International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I6P227

Volume 71 Issue 6, 259-273, June 2023

Review Article

Survey on Packet Dropping Detection Techniques in Wireless Sensor Network

Sebastian Terence[1], Jude Immaculate[2], P. Geethanjali[3]

[1]*Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India.*
[2] *Department of Mathematics, Karunya Institute of Technology and Sciences, Coimbatore, India.*
[3]*SELECT, VIT University, Vellore, India.*

[3]*Corresponding Author : pgeethanjali1@.vit.ac.in*

Received: 27 March 2023 Revised: 30 May 2023 Accepted: 14 June 2023 Published: 25 June 2023

Abstract *- Wireless sensors network does not have a fixed data communications infrastructure. These networks are used in different situations, mainly in times of disaster, field monitoring, forest monitoring and so on. These networks are mainly used in open environments where human interactions are much lower. The open environment and its communication nature lead to various attacks on these networks. Based on the nature of the attack, we have grouped three packet-dropping attacks, namely the blackhole attack, the grayhole attack and the sinkhole attack. These three attacks use the same methodology to initiate the attack, but the results of these attacks differ. In this paper, we have studied packet-dropping attacks and analyzed solutions against these packet-dropping attacks. The main goal of the study is to present different detection strategies for packet-dropping attacks. In the study, we have examined around 70 papers, classifying these detection techniques into seven categories: sequence number detection, route request/reply-based detection, cross-layer detection, bait route request detection and acknowledgement-based detection, multi-parameter-based detection and miscellaneous detection. In this study, we found that 30% of solutions were given against multiple attacks, and less than 3% of papers attempted to detect cooperative attacks. In this study, we also observe that 40% of techniques considered energy consumption in attack detection; similarly, 35% and 30% of solutions considered false positives and false negatives in malicious attack detection. Challenges and possible work directions of malicious package-dropping techniques are also discussed*.

Keywords *- Packet dropping attacks, Grayhole attack, Sinkhole attack, Wireless Sensor Network, Blackhole attack.*

1. Introduction

The traditional network needs certain infrastructure for communication, such as routers, access points, etc. But an Ad-hoc network is designed to provide communication without any infrastructure and is mainly used in places where there is no infrastructure [1]. Ad-hoc networks are classified into the mobile ad-hoc network (MANET), the wireless sensor network (WSN), the delay-tolerant network (DTN), etc. WSNs are used for data communication in different places, such as natural disaster areas, border fields, fire and animal monitoring in the forest, etc. Although WSN has a huge application, it has a few drawbacks. Security problems are among the key disadvantages of WSNs. WSN makes use of hop-to-hop communication. Each device depends on its peer devices for data communication in hop-to-hop communication. This fact is misused by the adversary to launch various attacks in WSN, namely attacks like a sinkhole, wormhole, grayhole and blackhole attack, etc. [2]. The adversaries use various mechanisms to launch these attacks. Among these assaults, the blackhole, grayhole, and sinkhole attacks all employ the same attack approach [3]. Though these three attacks use the same strategy, the consequences of these attacks differ. In these attacks, the adversary grabs the node and inserts fake information in these assaults. The node in which false details are inserted is called the compromised node. The ultimate objective of the compromised node is to track the traffic on the network. To achieve this, the compromised node broadcasts a fake routing advertisement claiming it has the shortest route to the base station. These attacks disturb networks through data drops and data modifications**.** Different detection mechanisms are proposed by researchers for these attacks, and all these detection techniques have their own benefits and drawbacks [4].

In this paper, we have examined different techniques for detecting blackhole, grayhole and sinkhole attacks in the WSN. We have analyzed and summarized different techniques for detecting blackhole, grayhole and sinkhole attacks in WSN. In this study, we have examined the

parameters such as detection approach, routing protocol, stimulator, network, attack, etc. We have also classified detection techniques as sequence number-based detection, route request number (RREQ)/route reply (RREP) received/forwarded based detection, bait RREQ-based detection, cross-layer based detection, acknowledgement (ACK) based detection, multi-parameter based detection and miscellaneous detection. Critical parameters for detection, such as energy consumption, false positive, false negative, and ability to handle multiple attacks and cooperative attacks, are also analysed. The paper is structured as follows; brief notes of WSN are given in Section 2. Packet-dropping attacks are outlined in section 3. Section 4 describes the paper selection strategy. Packet-dropping detection techniques are discussed in section 5. The future direction of research is given in section 6. In Section 7, the conclusion is provided.

2. Wireless Sensor Network

WSN comprises numerous sensors and a base station. Sensors are small computational devices used for environmental monitoring. These sensors are placed in an open environment to observe environmental changes. They are small in terms of size, storage capacity, energy and computation. As sensors are used commonly in remote places, most sensors are not connected with power; instead are equipped with rechargeable batteries. As sensors are small in size, they are limited by storage capacity and computation power [5]. The main function of a sensor is to observe environmental changes and to involve itself in the data transmission process. The base station is a powerful node, generally a device, computer (or) laptop. The main task of the base station is to collect data from the sensor node. Humans can interact with the base station to gather and work on the collected data. WSNs are used in multiple fields, such as battery fields, forest fire detection, and animal monitoring, to detect oil leakage in oil industries, air quality monitoring in industrial areas, early landscape detection, etc. WSNs are generally applied in human-isolated places to identify environmental changes [6]. Wide applications of WSN have turned researchers towards it in solving various research problems such as efficient energy management, data collection and management, quality of service (QoS), synchronization, heterogeneity, localization, security [7], etc.

3. Packet Dropping Attacks in WSN

Sinkhole attacks, blackhole attacks, and grayhole attacks all begin with a similar strategy. The adversary grabs the node and inserts fake information into these assaults. The node in which false details are inserted is called the compromised node. The ultimate objective of the compromised node is to track the traffic on the network. To achieve this, the compromised node broadcasts a fake routing advertisement claiming it has the shortest route to the base station. The neighbors of the compromised node believe in fake routing advertisements and send data packets to the compromised node for data dissemination to the base station. After attracting neighbor traffic, the compromised node may be involved in malicious activities based on the nature of the attack [8]. Based on malicious behaviour, these attacks are classified into blackhole attacks, grayhole attacks and sinkhole attacks. The infected node in a blackhole operation could discard all the information it received; in a grayhole threat, the infected sensor could discard information packets arbitrarily, as well as the case of a sinkhole threat, the infected node may engage in any of the following behaviours.: read, tamper, and drop selective data packets (or drop all the received data packets). All three attacks use the same strategy to initiate the attack, but their impact on the sensor network differs. Similar to all other attacks, these three attacks have a huge impact on the performance of the network, and this is what brings our attention towards these attack detection strategies. Various methods for detecting these attacks have been developed by researchers, which will be in section 5.

4. Related Work

The following survey works have been carried out in reviewing these malicious attacks. Kibirige et al. [77] reviewed sinkhole attack detection in WSN. The limitation of this work, experimental parameters are not included. Rani et al. [78] reviewed balckhole attack detection techniques. The major drawback of this work is that limitations of detection techniques are not given. Amulya et al. [79] analysed sinkhole detection techniques. Singh et al. [80] survived blackhole attack detection in WSN. Alansari et al. [81] projected routing attack detection techniques. Most of the existing work does not review methodology or implementation details such as simulator, number of sensor nodes, area, or malicious node. None of the existing work reviewed sinkhole, grayhole, and blackhole attacks. The above limitations are overcome in the current work.

5. Detection Techniques Against Packet Dropping Attacks in WSN

5.1. Sequence number-based Detection

The origin node examines its received route reply sequence number to the threshold value in the sequence number-based detection approach. If the recipient route's sequence number exceeds the allowed value, the related originator node is flagged as malicious. But many of these identification methods suffer from false positives and false negatives. Karuppiah et al. [9] employed a status bit and sequence number-based screening approach to strengthen the watchdog monitoring system to stop fraudulent packet-dropping assaults. Since the watchdog suffers due to collision and limited transmission power, it declares the normal node as a malicious node. The status bit decreases the possibility of a rogue node being misidentified. The two types of status bit values aid in recognising problematic

nodes with downstream and upstream nodes containing suspicious sequences. This technique is implemented in an NS2 stimulator with 10 sensor nodes and one malicious node. This method detects malicious nodes with 58% of less energy consumption. Salunke *et al.* [10] compared the sender sequence to the threshold value to detect malicious nodes. In order to identify blackhole attacks, periodically threshold for a sequence number is calculated. A threshold is calculated based on the highest sequence number generated by sensor nodes. Sequence numbers used in route replies are compared with a threshold value; if the sequence number is greater than the threshold value, then the route advertiser would be considered a malicious node. The main limitation of this method, since malicious node identification is based on a threshold value, there would be false positives and false negatives in malicious node detection. However, the author did not test false positives and false negatives for this technique.

5.2. Number of Route Requests (RREQ) / Route Reply (RREP) Received / Forward-Based Detection

Generally, malicious nodes forward less RREQ packets compared to a genuine node. On this basis, much research has been done to identify malicious nodes. Wazid *et al*. [11] projected a technique based on the packet drop behavior to detect malicious nodes. In this technique, sensor nodes are classified into coordinator nodes and sensing nodes. If a sensor triggers only route reply packets without forwarding data packets, it would be considered a malicious node. The coordinator node maintains the sensor id, malicious node details, etc. The limitation of this methodology is the lack of contribution towards threshold calculation, false positive and false negative.

Dutta *et al.* [13] applied dual methods to detect malicious nodes in the multipath routing protocol. In this technique, each cluster is monitored by a monitor node. The monitor node monitors the number of packets sent by each node. If any nodes send more number of route replies for route request packets, then it would be classified as a suspicious node. The monitor node sends a fake route request; if a suspicious node sends a reply to a fake route request, it would be considered a malicious node. The dual detection method helps to reduce false malicious identification.

Nam *et al.* [14] have developed a safe route against the malicious packet-dropping attack to avoid a compromised node in the route discovery process using a fuzzy logic system. Each node selects its next forwarding node using the fuzzy logic method in this method. It confirms the data delivery with the next forwarding node whenever it forwards data. Cryptography key management techniques are used to prevent data corruption. The advantage of this technique is that it consumes less energy compared with the LEAP protocol.

Sundararajan *et al.* [15] proposed an instruction detection technique for low-energy adaptive clustering hierarchy (LEACH). The base station employs screening methods to identify sinkhole and selective packet-dropping attacks. The number of packets sent values and the number of packets obtained values are gathered by the base station from the cluster head and cluster members. Using the received value, the message-losing ratio is computed, and if it is less than the threshold, the relevant cluster head is deemed a sinkhole node. This approach discovers sinkhole nodes only if the sinkhole node serves as a cluster node. This study does not address the prevention and identification mechanism for sinkhole node data tampering. Guo *et al*. [58] used a rule-based security strategy to detect various malicious behaviors in the wireless network. Amol *et al*. [16] suggested a multi-level trust system, such as peer-to-peer trust, cluster head-to-sensor trust, and base station-to-cluster trust, to detect malicious nodes.

Peer-to-peer trust is calculated based on the sensor node's past packet-forwarding nature and past behavior. Cluster head-to-sensor Trust is calculated based on the average trust value of sensor nodes in the cluster. The limitation of this technique is that it yields high false positives. Sahoo et al. [17] used applied trust in order to classify effective and ineffective transmission of nodes to detect malicious packet-dropping attacks. Bisen et al. [64] detected a blackhole attack in WSN by analyzing the packet-forwarding nature of sensor nodes. They detected a malicious node by its behaviour. The strategies discussed above mainly focus on the behavior of nodes and traffic information to detect malicious nodes.

5.3. Cross-Layer-Based Detection

Researchers used more than one layer of details to detect malicious activities, termed cross-layer techniques. Various cross-layer techniques are discussed below. Ren *et al.* [18] used multilayer details to detect malicious nodes. The normal packet loss rate and malicious packet loss of each node are evaluated by its neighbor during the evaluation period. The evaluated values are updated in the status table. Each node shares its status table with its neighbor so that other nodes can integrate the received values into their own status table. Normal packet loss rates are calculated during the channel estimation stage, where packet loss due to radio link quality and MAC layer collisions are considered to calculate the normal packet loss ratio. During data transmission, each node records the number of packets transferred to its neighbor and the number of packets forwarded by its neighbor. The sensor node uses a normal packet drop ratio and neighbor’s packet forwarding ratio to evaluate the neighbor reputation value of neighbor nodes. Each node evaluates its neighbor's reputation and propagates evaluated reputation value to its neighbor. The channel behavior is estimated by calculating the normal packet loss ratio; it helps to differentiate the selective forward attacks from normal

packet loss. The limitation of this method is that sensor nodes are static; the normal packet loss rate is difficult to estimate, whereas sensor nodes are mobile. Umar et al. [19] used a fuzzy logic system with the following elements like connectivity cost, residual energy and distance to find the malicious node in the sensor network. This methodology was evaluated using a MATLAB simulator, and the result shows that it yields a high packet delivery rate in the presence of less number of attackers. However, its packet delivery rate was rescued when the number of malicious nodes increased. In order to increase the performance, the same authors used more number of parameters to detect malicious nodes.

They have used the parameters extracted from the physical layer, the MAC layer and the network layer, namely remaining energy, remaining buffer capacity, relay packet rate, received signal-to-noise ratio, buffer occupancy period, packet waiting period, and traffic statistics to detect malicious nodes. The utilization of multiple parameters increases the packet. Qin *et al.* [21] located a malicious node based on the trust of the sensor node. The trust was calculated based on sensor characteristics such as residual energy, node movement, etc. Each node calculates direct trust and indirect trust. The false positive and false negative of the proposed techniques is not evaluated. Ghugar *et al.* [82] also located malicious nodes based on trust, whereas trust was measured from three layers such as a physical layer, a MAC layer, and a network layer.

Trusts are calculated based on a directional interaction between sensor nodes. The proposed solution is not suitable for outdoor experiments. The authors [66] used data link layer details. The sensor nodes were allowed to observe (overhear) the parent data transmission details to detect the network's sinkhole node. This technique uses the MAC layer and network layer details to detect sinkhole nodes, and the identified sinkhole nodes are isolated in the network layer. Multi-layer detection technology delivers good performance in terms of detection rate, packet delivery rate, throughput, etc. However, these techniques provide a high level of overhead compared to other detection methods.

5.4. Bait RREQ-Based Detection

Few researches have been performed using fake route requests to identify malicious nodes in the network. Periodically a fake route request [(i.e.) route request is generated for an unknown node] is created in the network. If any node sends a route reply to this fake route request, the corresponding node is considered to be malicious. Various bait route-based detection requests are discussed here. Dharini *et al.* [23] projected a decentralized fake route request methodology to detect packet drop and selective packet drop attacks. This fake route response technique helps to locate and isolate the malicious node in the network. However, the downside is that this decreases message overhead and increases communication costs.

5.5. Acknowledgement Based Detection

The infected node loses a data packet during data transmission, preventing the origin node from obtaining an acknowledgement packet from the destination node. On this basis, a number of acknowledgement-based detection techniques have been introduced. Yu *et al.* [59] introduced an intermediate multi-acknowledgement scheme to detect selective packet drops on the network. The system utilizes cryptography encryption and decryption functions to authenticate the data and acknowledgement packets. The system's limitation is that it did not differentiate between genuine and malicious packet loss. Altisen *et al.* [24] used end-to-end network layer acknowledgment to detect the network's blackhole, grayhole, wormhole and sybil node. This method calculates each node's reputation based on its packet delivery nature. It is a packet delivery nature accessed with the help of network acknowledgement. The limitation of this method is that since the sensor's reputation is not shared between another sensor node, the sensor reputation is not publically accessible. Terence *et al*. [3] utilized network layer end-to-end acknowledgement to identify malicious nodes. This technique used acknowledgement from the base station to calculate the suspicious value of the sensor node. This technique suffered due to high false positive and false negative. The end-to-end network layer acknowledgement mechanism helps to reduce the number of packet transfers needed to detect a malicious node.

5.6. Acknowledgement Based Detection

Researchers used several parameters to detect malicious packet drop operations, which improved detection accuracy and decreased the false detection rate. Fang *et al.* [25] calculated the trust of the nodes based on a behavioral and beta-reputation model for discovering malicious activity in the network. Wazid *et al.* [26] used the following parameter, namely the number of RREQ / RREP received and forwarded, delay, communication distance and energy to detect malicious nodes. In this technique, network data is applied to the K-means clustering algorithm, which can detect the sensor node's malicious activity. This technique can deal with multiple attacks and yields less false positives. Yang *et al.* [27] used a multi-parameter trust evaluation technique to identify malicious nodes in the network. Direct trust and indirect trust of sensor node calculated based on remaining energy and number of hops in route reply. The advantage of this technique is that it consumes less energy. Wang *et al.* [28] used a variety of technologies, such as reputation systems, k-means clustering, and shortest path analysis, to detect malicious nodes. The sensor node reputation is calculated based on past sensors' behaviours and location. Then, these nodes are classified by the k-means clustering algorithm. The limitation of this method is that it needs GPS to identify malicious nodes. Terence *et al.* [29] analyzed packet forwarding nature, sequence number, hop count and control packet details to find blackhole, grayhole and sinkhole attacks in WSN. The reputation of each node is

calculated based on above mentioned parameters. The least reputed nodes are predicted as malicious nodes. This method suffered due to false positives and false negatives.

5.7. AI and ML-Based Detection

Recently researchers applied AI and machine learning models to detect malicious behavior in WSN. Such AI and ML-based detection techniques are discussed here. Jiang et al. [57] applied multiple machine-learning algorithms in order to identify suspicious nodes in the WSN. More than 15 parameters are used as independent variables to predict and classify malicious attacks. It is found that LightGBM performed better in terms of accuracy compared with other algorithms such as LR, SVM, KNN, RF, etc. In [68], Almaslukh et al., 2021 used a publicly available WSN dataset and proposed an artificial neural network-based model called entity embedding. The proposed technique's performance is compared with SVM, Decision Tree, KNN, CNN, etc., and the proposed technique was able to detect different attacks with greater accuracy.

The disadvantage of this system is that the model was trained with a single dataset. In [69], Alruhaily et al. 2021, used Naïve bayes and a Random forest-based model to detect multiple attacks in a publically available WSN dataset. The models are implemented by Python 3.7 and Scikit-learn. The authors used 18 parameters, such as the number of advertisements, data packet, distance, energy, etc., as independent variables, and the result shows that it yields less true positive. Rezvi et al. 2021[70] applied support vector machine, Naïve bayes, logistic regression, Naïve bayes, K-nearest neighbour (KNN) machine learning algorithms and ANN models in WSN data set to detect packet dropping nodes. The authors used 19 parameters, and the dataset contains. 374661instances. They concluded that ANN and KNN yield better results than other techniques. Ashraf et al. [71] applied ML algorithms in the WSN data set and identified malicious nodes in the network. ML techniques such as ANN, Logistic regression, Support Vector Machine (SVM), Navie Bayes, and KNN are used to detect malicious attacks. They concluded that ANN and KNN performed better than other machine learning algorithms. Nithiyanandam *et al*. [72] applied AI-based rule-matching techniques to identify suspicious nodes in WSN. The sensor nodes were grouped, and sinkhole nodes were identified as sinkhole nodes based on the bee colony technique. Ifzarne et al. [62] identified malicious nodes using an online passive-aggressive algorithm and information gain ratio method. The authors used 18 parameters as independent variables to classify nodes as malicious and normal nodes. The system trains the dataset in offline mode and finds the abnormal behavior in online mode. Most of the detection techniques discussed above used offline data sets and some detection methodologies used less number of data sets, which led to poor accuracy.

5.8. Miscellaneous Detection Technique

Some researchers used miscellaneous detection methodologies, which are discussed here. Rassam et al. [12] applied various rules to identify sinkhole attacks in WSNs. Ngai *et al.* [30] examined the node network through the network flow graph to recognize the suspicious node in the network. Nagi *et al.* [31] analyzed the traffic flow of nodes and discovered a malicious node due to a lack of data flow during packet transmission. Krontiris *et al.* [32] projected a rule-based technique that used a data drop rate to identify the infected node in the network. Krontiris *et al*. [33] enhanced the watchdog mechanism by using a centralized voting mechanism to detect malicious activities in the network. Roy *et al*. [34] used the trust evaluation methodology to identify infected nodes in the network. Chen *et al.* [35] investigated the usage of the central processing unit (CPU) to detect infected nodes in the network. Reddy et al. [36] projected forward-checking and backwards-checking techniques to locate the malicious packets in the network. Samundiswary *et al.* [37] projected an alternative network path for identifying fake network response routes. Stafrace *et al.* [38] applied military commands based on malicious node detection. Mobile agents were used to communicate between sensors to recognise malicious nodes. Sharmila *et al.* [39] used a cryptography technique called a message digest algorithm to identify malicious activity in the network. Sheela et al. [40] utilized mobile agents to ensure the genuine path in route discovery and malicious nodes were identified by its activities.

Mishra *et al.* [41] used several routing paths to prevent malicious packets from dropping into the network. Shafiei *et al.* [42] found the malfunctioning node by analyzing the energy duplication of nodes in the network. Hamedheidari *et al.* [43] used a mobile agent to establish the trust of the sensor node in the network, helping to prevent the spread of fake routes during the route discovery process. Atassi *et al.* [60] implemented an empiric path loss model, where the network detects infected nodes through shadowing and fading effects. Zhang *et al.* [61] used a multi-path (or) redundancy data transfer technique to detect infected nodes in the network. Sreelaja *et al.* [44] applied a colony optimization technique that uses agent methodology to detect malicious nodes in the network. Motamedi *et al.* [45] used the moving part to ensure the position of the node in the network to prevent fake routing details from the malicious node. This method consumes high costs and is not feasible to implement. Abdullah *et al.* [46] examined path advertising hop count values to identify bogus routing advertisements in the wireless sensor network. Dewal *et al.* [47] discovered a packet-dropping node by its behavior in a cluster-based sensor network. Jahandoust [48] combined probability and timed automata to avoid malicious nodes and disperse data packets in a reliable data dissemination direction.

Table 1. Various Components of malicious packet dropping techniques

Author & Year	Simulator	No. of node	Area	Percentage/ number of malicious node	Methodology	Experiment Parameter	Outcome
Karuppiah et al., 2014 [9]	NS2	10	-	1 Blackhole Node	Enhanced watchdog mechanism	Energy Consumption: 75nJ	Sinkhole detection
Salunke et al., 2015 [10]	NS2.35	25	50*50	1 Blackhole Node	Sequence number-based threshold used for detection	Packet Delivery Rate (PDR): 43.79%	Blackhole detection
Wazid *et al*., 2013 [11]	-	30	1000* 500	1 blackhole node	Route reply-based threshold used for detection	Throughput: 65092.06 bps, End-to-end delay: 35.25 (msec)	Blackhole detection
Rassam et al., 2012 [12]	TinyOS	5 nodes	-	1 node	Multiple rule-based detections	-	Sinkhole detection
Dutta and Biswas, 2014 [13]	NS 2.34	10-100	1200 * 1200	-	No. of packets sent by each sensor node and multipath route request-based detection	PDR: 95-98%, End-to-end delay:4.8–5.8(s), Avg. power, consumption: 60-70%	Blackhole detection
Nam et al., 2015 [14]	-	4000	2000 * 2000 m^2	Up to 22%	Fuzzy logic based next node selection	Avg. energy consumption: Up to 550J	Sinkhole detection
Sundararajan et al., 2015 [15]	TETCOS NETSIM	100	-	1 sinkhole node	Packet-dropping ratio-based malicious node detection	Avg. energy consumption: 93-97%, Avg, network throughput: 70-98 (bytes/s), Avg. network lifetime: 170-380 (s)	Sinkhole detection
Amol et al., 2017 [16]	NS2	50	950*950	-	Multilevel trust is calculated based on the sensor's past behavior.	False positive, PDR, Detection Rate	Blackhole, Selective Forwarding, ONOFF attack detection
Sahoo et al. 2018 [17]	Matlab	-	-	Up to 50% of malicious node	Trust-based malicious node detection	-	Malicious packet-dropping node detection
Ren *et al*., 2016 [18]	OMNET++	0-200	50*50m	Up to 30%	Network layer and data link layer details	False detection: 20-99%, Detection ratio: 42-100%, PDR: Up to 70%	Selective forwarding attack detection
Umar et al., 2016 [19]	Matlab	196	150*150m	4 Attackers	MAC layer details with the fuzzy logic system used to detect malicious nodes.	PDR: 95-96%, Energy consumption: 0.05 – 0.25 J/Pkts, End-to-end delay: 400 – 2800 ms	Blackhole and selective forwarding attack detection

Umar *et al*., 2017 [20]	Matlab	196	150*150m	3%-10% of malicious node	MAC layer and the network layer parameters	PDR: 94-96%, Energy consumption: 0.05 – 0.22 J/Pkts, End-to-end delay: 400 – 2600 ms	Blackhole and Sybil attack detection
Qin et al., 2017 [21]	NS2	100	200 * 200m	-	MAC layer and network layer parameters	Routing overhead: 450 mJ, PDR: 95-100%	Bad-mouthing, grayhole, on-off attacks detection
Ghugar et al., 2019 [82]	Matlab	50	100 * 100m^2	2-25%	Physical, MAC and network layer parameters	Detection Accuracy: 95-100%, False positive: 5-32%, False negative: 5-32%	Sinkhole, jamming, blackhole and cross-layer attacks detection
Dharini *et al*.2015 [23]	NS2	-	-	Nine nodes	Fake route request methodology to detect malicious node	-	Flooding and grayhole attack detection
Altisen *et al*. (2016) [24]	NS2	100	1000 * 400 m^2	0%-30%	Network layer acknowledgement	PDR: 93%, End-to-end delay: 22.03, Network throughput: 93.23%, detection rate: 90%, False positive rate: 3.75%	Blackhole detection
Terence et al. (2019) [3]	NS-2.34	600	1000 * 1000	Up to 15%	Network layer acknowledgement	False positive: up to 7%, false negative: up to: 5.5%, PDR: 93-98%, RO: up to 9.5%, throughput: 1.8 Mbps	Blackhole, Sinkhole and Grayhole detection
Wazid and Das, 2016 [26]	Opnet 14.5	720	1000 * 400 m^2	10%	Network layer parameters	Delay: 0.03 s, traffic received: 2000bps, traffic sent: 1000 bps	Blackhole and misdirection node detection
Yang *et al*. 2018 [27]	NS2	50-300	1000 * 1000m^2	Up to 10	MAC and network layer details	PDR: 90-96%, network throughput: 110-125 Kbps, average energy consumption: 43-48 J	Malicious node detection
Wang et al. (2019) [28]	-	1000	100 * 100m	50	Based on the past behavior of the sensor node	PDR: 0.9-1%, Data transmission: up to 4.5 bits	Compromised node detection
Terence et al. (2019) [29]	NS2.34	250	1000 * 1000 m	Up to 25%	Hop count, packet forwarding nature and sequence number	False positive: 4–6%, False negative: 1.2-3%, PDR: up to 95%,	Grayhole, blackhole and sinkhole attack detection

						Throughput: up to 21 kbps, end-to-end delay: up to 22-48ms	
Ngai *et al*. (2006) [30]	-	400	200 * 200m	50 nodes	Graph theory	False negative: up to 10 %, false positive: up to 25%, energy consumption: 980 uJ	Sinkhole attack detection
Ngai *et al*. (2007) [31]	-	400	200 * 200m	Up to 80%	Traffic and data flow in the network	False negative: 80 -100%, false positive: 15 – 100%, energy consumption: 60 uJ	Sinkhole attack detection
Krontiris *et al*., 2007 [32]	TinyOS	100	-	One malicious node	Multiple rules used to detect sinkhole node	-	Sinkhole attack detection
Krontiris *et al*., 2013 [33]	-	1000	-	-	Centralized voting mechanism to detect malicious node	-	Malicious node detection
Roy *et al*., 2008 [34]	NS2	500	1500 * 1800 m	One sinkhole and blackhole node	Trust evaluation method	PDR, percentage of nodes affected	Sinkhole and blackhole attack detection
Chen et al. 2010, [35]	MATLAB	2000	-	5%	Based on CPU utilization	-	Sinkhole attack detection
Reddy *et al*., 2010 [36]	Python language	Up to 100	400 * 400m	Up to 10%	Forward and backward checking of nodes	-	Malicious node detection
Samundiswary *et al*., 2010 [37]	Glomosim	25 to 500	300 * 500m	Up to 10 to 50%	Alternative path used to find malicious node	Energy consumption: up to 4.75J, Delay: 0.5 – 2.5, delivery ratio: 40 – 80%	Sinkhole attack, selective forwarding attack detection
Stafrace et al. 2010 [38]	J-Sim (Java)	49	-	Up to 25%	Mo bile agents used to detect malicious node	Data pack loss: 10-90%, Overhead: 0.5-2.5%	Sinkhole attack detection
Sharmila et al. 2011 [39]	MATLAB	180	-	Up to 50%	Cryptography-based malicious node detection	-	Sinkhole attack detection
Sheela *et al*., 2011 [40]	JProwler (Java)	25-400	-	-	Mobile agent-based malicious detection	-	Sinkhole attack detection
Mishra *et al*., 2011 [41]	-	200	100 * $100m^2$	2 malicious node	Multiple routing paths used to detect malicious node	Packet delivery rate: 60-95%, false positive: 28-2%	Black hole attack detection
Shafiei *et al*., 2014 [42]	OMNeT++	Up to 300	50 * 50 m^2	6 malicious node	-	-	Sinkhole attack detection

Hamedheidari *et al*., 2013 [43]	Customized simulator by .NET framework	Up to 400	200 * 200m	10-20%	Mo bile agents used to detect malicious node	Energy: 0.5 -1J, false positive: 0.4-2x%, packet loss rate: 8-20%, overhead: 5-10%,	Sinkhole attack detection
Atassi *et al*., 2013 [60]	MATLAB	55	-	One malicious node	Applied empiric path loss model to detect malicious node	-	Malicious node detection
Zhang et al. [61]	NS2	Up to 50 nodes	1000 * 1000m	Up to 5 nodes	Multipath and data redundancy to detect malicious node	False positive: 1	Sinkhole attack detection
Sreelaja *et al*., 2014 [44]	-	UP to 100000	-	-	Colony optimization with mobile agent	-	Sinkhole attack detection
Motamedi *et al*., 2015 [45]	NS2	Up to 120		-	Node position used to detect malicious nodes.		Blackhole attack detection
Abdullah *et al*., 2015 [46]	-	100	100 * 100m	-	Hop count in the route advertisement.	Success Rate: 0-100%	Sinkhole attack detection
Dewal *et al*., 2016 [47]	-	-	-	-	Behaviour-based malicious node detection	-	Blackhole attack detection
Jahandoust et al., 2017 [48]	Java language and UPPAAL tool	60	-	Up to 54%	Probability and timed automata-based detection	Packet loss rate, false positive	Sinkhole attack detection
Farooq *et al*., 2016 [49]	NS2	100	-	Eight blackhole nodes	Fake routing details and traffic details	-	Blackhole attack detection
Kalkha *et al*., 2019 [50]	NS2	50	785 * 460m	One malicious node	Applied hidden markov model to detect malicious node	PDR: 0.5, end-to-end delay: 80, PDR: 20	Blackhole attack detection
Lodhi et al. 2020 [51]	NS2.34	-	-	-	Data packet buffer time analysis to detect malicious node	-	Malicious node detection
Devi et al. 2020 [52]	NS2	200	-	-	Slot scheduling, clustering, data aggregation	End-to-end delay: up to 20 ms, PDR: 0.5-0.9 packet drop: 8000 packets, overhead: up to 0.7, residual energy: 8J	Packet loss detection
Liu et al. 2018 [53]	OMNeT	Upto 1000	200 – 500m	-	Route verification in the reverse direction	Detection rate: 1-0.95, detection time: 2-14 min, drop rate: 2-15 %, lifetime: 100-140 min	Sinkhole attack detection
Jasmin et al. 2019[54]	NS 3.25	400	400 * 400 m^2, 1000 * 1000 m^2	8% to 30%	Homomorphic authentication, data fragmentation and	Detection rate: 0.9-1, energy consumption: up	Sinkhole attack, Sybil attack detection

					encryption techniques	to 3.8J, End-to-end delay: 0.08 s	
Zhang et al. 2006 [55]	Real sensor implementation	-	-	-	Location-based malicious node detection	Energy consumption: Up to 12J	Sybil, wormhole, sinkhole attack detection
Zhan et al. 2012 [56]	Real-time implementation	300, 1184	300 * 300 m	Up to 10%	Energy consumption and time to detect malicious node		Sinkhole attack, Sybil attack detection
Jiang et al.2020 [57]	NS2	200	-	-	20 parameters used to detect malicious activity	Accuracy: 0.96	Blackhole and Grayhole attack detection
Ifzarne et al. 2021 [62]	NS2	100	100 * 100m	-	18 independent variables used for malicious detection	Accuracy: 89 – 96%	Blackhole, Grayhole, Flooding node detection
Rao et al. 2021 [63]	NS2	50 to 250	1000 * 1000 m^2	10%	Probability-based detection	PDR: 88 – 92%, false positive: 13-18%,	Blackhole and Selectively packet-dropping node detection
Bisen et al. 2019 [64]	NS2	30 – 50	-	-	Packet forwarding nature-based detection	-	Blackhole attack
Ghugar et al. 2018 [65]	MATLAB	50	-	5-40%	Enhanced watchdog mechanism	-	Blackhole attack
Jamil et al. 2021[66]	Cooja and Contiki OS	11	-	1	Sensors are allowed to overhear parent data transmission	PDR: 88-90%	Sinkhole attack
Babaeer et al. 2020 [67]	OMNET++ and INET-2.0.0	100	-	-	Cryptography-based malicious detection	Delay: 3-5 s, throughput: 56-100 kbps, pdr: 20-92%, energy consumption: 0.4-2J	Sinkhole attack
Almaslukh et al., 2021 [68]	Entity Embedding Model	-	-	-	17 independent parameter	True positive: 0.75 – 0.99	Blackhole, Grayhole and Flooding node detection
Alruhaily et al., 2021 [69]	Python 3.7	-	-	-	19 independent parameters	True positive rate, false positive rate, precision	Blackhole, Grayhole. and Flooding attack detection
Rezvi et al. 2021[70]	Jypyter Notebook	100	-	-	19 independent parameters	True positive rate, false positive rate, precision	Blackhole, grayhole, flooding attack detection
Ashraf et al. 2020 [71]	-	-	-	-	19 independent parameters	Accuracy	Blackhole, Grayhole attack and Flooding attack detection
Nithiyanandam et al. 2019 [72]	-	-	-	-	AI Bee Colony based detection	-	Sinkhole attack detection

Farooq *et al.* [49] introduced an interaction-based malicious node identification method. In that method, a node that observes network traffic through fake routing details and does not involve in other interactions is identified as a malicious node. The same work was enhanced by the authors by adding the necessary cryptography and authentication mechanism for interaction-based malicious detection. Kalkha *et al.* [50] used the hidden markov model to get a short and reliable route against malicious packet-dropping attacks on the network. Lodhi *et al.* [51] analyzed the data packet time buffer to identify the compromised node in the network. Devi *et al.* [52] used various methodologies, such as clustering, data aggregation, and slot scheduling to detect packet drops on the network. Liu *et al.* [53] verified each minimum route reply with the reverse route to avoid fake route replies. Jasmin et al. [54] applied multiple verification methods, such as medium access control and encryption techniques, to prevent sinkhole attacks in WSNs. Zhang et al. [55] applied a geographical-based pairing technique with sensor-to-sensor authentication to detect sinkhole nodes in WSN. Zhan et al. [56] introduced two components, namely energy watcher and trust manager, to identify malicious nodes in WSN. Energy consumption and time synchronization were used to identify misbehavior nodes in WSN. In [63], Rao et al. 2021, applied watchdog based three-layer malicious node detection in WSN. Sensor nodes were divided into different zones, and monitor nodes watched the sensors in the zone. Node behaviors are monitored in order to identify malicious nodes.

Ghugar et al. [65] calculated the trust of the sensor node in WSN. They used the Watchdog methodology to monitor and for trust calculation of sensor nodes. Babaeer et al. [67] applied watermarking and homomorphic encryption to identify the sinkhole attack in WSN. This helped the system to identify malicious nodes before malicious activities. Parameter analysis of miscellaneous detection techniques is shown in Table 1. Various components of malicious detection techniques are shown in Table 1.

6. Discussion and Future Direction

We have reviewed the critical parameters such as energy consumption, overhead routing, computation costs, handling multiple and cooperative attacks, false positive, attack prevention, compatibility and false negative. Most of the abovementioned techniques do not address some of the parameters that could be added in future malicious node detection techniques.

6.1. Energy Consumption

Most of the current detection techniques do not consider energy consumption into account. Only 40% of articles have considered energy consumption in malicious node detection. Ad-hoc networks utilise batteries in most applications, and most detection strategies require more energy due to the additional stages in malicious detection strategy. Therefore, power is an essential component of these networks. Studies should be conducted for the purpose of reducing the amount of energy used in harmful detection, hence increasing the network's lifetime. [73].

6.2. Routing Overhead

Most detection techniques use additional routing messages to detect malicious behavior. Some techniques use network layer control packets, and few use multiple layer control packets for detection. These techniques absorb network bandwidth, which reduces the life of the network. Researchers can do their research using fewer messages in malicious node detection techniques [74].

6.3. Computation Cost

The run time (time complexity) of the detection algorithms is not discussed in some techniques. Detection algorithms should detect malicious nodes within the polynomial time. It should not exceed polynomial runtime. This helps with the efficiency of the network [75].

6.4. Handling Multiple and Cooperative Attacks

As shown in Figure 4, only 3% of techniques provide solutions to cooperative attacks (the attackers work collaboratively), and 30% of articles provide solutions to multiple attacks (more than one type of attack). Techniques should provide solutions in such a way that they can handle more than one attack. Researchers should pool the relevant attacks and provide solutions for more than one attack [29]. Also, the detection technique must provide solutions to cooperative attacks.

6.5. Attack Prevention

Most of the techniques discussed above detect malicious attacks. But researchers can use some of the prediction techniques to identify a malicious node before attackers start to attack. This helps keep the network from attacking. At the very least, the assault needs to be detected promptly, assisting in the reduction of losses caused by malicious attacks [11].

6.6. Compatibility

Detection techniques must be compatible with the use of new methodologies such as machine learning techniques, prediction algorithms, and data analysis methodologies. This helps to enhance malicious detection in a number of areas, such as attack prevention, early detection, multi-attack management and cooperative attacks. Figure 4 shows that only 8% of papers use other technologies to identify infected nodes in the network. Researchers can also expand their methodologies to detect malicious attacks on the Internet of Things (IoT) network [76].

6.7. False Positive and False Negative

False positive (genuine node mistakenly recognized as a harmful node) and False negative (harmful node detected as

a genuine node); these two parameters are unavoidable for malicious node detection. However, in malicious node detection, just 35% and 30% of articles calculated false positives and false negatives. This rate should be increased in the detection of malicious nodes. Most detection techniques do not use these two parameters in malicious node detection. It leads to a false detection rate.

7. Conclusion

MANET, WSN, and DTN ad-hoc networks are utilised in various applications. These networks are subject to a range of assaults because of their operating nature. Among these assaults, packet-dropping attacks such as sinkholes, black holes, and grayhole have a substantial impact on network performance. Existing detection techniques provide solutions for the identification of these attacks. These existing detection techniques have been categorized into seven categories, namely sequence number-based detection, route request/reply-based detection, cross-layer-based detection, bait route request-based detection, acknowledgement-based detection, multi-parameter-based detection and miscellaneous detection. Critical parameters of these detection techniques are studied. The major drawbacks of the existing detection techniques have also been identified. We believe this work will help researchers move in the right direction in the ad hoc network to find malicious nodes.

References

[1] Marcelo G. Rubinstein et al., "A Survey on Wireless Ad Hoc Networks," *IFIP International Conference on Mobile and Wireless Communication Networks*, Springer, Boston, MA, pp. 1-33, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[2] Su Man Nam, and Tae Ho Cho, "A Fuzzy Rule-Based Path Configuration Method for LEAP in Sensor Networks," *Ad Hoc Networks*, vol. 31, pp. 63-79, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[3] J. Sebastian Terence, and Geethanjali Purushothaman, "A Novel Technique to Detect Malicious Packet Dropping Attacks in Wireless Sensor Networks," *Journal of Information Processing Systems*, vol. 15, no. 1, pp. 203-216, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] Annie Mathew, and J. Sebastian Terence, "A Survey on Various Detection Techniques of Sinkhole Attacks in WSN," *International Conference on Communication and Signal Processing, IEEE*, pp. 1115-1119, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[5] Shengchao Su, and Shuguang Zhao, "An Optimal Clustering Mechanism based on Fuzzy-C Means for Wireless Sensor Networks," *Sustainable Computing: Informatics and Systems*, vol. 18, pp. 127-134, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] Reem E. Mohemed et al., "Energy-Efficient Routing Protocols for Solving Energy Hole Problem in Wireless Sensor Networks," *Computer Networks*, vol. 114, pp. 51-66, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[7] Abdelkrim Hadjidj et al., "Wireless Sensor Networks for Rehabilitation Applications: Challenges and Opportunities," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 1-15, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[8] Sanjay Madria, and Jian Yin, "SeRWA: A Secure Routing Protocol against Wormhole Attacks in Sensor Networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1051-1063, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[9] A.B. Karuppiah, and S. Rajaram, "False Misbehavior Elimination of Packet Dropping Attackers during Military Surveillance using WSN," *Advances in Military Technology*, vol. 9, no. 1, pp. 19-30, 2014. [Google Scholar] [Publisher Link]

[10] Abhijeet Salunke, and Dayanand Ambawade, "Dynamic Sequence Number Thresholding Protocol for Detection of Blackhole Attack in Wireless Sensor Network," *International Conference on Communication, Information & Computing Technology*, pp. 1-4, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mohammad Wazid et al., "Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network," *International Conference on Communication and Signal Processing*, pp. 576-581, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[12] Murad A. Rassam et al., "A Sinkhole Attack Detection Scheme in Mintroute Wireless Sensor Networks," *International Symposium on Telecommunication Technologies, IEEE*, pp. 71-75, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[13] Chaitali Biswas Dutta, and Utpal Biswas, "A Novel Blackhole Attack for Multipath AODV and Its Mitigation," *International Conference on Recent Advances and Innovations in Engineering*, pp. 1-6, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[14] Su Man Nam, and Tae Ho Cho, "A Fuzzy Rule-Based Path Configuration Method For LEAP In Sensor Networks," *Ad Hoc Networks*, vol. 31, pp. 63-79, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ranjeeth Kumar Sundararajan, and Umamakeswari Arumugam, "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks," *Journal of Sensors*, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[16] Amol R. Dhakne, and Prashant N. Chatur, "Design of Hierarchical Trust based Intrusion Detection System for Wireless Sensor Network [HTBID]," *International Journal of Applied Engineering and Research*, vol. 12, no. 8, pp. 1772-1778, 2017. [Google Scholar] [Publisher Link]

[17] Rashmi Ranjan Sahoo et al., "Guard against Trust Management Vulnerabilities in Wireless Sensor Network," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7229-7251, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[18] Ju Ren et al., "Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 5, pp. 3718-3731, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[19] Idris Abubakar Umar et al., "FuGeF: A Resource Bound Secure Forwarding Protocol for Wireless Sensor Networks," *Sensors*, vol. 16, no. 6, p. 943, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[20] Idris Abubakar Umar et al., "TruFiX: A Configurable Trust-Based Cross-Layer Protocol for Wireless Sensor Networks," *IEEE Access*, vol. 5, pp. 2550-2562, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[21] Danyang Qin et al., "Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network," *IEEE Access*, vol. 5, pp. 9599-9609, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[22] M.V Sangeetha, and J Bhavithra, "Applying Packet Score Technique in SDN for DDoS Attack Detection," *SSRG International Journal of Computer Science and Engineering*, vol. 5, no. 6, pp. 20-24, 2018. [CrossRef] [Publisher Link]

[23] N. Dharini, Ranjith Balakrishnan, and A. Pravin Renold, "Distributed Detection of Flooding and Gray Hole Attacks in Wireless Sensor Network," *International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials*, pp. 178-184, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[24] Karine Altisen et al., "SR3: Secure Resilient Reputation-Based Routing," *Wireless Networks*, vol. 23, no. 7, pp. 2111-2133, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[25] Weidong Fang et al., "BTRES: Beta-based Trust and Reputation Evaluation System for Wireless Sensor Networks," *Journal of Network and Computer Applications*, vol. 59, pp. 88-94, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[26] Mohammad Wazid, and Ashok Kumar Das, "An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 90, no. 4, pp. 1971-2000, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[27] Tao Yang et al., "A Secure Routing of Wireless Sensor Networks Based on Trust Evaluation Model," *Procedia Computer Science*, vol. 131, pp. 1156-1163, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[28] Na Wang, and Jian Li, "Shortest Path Routing with Risk Control for Compromised Wireless Sensor Networks," *IEEE Access*, vol. 7, pp. 19303-19311, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[29] Sebastian Terence, and Geethanjali Purushothaman, "Behavior based Routing Misbehavior Detection in Wireless Sensor Networks," *KSII Transactions on Internet & Information Systems*, vol. 13, no. 11, pp. 5354-5369, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] Edith C. H. Ngai, Jiangchuan Liu, and Michael R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," *IEEE International Conference on Communications*, Istanbul, Turkey, pp. 3383-3389, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[31] Edith C.H. Ngai, Jiangchuan Liu, and Michael R. Lyu, "An Efficient Intruder Detection Algorithm against Sinkhole Attacks in Wireless Sensor Networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2353-2364, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[32] Ioannis Krontiris et al., "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks," *International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics*, pp. 150-161, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[33] Krontiris Ioannis, Tassos Dimitriou, and Felix C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks," *Proceedings of 13th European Wireless Conference*, 2007. [Google Scholar] [Publisher Link]

[34] Suman Deb Roy et al., "Countering Sinkhole and Black Hole Attacks on Sensor Networks Using Dynamic Trust Management," *IEEE Symposium on Computers and Communications*, pp. 537-542, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[35] Changlong Chen, Min Song, and George Hsieh, "Intrusion Detection of Sinkhole Attacks in Large-Scale Wireless Sensor Networks," *IEEE International Conference on Wireless Communications, Networking and Information Security*, pp. 711-716, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[36] Yenumula Reddy, Jan Durand, and Sanjeev Kafle, "Detection of Packet Dropping in Wireless Sensor Networks," *Seventh International Conference on Information Technology: New Generations*, pp. 879-884, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[37] P. Samundiswary, Padma Priyadarshini, and P. Dananjayan, "Detection of Sinkhole Attacks for Mobile Nodes in Heterogeneous Sensor Networks with Mobile Sinks," *International Journal of Computer and Electrical Engineering*, vol. 2, no. 1, pp. 127-133, 2010. [Google Scholar] [Publisher Link]

[38] Stefan K. Stafrace, and Nick Antonopoulos, "Military Tactics in Agent-Based Sinkhole Attack Detection for Wireless Ad Hoc Networks," *Computer Communications*, vol. 33, no. 5, pp. 619-638, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[39] S. Sharmila, and G. Umamaheswari, "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms," *International Conference on Process Automation, Control and Computing*, pp. 1-6, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[40] D. Sheela, C. Naveen Kumar, and G. Mahadeva, "A Non Cryptographic Method of Sink Hole Attack Detection in Wireless Sensor Networks," *International Conference on Recent Trends in Information Technology*, pp. 527-532, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[41] Satyajayant Misra, Kabi Bhattarai, and Guoliang Xue, "*BAMBI: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks*," *IEEE International Conference on Communications, IEEE*, pp. 1-5, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[42] H. Shafiei et al., "Detection and Mitigation of Sinkhole Attacks in Wireless Sensor Networks," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 644-653, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[43] Sina Hamedheidari, and Reza Rafeh, "A Novel Agent-Based Approach to Detect Sinkhole Attacks in Wireless Sensor Networks," *Computers & Security*, vol. 37, pp. 1-14, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[44] N.K. Sreelaja, and G.A. Vijayalakshmi Pai, "Swarm Intelligence based Approach for Sinkhole Attack Detection in Wireless Sensor Networks," *Applied Soft Computing*, vol. 19, pp. 68-79, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[45] Maryam Motamedi, and Nasser Yazdani, "Detection of Black Hole Attack in Wireless Sensor Network Using UAV," *7th Conference on Information and Knowledge Technology*, pp. 1-5, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[46] Md. Ibrahim Abdullah, Mohammad Muntasir Rahman, and Mukul Chandra Roy, "Detecting Sinkhole Attacks in Wireless Sensor Network Using Hop Count," *International Journal of Computer Network and Information Security*, vol. 3, pp. 50-56, 2015. [Google Scholar] [Publisher Link]

[47] Prachi Dewal, Gagandeep Singh Narula, and Vishal Jain, "Detection and Prevention of Black Hole Attacks in Cluster Based Wireless Sensor Networks," *3rd International Conference on Computing for Sustainable Global Development, IEEE*, pp. 3399-3403, 2016. [Google Scholar] [Publisher Link]

[48] Ghazaleh Jahandoust, and Fatemeh Ghassemi, "An Adaptive Sinkhole Aware Algorithm in Wireless Sensor Networks," *Ad Hoc Networks*, vol. 59, pp. 24-34, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[49] Muhammad Umar Farooq et al., "Energy Preserving Detection Model for Collaborative Black Hole Attacks in Wireless Sensor Networks," *12th International Conference on Mobile Ad-Hoc and Sensor Networks*, pp. 395-399, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[50] Hanane Kalkha, Hassan Satori, and Khalid Satori, "Preventing Black Hole Attack in Wireless Sensor Network Using HMM," *Procedia Computer Science*, vol. 148, pp. 552-561, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[51] Amairullah Khan Lodhi et al., "Performance Improvement in Wireless Sensor Networks by Removing the Packet Drop from the Node Buffer," *Materials Today: Proceedings*, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[52] V. Seedha Devi, T. Ravi, and S. Baghavathi Priya, "Cluster Based Data Aggregation Scheme for Latency and Packet Loss Reduction in WSN," *Computer Communications*, vol. 149, pp. 36-43, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[53] Yuxin Liu et al., "Design and Analysis of Probing Route to Defense Sink-Hole Attacks for Internet of Things Security," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 356-372, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[54] Ahmed Abdulhadi Jasim et al., "Secure and Energy-Efficient Data Aggregation Method based on an Access Control Model," *IEEE Access*, vol. 7, pp. 164327-164343, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[55] Yanchao Zhang et al., "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 247-260, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[56] Guoxing Zhan, Weisong Shi, and Julia Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 184-197, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[57] Shuai Jiang, Juan Zhao, and Xiaolong Xu, "SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments," *IEEE Access*, vol. 8, pp. 169548-169558, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[58] Qi Guo et al., "MP-MID: Multi-Protocol Oriented Middleware-Level Intrusion Detection Method for Wireless Sensor Networks," *Future Generation Computer Systems*, vol. 70, pp. 42-47, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[59] Bo Yu, and Bin Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium*, pp. 8-16, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[60] Alaa Atassi et al., "Malicious Node Detection in Wireless Sensor Networks," *27th International Conference on Advanced Information Networking and Applications Workshops*, pp. 456-461, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[61] Fang-Jiao Zhang et al., "Sinkhole Attack Detection based on Redundancy Mechanism in Wireless Sensor Networks," *Procedia Computer Science*, vol. 31, pp. 711-720, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[62] Samir Ifzarne et al., "Anomaly Detection using Machine Learning Techniques in Wireless Sensor Networks," *Journal of Physics: Conference Series*, vol. 1743, no. 1, p. 012021, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[63] M Venkateswara Rao, and Srinivas Malladi, "Secure Intruder Information Sharing in Wireless Sensor Network for Attack Resilient Routing," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 2, 2021. [Google Scholar] [Publisher Link]

[64] Dhananjay Bisen et al., "Detection and Prevention of Black Hole Attack Using Trusted and Secure Routing in Wireless Sensor Network," *International Conference on Hybrid Intelligent Systems*, Springer, Cham, pp. 299-308, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[65] Umashankar Ghugar, and Jayaram Pradhan, "NL-IDS: Trust Based Intrusion Detection System for Network layer in Wireless Sensor Networks," *Fifth International Conference on Parallel, Distributed and Grid Computing, IEEE*, pp. 512-516, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[66] Ansar Jamil, Mohammed Qassim Ali, and Muhammed E. Abd Alkhalec, "Sinkhole Attack Detection and Avoidance Mechanism for RPL in Wireless Sensor Networks," *Annals of Emerging Technologies in Computing*, vol. 5, no. 5, pp. 94-101, 2021. [Google Scholar] [Publisher Link]

[67] Huda A. Babaeer, and Saad A. Al-Ahmadi, "Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network based on Homomorphic Encryption and Watermarking," *IEEE Access*, vol. 8, pp. 92098-92109, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[68] Bandar Almaslukh, "Deep Learning and Entity Embedding-Based Intrusion Detection Model for Wireless Sensor Networks," CMC *Computers, Materials & Continua*, vol. 69, pp. 1343-1360, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[69] Nada M. Alruhaily, and Dina M. Ibrahim, "A Multi-Layer Machine Learning-Based Intrusion Detection System for Wireless Sensor Networks," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[70] Md Alauddin Rezvi et al., "Data Mining Approach to Analyzing Intrusion Detection of Wireless Sensor Network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 516-523, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[71] Shahzad Ashraf, and Tauqeer Ahmed, "Sagacious Intrusion Detection Strategy in Sensor Network," *International Conference on UK-China Emerging Technologies*, *IEEE*, pp. 1-4, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[72] N. Nithiyanandam, and P. Latha, "Artificial Bee Colony Based Sinkhole Detection in Wireless Sensor Networks," *Journal of Ambient Intelligence and Humanized Computing*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[73] Antonio Moschitta, and Igor Neri, "Power Consumption Assessment in Wireless Sensor Networks," *ICT-Energy-Concepts towards Zero-Power Information and Communication Technology*, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[74] Amit Sarkar, and T. Senthil Murugan, "Routing Protocols for Wireless Sensor Networks: What the Literature Says?," *Alexandria Engineering Journal*, vol. 55, no. 4, pp. 3173-3183, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[75] Rodrigues, L.M., Montez, C., Budke, G., Vasques, F. and Portugal, P., 2017. "Estimating the Lifetime of Wireless Sensor Network Nodes through the Use of Embedded Analytical Battery Models," *Journal of Sensor and Actuator Networks*, vol. 6, no. 2, p. 8, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[76] Kuan Zhang et al., "Sybil Attacks and their Defenses in the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372-383, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[77] George W. Kibirige, and Camilius Sanga, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network," *Arxiv Preprint arXiv:1505.01941*, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[78] Bindu Rani, and Harkesh Sehrawat, "Blackhole Attack Detection and Prevention in Wireless Sensor Networks: A Study," *Journal of Emerging Technologies and Innovative Research*, vol. 5, no. 3, 2018. [Publisher Link]

[79] D. Amulya, and C.N. Chinnaswamy, "Survey on Mechanisms to Detect and Mitigate the Impact of Sinkhole Attack in Wireless Sensor Networks," *International Journal for Advance Research and Development*, vol. 2, no. 2, 2017. [Google Scholar] [Publisher Link]

[80] Vinay Singh, Ajit Singh, and Malik Mubasher Hassan, "Survey: Black Hole Attack Detection in MANET," *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[81] Zainab Alansari et al., "A Systematic Review of Routing Attacks Detection in Wireless Sensor Networks," *PeerJ Computer Science*, vol. 8, p. e1135, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[82] Umashankar Ghugar et al., "LB-IDS: Securing Wireless Sensor Network using Protocol Layer Trust-Based Intrusion Detection System," *Journal of Computer Networks and Communications*, 2019. [CrossRef] [Google Scholar] [Publisher Link]