Wireless Personal Communications (2022) 122:3687–3718
https://doi.org/10.1007/s11277-021-09107-6

# An analytical Survey of Attack Scenario Parameters on the Techniques of Attack Mitigation in WSN

**Karen Ávila[1] · Paul Sanmartin[2] · Daladier Jabba[1] · Javier Gómez[3]**

Accepted: 5 September 2021 / Published online: 25 September 2021


**Abstract**
Wireless sensor networks (WSN) were cataloged as one of the most important emerging technologies of the last century and are considered the basis of the Internet of Things paradigm. However, an undeniable disadvantage of WSN is that the resources available for these types of networks, such as processing capacity, memory, and battery, are usually in short supply. This limitation in resources implements security mechanisms a difficult task. This work reviews 93 recent proposals in which different solutions were formulated for the different attacks in WSN in the network layer; in total, 139 references were considered. According to the literature, these attacks are mainly Sybil, wormhole, sinkhole, and selective forwarding. The main goal of this contribution is to present the evaluation metrics used in the state of the art to mitigate the Sybil, wormhole, sinkhole, and selective forwarding attacks and show the network topologies used in each of these proposals.

**Keywords** Security · WSN · Attacks in wireless sensor networks · IoT · Sybil · Wormhole · Selective forwarding · Sinkhole

## 1 Introduction

Wireless sensors networks (WSN) have been very successful in the last decade; this is due to the many different areas in which they can be used and its impact on the Internet of Things paradigm (IoT). A wireless sensor network becomes one of the most important

✉ Paul Sanmartin
psanmartin@unisimonbolivar.edu.co

Karen Ávila
karena@uninorte.edu.co

Daladier Jabba
djabba@uninorte.edu.co

Javier Gómez
javiergo@comunidad.unam.mx

[1] Universidad del Norte, Barranquilla, Colombia

[2] Universidad Simon Bolivar, Barranquilla, Colombia

[3] Universidad Nacional Autónoma de México, Ciudad de México, México

ingredients of IoT applications [83]. One of the benefits of WSN is that they are adequate for monitoring environments with difficult access when human intervention is critical or is not possible [69]. The wireless sensor network is a set of independent sensors distributed in a region which is capable of sensing [17], that sensor nodes cooperate with each other for the collection, transmission, processing of monitoring data, etc [34, 136]. There are many areas in which WSN technology can be applied including agriculture, smart homes, care and health at home, transportation, shopping, among many others.

However WSN has a vulnerability that is an inherent part of the system and relates to the low processing capacity of the nodes or sensors [55, 90, 125], this shortcoming makes it difficult to implement algorithms that could potentially increase network security [55].

Additionally, this enormous growth has made software developers and hardware manufacturers forget a key element that is and will be important to the customers, as is the case with security and privacy. The main objective of this contribution is to show the network topologies used in the contributions focused on mitigating the sybil, wormhole, sinkhole, and selective forwarding attacks, as well as to present the evaluation metrics used in each of these proposals. The proposals analyzed correspond to the last 4 years only.

Based on the node role, WSN is divided into two groups, which are infrastructure and ad-hoc. Infrastructure types always have a leading node or parent, usually called a sink node or cluster head. Most of the time, the sink node has a higher processing capacity than the rest of the nodes in the network. This type of network is centralized. On the other hand, ad-hoc networks are decentralized networks, and the communication between the nodes is peer to peer. Figure 1 shows the different topologies that we can find in WSN depending on the role of each node.

Wireless sensor networks are the base for the IoT paradigm. Kevin Ashton proposed the concept of IoT in 1999, and referred to it as the connection and identification of objects in

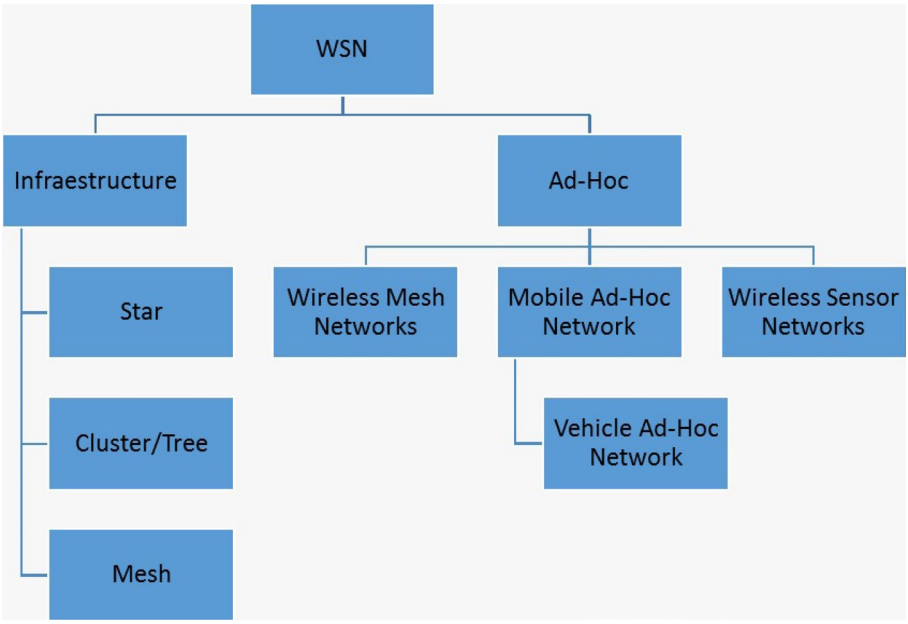



**Fig. 1** WSN Topologies

a unique and interoperable way with a radio frequency identification technology (RFID) [6]. Thanks to this technology, appliances, vehicles, sensors, etc., would have the ability to connect to the Internet, and as the consequence, it becomes possible to remotely manipulate these objects, through a computer, tablet or cell [51]. In many cases, IoT uses RPL (IPv6 Routing Protocol for LLNs) [104, 105, 131] as a routing protocol. The IoT paradigm is expected to focus more and more on cybercriminals because more and more devices are connected to the Internet, which is a challenge for experts and security companies. The enormous growth of the IoT paradigm, however, has historically forgotten a key element for their customers related to the management of security and privacy of information. Cybercriminals might take advantage of the vulnerabilities of devices connected to obtain a privileged position within corporate networks and hardware to which they are connected. The rest of the paper is organized as follows. In Sect. 2, the IoT architecture is specified. Section 3 shows the main areas implementing IoT solutions. Section 4 presents an analysis of the main existing security threats in view of the OSI model. Section 5 explains the main attacks on the network layer. Section 6 presents a literature review about the literary production of the last four years regarding the types of attack presented in Sect. 5. Finally, Sect. 7 concludes the document.

## 2 WSN and IoT Architecture

### 2.1 WSN Architecture

Most of the architectures designed in WSN follow the OSI Model. According to [3], a sensor network needs five layers: physical, data link, network, transport, and application layer. To these 5 layers, 3 more layers have been added to work transversally, as seen in Fig. 2. These new three layers are used to manage the network and make the sensors work together, increasing the overall of the network [3]. These layers are:

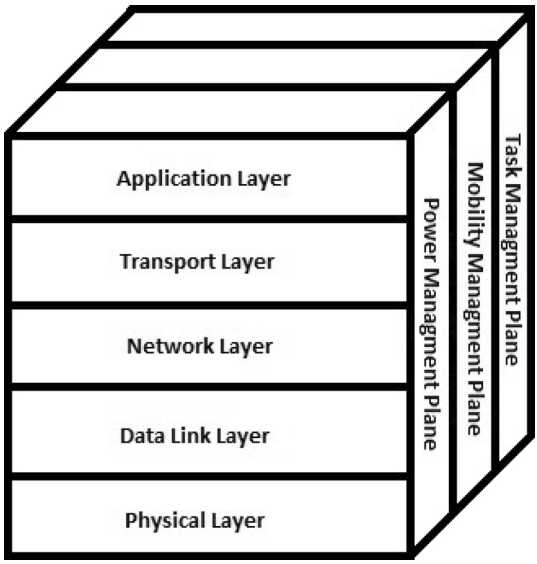



**Fig. 2** The architecture of WSN [3]

- Task Management Plane: needed to balance and schedule the sensing tasks given to a specific region.
- Mobility Management Plane: needed to detect and register the movement of sensor nodes. A route back to the user is always maintained, and the sensor nodes can keep track of who is their neighbor sensor nodes.
- Power Management Plane: needed to manage how a sensor node uses its power.

The difference between OSI and WSN are shown in Table 1, according to [10].

There are different routing protocols proposed in the literature in the network layer [68, 72, 137]. Some of them work the clustering approach with low energy consumption, as presented in [137]. Although they solve the routing problem, all these protocols are considered vulnerable since they handle wireless connections, and the transmission medium allows intruder attacks. This article seeks to present an analysis of topologies used in the design of WSN networks to analyze the vulnerabilities presented in this layer in future work.

### 2.2 IoT Architecture

As mentioned above, one of the bases of IoT is the WSN. For this reason, they inherit part of its architecture, making some changes in the organization of the layers in order to provide the required services. The architecture in WSN is based on 5 layers. In IoT, these layers are grouped into only 3, as detailed below.

According to the literature, the proposed architectures based on IoT are divided into 3 layers [47, 48, 88], Fig. 3 summarizes these layers:

- Perception layer: its main task is to gather information and its architecture consists of different sensors, gateways, RFID tags, barcode, etc.
- Network layer: it is composed of different types of networks: wired, wireless, private, public, etc. This is because the IoT concept based is based on heterogeneous networks. Its main task is to propagate and process information collected in the perception layer.
- Application layer: this layer is composed of various input/output interfaces and users. The related user interfaces and services are always based on the characteristics of the applications as such, that is an intelligent transport system, environmental monitoring, remote medical system, etc.

**Table 1** Wireless Sensor Networks and OSI Model

| Wireless Sensor Networks | OSI Model |
|---|---|
| WSN Application | Application Layer |
| WSN Middleware | Presentation Layer |
| None | Session Layer |
| WSN Transport Protocols | Transport Layer |
| WSN Routing Protocols | Network layer |
| Error Control—WSN MAC Protocols | Data Link Layer |
| Transceiver | Physical Layer |

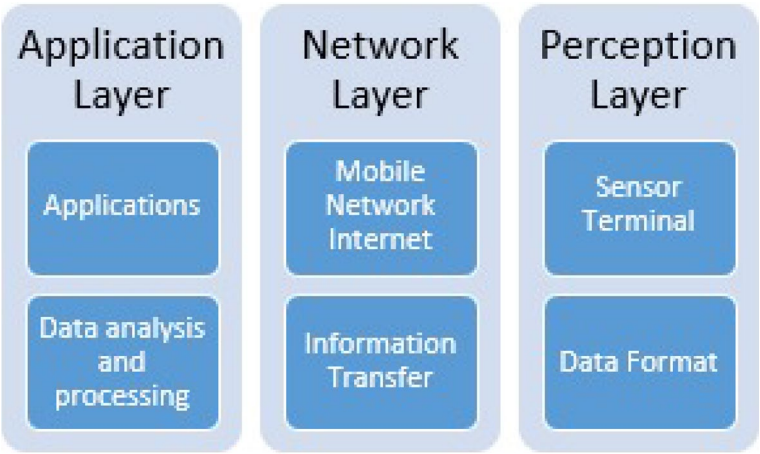



**Fig. 3** The architecture of IoT [88]

The perception layer in IoT consists of data capture and its format, grouping the link and physical layers of WSN. The network layer includes all the technologies and mechanisms used to transmit captured data, which groups the network and transport layers in WSN. Finally, the application layer in IoT is the data processing and the applications that make it possible to visualize them, which corresponds to the application layer in WSN.

## 3 Applications Based on WSN and IoT

Many areas can benefit from solutions based on the internet of things, in this review we include the areas of health and care at home, shopping, logistics and transportation, cities and smart homes.

### 3.1 Health and Home Care

Health and home care are some of the most important areas for IoT applications since it is directly related to the lives of people. In this area, there are all the solutions designed to improve the quality of life of patients, or in the effective and immediate communication between a patient and his family doctor. There are proposals in which the patients have devices attached to their bodies that constantly make readings of their vital signs (sugar, pressure, variables related to the functioning of the heart, etc.) generating alerts to medical staff if there are unusual values [16]. The various applications of IoT focused on health can be categorized in offering the following services [81, 123]:

- Telemedicine [40]: remote medical care-patient.
- Emergency [19]: ambulance.
- Medication and intelligent pharmaceutical packages [82]: verification taking medication by the patient.
- Social networks [41, 87, 106]: based on health.
- Home health [138]: Remote and personalized attention.

- Biomedical devices [22, 23, 63]: body sensors.

### 3.2 Shopping

Customer satisfaction is the main objective of a commercial organization. The implementation of solutions based on the Internet of Things paradigm can be used for the fulfillment of this objective. One of these proposals might be to ease the location of a given product in the store prior description. The authors of [96] propose a prediction scheme for the location of articles, based on current and previous locations, in which the objective is to locate products in the shopping store. On the other hand, the authors of [26] propose a system based on barcode and RFID technology to improve the shopping experience and provide the customer with the required information of the desired product.

### 3.3 Logistics and Transport

Logistics and transportation is an area with an increase in business solutions. It is important for employers to predict transport routes that optimize package delivery time, for example, fuel-saving routes. In the same way, devices have emerged in the market that allow to immediately know the data collected from vehicles, such as gasoline level, location, speed, etc. The authors of [122] propose a solution in which users can see in real time the availability of seats in public transport in order to avoid the agglomeration in the transport system. In [130] the authors propose a model of "intelligent logistic transport" to support the supply chain system.

### 3.4 Smart City

Smart cities are also a growing area of research within the internet of things paradigm. An intelligent city is one that is capable of adequately responding to the basic needs of institutions, companies, and citizens themselves, both economically and operationally, socially and environmentally. An example of a solution in this area would be the autonomous management of semaphores according to the current vehicular flow. In [45] the architecture of a middleware based on IoT is implemented and acts as a communication layer between the heterogeneous systems of a city, giving the authorities control over the infrastructure and collected data. Another example is the proposed research explained in [120], which describes a system for the management and reservation of parking spaces of vehicles in a city.

### 3.5 Smart Home

A smart home, in addition to providing comfort, can influence energy savings. This is done by installing sensors to make decisions and to detect certain behaviors, or home care, which goes very closely with the area of health and home care. Inside a smart home, people can control remote devices such as lights, curtains, appliances, etc. In [89] a pattern recognition system of human activities is proposed with the support of multiple devices, to be used for people with signs of Alzheimer's. In [35] authors design a smart home automation system turning a customary home to a smart home for accessing and controlling devices and appliances remotely, using Android based Smartphone applications.

## 4 Security Threats

One of the fundamental bases of IoT is the WSN, with the consequence that security problems presented in WSN are transferred to IoT. In this section, the main threats for each of the layers of the OSI model are discussed. Security controls in WSN should be designed taking into account each of the network components. On many occasions, security in the system is considered as an independent aspect of the architecture [88], which is a wrong approach. The security in a system must be considered from the beginning, taking into account security along all the other network components. As mentioned in the previous section, real-time monitoring is one key advantage of sensor networks once sensor nodes are connected to the Internet. Maintaining data confidentiality in WSN is important, but maintaining a secure architecture and topology is also necessary. Achieving both tasks simultaneously is a complex design problem given the wireless transmission medium used by WSN [132, 133] and the low processing capacity of the sensors. One key security goal of WSN is to ensure data security. This implies security requirements such as confidentiality, integrity, authenticity, and availability of all messages [50, 78].

- Confidentiality: It refers to the privacy of data and resources. Should ensure that the data disclosed do not reach unauthorized destinations.
- Integrity: It refers to the reliability of the data or resources.
- Authenticity: The goal is the authentication of all participants in the transmission and/or the data itself.
- Availability: Ability to use data or resources.
- Freshness: It refers to the frequency in which data is captured in order to have updated information.

Table 2 summarizes by layer which are the attacks to which the sensor networks are exposed.

Traditional wireless networks do not have as many limitations as WSN, which is why the implementation of security mechanisms is not an easy task [44], and many authors ignore this aspect in their proposals. The wireless sensor network, as compared to traditional computer networks, has certain limitations that are highlighted in [124], including:

- Limited resources: in many cases, the implementation of a secure mechanism requires the availability of certain resources, such as memory and power, however, these resources are limited in a wireless sensor network.

**Table 2** Attacks relevant to security in WSNl

| Layers | Attack |
|---|---|
| Application Layer | Fake, malicious data |
| Transport Layer | Flood, replay attacks |
| Network layer | Sybil, wormholes, sinkhole, selective forwarding |
| Link Layer | Collision attack |
| Physical Layer | Interference |

- Unreliable communication: this covers the reliability of received packets, the conflicts in the transmission, and network latency (total time delays).
- Unattended operation: a node cannot perform its function in the network for long periods of time; therefore, they may be exposed to physical attacks and/or remote management. Likewise, the decentralized operation of nodes involves greater organization of the network.

Next, we will discuss the attacks that may occur in the network layer according to [86].

## 5 Attacks on the Network Layer

The transmission medium is one of the reasons why wireless networks are vulnerable to certain types of attacks [57]. In general, a wired network is more secure than a wireless network. Features such as useful life, processing capacity, etc., significantly affect the security of the network. If a wireless network is composed of nodes with low processing capacity and useful lifetime, this network may be compromised. This is why WSN are even more vulnerable to attacks than traditional wireless networks. WNS typically cannot implement complex defense mechanisms because they can significantly affect the network's useful lifetime. In addition to other vulnerabilities related to the environment in which the WSN is deployed, this environment can become a hostile and dangerous place [57]. There are different security solutions that counteract the problems mentioned above. In this paper, we analyze different attacks (in the network layer) that can occur in wireless sensor networks as well as the network topologies being proposed during the attacks. We also analyzed the evaluation metrics implemented by the authors. The attacks analyzed in this paper are sybil, wormhole, sinkhole, and SF.

### 5.1 Sybil Attacks

The objective of this attack is to attract traffic to malicious nodes, and away from legitimate nodes. This attack is achieved by stealing the identity of legitimate nodes [57] can occur in two ways, causing a node to be in several places at the same time, or that the same node represents several nodes. This attack implies a modification in the routing tables. Different solution methods have been proposed for this attack [9, 11, 12, 18, 27, 32, 42, 43, 52, 58, 61, 62, 64, 67, 69, 71, 79, 80, 91–95, 97, 98, 101, 102, 107, 109–112, 134, 139], 34 proposals in total.

### 5.2 Wormhole Attack

A wormhole attack destroys the network topology. This attack infiltrates the network of 2 or more illegitimate nodes which send messages to each other using low latency and high bandwidth channel, which becomes attractive to legitimate nodes, causing them to use a compromised transmission medium. Different solution methods have been proposed for this attack [1, 8, 14, 20, 20, 21, 25, 28, 29, 33, 39, 44, 52, 56, 58, 59, 70, 84, 85, 108, 117, 118, 121, 126, 127, 129, 140], 27 proposals in total.

### 5.3 Sinkhole Attack

The goal of a sinkhole attack is to attract network traffic to a specific node, this is achieved by altering the routing tables of the network. Once the traffic arrives at the malicious node, the messages can be modified or deleted. Different solution methods have been proposed for this attack [5, 24, 36–38, 49, 53, 54, 60, 99, 103, 114–116, 119, 128, 129], 17 proposals in total.

### 5.4 Selective Forwarding

A SF attack occurs when a malicious node receives a packet and decides to resend it to a different node than the recipient of that message. Different solution methods have been proposed for this attack [2, 4, 7, 13, 30, 31, 46, 65, 66, 73–77, 100–102, 113, 135, 141], 20 proposals in total.

## 6 Network Topologies

The analysis presented in the following section includes the network topologies used in the revised proposals. For this reason, before entering the analysis, a brief description of each of them will be made. The topology of a network is a graphic description of how the nodes of the network are connected. There are several types of topology, star, tree, cluster, or mixed. With the technological advancements, it is common to find mixed topologies generated by MANET or VANET networks in which nodes must have the intelligence to redistribute their topology given their constant movement.

Figure 4 shows the most common types of topology, which are described below: Fig. 4a: Star Topology, where there is a central node, and the others are directly connected to it. Figure 4b: Tree topology, where there is a sink in which the other nodes are connected to it through a direct link or some route. Figure 4c: Cluster topology, where several groups are evidenced within the same network, in which each group has its sink node. Figure 4d: Mixed topology in which 2 or more topologies are agreed.

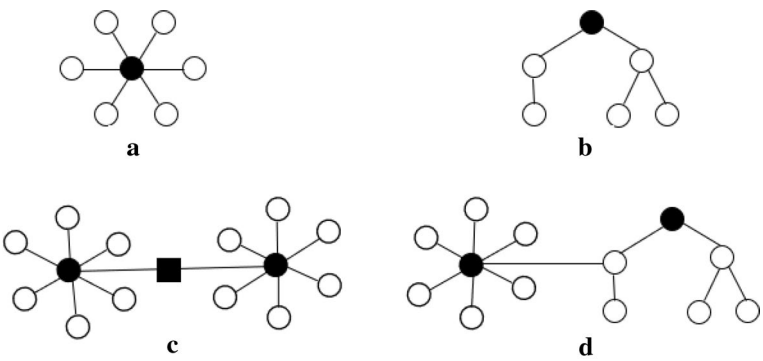



**Fig. 4** Topologies

## 7 Analysis of Proposals

In this section, we analyze the proposals that mitigate each one of the attacks evaluated in this revision. The analysis identifies aspects such as the topology implemented, if the proposal evaluates the detection of intruders or if the proposal detects or prevents the attack, as well as the metrics used for the evaluation of each of proposal. Among the proposals analyzed, there are different evaluation metrics used by the authors. These metrics include packet delivery ratio (PDR), forwarding misbehaviors, power consumption, time detection, latency, accuracy detection/detection rate, network lifetime, throughput, packet loss rate, delay, data transmitted, data packet overhead or computational overhead, collision avoidance, bit error rate, jitter, number of encryptions, the impact of signatures, position accuracy, exchange message, impact of attack frequency, the average localization errors of different average network connectivity, distance bounding and comparison of Intrusion Warning Score (IWS) at different motes. Figure 5 shows the distribution of attacks with a total of 93 proposals reviewed. It is important to mention that 5 of the proposals included in this revision mitigate more than one attack. These proposals are [52, 58, 101, 102, 129].

The attack that is the most popular with researchers is the Sybil attack, with 34 proposals. Likewise, the less popular one is the sinkhole attack, with 17 proposals. Table 3 shows the different network topologies that were found in these proposals. Figure 6 associates these topologies with each evaluated proposal.

According to Fig. 7, the most used topology by the authors is tree topology, also known as cluster or hierarchical. This topology accounts to 49.46 %, or what is the same to 46/93 proposals. Then follow Ad-Hoc WSN, MANET, VANET, Mesh, and Ad-Hoc WMN topologies which were used in 18, 17, 9, 2, and 1 proposal, respectively. With respect to the sources and databases consulted, 4 databases were used, they were IEEE, Science Direct, Springer and Google Scholar. Figure 6 shows the distribution of the proposals analyzed with their respective source.

Figure 7 shows that the largest reference source for this review was IEEE, followed by Google Scholar, Science Direct, and Springer. In these sources, keywords like "security in WSN", "attacks in WSN", "sybil attack WSN ", "wormhole attack WSN ", "sinkhole attack WSN ", "selective forwarding attack WSN " were used. For the purposes of this paper, only the last 4 years, from 2014, were taken into account and only those articles that proposed a new mechanism, scheme or protocol that mitigated each of these attacks mentioned before were selected.

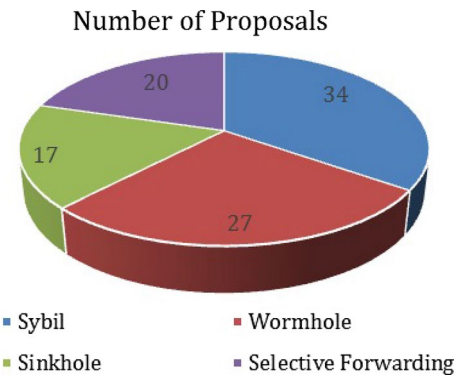



**Fig. 5** Number of proposals in the last 4 years

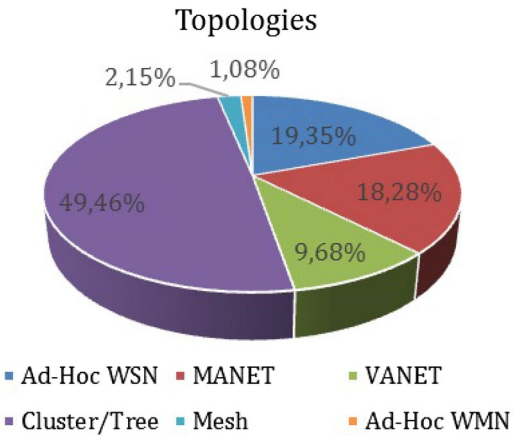



**Fig. 6** Topologies used by the authors

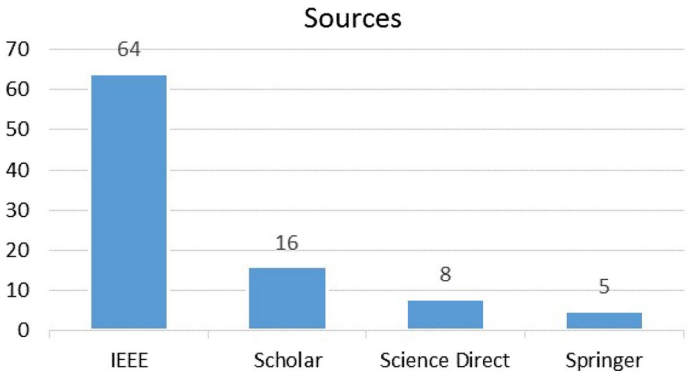



**Fig. 7** Reference sources

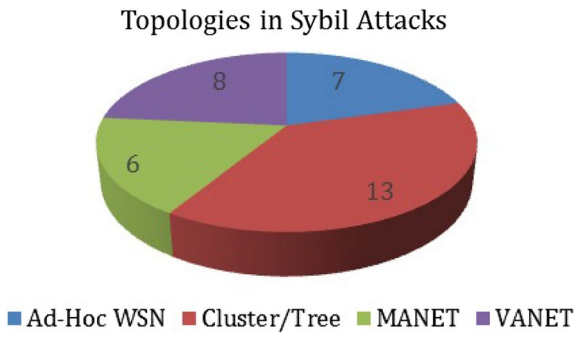



**Fig. 8** Topologies in sybil attack

### 7.1 Sybil Attacks

In this section, only the proposals that mitigate the sybil attack were analyzed. Figure 8 shows the distribution of the proposals that mitigate sybil attacks in terms of the

network topology used by the authors. The topologies used in these 34 proposals were Ad-Hoc WSN, cluster/tree, MANET and VANET being cluster/tree the most popular among researchers.

Table 3 shows the topologies used by each proposal, whether the proposal makes an analysis or takes into account the detection of false positives, and also if the proposal detects and prevents the sybil attack.

**Table 3** Detect and prevent technics in sybil attacks

| Paper | Topology | Analysis of false positives | Detect | Prevent |
|---|---|---|---|---|
| [101] | Cluster/Tree | No | No | Yes |
| [11] | Cluster/Tree | Yes | Yes | No |
| [97] | Cluster/Tree | No | No | No |
| [18] | Cluster/Tree | No | Yes | No |
| [98] | VANET | No | Yes | No |
| [15] | Ad-Hoc WSN | No | Yes | Yes |
| [111] | Cluster/Tree | Yes | Yes | No |
| [52] | Cluster/Tree | Yes | Yes | No |
| [62] | VANET | Yes | Yes | Yes |
| [62] | Cluster/Tree | No | Yes | No |
| [64] | MANET | No | Yes | Yes |
| [42] | Cluster/Tree | No | Yes | Yes |
| [9] | VANET | No | Yes | Yes |
| [67] | MANET | Yes | Yes | Yes |
| [94] | Cluster/Tree | Yes | Yes | No |
| [79] | MANET | Yes | Yes | Yes |
| [107] | VANET | No | Yes | Yes |
| [109] | VANET | No | Yes | Yes |
| [71] | MANET | No | Yes | Yes |
| [102] | Ad-Hoc WSN | No | Yes | Yes |
| [91] | Cluster/Tree | Yes | Yes | No |
| [58] | Ad-Hoc WSN | No | Yes | No |
| [61] | Ad-Hoc WSN | No | Yes | Yes |
| [112] | Ad-Hoc WSN | Yes | Yes | No |
| [80] | Cluster/Tree | No | Yes | No |
| [93] | Ad-Hoc WSN | Yes | Yes | No |
| [139] | MANET | No | No | Yes |
| [32] | VANET | Yes | Yes | No |
| [95] | VANET | No | Yes | Yes |
| [134] | VANET | Yes | Yes | Yes |
| [12] | Cluster/Tree | Yes | Yes | No |
| [92] | Cluster/Tree | No | Yes | No |
| [43] | Ad-Hoc WSN | No | Yes | Yes |
| [110] | MANET | Yes | Yes | No |

Figure 9 summarizes Table II and quantifies the last 3 columns. The 91,2% of the proposals detect the sybil attack, the 41,2% include in their proposal the detection of false positives, and 50% prevents the sybil attack.

Table 4 details the proposals that used each of the metrics found throughout this bibliographic review. The most used metric to evaluate the proposals that mitigate the sybil attack is the Accuracy Detection/Detection Rate, which is used by 17 proposals.

Figure 10 details the number of evaluation metrics used by authors whose proposals mitigate sybil attacks. 5 proposals [52, 71, 79, 98, 102] used 4 evaluation metrics, this was the highest number used. 2 proposals [80, 95] do not use evaluation metrics.

### 7.2 Wormhole Attack

In this section, only the proposals that mitigate the wormhole attack were analyzed. Figure 11 shows the distribution of the proposals that mitigate the wormhole attacks in terms of the network topology used by the authors. The topologies used in these 27 proposals were Ad-Hoc WSN, cluster/tree, MANET, mesh, and VANET being cluster/tree the most popular.

Table 5 shows the topologies used by each proposal, if this proposal makes an analysis or takes into account the detection of false positives, and also if the proposal detects and prevents the wormhole attack.

Figure 12 summarizes Table IV and quantifies the last 3 columns. The 96,29% of the proposals detect the wormhole attack, the 25,9% include in their proposal the detection of false positives and the 66,6% prevents the wormhole attack.

Table 6 shows which the different metrics found throughout this bibliographic review used by each proposal. The most used metric that mitigates the wormhole attack is the PDR used by 16 proposals.

Figure 13 shows the number of evaluation metrics used by authors whose proposals mitigate wormhole attacks. 6 proposals [85, 91, 108, 117, 127, 129] used 4 evaluation metrics. 2 proposals [8, 84] do not use evaluation metrics.

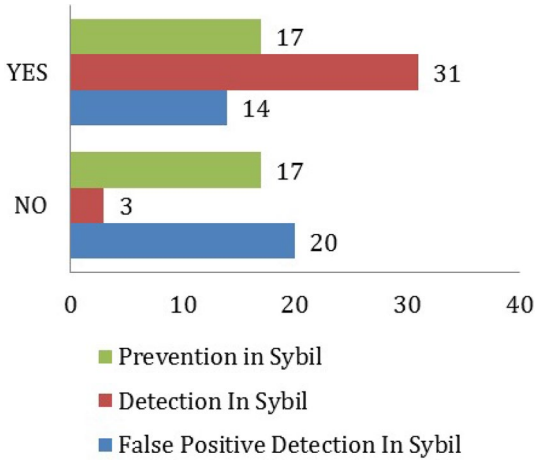



**Fig. 9** Detection and prevention in sybil attack

**Table 4** Metrics in sybil attacks

| Evaluation Metrics | Paper |
|---|---|
| Packet Delivery Ratio (PDR) | [52, 58, 92, 101, 102, 109] |
| Forwarding Misbehaviors | No one |
| Power Consumption | [12, 42, 43, 52, 71, 92, 101, 102, 111, 139] |
| Time Detection | [91] |
| Latency | No one |
| Accuracy Detection/Detection Rate | [11, 12, 15, 32, 43, 52, 62, 67, 79, 91, 93, 94, 102, 110–112, 134] |
| Network Lifetime | [42, 97, 111] |
| Throughput | [52, 58, 61, 67, 71, 79, 93, 98] |
| Packet Loss Rate | [79, 98] |
| Delay | [62, 71, 93, 107, 109] |
| Data Transmitted | [18, 98] |
| Data packet Overhead or Computational Overhead | [12, 18, 62, 79, 102] |
| Collision Avoidance | [98] |
| Bit Error Rate | [71] |
| Jitter | No one |
| Number of Encryption | [64] |
| Impact of Signatures | [9] |
| Position Accuracy | No one |
| Exchange Message | No one |
| Impact of attack frequency | [27] |
| The average localization errors of different average network connectivity | No one |
| Distance bounding | No one |
| Comparison of IWS at different motes | No one |

### 7.3 Sinkhole Attack

In this section, only the proposals that mitigate the sinkhole attack were analyzed. Figure 14 shows the distribution of the proposals that mitigate sinkhole attacks in terms of the network topology used by the authors. The topologies used in these 17 proposals were Ad-Hoc WSN, cluster/tree, and MANET. By far the most used topology was cluster/tree.

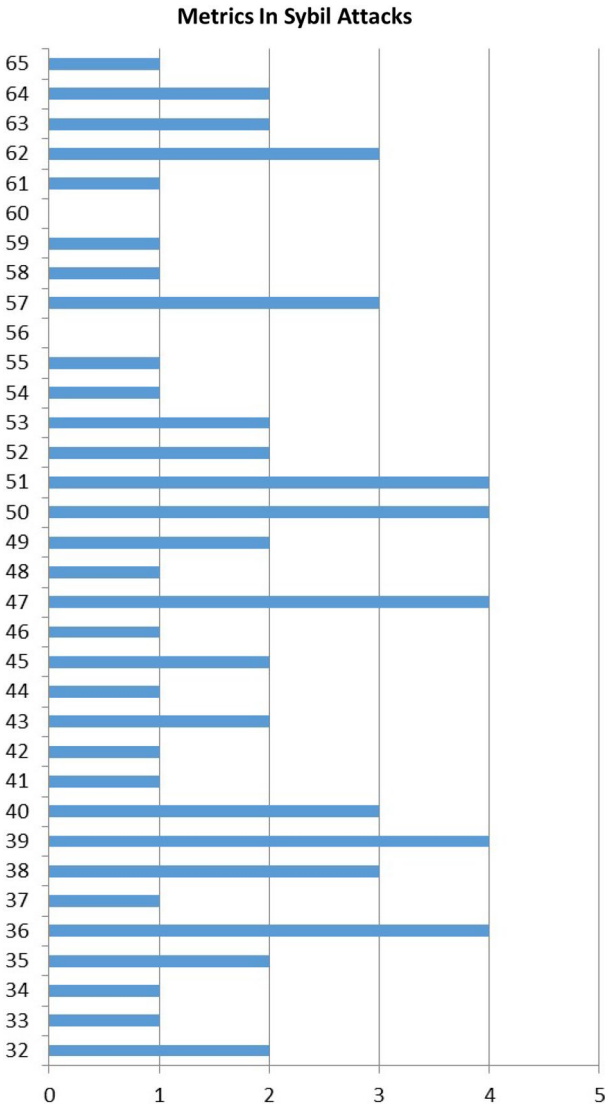
Table 7 shows the topologies used by each proposal, if this proposal makes an analysis or takes into account the detection of false positives, and also if the proposal detects and prevents the sinkhole attack.

Figure 15 summarizes Table IV and quantifies the last 3 columns. The 100% of the proposals detect the sinkhole attack, 52,9% include in their proposal the detection of false positives and the 41,2% prevents the sinkhole attack.

Table 8 shows which of the metrics found throughout this bibliographic review was used by each proposal. The most used metric to mitigate the sinkhole attack is the PDR, which is used by 8 proposals.

Figure 16 shows the number of evaluation metrics used by authors whose proposals mitigate sinkhole attacks. 1 proposal [115] used 6 evaluation metrics, being this the highest number used by any proposal.

**Fig. 10** Metrics in Sybil attack




### 7.4 Selective Forwarding Attack

In this section, only the proposals that mitigate the sinkhole attack were analyzed. Figure 17 shows the distribution of the proposals that mitigate SF attacks in terms of the network topology used by the authors. The topologies used in these 20 proposals include Ad-Hoc WMN, Ad-Hoc WSN, cluster/tree, MANET, and mesh. Again cluster/tree was the most popular used topology.

Table 9 shows the different topologies used by each proposal, whether the proposal makes an analysis or takes into account the detection of false positives, and also if it detects and prevents the SF attack.

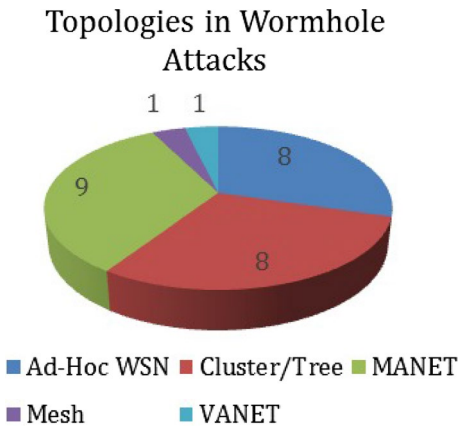



**Fig. 11** Topologies in wormhole attack

**Table 5** Detect and prevent technics in wormhole attacks

| Paper | Topology | Analysis of false positives | Detect | Prevent |
|---|---|---|---|---|
| [52] | Cluster/Tree | Yes | Yes | No |
| [58] | Ad-Hoc WSN | No | Yes | No |
| [25] | Ad-Hoc WSN | Yes | Yes | No |
| [28] | Cluster/Tree | No | Yes | No |
| [44] | Ad-Hoc WSN | No | Yes | No |
| [14] | MANET | No | Yes | Yes |
| [84] | MANET | No | Yes | Yes |
| [117] | MANET | Yes | Yes | Yes |
| [1] | MANET | Yes | Yes | Yes |
| [56] | MANET | No | Yes | Yes |
| [20] | Ad-Hoc WSN | No | Yes | Yes |
| [33] | MANET | No | Yes | Yes |
| [39] | MANET | No | Yes | Yes |
| [59] | Cluster/Tree | No | Yes | No |
| [118] | MANET | Yes | Yes | No |
| [85] | Mesh | No | Yes | Yes |
| [8] | VANET | No | No | Yes |
| [121] | MANET | No | Yes | Yes |
| [29] | Cluster/Tree | No | Yes | Yes |
| [140] | Ad-Hoc WSN | No | Yes | No |
| [127] | Cluster/Tree | Yes | Yes | Yes |
| [108] | Ad-Hoc WSN | No | Yes | No |
| [126] | Ad-Hoc WSN | No | Yes | Yes |
| [20] | Ad-Hoc WSN | No | Yes | Yes |
| [21] | Cluster/Tree | No | Yes | Yes |
| [70] | Cluster/Tree | No | Yes | Yes |
| [129] | Cluster/Tree | Yes | Yes | Yes |

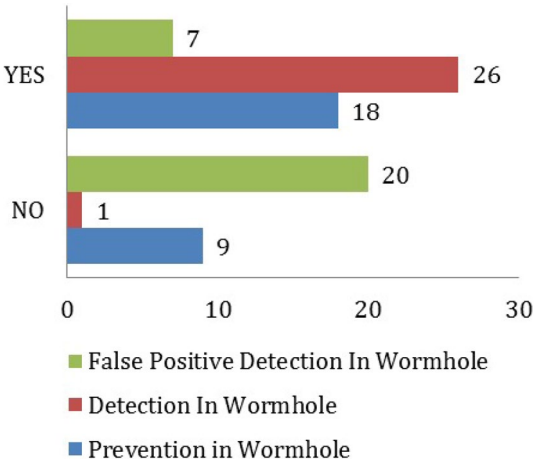



**Fig. 12** Detection and prevention in wormhole attack

**Table 6** Metrics in wormhole attacks

| Evaluation Metrics | Paper |
|---|---|
| Packet Delivery Ratio (PDR) | [1, 14, 20, 20, 28, 29, 33, 52, 56, 58, 59, 85, 108, 117, 121, 129] |
| Forwarding Misbehaviors | No one |
| Power Consumption | [15, 59] |
| Time Detection | No one |
| Latency | No one |
| Accuracy Detection/Detection Rate | [1, 25, 44, 52, 117, 118, 127, 129] |
| Network Lifetime | No one |
| Throughput | [20, 28, 29, 33, 39, 52, 56, 58, 85, 108, 117, 121, 127, 129] |
| Packet Loss Rate | [1, 25] |
| Delay | [14, 20, 20, 28, 29, 56, 85, 108, 117, 121, 127, 129] |
| Data Transmitted | [127] |
| Data packet Overhead or Computational Overhead | [85] |
| Collision Avoidance | No one |
| Bit Error Rate | No one |
| Jitter | [108] |
| Number of Encryptation | No one |
| Impact of Signatures | No one |
| Position Accuracy | [108] |
| Exchange Message | [21] |
| Impact of attack frequency | No one |
| The average localization errors of different average network connectivity | [140] |
| Distance bounding | [70] |
| Comparison of IWS at different motes | No one |

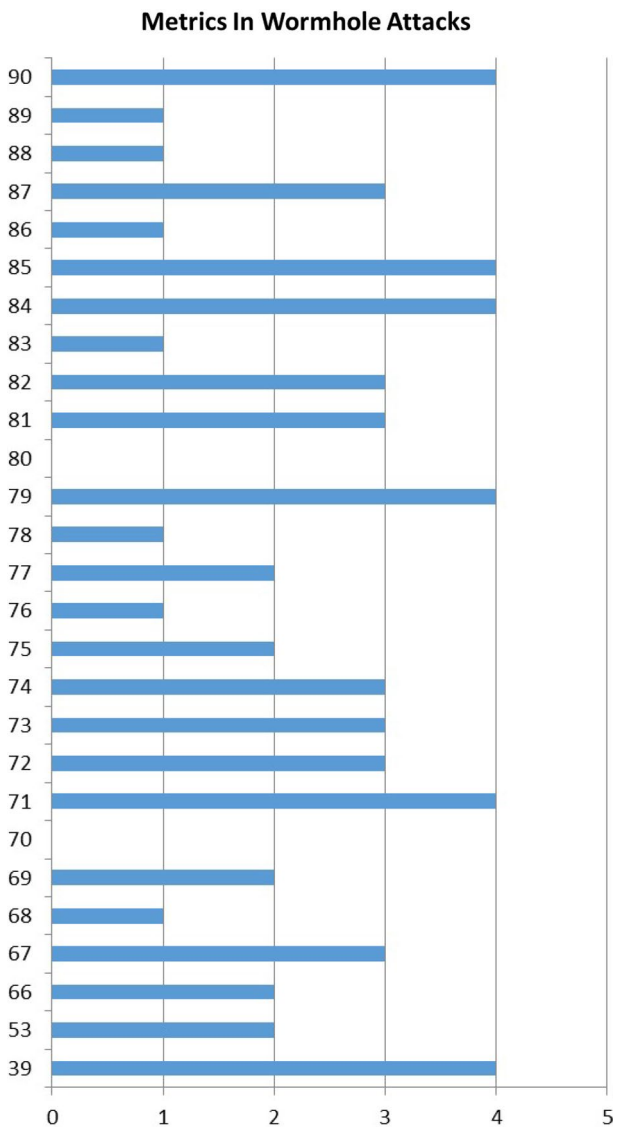



**Fig. 13** Metrics in wormhole attack

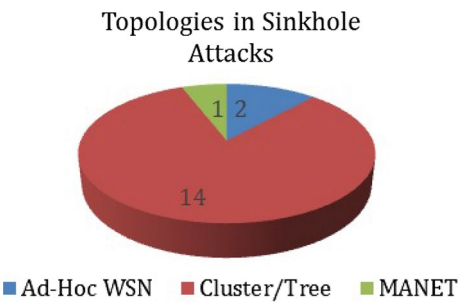



**Fig. 14** Topologies in sinkhole attack

**Table 7** Detect and prevent technics in sinkhole attacks

| Paper | Topology | Analysis of false positives | Detect | Prevent |
|---|---|---|---|---|
| [129] | Cluster/Tree | Yes | Yes | Yes |
| [5] | Cluster/Tree | Yes | Yes | No |
| [114] | Cluster/Tree | Yes | Yes | No |
| [37] | MANET | Yes | Yes | No |
| [116] | Cluster/Tree | No | Yes | Yes |
| [24] | Cluster/Tree | Yes | Yes | No |
| [103] | Cluster/Tree | No | Yes | No |
| [99] | Cluster/Tree | No | Yes | Yes |
| [53] | Cluster/Tree | No | Yes | No |
| [49] | Cluster/Tree | No | Yes | No |
| [115] | Cluster/Tree | No | Yes | No |
| [36] | Cluster/Tree | Yes | Yes | Yes |
| [54] | Ad-Hoc WSN | Yes | Yes | Yes |
| [119] | Ad-Hoc WSN | No | Yes | Yes |
| [128] | Cluster/Tree | Yes | Yes | Yes |
| [60] | Cluster/Tree | No | Yes | No |
| [38] | Cluster/Tree | Yes | Yes | No |

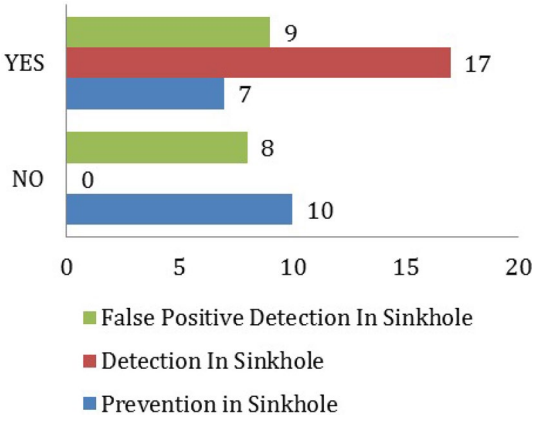



**Fig. 15** Detection and prevention in sinkhole attack

Figure 18 summarizes Table VIII and quantifies the last 3 columns. 85% of proposals detect the SF attack, 25% include the detection of false positives and 35% prevents the SF attack.

Table 10 shows which of the metrics found throughout this bibliographic review were used by each proposal. The most used metric to mitigate the sybil attack is power consumption, in fact, 12 proposals used this metric.

Figure 19 shows the number of metrics used by authors whose proposals mitigate SF attacks. 1 proposal [102] used 4 evaluation metrics, being this the highest number used by any metric.

**Table 8** Metrics in sinkhole attacks

| Evaluation Metrics | Paper |
|---|---|
| Packet Delivery Ratio (PDR) | [24, 38, 49, 54, 103, 115, 128, 129]] |
| Forwarding Misbehaviors | [60] |
| Power Consumption | [37, 38, 49, 114, 115, 119, 128] |
| Time Detection | [60] |
| Latency | No one |
| Accuracy Detection/Detection Rate | [24, 36, 37, 54, 128, 129] |
| Network Lifetime | [114, 115] |
| Throughput | [38, 49, 53, 103, 115, 128, 129] |
| Packet Loss Rate | [53, 54, 99, 115, 116] |
| Delay | [38, 49, 53, 54, 99, 128, 129] |
| Data Transmitted | No one |
| Data packet Overhead or Computational Overhead | [115] |
| Collision Avoidance | No one |
| Bit Error Rate | No one |
| Jitter | No one |
| Number of Encryptation | No one |
| Impact of Signatures | No one |
| Position Accuracy | No one |
| Exchange Message | No one |
| Impact of attack frequency | No one |
| The average localization errors of different average network connectivity | No one |
| Distance bounding | No one |
| Comparison of IWS at different motes | [5] |

## 8 Future Work

Future work is expected to identify vulnerabilities in wireless sensor networks inherited from the Internet of Things technology. These vulnerabilities can generate attacks in the network layer allowing access to confidential information of unauthorized people. Identifying these attacks in the network layer would lead us to the implementation of strategies that can mitigate that.

## 9 Conclutions

This paper presents an analysis of the relevant attacks in WSN focused on IoT. The IoT model is considered to be a heterogeneous network object, and one of the networks that are part of this heterogeneity is the WSN. It is important to highlight this type of analysis because of its benefits, disadvantages, and security problems that IoT inherited from WSN. Given the analysis presented in Sect. 6, several conclusions can be made: the most used topology is the tree or cluster, with a total of 46 proposals. The most used metric employed as a mechanism to evaluate their proposals is the detection accuracy,

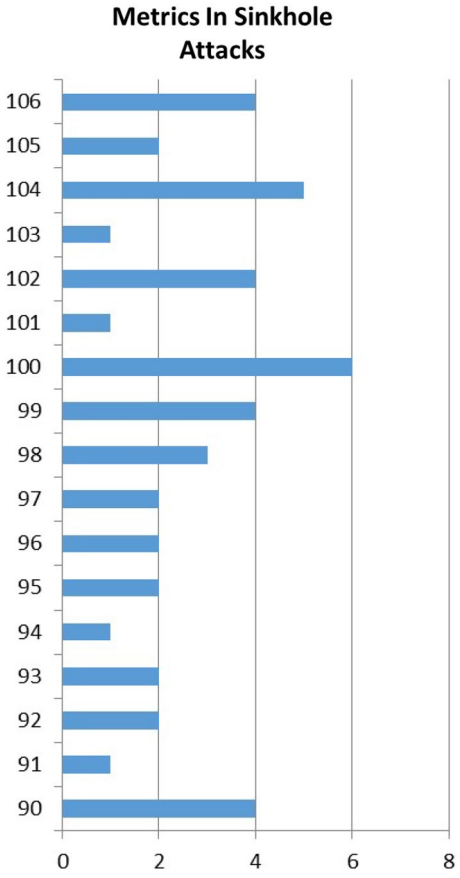



**Fig. 16** Metrics in sinkhole attack

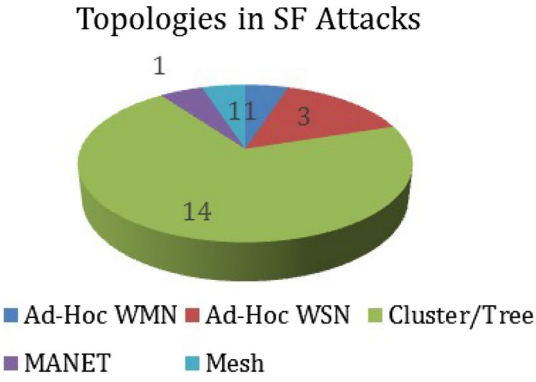



**Fig. 17** Topologies in SF attack

which is used by 34 proposals. This work also highlights the importance of including security mechanisms from the very beginning of the design of the topology of the network, these mechanisms cannot be treated in an exclusive manner. Finally, as a concluding remark, it is clear that it is time to give more importance to the area of security in

**Table 9** Detect and prevent technics in sinkhole attacks

| Paper | Topology | Analysis of false positives | Detect | Prevent |
|---|---|---|---|---|
| [99] | Ad-Hoc WMN | No | Yes | No |
| [73] | Cluster/Tree | No | Yes | No |
| [4] | Ad-Hoc WSN | No | Yes | No |
| [101] | Cluster/Tree | No | No | Yes |
| [75] | Cluster/Tree | No | Yes | No |
| [74] | Cluster/Tree | No | Yes | No |
| [100] | MANET | No | Yes | No |
| [65] | Cluster/Tree | Yes | Yes | No |
| [30] | Cluster/Tree | No | No | Yes |
| [141] | Cluster/Tree | Yes | Yes | No |
| [13] | Mesh | No | Yes | No |
| [2] | Cluster/Tree | No | Yes | Yes |
| [113] | Ad-Hoc WSN | No | Yes | No |
| [46] | Cluster/Tree | No | Yes | No |
| [76] | Cluster/Tree | Yes | Yes | Yes |
| [135] | Cluster/Tree | Yes | Yes | Yes |
| [31] | Cluster/Tree | Yes | Yes | No |
| [77] | Cluster/Tree | No | No | Yes |
| [7] | Cluster/Tree | No | Yes | No |
| [102] | Ad-Hoc WSN | No | Yes | Yes |

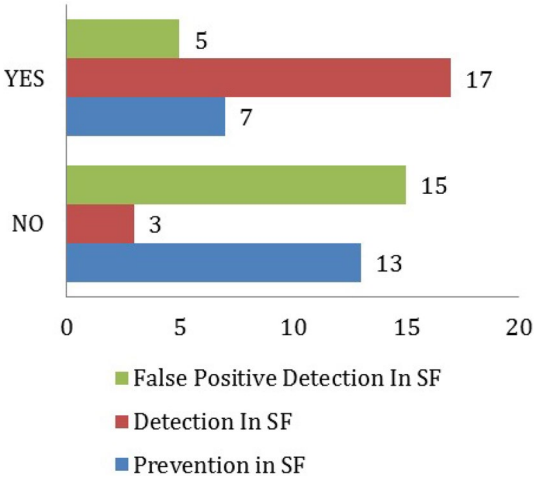


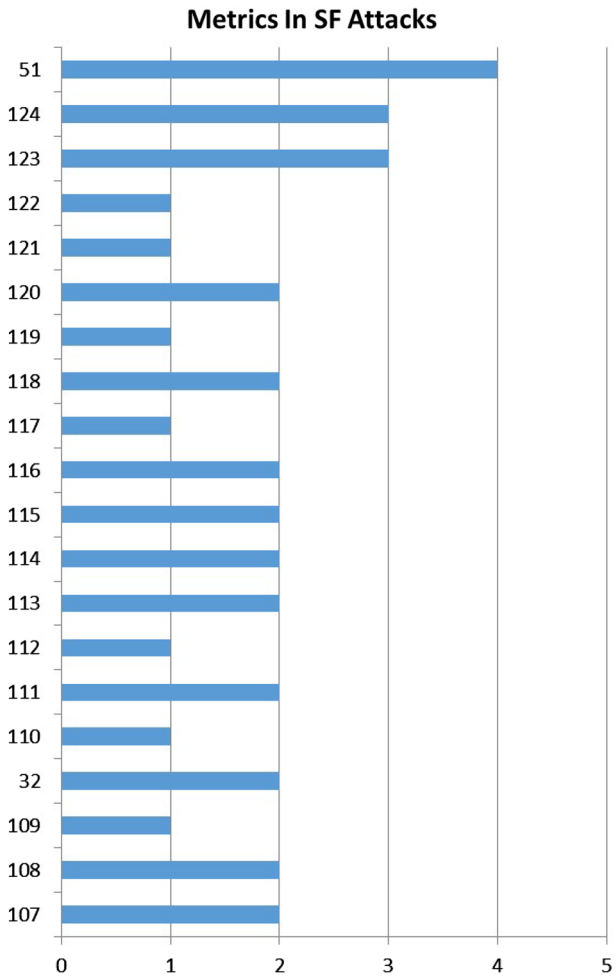

**Fig. 18** Detection and prevention in SF attack

the networks of sensors and the internet of things given their recent growth and the applications emerging around this paradigm.

**Table 10** Metrics in sinkhole attacks

| Evaluation Metrics | Paper |
|---|---|
| Packet Delivery Ratio (PDR) | [2, 13, 65, 66, 101, 102, 113] |
| Forwarding Misbehaviors | [66] |
| Power Consumption | [4, 7, 46, 65, 73, 74, 76, 77, 101, 102, 113, 141] |
| Time Detection | [73] |
| Latency | [75, 76] |
| Accuracy Detection/Detection Rate | [31, 74, 100, 102, 135] |
| Network Lifetime | [7, 30, 65, 141] |
| Throughput | [13] |
| Packet Loss Rate | [77, 102] |
| Delay | [7, 77] |
| Data Transmitted | No one |
| Data packet Overhead or Computational Overhead | No one |
| Collision Avoidance | No one |
| Bit Error Rate | No one |
| Jitter | No one |
| Number of Encryptation | No one |
| Impact of Signatures | No one |
| Position Accuracy | No one |
| Exchange Message | No one |
| Impact of attack frequency | No one |
| The average localization errors of different average network connectivity | No one |
| Distance bounding | No one |
| Comparison of IWS at different motes | No one |

**Fig. 19** Metrics in SF attack




**Funding** This work was supported by Universidad del Norte and Universidad Simón Bolívar.

## Declarations

**Conflict of interest** The author(s) declared no potential conflicts of interest concerning the research, authorship, and/or publication of this article.

## References


1. Acharjee, T., Borah, P., & Roy, S. A new hybrid algorithm to eliminate wormhole attack in wireless mesh networks. In *2015 International conference on computational intelligence and communication networks (CICN)*, pp. 997–1002.
2. Acharya, D., Agrwal, S., Sharma, P., Gupta, S. K., & Ghrera, S. P. (2016). *Performance Analysis of Detection Technique for Select Forwarding Attack on WSN*. 2016 fourth international conference on parallel, distributed and grid computing.
3. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422.
4. Alajmi, N. M., & Elleithy, K. M. (2015). Selective forwarding detection (sfd) in wireless sensor networks. *Systems, Applications and Technology Conference (LISAT)* (pp. 1–5). IEEE: IEEE Long Island.
5. Alam, A., Eyers, D., & Huang, Z. Y. (2015). Helping Secure Robots in WSN Environments by Monitoring WSN Software Updates for Intrusions. In *Proceedings of the 2015 6th International Conference on Automation, Robotics and Applications*.
6. Albrecht, K., & Michael, K. (2013). Connected: To everyone and everything [guest editorial: Special section on sensors]. *Technology and Society Magazine, IEEE, 32*(4), 31–34.
7. Alghamdi, W. Y., Wu, H., Kanhere, S. S., & Ieee. . (2017). Reliable and Secure End-to-End Data Aggregation Using Secret Sharing in WSNs. IEEE. *Wireless Communications and Networking Conference.*
8. Ali, S., Nand, P., & Tiwari, S. Secure message broadcasting in vanet over wormhole attack by using cryptographic technique. In *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 520–523.
9. Alimohammadi, M., & Pouyan, A. A. Sybil attack detection using a low cost short group signature in vanet. In *2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, pp. 23–28.
10. Alkhatib, A. A. A., & Baicher, G. S. Wireless sensor network architecture.
11. Alsaedi, N., Hashim, F., Sali, A., & Ieee. (2015). *Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks*. 2015 Ieee 12th Malaysia International Conference on Communications.
12. Alsaedi, N., Hashim, F., Sali, A., & Rokhani, F. Z. (2017). Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ets). *Computer Communications, 110*, 75–82.
13. Anand, C., & Gnanamurthy, R. K. (2016). Localized dos attack detection architecture for reliable data transmission over wireless sensor network. *Wireless Personal Communications, 90*(2), 847–859.
14. Anwar, R. W., Bakhtiari, M., Zainal, A., Abdullah, A. H., & Qureshi, K. N. Enhanced trust aware routing against wormhole attacks in wireless sensor networks. In *2015 International Conference on Smart Sensors and Application (ICSSA)*, pp. 56–59.
15. Atayero, A. A., Ilori, O. A., & Adedokun, M. O. (2015). Development of FIGA: A Novel Trust-Based Algorithm for Securing Autonomous Interactions in WSN. Lecture Notes in Engineering and Computer. *Science* 174–180.
16. Avila, K., Sanmartin, P., Jabba, D., & Jimeno, M. (2017). Applications based on service-oriented architecture (soa) in the field of home healthcare. *Sensors, 17*, 8.
17. Ayyappan, B., & Kumar, P. M. (2017). Security protocols in wsn: A survey. In *2017 Third International Conference on Science Technology Engineering and Management (ICONSTEM)* (2017), pp. 301–304.
18. Banerjee, P., Chatterjee, T., & DasBit, S. . Lo. E. N. A. (2015). *LoENA: Low-overhead Encryption based Node Authentication in WSN*. 2015 International Conference on Advances in Computing, Communications and Informatics.
19. Beltrame, F. (1997). Worldwide emergency telemedicine services: The randd eu projects perspective. In *Information Technology Applications in Biomedicine, ITAB '97., Proceedings of the IEEE Engineering in Medicine and Biology Society Region 8 International Conference*, IEEE, pp. 3–6.
20. Bhagat, S., & Panse, T. A detection and prevention of wormhole attack in homogeneous wireless sensor network. In *2016 International Conference on ICT in Business Industry and Government (ICTBIG)*, pp. 1–6.
21. Bilal, M., & Kang, S. G. (2017). An authentication protocol for future sensor networks. *Sensors, 17*, 5.
22. Cavalleri, M., & Reni, G. (2008). Active monitoring insole: A wearable device for monitoring foot load distribution in home-care context. In *Engineering in Medicine and Biology Society, EMBS 2008. 30th Annual International Conference of the IEEE*, pp. 4447–4450.

23. Cerutti, S., Magenes, G., & Bonato, P. (2010). Guest editorial special section on smart wearable devices for human health and protection. *Information Technology in Biomedicine, IEEE Transactions on, 14*(3), 691–693.
24. Cervantes, C., Poplade, D., Nogueira, M., & Santos, A. Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 606–611.
25. Chen, T., Huang, H., Chen, Z., Wu, Y., & Jiang, H. A secure routing mechanism against wormhole attack in ipv6-based wireless sensor networks. In *2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, pp. 110–115.
26. Dhauta, S., & Kapoor, S. Interactive intellegent shopping cart using rfid and zigbee modules. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 764–769.
27. Dong, W., & Liu, X. (2015). Robust and secure time-synchronization against sybil attacks for sensor networks. *IEEE Transactions on Industrial Informatics, 11*(6), 1482–1491.
28. Dutta, C. B., & Biswas, U. (2015). *Intrusion Detection System for Power-Aware OLSR*. 2015 International Conference on Computational Intelligence and Networks.
29. Dutta, C. B., & Biswas, U. (2015). Specification based IDS for Camouflaging Wormhole Attack in OLSR. *Mediterranean Conference on Control and Automation.,* 960–966.
30. Elhoseny, M., Yuan, X. H., El-Minir, H. K., & Riad, A. M. (2016). An energy efficient encryption method for secure dynamic wsn. *Security and Communication Networks, 9*(13), 2024–2031.
31. Gara, F., Saad, L. B., & Ayed, R. B. An intrusion detection system for selective forwarding attack in ipv6-based mobile wsns. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 276–281.
32. Garip, M. T., Kim, P. H., Reiher, P., & Gerla, M. Interloc: An interference-aware rssi-based localization and sybil attack detection mechanism for vehicular ad hoc networks. In *2017 14th IEEE Annual Consumer Communications and Networking Conference (CCNC)*, pp. 1–6.
33. Ghayvat, H., Pandya, S., Shah, S., Mukhopadhyay, S. C., Yap, M. H., & Wandra, K. H. Advanced aodv approach for efficient detection and mitigation of wormhole attack in manet. In *2016 10th International Conference on Sensing Technology (ICST)*, pp. 1–6.
34. Gomez, J., Campbell, A. T., Naghshineh, M., & Bisdikian, C. (2001). Conserving transmission power in wireless ad hoc networks. In *Proceedings Ninth International Conference on Network Protocols. ICNP 2001* (2001), pp. 24–34.
35. Govindraj, V., Sathiyanarayanan, M., & Abubakar, B. Customary homes to smart homes using internet of things (iot) and mobile application. In *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, pp. 1059–1063.
36. Grgic, K., Zagar, D., & Cik, V. K. (2016). System for malicious node detection in ipv6-based wireless sensor networks. *Journal of Sensors*
37. Guerroumi, M., Derhab, A., & Saleem, K. Intrusion detection system against sink hole attack in wireless sensor networks with mobile sink. In *2015 12th International Conference on Information Technology - New Generations*, pp. 307–313.
38. Gunasekaran, M., & Periakaruppan, S.. Ga.-dosld. (2017). Genetic algorithm based denial-of-sleep attack detection in wsn. Security and Communication. *Networks*
39. Gupta, C., & Pathak, P. Movement based or neighbor based tehnique for preventing wormhole attack in manet. In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, pp. 1–5.
40. Hailay, D., & Roine, R. (2002). Systematic review of evidence for the benefits of telemedicine. *Journal of Telemedicine and Telecare, 8,* 1–77.
41. Hwang, K. O., Ottenbacher, A. J., Green, A. P., Cannon-Diehl, M. R., Richardson, O., Bernstam, E. V., & Thomas, E. J. (2010). Social support in an internet weight loss community. *International Journal of Medical Informatics, 79*(1), 5–13.
42. Jan, M. A., Nanda, P., He, X., & Liu, R. P. A sybil attack detection scheme for a centralized clustering-based hierarchical network. In *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 318–325.
43. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2018). A sybil attack detection scheme for a forest wildfire monitoring application. *Future Generation Computer Systems, 80*, 613–626.
44. Jao, M. H., Hsieh, M. H., He, K. H., Liu, D. H., Kuo, S. Y., Chu, T. H., Chou, Y. H., & Ieee. (2015). *A Wormhole Attacks Detection using a QTS algorithm with MA in WSN*. IEEE International Conference on Systems Man and Cybernetics Conference Proceedings. 2015, pp. 20–25.
45. Joseph, T., Jenu, R., Assis, A. K., Kumar, V. A. S., Sasi, P. M., & Alexander, G. Iot middleware for smart city: (an integrated and centrally managed iot middleware for smart city). In *2017 IEEE Region 10 Symposium (TENSYMP)*, pp. 1–5.

46. Joshi, J., Awasthi, P., Mukherjee, S., Kumar, R., Kurian, D. S., Deka, M. J., & Ieee, S. E. E. D. (2016). *SEED: Secure and Energy Efficient Data Transmission in Wireless Sensor Networks*. 2016 4th International Conference on Information and Communication Technology.
47. Ju, Z., & Li, Y. (2011) Analysis on internet of things (iot) based on the "subway supermarket" e-commerce mode of tesco. In *Information Management, Innovation Management and Industrial Engineering (ICIII), International Conference on*, vol. 2, IEEE, pp. 430–433.
48. Kai, Z., & Lina, G. (2013). A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 9th International Conference on*, pp. 663–667.
49. Kalnoor, G., Agarkhed, J., & Ieee. (2016). *QoS based Multipath Routing for Intrusion Detection of Sinkhole Attack in Wireless Sensor Networks*. Proceedings of Ieee International Conference on Circuit, Power and Computing Technologies.
50. Kannan, V., & Ahmed, S. A resource perspective to wireless sensor network security. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on*, IEEE, pp. 94–99.
51. Kanuparthi, A., Karri, R., & Addepalli, S. Hardware and embedded security in the context of internet of things. In *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 61–65.
52. Katiravan, J., Duraipandian, N., & Dharini, N. (2015). A two level detection of routing layer attacks in hierarchical wireless sensor networks using learning based energy prediction. *Ksii Transactions on Internet and Information Systems, 9*(11), 4644–4661.
53. Kaur, M., & Singh, A. Detection and mitigation of sinkhole attack in wireless sensor network. In *2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*, pp. 217–221.
54. Keerthana, G., & Padmavathi, G. (2016). Detecting sinkhole attack in wireless sensor network using enhanced particle swarm optimization technique. *International Journal of Security and its Applications, 10*(3), 41–54.
55. Khan, S., Lloret, J., Song, H., & Du, Q. (2017). Qos based cooperative communications and security mechanisms for ad hoc sensor networks. *Journal of Sensors*.
56. Khobragade, S., Padiya, P. (2016). Detection prevention of wormhole attack based on delay per hop technique for wireless mobile ad-hoc network. In *International Conference on Signal Processing* (pp. 1332–1339). Power and Embedded System (SCOPES): Communication.
57. Kulkarni, G., Shelk, R., Gaikwad, K., Solanke, V., Gujar, S., & Khatawkar, P. Wireless sensor network security threats. In *Communication and Computing (ARTCom 2013), Fifth International Conference on Advances in Recent Technologies in*, IET, pp. 131–135.
58. Kumar, N. M. S., Deepa, S., Marimuthu, C. N., Eswari, T., & Lavanya, S. (2016). Signature based vulnerability detection over wireless sensor network for reliable data transmission. *Wireless Personal Communications, 87*(2), 431–442.
59. Kurmi, J., Singar Verma, R., & Soni, S. (2017). *An Efficient and Reliable Methodology for Wormhole Attack Detection in Wireless Sensor Network*, vol. 10.
60. Kurniawan, M. T., Yazid, S., & Ieee. (2017). *Mitigation Strategy of Sinkhole Attack In Wireless Sensor Network*. 2017 International Workshop on Big Data and Information Security.
61. Lakhanpal, R., & Sharma, S. Detection and prevention of sybil attack in ad hoc network using hybrid map and mac technique. In *2016 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC)*, pp. 283–287.
62. Lal, A. S., & Nair, R. Region authority based collaborative scheme to detect sybil attacks in vanet. In *2015 International Conference on Control Communication and Computing India (ICCC)*, pp. 664–668.
63. Lei, Y., Chungui, L., & Sen, T. (2011). Community medical network (cmn): Architecture and implementation. In *Mobile Congress (GMC), lobal*, pp. 1–6.
64. Li, P., & Lu, R. A sybil attack detection scheme for privacy-preserving mobile social networks. In *2015 10th International Conference on Information, Communications and Signal Processing (ICICS)*, pp. 1–5.
65. Liao, H. M., & Ding, S. F. (2015). Mixed and continuous strategy monitor-forward game based selective forwarding solution in wsn. *International Journal of Distributed Sensor Networks*
66. Lim, S., & Huie, L. (2015). Hop-by-hop cooperative detection of selective forwarding attacks in energy harvesting wireless sensor networks. In *Computing, Networking and Communications (ICNC), International Conference on*, IEEE, pp. 315–319.
67. Liu, Y., Bild, D. R., Dick, R. P., Mao, Z. M., & Wallach, D. S. (2015). The mason test: A defense against sybil attacks in wireless networks without trusted authorities. *IEEE Transactions on Mobile Computing, 14*(11), 2376–2391.

68. Loscri, V., Morabito, G., & Marano, S. (1999). A two-levels hierarchy for low-energy adaptive clustering hierarchy (tl-leach). In *IEEE vehicular technology conference* (2005), vol. 62, IEEE; p. 1809.
69. Low, K. S., Win, W. N. N., & Er, M. J. Wireless sensor networks for industrial environments. vol. 2, IEEE, pp. 271–276.
70. Luo, H. G., Su, J., Wen, G. J., & Ieee. (2017). A novel multi-hop distance-bounding protocol used in wireless sensor networks. *IEEE Global Communications Conference*.
71. Mahajan, S., Dahiya, N., & Kumar, D. A mechanism of preventing sybil attack in manet using bacterial foraging optimization. In *2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)*, pp. 1–5.
72. Manjeshwar, A., & Agrawal, D. P. (2001). Teen: Arouting protocol for enhanced efficiency in wireless sensor networks. *International Parallel and Distributed Processing Symposium 1*, 189.
73. Mathur, A., & Newe, T. (2015). *Medical WSN: Power, Routing and Selective Forwarding Defense*. Proceedings of the 13th International Conference on Telecommunications Contel 2015.
74. Mathur, A., Newe, T., & Ieee. (2015). *Medical WSN: Defense for Selective Forwarding Attack*. International Conference on Sensing Technology. pp. 54–58.
75. Mathur, A., Newe, T., & Rao, M. (2015). *Healthcare WSN: Cluster Elections and Selective Forwarding Defense*. 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies.
76. Mathur, A., Newe, T., & Rao, M. (2016). Defence against black hole and selective forwarding attacks for medical wsns in the iot. *Sensors, 16*, 1.
77. Mezrag, F., Bitam, S., Mellouk, A., & Ieee. (2017). Secure routing in cluster-based wireless sensor networks. In *IEEE Global Communications Conference (GLOBECOM)* IEEE Global Communications Conference.
78. Montoya, G., Velásquez-Villada, C., & Donoso, Y. (2013). Energy optimization in mobile wireless sensor networks with mobile targets achieving efficient coverage for critical applications. *International Journal of Computers Communications and Control, 8*,.
79. Moradi, S., & Alavi, M. A distributed method based on mobile agent to detect sybil attacks in wireless sensor networks. In *2016 Eighth International Conference on Information and Knowledge Technology (IKT)*, pp. 276–280.
80. Nalawade, A., Bharne, S., & Mane, V. Enhanced vote trust algorithm for sybil detection. In *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, pp. 399–403.
81. PANG, Z. (2013). Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being. *Thesis*
82. Pang, Z., Tian, J., & Chen, Q. Intelligent packaging and intelligent medicine box for medication management towards the internet-of-things. In *International Conference on Advanced Communication Technology, ICACT*, pp. 352–360.
83. Park, J., Gofman, M., Wu, F., & Choi, Y.-H. (2016). Challenges of wireless sensor networks for internet of thing applications. *International Journal of Distributed Sensor Networks, 12*(8), 1550147716665506.
84. Patel, A., Patel, N., & Patel, R. Defending against wormhole attack in manet. In *2015 Fifth International Conference on Communication Systems and Network Technologies*, pp. 674–678.
85. Patel, B. D., & Patel, A. D. A trust based solution for detection of network layer attacks in sensor networks. In *2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*, pp. 121–126.
86. Patel, M. M., & Aggarwal, A. (2013). Security attacks in wireless sensor networks: A survey. In *Intelligent Systems and Signal Processing (ISSP), International Conference on*, IEEE, pp. 329–333.
87. Patrick, K., Marshall, S. J., Davila, E. P., Kolodziejczyk, J. K., Fowler, J. H., Calfas, K. J., Huang, J. S., Rock, C. L., Griswold, W. G., Gupta, A., Merchant, G., Norman, G. J., Raab, F., Donohue, M. C., Fogg, B. J., & Robinson, T. N. (2014). Design and implementation of a randomized controlled social and mobile weight loss trial for young adults (project smart). *Contemporary Clinical Trials, 37*(1), 10–18.
88. Peng, S., Academy, B. D. C. C., Shen, H., Academy, . S. . T. C. C., and 573082406@qq.com. Security technology analysis of iot. 401–408.
89. Perumal, T., Chui, Y. L., Ahmadon, M. A. B., & Yamaguchi, S. Iot based activity recognition among smart home residents. In *2017 IEEE 6th Global Conference on Consumer Electronics (GCCE)*, pp. 1–2.

90. Pongle, P., & Chavan, G. (2015). A survey: Attacks on rpl and 6lowpan in iot. In *Pervasive Computing (ICPC), International Conference on*, pp. 1–6.
91. Prathap, U., Shenoy, P. D., Venugopal, K. R., & Ieee, C. M. N. T. S. (2016). *CMNTS:Catching Malicious Nodes with Trust Support in Wireless Sensor Networks*. 2016 Ieee Region 10 Symposium.
92. Raja, K. N., & Beno, M. M. (2017). Secure data aggregation in wireless sensor network-fujisaki okamoto(fo) authentication scheme against sybil attack. *Journal of Medical Systems, 41*(7), 6.
93. Rajan, A., Jithish, J., & Sankaran, S. Sybil attack in iot: Modelling and defenses. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 2323–2327.
94. Rashidibajgan, S. A trust structure for detection of sybil attacks in opportunistic networks. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 347–351.
95. Reddy, D. S., Bapuji, V., Govardhan, A., & Sarma, S. S. V. N. Sybil attack detection technique using session key certificate in vehicular ad hoc networks. In *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, pp. 1–5.
96. Rezazadeh, J., Sandrasegaran, K., & Kong, X. A location-based smart shopping system with iot technology. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pp. 748–753.
97. Roopashree, H. R., Kanavalli, A., & Ieee, S. T. R. E. E. (2015). *STREE: A Secured Tree based Routing with Energy Efficiency in Wireless Sensor Network*. Proceedings of the International Conference on Computing and Communications Technologies.
98. Saggi, M. K., Kaur, R., & Ieee. . (2015). Isolation of Sybil Attack in VANET using Neighboring Information. *IEEE International Advance Computing Conference.,* 33–38.
99. Saghar, K., Tariq, M., Kendall, D., & Bouridane, A. (2016). RAEED: A Formally Verified Solution to Resolve Sinkhole Attack in Wireless Sensor Network. *International Bhurban Conference on Applied Sciences and Technology.,* 334–345.
100. Sajjad, S. M., Bouk, S. H., & Yousaf, M. (2015). Neighbor Node Trust Based Intrusion Detection System for WSN, of. *Procedia Computer Science, 63,* 183–188.
101. Saleem, K., Derhab, A., Al-Muhtadi, J., Shahzad, B., & Orgun, M. A. (2015). Secure transfer of environmental data to enhance human decision accuracy. *Computers in Human Behavior, 51*, 632–639.
102. Saleem, K., Derhab, A., Orgun, M. A., Al-Muhtadi, J., Rodrigues, J., Khalil, M. S., & Ahmed, A. A. (2016). Cost-effective encryption-based autonomous routing protocol for efficient and secure wireless sensor networks. *Sensors, 16*(4), 23.
103. Salve, V. B., Ragha, L., & Marathe, N. Aodv based secure routing algorithm against sinkhole attack in wirelesses sensor networks. In *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1–7.
104. Sanmartin, P., Jabba, D., Sierra, R., & Martinez, E. (2018). Objective function bf-etx for rpl routing protocol. *IEEE Latin America Transactions, 16*(8), 2275–2281.
105. Sanmartin, P., Rojas, A., Fernandez, L., Avila, K., Jabba, D., & Valle, S. (2018). Sigma routing metric for rpl protocol. *Sensors, 18*, 4.
106. Sato, A., & Costa-i Font, J. (2013). Social networking for medical information: A digital divide or a trust inquiry? *Health Policy and Technology, 2*(3), 139–150.
107. Sharma, A. K., Saroj, S. K., Chauhan, S. K., & Saini, S. K. Sybil attack prevention and detection in vehicular ad hoc network. In *2016 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 594–599.
108. Sharma, M. K., & Joshi, B. K. (2016). *A Mitigation Technique for High Transmission Power based Wormhole Attack in Wireless Sensor Networks*. Proceedings of 2016 International Conference on Ict in Business Industry and Government.
109. Sharma, S. A defensive timestamp approach to detect and mitigate the sybil attack in vanet. In *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 386–389.
110. Shehni, R. A., Faez, K., Eshghi, F., & Kelarestaghi, M. (2018). A new lightweight watchdog-based algorithm for detecting sybil nodes in mobile wsns. *Future Internet, 10*(1), 17.
111. Shi, W., Liu, S. Y., & Zhang, Z. H. (2015). A lightweight detection mechanism against sybil attack in wireless sensor network. *Ksii Transactions on Internet and Information Systems, 9*(9), 3738–3750.
112. Silawan, T., & Aswakul, C. Sybilcomm: Sybil community detection using persuading function in iot system. In *2016 International Conference on Electronics, Information, and Communications (ICEIC)*, pp. 1–4.
113. Stavrou, E., Pitsillides, A., & Ieee. (2016). *WSN Operability During Persistent Attack Execution*. 2016 23rd International Conference on Telecommunications.
114. Sundararajan, R. K., & Arumugam, U. (2015). Intrusion detection algorithm for mitigating sinkhole attack on leach protocol in wireless sensor networks. *Journal of Sensors*

115. Surendar, M., Umamakeswari, A., & Ieee. (2016). *InDReS: An Intrusion Detection and Response System for Internet of Things with 6LoWPAN*. Proceedings of the 2016 Ieee International Conference on Wireless Communications, Signal Processing and Networking.
116. Taylor, C., & Johnson, T. Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid networks. In *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1835–1840.
117. Teotia, V., Dhurandher, S. K., Woungang, I., & Obaidat, M. S. Wormhole prevention using cota mechanism in position based environment over manets. In *2015 IEEE International Conference on Communications (ICC)*, pp. 7036–7040.
118. Tsitsiroudi, N., Sarigiannidis, P., Karapistoli, E., & Economides, A. A. Eyesim: A mobile application for visual-assisted wormhole attack detection in iot-enabled wsns. In *2016 9th IFIP Wireless and Mobile Networking Conference (WMNC)*, pp. 103–109.
119. Upadhyay, R., Bhatt, U. R., & Tripathi, H. (2016). DDOS attack aware DSR routing protocol in WSN, of *Procedia Computer Science 78* 68–74.
120. Vakula, D., & Kolli, Y. K. Low cost smart parking system for smart cities. In *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, pp. 280–284.
121. Verma, R., Sharma, R., Singh, U. New., & approach through detection and prevention of wormhole attack in manet. In, . (2017). International conference of Electronics. *Communication and Aerospace Technology (ICECA), 2*, 526–531.
122. Vidyasagaran, S., Devi, S. R., Varma, A., Rajesh, A., & Charan, H. A low cost iot based crowd management system for public transport. In *2017 International Conference on Inventive Computing and Informatics (ICICI)*, pp. 222–225.
123. Viloria Núñez, C. A., Sanmartín Mendoza, P., Avila Hernández, K., & Jabba Molinares, D. (2016). Internet de las cosas y la salud centrada en el hogar. *Revista Científica Salud Uninorte, 32*, 2.
124. Walters, J. P., Liang, Z., & Shi, W. (2007). *and Chaudhary, V*. Wireless sensor network security: A survey. Auerbach Publications.
125. Wang, T., Zhang, G., Yang, X., & Vajdi, A. (2016). A trusted and energy efficient approach for cluster-based wireless sensor networks. *International Journal of Distributed Sensor Networks, 12*(4), 3815834.
126. Wang, X. W., Hu, F., Zhai, C. X., Zhang, Y., Su, X. X., Li, Y., Wu, Z. K., Li, T. T., & Deng, Z. H. (2016).*Research on Improved DV-HOP Algorithm against Wormhole Attacks in WSN*, vol. 7 of *ITM Web of Conferences*.
127. Wazid, M., & Das, A. K. (2016). An efficient hybrid anomaly detection scheme using k-means clustering for wireless sensor networks. *Wireless Personal Communications, 90*(4), 1971–2000.
128. Wazid, M., & Das, A. K. (2017). A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks. *Wireless Personal Communications, 94*(3), 1165–1191.
129. Wazid, M., Das, A. K., Kumari, S., & Khan, M. K. (2016). Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. *Security and Communication Networks, 9*(17), 4596–4614.
130. Wibowo, A. A., & Suryanegara, M. On developing the model of smart logistic transport in indonesia. In *2016 IEEE International Conference on Management of Innovation and Technology (ICMIT)*, pp. 99–104.
131. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J. P., & Alexander, R. (2012). Rpl: Ipv6 routing protocol for low-power and lossy networks. Report 2070-1721.
132. Xiangyu, J., & Chao, W. The security routing research for wsn in the application of intelligent transport system. In *Mechatronics and Automation, Proceedings of the 2006 IEEE International Conference on*, IEEE, pp. 2318–2323.
133. Yang, K., Wang, R., Jiang, Y., Song, H., Luo, C., Guan, Y., Li, X., & Shi, Z. (2018). Sensor attack detection using history based pairwise inconsistency. *Future Generation Computer Systems, 86*, 392–402.
134. Yao, Y., Xiao, B., Wu, G., Liu, X., Yu, Z., Zhang, K., & Zhou, X. Voiceprint: A novel sybil attack detection method based on rssi for vanets. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 591–602.
135. Yaseen, Q., AlBalas, F., Jararweh, Y., & Al-Ayyoub, M. A fog computing based system for selective forwarding detection in mobile wireless sensor networks. In *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*, pp. 256–262.
136. Yi, L., & Zhongyong, F. The research of security threat and corresponding defense strategy for wsn. In *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*, pp. 1274–1277.
137. Younis, O., & Fahmy, S. (2004). Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on Mobile Computing, 3*(4), 366–379.

138. Yu, L., Jianwei, N., Lianjun, Y., & Lei, S. ebplatform: An iot-based system for ncd patients homecare in china. In *Global Communications Conference (GLOBECOM), 2014 IEEE*, pp. 2448–2453.
139. Zhang, P., Zhang, X., Sun, X., Liu, J. K., Yu, J., & Jiang, Z. L. Anonymous anti-sybil attack protocol for mobile healthcare networks analytics. In *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 668–674.
140. Zheng, J. H., Qian, H. Y., & Wang, L. (2015). *Defense Technology of Wormhole Attacks Based on Node Connectivity*. 2015 Ieee International Conference on Smart City/Socialcom/Sustaincom.
141. Zhou, H., Wu, Y. M., Feng, L., & Liu, D. L. (2016). A security mechanism for cluster-based wsn against selective forwarding. *Sensors, 16*, 9.



**Karen Ávila** System Engineering and PhD student in Computer Science at Universidad del Norte in Barranquilla, Colombia. Research assistant and professor of the Department of Systems Engineering at Universidad del Norte. Areas of Interest: IoT, WSN, Routing protocols, Software development.

**Paul Sanmartin** PhD and Msc in Computer Science , Universidad del Norte,Barranquilla Colombia, research professor at Universidad Simón Bolívar. Areas of Interest: Quality of Service on the Internet, IoT, WSN, Routing protocols, Urban Computing, Telematics Applications.

**Daladier Jabba** Ph.D. in Computer Science and Msc. in Computer Engineering, University of South Florida-Tampa. International Resources Manager R & D, Assistant Professor of the Department of Systems Engineering at Universidad del Norte. Member of the Research Group on Computer Networks and Software Engineering - Grecis. Areas of Interest: Wireless sensors, new protocols in the link layer and routing for wireless sensor networks, and the development of applications and interfaces in the mobile platform.

**Javier Gómez** received the BS degree with honors in Electrical Engineering in 1993 from the National Autonomous University of Mexico (UNAM) and the MS and PhD degrees in Electrical Engineering in 1996 and 2002, respectively, from Columbia University and its COMET Group. During his PhD studies at Columbia University, he collaborated and worked on several occasions at the IBM T.J. Watson Research Center, Hawthorne, New York. His research interests cover routing, QoS, and MAC design for wireless ad hoc, sensor, and mesh networks. Dr. Gomez is currently a full time professor at the Department of Telecommunications Engineering, School of Engineering (UNAM). Javier Gomez is member of the SNI (level II) since 2016.