techniques

Acronyms	Details
Se	Sensitivity
Sp	Specificity
PPV	Positive predictive value
NPV	Negative predictive value
Acc	Accuracy
DR	Detection rate
FPR	FPR
TP	True positive

are not efficient for solving all kinds of problems with requisite accuracy.

12 Research gap and potential solutions

Early wormhole detection techniques in ad-hoc network involve the usage of additional hardware such as antennas, GPS, and special radio trans-receivers. Involvement of additional hardware tends to increase the complexity of the network and may augment the overall cost of the network [196–200]. Later, software-based solutions were suggested by research community, which need some specific assumption (i.e., distance and time based) to work effectively. These solutions follow the assumptions that the time and distance data cannot be altered by malicious nodes [201]. Software-based solution and cryptography authentication methods can also be clubbed together to provide better solution with the aim of detecting the malicious nodes in WSNs; however, there would be need of deployment of secret key in network, which is not feasible every time and pose a big constraint in providing a real time solution of the stated problem [202,203]. Another efficient approach for wormhole detection may be based on the deployment of an AIS. As virus is detected in a human body, in the same way, the malicious nodes can also be detected in a network. In AODV, the source node immediately transmits the message as soon as it gets the RREP message for RREQ, without ensuring the route security, However, in AIS, the source node first checks the security related parameters using antibodies (set of rules) for malicious antigens (unsecure routes) before transmitting the message [128]. Jim et al. [204] reviewed the various AIS-based methods for intrusion detection. The negative selection algorithm has been widely used in literature over the years; however, the involvement of the biologist, engineers, and computer scientist is still needed to work in sync to improve its efficiency further.

Although, various methods have been explored in literature to detect WHA, most of the available methods possess some sort of limitations. As WHA are treated as a part of routing protocols, there is still scope of

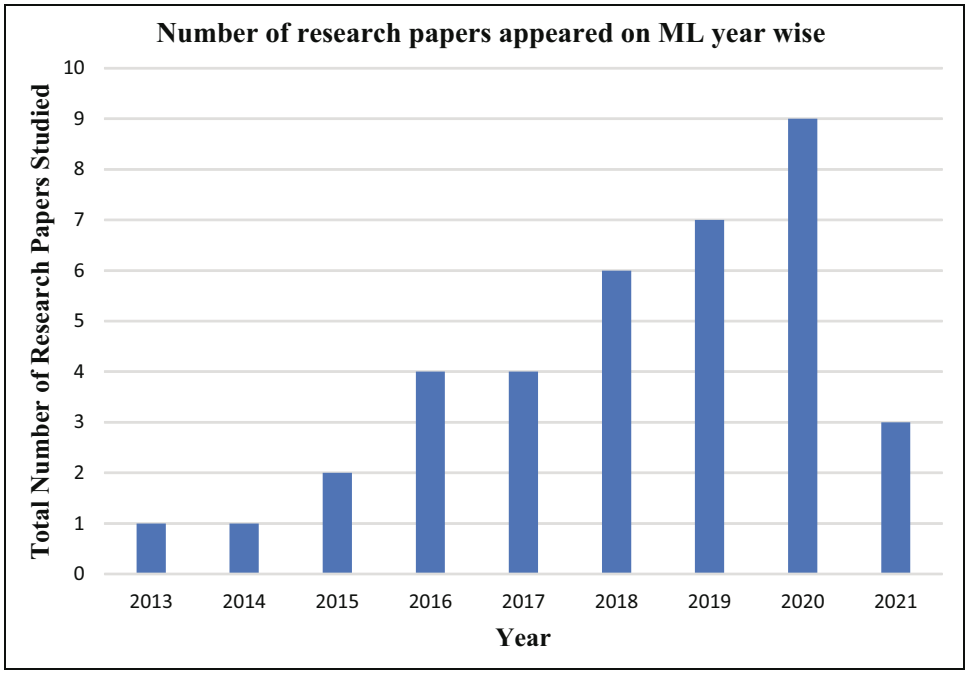

Figure 12: Research papers on ML for WHA detection, year wise.

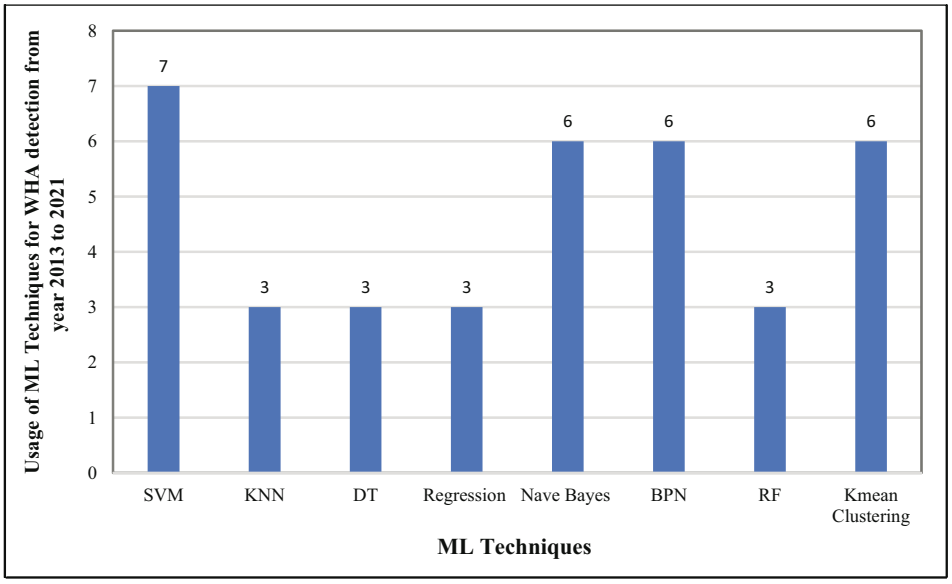

Figure 13: Contribution of MLTs in WSN for WHA detection from year 2013 to 2021.

improvement in routing protocol technique by incorporating new models such as ensemble methods and bootstrapping gradient methods into it, hence new hybrid methods can be employed to overcome the limitations of WHA detection techniques more efficiently. Despite ML methods not explored extensively for the above stated problems in WSN, these techniques have been found efficient and useful with the only limitation of needing large dataset that can be easily gathered within the stipulated time by simulating the network protocols as well as by monitoring the network traffic. Of all the abovementioned ML paradigms, the supervized learning models found to be more useful as per researcher and practitioners [176,185].

13 Conclusion

Ad-hoc network comprises mobile nodes with each node having the movement throughout the network. Communication among these mobile nodes happens through the wireless links by direct or intermediate nodes without possessing any fixed infrastructure because of their mobile nature. The node works as host as well as router for other nodes in network for transmission of data. The nodes need to cooperate with each other during communication. However, in ad-hoc network, nodes may not cooperate with each other to reduce the power consumption and bandwidth requirements. These non-cooperative nodes, which tend to drop as well as alter the data, without forwarding them, are referred to as malicious or selfish nodes. MANETs are vulnerable to security attacks owing to the following features such as shared radio channel, insecure open medium, dynamic changing topology, lack of cooperative algorithms and centralized monitoring, limited resource availability, and physical vulnerability. Attacks on MANET can be classified into two main categories, namely, active attacks and passive attacks. An active attack tends to destroy or alter the data packets and routing messages being exchanged in the network and is very harmful to the network security. For instance, Blackhole attack, WHA, and Rushing attack. Passive attack does not disrupt the operation of the network, for instance eavesdropping, snooping, masquerading, or spoofing. WHA is comparatively considered to be more severe due to causing disturbance in the routing information, which diminishes the network performance despite the network being authenticated and encrypted. In this article, we have thoroughly discussed various anomaly detection techniques and their countermeasures along with their advantages and limitations. Further, we have also discussed MLT for WHAD. According to the literature review, few research has been done in the field of WHAD using ML such as SVM, KNN, NB, and HWAD.

In the near future, ML might be part of every application as MLT technique results are accurate as well as reliable. Due to dynamic topology, the dataset is noisy in ad-hoc network and MLTs can generate models even for noisy dataset. Therefore, for anomaly detection in ad-hoc network MLTs are efficient. On the other hand, existing ML-based approaches focus on single layer network. We can develop a framework for securing future

wireless network by existing ML approaches to multilayer network. Finally, we have identified the areas where further research can be focused so that we can apply the WHA detection methods for larger topological area for more flexibility and accurate results.

Conflict of interest: Authors state no conflict of interest.

Data availability statement: Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

References

[1] N. Song, L. Qian, and X. Li, "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach," *In: 19th IEEE International Parallel and Distributed Processing Symposium*, Denver, 2005, p. 8.

[2] M. Masoud, Y. Jaradat, A. Manasrah, and I. Jannoud, "Sensors of smart devices in the internet of everything (IoE) era: big opportunities and massive doubts," *J. Sens.*, vol. 2019, p. 26, 2019.

[3] X. Liu, Z. Li, P. Yang, and Y. Dong, "Information-centric mobile ad hoc networks and content routing: A survey," *Ad Hoc Netw.*, vol. 58, pp. 255–268, 2017.

[4] H. Kim, M. Bae, W. Lee, and H. Kim, "Adaptive decision of wireless access network for higher user satisfaction," *Wirel. Commun. Mob. Comput.*, vol. 2018, p. 19, 2018.

[5] F. A. Khan, M. Imran, H. Abbas, and M. H. Durad, "A detection and prevention system against collaborative attacks in mobile ad hoc networks," *Future Gener. Computer Syst.*, vol. 68, pp. 416–427, 2017.

[6] M. Tareq, R. Alsaqour, M. Abdelhaq, and M. Uddin, "Mobile ad hoc network energy cost algorithm based on artificial bee colony," *Wirel. Commun. Mob. Comput.*, vol. 2017, p. 14, 2017.

[7] M. Fleury, D. Kanellopoulos, and N. N. Qadri, "Video streaming over MANETs: An overview of techniques," *Multimed. Tools Appl.*, vol. 78, pp. 23749–23782, 2019.

[8] S. S. Anjum, R. Md Noor, and M. H. Anisi, "Review on MANET based communication for search and rescue operations," *Wirel. Personal. Commun.*, vol. 94, pp. 31–52, 2017.

[9] X. Lei and S. H. Rhee, "Performance enhancement of overlapping BSSs via dynamic transmit power control," *J. Wirel. Com. Netw.*, vol. 2015, p. 8, 2015.

[10] G. Khanna, S. K. Chaturvedi, and S. Soh, "Reliability evaluation of mobile ad hoc networks by considering link expiration time and border time," *Int. J. Syst. Assur. Eng. Manag.*, vol. 10, pp. 399–415, 2019.

[11] V. Yazidi, U. C. Kozat, and M. O. Sunay, "A new control plane for 5G network architecture with a case study on unified handoff, mobility, and routing management," *IEEE Commun. Mag.*, vol. ,52, pp. 76–85, 2014.

[12] X. Wang and J. Li, "Improving the network lifetime of MANET through cooperative mac protocol design," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, pp. 1010–1020, 2015.

[13] C. F. Huang, Y. F. Chan, and R. H. Hwang, "A comprehensive real-time traffic map for geographic routing in VANET," *Appl. Sci.*, vol. 7, p. 129, 2017.

[14] A. Khan and M. H. Rehmani, "Reisslein, cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms and networking protocols," *IEEE Commun. Surv. Tutor.*, vol. 18, pp. 860–898, 2016.

[15] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surv. Tutor.*, vol. 17, pp. 757–789, 2015.

[16] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions," *IEEE Commun. Mag.*, vol. 52, pp. 86–92, 2014.

[17] F. Qamar, K. B. Dimyati, M. N. Hindia, K. A. Noordin, M. B. Mazid, and A. M. Al-Samman, "A comprehensive review on coordinated multi-point operation for LTE-A Computer," *Network*, vol. 123, pp. 19–37, 2017.

[18] R. H. Jhaveri and N. M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," *Int. J. Commun. Syst.*, vol. 30, no. 7. p. e3148, 2017.

[19] M. Wang and Z. Yan, "A survey on security in D2D communications," *Mob. Netw. Appl.*, vol. 22, no. 2. pp. 195–2008, 2017.

[20] M. S. Pathan, N. Zhu, J. He, Z. A. Zardari, M. Q. Memon, and M. I. Hussain, "An efficient trust-based scheme for secure and quality of service routing in MANETs," *Future Internet*, vol. 10, no. 2. p. 16, 2018.

[21] A. J. Goldsmith and S. B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks," *Wirel. Communications, IEEE*, vol. 9, pp. 8–27, 2002.

[22] A. Raheem and H. Ali, *Security Issues in Mobile Ad-Hoc Network & Solutions*, Network Security, Munich, GRIN Verlag, 2011. https://www.grin.com/document/200703.

[23] N. Sultana and S. S. Sarangdevat, "The goal of securing mobile ad-hoc network and solutions. communications in computer and information science," *book: Adv. Digital Image Process. Inf. Technol.*, vol. 2015, pp. 355–365, 2011.

[24] S. Zhang, S. Wang, H. Xia, and X. Cheng, "An attack-resistant reputation management system for mobile ad hoc networks," *Proc. Computer Sci.*, vol. 147, pp. 473–479, 2019.

[25] T. Lin, S. F. Midkiff, and J. S. Park, "A dynamic topology switch for the emulation of wireless mobile ad hoc networks," *27th Annual IEEE Conference on Local Computer Networks*, 2002.

[26] K. Sindhanaiselvan, J. M. Mannan, and S. K. Aruna, "Designing a dynamic topology (DHT) for cluster head selection in mobile adhoc network," *Mob. Netw. Application*, vol. 25, pp. 576–584, 2020.

[27] B. Krishna Tripathy, S. K. Jena, P. Bera, and S. Das, "An adaptive secure and efficient routing protocol for mobile ad hoc networks," *Wireless Personal Communications*, vol. 114, no. 2, pp. 1339–1370, 2020.

[28] J. Zhou, L. Liu, and H. Tan, "Traffic-predictive QoS on-demand routing for multi-channel mobile ad hoc networks," *J. Wirel. Commun. Netw.*, vol. 2018, p. 266, 2018.

[29] K. G. Preetha, A. Unnikrishnan, and P. Jacob, "Impact of bandwidth on multiple connections in AODV routing protocol for mobile ad-hoc network," *Second International Conference*

on Computer Science, Engineering and Applications, Proceedings published by Springer, 167, Berlin, Heidelberg, 2012.

[30] F. Sato, and S. Iijima, "Battery and power aware routing in mobile ad hoc networks," *Network-Based Information Systems. NBiS Lecture Notes in Computer Science*, T. Enokido, L. Barolli, M. Takizawa, (eds), 4658, Berlin, Heidelberg, Springer, 2007.

[31] N. L. Pradhan and T. Saadawi, "Power control algorithms for mobile ad hoc networks," *J. Adv. Res.*, vol. 2, no. 3. pp. 199–206, 2011.

[32] M. Rulnick, and N. Bambos, "Mobile power management for wireless communication networks," *Wirel. Netw.*, vol. 3, pp. 3–14, 1997.

[33] N. K. Ray and A. K. Turuk, "A hybrid energy efficient protocol for mobile ad hoc networks," *J. Computer Netw. Commun.*, vol. 2016, p. 11, 2016.

[34] M. Anand and T. Sasikala, "Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol," *Clust. Comput.*, vol. 22, pp. 12681–12687, 2019.

[35] M. Elhoseny and K. Shankar, "Reliable data transmission model for mobile ad hoc network using signcryption technique," *IEEE Trans. Reliab.*, vol. 69, no. 3. pp. 1077–1086, 2020.

[36] M. Faisal, S. Abbas, and H. Rahman, "Identity attack detection system for 802.11-based ad hoc networks," *J. Wirel. Com. Netw.*, vol. 2018, p. 128, 2018.

[37] Q. Wang, H. N. Dai, and Q. Zhao, "Eavesdropping security in wireless ad hoc networks with directional antennas," *2nd Wireless and Optical Communication Conference*, 5, Chongqing, China, 2013, p. 18.

[38] J. Kao and R. Marculescu, "Eavesdropping minimization via transmission power control in ad-hoc wireless networks,"*3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, Reston, VA, 2006, pp. 707–714.

[39] S. Sarika, A. Pravin, A. Vijayakumar, and K. Selvamani, "Security issues in mobile ad hoc networks," *Procedia Computer Sci*, vol. 92, pp. 329–335, 2016.

[40] H. Seno, S. A. Budiarto, and T. C. Wan, "A secure mobile ad hoc network based on distributed certificate authority," *Arab. J. Sci. Eng.*, vol. 36, pp. 245–257, 2011.

[41] Security in Ad Hoc Networks, *Ad Hoc Networking Towards Seamless Communications. Signals and Communication Technology*, Dordrecht, Springer, 2006.

[42] E. Fazeldehkordi, I. S. Amiri, and O. K. Akanbi, "Chapter 2 - Literature Review, A Study of Black Hole Attack Solutions," *Syngress*, vol. 2016, pp. 7–57, 2016.

[43] S. Aluvala, K. Raja Sekhar, and D. Vodnala, "A novel technique for node authentication in mobile ad hoc networks," *Perspect. Sci.*, vol. 8, pp. 680–682, 2016.

[44] R. Kumar, Y. Shiv, V. Kumar, and M. Wairiya, "An authentication technique in mobile ad hoc network using elliptic curve cryptography," *8th International Conference on Cloud Computing, Data Science & Engineering* (*Confluence*), 2018, 14-15. Noida.

[45] N. Ebrahimi Majid, N. Ho, T. Nguyen, and J. Stolmeier, "Evaluation of parameters affecting the performance of routing protocols in mobile ad hoc networks (MANETs) with a focus on energy efficiency," Lecture Notes in Networks and Systems, *Advances in Information and Communication*, FICC, 2019.

[46] N. Gupta and R. Gupta, "Optimization of performance metrics of LAR in ad-hoc network," *Int. J. Wirel. & Mob. Netw.*, vol. 2012, p. 4, 2012.

[47] D. A. Migov, and V. Shakhov, "Reliability of ad hoc networks with imperfect nodes," *Multiple Access Communications, MACOM*, 8715, 2014. Computer Science, 2014.

[48] C. Rezende, A. Boukerche, R. W. Pazzi, B. P. S. Rocha, and A. A. F. Loureiro, "The impact of mobility on Mobile Ad Hoc Networks through the perspective of complex networks," *J. Parallel Distrib. Comput.*, vol. 71, no. 9. pp. 1189–1200, 2011.

[49] I. Banerjee, M. Warnier, and F. M. T. Brazier, "Self-organizing topology for energy-efficient ad-hoc communication networks of mobile devices," *Complex. Adapt. Syst. Model.*, vol. 8, p. 7, 2020.

[50] O. Al Farraj, A. Al Zubi, and A. Tolba, "Trust-based neighbor selection using activation function for secure routing in wireless sensor networks," *J. Ambient. Intell. Humanized Comput.*, vol. 33, no. 8, 2018.

[51] S. Hasdemir, S. Yilmaz, and S. Sen, "A novel multi-featured metric for adaptive routing in mobile ad hoc networks," *Appl. Intell.*, vol. 49, pp. 2823–2841, 2019.

[52] B. K. Tripathy, S. K. Jena, and P. Bera, "An adaptive secure and efficient routing protocol for mobile ad hoc networks," *Wirel. Personal. Commun.*, vol. 114, pp. 1339–1370, 2020.

[53] B. K. Tripathy, S. K. Jena, and P. Bera, "An adaptive secure and efficient routing protocol for mobile ad hoc networks," *Wirel. Pers. Commun.*, vol. 114, pp. 1339–1370, 2020.

[54] R. J. Cai, W. C. Tan, and P. H. J. Chong, "An overview of trust-based routing design under adversarial mobile ad hoc network environment," *Wirel. Personal. Commun.*, vol. 96, pp. 3923–3946, 2017.

[55] H. Yih-Chun, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, pp. 370–380, 2006.

[56] F. Cai, C. Yongquan, H. Lansheng, and F. Zhicun, "Projection pursuit based wormhole detection in ad hoc network," *IEEE 10th International Conference on High Performance Computing and Communications & IEEE International Conference on Embedded and Ubiquitous Computing*, Zhangjiajie, 2013, pp. 1315-1322.

[57] M. Abu Zant and A. Yasin, "Avoiding and isolating flooding attack by enhancing AODV MANET protocol," *Hindawi, Security Commun. Netw.*, vol. 2019, Article ID 8249108, 2019.

[58] M. Khari, "Mobile ad hoc netwoks security attacks and secured routing protocols: A survey," Advances in Computer Science and Information Technology, Networks and Communications, vol. 84, pp. 119–124, 2012.

[59] A. Yasin and M. Abu Zant, "Detecting and isolating black-hole attacks in MANET using timer based baited technique," *Wirel. Commun. Mob. Comput.*, vol. 2018, Article ID 9812135, 2018.

[60] P. Mohammadi and A. Ghaffari, "Defending against flooding attacks in mobile ad-hoc networks based on statistical analysis," *Wirel. Pers. Commu*, vol. 106, pp. 365–376, 2019.

[61] L. Guaya-Delgado, E. Pallarès-Segarra, A. M. Mezher, and J. Forné, "A novel dynamic reputation-based source routing protocol for mobile ad hoc networks," *J. Wirel. Com. Netw.*, vol. 77, 2019. Doi: 10.1186/s13638-019-1375-7.

[62] M. Tripathi, M. S. Gaur, and V. Laxmi, "Comparing the impact of black hole and gray hole attack on LEACH in WSN," *Procedia Computer Sci.*, vol. 19, pp. 1101–1107, 2013.
[63] P. Tyagi and D. Dembla, " A secured routing algorithm against black hole attack for better intelligent transportation system in vehicular ad hoc network," *Int. J. Inf. Tecnol.*, vol. 11, pp. 743–749, 2019.
[64] A. Dorri, "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET," *Wirel. Netw.*, vol. 23, pp. 1767–1778, 2017.
[65] D. Mehetre, S. Roslin, and S. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust," *Clust. Comput.*, vol. 22, p. 1313, 2018.
[66] M. Mohanapriya and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," *Computes Electr. Eng.*, vol. 40, pp. 530–538, 2014.
[67] A. Baadache and A. Belmehdi, "Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks," *Computer Netw.*, vol. 73, pp. 173–184, 2014.
[68] M. Mohanapriya and I. Krishnamurthi, "Modifed DSR protocol for detection and removal of selective black hole attack in MANET," *Computers Electr. Eng.*, vol. 40, pp. 530–538, 2014.
[69] T. Poongodi and M. Karthikeyan, "Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks," *Wirel. Personal. Commun.*, vol. 90, pp. 1039–1050, 2016.
[70] P. Gupta, P. Goel, P. Varshney, and N. Tyagi, "Reliability factor based AODV protocol: prevention of black hole attack in MANET," *In book: Proceedings of the International Conference on Advanced Intelligent Systems*, 2019.
[71] D. Airehrour, J. A. Gutiérrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," *26th International Telecommunication Networks and Applications Conference* (*ITNAC*), 2016, pp. 115-120.
[72] T. Kavitha, K. Geetha, and R. Muthaiah, "India: Intruder node detection and isolation action in mobile ad hoc networks using feature optimization and classification approach," *J. Med. Syst.*, vol. 43, p. 179, 2019.
[73] S. Gurung and S. Chauhan, "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET," *Wirel. Netw.*, vol. 25, p. 3, 2019.
[74] S. Gurung and S. Chauhan, "A novel approach for mitigating gray hole attack in MANET," *Wirel. Netw.*, vol. 24, pp. 565–579, 2018.
[75] N. Schweitzer, A. Stulman, R. D. Margalit, and A. Shabtai, "Contradiction based gray-hole attack minimization for ad-hoc networks," *IEEE Trans. Mob. Comput.*, vol. 16, pp. 2174–2183, 2017.
[76] A. Vasudeva and M. Sood, "Survey on Sybil attack defence mechanisms in wireless ad hoc networks," *J. Netw. Computer Appl.*, vol. 120, pp. 78–118, 2018.
[77] H. Rajadurai and U. D. Gandhi, "Fuzzy based collaborative verification system for Sybil attack detection in MANET," *Wirel. Pers. Commun.*, vol. 110, pp. 2179–2193, 2020.
[78] R. Shyamala, and S. Valli, "Impact of blackhole and rushing attack on the location-based routing protocol for wireless sensor networks," *Advances in Computing and Information Technology*, 176, Berlin, Heidelberg, Springer, 2012.
[79] K. G. Reddy, and P. S. Thilagam, "Intrusion detection technique for wormhole and following jellyfish and byzantine attacks in wireless mesh network," *Advanced Computing, Networking and Security*, 7135, Berlin, Heidelberg, Springer, 2012.
[80] J. Liu, H. Chen, Z. Zhen, and M. Sha, "Intrusion detection algorithm for the wormhole attack in ad hoc network," *Proceedings of International Conference on Computer Science and Information Technology, Advances in Intelligent Systems and Computing*, 2014, p. 255.
[81] J. Li, D. Wang, and Y. Wang, "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network," *IET Wirel. Sens. Syst.*, vol. 8, no. 2. pp. 68–75, 2018.
[82] R. Sivakami and G. M. Kadhar Nawaz, "A radical block to byzantine attacks in mobile ad hoc networks," *Wirel. Pers. Commun.*, vol. 87, pp. 485–497, 2016.
[83] M. Selvan and S. Selvakumar, "Malicious node identification using quantitative intrusion detection techniques in MANET," *Clust. Comput.*, vol. 22, pp. 1–9, 2019.
[84] M. Ebenezarjebarani and B. P. Kumar, "A novel security authentication analysis onMANETs networks," *J. Crit. Rev.*, vol. 7, pp. 2765–2770, 2020.
[85] Islam, Noman, Security Issues in Mobile Ad Hoc Network, *Book: Wireless Networks and Security, Signals and Communication Technology*, Chapter: Security Issues in Mobile Ad hoc Network Publisher, Springer, 2013.
[86] M. Hauspie, D. Simplot, J. Carle, *Partition detection in mobile ad-hoc networks, ad-hoc network*, Mahdia, Tunisia, 2003, p. 6.
[87] B. Bhushan and G. Sahoo, "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks," *Wirel. Personal. Commun.*, vol. 98, pp. 2037–2077, 2018.
[88] P. Cong, S. Lim, J. Chae, and B. Jung, "Active detection in mitigating routing misbehaviour for MANETs," *Wirel. Netw.*, vol. 25, no. 4. pp. 1669–1683, 2019.
[89] F. A. Khan, M. Imran, H. Abbas, and M. Durad, "A detection and prevention system against collaborative attacks in mobile ad hoc networks," *Future Gener. Computer Syst.*, vol. 68, pp. 416–427, 2017.
[90] S. K. Das, and S. Tripathi, "Energy efficient routing formation algorithm for hybrid adhoc network: A geometric programming approach," *Peer-to-Peer Networking and Applications*, vol. 12, no. 1. pp. 102–128, 2019. Doi: 10.1007/s12083-018-0643-3.
[91] H. C. Chen, "TCABRP: a trust-based cooperation authentication bit-map routing protocol against insider security threats in wireless ad hoc networks," *IEEE Syst. J.*, vol. 11, no. 2. pp. 449–459, 2017.
[92] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," *Wireless Network Security, Signals and Communication Technology*, Y. Xiao, X. S. Shen, D. Z. Du, (eds), Boston, MA, Springer, 2007.
[93] K. Karthigadevi, S. Balamurali, and M. Venkatesulu, "Wormhole attack detection and prevention using EIGRP protocol based on round trip time," *J. Cyber Secur. Mobil.*, vol. 7, pp. 215–228, 2002.

[94] M. K. Garg, Singh, and P. Verma, *Fuzzy rule-based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs*, Procedia Computer Science, vol. 132, pp. 653–658, 2018. Doi: 10.1016/j.procs.2018.05.064.

[95] K. Gomathi, B. Parvathavarthini, and C. Saravanakumar, "An efficient secure group communication in MANET using fuzzy trust based clustering and hierarchical distributed group key management," *Wirel. Personal. Commun.*, vol. 94, pp. 2149–2162, 2017.

[96] A. Baadache and A. Belmehdi, "Fighting against packet dropping misbehaviour in multi-hop wireless ad hoc networks," *J. Netw. Computer Appl.*, vol. 35, pp. 1130–1139, 2012.

[97] G. Wu, X. Chen, L. Yao, Y. Lee, and K. Yim, "An efficient wormhole attack detection method in wireless sensor networks," *Computer Sci. Inf. Syst.*, vol. 11, no. 3. pp. 1127–1141, 2014.

[98] H. N. Jha, S. Gupta, and D. Maity, "Effect of wormhole attacks on MANET," *book: Des. Framew. Wirel. Netw.*, vol. 82, pp. 177–195, 2020.

[99] R. Matam and S. Tripathy, "Defence against wormhole attacks in wireless mesh networks," *Lecture Notes Computer Sci*, vol. 7671, pp. 181–193, 2012.

[100] M. Meghdadi, S. Ozdemir, and I. Güler, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks," *Proceeding of the IETE Technical Review*, Taylor & Francis, vol. 28, pp. 89–102, 2011.

[101] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xia, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," *Pervasive Mob. Comput.*, vol. 16, pp. 22–35, 2015.

[102] E. A. Panaousis, L. Nazaryan, and C. Politis, "Securing AODV against wormhole attacks in emergency MANET," *Multimed. Commun.*, vol. 2009, pp. 7–9, 2009.

[103] R. Singh, J. Singh, and R. Singh, "WRHT: A hybrid technique for detection of wormhole attack in wireless sensor networks," *Mob. Inf. Syst.*, vol. 2016, Article ID 8354930, 13 pages, 2016.

[104] R. A. Prakash, W. S. Jeyaseelan, and T. Jayasankar, "Detection, prevention and mitigation of wormhole attack in wireless adhoc network by coordinator," *Appl. Math.*, vol. 12, no. 1. pp. 233–237, 2018.

[105] M. Khabbazian, H. Mercier, and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless adhoc networks," *IEEE Trans. Wirel. Commun.*, vol. 8, no. 2. pp. 736–745, 2009.

[106] D. Sarkar, S. Choudhury, and A. Majumder, "Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network," *J. King Saud. University, Computer Inf. Sci.*, vol. 32, pp. 1–25, 2018.

[107] B. Tian, Q. Li, Y. X. Yang, D. Li, and Y. Xin, "A ranging based scheme for detecting the wormhole attack in wireless sensor networks," *J. China Universities Posts Telecommun.*, vol. 19, pp. 6–10, 2012.

[108] R. Matam and S. Tripathy, "WRSR: wormhole-resistant secure routing for wireless mesh networks," *J. Wirel. Com. Netw.*, vol. 180, 2013. Doi: 10.1186/1687-1499-2013-180.

[109] F. Shi, W. Liu, D. Jin, and J. Song, "A countermeasure against wormhole attacks in MANETs using analytical hierarchy process methodology," *Electron Commerce Research*, vol. 13, pp. 329–345, Springer, 2013. Doi: 10.1007/s10660-013-9122-3.

[110] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," *Wireless Network Security*, Springer, Signals and Communication Technology, 2007. Doi: 10.1007/978-0-387-33112-6_5.

[111] A. S. Mhd. Nurul and K. Ferens, "A computationally intelligent approach to the detection of wormhole attacks in wireless sensor networks," *Adv. Science, Technol. Eng. Syst. J.*, vol. 2, no. 3. pp. 302–320, 2017.

[112] J. Karlsson, L. S. Dooley, and G. Pulkkis, "A new MANET wormhole detection algorithm based on traversal time and hop count analysis," *Sensors*, vol. 11, pp. 11122–11140, 2011.

[113] F. Shi, W. Liu, D. Jin, and J. Song, "A countermeasure against wormhole attacks in MANETs using analytical hierarchy process methodology," *Electron. Commer. Res.*, vol. 13, pp. 329–345, 2013.

[114] J. Karlsson, L. S. Dooley, and G. Pulkkis, "Identifying time measurement tampering in the traversal time and hop count analysis (TTHCA) wormhole detection algorithm," *Sensors*, vol. 13, p. 5, 2013.

[115] Z. A. Khan, and M. H. Islam, "Wormhole attack: A new detection technique," *Proceedings International Conference on Emerging Technologies, ICET*, 2012, 1-6.

[116] P. Sharma, and R. K. Dwivedi, "Detection of high transmission power based wormhole attack using received signal strength indicator (RSSI)," *First International Conference, CNC*, Gwalior, India, March 2018, pp. 22-24.

[117] S. U. Qazi, Contributions to securing mobile ad hoc networks against wormhole attacks n multirate transmission, Doctor of Philosophy thesis, School of Computer Science and Software Engineering, University of Wollongong, 2016.

[118] S. Hazra, and S. K. Setua, "Trust oriented secured AODV routing protocol against rushing attack," *Advances in Intelligent Systems and Computing*, vol. 176, Berlin, Heidelberg, Springer, 2012. Doi: 10.1007/978-3-642-31513-8_79.

[119] P. Amish and V. B. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," *Procedia Computer Sci*, vol. 79, pp. 700–707, 2016.

[120] G. Liu, Z. Yan, and W. Pedrycz, "Data collection for attack detection and security measurement in mobile ad hoc networks: A survey," *J. Netw. Computer Appl.*, vol. 105, pp. 105–122, 2018.

[121] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, "Analysis of detection features for wormhole attacks in MANETs," *Procedia Computer Science*, Elsevier, vol. 56, pp. 384–390, 2015.

[122] L. Lu, M. J. Hussain, G. Luo, and Z. Han, "Pworm: passive and real-time wormhole detection scheme for WSNs, Hindawi Publishing Corporation," *Int. J. Distrib. Sens. Netw.*, p. 16, 2015.

[123] N. A. Mhd, K. Shaon, and A. Ferens, "Computationally intelligent approach to the detection of wormhole attacks in wireless sensor networks," *Adv. Science, Technol. Eng. Syst. J.*, vol. 2, no. 3. pp. 302–320, 2017.

[124] S. M. Jen, C. S. Laih, and W. C. Kuo, " A hop-count analysis scheme for avoiding wormhole attacks in MANET," *Sensors*, vol. 9, pp. 5022–39, 2009.

[125] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, and P. Kar, "Wormhole detection based on ordinal MDS using RTT in wireless sensor network," *Hindawi Publishing Corporation Journal of Computer Networks and Communications*, 2016, 15.

[126] E. Zamani, and M. Soltanaghaei, "The improved overhearing backup AODV protocol in MANET," *Hindawi Publishing Corporation Journal of Computer Networks and Communications*, 2016, 8.

[127] T. V. P. Sundararajan, S. M. Ramesh, R. Maheswar, and K. R. Deepak, "Biologically inspired artificial intrusion detection system for detecting wormhole attack in MANET," *Springer Science Business Media New York, Wireless Network*, 2013.

[128] S. Jamali, and R. Fotohi, "DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system," *J Supercomput*, 73, 2017, 5173-5196.

[129] G. Farjamnia, Y. Gasimov, and C. Kazimov, "Review of the techniques against the wormhole attacks on wireless sensor networks," *Wireless Personal Communications, Springer Science, Business Media*, 2019.

[130] D. Sharma, V. Kumar, and R. Kumar, "Prevention of wormhole attack using identity based signature scheme in MANET," *Comput. Int. Data Min.*, pp. 475–485, 2016.

[131] V. Kumar and R. Kumar, "An Optimal Authentication Protocol Using Certificateless ID-Based Signature in MANET," *Security Comp. & Comm.*, vol. 536, pp. 110–112, 2015.

[132] M. Sookhak, A. Akhundzada, A. Sookhak, M. Eslaminejad, A. Gani, M. Khurram Khan, et al., "Geographic wormhole detection in wireless sensor networks," *PLoS ONE*, vol. 10, no. 1. p. e0115324, 2015.

[133] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A Passivity framework for modelling and mitigating wormhole attacks on networked control systems," *IEEE Trans. Autom. Control.*, vol. 59, no. 12. pp. 3224–3237, 2014.

[134] D. U. Kim, H. W. Kim, G. Kim, and S. A. Kim, "Counterattack-detection scheme in transmission time-based wormhole detection methods," *Int. J. Distrib. Sens. Netw.*, vol. 9, no. 3. p. 184931, 2013.

[135] H. S. Chiu, and K. S. Lui, "DelPHI: Wormhole detection mechanism for ad hoc wireless networks," *International Symposium on Wireless Pervasive Computing ISWPC*, Phuket, 2006, 6.

[136] T. P. Van Tran, Y. K. Le Xuan Hung, S. Lee, and H. Lee, "Transmission time based mechanism to detect wormhole attack," *Proceedings of the IEEE Asia-Pacific Service Computing Conference*, 11–14, 2007, 172-178.

[137] S. M. Jen, C. S. Laih, and W. C. Kuo, "A hop-count analysis scheme for avoiding wormhole attacks in MANET," *Sensors*, vol. 9, pp. 5022–39, 2009.

[138] F. N. Abdesselam, B. Bensaou, and T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks," *Security In Mobile Ad Hoc and Sensor Networks*, IEEE Communications Magazine, 2008.

[139] S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Multirate DelPHI to secure multirate ad hoc networks against wormhole attack," *J. Inf. Security Appl.*, vol. 39, pp. 31–40, 2018.

[140] C. Gupta, and P. Pathak, "Movement based or neighbour-based technique for preventing wormhole attack in MANET," *Symposium on Colossal Data Analysis and Networking* (*CDAN*), Indore, India, 2016, 1-5.

[141] C. Lee and J. Suzuki, "SWAT: A decentralized self-healing mechanism for wormhole attacks in wireless sensor networks," *Handb. Sens. Netw.*, pp. 511–532, 2010.

[142] S. M. Jen, C. S. Laih, W. C. Kuo, and A. Hop-Count, "Analysis scheme for avoiding wormhole attacks in MANET," *Sensors*, vol. 9, pp. 5022–5039, 2009.

[143] L. Qian, N. Song, and X. Li, "Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach," *J. Netw. Computer Appl.*, vol. 30, pp. 308–330, 2007.

[144] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," *IEEE Conference on Wireless Communications and Networking*, 2, 2005, 1193-1199.

[145] Z. Yifeng, L. Lamont, and L. Li, "Wormhole attack detection based on distance verification and the Use of hypothesis testing for wireless ad hoc networks," *IEEE Conference on Military Communications*, Boston, MA, 2009, 1-7.

[146] S. Capkun, L. Buttyan, and J. P. Hubaux, "Sector: Secure tracking of node encounters in multi-hop wireless networks," *Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks* (*ACM SANS*), 2003, 21-32.

[147] M. O. Johnson, A. Siddiqui, and A. Karami, "A wormhole attack detection and prevention technique in wireless sensor networks," *Int. J. Computer Appl.*, vol. 174, no. 4. pp. 1–8, 2017.

[148] S. Bai, Y. Liu, Z. Li, and X. Bai, "Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures," *Computer Netw*, vol. 150, pp. 190–200, 2019.

[149] F. Barani, "A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system," *Iranian Conference on Intelligent Systems*, ICIS, 2014.

[150] L. E. Jim and M. A. Gregory, "A review of artificial immune system based security frameworks for MANET," *Int. J. Communications, Netw. Syst. Sci.*, vol. 9, pp. 1–18, 2016.

[151] S. Jamali and R. Fotohi, "Defending against wormhole attack in MANET using an artificial immune system," *N. Rev. Inf. Netw.*, vol. 21, no. 2. pp. 79–100, 2016.

[153] S. Upadhyay, and B. K. Chaurasia, "Detecting and avoiding wormhole attack in MANET using statistical analysis approach," *Advances in Computer Science and Information Technology. Networks and Communications, CCSIT*, 84, Springer, 2012.

[154] S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Securing DSR against wormhole attacks in multirate ad hoc networks," *J. Netw. Computer Appl.*, vol. 36, no. 2, pp. 582–592, 2013.

[155] D. Kim, H. Kim, G. Kim, and S. Kim, "A counterattack-detection scheme in transmission time-based wormhole detection methods," *Hindawi Publ. Corporation, Int. J. Distrib. Sens. Netw.*, vol. 9, no. 3. p. 184931, 2013.

[156] J. Karlsson, L. S. Dooley, and G. Pulkkis, "Identifying time measurement tampering in the traversal time and hop count analysis (TTHCA), wormhole detection algorithm," *Sensors*, vol. 13, no. 5. pp. 6651–6668, 2013.

[157] T. Giannetsos and T. Dimitriou, "LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks," *J. Computer Syst. Sci.*, vol. 80, no. 3. pp. 618–643, 2014.

[158] M. Sookhak, A. Akhundzada, A. Sookhak, M. Eslaminejad, A. Gani, M. Khurram Khan, et al., "Geographic wormhole detection in wireless sensor networks," *PLoS One*, vol. 10, no. 1. p. e0115324, 2015.
[159] S. Ji, T. Chen, and S. Zhong, "Wormhole attack detection algorithms in wireless network coding systems," *IEEE Trans. Mob. Comput.*, vol. 14, no. 3. pp. 660–674, 2015.
[160] S. Qazi, R. Raadb, Y. Mua, and W. Susiloa, "Multi-rate DelPHI to secure multi-rate ad hoc networks against wormhole attacks," *J. Inf. Security Appl.*, vol. 39, pp. 31–40, 2018.
[161] D. S. K. Tiruvakadu and V. Pallapa, "Confirmation of wormhole attack in MANETs using honeypot," *Computers & Security*, vol. 76, pp. 32–49, 2018.
[162] S. Sankara Narayanan, and G. Murugaboopathi, "Modified secure AODV protocol to prevent wormhole attack in MANET," *Special Issue on Advances in Metaheuristic Optimization Algorithms (AMOA2018), willey*, John Wiley & Sons Ltd, 2018.
[163] K. Karthigadevi, S. Balamurali, and M. Venkatesulu, "Wormhole attack detection and prevention using EIGRP protocol based on round trip time," *J. Cyber Security Mobil.*, vol. 7, no. 1. pp. 215–228, 2018.
[164] S. Bai, Y. Liu, Z. Li, and X. Bai, "Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures," *Computer Networks, IEEE Access*, vol. 150, pp. 190–200, 2019.
[165] X. Luo, Y. Chen, M. Li, Q. Luo, K. Xue, S. Liu, et al., "CREDND: A novel secure neighbour discovery algorithm for wormhole attack," *IEEE Access*, vol. 7, pp. 18194–18205, 2019.
[166] W. A. Aliady and S. A. Al-Ahmadi, "Energy preserving secure measure against wormhole attack in wireless sensor networks," *IEEE Access*, vol. 7, pp. 84132–84141, 2019.
[167] N. Tamilarasi, and S. G. Santhi, "Detection of wormhole attack and secure path selection in wireless sensor network," *Wireless Pers Commun*, 114, 2020, 329-345.
[168] M. M. Singh, N. Dutta, T. R. Singh, and U. Nandi, "A technique to detect wormhole attack in wireless sensor network using artificial neural network," *Evolutionary Computing and Mobile Sustainable Networks*, 53, Springer, 2020.
[169] P. Kaur, D. Kaur, and R. Mahajan, "Wormhole attack detection technique in mobile ad hoc networks," *Wirel. Personal. Commun.*, vol. 97, pp. 2939–2950, 2017.
[170] M. Xie, J. Hu, S. Han, and H. -H. Chen, "Scalable hypergrid KNN-based online anomaly detection in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, p. 8, 2013.
[171] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on KNN classification algorithm in wireless sensor network," *J. Electr. Computer Eng.*, pp. 1–8, 2014.
[172] C. Titouna, M. Aliouat, and M. Gueroui, "Outlier detection approach using Bayes classifiers in wireless sensor networks," *Wirel. Pers. Commun.*, vol. 85, pp. 1009–1023, 2015.
[173] M. Wazid and A. K. Das, "An efficient hybrid anomaly detection scheme using K-means clustering for wireless sensor networks," *Wirel. Pers. Commun.*, vol. 90, pp. 1971–2000, 2016.
[174] B. Subba, S. Biswas, and S. Karmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation," *Eng. Sci. Technology, an. Int. J.*, vol. 19, no. 2. pp. 782–799, 2016.
[175] Z. Feng, J. Fu, D. Du, F. Li, and S. Sun, "A new approach of anomaly detection in wireless sensor networks using support vector data description," *Int. J. Distrib. Sens. Netw.*, vol. 13, 2017.
[176] H. Saeedi Emadi and S. M. Mazinani, "A novel anomaly detection algorithm using DBSCAN and SVM in wireless sensor networks," *Wirel. Pers. Commun.*, vol. 98, pp. 2025–2035, 2018.
[177] M. S. Khan, L. Khan, N. Gul, M. Amir, J. Kim, and S. M. Kim, "Support vector machine-based classification of malicious users in cognitive radio networks," *Wirel. Commun. Mob. Comput.*, p. 11, 2020.
[178] K. G. Reddy and P. S. Thilagam, "Naïve Bayes classifier to mitigate the DDoS attacks severity in ad-hoc networks," *Int. J. Commun. Netw. Inf. Security (IJCNIS)*, vol. 12, no. 2. pp. 221–6, 2020.
[179] S. A. Elsaid, and N. S. Albatati, "An optimized collaborative intrusion detection system for wireless sensor networks," *Springer-Verlag GmbH Germany, Soft Computing*, Springer Nature, 2020.
[180] W. Zhang, D. Han, K. C. Li, and F. I. Massetto, "Wireless sensor network intrusion detection system based on MK-ELM," *Soft Computing, Springer-Verlag GmbH Germany*, Springer Nature, 2020.
[181] K. S. Sankaran, N. Vasudevan, K. R. Devabalaji, T. S. Babu, H. H. Alhelou, and T. Yuvaraj, "A recurrent reward based learning technique for secure neighbor selection in mobile ad-hoc networks," *IEEE Access*, vol. 9, pp. 21735–45, 2021.
[182] R. Meddeb, F. Jemili, B. Triki, and O. Korbaa, "Anomaly-based behavioral detection in mobile ad-hoc networks," *Procedia Computer Sci*, vol. 159, pp. 77–86, 2020.
[183] M. Prasad, S. Tripathi, and K. Dahal, "Wormhole attack detection in ad hoc network using machine learning technique," *10th ICCCNT*, IEEE – 45670, IIT – Kanpur, 2019.
[184] M. Tahboush and M. Agoyi, "A hybrid wormhole attack detection in mobile ad-hoc network (MANET)," *IEEE Access*, vol. 9, pp. 11872–83, January 13, 2021.
[185] J. Zhang, I. Vukotic, and R. Gardner, "Anomaly detection in wide area network mesh using two machine learning anomaly detection algorithms," *CoRR*, Cornell university, 2018, 1801-10094.
[186] P. K. Singh, R. R. Gupta, S. K. Nandi, and S. Nandi, "Machine learning based approach to detect wormhole attack in VANETs," *Dev. Primatology: Prog. Prospect.*, pp. 651–661, 2019.
[187] M. Abdan and S. A. H. Seno, "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)," *Wirel. Commun. Mob. Comput.*, p. 2375702, 2022, Doi: 10.1155/2022/2375702
[188] H. Shahid, H. Ashraf, H. Javed, M. Humayun, N. Jhanjhi, and M. A. AlZain, "Energy optimised security against wormhole attack in IoT-based wireless sensor networks," *Computers, Mater. Continua*, vol. 68, no. 2. pp. 1967–81, 2021 Jan 1, Doi: 10.32604/cmc.2021.015259.
[189] A. M. Alajlan, "Multi-step detection of simplex and duplex wormhole attacks over wireless sensor networks," *Computers,Materials Continua*, vol. 70, no. 3. pp. 4241–59, 2022, Doi: 10.32604/cmc.2022.020585.
[190] L. Singh, A. Alam, K. V. Kumar, D. Kumar, P. Kumar, and Z. A. Jaffery, "Design of thermal imaging-based health condition monitoring and early fault detection technique for porcelain insulators using Machine learning," *Environ. Technol. Innov.*, vol. 24, p. 102000, 2021.

[191] A. Alam, L. Singh, Z. A. Jaffery, Y. K. Verma, and M. Diwakar, "Distance-based confidence generation and aggregation of classifier for unstructured road detection," *Journal of King Saud University-Computer and Information Sciences*, 2021.

[192] P. Das, J. K. P. S. Yadav, and L. Singh, "Deep learning-based tomato's ripe and unripe classification system," *Int. J. Softw. Innov.*, vol. 10, no. 1, 2022, Doi: 10.4018/IJSI.292023.

[193] K. D. Rose, K. V. Kumar, L. Singh, and S. K. Sharma, "Computer aided diagnosis for breast cancer detection and classification using optimal region growing segmentation and mobile net model," *Concurrent Eng*, 2022, Doi: 10.1177/1063293X221080518.

[194] R. Boutaba, M. A. Salahuddin, N. Limam, S. Ayoubi, N. Shahriar, F. Estrada-Solano, et al., "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities," *J. Internet Serv. Appl.*, vol. 9, p. 16, 2018.

[195] M. A. Hossain, R. M. Noor, K. -L. A. Yau, S. R. Azzuhri, M. R. Z'aba, and I. Ahmedy, "Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks," *IEEE Access*, vol. 8, pp. 78054–78108, 2020.

[196] L. Hu, and D. Evans, "Using directional antennas to prevent wormhole attacks," *Proceedings of Network and Distributed System Security Symposium* (*NDSS*), San Diego, California, USA, 2004.

[197] R. R. Choudhury, X. Yang, N. H. Vaidya, and R. Ramanathan, "Using directional antennas for medium access control in ad-hoc networks," *Proceedings of the 8th annual international conference on Mobile computing and networking*, 2002, 59-70.

[198] S. Yi, Y. Pei, and S. Kalyan Raman, "On the capacity improvement of ad-hoc wireless networks using directional antennas," *Proceedings of the 4th ACM international symposium on Mobile ad-hoc networking and computing*, 108–16, 2003. New York, NY, USA, ACM Press.

[199] L. Singh, and A. Alam, "An efficient hybrid methodology for an early detection of breast cancer in digital mammograms," *Journal of Ambient Intelligence and Humanized Computing*, 1-24. Doi: 10.1007/s12652-022-03895-w.

[200] M. Takai, J. Martin, R. Bagrodia, and A. Ren, "Directional virtual carrier sensing for directional antennas in mobile ad-hoc networks," *Proceedings of the 3rd ACM international symposium on Mobile ad-hoc networking and computing*, 2002, 183-9.

[201] S. Brands, and D. Chaum, "Distance-bounding protocols," *Theory and Application of Cryptographic Techniques*, 1993, 344-59.

[202] D. Liu, P. Ning, and R. Li, "Establishing pair-wise keys in distributed sensor networks," *ACM Trans. Inf. Syst. Security*, vol. 8, no. 1. pp. 41–77, 2005.

[203] S. Ozdemir, Functional reputation based reliable data aggregation and transmission for wireless sensor networks, *Computer Communications*, vol. 31, no. 17, pp. 3941-53, 2008.

[204] L. E. Jim and M. A. Gregory, "A review of artificial immune system based security frame works for MANET," *Int. J. Communications, Netw. Syst. Sci.*, vol. 9, pp. 1–18, 2016.