Wireless Personal Communications (2019) 106:2291–2313
https://doi.org/10.1007/s11277-018-6040-7

Sinkhole Attacks in Wireless Sensor Networks: A Survey

Aqeel-ur Rehman[1] · **Sadiq Ur Rehman**[1] · **Haris Raheem**[1]

Published online: 24 October 2018

Abstract
Wireless sensor networks (WSNs) consist of a large number of nodes, communicating sensor readings to the base stations through other nodes. Due to their energy limitations and positioning in hostile environments, WSNs are vulnerable to various routing attacks. From a security point of view in WSN, data authenticity, confidentiality, Integrity, and availability are the important security goals. It is in common practice that a security protocol used to be created by focusing a particular attack in WSN. Most renowned attacks in WSN are Sybil attack, Denial of Service attack, wormhole attack, selective attack, HELLO Flooding attack, Sinkhole attack etc. This survey focuses on one of the most challenging routing attacks, called Sinkhole attack. A Sinkhole attack is one of the sternest routing attacks because it attracts surrounding nodes with misleading routing path information and performs data forging or selective forwarding of data passing through it. It can cause an energy drain on surrounding nodes resulting in energy holes in WSNs and it can cause inappropriate and potentially dangerous responses based on false measurements. Researchers had presented several ways to detect and identify sinkhole attacks. This survey reviews related work on Sinkhole attack detection, prevention strategies, and attack techniques and also highlights open challenges in dealing with such attacks. Among many discussed techniques, fuzzy logic-based systems are considered to be good in performance in intruder detection system (IDS).

Keywords Wireless Sensor Network · WSN · Sinkhole attacks · Routing attacks · Intruder detection

✉ Aqeel-ur Rehman
aqeel.rehman@hamdard.edu

Sadiq Ur Rehman
sadiq.rehman@hamdard.edu.pk

Haris Raheem
haris_raheem@hotmail.com

[1] Department of Computing, Faculty of Engineering Science and Technology, Hamdard University, Hakim Mohammad Said Road, Karachi, Pakistan

1 Introduction

Wireless Sensor Networks (WSN) are composed of a large number of tiny sensor nodes each capable of monitoring some phenomenon, having data processing and communication capabilities [1]. These nodes form an Adhoc network in which nodes communicate in short ranges, relying on neighboring nodes to relay data to base station/sink nodes. Wireless sensor networks are usually installed and configured in an environment where it is not easy to access sensors physically e.g. battlefields, border conflict zones, animal tracking etc. Such an Adhoc communication network is highly vulnerable but is unable to counter an adversary's attempt to accommodate the network. For the operation of a system, data confidentiality and integrity is very crucial. Limited resources, on the other hand, are also the most challenging factor in WSN. Reliability, energy efficiency and availability are the three key parameters required in WSNs, details can be seen in [2]. For secure operation, security requirements of WSN [3] must be kept in mind. With the modern research, there has been a significant progress in WSN's security mechanisms which includes secure aggregation [4], key establishment [5], or localization security [6] etc. Moreover, limited resources, a pattern of communication, false alarm and detection rate are the most important challenges of WSNs.

It is common practice that the security protocols are normally designed for particular attacks in WSN like the sinkhole [7], wormhole [8], selective attack [9] etc. In this paper, the focal point will be sinkhole attacks, which occurs in the network layer. Sinkhole attack is considered to be the most dangerous attack in WSN as in this attack compromised node wants to attract most of the traffic from a specific area by advertising its false routing metric. Sinkhole attack can also be used to launch other attacks and send false information to the base station [10].

Many solutions are now available to detect and identify the sinkhole attack from different researchers [11–23] etc. Their work detail regarding sinkhole detection can be found in Table 2 that has been extracted from [24]. The latest research work in the area of sinkhole attack can be found in [23], in which researcher has proposed an adaptive sinkhole aware algorithm in WSN which provides better computational results. In [25], the researcher has proposed the method to monitor traffic flow and its features. With the help of this method, performance improvement of the network can be achieved.

The following paper is divided into the eight parts, at first, there will be an introduction. Section 2 is related to the background of WSN. Discussion on sinkhole attack techniques for WSN protocols is in Sect. 3 and detection of sinkhole attacks will be in Sect. 4, discussion regarding countermeasures will be in Sect. 5. Open challenges in a detection of sinkhole attacks in WSNs are covered in Sects. 6, 7 is regarding performance analyzing parameters and survey's conclusion along with the future work will be in Sect. 8.

2 Background

In real-world deployment scenarios [26], there can be various types of anomalies in the WSN that can affect their functionality. It could be possible that the node may or may not be to provide connectivity whenever coverage hole, black hole, wormhole or routing holes exist in the topology so the WSN will fail to achieve its objectives. Most of the time adversaries that usually compromise the network, deliberately create these anomalies. These

adversaries replicate the legitimate nodes using, captured node IDs and cryptographic material which in result cause the jamming of communication by forming the jamming holes.

Below is a brief introduction of different holes present in WSNs.

2.1 Coverage Holes

A coverage hole [27, 28] consists of an area in a network where sufficient nodes are not available to provide the needed amount of coverage for the specific application.

2.2 Jamming Holes

A jamming hole [29, 30] occurs if an adversary targeted area which is equipped with the capability of jamming the radio frequency that is going to be used for sensor node communication.

2.3 Routing Holes

In WSN, routing holes [31–33] consists of a region in which there is either the node of absence or the present node is somehow unable to play any role in the routing of the message. These holes are created due to the failure of sensor nodes including malfunctioning, battery depletion or a malicious attack.

2.4 Black/Sink Holes or Worm Holes

If the data get missed in between the traffic, the creation of a black hole [7, 30, 34] took place. It is one of the types of Denial of Service (DoS) attack [35]. The reception or transmission of data is unknown at both the end (transmitting side and receiving side). In wormholes [8, 30], malicious nodes establish a tunnel in between each other and start the sending or receiving of packets by creating an individual channel for radio communication

3 Sinkhole Attack Techniques for WSN Protocols

WSN routing protocols are highly vulnerable to sinkhole attacks. Adversaries try to manipulate traffic flows, network latency, and other factors with a goal to disable the network to the maximum extent. In this section, we will review the most popular WSN routing protocols and the techniques adversaries use to launch a sinkhole attack on them.

3.1 Directed Diffusion

It is a data-centric routing algorithm for fetching specific knowledge from a sensor network [26]. It is the responsibility of base stations to send requests for specific data elements, nodes that are having the capability to satisfy the queries will send the information from a reverse path. If there is a situation when multiple nodes from the surrounding send the same query to a node, then the node may propagate events along the corresponding

multiple links. A powerful adversary is a reason that can create a wormhole in-between node "A" and "B" located adjacent to the base station and to source nodes respectively. A wormhole is responsible for carrying the queries from a base station and node B replays them. Broadcasting of spoofed strong positive and negative reinforcements to all surrounding node is done by node "B" and node "A" respectively (Fig. 1).

3.2 TinyOS Beaconing

A beaconing protocol named the TinyOS [30, 36] works by constructing a breadth-first spanning tree with a base station at the root. The base station regularly broadcasts route updates. On receiving the updates, the base station is sported as a parent by the node and broadcast the renewed message to their neighbors. Neighbor nodes mark this node as its parent and this process continues recursively. The drawback with this approach is that it provides the ability to other nodes to count themselves as a base station and attract network's traffic because routing updates are not authenticated. Although authentication will not allow an adversary to count itself as a base station, however an adversary with the powerful transmitter can still easily destroy the network.

To launch the attack first, the adversary used to grab two nodes, among which one is near the area to be a target and the second one is near the base. Then a wormhole is to be created in between these two nodes and authenticated routing updates are forwarded through this wormhole. These updates will quickly reach the targeted area and allow the adversary to attract a big routing sub-tree in the targeted area. It will enable the adversary to create a sinkhole as the entire traffic from the targeted area is not routed through it (Fig. 2).

3.3 Minimum Cost Forwarding

It is a distributed shortest-paths algorithm [30, 36] in which nodes to sustain certain path information is not required, however, requires every node to maintain the minimum cost to reach the base station. This cost can be based on metrics like hop count, losses, energy used, latency and much more. Nodes start with cost one while Base station has cost zero. Base station advertises its cost that is propagated on the entire network. All the nodes

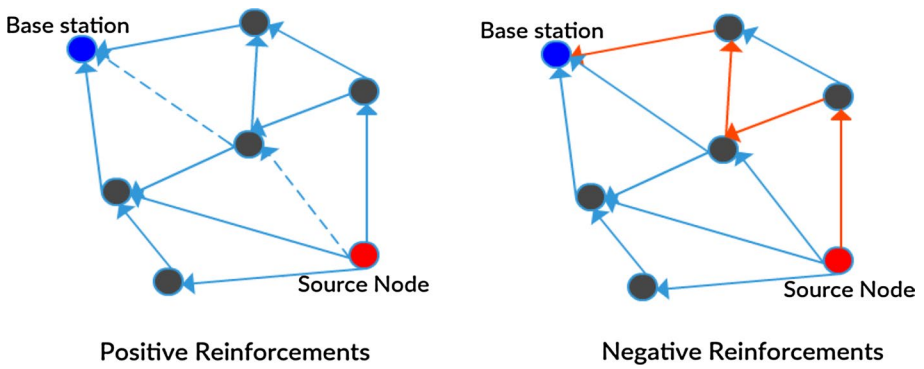

Fig. 1 Directed diffusion sinkhole model

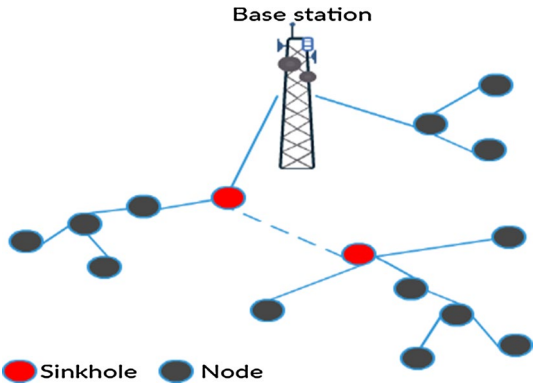

Fig. 2 TinyOS beaconing Sinkhole model

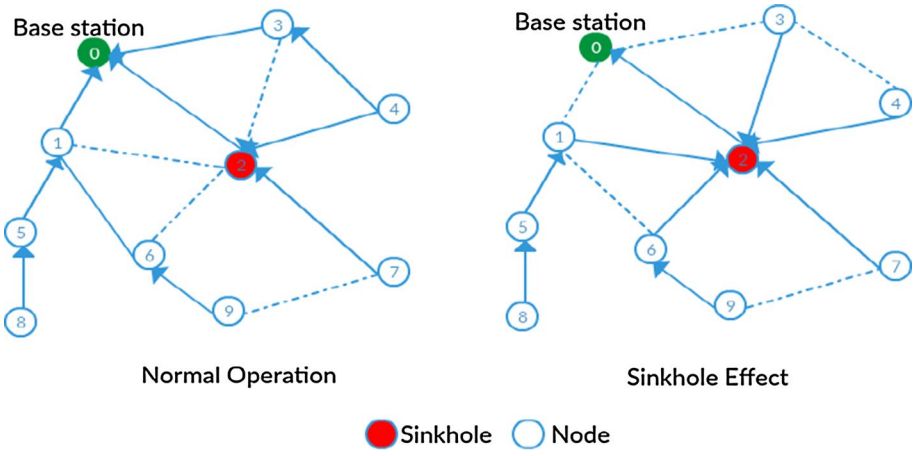

Fig. 3 Minimum cost forwarding sinkhole model

receiving this message update their cost and immediately send out a new advertisement with their updated cost (Fig. 3).

3.4 Leach

LEACH [30, 36] uses a clustering approach to smoothly route queries and sensor data in the network. It is based on assumption that every node is capable of reaching the base station directly using high-power transmissions. LEACH organizes nodes into clusters and each cluster has a cluster-head. Each node sends sensor data to their cluster-head only; cluster-head is responsible for the aggregation and compression of this data coming from all the child nodes and then send this data to the base station. Since cluster heads perform more computation and communication, they face the problem of a rapid decrease in energy. To overcome this problem of energy loss, evenly distribution of energy consumption on every node of a network is performed by selecting a cluster head on a randomized rotation basis.

Since cluster-head selection is depended on the strength of the received signal. A powerful adversary can paralyze the network by sending a powerful advertisement to an entire network. Based on the advertisement's signal strength, all nodes will select the adversary, consider it as a cluster head that results in the creation of a sinkhole, dropping all data transmissions it receives, and effectively disable the rest of the network (Fig. 4).

3.5 MintRoute

MintRoute constructs a routing tree towards the base station using link quality estimates as the routing cost metric [36]. Each node maintains a table (of neighbor ids and link cost) which is updated on receiving the latest packet. Selection of neighbor as a parent from a table depends on the quality of a link. Changing of the parent is only possible on two mechanisms, first, if the quality of more than one node become 75% better than the selected parent. Second, if the link quality of the selected parent drops below the threshold level.

To launch the attack an adversary will try to trigger parent changing mechanism on its neighbors so that they select the sinkhole node as their new parent. To trigger this parent changing mechanism an adversary will advertise an attractive link quality for itself or make other nodes look like they have dropped their link quality.

Since the protocol doesn't allow triggering of parent changing mechanism very often so the attacker is unable to launch a sinkhole attack by simply advertising a lower hop count to the base station and advertising a high link quality. It has to make the current parents look like having poor link quality by spoofing link quality estimates within route update packets (Fig. 5).

4 Approaches for Sinkhole Attack Detection

Sinkhole detection in WSN requires a mechanism to constantly monitor the network behavior at different layers. These mechanisms analyze the traffic patterns to detect malicious activities. Majority of the work has been done by considering two types of such mechanism. A mechanism known as signature-based is the one where a log is maintained for different security attacks in a database, this mechanism helps in providing the necessary

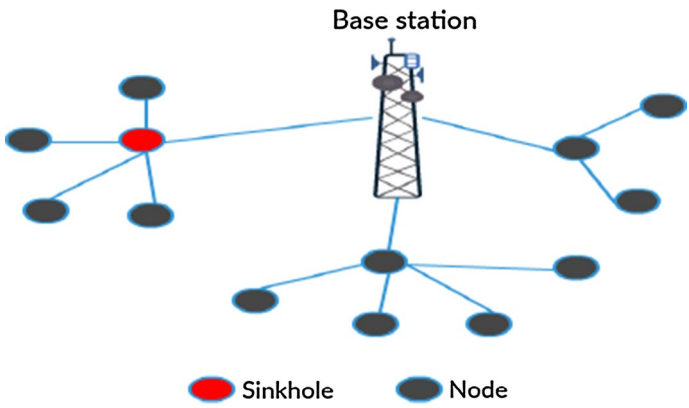

Fig. 4 LEACH sinkhole model

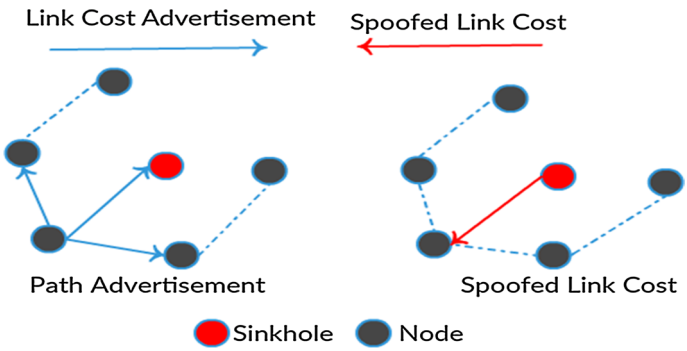

Fig. 5 MintRoute Sinkhole model

security against well-known attacks but will face difficulties (due to the absence of signatures in a database) whenever new attacks are to be detected. The other type is anomaly-based; this mechanism is best suited for the detection of previously unknown attacks. The problem with this type of mechanism is that it sometimes misses the known security attack (as the database is not maintained). These mechanisms can operate in many modes i.e. standalone, distributed, cluster or a combination of these modes.

Table 1 provides a comparison of some of the approaches based on either the signature-based or anomaly-based mechanism. Table 2 provides the latest approaches which are sorted year-wise and may include the signature-based, anomaly-based mechanism or an entirely new mechanism.

The brief introduction of each approach that is present in Table 1 can be found below.

4.1 Distributed and Collaborative Agents

This approach [12, 13], [37] follows a distributed architecture where all individual nodes run an identical IDS client in the network. Each IDS client constantly listens and examines individual packets being routed in its neighborhood. It analyses patterns from this data and matches with a signature database to detect attacks, i.e. deviations from normal behavior.

4.2 Cooperative Clustering

This is a decentralized, cooperative intrusion detection approach [14, 38] where a network is organized as a dynamic hierarchy. Nodes actively listen to packets being forwarded and detect anomalies based on behavior. Anomaly detection data is incrementally aggregated, reduced, and analyzed at each step as it flows upward towards the root. Threat detection directives flow downward from the root towards the nodes. In [20], using the concept of cooperative clustering, Intrusion detection system with the capability of protecting critical information from attacks directs from its WSN is present.

4.3 Statistical Detection

Statistical detection is based on a statistical analysis of traffic transmission patterns [39]. Statistical analysis is resource intensive so it is most suitable for cooperative cluster

Table 1 Comparison of signature-based and anomaly-based sinkhole detection techniques

Classification	System	Algorithm	Characteristics	Distributed	Intensive computation
Signature-based	Distributed and collaborative agents	Behaviour analysis [37]	IDS agents at nodes, scalable, moderate computation requirements	Yes	No
		LEACH [12]	IDS agent compute intrusion ration, IDS alter the system to stop transmission when sinkhole attack is detected	Yes	No
		Geostatistical [13]	Geostatistical sampling for sinkhole detection, mitigation scheme to overcome the problem of traffic flow in the direction of sinkholes	Yes	No
Signature-based	Cooperative clustering	Behaviour analysis [18]	IDS agents at cluster heads, scalable, low computation requirements	Yes	No
		Message digest [14]	An algorithm is robust, work only when digest from the trusted path and node are different	Yes	No
		Critical infrastructures (Cis) [20]	Hybrid approach for the detection of a malicious node	Yes	No
Anomaly-based	Statistical detection	Bayesian classification [39]	IDS engine at the sink node, centralized, high computation requirements	No	Yes
		Girshick-RubinShyriaev [16]	CPU usage was monitored at each node, its difference is calculated and compared with a threshold value to identify the malicious node which was calculated in a short time	Yes	No
		Adaptive sinkhole aware [23]	Algorithm for the calculation and decision of a reliable/safe path	Yes	No
		AODV routing protocol [11]	The hybrid system used to monitor network performance by using destination sequence number and one hop neighbor	No	Yes
		LQI based routing [18]	Simplifies AODV routing protocol with the help of LQI (Link Quality Indicator)	No	Yes
Anomaly-based	Genetic algorithm	Genetic programming [40]	IDS engine at the sink node, centralized, moderate to high computation requirements based on genetic expressions	No	Yes

Table 1 (continued)

Classification	System	Algorithm	Characteristics	Distributed	Intensive computation
Anomaly-based	Zone-based system	Markov chain [41]	IDS agents at nodes, hierarchical decision making, moderate computation requirements at gateway nodes	Yes	No
		Cryptographic [17]	Suggested two RESIST protocols that are to be used to increase resilience to sinkhole attack in WSN	Yes	No
Signature-based	Emotional ants system	Ant Colony [42]	Monitoring agents at each node, path rating based decision making, moderate network overhead	Yes	No
Signature-based	Game theory	Two player signalling game [43]	IDS agents at nodes, scalable, low computation requirements	Yes	No
Signature-based	Misbehavior detection	Traffic behaviour analysis [44]	Watchdogs at nodes, scalable, low power consumption, moderate network overhead	Yes	No
Signature-based	Fuzzy based	Fuzzy logic [21, 45]	Distributed or centralized, scalable, low to high computation requirements based on classifiers used	Yes	No
			The proposed system is used for the detection of sinkhole attacks when using Mintroute wireless sensors network	Yes	No
Anomaly-based	Fuzzy Rule-based	Unsupervised fuzzy ART [46]	IDS agents at each node, scalable, low computation requirements	Yes	No
		Agent navigation and data routing [15]	Two algorithms were used in the proposed approach, things related to a mobile agent like information to node and visiting node is given by navigation algorithm. To route data packets, how the node uses global information is the responsibility of data routing. High overhead if nodes get increased	No	Yes
		Network deployment and maintenance [22]	3 steps negotiations, in term of memory overhead, energy utilization and cryptography, this approach is very effective	No	Yes

Table 2 Extracted and Extended work on sinkhole detection [24]

Year	Approach	Suggested by	Suggested solution	Outcomes
2017	Probabilistic	Jahandoust and Ghassemi [23]	An adaptive sinkhole aware algorithm for the calculation and decision of a reliable/safe path	To detect the sinkhole attacks, the subjective logic model was used as an adaptive engine The proposed algorithm has the property to stay robust to confuse detection mechanism
2016	Statistical	Gupta et al. [11]	Use of Advance secure AODV routing protocol	Better efficiency for malicious node detection Better throughput and packet delivery ratio
2015	Intrusion Detection System (IDS),	Sundararajan and Arumugam. [12]	The mechanism for the detection of intruder present in the network that uses LEACH protocol for its routing protocol	2% less energy compared to MS-LEACH Energy efficient method 52% more network lifetime as compare to MS-LEACH Increases the network throughput by 15% more than MS-LEACH
2014	Geostatistical sampling and Distributed monitoring	Shafei et al. [13]	Estimation of energy holes with the help of Geostatistical sampling	For the detection of the sinkhole in all regions, Geostatistical sampling approach was utilized A scheme named as mitigation scheme was used to overcome the problem of traffic flow in the direction of sinkholes
2013	Agent-based	Hamedheidari et al. [22]	The suggested approach is used to prevent sinkhole attack in a network of mobile nodes	3 steps negotiations in between neighbor nodes, validation of agent on the valid node, on adversary node and fake agent on the valid node Work has been evaluated based on the parameters of energy, packet loss, throughput and agent's overhead In term of memory overhead, energy utilization and cryptography, this approach is very effective

Table 2 (continued)

Year	Approach	Suggested by	Suggested solution	Outcomes
2012	Fuzzy Rule-based	Rassam et al. [21]	The mechanism for the detection of sinkhole attacks in the mint route-based WSN	The testbed was developed in TinyOS environment The proposed scheme is very efficient to detect sinkhole attacks for small-scale WSNs The scheme can also be used to monitor the detection ability of large-scale multi-hop WSN
2011	Data Mining	Vuppala et al. [39]	Identification of sinkhole attacks and flooding attacks are identified by using the scheme of hierarchical data clustering in MANET	Anomaly detection was performed by using the data mining technique Network packets were observed in order to trace sinkhole of flooding attacks
	Anomaly-based	Sharmila and Umamaheswari [14]	The suggested algorithm of a message digest for the sink node detection	Excellent working on the algorithm in case, when malicious nodes are under 50% Achievement of the algorithm can be seen in term of data authenticity and integrity Usual value of false -ve error was 10%
	A non-cryptographic	Sheela et al. [15]	Present the strategy in which mobile agents were used for the protection against attacks	There is an inverse relationship in between the probability of sinkhole and the number of nodes The issue with this strategy is large network overheads

Table 2 (continued)

Year	Approach	Suggested by	Suggested solution	Outcomes
2010	Statistical	Chen et al. [16]	Algorithm for the sinkhole attack detection and intruder identification	The relation between the detection time and threshold level is directly proportional and is inversely proportional to the false +ve rate No result on network overhead
	Hybrid	Coppolino et al. [20]	Intrusion detection system with the capability of protecting critical information from attacks directs from its WSN	When the sensor packet was altered by the malicious node, the detection rate was 95–97% If the received and control packet was altered by the malicious node, the detection rate was 93–96% 3% +ve false rate
2009	Key management	Papadimitriou et al. [17]	Suggested two RESIST protocols that are to be used to increase resilience to sinkhole attack in WSN	Two RESIST protocols Resist-0 and RESIST-1 Resist-0 is high resilience to sinkhole attacks as compared to RESIST-1 The impact from collusion node will only be on RESIST-0
	Anomaly-based	Choi et al. [18]	Approach for the detection of sinkhole attack by using link quality indicator (LQI)	The relation between the detection node and detection rate is directly proportional The false +ve rate depends on the extent of the tolerance value No mobility for any sensor node

Table 2 (continued)

Year	Approach	Suggested by	Suggested solution	Outcomes
2008	Rule-Based	Krontiris et al. [19]	Rules for the indication of an existing attack to the legitimate node	Vulnerabilities of Multi-hop LQI can be exploited by sinkhole node Suggested rules were unable to provide any sinkhole node ID. However, these rules make the protocol more resilient
	Fuzzy Rule-based	Li and Parker [46]	The mechanism for the getting higher accuracy in intruder detection with the use of the mobile robot and wireless sensor network	Claimed as a first system to detect intruders by using a sensor network and with the help of a robot, a location can be reached where an intruder was detected Fuzzy art system was modified to detect changes rapidly
2007	Cooperating agents	Krontiris et al. [37]	To detect the effective node, use distributed computing and inter-agent communication	Alarms were being generated according to the particular identified attack signature MintRoute routing protocols were used in TinyOS and specifications were built to work on IDS system for the effective sinkhole detection
	Genetic Programming	Abraham et al. [40]	A program named as Intrusion Detection Program was created to identify and sense know attack patterns	Genetic Algorithm is more effective as compare to any other machine learning mechanism In real-time intrusion detection, this programming gives around 99.7% accurate detection rate
2006	Game Theory	Patcha and Park [43]	Analyzation of intrusion detection was performed by using the model of game-theoretic in the network of mobile ad-hoc system	Interaction has been performed in between attackers and an individual node The designed model has been claimed as a more realistic model as compare to all previous approaches

Table 2 (continued)

Year	Approach	Suggested by	Suggested solution	Outcomes
2005	Clustering techniques	Sterne et al. [38]	An architecture model was designed based on distributed intrusion detection which detects the MANET specific attacks	An architecture model was a dynamic hierarchy, leaves are responsible for data detection At the top, security directive flow from nodes. Reconfiguration of the hierarchy is performed automatically to maintain communication efficiency
	Emotional ants	Banerjee et al. [42]	A mechanism that can keep the path record of intruder trials	A mechanism can work in combination with a machine-based technique for the protection of sensor networks. system use probability values to perceive behavioral patterns.
	Fuzzy Rule-based	Mukkamala et al [45]	Intrusion detection using Ensemble approach for better accuracy	Ensemble approach of Artificial Neural Networks, Support Vector Machines and Multivariate Adaptive Regression Splines was considered Support Vector Machines is better than other two approaches in term of scalability In term of accuracy, Artificial Neural Network is better than the other two approaches
2003	Markov Chain	Sun et al [41]	The non-overlapping system named as Zone-Based Intrusion Detection System	Protection regarding MANET routing protocols were focused, collaboration was performed in between system agents and gateway nodes algorithm Occurred attacks were informed by means of alerts.
2000	Dynamic Source Routing	Marti et al [44]	Mechanism to improve throughput	By using the two approaches (watchdog) and (pathrater), throughput increase by 17% with the presence of about 40% of misbehaving nodes when there was an increment of around 8% overhead transmission

schemes. Agents at each node collect the network traffic information and share with the base station that performs statistical analysis using an algorithm known as intrusion detection and is based on Bayesian classification criteria. In [16], the same concept of the system was implemented by using Girshick-RubinShyriaev method to detect sinkhole attacks. Moreover, in [23], Ghazaleh Jahandoust and Fatemeh Ghassem preset the adaptive sinkhole aware algorithm for the calculation and decision of a reliable/safe path which uses the key concept of statistical detection.

An approach used in [11] can be used for the detection of sinkhole attack on compromised nodes. Data has been transmitted by using the different sensor in a network, a reactive routing protocol has been used in this approach. Transmitted data contain the information regarding the source, destination ID, hop count number and the destination sequence number. The approach in [11] provides a better packet delivery ratio, better efficiency in the detection of sinkhole nodes and better throughput. In [18], this approach has been simplified by using LQI (Link Quality Indicator).

4.4 Genetic Algorithm

Genetic programming (GP) techniques [40] are the core concepts of genetic algorithm and it is capable of detecting known attacks. However, genetic algorithms are resource intensive and not suitable for distributed decentralized network schemes.

4.5 Zone-Based System

In this approach [41], the division of network is into the non-overlapping zones. For inter-zone communication, there are Gateway zones that are physically connected to the nodes in different zones. Each node runs an IDS agent which uses a Markov Chain based anomaly detection algorithm. They monitor messages being routed in the neighborhood and generate alerts (indicate possible attacks) locally and then broadcast inside the zone. Gateway zones perform aggregation and correlation of these alerts and generate network-wide alarms.

4.6 Emotional Ants System

This approach [42] uses an ant colony theory-based intrusion detection algorithm. The key concept of this algorithm is to detect the path with the minimum activity of sensor network which is affected by the intrusion. Agents keep track of whether or not the path has already been visited and each visit to a path has the effect of making it less and less attractive for other agents so they are encouraged to search for paths not yet visited. Agents propagate path status updates across networks to update the nodes on best available paths and to avoid any potentially compromised paths.

4.7 Game Theory

Game theory [43] is a technique that uses a game theory-based algorithm to analyze anomalies in the network. In this technique, an interaction between two players (i.e. attacker and host-based IDS) took place. Cooperative game and non-cooperative games are the two main categories of game types which are used to address security issues of WSNs. In the

intrusion game, the primary task of the attacker will be to dispatch the infected message from a random node with the objective of striking the target node. Once the infected message reached the targeted machine without being encounter by the host IDS, the intrusion is supposed to be successful.

4.8 Misbehavior Detection

In this approach [44], nodes are classified based on their dynamically measured behavior. Watchdogs are used to not only determine the misbehaving nodes but also the path evaluating system which supports the routing protocols to bypass these nodes.

When the forwarding of packets takes place from a node, it is the responsibility of node's watchdog to check the next node (which is in the path) having the capability of packet forwarding. If the node is unable to forward the packets, it will count as a misbehaving. Path evaluating system will record this information (of misbehaving nodes) and select the network path in which the delivery of packets is possible.

4.9 Fuzzy Rule

In this approach [45], Nodes run an intelligent agent, based on neural networks, approximate reasoning, fuzzy inference system and derivative-free optimization. Detection accuracy is based on the combination of different classifiers (as one classifier is unable to give the authentic result for all attacks) used for different attacks.

This approach guarantees a 100% detection rate if all 42 classifiers are used but it becomes computationally intensive. To make it adaptable to WSN 12 classifiers are proposed with a compromise on accuracy which drops to 94%. In [21], the proposed scheme was based on the fuzzy rule-based system for the detection of the sinkhole was performed on Mintroute wireless sensor network.

In [46], an approach that is based on unsupervised fuzzy ART (Adaptive Resonance Theory) neural network to gain the knowledge and detect the already unknown attacks was introduced. Continuously learning from new events, performing pattern classification and dimensionality reduction can be achieved by the unsupervised Artificial Neural Network (ANN). The intelligent mobile robot approach [46] uses the Markov model to learn and detect changes that are time-related and were not supported in the original fuzzy ART neural network approach. This algorithm is straightforward, lightweight and easily applicable for low-cost sensor nodes. In this approach, the network is organized in a hierarchical structure where each node runs an identical agent. The nodes are initially trained on a specific environment model. After deployment, if there is any change compared to the original model then they will be considered an attack or an anomaly which generates an alert. On receiving an alert an autonomous mobile robot responds to the alert and moves towards the region to respond to a threat.

This approach has also been used in [15] where Agent navigation and data routing algorithm was used for sinkhole attacks detection.

In [22], the Suggested approach is used to prevent sinkhole attack in a network of mobile nodes using the same concept of an Intelligent mobile robot.

Table 2 provides the latest approaches which are sorted year-wise and may include the signature-based, anomaly-based mechanism or an entirely new mechanism. This table has been extracted from [24] and extended accordingly.

5 Countermeasure for Sinkhole Attacks

There are several methods to encounter and avoid sinkhole attacks, which includes approaches like network flow information and data consistency, scheme of monitoring hop count, scheme based on Received Signal Strength Indicator (RSSI), monitoring node's CPU usage, approach based on Mobile Agent, Message Digest Algorithm etc. details regarding the above mention approaches can be found in [47]. Some other most popular approaches are discussed in detail below that provides defense and avoidance against the sinkholes.

5.1 Authorization

Authorization [48, 49, 51], is one of the best defenses against sinkhole attacks. It allows only authorized nodes to exchange routing information [48]. For this purpose, public-key encryption infrastructure may be used to sign and verify routing updates. A centralized certification authority will be a single point of failures so mechanisms are proposed to distribute the certification function among multiple servers.

5.2 Probing

The approach [50, 51] is to periodically send probes across the network's diameter. Probes must look like normal traffic otherwise malicious nodes will identify it and always route them correctly and make probing ineffective. A probing node can identify blackout regions and then the network can take measures to overcome it.

5.3 Redundancy

Redundancy [52] can play important role in reducing the chances of messages being dropped by a malicious node. In this approach, nodes send duplicate messages along the same path. Each message uses a different path so that one of them may bypass adversaries or sinkholes.

5.4 Limited Broadcast Using One-Way Hash Chains

In this scheme [36, 53], base stations are only responsible for launching flooding of the network, e.g. setting up routing information. All broadcast packets are stamped with the base station with a one-way hash chain (OHC) number. These numbers keep changing with each broadcast and they are not easy to predict so it will be hard for intruders to predict the next number in OHC.

5.5 Limited Routing Updates

In [53], the base station is only authorized to update a node's routing tables. A secret pairwise key is shared in-between sensors of each node and the base station. Encryption of routing updated messages with the secret key is done by the base station which then sends this message to each node separately. Nodes only update their routing table if the routing

update can be decrypted by their key. Sinkhole attacks depend on spoofing the routing information updates to attract traffic towards them but this scheme will not allow the attacker to access routing information which will limit the effects of compromised nodes to a minimum access for base stations.

5.6 Multi-path, Multi-base Station Routing

In [53, 54], For WSN, an essential thing is to have a successful delivery of the packet to the base station (BS) rather than prevention of data captured by an adversary. The objective of this scheme is to have a successful packet's delivery to the base station even with the existence of sinkhole nodes by the placement of multiple BS and use of multiple paths to each BS for each sensor node.

6 Challenges in the Detection of Sinkhole Attacks in WSNs

By reviewing several research papers/blogs regarding sinkhole, attack in WSNs, listing down some of the main challenges present in the detection of sinkhole attack in WSNs.

6.1 Pattern of Communication

Since in WSNs, a base station is the one to whom all the messages are destined for sensor nodes causing the sinkhole to propel an attack. The generation of a sinkhole attack occurs when a compromised node sends the forged information to all the other nodes present in a network with the objective to attract the bulk amount of traffic. Depending on the communication pattern, the burglar will only negotiate with the node that is closer to the base station. Based on this behavior of communication pattern, an opportunity is provided for that attack.

6.2 Physical Attack

In a wireless sensor network, the deployment environment is an unfriendly environment that is most the time left open for other to get access. This causes a freedom for an intruder to attack a node and get all the access to the important information [55].

6.3 Packet Delivery Ratio and Message Drop

In WSNs, when the data is considered to be traveled through various nodes, the chances of getting message dropped due to any reason are highly possible. Packets delivery ratio is the key parameter to analyze the performance of the network.

6.4 False Alarm and Detection Rate

There are multiple attacks present in WSNs. Calculating the number of correct attacks detected by the number of total attacks occurs in the network are the key challenges as the accurate count is required based on which alarm rate is dependent.

6.5 Unexpected Nature of Sinkhole Attacks

Using routing matric, different routing protocols were exercised by WSN for packet transmission [56]. The affected node uses its routing matric from routed protocol and generates the sinkhole attack which in result causes all the data to flow from the compromised node. Depending on the metric of routing protocol, sink attack technique contains variations.

6.6 Limitation of Resources

Resource constraints are one of the most crucial challenges in the detection of sinkhole attacks in WSNs which do enforce the requirement of the strong security system. All the nodes being operated in WSN are having limited power with the capability to communicate in short distance by having minimum memory and high computational performance.

7 Performance Analysing Parameters

A lot of parameters are there for calculating the performance and detection rate of sinkhole attack. Some of the most important parameters include the load of network, efficiency, sinkhole detection rate, energy consumption etc.

The available formulas (see Eqs. 7.1–7.4) for the above-mentioned parameters have been taken from [57];

7.1 Load of Network

Load of the network can be calculated by using Eq. 7.1.

$$\mathrm{L(t)} = nb_{event} + nb_{attack} \tag{7.1}$$

where L (t) is a load of the network in a time domain, nb_{event} and nb_{attack} are the numbers of generated events and number of sinkhole attack generated respectively.

7.2 Energy Consumption

$$\mathrm{E} = E_{tx} + E_s + E_p + E_{rx} \tag{7.2}$$

In the above-mentioned formula (see Eq. 7.2), E is the total expended energy, E_{tx} is the energy to be transmitted, E_s is the energy to be used by a carrier, E_p is the energy to be utilized in sleeping mode and E_{rx} is the energy to be consumed at the receiver side.

7.3 Sinkhole Detection Rate

To calculate the sinkhole detection rate, the number of detected attacks are divided by the number of injected attacks as can be seen in Eq. 7.3.

$$\mathrm{S_{DR}} = N_{AD}/N_{AG} \tag{7.3}$$

Here, N_{AD} number of detected attacks and N_{AG} number of injected attacks.

7.4 Efficiency

To calculate the efficiency, Eq. 7.4 is to use,

$$E = D_T - O_T \tag{7.4}$$

where D_T is the first sinkhole attack detection time and O_T is first sinkhole attack performing time.

Based on the above mention formulas, one can find the value of these parameters by simply placing a number of sensor nodes in a testing area. Sensor nodes can have variation in their numbers to calculate the density. To create a sinkhole attack, simple select some random set of sensor nodes and advertise the fake position of sink during simulation.

8 Conclusion and Future Work

In this survey paper, we have reviewed the sinkhole attacks on WSNs. We have covered the discussion on the most popular WSN routing protocols and the techniques adversaries used to launch a sinkhole attack on them. The critical observations had been paid on intruder detection mechanisms and reviewed various techniques proposed in the literature to detect sinkholes. Each approach has its own advantages and disadvantages. Based on the reviewed techniques for the intruder detection, a fuzzy logic-based approach is considered as one of the best techniques as this scheme is scalable, can be distributed or centralized, perform fast computations etc. Countermeasures and the best practices to protect a sensor network from such attacks was also the discussion part of this survey paper. Formulae were presented to calculate some important performance analysis parameters for sinkhole attack.

In the future, more effective solutions are required for minimizing the most common issues of WSN that include network overheads, power utilization, a rate of detection and validation.

References

1. Hidoussi, F., Toral-Cruz, H., Boubiche, D. E., Lakhtaria, K., Mihovska, A., & Voznak, M. (2015). Centralized IDS based on misuse detection for cluster-based wireless sensors networks. *Wireless Personal Communications, 85*(1), 207–224.
2. Bhushan, B., & Sahoo, G. (2018). Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. *Wireless Personal Communications, 98*(2), 2037–2077.
3. Alajmi, N. (2014). Wireless sensor networks attacks and solutions. arXiv preprint arXiv:1407.6290.
4. Dimitriou, T., & Krontiris, I. (2006). Secure in-network processing in sensor networks. In Y. Xiao (Ed.), *Security in sensor networks* (pp. 275–290, Chap. 11). Taylor and Francis Group, CRC press.
5. Camtepe, S. A., & Yener, B. (2005). *Key distribution mechanisms for wireless sensor networks: A survey*. Rensselaer Polytechnic Institute, Troy, New York, Technical Report, 05-07.
6. Lazos, L., & Poovendran, R. (2005). SeRLoc: Robust localization for wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN), 1*(1), 73–100.
7. Ngai, E. C. H., Liu, J., & Lyu M. R. (2006). On the intruder detection for sinkhole attack in wireless sensor networks. In *IEEE international conference on communications, 2006. ICC'06* (Vol. 8, pp. 3383–3389). IEEE.

8. Hu, Y. C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. In *INFOCOM 2003, twenty-second annual joint conference of the IEEE computer and communications. IEEE Societies* (Vol. 3, pp. 1976–1986). IEEE.
9. Yu, B., & Xiao, B. (2006). Detecting selective forwarding attacks in wireless sensor networks. In *20th international parallel and distributed processing symposium, 2006. IPDPS 2006* (pp. 8). IEEE.
10. Othman, S. B., Bahattab, A. A., Trad, A., & Youssef, H. (2015). Confidentiality and integrity for data aggregation in WSN using homomorphic encryption. *Wireless Personal Communications, 80*(2), 867–889.
11. Gupta, D., Kaur, H., & Kumar, R. (2016). Detection of sink hole attack in wireless sensor network using advanced secure AODV routing protocol. *International Journal of Computer Applications*, *156*(11), 1–5.
12. Sundararajan, R. K., & Arumugam, U. (2015). Intrusion detection algorithm for mitigating sinkhole attack on LEACH protocol in wireless sensor networks. *Journal of Sensors, 2015*, 203814.
13. Shafiei, H., Khonsari, A., Derakhshi, H., & Mousavi, P. (2014). Detection and mitigation of sinkhole attacks in wireless sensor networks. *Journal of Computer and System Sciences, 80*(3), 644–653.
14. Sharmila, S., & Umamaheswari, G. (2011). Detection of sinkhole attack in wireless sensor networks using message digest algorithms. In *2011 international conference on process automation, control and computing (PACC)* (pp. 1–6). IEEE.
15. Sheela, D., Kumar, C. N., & Mahadevan, G. (2011). A non-cryptographic method of sinkhole attack detection in wireless sensor networks. In *2011 international conference on recent trends in information technology (ICRTIT)* (pp. 527–532). IEEE.
16. Chen, C., Song, M., & Hsieh, G. (2010). Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. In *2010 IEEE international conference on wireless communications, networking and information security (WCNIS)* (pp. 711–716). IEEE.
17. Papadimitriou, A., Le Fessant, F., Viana, A. C., & Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree-based routing in wireless sensor networks. In *5th IEEE workshop on secure network protocols, 2009. NPSec 2009* (pp. 43–48). IEEE.
18. Choi, B. G., Cho, E. J., Kim, J. H., Hong, C. S., & Kim, J. H. (2009). A sinkhole attack detection mechanism for LQI based mesh routing in WSN. In *International conference on information networking, 2009. ICOIN 2009* (pp. 1–5). IEEE.
19. Krontiris, I., Giannetsos, T., & Dimitriou, T. (2008, October). Launching a sinkhole attack in wireless sensor networks; the intruder side. In *IEEE international conference on wireless and mobile computing networking and communications, 2008. WIMOB'08* (pp. 526–531). IEEE.
20. Coppolino, L., D'Antonio, S., Romano, L., & Spagnuolo, G. (2010). An intrusion detection system for critical information infrastructures using wireless sensor network technologies. In *2010 5th international conference on critical infrastructure (CRIS)* (pp. 1–8). IEEE.
21. Rassam, M. A., Zainal, A., Maarof, M. A., & Al-Shaboti, M. (2012). A sinkhole attack detection scheme in mint route wireless sensor networks. In *2012 international symposium on telecommunication technologies (ISTT)* (pp. 71–75). IEEE.
22. Hamedheidari, S., & Rafeh, R. (2013). A novel agent-based approach to detect sinkhole attacks in wireless sensor networks. *Computers & Security, 37,* 1–14.
23. Jahandoust, G., & Ghassemi, F. (2017). An adaptive sinkhole aware algorithm in wireless sensor networks. *Ad Hoc Networks, 59,* 24–34.
24. Kibirige, G. W., & Sanga, C. (2015). A survey on detection of sinkhole attack in wireless sensor network. arXiv preprint arXiv:1505.01941.
25. Devibala, K., BalaMurali, D. S., Ayyasamy, D. A., & Archana, D. M. (2017). Flow-based mitigation model for sinkhole attack in wireless sensor networks using time-variant snapshot. *International Journal of Advances in Computer and Electronics Engineering, 2*(05), 14–21.
26. Ahmed, N., Kanhere, S. S., & Jha, S. (2005). The holes problem in wireless sensor networks: A survey. *ACM SIGMOBILE Mobile Computing and Communications Review, 9*(2), 4–18.
27. Huang, C. F., & Tseng, Y. C. (2005). The coverage problem in a wireless sensor network. *Mobile Networks and Applications, 10*(4), 519–528.
28. Ma, W., Yan, F., Zuo, X., Ren, L., Xia, W., & Shen, L. (2017). Coverage hole detection algorithm without location information in wireless sensor networks. In *2017 3rd IEEE international conference on computer and communications (ICCC)* (pp. 357–361). IEEE.
29. Wood, A. D., Stankovic, J. A., & Son, S. H. (2003). JAM: A jammed-area mapping service for sensor networks. In *24th IEEE real-time systems symposium, 2003. RTSS 2003* (pp. 286–297). IEEE.
30. Karmakar, S., & Roy, A. (2014). Holes detection in wireless sensor networks: A survey. *International Journal of Modern Education and Computer Science, 6*(4), 24.

31. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks, 1*(2–3), 293–315.
32. Chaturvedi, P., & Daniel, A. K. (2014). Recovery of holes problem in wireless sensor networks. In *2014 international conference on information communication and embedded systems (ICICES)* (pp. 1–6). IEEE.
33. Mohemed, R. E., Saleh, A. I., Abdelrazzak, M., & Samra, A. S. (2017). Energy-efficient routing protocols for solving energy hole problem in wireless sensor networks. *Computer Networks, 114,* 51–66.
34. Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2016). A modified algorithm to improve the security and performance of AODV protocol against black hole attack. *Wireless Networks, 22*(5), 1505–1511.
35. Oriyano, S. P. (2016). *Denial of service. CEH™ v9: Certified ethical hacker version 9 study guide* (pp. 305–329). New York: Wiley.
36. Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN), 2*(4), 500–528.
37. Krontiris, I., Dimitriou, T., Giannetsos, T., & Mpasoukos, M. (2007). Intrusion detection of sinkhole attacks in wireless sensor networks. In *International symposium on algorithms and experiments for sensor systems, wireless networks and distributed robotics* (pp. 150–161). Springer, Berlin, Heidelberg.
38. Sterne, D., Balasubramanyam, P., Carman, D., Wilson, B., Talpade, R., Ko, C., & Bowen, T. (2005). A general cooperative intrusion detection architecture for MANETs. In *Proceedings of the third IEEE international workshop on information assurance, 2005* (pp. 57–70). IEEE.
39. Vuppala, S., Banerjee, A., Pal, A., & Choudhury, P. (2011). An attack identification scheme using hierarchical data clustering in MANET. In *International conference on computer engineering and technology, 3rd (ICCET 2011)*. ASME Press.
40. Abraham, A., Grosan, C., & Martin-Vide, C. (2007). Evolutionary design of intrusion detection programs. *IJ Network Security, 4*(3), 328–339.
41. Sun, B., Wu, K., & Pooch, U. W. (2003). Zone-based intrusion detection for mobile ad hoc networks. *International Journal of Ad Hoc and Sensor Wireless Networks, 2*(3), 2003–2009.
42. Banerjee, S., Grosan, C., & Abraham, A. (2005). IDEAS: intrusion detection based on emotional ants for sensors. In *Proceedings of the 5th international conference on intelligent systems design and applications, 2005. ISDA'05* (pp. 344–349). IEEE.
43. Patcha, A., & Park, J. M. (2006). A game theoretic formulation for intrusion detection in mobile Ad Hoc networks. *IJ Network Security, 2*(2), 131–137.
44. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on mobile computing and networking* (pp. 255–265). ACM.
45. Mukkamala, S., Sung, A. H., & Abraham, A. (2005). Intrusion detection using an ensemble of intelligent paradigms. *Journal of Network and Computer Applications, 28*(2), 167–182.
46. Li, Y., & Parker, L. E. (2008). Intruder detection using a wireless sensor network with an intelligent mobile robot response. In *Southeastcon, 2008. IEEE* (pp. 37–42). IEEE.
47. Soni, V., Modi, P., & Chaudhri, V. (2013). Detecting sinkhole attack in a wireless sensor network. *International Journal of Application or Innovation in Engineering & Management, 2*(2), 29–32.
48. Diallo, C., Sawaré, A., & Sow, M. T. (2017). Security issues and solutions in wireless sensor networks. *International Journal of Computer Science and Information Security, 15*(3), 6.
49. Kaur, M., & Singh, A. (2016, September). Detection and Mitigation of Sinkhole Attack in Wireless Sensor Network. In *2016 International conference on micro-electronics and telecommunication engineering (ICMETE)* (pp. 217–221). IEEE.
50. Sharma, P., & Singh, A. (2017). Probing and removal of denial of service attack in wireless sensor networks. *Imperial Journal of Interdisciplinary Research*, *3*(2), 975–978.
51. Dalal, S., & Devi, S. (2016). Survey on attacks pertaining to wireless mesh networks and approach towards counter measures. *International Journal of Computer Applications*, *149*(12), 20–26.
52. Singh, A., & Singh, T. (2016). Review on detection and prevention of sink hole attack in network. *Global Journal of Computers & Technology, 5*(2), 289–292.
53. Deng, J., Han, R., & Mishra, S. (2006). INSENS: Intrusion-tolerant routing for wireless sensor networks. *Computer Communications, 29*(2), 216–230.
54. Misra, S., Bhattarai, K., & Xue, G. (2011, June). BAMBi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks. In *2011 IEEE international conference on communications (ICC)* (pp. 1–5). IEEE.
55. Sen, J. (2010). A survey on wireless sensor network security. arXiv preprint arXiv:1011.1529.
56. Roy, S. D., Singh, S. A., Choudhury, S., & Debnath, N. C. (2008). Countering sinkhole and black hole attacks on sensor networks using dynamic trust management. In *IEEE symposium on computers and communications, 2008. ISCC 2008* (pp. 537–542). IEEE.

57. Kalnoor, G., Agarkhed, J., & Patil, S. R. (2017). Agent-based QoS routing for intrusion detection of sinkhole attack in clustered wireless sensor networks. In *Proceedings of the first international conference on computational intelligence and informatics* (pp. 571–583). Springer, Singapore.

Dr. Aqeel-ur Rehman is a Professor, Deputy Director (Admin)-HIET and Chairman of Department of Computing at Hamdard Institute of Engineering and Technology, Faculty of Engineering Sciences and Technology, Hamdard University, Karachi, Pakistan. He is associated with Hamdard University since last 18 years. Dr. Aqeel-ur Rehman has over 19 years of teaching, research, and academic administration experience. He obtained Ph.D. degree in Computer Science with specialization in Ubiquitous Computing from National University of Computer and Emerging Sciences, Karachi, Pakistan in 2012. He completed MS in Information Technology from Hamdrad University, Karachi, Pakistan and BS in Electronic Engineering from Sir Syed University of Engineering and Technology, Karachi, Pakistan in 2001 and 1998 respectively. He is the author of 47 research articles in journals, conferences and book chapters of international repute. His current research interests include Sensor Networks, Ubiquitous Computing, Computer Networks and Smart Agriculture.

Engr. Sadiq Ur Rehman is a lecturer in electrical department at Hamdard Institute of Engineering and Technology, Faculty of Engineering Sciences and Technology, Hamdard University, Karachi, Pakistan. He is associated with Hamdard University since April 2016 and also doing his Ph.D. in Electrical Engineering (Specialization in Communication System and Networks) from the same University. Engr. Sadiq Ur Rehman has done MS in Computer Science and Communication Engineering from University Duisburg-Essen, Germany in 2015 and BE in Electronics Engineering from Usman Institute of Technology (UIT), Karachi, Pakistan in 2008 respectively. His current research interests include Sensor Networks, Wireless Body Area Network and IoT.

Haris Raheem is a Technology Consultant with more than a decade of experience in IT solutions development. He has worked on various national and international assignments with various organizations in his career. He completed MS in Information Technology from Hamdard University, Karachi, Pakistan in 2017 and BS in Computer Science from Shah Latif University, Pakistan in 2003. His current research interests include Sensor Networks, Computer Networks and IoT.