Annals of Emerging Technologies in Computing (AETiC)
Vol. 2, No. 4, 2018

Long Article

Sensor Networks Attacks Classifications and Mitigation

Ahmed S. Abu Daia[1,*], Rabie A. Ramadan[2,3], Magda B. Fayek[1]

[1]Department of Computer Engineering, Cairo University, Egypt
ahmed.shawky@outlook.com, magdafayek@ieee.org
[2]Department of Computer Engineering, Cairo University, Egypt
rabie@rabieramadan.org
[3]Department of Computer Science and Software Engineering, University of Hail , KSA
r.ramadan@uoh.edu.sa
*Correspondence: ahmed.shawky@outlook.com

Received: 15th July 2018; Accepted: 6th August 2018; Published: 1st October 2018

Abstract: Wireless Sensor Networks (WSNs) are exposed to many security attacks, and it can be easily compromised. One of the main reasons for these vulnerabilities is the deployment nature, where sensor nodes are deployed without physical guarding duty. That makes the network susceptible to physical attacks. The communication nature between sensor nodes is another reason, where intruders can easily send/receive information if they are located in the network communication range. In this paper, most of the possible WSN attacks are discussed, different security services expected in WSN are explained, and trust-based solutions proposed in the literature are listed. Moreover, the state-of-the-art of the attacks' mitigation and avoidance techniques are presented. Besides, this paper is enriched with a new classification of the WSNs attacks regarding attacks' characteristics. It will be beneficial to researchers in the field of WSNs security if they can distinguish between different attacks that have common characteristics.

Keywords: *Wireless sensor networks; WSN possible attacks; WSN attacks' detecting features; WSN security services; WSN trust-based solutions; WSN attacks mitigation techniques; WSN attack avoidance techniques*

1. Introduction

Wireless technologies have been emerged to cover many activities and support many requirements of our life. WSN is one of the examples of wireless networks that are used in a wide range of useful applications and most of these applications manipulate sensitive data. In addition, in smart cities, WSNs play a significant role in capturing critical information from the surrounding environment. Protecting networks from intrusions and attacks is an important task. At the same time, it is not an easy job to do. Examples of WSNs applications include: Battlefield [1] such as (identification of enemy capabilities and positions, and recognizing soldier activities in the field [2], In hospitals for health care [3][4], in roads for traffic monitoring [5] [6], railway bridge monitoring [7], disasters detection (such as fire [8], volcano [9] , landslide, or earthquake [10]), identification of low-level point radiation sources [11], air pollution detection and monitoring [12], atmospheric observation [12][13], wildlife animals observation [14], and smart agriculture systems [15].

Ahmed S. Abu Daia, Rabie A. Ramadan and Magda B. Fayek, "Sensor Networks Attacks Classifications and Mitigation", Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 28-43, Vol. 2, No. 4, 1st October 2018, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2018.04.003, Available: http://aetic.theiaer.org/archive/v2/v2n4/p3. html.

These applications are susceptible regarding their data. Some of them, if not all, deal with people's life information. Therefore, securing such information from intrusion became essential and highly required. Intruders may inject false data into the network, prevent the occurrence of events, break down some nodes that in turn pull some part(s) of the network into isolation, or in the worst case; the entire network may stop working. Therefore, it is highly demanded to protect the network from intruders and quickly isolate the infected nodes. Unfortunately, traditional methodologies such as asymmetric cryptography are not suitable for wireless networks [16] due to limited power sources and small communication range of the nodes. Therefore, some new techniques proposed for compromised node detection and isolation. These techniques could be classified into two classes[17]:

A. Misuse Intrusion Detection (MID) [18]. These techniques/algorithms assume that the characteristics of attacks have a certain signature that can be predicted. Hence, the detection system is constantly monitoring and looking for activities that match a predefined signature.

B. Anomaly-based Intrusion Detection (AID) [19]. These techniques assume that the intruder's behavior deviates from the normal network nodes. So, each node will monitor its neighbors' behavior looking for abnormality.

This paper organized as follows: the popular security services and requirements presented in Section II. WSN possible attacks discussed in Section III, and the proposed attacks' detecting features explained in Section IV. A brief review of trust and different trust methodologies are presented in Section V. WSN attack's mitigation techniques survey is discussed in Section VI. The attacks avoidance techniques also addressed in Section VII. Finally, open research issues are presented in Section VIII.

2. WSN Security Services

The security services are the requirements which ensure that data transfer between nodes is secure and protected from different intrusions and attacks. Some of these services defined by the Open Systems Interconnection model (OSI model) and other communication standards. Hence, the following security requirements should be fulfilled to have secure data transfer channels:

1. **The authentication** service can be provided at two levels:

    a. **Peer Node Authentication:** the authentication check is performed on the claimed sender node; where the receivers verify whether the claimed network node sends the message or not.

    b. **Data Authentication:** the authentication check is performed on the data; where the receivers verify that the claimed network node sends the data.

2. **Access Control** prevents an unauthorized use of any network node.

3. **Data Confidentiality** prevents an unauthorized use of content data, by preventing intruders to snoop on transmitted data.

4. **Data Integrity** prevents unauthorized users from modifying or altering the data packets.

5. **User privacy** prevents unauthorized users from knowing the sender/receiver of data packets.

6. **Data Freshness** ensures that readings received by the base station are fresh and no old readings have been replayed.

7. **Non-Repudiation** ensures that network activities such as sending and receiving data packets are made by the node claiming this activity, and the claiming nodes cannot deny the ownership of these activities.

8. **Data Availability** ensures that the data is accessible anytime.

9. **Self-organization** ensures that the compromised nodes can be excluded and separated from the network.
10. **Time synchronization** ensures that all network nodes have synchronized time.
11. **Survivability** ensures that the network is alive the most prolonged period and can resist the intruders' attacks.
12. **Secure localization** ensures that network nodes get its locations from authenticated beacon nodes.

3. WSN Possible Attacks

This section presents most of the possible attacks, which might be used by intruders to break down the Wireless Sensor Network (WSN).

1. **Bad Mouthing Attack:** this attack occurs when an intruder tries to distort the innocent nodes' reputation by sending negative reputation values about these nodes [20][21] . For example, a malicious node (A) announces negative reputation about an innocent node (B). Such case will let other sensor nodes avoid sending any data to the node (B), while node (B) is not an attacker node. If the network has such an attack, after a while, the number of isolated nodes will increase because attackers will repeat such behavior with all its neighbors. The purpose of this attack is to isolate as much as possible network nodes.
2. **Good Mouthing attack:** in this attack, intruders try to deceive the base station or the cluster heads by sending positive reputation values about bad nodes [20][21]. This attack is the contrary of bad mouthing attack. It has the following form, malicious node (A) announces positive reputation of another malicious node (B). The purpose of this attack is to dominate the network traffic, to break down the entire network.
3. **Whitewashing Attack:** this attack occurs when a malicious node tries to re-enter the network with a new identifier and a new reputation [16][19]. This attack occurs when the system successfully detects a malicious node and isolates it from the network; then this malicious node tries to re-join the network with a new identifier to delude the system and have a new trust value.
4. **Energy Drain Attack:** in this attack, a malicious node asks the neighbor nodes to respond to useless traffic [22][23]. Usually, the malicious node has unlimited power and high communication range to be able to send a lot of useless messages to its neighbors, such as control message or corrupted data. The purpose of this attack is to break down the entire network quickly.
5. **Exhaustion Attack:** this attack has a form where the attacker asks neighbor nodes to retransmit messages even there is no collision [24][25]. The exhaustion attack is similar to the energy drain attack, where malicious nodes aim to destroy the network by discharging nodes' batteries. However, in this attack, the malicious node pretends that data transmission is failed and asks for retransmission multiple times.
6. **Homing Attack:** in this attack, intruders investigate the network traffic to understand the geographical area of cluster heads or base station [25] . When intruders know the network structure, they will be able to determine the most critical nodes and then attack these nodes to destroy the entire network quickly.
7. **Node Replication Attack:** this attack occurs when there exists a duplication of the node's unique identifier [26]. In this attack, the malicious node appears with an identifier that is assigned to another node; this case leads to inaccurate data aggregation. Also, the location estimation techniques that depend on the nodes' identifiers will not be accurate. Figure 1

below demonstrates the case in which two nodes are added to the network with the same address; which is not allowed.

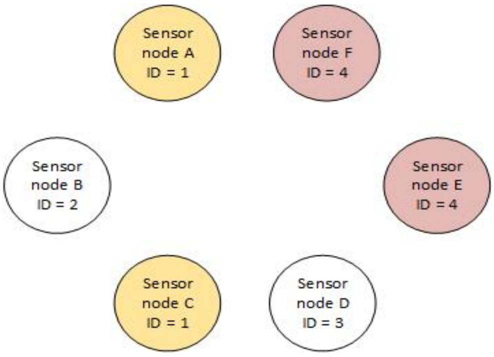

Figure 1. Node Replication Attack [26]

8. **Sybil Attack:** this attack occurs when a malicious node has multiple identities within the network [27][28] . It is similar to the node replication attack, but the malicious node appears with a different identifier. Figure 2 illustrates Sybil attack and how it may occur in networks, where the malicious node has more than one identifier A, B, and C. However, other normal nodes have only one identifier, such as nodes X, Y, Z, etc. The purpose of this attack is to disrupt the data aggregation process.

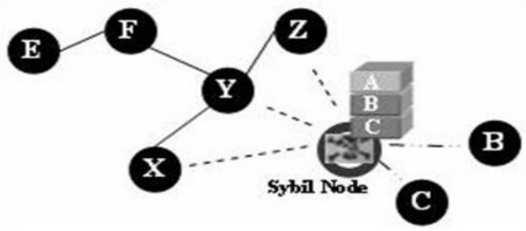

Figure 2. Sybil Attack [27][27][28]

9. **Sinkhole Attack:** a malicious node in this attack adverts itself as the closest node to base station to capture the entire network traffic, then it drops data packets instead of forwarding it to the base station [29][30][31] . Figure 3 demonstrates Sinkhole attack and how it occurs in networks. The centralized node (colored in orange) receives most of the network packets from its neighbors then destroy it, instead of sending it to the base station. In this attack, the rate of delivered packets to the base station is decreased significantly. The intruder in this attack is a very active node (has high remaining power, and low power consumption rate), and highly social by having a excellent communication range and neighbors number.

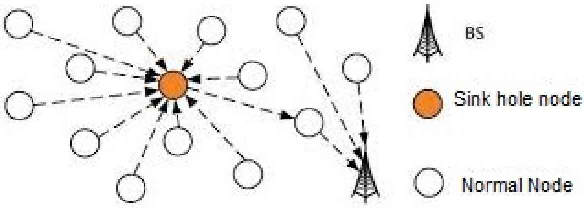

Figure 3. Sinkhole Attack [29][30][31]

10. **Sniffing Attack:** the sniffer node imposes into the network to capture the network's valuable data [20]. The malicious node, in this case, does not affect the network performance nor its lifetime instead, it eavesdrops the sent packet looking for any valuable information. The effect of this attack can be horrible in sensitive data applications such as military field services. Usually, the malicious sniffing node has unlimited power and high communication range, as illustrated in figure 4 below, where the intruder

eavesdrops any communication channel between two nodes, or between a sensor node and the base station.

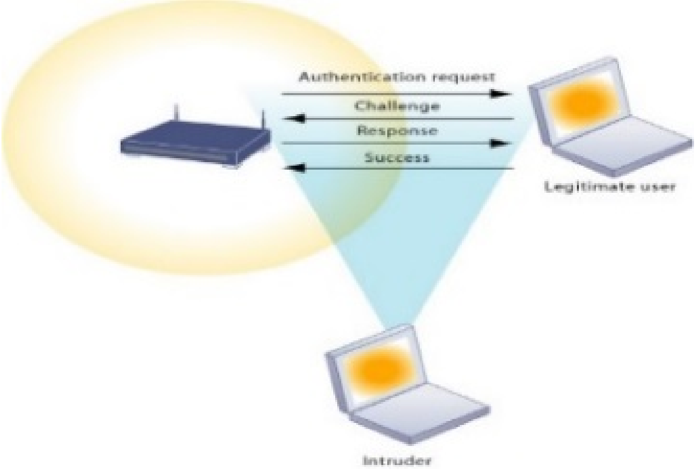

Figure 4. Sniffer attack [20]

11. **Neglect and Greed Attack:** this attack occurs when the malicious node forces multi-hopping in the network, by routing the packets towards a wrong node [20]. The malicious node selects the longest path to send the data to a destination node. For example, in figure 5, node (X) needs to send data to node (D). Instead of sending the data to the node (D) directly, it sends the data through a long route with multiple nodes within this path. This behavior will decrease the remaining power of the nodes found in that route, hence breakdown the network quickly.

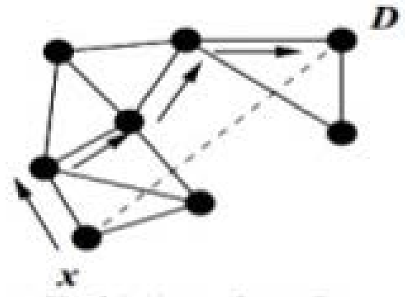

Figure 5. Neglect and Greed Attack [20]

12. **Grey-hole Attack:** the attacker in this attack drops certain types of packets [32][33]. This attack is a particular case of sinkhole attack, where grey-hole does not drop all packets. Instead, it drops a specific packet. For example in figure 6 below node 3 and 5 drops the packets going to node 6, while they send data to other network nodes. The purpose of such behavior is to stay undetectable as much as possible. So, this attack is harder to detect than the sinkhole attack.

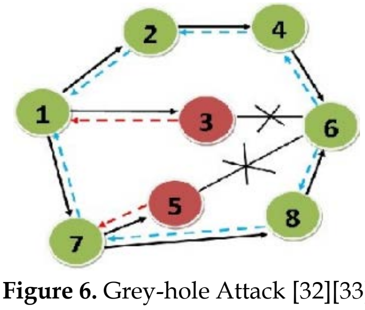

Figure 6. Grey-hole Attack [32][33]

13. **Hello Flood Attack:** this attack is a special case of Energy Drain attack, where the malicious nodes overflow its adjacent nodes with HELLO messages [34]. The following figure 7 illustrates the hello flood attack. The intruder in this attack has an unlimited power supply and low power consumption. Its data traffic measures (transmit and

receive) are too high. Moreover, it has high communication range and an enormous number of neighbors. The purpose of such an attack is to consume nodes energy and jam the network with useless packets.

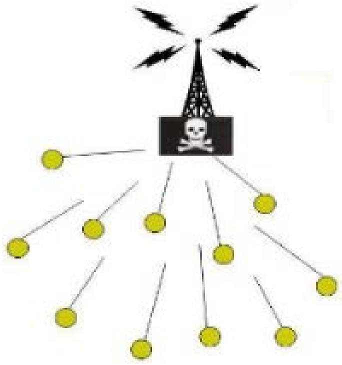

Figure 7. Hello Flood Attack [35][34]

14. **Node outage:** the malicious node in this attack could be a cluster head, halts working nodes within its cluster, and does not wake them up again [20][23][24] . The characteristics of the malicious node, in this case, being a cluster head for a long time. So the cluster head role should be changed periodically between the cluster members to avoid such attack. Malicious nodes in such an attack usually have endless energy.

15. **Garnished Attack:** in this attack, the malicious node is smart enough to behave both good and bad with the aim of remaining undetected [1]. The behavior of the malicious node varies according to time, or feature. For example, a malicious node (A) drops the received packets every specific period, while after and before that time, it sends and receives packets normally. Another form of this attack may occur when a malicious node (B) is a multi-model node and sense more than one feature such as temperature, humidity, pressure, and brightness; then it forwards all data packets for all features except the pressure or forward it in a corrupted way. The purpose of doing so is to stay undetectable as much as possible.

16. **Replay Attack:** the intruder in this attack records some data packets and resends it later instead of sensing, collecting, and sending real information. The objective of this behavior is to mislead the base station and corrupt its query answers [1]. As illustrated in figure 8, the intruder eavesdrops the network and records a real data packets and then forward it later as if it is real data. The intruder, in this case, is harder to be detected because it sends a valid and not corrupted but obsolete data.

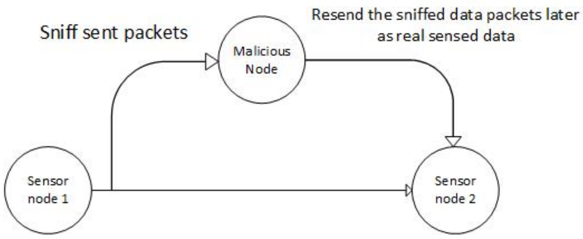

Figure 8. Replay Attack [17]

17. **DoS Attack:** it is called Denial of Service attack, where the attacker tries to prevent a network node or base station from delivering its function correctly or disable it for an amount of time [35][36]. The denial of service attack can be on different layers, for example, it may occur at the medium access layer (MAC), the network layer, or at the application layer. The purpose of the malicious nodes it to consume and deplete the nodes' resources (remaining power, CPU usage, and bandwidth). In this attack the malicious node can behave in two forms; first, it may send a massive number of packets to the sender which fill its buffer and disable it to receive any more packet. In the second

form, the malicious node sends large size packets which require a lot of processing time and resources.

18. **Stealthy Attack:** in this attack, the malicious node injects an incorrect or non-exist data into the network [37]. The intruder in this attack intends to cause a false alarm in the network, or delay the detection of an alarm.

19. **Wormholes:** in this attack, two malicious nodes construct a low-latency junction between two sections of a network [38][38][39][40]. The malicious nodes create a tunnel between them to cheat other nodes that this is the best and shortest path. Figure 9 demonstrates the wormhole attack, where the malicious nodes are S2 and S9, and they created a tunnel between them instead of using the path which contains the following nodes S9, S8, S6, S5, and finally S2. The purpose of having such a tunnel is to deceive the innocent nodes that the data packet is received successfully to the other side, while the malicious node drops it. When the original sender requests an acknowledgment, the malicious nodes create such fake acknowledgment packet to delude the sender nodes.

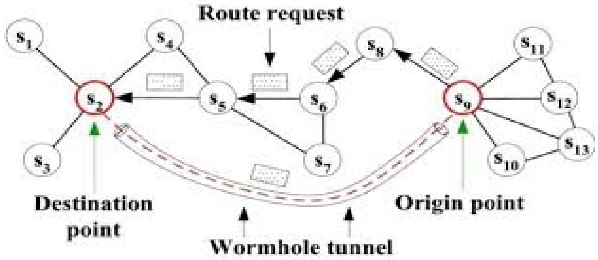

Figure 9. Wormhole Attack [38][39][40]

20. **Jamming:** the intruder in this attack attempts to interrupt the physical layer of the WSN structure [36]. It is deferent than the DoS attack, where DoS attack target specific node(s), but jamming target the entire network. The malicious node sends a huge number of packets trying to make a collision in the network. The collision cases are much expensive, where it drops all transmitted packets and asks every node to resend its data again, the network nodes should communicate with other nodes to resolve that collision before they resend data again, which is a communication overhead. Repeating the collision cases depletes the nodes' power for resolving such collision. Jamming attack aims to make a denial of service but on the physical and medium access layer.

21. **Acknowledgment Spoofing:** the malicious node sniffs the packet transfer from its adjacent nodes and cheats the acknowledgments [41]. For example, in figure 10 node (E) sends data to the node (C); while the sender node (E) is waiting for the received acknowledgment from node (C), the malicious node (AD) sends the acknowledgment instead of the node (C). The data may be dropped in its path to the destination, so node (C) does not send the acknowledgment, but the malicious node (AD) sent it to the node (E) to deceive the sender that data is received successfully.

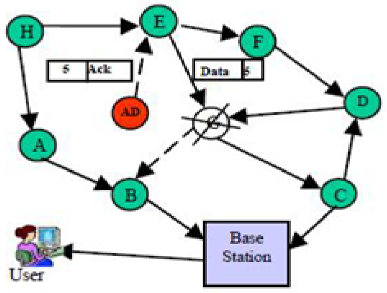

Figure 10. Acknowledgment Spoofing Attack [41]

22. **Intelligent Attack:** The attacker, in this case, is smart enough to behave according to the threshold which defines the malicious nodes [18]. If the attacker found its trust value near to the malicious threshold, it behaves normally until its trust value raised again then re-attack the network again. This type of attack is harder to detect, and it may require a long time to detect.

Table 1 summarizes the mentioned above WSN attacks. Moreover, it contains proposed features used to detect or avoid such attacks

Table 1. Detecting features of different attacks

Attack	Detecting Features	Attack	Detecting Features
Bad or Good Mouthing [24][21] *Whitewashing [16][19]*	1. Nodes' historical trust value 2. Nodes' current trust value 3. Path trust value	*DoS Attack [35][36]* *Node outage [23][24]*	1. Nodes' sleeping time 2. Cluster head lifetime 3. Power consumption rate 4. Remaining power
Energy Drain [22][23][42] *Exhaustion Attack [24][25]*	1. Power consumption rate 2. Remaining power 3. Uptime 4. Sent packets rate 5. Received packets rate 6. Power utilization threshold 7. Nodes' performance 8. Nodes' memory access rate	*Jamming[43]*	1. Collision ratio 2. Communication Range 3. Power consumption rate 4. Remaining power 5. Uptime 6. Sent packets rate 7. Received packets rate 8. Nodes' performance 9. Nodes' memory access rate
Homing Attack [25]	1. Number of initialization packets 2. Number of sent location packets 3. Communication Range 4. Power consumption rate 5. Remaining power 6. Power consumption rate	*Stealthy Attack[37]*	1. Nodes' reputation 2. Nodes' performance
Hello flood [34]	1. Communication Range 2. Power consumption rate 3. Remaining power 4. Power consumption rate 5. Number of sent initialization packets 6. Route Quality 7. Nodes' sent packets rate	*Acknowledgment Spoofing[41]*	1. Base stations' received packets 2. One node has huge connections number 3. Nodes' lost packets 4. Node's Link costs to the base station 5. Power consumption rate 6. Remaining power 7. Distance to the base station
Sinkhole Attack [30][31][32] *Wormholes[38] [39][40]*	1. Base stations' received packets 2. One node has huge connections number 3. Nodes' lost packets 4. Link costs to base station 5. Power consumption rate 6. Remaining power 7. Distance to the base station	*Intelligent Attack [18]*	1. Nodes' reputation 2. Communication Range 3. Power consumption rate 4. Remaining power 5. Base stations' received packets 6. One node has huge connections number 7. Nodes' sent\lost packets
Sniffing[20]	1. Nodes' high receive traffic 2. Nodes' low transmit traffic	*Garnished Attack [16]*	1. Nodes' reputation
Neglect and Greed [20]	1. One node has huge connections number 2. Nodes' sent\lost packets 3. Nodes' high receive traffic 4. Nodes 'low transmit traffic	*Replay Attack[16]*	1. Nodes' reputation 2. Communication Range 3. Power consumption rate 4. Remaining power
Grey-hole Attack [32][33]	1. Nodes' reputation 2. Freshness of the route 3. Base stations' received packets 4. One node has huge connections number 5. Nodes' sent\lost packets	*Node Replication [38][20]* *Sybil Attack [27][28]*	1. Number of lost network packets 2. Number of newly added nodes 3. Nodes in two different locations claim the same ID

4. WSN Attacks Detection Features

In this section, we will summarize the detection features of the previously mentioned attacks. The attack detecting features help for identifying and recognizing that attack. These features are summarized in Table 2. As can be noticed, some attacks might have common features. These features are defined as follows:

1. Node's current/historical trust value: it is the data trust value for a node; this trust value represents the nodes' neighbor trust in the node's data, the service provided by that node, or the communication link between them. This feature can be used to detect the following attacks: bad mouthing, good mouthing, and whitewashing.
2. Path trust value: this feature represents how much the sender trusts in a path to be used for sending data to the destination node. We use this feature to detect the following attacks: bad mouthing, good mouthing, and neglect and greed.
3. Remaining power: it is the percentage of the power remain in the sensor node. The depletion of this feature could be an indicator for exhaustion and energy drain attacks.
4. Uptime (lifetime): it is the actual amount of time in which the node stays on; where the node's sleeping time is not considered in that time. So the uptime can be calculated using the following formula:
$$\mathrm{up}_{\mathrm{time}} = \sum(Wakeup_{time} - Sleep_{time}) \qquad (1)$$
5. Power consumption rate: this indicator guides us for determining active nodes which have unlimited power supply. This feature can be calculated by equation (2).
$$consum_{rate=} (100 - Remaing_{Power})/\mathrm{up}_{\mathrm{time}} \qquad (2)$$

   The power consumption rate in cooperation with the remaining power, and the up time indicators are common detection features for attacks like energy drain, exhaustion, homing, sinkhole, hello flood, node outage, replay, DoS, wormhole, jamming, acknowledgment spoofing, and intelligent.
6. Sent and Received packets rate: these two features are used to determine the high traffic nodes. Such nodes send and receive packets with a high rate, while other network nodes have a low or medium traffic rate. Usually, these indicators are high for malicious nodes having the following attacks: jamming, hello flood, sniffing, neglect and greed, exhaustion, and energy drain. Sent and received packets rate indicators can be calculated using equations
$$sent_{rate} = sent_{packets} / time \qquad (3)$$
$$received_{rate} = received_{packets}/time \qquad (4)$$

   These indicators take into consideration the different packets types such as data, initialization, control, and localization packets.
7. Base stations' received packets: it measures the number of data packets delivered to the base station, and this number decreases in case of having one of the following attacks: Sinkhole, Grey-hole, Wormholes, Acknowledgment spoofing, Intelligent, Energy drain, and Exhaustion. This feature is vital because its reduction means there is a serious problem in the network either the nodes do not send its data, the sensor nodes' power depleted, or nodes were totally isolated.
8. The Number of sent initialization packets: this feature traces the number of initialization packets sent by a specific node. High value for this feature points out that this node may have Homing or Hello flood attacks.
9. The Number of sent location packets: this is a special case of the sent and received packets rate, where it measures the number of the location definition packets. This feature helps in detecting Homing attack, where malicious nodes try to discover sensor nodes' location.
10. Nodes in two different locations claim the same ID: this metric points to the existence of either node replication or Sybil attacks. In other words, two nodes have the same identifier, or one node has two identifiers. This feature can be detected in a clustered network by querying the nodes' identifier; then every cluster head responds by the identifiers of its nodes. Hence, the duplication in the concatenated identifiers list means that two different nodes have the same

identifier. Another method can be accomplished by querying a pair of node's identifier and location; hence, we could determine if one place has two identifiers or not, or two different nodes into different locations have the same identifier or not.

11. The Number of newly added nodes to the network: usually this measure has high value at the beginning of the deployment, or in case most of the network nodes were dead and replaced by new nodes. The importance of this measure appears in cases where the initialization and location packets are high in the network while there are no new nodes added; hence it points out that there is a malicious node within the network.
12. Nodes' lost packets: this feature measures the nodes' data loss rate. When this measure has high value, it means that there are either collision or a malicious node drops that packets. This feature can be used in detecting sinkhole, worm holes, and acknowledgment spoofing attacks. This feature can be calculated using the following formula:

$$lost_{packets} = lost_{data} / \ time \qquad (5)$$

13. Node's sent/lost packets ratio: it is the percentage of lost data packets out of the sent packets, and it can be calculated using formula 6.

$$data\_lost_{ratio} = \ sent_{data} \ / \ lost_{data} \qquad (6)$$

This feature can be used in detecting neglect and greed, grey-hole, and intelligent attacks.

14. Node's performance: this feature measures the node's CPU usage, and it reflects the nodes' processing capability, where the malicious nodes may assign recursive tasks to other nodes to consume its processing unit. After a while, the sensor node will lose its remaining power in useless processing activity.
15. Node's memory access rate: this is another point of view for measuring the sensor nodes' performance, where very high memory access rate and very high CPU usage may indicate the existence of energy drain or exhaustion attacks.
16. Communication Range: we use this feature to detect the highly social node in the network. High communication range gives nodes the ability to have a wide range of neighbors; but we have to pay attention to nodes which have a very high communication range, very high remaining power, and very low power consumption rate, because these nodes are highly candidate to be malicious nodes.
17. The Number of connections: this is another feature that gives us the ability to detect the highly social sensor node. This feature is used to detect any of the following attacks: Sinkhole, Neglect and Greed, Grey-hole, Wormholes, Acknowledgment Spoofing, and Intelligent attacks.
18. Link costs to the base station: link cost between a node and base station can be calculated depending on the number of hops in that path, the remaining power of the nodes located in that path, or the reputation (trust) value of nodes located in that path. Usually, the malicious nodes (nodes having Sinkhole, Wormholes, or Greyhole attacks) announce that they are located in the lowest cost path to the base station; then they can drop or alter the data packets. Malicious nodes declare their existence in the lowest cost path to increase their neighbors and sociality.
19. Distance to the base station: it means the distance to the base station represents the number of hops found in that path, and it is similar to the link cost to the base station where it is used to detect the sinkhole, wormholes, or gray hole attacks.
20. Route Freshness: the freshness of the route measures the percentage of newly added nodes in a path to the base station. The sensor nodes should not fully depend on the fresh route, where it may have malicious or untrusted nodes. This measure is used to detect grey-hole or whitewashing attacks.
21. Collision ratio: the malicious nodes procedures collision trying to consume nodes' remaining power and resources. This measure can be calculated by the number of retransmission in a period. So this feature is necessary to detect the jamming attack.
22. Nodes' sleeping time: nodes go into sleep mode to reduce the power consumption, but the malicious node may put another node in sleeping mode and does not wake up it again. So, this measure keeps tracking the summation of all sleeping time for a node, and raise the danger flag

if the sleeping time was too long. This feature is used in detecting the node outage, and DoS attack.

23. Cluster head lifetime: cluster head role should be rounded between the cluster members, but malicious nodes with high power may stay a long time being a cluster head. So this measure is used to keep track such nodes which have been selected as cluster heads for a long time, these nodes might be malicious nodes and breakdown the entire cluster nodes or drop its data packets.

For readers to benefit from this summary of attacks detecting features, Table 2 summarizes detection features and possible detected attacks by each feature.

Table 2. Possible detected attacks by features

Feature	Possible attacks to be detected	Feature	Possible attacks to be detected
Node's current/historical trust value	- Bad mouthing, - Good mouthing, - Whitewashing	*Node's sent/lost packets ratio*	- Neglect and Greed, - Grey-hole Attack, - Selective forwarding, - Intelligent Attack
Path trust value	- Bad mouthing, - Good mouthing	*Route Freshness*	- Grey-hole Attack
Uptime (lifetime), *Remaining power,* *Power consumption rate*	- Energy Drain, - Exhaustion Attack, - Homing Attack, - Sinkhole Attack, - Hello flood, - Node outage, - Replay Attack, - DoS Attack, - Wormholes, - Jamming, - Acknowledgment Spoofing, - Intelligent Attack	*Nodes' performance* *Nodes' memory access rate,* *Power consumption rate*	- Energy Drain, - Exhaustion Attack, - Jamming
Uptime (lifetime) *Sent and Received packets rate*	- Energy Drain, - Exhaustion Attack, - Hello flood, - Jamming	*Communication Range*	- Homing Attack, - Hello flood, - Replay Attack, - Jamming, - Intelligent Attack
Base stations' received packets	- Sinkhole Attack, - Grey-hole Attack, - Selective forwarding, - Wormholes, - Acknowledgment Spoofing, - Intelligent Attack	*Number of connections*	- Sinkhole Attack, - Neglect and Greed, - Grey-hole Attack, - Selective forwarding, - Wormholes, - Acknowledgment Spoofing, - Intelligent Attack
Number of sent initialization packets	- Homing Attack, - Hello flood	*Link costs to the Base station,* *Distance to the base station*	- Sinkhole Attack, - Wormholes, - Acknowledgment Spoofing
Number of sent location packets	- Homing Attack	*Collision ratio*	- Jamming
Nodes in two different locations claim the same ID, *Number of newly added nodes to the network*	- Node Replication, - Sybil Attack	*Nodes' sleeping time,* *Cluster head lifetime*	- Node outage, - DoS Attack
Nodes' lost packets	- Sinkhole Attack, - Wormholes, - Acknowledgment Spoofing		

5. Attacks Avoidance Techniques

Instead of reacting after the attack occurrence and mitigating the attack effects, avoidance techniques give networks the ability to prevent the occurrence of such attacks. Avoidance techniques aim to save network resources before malicious nodes waste it. Therefore, many researchers proposed new techniques and protocols to avoid network attacks. For instance, Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) protocol provides a link layer technique to prevent the occurrence of collisions in the network and hence reduces the collision ratio. Upon decreasing the collision ratio, occurrence of the following attacks: Jamming, Exhaustion, and Denial of Service (DoS) will be avoided.

Deng et al. [44] proposed a dynamic threshold and adaptive detection technique based on CSMA/CA protocol. Another work made by Felix in [46], where he proposed a methodology to prevent the Distributed Denial-of-Service attack that is based on three steps which are infiltrating the remote control network, analyzing network data in detail, and finally shutting down the remote control network. In this way, the communication link between malicious nodes and the attacker will be disconnected.

kumar et al. [45] proposed a technique named "Delphi method" that tracks misbehaving nodes and forces these nodes to change current routing paths and selects an alternative path. This technique depends on the route discovery procedure and does not require clock synchronization, position information, nor special hardware. However, it cannot determine the exact attacker location.

Freiling et al. [46] proposed a technique that adds maximum allowed transmission distance property to packets; this ensures that the destination address is located within the allowed distance from the source node.

Another proposed technique by Kaushal et al. [47] that uses accurately synchronized clocks between the network nodes. This will lead to prior knowledge or estimation of packets arrival time at the destination node. If the receiver checked the packet timing and found a reasonable change and deviation from the estimated time, it raises the flag about a possibility that sender might be an attacker.

Another technique proposed in [34] is used to avoid the wormhole attack, it is based on the distance between network nodes. Authors used the round-trip signal time and signal speed to estimate the distance between nodes. Therefore, every node in the network will be aware of the suitable and the trusted shortest path.

Singh [36] proposed a cluster-based avoidance mechanism to avoid wormhole attack where they partitioned the network into 3-level hierarchical clusters, as illustrated in figure 15. Every node has a unique address; this address is based on the hierarchical structure of the network.

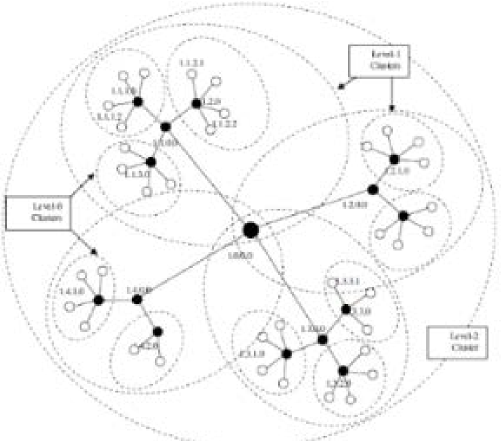

Figure 11. 3-levels clustered network

The proposed address schema gives network nodes the ability to determine a valid and shortest path to a specific node. So, if nodes received a packet of an invalid address in the route from source to destination, it raises a flag about that path. This approach does not require any special hardware nor accurately synchronized clocks between network nodes. It also does not depend on nodes' statistical data.

6. Open Research Issues

Although there are many of the mitigation for WSN attack, there are many of the open security problems. In this section, we briefly list some of these problems for future work.

1) Sensor nodes are still limited in terms of energy, memory, and processing capabilities. Therefore, for cryptographic techniques, especially private key operation where its generation is expensive, there is a need for elegant techniques for WSNs.
2) Sensors mobility is another challenge for WSNs security. In WSNs, either sensors, sink nodes, or both of them could be mobile. In fact, the current routing protocols are based on a stationary WSNs. Although, there are few trials for securing mobile WSNs as in [48][49][50][51][52], they are either designed for specific attacks or for general ad hoc networks with different network characteristics.
3) Nodes in WSNs are deployed in large numbers that could be hundreds or hundreds of thousands. This leads to scalability problem where there is a need for efficient security protocol that can deal with large scale nodes.
4) Most of the current security algorithms like μTESLA [53] and its successors [1][2] does not take synchronization into consideration while most of the protocols are based on synchronization among the node or between the nodes and the sink node.
5) WSNs are currently used with data stream including audio and video while the current security algorithms may focus on discrete events. Therefore, new security algorithms have to consider data stream in WSNs.
6) Security always comes with Quality of Service (QoS) issues. However, WSNs are used in much critical applications that require high-quality services. Thus, another issue to be considered in WSNs security is the QoS.

7. Conclusion

Due to the importance of sensor networks and its usage in many of the critical applications, it is very important to investigate their security. In fact, avoiding and/or mitigating sensor networks attacks on sensor networks is challenging due to the limited capabilities of the networks and their nodes. Therefore, the purpose of this paper is to review the current and up-to-date attacks on the sensor networks. In addition, it explores different mitigation methods that recently appeared in the literature. Moreover, one of the important contributions of this paper is the summarization of each attack characteristics and parameters. In the future, we plan to investigate the trust models used in sensor networks considering the different attacks presented in this paper.

References

[1] Qabulio, M. (2016). A Framework for Securing Mobile Wireless Sensor Networks against Physical Attacks. In 2016 International Conference on Emerging Technologies (ICET).

[2] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS : Security Protocols for Sensor Networks. Wireless Networks, 8(5), 521–534.

[3] Hu, Y., Perrig, A., & Johnson, D. B. (2006). Wormhole Attacks in Wireless Networks. IEEE Journal on Selected Areas in Communications , 24(2), 1–11.

[4] Schaller, P., Lafourcade, P., Basin, D., Capkun, S., & Hubaux, J. (2008). . Security in Mobile Ad Hoc and Sensor Netwok and Secure Neighborhood Discovery : A Fundamental Element for Mobile Ad Hoc Networking. Security in Mobile Ad Hoc and Sensor Netwoks, (February), 132–139.

[5] Ko, B. J., Lu, C., Srivastava, M. B., Stankovic, J. A., Ieee, F., Terzis, A., & Welsh, M. (2010). Wireless Sensor Networks for Healthcare. Proceedings of the IEEE, 98(11). https://doi.org/10.1016/j.comnet.2010.05.003

[6] Nouha Sghaier, Abdelhamid Mellouk, Brice Augustin, Yacine Amirat, Jean Marty, Mohamed El Amine Khoussa, Amine Abid, and R. Z. (2011). Wireless Sensor Networks for medical care services. In 7TH International Wireless Communications and Mobile Computing Confrence (IWCMC).

[7] Banerjee, S., & Majumder, K. (2014). Wormhole Attak Mitigtion in MANET : A. International Journal of Computer Networks & Communications (IJCNC), 6(1), 45–60.

[8] Barbagli, B., Bencini, L., Magrini, I., Manes, G., Marta, S., & Manes, A. (2011). A Real-Time Traffic Monitoring Based on Wireless Sensor Network Technologies. In Proc. 7th IWCMC (pp. 820–825).

[9] Hodge, V. J., Keefe, S. O., Weeks, M., & Moulds, A. (2015). Wireless Sensor Networks for Condition Monitoring in the Railway Industry : A Survey. IEEE Transactions on Intelligent Transportation Systems , 16(3), 1088–1106.

[10] Bolourchi, P., & Uysal, S. (2013). Forest Fire Detection in Wireless Sensor Network Using Fuzzy Logic. In 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks (pp. 83–87). https://doi.org/10.1109/CICSYN.2013.32

[11] Wemer-allen, G., Johnson, J., Ruid, M., Lees, J., & Welsh, M. (2005). Monitoring Volcanic Eruptions with a Wireless Sensor Network. In Proceedings of the Second European Workshop on Wireless Sensor Networks (EWSN',05).

[12] Zambrano, A., Perez, I., & Esteve, M. (2017). Quake Detection System Using Smartphone-Based Wireless Sensor Network For Early Warning. In The Fourth International Workshop on Pervasive Networks for Emergency Management, (Vol. 1995, pp. 297–302).

[13] Swagarya, G., Kaijage, S., & Sinde, R. S. (2014). A Survey on Wireless Sensor Networks Applications for Air Polution Monitoring . International Journal Of Engineering And Computer Science, 3(5).

[14] C. Oliveira, G. G. (2010). Environmental Monitoring Service and Wireless Sensor Networks applied on Urban Space. In 2010 IEEE International Conference on Automation Quality and Testing Robotics (AQTR), (pp. 228–230).

[15] Firdaus, F. (2014). Wireless Sensor Networks for Microclimate Telemonitoring using ZigBee and WiFi. In 2014 IEEE International Conference on Aerospace Electronics and Remote Sensing Technology (ICARES) (pp. 200–204).

[16] Collins, M., Simon, D., & Nixon, P. (2008). A Secure Lightweight Architecture for Wireless Sensor Networks. In Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM '08. https://doi.org/10.1109/UBICOMM.2008.65

[17] S, S. R., G, E. P. K., & B. Juswin Thilak. (2014). A Comprehensive Review on Reduction of Malicious Nodes in Clustered Wireless Sensor Networks Using Different Trust Management Schemes. International Journal of Innovative Research in Science, Engineering and Technology, 3(3).

[18] Anand, J., & Ece, P. G. S. (2013). Preserving National Animal using Wireless Sensor Network based Hotspot Algorithm. In Proceedings of 2013 International Conference on Green High Performance Computing.

[19] Sharma, K., & Ghose, M. K. (2009). Complete Security Framework for Wireless Sensor Networks. Int. Journal of Computer Science and Information Security, 3(1).

[20] Thaile, M., & Ramanaiah, O. B. V. (2016). Node Compromise Detection Based on NodeTrust in Wireless Sensor Networks. In International Conference on Computer Communication and Informatics(ICCCI -2016).

[21] Hi, E. L. S., Errig, A. D. P., & Niversity, C. A. M. E. U. (2004). Design Secure Sensor Netwoks. Wireless Communications Magazine, 6(11), 38–43.

[22] Pathan, A. K., Lee Hyung-woo, & Choong Seon Hong. (2006). Security in Wireless Sensor Networks : Issues and Challenges. In Proceedings of 8th IEEE ICACT 2006 (pp. 1043–1048). https://doi.org/10.1109/ICACT.2006.206151

[23] Umakanth, B., Damodhar, J., & Dt, K. (2013). Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks. International Journal of Engineering Trends and Technology (IJETT), 4(8), 3691–3695.

[24] Dubey, A., Jain, V., & Kumar, A. (2014). A Survey in Energy Drain Attacks and Their Countermeasures in Wireless Sensor Networks. International Journal of Engineering Research & Technology (IJERT), 3(2), 1206–1211.

[25] Znaidi, W., Minier, M., Babau, J., Znaidi, W., Minier, M., An, J. B., & Sensor, W. (2008). An Ontology for Attacks in Wireless Sensor Networks. Institute National de Recherche en Informatique et en Automatique.

[26] Agah, A., & Das, S. K. (2007). Preventing DoS Attacks in Wireless Sensor Networks : A Repeated Game Theory Approach. International Journal OfNetwork Security, 5(2), 145–153.

[27] Mohammadi, S., Atani, R. E., & Jadidoleslamy, H. (2011). A Comparison of Link Layer Attacks on Wireless Sensor Networks. Journal of Information Security, 2011(April), 69–84. https://doi.org/10.4236/jis.2011.22007

[28] Malik, M. Y. (2013). An Outline of Security in Wireless Sensor Networks : Threats , Countermeasures and Implementations. In Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management. https://doi.org/10.4018/978-1-4666-0101-7.ch024

[29] Demirbas, M., & Song, Y. (2006). An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks. In 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06). https://doi.org/10.1109/WOWMOM.2006.27

[30] Ngai, E. C. H., Liu, J., & Lyu, M. R. (2007). An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Computer Communctions, 30, 2353–2364. https://doi.org/10.1016/j.comcom.2007.04.025

[31] Ngai, E., Liu, J., & Lyu, M. (2006). On the intruder detection for sinkhole attack in wireless sensor networks. In ICC '06.

[32] Krontiris, I., Giannetsos, T., & Dimitriou, T. (2008). Launching a Sinkhole Attack in Wireless Sensor Networks ; the Intruder Side. In Proc. IEEE Int',l Conf. Wireless and Mobile Computing, Networking and Comm. (WIMOB ',08) (pp. 526–531).

[33] Liu, Q., Yin, J., Leung, V. C. M., & Cai, Z. (2013). FADE : Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs. IEEE Transactions on Wireless Communications , 12(10), 5124–5137.

[34] Pandey, J., & Deshmukh, A. (2016). Distributed Detection of Malicious Node in Wireless Sensor Network under Byzantine. International Journal of Innovative Research in Computer and Communication Engineering, 4(7), 14481–14490. https://doi.org/10.15680/IJIRCCE.2016.

[35] Renold, A. P., Poongothai, R., & Parthasarathy, R. (2012). Performance Analysis of LEACH with Gray Hole Attack in Wireless Sensor Networks. In 2012 International Conference on Computer Communication and Informatics.

[36] Singh, V. P., Jain, S., & Singhai, J. (2010). Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. IJCSI International Journal of Computer Science Issues, 7(3).

[37] Amish, P., & Vaghela, V. B. (2016). Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol. Procedia - Procedia Computer Science, 79, 700–707. https://doi.org/10.1016/j.procs.2016.03.092

[38] Lu, N., Sun, Y., Liu, H., & Li, S. (2018). Intrusion Detection System Based on Evolving Rules for Wireless Sensor Networks. Journal of Sensors, 2018. https://doi.org/10.1155/2018/5948146

[39] Sunilkumar, K. N. (2017). A Review on Security and Privacy Issues in Wireless Sensor Networks. In IEEE International Conference On Recent Trends In Electronics Information & Communication Technology (pp. 1979–1984).

[40] Buch, D., & Jinwala, D. (2011). Previntion of Wormhole Attack in Wireless Sensor Networks . International Journal of Network Security & Its Applications (IJNSA), 3(5), 85–98.

[41] Jakobsson, M., Wetzel, S., & Yener, B. (2003). Stealth Attacks on Ad-Hoc Wireless Networks. In Proceeding of IEEE VTC 2003 (pp. 2103–2111).

[42] Bankovi, Z., Vallejo, J. C., Fraga, D., & Moya, J. M. (2011). Detecting Bad-Mouthing Attacks on Reputation Systems Using Self-Organizing Maps. Lecture Notes in Computer Science., 1(6694), 9–16.

[43] Padmavathi, G. (2009). A Survey of Attacks , Security Mechanisms and Challenges in Wireless Sensor Networks. In) International Journal of Computer Science and Information Security (Vol. 4, pp. 1–9).

[44] Deng, J., Han, R., & Mishra, S. (2005). Defending against Path-based DoS Attacks in Wireless Sensor Networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. https://doi.org/10.1145/1102219.1102235

[45] Kumar, V., & Kumar, R. (2015). An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc. Procedia - Procedia Computer Science, 48(Iccc), 472–479. https://doi.org/10.1016/j.procs.2015.04.122

[46] Freiling, F. C., Holz, T., & Wicherski, G. (2005). Botnet Tracking : Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks. In 10th European Symposium on Research in Computer Security Milan (pp. 319–335).

[47] Kaushal, S., & Aggarwal, R. (2015). Avoidance of Wormhole Attack by using Delphi method. International Research Journal of Engineering and Technology (IRJET), 2(7), 1287–1292.

[48] Tylman, W. (2008). Misuse-Based Intrusion Detection Using Bayesian Networks. In Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2008 (pp. 203–210). https://doi.org/10.1109/DepCoS-RELCOMEX.2008.48

[49] Bairaktaris, K., & Spirakis, P. G. (2008). Adaptive Probabilistic Secure Routing in Mobile Wireless Sensor Networks. In 2008 16th International Conference on Software, Telecommunications and Computer Networks (Vol. 15964).

[50] Teng, L. (2010). SeRA : A Secure Routing Algorithm against Sinkhole Attacks for Mobile Wireless Sensor Networks. In 2010 Second International Conference on Computer Modeling and Simulation SeRA: https://doi.org/10.1109/ICCMS.2010.95

[51] Kumar, A. H., Sarma, D., Kar, B. A., Mall, C. R., & Member, S. (2011). Secure Routing Protocol for Mobile Wireless Sensor Network. In 2011 IEEE Sensors Applications Symposium.

[52] Bruce, N., & Lee, H. J. (2013). A Secure Authentication Protocol among Mobile Phone and Wireless Sensor Networl (s. In 2013 15th International Conference on Advanced Communications Technology (ICACT) (pp. 52–59).

[53] Qabulio, M., Malkani, Y. A., & Keerio, A. (2015). Securing Mobile Wireless Sensor Networks (WSNs) against Clone Node Attack. In 2015 Conference on Information Assurance and Cyber Security (CIACS) Securing (pp. 20–21).