electronics

MDPI

*Review*

# A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues

**Gaurav Sharma [1,*], Stilianos Vidalis [1], Niharika Anand [2], Catherine Menon [1] and Somesh Kumar [3]**

[1] School of Computer Science & Engineering, University of Hertfordshire, Hatfield AL10 9AB, UK; s.vidalis@herts.ac.uk (S.V.); c.menon@herts.ac.uk (C.M.)
[2] Indian Institute of Information Technology Lucknow (IIITL), Lucknow 226002, India; niharika@iiitl.ac.in
[3] ABV-Indian Institute of Information Technology & Management Gwalior, Gwalior 474015, India; somesh@iiitm.ac.in
* Correspondence: g.gaurav@herts.ac.uk

**Abstract:** Security is a mandatory issue in any network, where sensitive data are transferred safely in the required direction. Wireless sensor networks (WSNs) are the networks formed in hostile areas for different applications. Whatever the application, the WSNs must gather a large amount of sensitive data and send them to an authorized body, generally a sink. WSN has integrated with Internet-of-Things (IoT) via internet access in sensor nodes along with internet-connected devices. The data gathered with IoT are enormous, which are eventually collected by WSN over the Internet. Due to several resource constraints, it is challenging to design a secure sensor network, and for a secure IoT it is essential to have a secure WSN. Most of the traditional security techniques do not work well for WSN. The merger of IoT and WSN has opened new challenges in designing a secure network. In this paper, we have discussed the challenges of creating a secure WSN. This research reviews the layer-wise security protocols for WSN and IoT in the literature. There are several issues and challenges for a secure WSN and IoT, which we have addressed in this research. This research pinpoints the new research opportunities in the security issues of both WSN and IoT. This survey climaxes in abstruse psychoanalysis of the network layer attacks. Finally, various attacks on the network using Cooja, a simulator of ContikiOS, are simulated.

**Keywords:** Denial of Service; Internet-of-Things; routing protocol; low power; lossy network (RPL), physical attacks; sybil attacks; Wireless Sensor Network (WSN)

**Citation:** Sharma, G.; Vidalis, S.; Anand, N.; Menon, C.; Kumar, S. A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues. *Electronics* **2021**, *10*, 2365. https://doi.org/10.3390/electronics10192365

Academic Editors: Dmitry Korzun, Ilya Shegelman and Anatoly Voronin

Received: 23 August 2021
Accepted: 26 September 2021
Published: 28 September 2021

## 1. Introduction

A wireless sensor network (WSN) is a distributive network consisting of tiny sensors capable of collecting the data like temperature, humidity, pressure, voice, etc. [1]. These remote sensors have a limited energy source, storage, and short radio range. The sensors hook up together to form an ad-hoc network that reports the activities on the web, and finally, the data collected reach the sink. WSNs find applications in health monitoring, disaster management, target tracking, habitat monitoring, and many more. Sensor networks comprise tiny sensor nodes with many resource constraints like inadequacy of power and data storage. These inadequacies do not allow the use of traditional network security techniques in sensor networks. The security issues are more complicated in WSNs than wireless communication techniques due to unreliable communication channels and unattended operations. The existing security protocols are suitable for implementing traditional ad-hoc networks, whereas the sensor network is unique. These unique features of a sensor network that are different from the conventional ad-hoc network are [2]:

- A sensor network has a higher amount of sensor nodes present in the network than the traditional ad-hoc network, with limited nodes.
- Nodes in the sensor network are deployed very densely to provide better coverage of the target area.
- A sensor network has many resource constraints and is more prone to failure due to the harsh environment.
- There are no global ids of the sensing nodes; the local ids that are valid only for that sensor network are responsible for identifying the nodes.

The Internet-of-Things (IoT) has emerged as a big advance in all the technologies that follow the Internet. The market of IoT is expected to grow up to 75 billion by the year 2025. In the upcoming years, every person on the earth may have 20–25 personal IoT devices. That means IoT is going to have a substantial influence on our lives [3]. WSN has come out to be the backbone of IoT, where countless sensor nodes unite the Internet, focusing on collaborating with other sensor nodes to monitor and sense their environment. IoT can interconnect the environment and people by using WSN in the future [4], resulting in escalated environmental apprehension [5].

The sensor networks have an inherent feature of unattended nodes, due to which the physical attacks play a vital role in sensor network operation. Security undoubtedly is a crucial issue in WSN and IoT, mainly for tasked security attacks. For example, no patient wants that his confidential health reports to be revealed to the world. In [6], authors have reported such an issue caused due to data leakage from misbehaving nodes. To understand the whole security system of WSN and IoT, it is essential to know about the obstacles of sensor network security, security requirements, types of attacks, and possible defensive measures. Methodologies designed for securing WSN will also be relevant for IoT [7]. The three essential components of security attacks are prevention, detection, and mitigation [8]. This survey aims to suggest layer-wise security attacks on WSN and IoT. This survey, according to us, will be beneficial for researchers who want to form secure algorithms for IoT.

WSN comprises sensor nodes that are capable of low-level communication. Nonetheless, on the other hand, IoT contains internet-enabled sensor nodes that are internet-enabled, and hence the data sensed by IoT nodes are directed to the sink, which will also be Internet-based. Moreover, IoT networks may also need to interact with the emanating approaches of cloud computing and big data. This survey paper aims to compile the work from various research papers in the field of IoT security. This work discusses WSN and IoT protocol stacks by comparing the attacks on different stacks and possible preventive measures. Finally, the effect of various attacks on the network's performance is quantized using the Cooja, a simulator of ContikiOS.

The rest of the manuscript is as follows. Section II presents the IoT history and technical issues. Section III examines the security characteristics in IoT and WSN. Section IV discusses the WSN and IoT standards and protocols. Section V and Section VI illustrate open issues of cybersecurity in IoT and security attacks evaluation in ContikiOS. Finally, Section V concludes the paper and suggests future works.

## 2. IoT History and Technical Issues

"Internet-of-Things" is a term coined by Kevin Ashton of Proctor and Gamble in 1999. IoT since then has progressed rapidly into a field that necessitates the interaction of objects which have embedded sensors, processors and can communicate with fellow devices to furnish the various automated services [3,9,10]. IoT is not a single technology. It is a confluence of real-time computing, actuation, embedded systems, and, most important, WSN, shown in Figure 1. In our day-to-day life, there are various IoT standalone devices such as smartphones, smartwatches, home lighting [11], etc. The upcoming future of IoT will aim to use smaller and energy-efficient sensor technology along with state-of-art communication, data analytics, and advanced actuators to collect and process data more intelligently [11,12]. IoT implementation will increase energy management at homes and industry, monitoring consumables, fitness monitoring, etc., is anticipated to become ubiquitous [13,14].

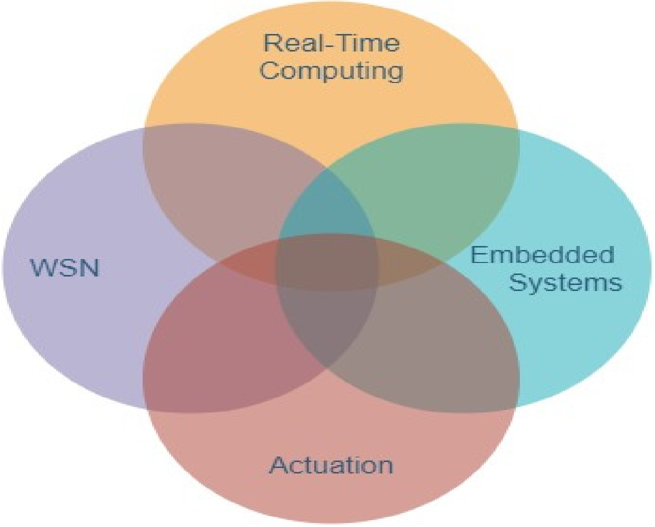

**Figure 1.** IoT is the union of several technologies.

The networking infrastructure for cyber-physical systems (CPS) [9] is IoT. The technological advances in CPS can enable scalability, safety, resiliency, adaptability, and capability. CPS is modifying the way we communicate with engineered systems. CPS's domains are aeronautics, transportation, health care, infrastructure, automation, and energy [14]. Advances in IoT will impact numerous services and applications, including intelligent transportation, smart homes, industrial IoT, smart agriculture, and retail IoT. These IoT-enabled services and applications will also prove to be an economic boom for society [14]. The sensor network is a different network, having many resource constraints, and thus the implementation of traditional Security into a sensor network is quite problematic. Similarly, structuring an IoT network has many technological issues while preparing security algorithms for IoT networks. Some of the challenges in IoT can be as follows as discussed in [15]:

- Communication: In IoT, wired and wireless communication is used, such as LPWAN, ZigBee, etc.
- Scalability: IoT network comprises many nodes, and naming addressing, and managing many such devices is challenging.
- Heterogeneity: IoT is a network of various devices from assorted families like actuators, sensors, switches, gateways, mobiles, etc. Different devices engage different algorithms, protocols, and circuitry.
- Energy Consumption: In the case of both WSN and IoT, energy is a most challenging constraint. Thus, the researchers always struggle to design the algorithm for IoT and WSN with minimum processing requirements.
- Interoperability: IoT network consists of various devices, which exchange data and collaborate among themselves. Thus, there is always a need for a predefined standard for data exchange.
- Self-Awareness: IoT devices should automate autonomously in such a way that there is minimum human intervention required.
- Data Privacy: Data Privacy is another crucial issue in IoT. The IoT network is designed for both public and private affairs. As described in [16,17], IoT devices may share the information to the sink in a public network, whereas transmitting location information can be risky in a private network.

## 3. Security Characteristics in IoT and WSN

IoT and WSN are special wireless networks, and they are structureless networks comprising thousands of tiny sensor nodes. The sensing nodes collect the data, and after several data conditioning techniques, the data are sent to the gateways and finally to the base station. Some of the features in IoT and WSN, which make them even more vulnerable to security attacks are listed below.

- Organization: Sensors do not possess any fixed structure, and the location of the sensors is random. The solution to the failures in the network is the self-organizing behavior of WSN and IoT network by discovering the nearest neighbour [18].
- Resource Constraints: IoT and WSN have many resource constraints like restricted communication bandwidth, storage capacity, and processing powers, which permit the utilization of whippersnapper security methods only. These security methods offer security from external attacks only [19].
- Central Control: The central system, the base station, control the sensing nodes. The data gathered by the nodes flow in the network depending upon the routing algorithm applied. The major problem in this approach is that most routing algorithms' development is without any conquer thoughtfulness of security measures.
- Flow Control: The transmission flow is acquainted with enhancing network performance degradation by analyzing the number of transmission errors and quality of flow [20].
- Environmental Issues: Sensor nodes are deployed in an open environment, accessible to the antagonists; this may result in introducing one or many compromised nodes, which disturbs the network externally and may take the network's total control, leading to the complete fallout of the network.

The characteristics described above point towards the security mechanism(s) requirement to optimize the security requirements of IoT and WSN and contribute to increasing the reliability and efficiency of the network.

### *3.1. Security Requirements*

IoT and WSN pose some inherent properties of conventional wireless communication and have several exclusive features. That means that the security requirements for IoT and WSN circumscribe both traditional wireless network and sensor network requirements.

#### 3.1.1. Data Confidentiality

In network security, there should always be data confidentiality. There is always an addressing problem in any network security system. There are many examples, such as military, where sensitive data are transferred between the nodes, the data must be transferred to the correct node and not to the neighbouring enemy node. The distribution of keys requires a secure channel and addressing for sensitive data. The IoT network also has public information like public keys and node identities. To protect the network against traffic analysis attacks, this general information should also be encrypted to some extent. Data confidentiality can be achieved by encrypting the data before broadcasting [21].

#### 3.1.2. Data Integrity and Data Freshness

Data confidentiality makes it unable for antagonists to steal the information, but this does not assure that the data are secure. The data can be tampered with by the antagonists even after data confidentiality by changing the accurate data. A malicious node can manipulate the information within the packet, and the reviewer will then receive the new packet. The malicious nodes, but the harsh communication environment, also result in damage or loss of data. Thus, data integrity is needed to ensure that the data received are not altered [22].

Along with data confidentiality and freshness, it is essential for security purposes that the data coming from the sensors to the receiver should be fresh and recent. This means that the action taken by the base station is based on current information. For security purposes shared critical approach is applied, data freshness is a vital aspect. These shared keys keep changing in time, and the new keys must be propagated on the network; in such cases, data freshness is essential. Some time is required for propagating the new key within the network, and it is easy for the antagonists to attack the network while the process of key distribution is taking place.

### 3.1.3. Self-Organization

WSN is a particular type of ad-hoc network, which should be malleable enough to adapt according to the application and area where the sensor nodes are deployed. WSNs have the fundamental property of being self-healing and self-organizing according to the situation [2]. For network management, no fixed infrastructure is available in the sensor network. These inherent properties of WSNs are significant challenges for the security of the sensor network. There are several symmetric encryption techniques proposed in [23,24]. For applying public-key cryptography, a public key distribution mechanism is also required. The distributed sensor network must be self-organized for multi-hop routing to build confidence among the sensors and key management. Therefore, it implies that there may be a few unavoidable attacks if a sensor network lacks self-organization.

### 3.1.4. Time Synchronization

There is some form of time synchronization in all WSN and IoT networks depending upon their design.

- For power conservation, the radio of the individual sensing node is turned off.
- Sensors compute an end-to-end delay of packets, as the packets are transferred between a pair of sensor nodes.
- Group synchronization is required for the tracking application.

The authors propose synchronization protocols for security in [25] for group synchronization, pairwise synchronization, and multi-hop sender-receiver synchronization.

### 3.1.5. Authentication

Antagonists can reshape the packets and even change the whole packet stream by infusing additional packets into it. Thus, the receiver’s responsibility is to ensure that the data based on the decision is authentic and appropriate. In WSN and IoT networks, authentication is necessary for controlling the sensing node duty cycle, network reprogramming, etc. The authentication of data helps the receiver ensure whether the data received is from the genuine sender. When there is a two-party communication, the authenticity can be checked by sharing a secret key and message authentication code (MAC) for all data being communicated. The transmission in WSN and IoT networks is between many sensing nodes to a receiver or sink. For secure communication, there is a need for secure broadcast protocol; one such approach is given by authors in [26] named µTESLA, which provides asymmetric key cryptography. In this approach, the message key broadcasted by the sender is generated by a secret key, and the receiver will buffer the received packet until the secret key is retrieved. Once the private key is retrieved, the receiver can authenticate the received packet is from the genuine sender and not from any antagonist. The drawback of µTESLA is that for authentication, before broadcasting the secret key, some basic information must be unicast among the sensing nodes. Although several protocols provide secure communication in WSN and IoT networks, none is secure enough to provide the desired security. A comparison among such claimed secure protocols is described in Table 1.

**Table 1.** Comparison of secure routing protocols for broadcast authentication.

| Protocols | Routing | Confidentiality | Broadcast Authentication |
|---|---|---|---|
| SNEP [26] | Flat | Yes | No |
| LKHW [27] | Flat/Hierarchical | Yes | No |
| μTESLA [26] | Flat/Hierarchical | Yes | Yes |
| Multilevel Key Chains [28] | Flat/Hierarchical | No | Yes |
| LEAP Hierarchy [29] | Flat/Hierarchical | Yes | Yes |

### *3.2. Security Vulnerabilities*

WSN and IoT have a wireless communication medium, a deficiency of physical security and many resource limitations. These all lead WSN and IoT to be vulnerable to many external or internal security attacks. Considering external attacks, the attacker may not have access to the node directly but is capable of tampering or replacing the actual node with the malicious node to empower malicious actions and disturb the natural performance of the network. On the other hand, in internal attacks, the attacker has access to the internal protocols and thus promotes various malicious activities. There is no borderline to differentiate clearly between internal and external attacks. In this research, we give a classification of multiple attacks concerning different layers of IoT. The layered architecture of WSN and IoT, as described in [4], has five layers, namely physical layer, data link layer, network layer, transport, and application layer. Figure 2 depicts the layered architecture of IoT.

1. Physical Layer Attacks: In the physical layer, which is the lowest layer in the sack, the physical characteristics of the network are stipulated. The wireless communication medium has a broadcast nature, making this layer vulnerable to node tampering, hardware hacking, jamming, and even eavesdropping.
2. Data Link Layer (DLL) Attacks: The DLL facilitates the nodes with shared resource usage, error control, and data flow control. The attacks in DLL are more likely to have pertained within the medium access control (MAC) sublayer of DLL. The standard attacks in this layer are collision and jamming.
3. Network Layer Attacks: This layer caters to the routing of the data packets within the network. The presence of any malicious node can hamper the normal functioning of the network and initiates attacks like hello flood, replication attack, black hole, wormhole, and selective forwarding.
4. Transport Layer Attacks: This layer leads to reliable transportation in the network. Due to attacks, the connection between the nodes can be compromised, giving rise to energy drain attacks, desynchronize attacks, and data integrity attacks.
5. Application Layer Attacks: The application layer interacts directly with the end-user and performs data aggregations. This layer is prone to attacks that can affect the application programs.

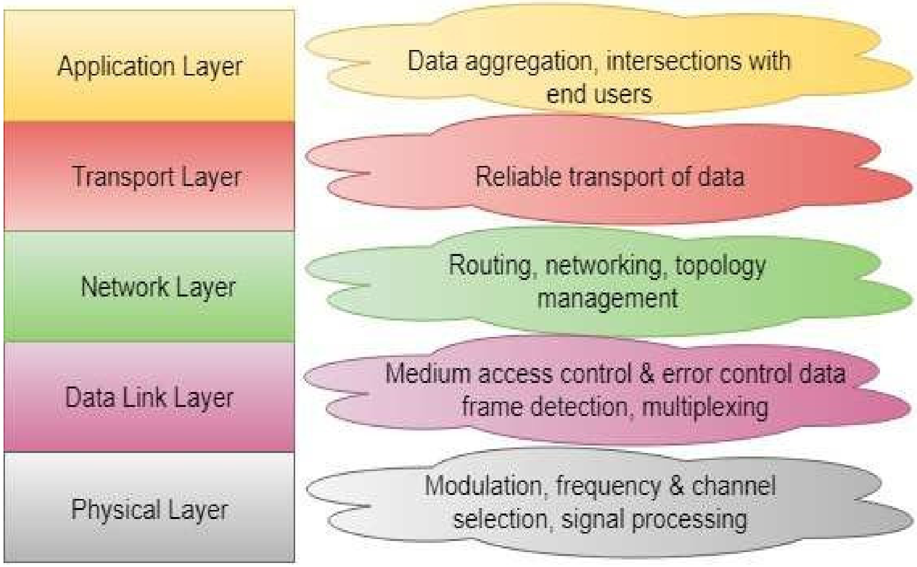
Application Layer
Data aggregation, intersections with end users
Transport Layer
Reliable transport of data
Network Layer
Routing, networking, topology management
Data Link Layer
Medium access control & error control data frame detection, multiplexing
Physical Layer
Modulation, frequency & channel selection, signal processing

**Figure 2.** IoT layered architecture.

### *3.3. Security Structure*

After learning about all the possible security issues in the sensor network, we will now discuss the possible defensive measures. Table 2 enlists some of the security schemes in the literature, along with the type of attacks prohibited by them and their corresponding network architecture. In this section, the critical establishment is discussed, which is the base of the security systems in WSN and IoT, followed by the defence against DoS attacks, secure broadcasting, and defence against attacks on routing protocols.

**Table 2.** Classification of attacks, with their consequences.

| Security Scheme | Attacks Prohibited |
|---|---|
| **JAM** [30] | DoS Attack |
| **Wormhole** [31] | DoS Attack |
| **Statistical En-Route Filtering** [32] | Information Spoofing |
| **Random Key Pre-distribution** [33] | Sybil Attack |
| **Bidirectional Verification** [34] | Hello, Flood Attack, |
| **On Communication Security** [35] | Data Spoofing |
| **TIK** [36] | Wormhole Attack and Data Spoofing |
| **Random Key Distribution** [37] | Data Spoofing, Attacks in Transmitting information |
| **REWARD** [38] | Blackhole attacks |
| μ **TESLA** [26] | Data Spoofing and Attacks on reply to messages |
| **Range Based Secure Localisation** [39] | Malicious anchors |

#### 3.3.1. Key Establishment

Key establishment is the foundation to assure that a security system exists in a WSN and IoT. The target of key establishment is to create an essential key between the sensing nodes. This security feature is versatile enough to support the addition and subtraction of the sensor nodes in the network. Symmetric-key cryptography is the base of key establishment. Figure 3 shows the taxonomy of the key establishment schemes in WSN and IoT. The key establishment in the sensor network is broadly done based on network structure and the probability of key sharing. In the network structure, the key establishment is done based on centralized and distributed key schemes. In the centralized key method, a single, centralized body, known as a key distribution centre (KDC), the keys' distribution, generation, and regeneration. One such scheme in literature is named logical key hierarchy (LKH) [27]. In this approach, the base station works as KDC. The drawback of the KDC scheme is that the single distribution center cannot handle all sensing nodes for a dense network. If the central controlling body fails, then the whole security system of the network will be adversely affected. The other approach for a Network structure-based key establishment scheme is the distributed key scheme where different controllers handle the key distribution, generation, and regeneration. Thus, the failure of one controller is not responsible for the loss of the whole security system. The overall security system is robust in the case of a distributed key establishment scheme. Some distributed key mechanisms in the literature are LEAP [29], BROSK [40], random key scenarios [24], etc.

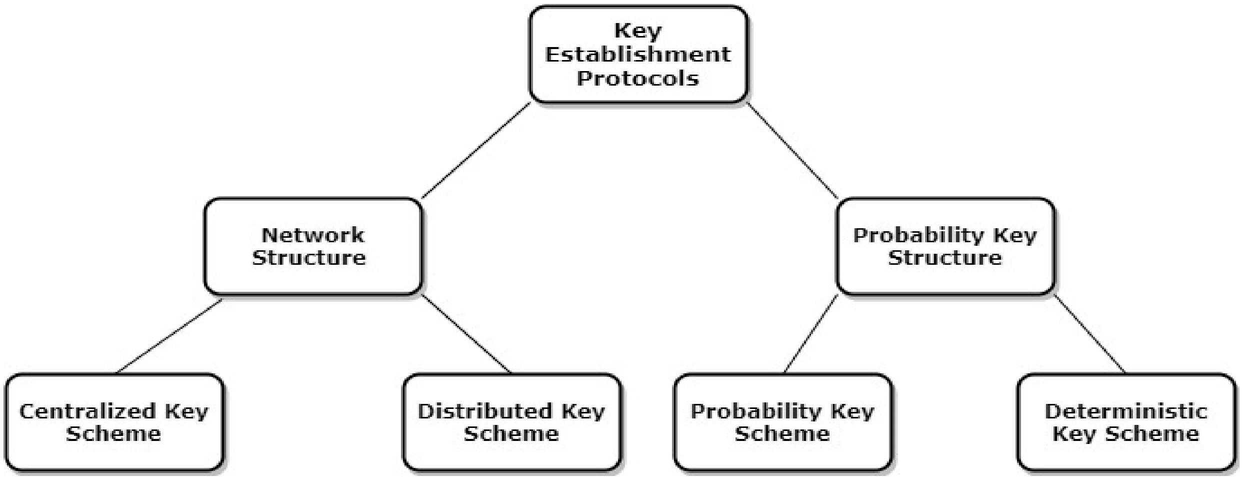

**Figure 3.** Key establishment protocols.

3.3.2. Defense against DoS Attacks

Table 3 enlists the layers of a sensor network and the common attacks at different layers with possible defensive measures. At the physical layer, the expected attacks on the sensor network are jamming and tampering. The possible solution for jamming is to reroute the traffic after identifying the jammed portion of the network. In [30], the authors have given a practical approach to overcome jamming. In this proposed approach, the nodes in the perimeter of the jammed portion of the network report jamming to their neighbours, which cooperate with the other nodes for forming new routing paths. The standard attacks in the link layer of the sensor network are a collision of packets, exhaustion due to low data rates, collision of the packets, and unfairness due to frame size. These attacks can be overcome by introducing error-correcting codes and increasing data rates. Flooding denial of service occurs at the transport layer, which can be defended by client puzzles given by Aura et al. in [41]. In Table 4, some of the elucidations against DoS attacks are abridged.

**Table 3.** Layer-wise cyber attacks in WSN and IoT.

| Layer | Attacks | Outcomes of Network operation's | Proposed Solutions for Mitigation |
|---|---|---|---|
| **Physical Layer** | Basic Jammer | Congestion, signal distortion, draining of nodes' energy Admittance to the sensitive data. | Spread Spectrum [42], JAM[30], Swarm intelligence [43], Wormhole technique [44] |
| | Node Tapering | Tampering sensitive information like routing tables and cryptographic keys. | JTAG [45], Camouflaging [46] |
| **Data Link Layer** | Hardware Hacking | Nodes become vulnerable to attacks. | Error correction codes [46] |

| | | | |
|---|---|---|---|
| | Collision | Increasing congestion | Irregular detection of motes [47] |
| | Denial of sleep | Interference | TDM |
| | *De-Synchronization* | Packet Loss | *6TiSCH* [48] |
| | *6LoWPAN* | No end-to end security | *6LowPseC* [49] |
| **Network Layer** | Jamming | Congestion, signal distortion, draining of node's energy | Multipath routing [50], Active trust routing [51], REWARD routing [52], MOADV [53], BAMBi [54] |
| | Replay Attack | Increase in congestion and interference, route disturbance and fake error messages, data loss, and traffic reduction | Source authorisation [42], Multipath routing [47] |
| | Black-hole | Routing loops, repulsing network traffic Data loss, and reduction of traffic | Source routing algorithm [55] |
| | Spoofed Selective Forwarding | Data loss and reduction of traffic, conciliatory of transmission routes | Identity verification, Isolation, [33], Indirect validation [47] |
| | Sinkhole Wormhole | Transmission of data to the wrong destinations | Multi-level clustering [56], ID-based public keys [57], Location-based key management [58] |
| | Sybil Attack Hello Flood | Hello Flood | ID-based public keys [56] |
| | Node Replication | Hello Flood | ID-based public keys [56] |
| | *RPL rank* | Disturbance in the transmission routes Collision, false transmission routes, and energy degradation | *VeRA* [59], *TRAIL* [60] |
| | *RPL DODAG* | Eavesdropping, disturbance in the transmission route. | *VeRA* [59], *Integrity check* [61] |
| **Transport Layer** | Desynchronization attack | Failed communication links and disturbed transmission routes | Authentication via header [30] |
| | Energy Drain | False messages can tamper with the overall functioning of the network. | Light-weighted algorithm for authentication [62] |
| | *MQTT exploit* | Draining energy resources | *SMQTT* [63], *Enforcement of security policies* [64] |
| **Application Layer** | Malicious Code Attacks | Extinguishes the capacity of the network to perform the expected Collision and energy draining | Collective secret [32] |
| | Attacks on Reliability Path-based DoS | Extinguishes the capacity of the network to perform the expected Collision and energy draining | One-Way hash chains [37] |
| | *CoAP exploit* | Extinguishes the capacity of the network to perform the expected Collision and energy draining | *Employment of DTLS* [65] |
| **Multi-Layer** | Man in the middle | Admittance to the sensitive data Rules out the capacity of the network | Key pre-distribution [23,37] |
| | Denial of Service | Admittance to the sensitive data Rules out the capacity of the network | Link Layer encryption [26,66] |

| | | | |
|---|---|---|---|
| | Eavesdropping | Admittance to the sensitive data<br>Rules out the capacity of the network | Sensor-Wave communication [26] |

**Table 4.** Defensive measures against DOS attacks in WSN.

| DoS Attacks | Possible Defense Approach |
|---|---|
| Physical tampering | Using tamper-resistant nodes |
| Radio Interference | Using Spread-Spectrum communication |
| Black-hole | Using Multiple routing paths |
| Misdirection | Using source authorization |
| Denying Channel | Using error correction codes |
| Flooding | Restraining total connections |

#### 3.3.3. Secure Broadcasting and Multicasting

The communication pattern in WSN and IoT networks can be 1-to- N or N-to-1, or N-to-M, other than traditional point-to-point communication. The security issues in WSN and IoT are also due to the secret key, which is needed by the sensing nodes to decrypt the broadcast message. It has already been discussed in the previous sections that both WSN and IoT networks have severe resource constraints, so reducing the overhead broadcasting of messages is done. Broadcasting or multicasting in WSN and IoT networks are done with the help of the security key so that the messages are received by the authorized receivers only. The security, distribution, and generation are managed by various key management schemes [67].

#### 3.3.4. Defense against Attacks on Routing Protocols

Table 3 enlists the various routing protocols that secure routing in the WSN and IoT network (the IoT-specific attacks are written in italic). SNEP [26] is a flat routing that keeps confidentiality, with good scalability, and provides point-to-point authentication. SNEP does not provide broadcast authentication. LKHW [27] is another secure routing algorithm having limited scalability but provides good confidentiality. Perrig et al. in [26] have given another routing protocol, μ TESLA that has medium scalability and provides secure broadcast. In [16] multilevel key chain scheme is introduced for broadcast authentication and has good scalability. Zhu et al. in [29] introduced a hierarchical routing scheme for both point-to-point and broadcast authentication, with medium scalability.

## 4. WSN and IoT Standards and Protocols

In the previous sections, the security requirements for the WSN and IoT are discussed. Figure 4 depicts the various protocols following the different layers. These protocols follow IETF standardization [68] and can be layered on top of each other.

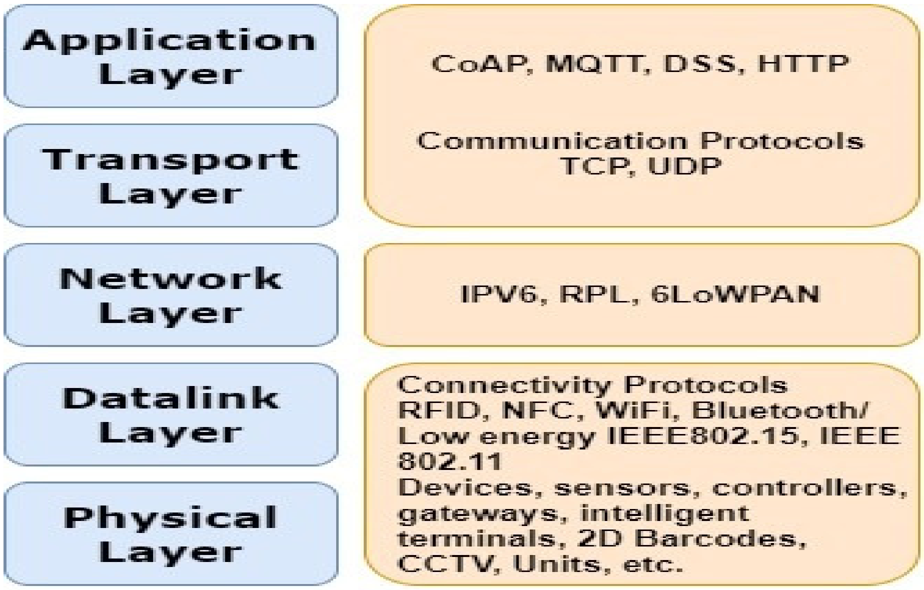
Application Layer
Transport Layer
Network Layer
Datalink Layer
Physical Layer
CoAP, MQTT, DSS, HTTP
Communication Protocols TCP, UDP
IPV6, RPL, 6LoWPAN
Connectivity Protocols RFID, NFC, WiFi, Bluetooth/ Low energy IEEE802.15, IEEE 802.11
Devices, sensors, controllers, gateways, intelligent terminals, 2D Barcodes, CCTV, Units, etc.

**Figure 4.** Communication standards and protocols following different layers of IoT.

### *4.1. IEEE 802.15.4 for Physical Layer Communication*

Wireless communication supports low-power, low data rate communication, and IEEE 802.15.4 [69] defines wireless communication's physical and MAC layers. This IEEE standard has properties like high flexibility, low cost, and low power consumption, making it suitable for many industrial and research-based applications, health monitoring [70], and home automation systems [71]. The archetype IEEE 802.15.4 has been facilitated with time and has now become IEEE 802.15.4e. The new version supports channel hopping in time synchronization. Figure 5 shows the detailed frame structure of IEEE 802.15.4. As far as the security mechanism is concerned, it applies only to the MAC layer, not the physical layer.

- IEEE 802.15.4 (Physical Layer): This standard patronizes 16 channels in the industrial, scientific, and medical (ISM) band and 11 channels in 868/915 MHz, low-frequency band. The various modulation schemes are used to lower down the co-channel interferences [72].
- IEEE 802.15.4 (MAC Layer): This standard utilizes carrier sense multiple access-collision avoidances (CSMA- CD) and supervises the admittance to time slots and physical channels. The network topologies used here are cluster, peer-to-peer, and star [73]. The IEEE 802.15.4 MAC layer has a security model that meets the four security prerequisites, i.e., data encryption, access control, sequential freshness, and frame integrity [74]. Several security suits endure these security prerequisites, like the Advanced Encryption Standard (AES) [72]. AES has different modes of operations, namely counter mode (CTR), cypher block chaining (CBC-MAC), and authentication and encrypts block cypher mode (CCM). CTR, CBC-MAC, and CCM support the length of 32,64 and 128 bits [74]. Table 5 shows the comparison of security by a piece security suite.
- IEEE 802.15.4e (MAC Layer): This standard supports multi-hopping by using a time-synchronized mesh protocol. The devices are also synchronized to choose the correct nearest neighbour along with the channel. IEEE 802.15.4e provides security against reactive jamming and sweep [75].

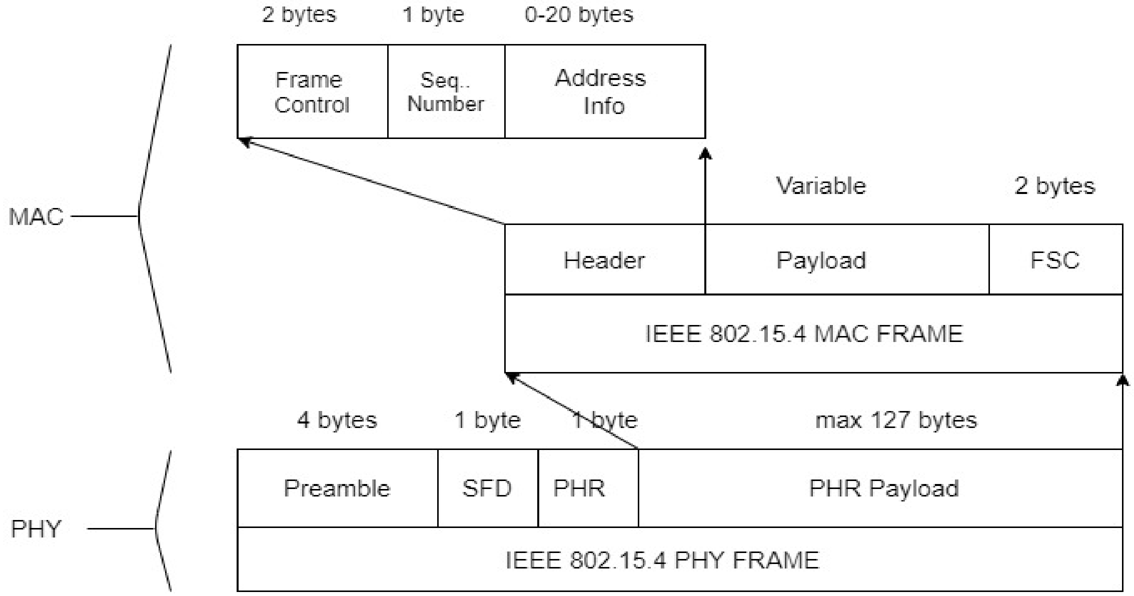

**Figure 5.** IEEE 802.15.4 frame on 2.4GHz Network.

**Table 5.** Security Suits for IEEE 802.15.4.

| Security Suite | Data Encryption | Access Control | Seq. Fresh. | Frame Integration |
|---|---|---|---|---|
| **None** | No | No | No | No |
| **CTR** | Yes | Yes | Yes | No |
| **CBC-MAC-128** | No | Yes | No | Yes |
| **CBC-MAC-64** | No | Yes | No | Yes |
| **CBC-MAC-32** | No | Yes | No | Yes |
| **CCM-128** | Yes | Yes | Yes | Yes |
| **CCM-64** | Yes | Yes | Yes | Yes |
| **CCM-32** | Yes | Yes | Yes | Yes |

### *4.2. B-MAC*

Berkeley media access control (B-MAC) [76] is an energy-efficient protocol that uses the sleep/listening agenda. In this protocol, the communication channel is chosen randomly. Not all the time receiver is in active mode. Whenever the transmitter has data to send to the receiver, it transmits a long preamble that the receiver can hear, and then the receiver becomes ready to receive data [77]. The disadvantage of B MAC is using the long preamble by the transmitter and overhearing by the receiver. As far as security is concerned, there is no well-defined security mechanism for B-MAC. Still, like other MAC layer protocols, it is vulnerable to collision and jamming during different operations. However, B-MAC is immune to periodic jamming, as it uses a recurring cycle for listening only and not for sending.

### *4.3. LoWPAN*

6LoWPAN stands for IPv6 over low power wireless personal area network, and it is good at offering ecumenical Internet connectivity to the low-power wireless nodes. 6LoWPAN has enabled the usage of IPv6 for low-energy wireless communication devices [72]. It has also made it possible to broadcast IPv6 over IEEE 802.15.4; this is an adaptation layer [78]. The job of the adaptation layer is to break the IPV6 into smaller sections, as IPv6 supports 1280 bytes, as compared to 127 bytes long packets in IEEE 802.15.4. The next task of the adaptation layer is to squeeze the header for the optimized usage of restricted payload space. The significant advantage of 6LoWPAN multi-hop communication and its major disadvantage is that it provides optimal routing solutions for limited resource and power communication. This limitation leads to the use of RPL.

### *4.4. RPL*

Routing protocol for low power and lossy network (RPL) is distance vector protocol, and it backs many forms of link-layer technologies; IEEE 82.15.4 is one of them [79]. RPL is a self-healing protocol. In WSN's, RPL specifies two elements: WSN nodes, hosts, or arbitrates routers, and the other element is local border routers (LBR) [80]. LBR supports packet transmission from the Internet to the host. RPL supports point-to-point, point-to-multipoint, and multipoint-to-point topologies.

### *4.5. BCP*

Backpressure collection protocol (BCP) is a protocol that works in real-time experiments, and it is a low-overhead protocol and highly scalable [81]. In BCP, there is no explicit path figuring between the source and destination, but the dynamic backpressure routing is the central working concept of this protocol. In other words, it is routing without routes. The nodes compute the weights for all the neighbouring nodes when the forwarding queue is not empty. The node then forwards the packet to the neighbour node having the highest positive weight. In case none of the neighbouring nodes has a positive weight, the sending node, in that case, waits for the back-off period and then recalculates the weights. BPL works on the concept of LIFO (last-in-first-out). On the other hand, the null packets are sent to determine the virtual queue whenever the forwarding key is empty.

### *4.6. CTP*

As the name implies, collection tree protocol (CTP) is a tree-based routing scheme, which does not guarantee 100% honest delivery, but it is a best-effort protocol. CTP provides many-to-one and one-to-many communication [82]. This protocol prevents duplication of packets. CTP uses ETX to route packets from different routes to the tree, as CTP is an address-free protocol. The ETX of a node is the sum of its parents and ETX of the link to its parents. When there are many valid routes, then the route with minimum ETX is considered for transmission. In the case of disparity in the topology, routes are updated and not periodically.

### *4.7. CoAP*

CoAP stands for constrained application protocol and backs the application-layer communication and web transfer within IoT [83]. CoAP is an advanced HTTP version (hypertext transfer protocol) and uses Representational State Transfer (REST) architecture. The resource requirement of CoAP is lesser than HTTP, which makes it less complex than its denser cousin HTTP [83]. Figure 6 shows the protocol stack along with the message and header format of CoAP. The architecture of CoAP is consists of two parts, i.e., message layer and request-response layer. Table 6 summarises the various protocols, their significant attacks, and the aforementioned defensive methods.

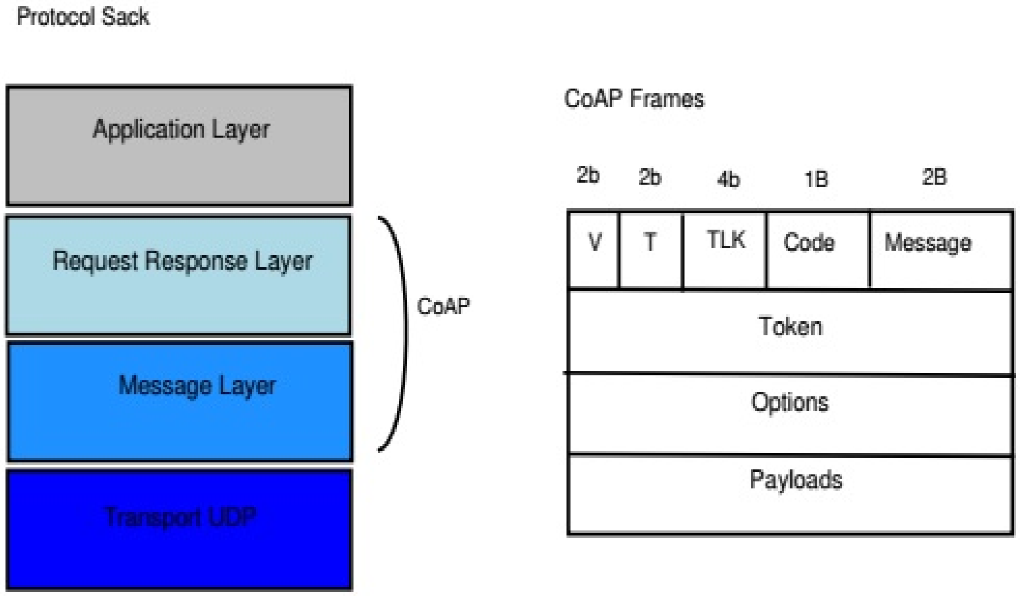

**Figure 6.** CoAP protocol stack.

**Table 6.** Summary of attacks against various communication standards and protocols and existing defensive measures.

| Protocol | Significant Attacks | Proposed Defensive Measures | Comments |
|---|---|---|---|
| **IEEE 802.15.4** | Eavesdropping and faking Acknowledgement (ACK )frame | Message Integrity Code (MIC) [74] | MIC has built-in CBC-MAC suits, which increases the overhead and delays the frame transmission. |
| | Reactive jamming and sweep | IEEE802.15.4e [75] | Channel hopping and secured ACK. Do not ensure defence for wideband jamming |
| | Denying of data through physical and MAC header | Encrypted data payload [75] | It Covers MAC payloads, not the headers. |
| **B-MAC** | Denial of sleep attack | Broadcast attack defense, anti-replay protection and link-layer authentication [84] | Attackers are awake most of the time in the case of B-MAC protocol. |
| | Statistical Jamming | Reduction in preamble size [77] | Reducing the preamble size too much overcomes its function. |
| **6LoWPAN** | Authentication Attack | Framework for network access control [85] | Enables one border router and provides identification to nodes |
| | Eavesdropping and spoofing, Man in the middle | IPsec [86] | The end-to-end secure mechanism, the key mechanism, is pre-shared but not very flexible. |
| | Fragmentation attack | Timestamps are given to bidi reactional and unidirectional fragmented packets [87]. Use of split buffer scheme [88] | Redefinition of fragmented packets. |

| | | | |
|---|---|---|---|
| **RPL** | Sybil Attack | To store graphical location of sensor nodes, a distributed hash table (DHT) is used [89] | Non-scalable and challenging to identify the node location securely. |
| | Wormhole Attack | The separate key for each segment of the network [89]. | End-to-end delay and high jitter |
| | Selective forwarding attack | Lightweight Heartbeat [89] | No defence after attack detection. The delivery ratio is improved, but energy consumption increases. |
| | Rank attack selective forwarding altered information | RPL resilient technique [90]<br>TRAIL [59] and VeRa [59]<br>SVELTE [91] | Dependent on network size and do not require cryptography.<br>Overhead is small, but the positive rate is not 100% due to false alarms |
| **BCP** | Selective forwarding, black-hole and multiple attacks | Secure backpressure algorithm [92] | The throughput performance is maintained under attacks. |
| | Data Modifications, False routes and data modification | VAR trust model [93] | Overhead increased |
| **CTP** | Data alteration, data loss, sinkhole and selective for warding | Kinesis [94,95] | An automated reaction scheme for attacks and abnormalities.<br>Segmentation of neighbourhoods gives rise to redundant data. |

## 5. Open Issues of Cybersecurity in IoT

IoT cybersecurity is in its early phase of development, and thus there is a need for further research and investigation in this field [96]. Table 7 enlists some of the open issues in the field of cybersecurity in IoT. The issues enrolled in this survey are layer-wise but are not limited to the problems listed in Table 7.

- Wireless Communication Security: Wireless communication cannot ensure secure communication on its own [97]. Also, the protection of the physical layer cannot entirely prevent security infringement. Secure higher-order layers can provide the safety of the physical layer. A primary authentication mechanism is necessary for any wireless communication. The key size should be long enough to beat the attackers, and the key updating should be done frequently to protect the key identity from the attackers [98,99].
- Sensor-Based Threats: Authors in [100] have pinpointed the issues of sensor-based threats in the IoT network. There is a lack of Security available at the sensor nodes, which makes them vulnerable to attackers. The attackers can extract information from the sensor nodes and inject malware to the nodes without being noticed.
- Defence against Botnet: QBot botnets were discovered in 2014, eventually infected about 1 million IoT devices. Like a computer virus, QBot botnets have precursors named Mirai botnet and Torii botnet. Botnets result from weaknesses of IoT like bad user habits and lack of rigid security precautions [101].
- Integration with cloud/fog: IoT is a heterogeneous network consisting of various sensing modes. These different nodes collect massive data, which has to be stored and processed from time to time. The data communication techniques used in IoT have to be robust enough to avoid the management issues in handling the diverse data collection done by the different nodes. These situations make it difficult for cloud computing to cope effectively and efficiently with data handling and processing in IoT. The sole use of cloud computing in data handling can result in high bandwidth consumption and high communication cost. It is crucial to take care of the cloud data while handling and securing sensitive data. Due to these problems,

the fog computing paradigm and cloud computing in IoT [12]. Integrating fog computing and cloud computing is a substantial open issue for designing a secure IoT network.

- Other Concerns: The Internet of Drones is a recent application of IoT in both research and industry. Authors in [102] have been concerned that drones are commonly designed without considering the basic security concepts, making it a security issue in IoT. The number of IoT vendors is increasing with the day-by-day increase in users of IoT, but the lack of a security framework for the vendors makes the IoT network more prone to cyber-attacks. Authors in [103,104] have analysed this growing concern in their research and have stressed that this security issue must be considered in the upcoming study.

**Table 7.** Open Issues for cybersecurity in IoT.

| Open Issues | Source | Layer |
|---|---|---|
| Wireless Communication security | Burg et.al [99] | Physical and MAC |
| Sensor-based threats | Sikder et.al [100] | Physical and MAC |
| Defence against botnet attacks | Torii botnet [101] | Application |
| Lack of security framework | Zhang et.al [103] | Application |
| Integration with cloud/fog | Butun et.al [12] | All Layers |
| Security of Internet of drones | Lin et.al [102] | All Layers |

## 6. Security Attacks Evaluation in ContikiOS

Depending upon the manoeuvring nature of IoT, they are prone to a wide variety of attacks, as discussed in the previous section. Most of the time, the nodes are deployed in the approachable region, making the network more accessible for attackers. Other than these, malicious nodes can be easily added to the network to infect it. The best way of avoiding DoS [105] is to understand the consequences and impingement of attacks on the network's performance. A better way of designing a secure and lively sensor network is precise and profligate simulations of IoT. In this research, we use Cooja, a simulator of Contiki O.S. [106]. Cooja is very famous among researchers in the field of sensing networks. Our main objective behind using Cooja is to analyse the possibility of exploiting it to measure the impact of attacks and the development of security measures. In this research, we examine the effect of internal attacks on RPL based sensor networks.

### *6.1. Network Model*

Let the devices in the network communicate in a multi-hop fashion and the sensor network $N = S \cup C.$ $S$ is the set of sensor nodes responsible for generating and forwarding the data packets, and $C$ the set of data collecting roots. The set of one-hop neighbours is given by $N_x \subseteq N$ and node $x \in N$. The communication time slot is $t$ and $t \in \{1,2,3, \ldots.., t_n\}, t_n < \infty$. All the potential links are given $L$ such that all the node pairs $x, y \in L$, and the whole network is sculptured as a time-weighted graph $G\ (N, L)$. In the possible connections, $L$ let $x$ be the source node and $y$ be the destination node. Adopting the standard layered architecture of WSN and IoT, we address the following attacks in our simulation: hello flood attack, selective forwarding attack, replay attack, black hole attack, Sybil attack, and sinkhole attack.

### *6.2. Execution of Attacks*

Let $x_a$be the infected node, and at times t it can perform one of the following attacks.

- Hello Flood Attack: Here, $x_a$ It broadcasts the hello packet every 15 M.S. and causes the collision.
- Selective Forwarding Attack: This $x_a$ deliberately fails to forward data packets from neighbours, and a set of neighbour's changes every 50 s.

- Replay Attack: Here $x_a$ overhears traffic from the nearest neighbour and transmission in the replay.
- Blackhole Attack: The infected node $x_a$ miscarries the packets received from its one-hop neighbour.
- Sybil Attacks: Here, $x_a$ will copy the identity of the neighbouring node and thus, the packet to be sent to y will also be sent to $x_a$.
- Sinkhole Attack: The node $x_a$ publicise that it is a sink node.

### *6.3. Valuation of Attacks*

In this section, we discuss the effect of every attack on the performance of the network. Table 8 gives all the simulation parameters. The deployment of the nodes is randomly in the Cooja. The simulation is done in two phases; in the first phase, there is no malicious activity, and in the second phase, a malicious node is included in the network. Figure 7 shows the simulation environment.

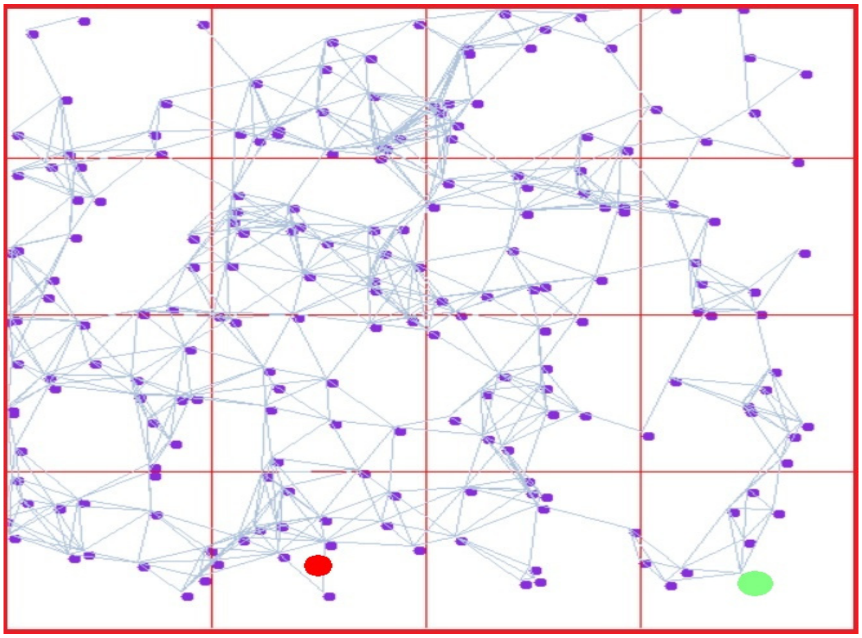

**Figure 7.** Simulation environment.

**Table 8.** Simulation parameters.

| Parameters | Values |
|---|---|
| Simulator | Cooja, simulator of Contiki O.S. |
| Radio Environment | Unit Disk Graph (UDG) |
| Type of nodes | Arago system, Wismote mote |
| Number of nodes | 300 (Contiki MAC) and 1 sink node Malicious Nodes |
| Physical Layer | IEEE802.15.4 |
| MAC Layer | ContikiMAC |
| Network Layer | Contiki RPL |
| Transport Layer | UDP Simulation duration |
| Sending rate | One packet every 5 sec |

The red node is the malicious node, and the green node is the sink node. The malicious node is placed in such a way that it impacts the performance of the network. To analyse the execution of RPL in the comportment of the malicious node, we employ the following matrices:

- Packet Delivery Ratio (PDR): PDR is the ratio of packets successfully received by the sink and the number of nodes sent by the source node. Figure 8 shows the PDR vs. number of attackers. According to the graph, the attacks that reduce PDR are selective forwarding, blackhole, sinkhole, replay, and hello flood attacks. At the same time, the Sybil attack does not affect the PDR with an increase in the number of attackers.
- End-to-end Delay (E2E): E2E is the time taken by the data packet to reach the destination or sink from the source. Figure 9 shows the effect on E2E with the increase in attackers. The attacks that increase E2E are replay attacks, hello flood attacks. On the other hand, the attacks that reduce the E2E are selective forwarding, sinkhole, and blackhole. The attack that does not change either PDR or E2E is the Sybil attack.

The simulation results can be categorised into the following three categories:

- Blackhole, selective forwarding and sinkhole attacks reduce PDR and E2E delay and faster delivery as the malicious node drops data.
- Hello flood and replay attack increase E2E but decreases PDR as the total number of packets increase.
- Sybil attacks do not affect any matrix drastically, as some other matrices are required.

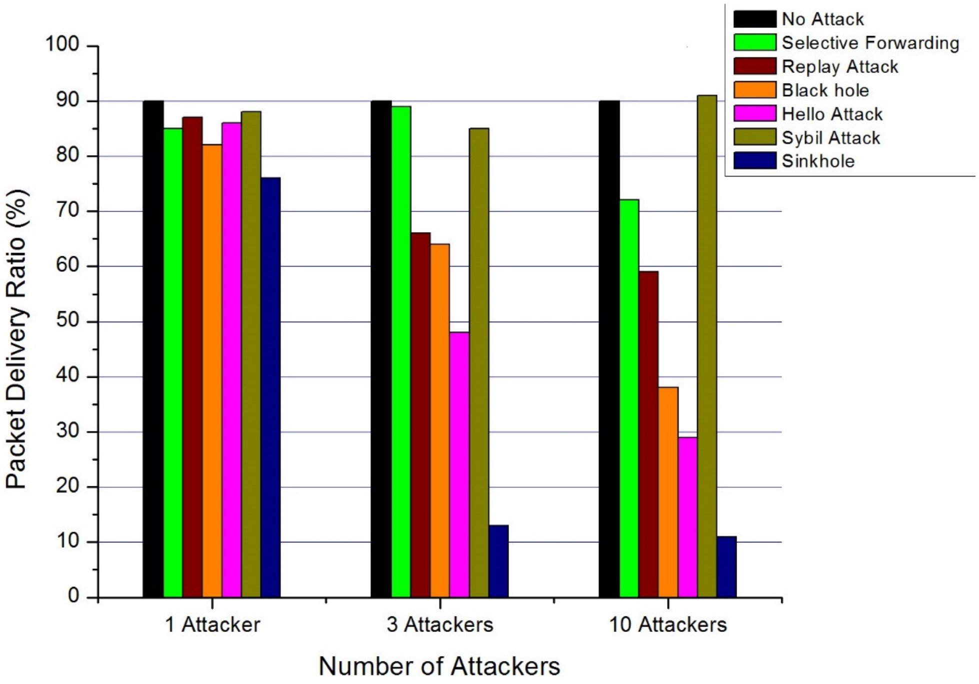

**Figure 8.** Packet delivery ratio vs. no. of attackers.

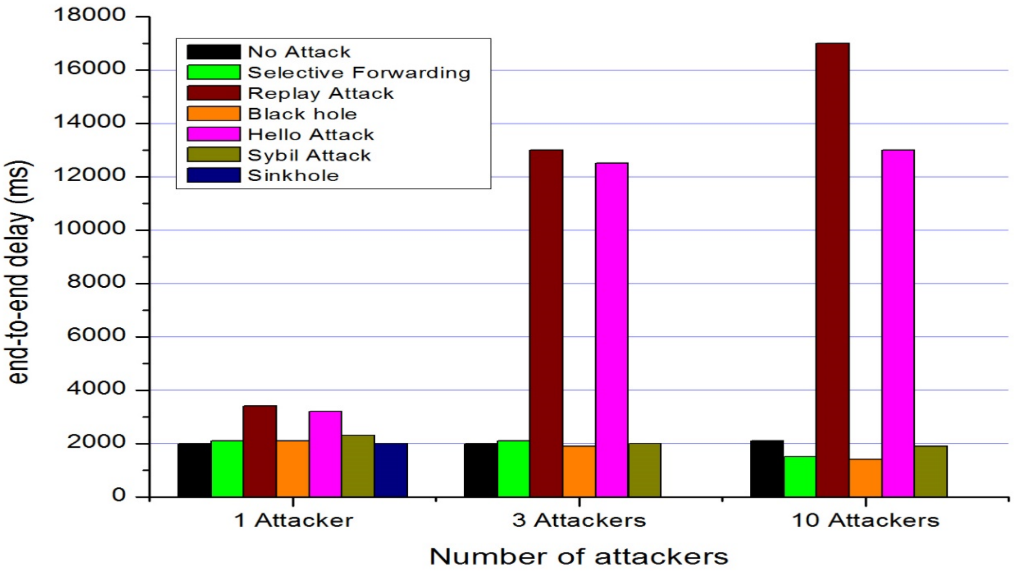

**Figure 9.** End-to-end delay vs. no. of attackers.

### *6.4. Endorsement for Using ContikiOS in Designing Countermeasures*

The regular operation of an IoT can be relentlessly disturbed by various attacks. By encompassing the features of Cooja, we quantified and expediently measured this disturbance. This apprehension of the behaviour and impact is required for protecting the network from unwanted attacks. In this simulation environment, we have reconnoitred two different metrics, but there are many other metrics. The measurement of countermeasures will allow the researchers to build resilience towards the attacks on the network before deploying the sensor network.

## 7. Conclusions

IoT is growing at a very rapid pace day by day. The latest research has extended IoT applications in cyber-physical systems, cloud-based systems, intelligent communities, and many more. IoT comprises a large number of heterogeneous devices. Thus, reliability, scalability and transparency are the key issues that have to be solved. Both high and low-level architecture security needs conceptualisation. This survey deals with studying the challenges for providing secure data transfer and aggregation in sensor networks. There are various resource constraints in WSN and IoT that make it impossible the use traditional security systems. The exclusively designed protocols for secure sensor networks should make the system safe without increasing theoverheads on the network. The future security protocols should be flexible enough to provide security on all the layers of the sensor network without harming the efficiency and increasing the power consumption. In addition to the survey, we have also undertaken a small simulation using Cooja, a simulator of ContikiOS that appropriates the analysis of the network's performance in the comportment of malicious nodes/activities. Several attacks can hamper the overall performance of any sensor network; this survey tries to enlist them and compare them. In the future, we would like to create such a sensor network that has resilience towards built-in attacks, and the actual deployment shall take place after considering the possible attacks on the network to make a WSN and IoT as secure as possible.

**Author Contributions:** Conceptualization, G.S. and S.V.; methodology, G.S., S.V. and N.A.; software, N.A.; validation, G.S., S.V. and N.A.; formal analysis, G.S.; investigation, N.A.; resources, N.A.; data curation, G.S., S.V., C.M. and N.A.; writing—original draft preparation, G.S.; writing—review and editing, G.S., N.A., S.K., C.M. and S.V.; visualisation, G.S. and S.K.; supervision, S.V.;

project administration, S.V.; funding acquisition, S.V. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** The data presented in this study are available upon request from the Corresponding author.

**Acknowledgments:** We are grateful for the anonymous reviewers' hard work and comments that allowed us to improve the quality of this paper.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Basagni, S.; Conti, M.; Giordano, S.; Stojmenovic, I. *Mobile ad Hoc Networking*; John Wiley & Sons: Hoboken, NJ, USA, 2004.
2. Akyildiz, I.F.; Melodia, T.; Chowdhury, K.R. Wireless multimedia sensor networks: A survey. *IEEE Wirel. Commun.* **2007**, *14*, 32–39.
3. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142.
4. Kocakulak, M.; Butun, I. An overview of Wireless Sensor Networks towards the internet of things, In Proceedings of the 2017 IEEE 7th annual computing and communication workshop and conference (CCWC), Las Vegas, NV, USA, 9–11 January 2017; pp. 1–6.
5. Fang, S.; Da Xu, L.; Zhu, Y.; Ahati, J.; Pei, H.; Yan, J.; Liu, Z. An integrated system for regional environmental monitoring and management based on internet of things. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1596–1605.
6. Gope, P.; Hwang, T. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sens. J.* **2015**, *16*, 1368–1376.
7. Li, S.; da Xu, L.; Zhao, S. The internet of things: A survey. *Inf. Syst. Front.* **2015**, *17*, 243–259.
8. Butun, I.; Morgera, S.D.; Sankar, R. A survey of intrusion detection systems in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 266–282.
9. Rawat, D.B.; Brecher, C.; Song, H.; Jeschke, S. *Industrial Internet of Things: Cybermanufacturing Systems*; Springer: Cham, Switzerland, 2017.
10. Forsström, S.; Butun, I.; Eldefrawy, M.; Jennehag, U.; Gidlund, M. Challenges of securing the industrial internet of things value chain. In *2018 Workshop on Metrology for Industry 4.0 and IoT, Brescia Italy*; **2018**, pp. 218–223.
11. Rani, S.; Ahmed, S.H.; Talwar, R.; Malhotra, J.; Song, H. IoMT: A reliable cross-layer protocol for internet of multimedia things. *IEEE Internet Things J.* **2017**, *4*, 832–839.
12. Butun, I.; Sari, A.; Österberg, P. Security implications of fog computing on the internet of things, In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Berlin, Germany, 8–11 September 2019; pp. 1–6.
13. Song, H.; Fink, G.A.; Jeschke, S. *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2021.
14. Song, H.; Srinivasan, R.; Sookoor, T.; Jeschke, S. *Smart Cities: Foundations, Principles, and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2017.
15. Balte, A.; Kashid, A.; Patil, B. Security Issues in the Internet of things (IoT): A survey. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2015**, *5, 450-455.*
16. Butun, I.; Gidlund, M. Location Privacy Assured Internet of Things.. *ICISSP* **2019**, *19*, 1–8.
17. Butun, I.; Österberg, P.; Gidlund, M. Preserving location privacy in cyber-physical systems, In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 1–6.
18. Sohrabi, K.; Gao, J.; Ailawadhi, V.; Pottie, G.J. Protocols for self-organization of a wireless sensor network. *IEEE Pers. Commun.* **2000**, *7*, 16–27.
19. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an analysis of security issues, challenges, and open problems in the internet of things, In Proceedings of the 2015 IEEE world congress on services, New York, NY, USA, 27 June–2 July 2015; pp. 21–28.
20. Yinbiao, S., Lee, K., Lanctot, P., Jianbin, F., Hao, H., Chow, B., & Desbenoit, J. P. Internet of Things: Wireless Sensor Networks. White Paper, International Electrotechnical Commission, *http://www. iec. ch, 11.*
21. Whitman, M.E.; Mattord, H.J. Principles of information security. Cengage Learning, Receive. US Pat. Pers. Identify. Device. (2005). *Wirel. News* **2011**, 1, Fourth Edition
22. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765.
23. Chan, H.; Perrig, A.; Song, D. Random key predistribution schemes for sensor networks. *Symp. Secur. Priv.* **2003**, *2003*, 197–213.
24. Eschenauer, L.; Gligor, V.D. A key-management scheme for distributed sensor networks, In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002; pp. 41–47.
25. Ganeriwal, S.; Čapkun, S.; Han, C.-C.; Srivastava, M.B. Secure time synchronisation service for sensor networks. In Proceedings of the 4th ACM Workshop on Wireless Security, New York, NY, USA, 2 September 2005; pp. 97–106.

26. Perrig, A.; Szewczyk, R.; Tygar, J.D.; Wen, V.; Culler, D.E. SPINS Security protocols for sensor networks. *Wirel. Netw.* **2002**, *8*, 521–534.
27. di Pietro, R.; Mancini, L.V.; Law, Y.W.; Etalle, S.; Havinga, P. "LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. In Proceedings of the 2003 International Conference on Parallel Processing Workshops, Kaohsiung, Taiwan, 6–9 October 2003; pp. 397–406.
28. Liu, D.; Ning, P. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. North Carolina State University. Dept. of Computer Science: Raleigh, NC, USA, 2002.
29. Zhu, S.; Setia, S.; Jajodia, S. LEAP+ Efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans. Sens. Netw.* **2006**, *2*, 500–528.
30. Wood, A.D.; Stankovic, J.A.; Son, S.H. JAM: A jammed-area mapping service for sensor networks. In Proceedings of the RTSS 2003, 24th IEEE Real-Time Systems Symposium, Cancun, Mexico, 3–5 December 2003; pp. 286–297.
31. Cagalj, M.; Capkun, S.; Hubaux, J.-P. Wormhole-based antijamming techniques in sensor networks. *IEEE Trans. Mob. Comput.* **2006**, *6*, 100–114.
32. Ye, F.; Luo, H.; Lu, S.; Zhang, L. Statistical en-route filtering of injected false data in sensor networks. *IEEE J. Sel. Areas Commun.* **2005**, *23*, 839–850.
33. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The Sybil attack in sensor networks: Analysis & defences. In *Third International Symposium on Information Processing in Sensor Networks***; 2004**, Berkeley, CA, USA; pp. 259–268.
34. Hamid, M.A.; Rashid, M.O.; Hong, C.S. Routing Security in sensor network: Hello flood attack and defence. *IEEE NEWS* **2006**, *2*, 2–4.
35. Slijepcevic, S.; Potkonjak, M.; Tsiatsis, V.; Zimbeck, S.; Srivastava, M.B. On communication security in wireless ad-hoc sensor networks. In Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Linz, Austria, 11 June 2002; 139–144.
36. Hu, Y.-C.; Perrig, A.; Johnson, D.B. Packet leashes: A defence against wormhole attacks in wireless networks. In Proceedings of the IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428), San Francisco, CA, USA, 30 March–3 April 2003; Volume 3, pp. 1976–1986.
37. Du, W.; Deng, J.; Han, Y.S.; Varshney, P.K.; Katz, J.; Khalili, A. A pairwise key predistribution scheme for wireless sensor networks. *ACM Trans. Inf. Syst. Secure.* **2005**, *8*, 228–258.
38. Karakehayov, Z. Using REWARD to detect team blackhole attacks in wireless sensor networks. *Wksp. Real-World Wirel. Sens. Netw.* **2005**, 20–21.
39. Anand, N.; Ranjan, R.; Varma, S. MSVR based range-free localisation technique for 3-D sensor networks. *Wirel. Pers. Commun.* **2017**, *97*, 6221–6238.
40. Lai, B.; Kim, S.; Verbauwhede, I. Scalable session key construction protocol for wireless sensor networks. In Proceedings of the IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES), *December-*2002. Los Angeles, CA, USA, Volume 7.
41. Aura, T.; Nikander, P.; Leiwo, J. DOS-resistant authentication with client puzzles. In Proceedings of the International workshop on security protocols, Cambridge, UK, 10–12 April 2000; pp. 170–177.
42. Agah, A.; Das, S.K. Preventing DoS attacks in wireless sensor networks: A repeated game theory approach.. *Int. J. Netw. Secure.* **2007**, *5*, 145–153.
43. Muraleedharan, R.; Osadciw, L.A. Cross-layer denial of service attacks in wireless sensor network using swarm intelligence. In Proceedings of the 2006 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 22–24 March 2006; pp. 1653–1658.
44. Li, K.; Wang, C.; Lei, M.; Zhao, M.-M.; Zhao, M.-J. A Local Reaction Anti-Jamming Scheme for UAV Swarms. In Proceedings of the 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, 18 November–16 December 2020; pp. 1–6.
45. Vasilyev, V.; Shamsutdinov, R. Security analysis of wireless sensor networks using SIEM and multi-agent approach. In Proceedings of the 2020 Global Smart Industry Conference (GloSIC), Chelyabinsk, Russia, 17–19 November 2020; pp. 291–296.
46. Boubiche, D.E.; Athmani, S.; Boubiche, S.; Toral-Cruz, H. Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions.. *Wirel. Pers. Commun.* **2021**, *117*. P-177-213
47. Karthigha, M.; Latha, L.; Sripriyan, K. A comprehensive survey of routing attacks in wireless mobile ad hoc networks. In Proceedings of the 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26–28 February 2020; pp. 396–402.
48. Accettura, N.; Piro, G. Optimal and secure protocols in the IETF 6TiSCH communication stack. In Proceedings of the 2014 IEEE 23rd International Symposium on Industrial Electronics (ISIE), Istanbul, Turkey, 1–4 June 2014; pp. 1469–1474.
49. Glissa, G.; Meddeb, A. 6LowPSec: An end-to-end security protocol for 6LoWPAN. *Ad Hoc Netw.* **2019**, *82*, 100–112.
50. Salau, A.O.; Marriwala, N.; Athaee, M. Data Security in Wireless Sensor Networks: Attacks and Countermeasures. In *Mobile Radio Communications and 5G Networks*; Springer: 2021; pp. 173–186, Kurukshetra, India.
51. Kanthuru, V.A.; Kumar, K.A. Black Hole Detection and Mitigation Using Active Trust in Wireless Sensor Networks. In *Advances in Distributed Computing and Machine Learning;* Springer: 2021, pp. 25–34, Vellore, India
52. Kaushik, I.; Sharma, N. Blackhole attack and its security measure in wireless sensors networks. In *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*; Springe: 2020, pp. 401–416, ISBN:978-3-030-40305-8.

53. Gurung, S.; Chauhan, S. A survey of black hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability. *Wirel. Netw.* **2020**, *26*, 1981–2011.
54. Lim, J.; Keum, D.; Ko, Y.-B. A stepwise and hybrid trust evaluation scheme for tactical wireless sensor networks. *Sens. Vol.* **2020**, *20*, 1108.
55. Teng, L.; Zhang, Y. SeRA: A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks. *Second. Int. Conf. Comput. Modeling Simul.* **2010**, *4*, 79–82.
56. Butun, I.; Ra, I.-H.; Sankar, R. An intrusion detection system based on multilevel clustering for hierarchical wireless sensor networks. *Sensors* **2015**, *15*, 28960–28978.
57. Zhang, Y.; Liu, W.; Lou, W.; Fang, Y. Location-based compromise-tolerant security mechanisms for wireless sensor networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 247–260.
58. Duan, M.; Xu, J. An efficient location-based compromise-tolerant key management scheme for sensor networks. *Inf. Process. Lett.* **2011**, *111*, 503–507.
59. Dvir, A.; Buttyan, L. VeRA-version number and rank authentication in RPL. In Proceedings of the 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, Spain, 17−22 October 2011; pp. 709–714.
60. Perrey, H.; Landsmann, M.; Ugus, O.; Schmidt, T.C.; Wählisch, M. TRAIL: Topology authentication in RPL. *arXiv* **2013**, arXiv1312.0984.
61. Mayzaud, A.; Sehgal, A.; Badonnel, R.; Chrisment, I.; Schönwälder, J. A study of RPL DODAG version attacks. In Proceedings of the IFIP international conference on autonomous infrastructure, management and security, Zurich, Switzerland, 10-13 July 2014; pp. 92–104.
62. Song, S.; Choi, H.-K.; Kim, J.-Y. A secure and lightweight approach for routing optimisation in mobile IPv6. *EURASIP J. Wirel. Commun. Netw.* **2009**, *2009*, 1–10.
63. Singh, M.; Rajan, M.A.; Shivraj, V.L.; Balamuralidhar, P. Secure MQTT for the internet of things (IoT). In Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015; pp. 746–751.
64. Neisse, R.; Steri, G.; Baldini, G. Enforcement of security policy rules for the internet of things. In Proceedings of the 2014 IEEE 10th international conference on wireless and mobile computing, networking and communications (WiMob), Larnaca, Cyprus, 8–10 October 2014; pp. 165–172.
65. Rahman, R.A.; Shah, B. Security analysis of IoT protocols: A focus in CoAP. In Proceedings of the 2016 3rd MEC international conference on big data and smart city (ICBDSC), Muscat, Oman, 15–16 March 2016; pp. 1–7.
66. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Netw.* **2003**, *1*, 293–315.
67. Rafaeli, S.; Hutchison, D. c *ACM Comput. Surv.* **2003**, *35*, 309–329.
68. Deering, S.; Hinden, R. *Internet Protocol, Version 6 (IPv6) Specification*; RFC 2460;Pub.: RFC Editor, 1998.
69. Howitt, I.; Gutierrez, J.A. IEEE 802.15. 4 low rate-wireless personal area network coexistence issues. In Proceedings of the 2003 IEEE Wireless Communications and Networking, New Orleans, LA, USA, 16–20 March 2003; Volume 3, pp. 1481–1486.
70. Chen, F.; Talanis, T.; German, R.; Dressler, F. Real-time enabled IEEE 802.15. 4 sensor networks in industrial automation. In Proceedings of the 2009 IEEE International Symposium on Industrial Embedded Systems, Lausanne, Switzerland, 8–10 July 2009; pp. 136–139.
71. Han, D.-M.; Lim, J.-H. Smart home energy management system using IEEE 802.15. 4 and ZigBee. *IEEE Trans. Consum. Electron.* **2010**, *56*, 1403–1410.
72. Granjal, J.; Monteiro, E.; Silva, J.S. Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1294–1312.
73. Daidone, R.; Dini, G.; Tiloca, M. On experimentally evaluating the impact of security on IEEE 802.15. 4 networks. In Proceedings of the 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Barcelona, Spain 27–29 June 2011; pp. 1–6.
74. Xiao, Y.; Sethi, S.; Chen, H.-H.; Sun, B. Security services and enhancements in the IEEE 802.15. 4 wireless sensor networks. In Proceedings of the GLOBECOM'05. IEEE Global Telecommunications Conference, St. Louis, MO, USA, 28 Nov.−2 Dec, 2004;Volume 3, pp. 5.
75. O'Flynn, C.P. Message denial and alteration on IEEE 802.15. 4 low-power radio networks. In Proceedings of the 2011 4th IFIP International Conference on New Technologies, Mobility and Security, Paris, France, 7−10 Feb 2011; pp. 1–5.
76. Polastre, J.; Hill, J.; Culler, D. Versatile, low power media access for wireless sensor networks. In Proceedings of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 3−5 Nov. 2004; pp. 95–107.
77. Law, Y.W.; Palaniswami, M.; van Hoesel, L.; Doumen, J.; Hartel, P.; Havinga, P. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. *ACM Trans. Sens. Netw.* **2009**, *5*, 1–38.
78. Palattella, M.R. et al., Standardised protocol stack for the internet of (important) things. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 1389–1406.
79. Winter, T. et al., RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. *RFC* **2012**, *6550*, 1–157.
80. Le, A.; Loo, J.; Lasebae, A.; Aiash, M.; Luo, Y. 6LoWPAN: A study on QoS security threats and countermeasures using intrusion detection system approach. *Int. J. Commun. Syst.* **2012**, *25*, 1189–1212.

81. Moeller, S.; Sridharan, A.; Krishnamachari, B.; Gnawali, O. Routing without routes: The backpressure collection protocol. In Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, Stockholm, Sweden,12–16 April, 2010; pp. 279–290.
82. Gnawali, O.; Fonseca, R.; Jamieson, K.; Moss, D.; Levis, P. Collection tree protocol. In Proceedings of the 7th ACM conference on embedded networked sensor systems, Barkeley, CA, USA, 4–6 Nov 2009; pp. 1–14.
83. Bormann, C.; Castellani, A.P.; Shelby, Z. Coap: An application protocol for billions of tiny internet nodes. *IEEE Internet Comput.* **2012**, *16*, 62–67.
84. Raymond, D.R.; Marchany, R.C.; Brownfield, M.I.; Midkiff, S.F. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. *IEEE Trans. Veh. Technol.* **2008**, *58*, 367–380.
85. Oliveira, L.M.L.; Rodrigues, J.J.P.C.; de Sousa, A.F.; Lloret, J. A network access control framework for 6LoWPAN networks. *Sensors* **2013**, *13*, 1210–1230.
86. Raza, S.; Duquennoy, S.; Chung, T.; Yazar, D.; Voigt, T.; Roedig, U. Securing Communication in 6LoWPAN with Compressed IPsec. In Proceedings of the 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Barcelona, Spain, 27–29 June 2011; pp. 1–8.
87. Kim, H. Protection against packet fragmentation attacks at 6LoWPAN adaptation layer. In Proceedings of the 2008 International Conference on Convergence and Hybrid Information Technology, Daejeon, Korea, 28–30 August 2008; pp. 796–801.
88. Hummen, R.; Hiller, J.; Wirtz, H.; Henze, M.; Shafagh, H.; Wehrle, K. 6LoWPAN fragmentation attacks and mitigation mechanisms. In Proceedings of the Sixth ACM Conference on Security and privacy in wireless and mobile networks, Budapest, Hungary, 17–19 April, 2013; pp. 55–66.
89. Wallgren, L.; Raza, S.; Voigt, T. Routing attacks and countermeasures in the RPL-based internet of things. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 794326, 2013.
90. Heurtefeux, K.; Erdene-Ochir, O.; Mohsin, N.; Menouar, H. Enhancing RPL resilience against routing layer insider attacks. In Proceedings of the 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, Gwangiu, South Korea, 24 March 2015; pp. 802–807.
91. Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2661–2674.
92. Lu, Z.; Sagduyu, Y.E.; Li, J.H. Securing the backpressure algorithm for wireless networks. *IEEE Trans. Mob. Comput.* **2016**, *16*, 1136–1148.
93. Venkataraman, R.; Moeller, S.; Krishnamachari, B.; Rao, T.R. Trust-based backpressure routing in wireless sensor networks. *Int. J. Sens. Netw.* **2015**, *17*, 27–39.
94. Sultana, S.; Midi, D.; Bertino, E. Kinesis: A security incident response and prevention system for wireless sensor networks. In Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems, New York, NY, USA, 3–6 November 2014; pp. 148–162.
95. Sharma, G.; Vidalis, S.; Menon, C.; Anand, N.; Kumar, S. Analysis and Implementation of Threat Agents Profiles in Semi-Automated Manner for a Network Traffic in Real-Time Information Environment. *Electronics* **2021**, *10*, 1849.
96. Korzun, D.; Balandina, E.; Kashevnik, A.; Balandin, S.; Viola, F. *Ambient Intelligence Services in IoT Environments: Emerging Research and Opportunities: Emerging Research and Opportunities*; IGI Global: Pennsylvania, US, 2019.
97. Gurtov, A.; Liyanage, M.; Korzun, D. Secure communication and data processing challenges in the Industrial Internet. Balt. J. Mod. Comput. **2016**, *4*, 1058–1073.
98. Burg, A.; Chattopadhyay, A.; Lam, K.-Y. Wireless communication and security issues for cyber-physical systems and the Internet-of-Things. *Proc. IEEE* **2017**, *106*, 38–60.
99. Fagan, M.; Megas, K.; Scarfone, K.; Smith, M. Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft). In *National Institute of Standards and Technology*, CSRC, USA, 2019.
100. Sikder, A.K.; Petracca, G.; Aksu, H.; Jaeger, T.; Uluagac, A.S. A survey on sensor-based threats to internet-of-things (IoT) devices and applications. *arXiv* **2018**, arXiv1802.02041.
101. Osborne, C. Meet torii, a new iot botnet far more sophisticated than mirai variants. Available online: https//www. zdnet. com/article/meet-torii-a-new-iot-botnet-far-more-sophisticated-than-mirai (accessed on 28 September 2018).
102. Lin, C.; He, D.; Kumar, N.; Choo, K.-K.R.; Vinel, A.; Huang, X. Security and privacy for the internet of drones: Challenges and solutions. *IEEE Commun. Mag.* **2018**, *56*, 64–69.
103. Zhang, N., Demetriou, S., Mi, X., Diao, W., Yuan, K., Zong, P., Qian, F., Wang, X., Chen, K., Tian, Y. and Gunter, C.A., Understanding IoT security through the data crystal ball: Where we are now and where we are going to be. *arXiv* **2017**, arXiv1703.09809, 2017.
104. Yahuza, M.; et al., Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges. *IEEE Access* **2021**, *9*, 57243–57270.
105. Paredes, C.M.; Martínez-Castro, D.; Ibarra-Junquera, V.; González-Potes, A. Detection and Isolation of DoS and Integrity Cyber Attacks in Cyber-Physical Systems with a Neural Network-Based Architecture. *Electronics* **2021**, *10*, doi:10.3390/electronics10182238.
106. Dunkels, A.; Gronvall, B.; Voigt, T. Contiki-a lightweight and flexible operating system for tiny networked sensors. In Proceedings of the 29th annual IEEE international conference on local computer networks, Tampa, FL, USA, 16–18 Nov., 2004; pp. 455–462.