11-13-2019

Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures

Ismail Butun
Member, IEEE

Houbing Song
Embry-Riddle Aeronautical University, SONG4@erau.edu

Patrik Osterberg
Mid Sweden University

Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures

Ismail Butun, *Member, IEEE,* Patrik Österberg, *Member, IEEE,*
and Houbing Song, *Senior Member, IEEE*

Abstract—Wireless Sensor Networks (WSNs) constitute one of the most promising third-millennium technologies and have wide range of applications in our surrounding environment. The reason behind the vast adoption of WSNs in various applications is that they have tremendously appealing features, e.g., low production cost, low installation cost, unattended network operation, autonomous and longtime operation. WSNs have started to merge with the Internet of Things (IoT) through the introduction of Internet access capability in sensor nodes and sensing ability in Internet-connected devices. Thereby, the IoT is providing access to huge amount of data, collected by the WSNs, over the Internet. However, owing to the absence of a physical line-of-defense, i.e. there is no dedicated infrastructure such as gateways to watch and observe the flowing information in the network, security of WSNs along with IoT is of a big concern to the scientific community. More specifically, for the application areas in which CIA (confidentiality, integrity, availability) has prime importance, WSNs and emerging IoT technology might constitute an open avenue for the attackers. Besides, recent integration and collaboration of WSNs with IoT will open new challenges and problems in terms of security. Hence, this would be a nightmare for the individuals using these systems as well as the security administrators who are managing those networks. Therefore, a detailed review of security attacks towards WSNs and IoT, along with the techniques for prevention, detection, and mitigation of those attacks are provided in this paper. In this text, attacks are categorized and treated into mainly two parts, most or all types of attacks towards WSNs and IoT are investigated under that umbrella: "Passive Attacks" and "Active Attacks". Understanding these attacks and their associated defense mechanisms will help paving a secure path towards the proliferation and public acceptance of IoT technology.

Index Terms—Cryptography, Detection, DoS, IoT, Prevention, Survey, WSN, 6LowPAN, RPL, Block-chain, TSCH, MQTT, CoAP, CoAPs, 6LowPSec, 6TiSCH.

1 Introduction

Recent developments in wireless communications and Micro Electro Mechanical Systems (MEMS) technologies facilitated the design of Wireless Sensor Networks (WSNs), in which sensor nodes collect the intelligible data from their surrounding environments and share them in a wireless fashion to send the information towards a meaningful data sink. According to scientific predictions, the total number of wireless sensors deployed is expected to reach 60 trillion at the end of the year 2022, meaning 10 thousand sensors for every person on the world [1]. Therefore, all the problems and challenges concerning WSNs will expose plentiful topics for the researchers.

Owing to their easy and cheap deployment features, WSNs has wide-scale application areas in science as shown in Fig. 1: To monitor environment-related events (such as wildfire, earthquake, ocean, pollution, water quality, wildlife), to collect information regarding human-related activities and observation of human behavior (such as elder-care, nursery, healthcare), to provide mission-critical information (such as military operations, highway traffic); to monitor industrial sites (such as industrial automation, manufacturing machinery performance), and so on [2].

Internet of Things (IoT) is revolutionizing the IT sector and will be next big leap of the technology following Internet. IoT market is expected to grow from more than 15 billion devices in 2015 to more than 75 billion in 2025 [3]. This prediction means that on average, each person on earth will have at least 25 personal IoT devices in 7 years time. Henceforth, IoT is expected to have a dramatic impact on our lives in near future [4]. During this period, WSNs will be integrated into IoT and innumerable sensor nodes will join the Internet aiming at cooperating with other nodes to sense and monitor their environment. IoT will provide an interaction between people and environment by using the WSNs more and more in near future [5]. For instance, our earth will benefit from this integration by the result of the increased environmental awareness [6].

The vision behind IoT is to let people and smart things to be connected at any time, in any place, to anything and anyone, via any network and service [7]. So by following this vision, application areas of IoT will increase continuously and dramatically for every aspect of life. For example, nowadays, with the diverse installation of IoT devices, we are able to remotely sense and act upon situations regarding our houses or offices. E.g. in an event of intrusion to the premises, an alert can reach to our smartphone asking immediate attention or trigger an automatic response on

- *I. Butun is the corresponding author of this manuscript.*
  I. Butun is with Department of Computer Science and Engineering, Chalmers University of Technology, Gothenburg, Sweden.
  E-mail: ismail.butun@chalmers.se
- *P. Osterberg is with Department of Information Systems and Technology (IST), Mid Sweden University, Sundsvall, Sweden.*
  E-mail: patrik.osterberg@miun.se
- *H. Song is with Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, FL, USA.*
  E-mail: h.song@ieee.org

Manuscript received March 5, 2019.

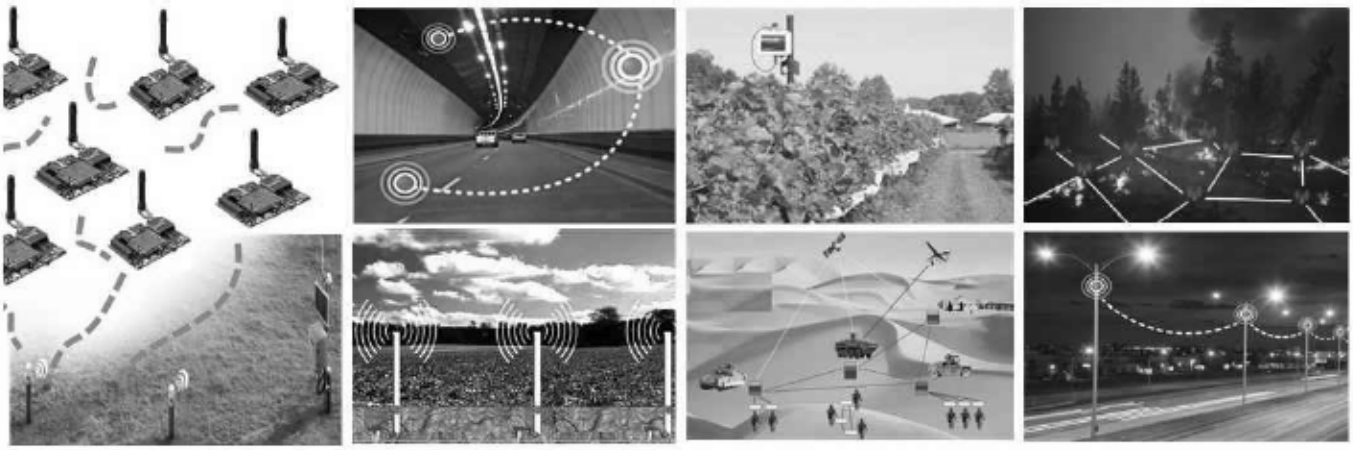

Fig. 1. Various application fields of IoT enabled WSNs.

our behalf. The pictures and videos being taken can be sent directly to the police so that they may approach the crime scene better prepared with the intelligence they gathered in advance.

Security in WSNs and IoT, is an important issue, especially if they are commissioned for mission-critical tasks. For instance, in tactical military applications where a security gap in the network could cause casualties for the friendly forces on a battlefield. Another example would be from health-care sector (IoT applications): A recent paper [8] revealed that most of the current used systems fail to embed strong security services that could be preserve patient privacy. None of the patients would be happy if their confidential health data were exposed through the leakages from misbehaving nodes or due to system failures.

Algorithms and methodologies designed for securing WSNs will be relevant to any IoT that comprises one or more sensor networks. As also mentioned earlier, WSNs most probably will be integrated with IoT in the near future [9]. Therefore, all cyber-security related issues, especially attacks, their prevention and mitigation are very important for establishing secure and reliable IoT.

WSNs are vulnerable to a wide range of attack types which might put critical threats to the security of those networks. Therefore these attack types need to be investigated thoroughly. Security related attacks against WSNs can be branched into two main categories: Active attacks and Passive attacks. In the *passive attacks* category, attackers are generally hidden (camouflaged) and either damage the functioning components of the network; or tap the communications link to collect useful information. Passive attacks can also be further categorized into eavesdropping, node destruction, node malfunctioning, node outage and traffic analysis types. Whereas in the *active attacks* category, an attacker effects the functions and operations of the targeted network. The result of this ill-effect can be the real objective of the attacker and can also be detected by security mechanisms (intrusion detection). For instance, network services might be vulgarized as a consequence of this type of attacks. Active attacks can also be further categorized into jamming, flooding, Denial-of-Service (DoS), blackhole, wormhole, sinkhole and Sybil types.

In Computer Science, solutions to defend against security attacks towards networks comprise of three essential components [2]:

- Prevention: This component aims at preventing attacks before they happen. In this case, any proposed method needs to be able to devise measures to defend against the specific type of attack(s). Intrusion prevention mechanisms can resist external attackers towards WSNs and IoT, but they are not specifically designed to resist the internal attackers.
- Detection: In an event of an attack, if an adversary manages to advance the measures taken by the prevention component, this means that defense against the attack has failed. At the moment, security solutions that are devised for the detection component of the related attack would take in-charge and work at especially in identifying those nodes that are compromised. The only way of reacting against ongoing attacks, especially internal attacks, is using the Intrusion Detection Systems (IDSs). After an intrusion is detected, then a mitigation mechanism would be issued to minimize the adverse effects of the ongoing attack.
- Mitigation: Final component aims at mitigating attacks after they happen, for example, in order to secure network, a security measure should be taken, such as 'dismissing the affected nodes in a network' or 'disabling the ports of a computer which were used during the attack'.

Thereby, all these three components constitute a whole security structure and cannot be considered separately in defending WSNs and IoT against diverse kinds of attacks.

In the literature, various surveys are provided to present security issues in WSNs: Butun *et al.* [2] provided a survey of intrusion detection systems, Zhu *et al.* [10] provided a survey of detecting node replication attacks, Chen and Chao [11] provided a survey of key distribution, Han *et al.* [12] provided a survey of trust management. Finogeev *et al.* [13] provided a survey on attacks and security in WSNs of industrial SCADA systems. Following publications provided limited surveys of security issues and attacks against

WSNs (and IoT) and their classifications: Padmavathi and Shanmugapriya [14], Pathan *et al.* [15], Shabana *et al.* [16], Bartariya and Rastogi [17], Sharma and Ghose [18], and Borgohain *et al.* [19]. However, according to the best of our knowledge, the survey provided in this paper is the most comprehensive and the detailed one covering all the attacks towards WSNs along with their related detection, prevention, and mitigation techniques. Besides, our paper also provides a path to defend IoT, by considering the lessons learned while securing WSNs.

Security analysis of sub-domains of IoT, such as LPWAN networks, is omitted in this manuscript. E.g., readers that are interested in the security of LoRaWAN can refer to following works: Butun *et al.* [20], [21], Eldefrawy *et al.* [22], Haxhibeqiri *et al.* [23], and Sinha *et al.* [24]. Privacy and trust related issues of IoT are also omitted in this text, in order to keep the focus on "attacks and mitigation". Readers that are interested in that specific topic may refer to following works: Butun [25], Chen *et al.* [26], Ott *et al.* [27], Sicari *et al.* [28], and Yan *et al.* [29].

Security of the IoT is a very wide (attacks and their counter-measures, privacy, trust, key-distribution, patch-management, access-control, etc.) and also an emerging topic. Hence, the aim of this survey is to present all cyber-security attacks against WSNs and IoT along with their related defense mechanisms. We believe that this would shed light on researchers who are considering to devise security algorithms for IoT. For this sake, we also provide a section discussing the state-of-art networking technologies in IoT. However, additional reading is advised as follows: Shelby *et al.* [30] and Hartke [31] for CoAP, Banks *et al.* [32] and Yokotani *et al.* [33] for MQTT, Brandt *et al.* [34] and Zhang *et al.* [35] for RPL, Nikshepa *et al.* [36] and Fabre *et al.* [37] for 6LoWPAN, Dujovne *et al.* [38] and Watteyne *et al.* [39] for 6TiSCH, and finally Chang *et al.* [40] and Watteyne *et al.* [41] for TSCH.

In this survey, prevention, detection, and mitigation of attacks towards WSNs and IoT is the topic of interest. Therefore, the rest of the paper is organized as follows: Section 1.1 briefly overviews the definition of IoT along with trends, impact and future projections. Section 2 presents various types of attacks towards the WSNs and IoT. Section 3 provides the defense strategies including prevention, detection, and mitigation, against those attacks mentioned in Section 2. Cyber-security of IoT including open challenges, cyber-attacks, and defense mechanisms are discussed in Section 4. Section 5 presents unique security solutions in the field, discusses the inclusion of security during WSN-IoT integration, and presents final remarks. Section 6 concludes the paper. List of abbreviations is presented in the Appendix section.

1.1 Internet of Things: Definition, Trends, Impact, and Future Projections

The term "Internet of things" was coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999. Since then, the Internet of Things (IoT) has rapidly evolved into a field that involves the interconnection and interaction of smart objects, which are objects or devices with embedded sensors, on-board data processing capability, and a means of communication, to provide automated services

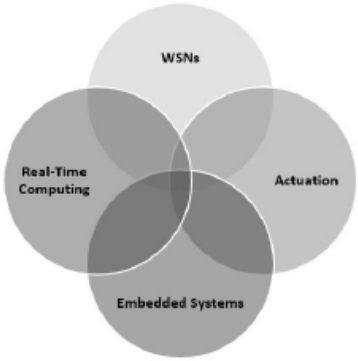

Fig. 2. IoT is the Confluence of Several Technologies.

and applications [4], [42], [43]. Rather than a single technology, IoT involves the convergence of WSNs, real-time computing, embedded systems, and actuation technologies [44], as shown in Fig. 2.

Today, most of what we consider as IoT is a variety of largely stand-alone devices and isolated systems, such as wearable fitness monitors [45], smart watches, smart phones, home thermostats and lighting [46], and remote video streaming [47]. Emerging IoT implementations will use smaller and more energy- efficient embedded sensor technologies, enhanced communications, advanced data analytics, and more sophisticated actuators to collect and aggregate information and enable intelligent systems that understand context, track and manage complex interactions, and anticipate requirements [48], [49], [50], [51], [52].

IoT is expected to become ubiquitous, with implementations in the smart home for management of energy use, control of appliances, monitoring of food and other consumables [46], [47], [53], [54]; consumer applications such as health and fitness monitoring, condition diagnosis [45]; manufacturing and industrial settings for supply chain management, robotic manufacturing, quality control, health and safety compliance [42]; utility grids and other critical infrastructure for grid optimization, automated fault diagnosis, automated cyber security monitoring and response [53]; and automotive/transportation for optimization for driving conditions, assessing driver alertness, collision/accident avoidance, and managing vehicle health [55], [56].

IoT is a networking infrastructure for Cyber-physical systems (CPS) [42], which are engineered systems that are built from, and depend upon, the seamless integration of computation and physical components [44]. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability. CPS technologies are transforming the way people interact with engineered systems, just as the Internet has transformed the way people interact with information. CPS have been applied successfully in a range of application domains including agriculture, aeronautics, building design, civil infrastructure, energy, environmental quality, healthcare and personalized medicine, manufacturing, and transportation [44].

Innovations in IoT potentially impact a variety of applications and services, such as connected cities and homes, smart transportation, smart agriculture, industrial IoT, and

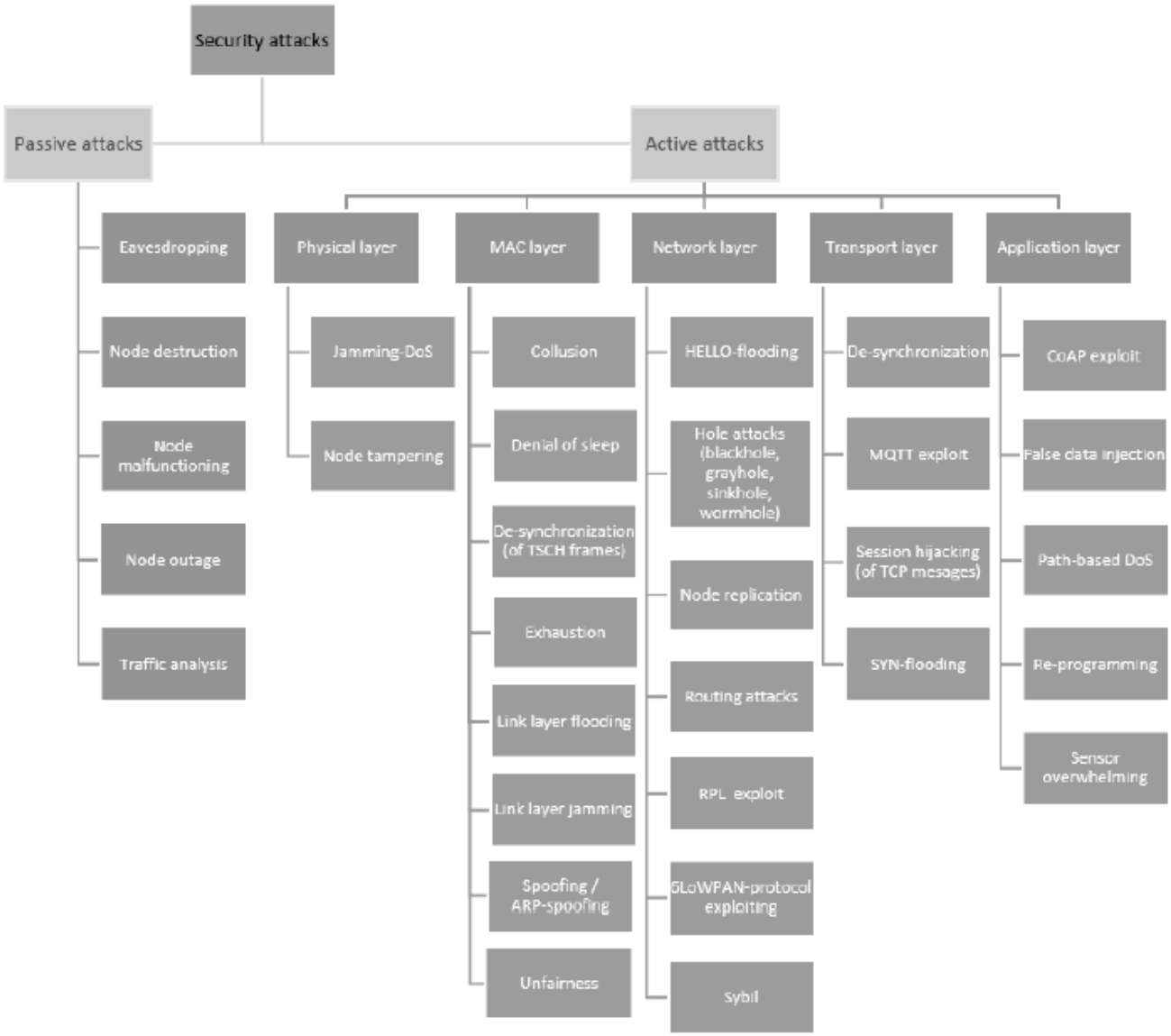

Fig. 3. Security attacks towards the WSNs and IoT - OSI stack protocol layered description.

retail IoT. IoT enabled smart and connected communities will bring about new levels of economic opportunity and growth, safety and security, health and wellness, and overall quality of life [54]. IoT enabled smart transportation will provide improved safety, mobility, and energy conservation in the development and operation of the highway system [55]. Smart agriculture will deliver food, fiber, fuel, and feed within a changing global climate while reducing agriculture's environmental footprint and managing biotic threats to production [44]. Industrial IoT will enable an increasingly wide range of value-added manufacturing services by being intelligent, precise, predictable, reliable, secure, and adept with fabricating new materials; connected and broadly accessible, with capabilities that are transparent to users; connected to applications that reside in the cloud and plug into an expansible, interactive architecture; accessible at low cost to innovators and entrepreneurs, including both users and providers of manufacturing services; clean, green, and resource-efficient; and resilient to disruptions [42]. Retail IoT will increase business efficiency, drive more sales and improve customer satisfaction [54].

2 Attacks towards the WSNs and IoT

In the literature, there is a variety of classifications for attacks towards the WSNs [14], [57], [58], [59], [60], [61], [62], [63]. Among these, we will consider the activity of the attacker (passive/active) as main categorization and the targeted Open Systems Interconnection (OSI) model (layered description of stack protocol) as sub-classifications as shown in Fig. 3. Following subsections include descriptions of each item in the Fig. 3:

2.1 Passive Attacks

Passive attacks are performed in a way that it cannot be sensed by any means. This is because of the fact that the adversaries do not make any radio emissions. Since wireless links are easier to tap, wireless networks are more susceptible to passive attacks, such as eavesdropping, which can be performed easily listening to the wireless communication amongst sensor nodes in the WSN without capturing any of them. Passive attacks are mainly against data confidentiality.

In passive attacks, attackers are typically camouflaged, i.e. hidden, and tap the communication lines to collect data. Passive attacks can be grouped into eavesdropping, node malfunctioning, node tampering/destruction, node outage and traffic analysis types (see Fig. 3) [1].

Here, it is important to state that node malfunctioning, node outage and node tampering are considered as *active attacks* in some papers [14], [57], [58], [59], [60], [61], [62], [63]. We present them as *passive attacks* in this paper, hence they do not introduce big concern (they do not constitute a single point of failure, as the network can continue its operation without the contribution of the failed nodes!) to the network compared to other more impactive active attacks.

2.1.1 Passive Information Gathering (Eavesdropping)

Eavesdropping is also known as "Passive information gathering". Classified data can be eavesdropped by tapping communication lines. Hence wireless links are easier to tap, wireless networks are more susceptible to passive attacks. Since WSNs use short-range communications, an attacker must be in proximity in order to gather useful information by eavesdropping. WSNs are a little more secure against tapping compared to other long-range wireless technologies because signals are sent over shorter distances. Interception of the messages transmitted through WSNs might reveal following useful information: physical location of specific nodes such as cluster heads, gateways, key distribution centers, etc.; message identities (IDs), timestamps, other fields, almost anything that is not encrypted.

2.1.2 Node Destruction

Physical destruction (with the usage of electrical surge, physical force or ammunition) of the nodes by any means.

2.1.3 Node Malfunctioning

This may happen due to many different factors from faulty sensors or energy depletion due to sensor overwhelming or other DoS attacks.

2.1.4 Node Outage

This attack occurs whenever a node fails its regular functionality. For example, if a cluster head of a heterogeneous network fails at regular operation, then the WSN protocols have to be strong enough to mitigate the negative effects of this kind of node outages, by electing new cluster heads and/or providing alternate routes for network paths.

2.1.5 Traffic Analysis

The traffic pattern of a network may be as valuable as the content of data packets for adversaries. Important information about the networking topology can be derived by analyzing traffic patterns. In WSNs, the nodes closer to the base station, i.e. the sink, make more transmissions than the other nodes because they relay more packets than the nodes farther from the base station. Similarly, clustering is an important tool for scalability in WSNs and cluster heads are busier than the other nodes in the network. Detection of the base station, the nodes close to it or cluster heads may be very useful for adversaries because a denial-of-service attack against these nodes or eavesdropping the packets destined for them may have a greater impact. By analyzing the traffic, this kind of valuable information can be derived. Moreover, traffic patterns can pertain to other confidential information such as actions and intentions. In tactical communications, silence may indicate preparation for an attack, a tactical move or infiltration. Similarly, a sudden increase in the traffic rate may indicate the start of a deliberate attack or raid.

2.2 Active Attacks

In the active attacks, malicious acts are carried out not only against data confidentiality but also data integrity. Active attacks can also aim for unauthorized access and usage of the resources or the disturbance of an opponent's communications. An active attacker makes a radio emission or action that can be sensed by the WSN elements [61]. An example is DoS attack in the physical and/or network layer that would cause network elements to drop data packets.

A Denial-of-Service (DoS) attack mainly targets the availability of network services. A DoS is generally explained as any kind of situation that consumes resources and diminishes the capacity of a network, therefore diverts the network from performing its expected functionality correctly or in a timely manner. A node is isolated from the rest of the network by blocking the incoming and outgoing packets. In DoS attack, an adversary attempts to prevent legitimate and authorized users of services offered by the network from accessing those services. The classic way to achieve this is to flood packets to any centralized resource (access point) used in the network so that the resource is no longer available to the nodes in the network, resulting in the network no longer operating what was designed for. This may lead to a failure in the delivery of guaranteed services to the end users.

In the active attacks, an adversary actually affects the operations of the attacked network. This effect may be the objective of the attack and can be detected. For example, the networking services may be degraded or terminated as a result of these attacks. Sometimes the adversary tries to stay undetected, aiming to gain unauthorized access to the system resources or threatening confidentiality and/or integrity of the content of the network. Active attacks of our interest (for WSNs) are grouped into five main groups, by following the OSI stack protocol layered structure, as shown in Fig. 3.

The OSI network structure consists of 5 layers for WSNs (and IoT) as described in [5]: Physical, Data-Link (MAC), Network, Transport, and Application. It should be noted

that Session and Presentation layers of the traditional OSI network model are all considered in the Application layer of WSNs (and IoT).

2.2.1 Attacks towards Physical Layer

2.2.1.1 Jamming DoS: It is a DoS attack at the physical layer [62]. A malicious device can jam a signal by transmitting at the same frequency. The jamming signal contributes to the noise in the carrier and its strength is enough to reduce the signal-to-noise ratio below the level that the nodes using that channel need to receive data correctly. Jamming can be conducted continuously in a region, which thwarts all the nodes in that region from communication. Alternatively, jamming can be done temporarily with random time intervals, which can still very effectively hamper the transmissions.

2.2.1.2 Node Capture (Tampering): An adversary takes over the control of the sensor node by a physical attack, e.g. attaching cables to its circuit board and reading stored data as well as ongoing transmission in the WSN [1]. Besides, by tampering adversaries can change the original wiring of the electronic board or change the content of the memory of the nodes and use the captured slave node by any means. Capturing a node might expose its critical data, especially revealing of cryptography-related keys and therefore might cause compromisation of the whole WSN. Two problems arise in this case:

- Captured node can make arbitrary queries on behalf of the attacker (DoS attack against availability).
- Captured node can provide false data to the legitimate users (attack against integrity).

2.2.2 Attacks towards Data Link Layer

The algorithms in the data link layer, especially MAC schemes, present many exploitation opportunities for DoS attacks. For example, MAC layer DoS attacks may continuously jam a channel. More complex DoS attacks can be designed based on MAC layer addressing schemes. Data link layer attacks are categorized as follows: Collision, denial of sleep, de-synchronization, exhaustion, flooding, link layer jamming, spoofing, and unfairness.

2.2.2.1 Collision: In collision attack, an adversary starts transmitting packets from the same channel of a legitimate node of the network, whenever the legitimate one starts transmission. Hence, as a result, both transmitted packets collide and the targeted receiver does not receive the whole meaningful packet from the transmitter due to the collision loss in the transmission. Hence it is useless, the received packet is discarded and the transmitter is asked for re-transmission of the packet [19]. Causing collusions of a single byte of a message would be sufficient to cause a CRC (Cyclic Redundancy Check) error and eventually corrupt the whole message. From the attacker point of view, the collision attack is more advantageous compared to the jamming attack, since consumed transmission energy is lower (because the radio is used just only for a short duration of time) as well as the probability of detection [63].

2.2.2.2 Denial of Sleep (Sleep Deprivation Torture): Preventing a node from going to sleep leading to energy depletion from draining the battery. This can be from collision attacks or repeated handshaking i.e. Request to Send (RTS) and Clear to Send (CTS) flow control signals. In this attack, a node is forced to deplete whole energy stored in its batteries [64].

2.2.2.3 De-synchronization: Time Synchronized Channel Hopping (TSCH) is a MAC layer protocol presented in IEEE 802.15.4e standard. It empowers extreme consistency and possesses small duty cycles through the time synchronization and channel hopping techniques. [65] Attacks against the TSCH time synchronization can happen when an attacker transmits the messages in the time-slots that are alloted to the other users. This causes the packets to collide and to be lost. After carefully observing the back-off times an attacker can cause a series of these events which eventually would cause the neighboring motes to be de-synchronized. Hence, this attack can be taught of as an advanced version of collusion attack.

2.2.2.4 Exhaustion: If the collusion attack described above, continues until the targeted node depletes its energy, this is called *exhaustion attack* [63]. This kind of attack can be executed by using an ordinary node or a laptop, which have the ability to transmit radio signals in the same band as the rest of the sensors do.

2.2.2.5 Link Layer Flooding: In this type of attack, a malicious node abuses the fairness of medium access by sending excessive MAC data packets or MAC control packets to its neighboring nodes. In the end, victim nodes suffer from DoS or the power of their batteries get exhausted. Additionally, this attack may also exhaust channel bandwidth resources. [66]

2.2.2.6 Link Layer Jamming: In this type of attack, the most useful packets, i.e. data packets, are targeted to be jammed. The probability distribution of the packet arrival times is acquired and used against the packets transmission. This attack is shown to be successful against these MAC protocols: B-MAC, L-MAC, and S-MAC [63].

2.2.2.7 Spoofing/ ARP-Spoofing: In the spoofing attack, a malicious node spoofs MAC address of another victim node and then creates a number of various legitimate identities out of the victim node and uses these identities anywhere else in the network [16]. Whereas in ARP-spoofing attack, an attacker sends spoofed ARP (Address Resolution Protocol) messages into the network. Generally, the aim is to associate the attacker's MAC address with the IP address of a higher ranked node such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

2.2.2.8 Unfairness: Sporadic usage of *exhaustion attack* or mis-usage of cooperative MAC protocols can cause unfairness in the network [57]. Unlike a DoS attack, this attack does not cause a user or a node completely to be disconnected from the network, but it causes intermittent blackouts in which users send/receive delayed messages. This attack degrades the quality of service in the network, hence it provides an advantage to the least number of the sensor nodes and disadvantage to the rest of the network, as the rest of the nodes miss their transmission deadlines in real-time MAC protocol configuration.

2.2.3 Attacks towards Network Layer

In the case of *network layer attacks*, an attacker injects a significant amount of packets into the network which causes congestion in the network traffic as well as deprivation of power resources throughout the network. Example: "Routing table overflow attack: Creation of the routes to the non-existing nodes" [67]. Network layer attacks are categorized as HELLO flooding, hole attacks (blackhole, sinkhole, wormhole), node replication, routing, selective forwarding, and Sybil types.

2.2.3.1 HELLO-flooding: In this kind of attack, an attacker (has longer transmission range than normal nodes) broadcasts advertisement messages to the whole network and convinces other nodes that it is located in their neighborhood.

In a more technical description; routing protocols broadcast "HELLO" message to inform of their presence to one-hop neighbors. A node receiving such a packet assumes that it is within the radio range of the sender which may not be true during this attack. A malicious node may flood "HELLO" packets with high enough transmission power to convince every node in the network that it is their neighbor. When the other nodes send their packets to the malicious node, those packets are not received by any node.

Many network and MAC layer protocols ask nodes to broadcast "HELLO" packet for announcing their presence towards their neighbors. Any node, receiving such a packet might consider that it is enclosed in the normal radio-range of the packet sender. This assumption would be falsified in some specific cases as follows: A laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor.

"Flooding" is usually used to denote the epidemic-like propagation of a message to every node in the network over a multi-hop topology. In contrast, despite its name, the HELLO flood attack uses a single hop broadcast to transmit a message to a large number of receivers [59].

2.2.3.2 Hole Attacks:

- **Blackhole:** A malicious node may drop all the packets that it receives for forwarding. This attack is especially effective when the blackhole node is also a sinkhole. Such an attack combination may stop all the data traffic around the blackhole. In some texts, this attack is also referred as "Selfishness".
- **Sinkhole:** A malicious node can advertise by broadcasting to all the neighbor nodes that it is the best next hop for sending the packets to its destination. When a node becomes a sinkhole, it becomes the hub for its vicinity and starts receiving all the packets going to the base station. All traffic of the network is directed to this single node but in this case, sinkhole node does not drop any packets. By this way, it expects to remain undetected by the IDS. This creates many opportunities for any follow-on attacks. Since all traffic of the network passes through this particular node which literally "sinks" all the data it receives, the name is given to this attack.
- **Selective Forwarding (Grayhole):** It is a special kind of blackhole attack, in which malicious node acts more cleverly and does not drop every packet it receives but the ones it selects. By this way, attacker expects to remain undetected by the IDS. This type of attack is also called "grayhole attack" as it is a variant of blackhole attack.

  Similar to sinkhole attacks, a malicious node subverts the routing protocol by making itself part of many routes but instead of dropping of all packets selectively drop some packets while forwarding others in order to avoid detection. Forwarding packets is a major responsibility of a routing node. However, a malicious node intentionally may drop any packet and forward other ones.

  Multi hopped networks are generally built upon the following assumption: The participant sensor nodes would be faithful in forwarding the messages they receive. In a selective-forwarding attack, adversary nodes might reject forwarding some certain messages by simply dropping them and making sure that these packets are not distributed anymore. As an example of this kind of attack, a malicious node behaves like a blackhole and refuses to forward every packet it receives. However, such an attacker has the following risk: Neighboring nodes will conclude that it has failed and they may decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a select few nodes can reliably forward the remaining traffic and limit suspicion of his/her wrongdoing.
- **Wormhole:** A tunnel (out of the band fast transmission path) is created between two nodes that can be utilized to transmit packets in a faster way. This way, two far parts of the network advertised as neighbors to attract the surrounding traffic [68].

  A malicious node can eavesdrop or receive data packets at a point and transfer them to another malicious node, which is at another part of the network, through an out-of-band channel. The second malicious node then replays the packets. This makes all the nodes that can hear the transmissions by the second malicious node believe that the node that sent the packets to the first malicious node is their single-hop neighbor and they are receiving the packets directly from it. The packets that follow the normal route reach destination node, later than those conveyed through the wormhole and are therefore dropped because they do more hops - wormholes are typically established through faster channels.

  Wormholes are very difficult to detect and can impact on the performance of many network services such as time synchronization, localization, and data fusion.

2.2.3.3 Node-Replication (Clone): An attacker intentionally puts replicas of a compromised node in many places in the network to incur inconsistency. Node-replication (clone) attack is one of the particularly most dreadful attacks hence it causes an attacker to be able to divert the behavior of a network by just using a few copies

of a previously hacked nodes [69]. Like the Sybil attack, the node-replication (clone) attack also can enable attackers to subvert data aggregation, misbehavior detection, and voting protocols by injecting false data or suppressing legitimate data [70].

2.2.3.4 Routing Attacks:

- **Misdirection:** In misdirection attack, an attacker forwards ongoing messages to the wrong paths intentionally. This can be achieved by fabricating false routing advertisements and causing routing tables of the neighboring nodes' to update these false information [57]. This attack is also categorized as DoS attack, hence targeted nodes are blacked out completely and do not receive any further packets after the advertisement of the false routing information.
- **Network Partitioning:** A fully connected network is portioned to sub-networks in which the nodes in different sub-networks cannot communicate each other although they are connected.
- **Routing Loop:** A routing loop is introduced in a route path. It is created by spoofing routing updates. Suppose an adversary can determine that node A and node B are within radio range of each other. An adversary can send a forged routing update to node B with a spoofed source address indicating it came from node A. Node B will then mark node A as its parent and rebroadcast the routing update. Node A will then hear the routing update from node B and mark B as its parent. Messages sent to either A or B will be forever forwarded in a loop between the two of them. This leads to energy depletion and eventual node/network failure [59].
- **Rushing:** When this attack is performed against "on-demand ad hoc network routing protocols", it results in DoS in the network. For instance; AODV, DSR, and more secure protocols based on these, i.e. ARAN, SAODV, and Ariadne, are not capable of discovering routes that are longer than two-hops when they are subjected to this kind of attack. The rushing attack is especially harmful to networks hence it can be executed by relatively weak adversaries [71].
- **Spoofed, Altered or Replayed Routing Information:** Routing information exchanged among nodes can be altered by malicious nodes to have a detrimental effect on the routing scheme.

2.2.3.5 RPL Exploit: IoT consist of devices that are limited in resource like battery powered, memory, processing capability, etc. For this kind o networks, a new network layer routing protocol is designed called RPL (Routing Protocol for Low-power and lossy networks) [72]. RPL is light weight and does not have the full functionality of traditional routing protocols. RPL was proposed especially for data-sinks (multi-point to point communications) and is being adopted by IoT recently. Many attacks against the RPL of IoT have been presented in [73].

As discussed and proposed in our paper, IoT is also susceptible to most of the attacks against WSNs. The attacks presented in [73] and [74] support this idea in a sense that other than a few attacks (which are specifically against RPL protocol), all of the attacks are same as the "Attacks against Routing Layer" presented in this section. These specific attacks against RPL protocol are: Local-Repair attack, Rank attack , DODAG version attack, DIS attack, and finally Neighbor attack. [73]

In local repair attack, an attacker intentionally and periodically sends the local repair message which is originally used for improvement of the link quality. This causes the neighboring nodes to go into local repair cycle. This attack creates more impact on delivery ratio than any other kind of attack, generates more control packets and increases the end to end delay [73].

DODAG stands for Destination Oriented Directed Acyclic Graph, which is created by RPL by forming a loop-free topology. DODAG organizes nodes in a hierarchical manner as single root, children and their further descendants [75].

In RPL, rank value increases from root to child node. In RPL DODAG rank attack, an attacker can exploit DODAG version system by advancing its rank in the hierarchical tree and gaining many children which are forced to route packets through the attacker parent. So, by intentionally changing the ranking value of itself, an attacker can attract many child nodes for selecting it as parent, and thereby attracts large traffic going toward the root node (main branch) to flow through itself.

Another exploit of RPL DODAG version system is called DODAG version attack. It is executed by publishing a higher version number of the DODAG tree. When nodes receive the new higher version number in the DODAG Information Object (DIO) messages, they start forming a new DODAG tree. This can cause the generation of new un-optimized topology and will bring inconsistencies in the network topology. The loops and rank inconsistencies created by the attack are generally located around the neighborhood of the attacker. [73]

In DODAG Information Solicitation (DIS) attack, an attacker sends DIS messages with fake IP addresses which causes the recipient node to re-generate the DIO messages, which eventually increases the overhead.

In RPL neighbor attack, a malicious node broadcast DIO messages that it received without adding information of itself. The node which receives this type of message may think that new neighbor node is sending this DIO message. The victim node tries to change the routing tables so that the pointed node is also included. This attack is somehow similar to the selective forwarding attack in which DIO messages selected only. This attack affects network by slightly increases the end to end delay, change in network topology, and some control overhead. However, it might have serious consequences when combined with other attacks.

2.2.3.6 6LoWPAN Exploit: 6LoWPAN is an Internet protocol devised for the IoT for the sake of extended usage of IPv6 by the smart-things. 6LoWPAN integrates IP-based infrastructures and WSNs by specifying how IPv6 packets are to be routed in constrained networks such as IEEE 802.15.4 networks by fragmentation and reassembly of datagram data fields.

A specific attack for 6LoWPAN is fragment duplication attack, in which an attacker puts his own fragments in the fragmentation chain. The fragment duplication attack takes the advantage of the fact that a recipient cannot verify at

the 6LoWPAN layer if a fragment originates from the same source as previously received fragments of the same IPv6 packet. Hence no authentication mechanism exists on the receiver at the time of reception for checking whether received fragment is an original or spoofed duplicate fragment, this attack can easily fool the receiver. The receiver cannot distinguish legitimate fragments from spoofed duplicates. Instead, it has to process all fragments that appear to belong to the same IPv6 packet according to the sender's MAC address and the 6LoWPAN datagram tag. Thus, an attacker can pretend as a legitimate node and exploit this weakness to engage in further attacks such as a DoS attack. [73], [76].

2.2.3.7 Sybil Attack: A single node presents multiple identities to other nodes of the network. This causes confusion in the network; nodes receive contradicting routing paths that are passing through the attacker. This reduces the effectiveness of fault-tolerance schemes and poses a significant threat to geographic routing protocols [77]. Apart from these services it may also affect the performance of other schemes such as misbehavior detection, voting-based algorithms, data aggregation, fusion and distributed storage [**?**].

2.2.4 Attacks towards Transport Layer

The transport layer of the OSI protocol stack manages end-to-end connections of the two nodes. At the transport layer, attacks exploit the protocols that maintain connection information at either end. [60] All transport layer attacks are categorized and described as follows:

2.2.4.1 De-Synchronization: An attacker disrupts actual links among two nodes by de-synchronizing the transmissions in between them. An example of this type of attack is sending fabricated messages, such as faulty flag kind of sequences, (by transmitting forged packets with bogus sequence numbers or control flags that desynchronize endpoints so that they will re-transmit the data [60]) continuously to both sides of the communicating parties, as a result, to force them losing their synchronization [57], [63].

2.2.4.2 MQTT Exploit: The Message Queue Telemetry Transport (MQTT) [78] is a lightweight publish-and-subscribe connectivity protocol aimed at working on resource-constrained devices such as low power embedded sensors to enable them communicating. In the IoT context, MQTT is widely used to enable the communication between devices using a publish-and-subscribe messaging approach. However, MQTT does not include security layer by default and it is the user's responsibility to address security issues. In this direction, it is suggested to enable security for MQTT by issuing SSL/TLS with certificates and session key management. That is being said, owing to the multitude of heterogeneous devices, storing and managing the certificates and key exchanges for every session of IoT is burdensome. Furthermore, SSL/TLS can suffer from attacks such as BEAST, CRIME, RC4, and Heartbleed. Thus a scalable, lightweight and robust security mechanism is required for MQTT and its variants for deployment in IoT. [79]

2.2.4.3 Session Hijacking: In computer science, this attack is referred as the "exploitation of" and "tampering with" a valid communication session (which is also called as session key) to gain unauthorized access on information or services of a system. As being an extension of IP networks, session hijacking of TCP messages will also be affecting and troublesome for IoT networks.

2.2.4.4 SYN-flooding: In a flooding attack, an attacker aims at exhausting the energy and/or the memory of a node, by flooding it with spurious messages. This is achieved, for instance, by sending multiple connection requests without ever completing the connection, thus overwhelming the buffer and eventually causing the node to be dead [57], [63].

More specifically, in a TCP SYN (synchronize) flooding attack, an adversary sends multiple TCP connection requests without ever completing the connection, thus overwhelming the target's half-open connection buffer. [60]

2.2.5 Attacks towards Application Layer

Application layer protocols can also be exploited by DoS attacks. Protocols like node localization, time synchronization, data aggregation, association, and fusion can be cheated or hindered. For example, a malicious node that impersonates a beacon node and gives false location information or cheats with regard to its transmission power, i.e. transmitting with less or more power than it is supposed to do, may hamper the node localization scheme. Since this kind of attack diminishes the related network service, they can also be categorized as DoS attacks. An example of application layer DoS attack is path-based DoS attack and will be described below. All application layer attacks are categorized and described as follows:

2.2.5.1 CoAP Exploit: Constrained Application Protocol (CoAP) [80] is an application layer protocol designed as a replication of the HTTP for the small devices of IoT to provide communication ability with the rest of the Internet. Recently, many implementations of IoT are using CoAP, which indicates that it will have a crucial role in the future of IoT applications.

As mentioned in [81], there are several challenges related to security by the introduction of CoAP. It does not translate full functionality of HTTP, which creates security problems for multicast messages.

2.2.5.2 False Data Injection: In order to influence the overall result of a measurement or a reading, captured nodes intentionally inject false data in the WSN. Therefore, it can be stated that this attack happens in a semantic level, hence it does not affect anything but the logic.

2.2.5.3 Path-based DoS: As the name implies, this attack is a DoS attack that happens in the application layer. In this attack; an attacker overwhelms nodes but this time from long distance by again flooding an end-to-end communications path with either fabricated packets or replayed packets [82]. So, as a result, all the nodes along the path, from the source to destination (attacker to the base station) are affected by this attack.

2.2.5.4 Re-programming: Once in a while, every network element either needs to be patched or re-programmed for version control, code acquisition, encoding-decoding, or when switching to a newly written program. That's also true for WSNs and IoT. If this re-programming (or patch management per say) schedule is not kept secret, then adversaries can take advantage of this vulnerable time of the network by simply sending bogus

messages to the nodes and pushing them into unstable or dead state [83].

2.2.5.5 Sensor Overwhelming: Attacking or altering the sensitivity of the sensor measurements. Targeting sensors with spurious interference or completely overwhelming them with fake messages and inundating them with false stimuli.

3 Defending Against Various Attacks towards the WSNs and IoT

Routing protocols can be designed such that an adversary cannot compromise nodes/messages or make the routing scheme dysfunction. This is the most effective approach with respect to the cost of the security scheme and effectiveness in defense of WSNs against the threats. Therefore, most of the techniques fall into this category.

Preventive approaches are designed to counter known threats and may not be effective against new threats. Detection schemes for misbehaving or malfunctioning nodes can be designed in a more generic fashion. On the other hand, they can be more costly than preventive approaches. Finally, routing can be designed such that it still delivers the data packets to the destination when there is an attack. Such resilient techniques are also costly.

Following subsections provide solutions (strategies and techniques) to defend (detect, prevent or mitigate) against various attacks towards the WSNs on all of the layers of the OSI protocol stack:

3.1 Defense against Passive Attacks

3.1.1 Defense against Passive Information Gathering

The communications in WSNs are achieved through the air, and therefore we do not know whether the packets arrive the intended people only or not. Hence detection of eavesdropping is almost impossible.

Link layer encryption would prevent outsider attacks such as eavesdropping, and some of the solutions are provided in [59], [84], [85], [86], [87]. The bulk of the external attacks towards WSNs can be avoided by link-layer encryption and authentication by using globally-shared keys. For example, to provide link layer encryption, Karlof *et al.* [88] proposed TinySec for WSNs. SNEP (Secure Network Encryption Protocol) under the SPINS [84] protocol set, is also one another famous encryption protocol that is devised for WSNs.

In [89], authors proposed SensorWare communication multicast model in which 3 different levels of link-layer encryption are provided by using the RC6 algorithm. They have chosen the RC6 algorithm, because its selection of the number of rounds parameter, has a direct effect on the security level of the algorithm. An initial set of master keys are shared by all sensors in the network. At any time, one of the master keys in the list of the master keys is active. The reason is, in order to expose less data for known-ciphertext attacks, more keys will be necessary as the lifetime of the network extends. This selection of the keys is executed pseudo-random way, every node uses the same seed for randomizing function. Then, the random number is coupled to the list of the master keys to obtain the active master key.

TABLE 1
Solutions to defend WSNs against DoS attacks

DoS attack	Defense strategy
Radio interference	Usage of spread-spectrum communication
Physical tampering	Usage of tamper-resistant nodes
Denying channel	Usage of error correction codes
Blackhole	Usage of multiple routing paths
Misdirection	Usage of source authorization
Flooding	Limiting the total number of connections

For the rest of the security model, the required keys for the 3 different levels of security are gathered from this active master key.

Random key pre-distribution schemes [90], [91], [92] help link layer encryption schemes by distributing the keys needed by the encryption algorithms, hence they help WSNs to protect information in transit and prevent eavesdropping, data and information spoofing.

3.2 Defense against Active Attacks

In Table 1, some of the solutions [93] to defend WSNs against various DoS attacks are summarized. However, this presentation is too generic and that's why we needed to present Table 2 in an effort to give the whole picture with a detailed categorization.

3.2.1 Defense on Physical Layer

In [94], authors propose a cross-layer security mechanism, namely "Swarm Intelligence", to detect Jamming-DoS attacks. They also provide countermeasures to mitigate this kind of attack. JAM − a jammed area mapping service [95], is proposed for detecting jamming DoS attack against WSNs. JAM provided a mapping protocol to detect a jammed region in a WSN. Besides, in terms of mitigation, JAM avoided the jammed part of the WSN by re-routing the packets thus provided a remedy for the Jamming DoS attack.

In [96], authors proposed wormhole technique, normally known to be an attack against WSNs, which could be effectively used to defer Jamming DoS attack against WSNs.

In order to defend WSN from node tampering attacks, nodes might be equipped with tamper-resistant hardware, in which any kind of tamper attempt would wipe out the memory (and also any other data storage) so that confidential information (such as the secret keys) would not be leaked. Although this is a wise and excellent solution, it comes with an additional cost of hardware which would increase the total cost of the WSN installation and cripple the most appealing feature of such networks: "low cost". Other ways of fighting against node tampering would be disabling JTAG interface of the sensors and the use of good password protection for the bootstrap loader of the sensor boards [63]. Finally, a naïve way of protecting the nodes against this kind of attacks would be simply hiding the nodes by camouflaging [18].

Detection of the tampering attempts would require routinely physical checking of the sensor nodes by eye or with special equipment such as magnifiers. Though, this task might be tedious considering the fact that sometimes nodes

are deployed across dangerous and hard to reach places such as flooded zones, nuclear leakage areas, etc.

3.2.2 Defense on Data Link Layer

3.2.2.1 Defense against Collusion and Exhaustion: In order to defend WSNs against collusion and exhaustion attacks, request rate of each node might be limited to some certain value (by decreasing the MAC admission control rate), so that the network can discard extra requests from the same node (attacker) [63]. Another solution would be the employment of time division multiplexing (TDM) technique which would provide dedicated time slots to each node to transmit their packets. This would allow each node to have a tiny period of time to access the channel. By this way, the channel usage of each node is limited and attacks related to channel abusing are prevented. If the corruption of the packets occurs partially (in bursts), employment of error detection and error correction codes would be beneficial tools to fight against this kind of attacks [18].

3.2.2.2 Defense against Denial of Sleep and Link Layer Flooding: Liu et al.'s anomaly detection-based IDS proposal works on ad hoc networks and therefore fits well to the WSNs and IoT. In their proposal, each node participates to the detection of the abnormal nodes. Packet traffic at MAC layer is analyzed and evaluated. Distributed and cooperative anomaly detection is achieved by creating feature vectors at each node and then fulfilling cross-feature analyses. This is resulted with local or global response (either response from single node or a collaborative response from multiple nodes) according to the seriousness of the attack situation. The proposed IDS has shown to be effective against MAC layer attacks, especially on denial of sleep and flooding attacks. [66]

3.2.2.3 Defense against De-synchronization: Many applications require the IoT to have a low and deterministic delay, especially for IIoT applications where delay tolerance is low. Having a deterministic network delay in a WSN is challenging in the best case when traditional MAC protocols are employed. To enable low power, high reliability and deterministic WSNs, IETF recently proposed 6TiSCH protocol that uses time slotted channel hopping (TSCH) MAC with IPv6 addressing. This protocol dynamically assigns bandwidth resources to the nodes in the network according to the application requirements, hence it provides a communications stack for low power and lossy networks such as IoT. The proposal includes secure communication of MAC layer frames so that any kind of eavesdropping or packet capturing would have no benefit of these. [97]

3.2.2.4 Defense against Unfairness: In [57], usage of small frames is offered as a defense solution to this kind of attack. By this way, an attacker would capture the channel only for a small period of time and unfairness would be avoided.

3.2.3 Defense on Network Layer

3.2.3.1 Defense against Blackhole: Liu et al.'s anomaly detection-based IDS proposal works on each node and have also shown to be effective (but less compared to detecting attacks against MAC layer) on network layer, especially for detection of blackhole and grayhole (packet-dropping) attacks. [66]

In [98], authors proposed REWARD scheme, in order to detect blackhole attacks against WSNs. Besides, this scheme provides a routing algorithm, in which detected blackholes are avoided hence the WSN resumes normal operation under blackhole attack.

In [99], authors discussed the effects of network topology selection in WSNs on blackhole attacks. Their findings suggest that mesh topology is more resilient against blackhole attacks compared to star and tree topologies.

In [100], Prathapani *et al.* proposed the use of Honeypots, which are strolling software agents that create dummy Route-Request (RREQ) packets to attract and catch blackhole attack performers. Authors have illustrated the positive performance of the proposed detection approach by extensive simulation results using the ns-2 simulator.

Watchdog based intrusion detection system proposed in [101], is efficient in detecting blackhole and selective forwarding attacks. Sensor nodes in the clustered-WSN watch their neighbors and collaborate with the head of the cluster in order to be able to detect misbehavior. Although sensor nodes do not have an exhaustive view of the network, still they can be effective in detecting intrusions with some definite probability and report it to the head of the cluster.

In [102], Medadian *et al.* presented a method to cope with the blackhole attacks which introduces negotiating with neighboring nodes that claim to possess a route to the destination. If a node receives an RREP packet (corresponding answer to an RREQ packet) then it forwards this packet to the source and starts an evaluation procedure about the replier. The evaluation procedure is based upon opinions of the nodes about the replier. All activities of a node are saved by its neighbors. Whenever the neighbors of a particular node are asked to send their opinions about it, requester node gathers all opinions of the neighbors and concludes about the maliciousness of the replier node. The conclusion is based on several rules. According to authors' simulation results, it has shown that the presented MAODV protocol provided not only better security but also performed better in terms of packet delivery ratio than the legacy AODV protocol in the existence of blackholes with minimum added delay and overhead.

In ActiveTrust [103], in order to detect blackhole attacks in WSNs, authors have created multi-detection routes in the areas which have remaining energy. Hence an adversary does not know the detection routes, (s)he will target those and while executing the action (s)he will be disclosed. By this method, location and behavior of an adversary can be determined by ActiveTrust to be used for avoiding blackholes during the creation of the final data routes.

In [104], authors presented a technique for detecting and preventing blackhole attacks in clustered-WSNs. In this methodology, a node called coordinator is selected by all nodes dependent on the cluster-head election criterion. Coordinator node has the responsibility in the authentication process, detection of intermediate node failures as well as blackhole attacks. If a blackhole attacker is detected in the cluster, then the coordinator removes it from the cluster, hence all the communications with this specific node are terminated.

Misra *et al.* [105] proposed a method called BAMBi, which is based on the deployment of spatially diverse

base stations in the WSN to cope with the consequences of having blackholes on the data transmission. Presented method demands transmission of extra copies of a packet from each node to all base stations. To ensure that every node has a route to it, each base station uses TinyOS beaconing. The beacon packet from any BS consists of: the ID of the sender of the packet, the ID of the base station from which it originated, and the hop count of the sender from the base station to the node. This beaconing process creates a routing tree in the network and used for detection and mitigation of blackhole attacks against the network. According to their simulation results, authors have shown that the proposed method has achieved over 99% success rate in packet deliveries in the presence of blackhole attack.

In [106], Amouri *et al.* proposed a framework of intrusion detection for MANETs. The framework considered a hierarchical architecture where the intrusion detection is distributed through a set of promiscuous zones (PZ). Unlike the traditional approach where the nodes are promiscuous all the time, in their scheme the nodes are promiscuous for the period that they are in the PZ. Once a node leaves the virtual PZ its promiscuity is turned off in order to save energy. Authors have used a C4.5 decision tree to learn the network behavior under blackhole attack, and after exhaustive evaluation, authors have shown that their approach was able to recognize blackhole attacks with up to 97% accuracy.

3.2.3.2 Defense against HELLO Flooding: One possible solution to this problem is provided in [59]: Force every node to authenticate each of its neighbors with an identity verification protocol using a trusted base station. If the protocol sends messages in both directions over the link between the nodes, HELLO floods are prevented when the adversary only has a powerful transmitter because the protocol verifies the bi-directionality of the link.

In [107], authors presented a shared-secret method based on probability to defend against HELLO flooding attack. The proposed method has 2 steps in terms of defense: 1) Bidirectional verification technique to detect HELLO floods. 2) "Multi-path multi-base station routing" in order to defer HELLO floods.

μ-TESLA "(Micro Timed Efficient Streaming Loss-tolerant Authentication) protocol", under the SPINS [84] protocol set, has been proposed to provide authenticated broadcasting in an effort to prevent HELLO flooding attack; and achieved this by employing symmetric key cryptography which required minimum packet overhead.

3.2.3.3 Defense against Node-Replication (Clone): In [108] and [109], authors proposed location based Public Key Cryptography (PKC) algorithms in order to prevent clone attacks. Every sensor node has a private key associated with the location of itself. These location-based keys are employed to prevent node replications.

In detecting clone attacks, there are a variety of solutions provided. More interested readers would refer to [10], hence detailed comparisons of the schemes proposed to detect node-replication attacks are provided in. Here, they are summarized under 2 categories:

Centralized Solutions: Conventional methods to detect a node replication attack usually include centralized computing based on node locations or the number of simultaneous connections, which is vulnerable to the single-point failure [70]. Mostly, centralized detection schemes do not have significant advantages over distributed detection schemes; and bear similar deficiencies (such as any compromisation at the base-station would transform the provided-solution to an ineffective one).

Choi *et al.* [110] presented a scheme to detect centralized node-replication attacks and named it as "SET". SET aims at reducing the overhead caused by the detection, with computation set of operations ("intersection", "union") related to exclusive subsets of the WSN. Not only SET protocol is very complicated to implement (owing to complex components like interleaved authentication and authenticated subset covering), but also has an increased overload.

Brooks *et al.* [111] presented a protocol to detect clone attacks based on "random pairwise key pre-distribution schemes". Proposed scheme addressed the problem of detecting replicated cryptographic keys instead of the replicated sensor nodes. By analyzing statistical data from the sensor node authentications, the proposed scheme detects the replicated keys as follows: The keys that are exceeding a predefined usage count (threshold) are declared as replicated and revoked from the WSN.

Xing *et al.* [112] presented a method to detect node-replication attacks with the encoded information related to nodes' community network called the "social fingerprint". In this method, nodes collaborate to create each other's fingerprints then send these data to the base station for further conclusion process. However, in the proposed scheme, the expected number of nodes is not adjustable; therefore not only node addition but also node revocation cannot be managed, causing the flexibility of the WSN to disappear.

Ho *et al.* [113] presented an efficient and fast node-replication detection model for mobile WSNs called "speed test". In this model, the base-stations compute the instant maximum speed of a node, and denote it as $Vmax$ and then compare it with the system configured maximum theoretical speed $Vmax - T$. An authentic node should be never moving faster than $Vmax - T$. If the instant-measured $Vmax$ is to be found above the configured $Vmax - T$, then it is most probable that there are at least two sensor nodes using the same ID in the WSN, the indication of a replication attack. Although the proposed scheme sounds very appealing, it might introduce errors causing high false-negative and false-positive outcomes due to the synchronization errors.

Butun *et al.* [114] proposed an IDS system for clustered-WSNs based on multi-level clustering. In their approach, all the member nodes of each cluster share secret keys with their cluster head. Each node is specific to their unique cluster and cannot be used in any other cluster elsewhere in the network. Therefore, any attempt of node replication attack is easily detected and prevented by using this kind of clustered approach.

Distributed Solutions: In [70], Parno *et al.* presented a method for distributed detection of the clone attacks. On this approach, each sensor node is considered to know its own location, and it is mandatory to send this location information to a set of watchdog sensors. If a watchdog sensor detects an abuse in the location declarations of a sensor node, this node then becomes as suspicious of having a replicated (once or more) identity in the network. In

order to cope with this problem and to certify the authentic location claims of the nodes, public-key cryptography is employed.

Another distributed detection method of clone attacks is devised by Conti *et al.* [69]. In their proposal, "HIP-HOP (History Information-exchange Protocol and its optimized version)" protocol is devised. Proposed protocols make use of local neighborhood (one-hop) communications and mobility of nodes, and can be considered as light-weight for the amount of computation required. While detecting clones, the proposed protocols work in an effective, distributed and cooperative way.

In node-to-network broadcasting (N2NB) scheme [70], the whole network is flooded by every node with authenticated-broadcast messages. This is in an effort of each node by claiming its own location. In the pre-condition that the broadcast messages reach each node, the N2NB protocol is reported to achieve 100% detection rate.

In deterministic multicast (DM) scheme [70], the aim of the design is to reduce the communications cost, and the main goal is sending location claim of a node only towards a certain number of nodes, chosen in a deterministic way, to serve as watchdogs in the network.

"Randomized multicast (RM)" and "line-selected multicast (LSM)" protocols are two probabilistic algorithms, both proposed by Parno *et al.* [70]. RM protocol dissipates node-location claims to a selected random number of watchdogs, leveraging "combinatorics theory" in detecting replicas; while LSM leverages the network topology related to routing to assign extra watchdogs for the claimer and employs "geometric probability" methodology for the detection.

Zhu *et al.* [115] presented 2 schemes: "Single deterministic cell (SDC)" and "parallel multiple probabilistic cells (P-MPC)". Both schemes are derived from DM, and can be employed as "network-wide deterministic multicast" protocol, followed by probabilistic storage and in-cell broadcast methodologies.

Conti *et al.* [116] presented "randomized, efficient, and distributed (RED) protocol". This method combined both advantages of RM and DM. In the state of the art, RED is one of the most appealing clone-detection algorithms.

In [117], Zhang *et al.* proposed 4 clone-detection protocols with the name of "memory efficient multicast (MEM)".

Li and Gong [118] proposed a simple form of N2NB named as "randomly directed exploration (RDE)", in which location claims along with the claimer's neighborhood list are sent so that each of the forwarding nodes on the path fairly constitutes a line. RDE is only feasible for ideal network model, hence detection rate might not be at an important level even for a convex deployment field.

3.2.3.4 Defense against Selective Forwarding (Grayhole): There are two approaches to defend against selective forwarding attacks:

- Detecting the nodes that selectively forwarding.
- Developing routing schemes that are more resilient and can deliver packets even when there is a selective forwarding attack.

One approach in detecting the nodes that are selectively forwarding is based on acknowledgments [119]. Every intermediate node that forwards a packet waits for an acknowledgment from the next hop. If the next hop node does not return the same number of acknowledgments as the number of packets sent, the node generates an alarm about the next hop node. However, compromised nodes can also generate acknowledgments for the packets that they dropped, which make this scheme fail.

Multi-path routing can be an effective way to mitigate selective forwarding and blackhole attacks [59]. This requires at least link-disjoint paths, where two paths may share some nodes but no link. Of course, node-disjoint paths, where two paths do not have any node in common, are better and reduce the risk of selective forwarding attack compared to link-disjoint paths. However, disjoint paths are not always available, and when paths are not disjoint, if the selectively forwarding node is the node common to all the paths, then the attack can become as effective as in single-path routing.

Braided paths [120] may have nodes in common, but have no links in common (i.e., no two consecutive nodes in common). The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information.

In [121], Hai and Huh proposed a lightweight detection algorithm to detect selective forwarding attacks in WSNs. The proposed algorithm is based on two-hop neighbor knowledge including two routing rules. The proposed algorithm has been evaluated for WSNs and has found to be effective even under high-density network conditions along with the high probability of collisions.

In [122], authors describe an efficient scheme for reporting packet drops. They also present an effective scheme, namely "Wald's Sequential Probability Ratio Test", for detecting the selective forwarding attack in a heterogeneous sensor network. According to presented simulation results, proposed scheme not only achieves high detection ratio but also low false alarm rate.

Wang *et al.* [123] proposed a failure detection framework to detect the selective forwarding attack. The observation is that for a routing node, the number of packets it forwards must be equal to the number of packets it receives. In their framework, each sensor node can work under a promiscuous mode so that it can overhear the transmission of neighboring nodes. If a neighbor of a suspected node finds that the number of packets that the suspected node fails to forward exceeds a certain threshold, the neighbor can collaborate with other neighbors of the suspected node, and the opinions from the neighbors of the suspected node are collected to form a decision about the suspected node.

3.2.3.5 Defense against Sinkhole: An algorithm which detects sinkhole attacks is presented in [124]. Proposed algorithm first finds a list of suspected nodes, and then effectively identifies the intruder in the list through a network flow graph.

In Shafiei *et al.*'s [125] proposal; two schemes in an effort of detecting sinkhole attacks are presented. The idea behind these schemes is that the sensor nodes in the vicinity of the sinkhole would deplete their energies more rapidly compared to other sensor nodes. This is due to the fact that, routes to the base station passing through sinkhole are supposedly more found to be more attracting thus are chosen more often. Therefore, an energy hole forms in the vicinity of each and every sinkhole. The first scheme has

proposed that base stations to utilize a geo-statistical sampling methodology for detecting possible sinkholes in the entire area of the WSN using the energy spending pattern (remaining energies of each area) and issuing an estimator based on the data extracted from the statistics. Depending on the result of the estimator, base station commands all nodes to bypass the doubtful area (possible attack region) in their process of routing. The second scheme utilizes distributed monitoring methodology in order detecting areas having less average remaining energy level.

Zhang *et al.* [126] presented a scheme for detecting sinkhole attacks towards WSNs based upon redundancy mechanism. In the proposed scheme; in order to detect sinkholes, messages are sent to the suspicious nodes through multipaths. By evaluating the replied messages by the suspicious nodes comprehensively, the attacker nodes are confirmed.

Teng and Zhang [127] proposed "SeRA: A secure routing algorithm against sinkhole attacks for mobile WSNs". The proposed algorithm is based on the Tiny-AODV protocol. First, a couple of mobile-agents communicate each sensor node to gather the network connection data to construct the global data matrix of the sensor nodes. Then, through the SeRA routing algorithm, the sinkhole node can be efficiently avoided.

3.2.3.6 Defense against Sybil: In order detecting the Sybil-attack, two protocols are presented in [128]. The first protocol employs "radio resource testing" in which every sensor node declares a unique-channel to each of its neighbors. Then, it tests to see whether the neighbors communicate with itself through the pre-declared channels. Hence radio circuitry of a sensor node generally cannot handle simultaneous send and receive actions on more than one channel, the failure at the communications through one channel might be an indication of the Sybil-attack. The other protocol employs the "ID-based symmetric keys". For instance, there is a global pool of keys that each sensor node has a key associated to its ID, and every node is pre-loaded with these keys. The ID of a suspicious sensor node is examined by witness nodes based on keys shared in between the suspicious sensor node and the witness sensor nodes.

In [129], authors proposed "rule-based anomaly detection system (RADS)" in order monitor and detect Sybil-attack towards sensor networks on time. The presented method relied on "ultra-wideband ranging-based detection algorithm". RADS works in a distributed fashion in which every node have the ability to trigger alarms, in case they are suspicious of a node in their vicinity. The presented method not only detects Sybil-attack in the absence of central management authority or a third party trusted-network-entity but also provides defending methods against the adversaries by using isolation technique towards both the attacker sensor node and the compromised Sybil-nodes.

To defend against Sybil attacks, the identities of every node should be verified. This can be done either directly or indirectly. In the direct validation, a node directly verifies whether the identity of a neighboring node is valid. For example, a node may assign each of its neighbors a separate channel to communicate and ask them to transmit during a period. Then it checks these channels in a random order within that period. If a node is transmitting in its assigned channel, the node is a physical node. If no transmission is detected on a channel, it indicates that the node assigned to that channel may not be a physical node [128].

In indirect validation method, another trusted node provides the verification for the identity of a node. For example, every node may share a unique key with the base station. When two nodes need to establish a link between them, they verify each other's identity through the base station by using these keys [59]. At the same time, they can be assigned a session key. Nodes can also be allowed to establish links with a limited number of neighboring nodes. Thus, compromised nodes can only communicate with a limited number of verified neighboring nodes, which also limits the impact of Sybil attacks.

Moreover, ID-based public keys [108] also can defeat the Sybil attack because both the ID and location information were taken into the generation of key material during the initialization phase, hence multiple identities need multiple keys, and this is impossible for a malicious node to achieve.

3.2.3.7 Defense against Wormhole: Wormholes are difficult to detect because an adversary passes the packets to a distant point from the point at which they are received by using a single hop out-of-band channel. This channel cannot be listened to by the network. Moreover, the real copy of the packet reaches the point that receives the replayed copy later than the replayed copy. Therefore, the replayed copy is fresher than the real copy.

Detection mechanisms against wormhole attacks can be based on temporal and spatial analysis of the packets. To detect the Wormhole attack, Hu *et al.* proposed to use packet leashes [68], where location or timing information is embedded in packets, to limit the maximum range over which packets can be tunneled. They require that each node either knows its location or has a tightly synchronized clock so that this information can be used to calculate the maximum distance that a relayed packet could travel.

Directional antennas [130] were also used to defend against the Wormhole attack, where some direction information is used to detect the replayed packets. However, these defenses target ad hoc networks and require expensive hardware devices, which may be infeasible for most resource-constrained sensor networks.

Wang and Bhargava [131] proposed to use centralized computing to detect the Wormhole attack in sensor networks, in which a controller collects the location information for all nodes to reconstruct the network topology such that any topological distortion can be visualized. However, the visualization approach incurs too much communication overhead, especially when malicious nodes move around in the entire network because each location change of the Wormhole triggers a new round of execution of the topology reconstruction algorithm.

Location-based keys [108] can effectively prevent the Wormhole attack because each packet is authenticated by the location-based key, which includes authentication information in accordance with the position information of the nodes. This method excludes the effects of wormholes by attesting the position of the nodes along with their location-based keys. Attacker nodes would simply be denied to join the network if their location-based keys are invalid.

Kaissi *et al.* [132] proposed "DAWWSEN", a proactive routing protocol based on the construction of a hierarchical tree where the base station is the root node, and the sensor nodes are the internal or the leaf nodes of the tree. DAWWSEN fights against wormhole attacks by creating a hierarchical 3-way handshake routing tree and any attempt of creating wormholes are discarded by this generated routing tree.

3.2.3.8 Defense against 6LoWPAN Exploit: In [133], authors proposed a new security protocol referred to as 6LowPSec, providing a favorable end-to-end security solution that will be working on 6LoWPAN protocol. 6LowPSec employs existing hardware security features specified by the MAC security sublayer. However, the proposed solution functions at the adaptation layer and has not been evaluated by the research community yet.

A specific solution to 6LoWPAN fragment duplication attack is proposed by Hummen *et al.*; the content chaining scheme uses cryptography to verify that received fragments belong to the same packet, so that spoofed (duplicated) fragments would be avoided [76].

3.2.3.9 Defense against RPL Exploit: As RPL is a newly proposed networking technology, attacks towards it are being discovered these days. Hence, there are not many solutions proposed in defending it against those attacks.

TRAIL (TRust Anchor Interconnection Loop) [134] , is proposed as a generic scheme for topology authentication in RPL. It detects and prevents topological inconsistencies by enabling each node to validate its upward path to the root and to detect rank spoofing on it. TRAIL also minimizes network message exchanges and node resource consumption. Hence it protects RPL against *rank attack*.

As suggested in [75], those newly developed defense solutions need to be as simple as possible considering that RPL works on low-power lossy networks. Same authors suggest integrity check for the version field of the DIO messages to thwart *DODAG version attack* against RPL.

To defend against RPL rank attacks, VeRA (Version number and Rank Authentication) is proposed by Dvir *et al.* [135]. It is a security scheme that prevents misbehaving nodes manipulating their rank values for attack purposes. VeRA prevents publishing an illegitimate rank value by generating the hash chaining using random numbers chosen by the root node. An attacker cannot change the rank value as it requires the previous hash chain value to generate the new one. In order for a node to change its rank, rank authentication is needed. That is provided by the root node consisting of MAC (Message Authentication Code) generated from the max rank hash value and next version number as key. VeRA security scheme also prevents DODAG version attack by providing verification to version number using digital signature and MAC.

To defend against RPL local repair attacks, inclusion of timer (with a long waiting time setting) to the local link repair requests might be a good solution. Of course, VeRA will also partially defend the network against this kind of misuse, as misbehaving nodes are excluded from the network.

3.2.4 Defense on Transport Layer

3.2.4.1 Defense against De-Synchronization: As pointed out in [57], one way of defending against this kind of attack is authenticating all of the packets being exchanged, inclusively entire control field existed in the transport protocol header. On the assumption that an adversary cannot forge authentication, the endpoints of the communication would detect and ignore any malicious packets.

3.2.4.2 Defense against SYN-Flooding: Connectionless transport protocols are immune to SYN-Flooding attacks, but they might not provide the necessary transport-layer functionality to applications. One way of defense against this type of attack is SYN-cookies, which encode information from the client's TCP-SYN message and return it to the client to avoid maintaining state at the server. However, this technique's computational and message overhead makes it undesirable for WSNs and IoT [60].

As stressed out in [57], usage of client puzzles is a solution to defend against flooding attacks. The method presented in [136] requires clients to demonstrate the commitment to solve "client puzzles" in each connection. The server or base station is dedicated to create and verify puzzles for each client. The Base station has the responsibility to dissipate the puzzles to the network members (nodes) and whoever wishing to connect to the base station needs to solve the puzzle beforehand.

3.2.4.3 Defense against MQTT Exploit: Neisse *et al.* [137] have proposed enforcement of security policy rules at the MQTT layer, which can be used to support security and privacy requirements. Performance results of their presented implementation show that enforcing complex security policies introduce an additional delay of 10 ms. However, in mission-critical applications such as traffic control or IIoT [138], any value above 1 ms may not be tolerable and can cause system failures or accidents. Therefore, in order to be applicable for those scenarios, the delay related performance of the proposed scheme needs to be improved.

Singh *et al.* have proposed a Secure MQTT (SMQTT) protocol which augments security feature for the existing MQTT protocol and its variants based on lightweight Attribute Based Encryption (ABE) over elliptic curves. They take advantage of using ABE which supports broadcast encryption: With one cycle of encryption a message is delivered to multiple intended recipients and thus suitable for IoT applications [79].

3.2.4.4 Defense against Session Hijacking: Lightweight user authentication algorithm for optimized routing in mobile networks for defending against session hijacking attacks by Song *et al.* [139].

3.2.5 Defense on Application Layer

3.2.5.1 Defense against CoAP Exploit: As mentioned in [81], the Transport Layer Security (TLS) variant for CoAP is Datagram Transport Layer Security (DTLS) - it is called CoAPs in this phase, which provides an additional protection layer. However, this comes with a heavy cost of additional computation and big amount of handshake content in the message, which causes message fragmentation.

3.2.5.2 Defense against False Injection: Ye *et al.* [140] presented "statistical en-route filtering (SEF)" technique for detecting false information (data) injected in the WSN. Besides, as a mitigation, a methodology is provided in order to filter those injected data and how to achieve a consensus on a measurement by introducing a collective secret.

3.2.5.3 Defense against Path-Based DoS: To defend against Path-based DoS (PDoS) attacks, Deng *et al.* presented a light-weight, efficient and robust method which employed "one-way hash chains" that allowed intermediate sensor nodes to detect replayed and spurious packets [82]. In general, PDoS attack targets at intermediary sensor nodes in a "multi-hop end-to-end data path" of sensor networks. In the proposed solution of Deng *et al.* [82], a "one-way hash chain" in each sensor node towards a communications path is configured which enabled each intermediary sensor node ability in the detection of PDoS attacks. Hence, intermediary sensor nodes block the dissipation of fabricated and/or replayed packets. Each packet destined from an end-point includes a completely new "one-way hash chain" number, thereby replaying is prevented this way.

3.3 Summary of the Security Solutions

Table 2 summarizes all the attacks against WSNs and IoT along with the proposed defense (detection, prevention or mitigation) solutions related to corresponding attacks. Understanding these attacks and their associated defense mechanisms will help researchers to provide a secure path in building public trust and acknowledgment while developing algorithms, systems, and concepts for IoT.

Among those attacks, sinkhole and wormhole pose significant challenges to secure routing protocol design, and it is unlikely to devise effective countermeasures against these attacks that can be applied after the design of a protocol is completed. It is, therefore, crucial to design routing protocols in which these attacks are meaningless or ineffective. Geographic routing protocol [77] is one class of protocol that holds promise in this sense.

An ultimate limitation of building a multi-hop routing topology around a fixed set of base stations is that those nodes within one or two hops of the base stations are particularly attractive for compromise. After a significant number of these nodes have been compromised, all the network is lost. This indicates that clustering protocols like LEACH [141] and PCAC [142], where cluster-heads communicate directly with a base station, may ultimately yield the most secure solutions against node compromise and insider attacks.

4 Challenges, Open Issues and Solutions on Cyber-Security of the IoT

4.1 Technological Challenges

Building up an IoT network is a challenge by itself and this provides us a path to understanding the overall challenges while devising security algorithms for IoT. As discussed in [143], challenges of IoT can be summarized as but are not limited to:

- **Heterogeneity:** IoT consists of a variety of devices belonging to various families such as gateways, switches, sensors, actuators, smart appliances, mobile systems, etc. These devices all run on different circuitry, use diverse protocols for communications, and employ distinct data processing algorithms.
- **Scalability:** Addressing, naming, managing and servicing millions of devices is a unique challenge.
- **Communications:** Various technologies are used by IoT devices, such as wired or wireless communications e.g., Bluetooth, ZigBee, LPWAN.
- **Energy consumption:** This is one of the main challenging constraints of the IoT. Any kind of algorithm running on IoT devices needs to be designed with light-weight processing requirement.
- **Location privacy:** In the regular operation mode, things of the IoT should preserve their location privacy and when needed, they should provide this to network administrators.
- **Self awareness:** Smart objects of the IoT should self-organize themselves autonomously in order to fulfill some pre-determined specific tasks in responding real-word environmental situations without too much human intervention.
- **Interoperability:** In order for heterogeneous IoT devices to communicate, collaborate and share data with each other, there should be a pre-determined and standardized data exchange format.

4.2 Open Issues

The rapid development of IoT, Industrial IoT (IIoT) and Cyber-Physical Systems (CPS) has brought tremendous demand for smart-things (sensors, equipment, and devices, mostly referred as things) which are capable of sensing information from their surrounding, processing and transmitting it to far placed locations (mostly referred as data sinks) for further analysis and conclusions. Due to this extreme demand, cyber-security of these IoT enabled devices is somewhat disregarded [144]. Therefore, both industrially and commercially used IoT devices are vulnerable to several classes of attacks and possess potential back-doors to the systems they have been attached to [145].

For instance, as discussed in [146], smart home IoT-enabled appliances such as power switches, thermostat controls, smoke/fire alarms, ambient lighting systems, etc., bring security concerns to the attention of the public as they allow data sniffers to observe and conclude about the private activities of the house habitants. Apthorpe *et al.* [147] clearly has shown that an Internet Service Provider (ISP) or a network sniffer can easily infer inside activities of the house habitants and revoke their privacy even if they are employing encryption techniques to protect the content of data they are transmitting, by simply analyzing the Internet traffic pattern created by the smart home IoT devices.

Because of lacking rigid security precautions and bad user habits (sometimes the IoT implementers do not bother issuing a user and password for their devices, and sometimes they just continue with the default user name and password from the manufacturer), IoT devices are leveraged as a workforce of the botnets by ill mannered hackers. An example of this is *QBot botnet*, which is also known as Bashlite, Gayfgt, Lizkebab and Torlus. This IoT botnet was

TABLE 2
Layered categorization of cyber-security attacks towards WSNs and IoT along with the proposed solutions to defend against those attacks.

Attack type	**Layer**	**Proposed Solutions for Detection**	**Proposed Solutions for Prevention/Mitigation**
Eavesdropping	All layers	N/A	Link-layer encryption [59], [84], [85], [86], [87], [88], SensorWare communication multicast model [89], Key pre-distribution [90], [91], [92]
Jamming-DoS	Physical	Swarm intelligence [94], JAM (mapping) [95]	Usage of spread-spectrum communication [93], JAM (re-routing) [95], Wormhole technique [96]
Tampering	Physical	Routinely executing physical checks	Tamper resistant hardware, disabling JTAG and/or protecting bootstrap loader [63], camouflaging [18]
Collusion and Exhaustion	MAC	Error detection codes [18]	TDM, Error correction codes [18]
Denial of sleep and flooding	MAC	Anomaly detection on motes [66]	N/A
De-Synchronization	MAC	N/A	6TiSCH [97]
Unfairness	MAC	N/A	Usage of small frames [57]
Blackhole	Network	Anomaly detection on motes [66], REWARD [98], ActiveTrust [103], Packet count [104], TinyOS beaconing [105], Honeypot [100], Watchdog [101], Pseudo clustering algorithm [106]	REWARD routing [98], Multi-path routing [59], [93], [120], Mesh network topology [99], ActiveTrust routing [103], Isolation [104], BAMBi [105], MAODV [102]
HELLO flooding	Network	Bidirectional verification technique [107]	Identity verification protocol [59], Multi-path multi-base station routing [107], μ-TESLA [84]
Node-Replication (Clone)	Network	*Centralized solutions:* SET [110], Random pair wise key pre-distribution [111], Social fingerprinting [112], Speed test [113], Multi-level clustering [114] *Distributed solutions:* HIP-HOP [69], N2NB, DM, RM and LSM [70], SDC and P-MPC [115], RED [116], MEM [117], RDE [118]	ID-based public keys [108], Location-based key management [109], Multi-level clustering [114]
RPL DODAG version	Network	N/A	Integrity check [75], VeRA [135]
RPL local repair	Network	N/A	Inclusion of timer in local link repair messages, VeRA [135]
RPL rank	Network	N/A	TRAIL [134], VeRA [135]
Selective forwarding (Grayhole)	Network	Anomaly detection on motes [66], Acknowledgment monitoring [119],Neighbor knowledge [121], Reporting packet drops [122], Failure detection framework [123], Watchdog [101]	Multi-path routing [59], [120], Usage of source authorization [93]
Sinkhole	Network	Network flow graph [124],Geo-statistical sampling approach and distributed monitoring approach [125], Redundancy mechanism [126]	Secure routing algorithm [127]
6LoWPAN exploit	Network	N/A	6LowPSec [133], Content chaining scheme [76]
Sybil	Network	Radio resource testing, ID-based symmetric keys, registration, position verification, code attestation [128], RADS [129]	Indirect validation [59], Identity verification [128], Isolation [129], ID-based public keys [108]
Wormhole	Network	Packet Leashes [68], Directional antennas [130]	Location-based keys [108], Centralized computing [131], DAWWSEN [132]
De-Synchronization	Transport	N/A	Usage of authentication including transport layer protocol headers [57]
SYN-flooding	Transport	N/A	SYN-cookies [60], Client puzzles [136]
MQTT exploit	Transport	N/A	Enforcement of security policies [137], SMQTT [79]
Session hijacking	Transport	N/A	Light-weight user authentication algorithm for optimized routing in mobile networks [139]
CoAP exploit	App.	N/A	CoAPs, employment of DTLS [81]
False data injection	App.	SET [140]	Collective secret [140]
Path-based DoS	App.	N/A	One-way hash chains [82]

discovered in 2014 with the source code published in 2015. Some variants of Qbot botnet reached over 100,000 infected devices, serving as the precursor to Mirai botnet [148].

Mirai malware is another very good example to show the weaknesses of the things of IoT. *Mirai malware* is devised against Linux OS based IoT devices and gains shell access of the devices to divert their operations towards the benefit of the *Mirai botnet*. The Mirai botnet then uses this kind of captured zombie devices to perform further DDoS attacks against more advanced targets [149]. Most probably the users of those IoT devices won't even notice this unless inspected carefully. Therefore, in order to address this challenge, distributed and collaborative security solutions need to be optimized for IoT systems.

Recently revealed the *Torii botnet*, is a cut above both the Mirai and QBot variants, according to researchers from Avast, as it possesses sophistication "a level above anything we have seen before" botnet attack has shown that security of IoT needs to be considered more seriously than ever [150].

Unfortunately, enslavement of thousands of IoT devices by botnets shows us that many IoT ecosystems do not even possess basic security elements. According to an investigation among commercial off the shelf IoT products [151], the following are deduced: On average, 25 vulnerabilities are detected per device, 60% had vulnerable interfaces and firmware, 70% did not encrypt any communications at all, 80% failed to request secure length-ed password for authentication.

4.3 Security Proposals

IoT enabled Cyber-Physical Human Systems (CPHS) are one of the main components of the new era's cyber cities. As mentioned in [152], the human is one of the key components of the CPHS. For the cyber-security of CPHS, besides IoT systems, human interactions with the CPHS needs to be considered. According to [152], 95% of all security incidents happened due to human errors. Therefore, to defeat collaborative attacks against human errors, authors introduced an Intrusion Tolerant System (ITS) to support IoT enabled CPHS. The proposed ITS employs the Byzantine-resilient state machine approach, which combines replica diversity, voting, and cryptographic schemes to mask a number of compromised replicas of the nodes so that the CPHS can resume normal operation without distortion.

In [154], a privacy-preserving home automation network is proposed. An encrypted overlay network is created over commercially available Virtual Private Network (VPN) services to improve the privacy of the IoT users, especially the ones using the smart home systems.

In [153], authors proposed employment of hardware-based Physical Unclonable Functions (PUFs), to enhance and enable security-related operations to be handled at the sensor level in IoT. Usage of PUFs will help in increasing the security level of the IoT, by allowing low-level security implementations on the things and also by devising cryptography software to perform special tasks such as verification.

To enhance the security of IoT, [158] proposed remote attestation for trust establishment. According to authors, this is a non-trivial task because of the complexity of the design regarding the trust attestation schemes. These schemes, either hardware-based (e.g. PUFs) or software-based (e.g. control flow integrity checking), demand high power consumption along with extra economical cost, which is not suitable for vast implementation in the IoT. Some intermediate hybrid solutions (tailored in conjunction with the requirements and capabilities of the things) can be proposed in the near future, by blending both hardware- and software-based remote attestation schemes for trust establishment of IoT. These hybrid solutions need to be tested and verified for IoT, that they would able to work in scalable conditions and under the cyber-attacks such as DoS and against the condition of malicious verifiers.

Block-chain technology is a newly booming technology which was proposed for digital crypto-currencies. This technology was originally designed and invented by Bayer, Haber and Stornetta in 1992 [159] and incorporated Merkle trees to provide the efficiency and reliability of the digital timestamps. As discussed in [160], F.A. Hayek published his classic book 'Denationalization of Money' in 1976 [161] and argued that money is not different than other commodities and needs to be supplied by competition among private providers, not by the government. Crypto-currency has urged from that perspective, nowadays uses the block-chain technology and is a very hot topic. Besides, it attracted the public attention to the block-chain technology. Many researchers are working to bring and provide this technology for today's technological needs. Block-chain-based security algorithms provide a decentralized solution but involve significant energy, delay and computational overhead which is not suitable for resource constraint things of IoT. For instance, authors of [155] have proposed usage of block-chain technology in security and privacy of IoT. In their proposal, authors employed high processing enabled miner devices, additionally attached to the home network, to provide needs and functionalities of the block-chain algorithms. However, proof-of-concept applications need to be developed and further analyzed in this manner.

A solution employing Software Defined Networking (SDN) is proposed by [156] to detect and mitigate dynamic attacks against IoT. In the proposed "SoftThings" framework, *machine learning* is used at the SDN controller to monitor and learn the behavior pattern of IoT things over time. Anything out of the pre-determined behavior pattern is declared as an attack. The proposed scheme would be very effective on high processing capable IoT devices such as gateways and switches, but will not work on low-end IoT devices such as sensors and actuators.

Pacheco and Hariri [157] proposed a threat model for IoT to be employed for smart cyber-infrastructures which helps IoT network administrators in identifying potential attacks against each layer. The proposed threat model consists of four layers: things, network, services, and applications.

Providing security in IoT is challenging not only owing to the limited resources of the end-devices along with lossy communication links, but also due to the novel communications and networking technologies that are recently introduced such as RPL, 6LoWPAN, TSCH, MQTT, CoAP etc. Implications of using these technologies (one or many at the same time) under consideration of IoT network and device limitations need to be evaluated while taking security precautions. In this manner, researchers are working in the field

TABLE 3
Promising cyber-security solutions for IoT

Security proposal	Cyber-defense strategy
ITS [152]	Byzantine-resilient state machine approach for CPHS
PUFs [153]	Hardware embedded security functions
Privacy-preserving home automation network [154]	Usage of encrypted overlay network over commercially available VPN
Smart-home security [155]	Block-chain technology in security and privacy of IoT
6LowPSec [133]	End-to-end security solution that works on 6LoWPAN protocol
CoAP protocol [80]	Employment of DTLS which provide TLS equivalent security
MQTT-Security [137]	Enforcement of security policy rules for IoT
SoftThings [156]	Machine learning is used at the SDN controller
IoT security framework [157]	A threat model for IoT to be employed for smart cyber-infrastructures

and Table 3 presents summary of promising cyber-security solutions that are proposed for IoT.

5 Discussions and Final Remarks

Section II provided all possible attack scenarios towards WSNs and IoT. Section III presented not only the detection techniques of attacks but also the prevention and mitigation techniques. Whereas, Section 4 specifically considered the cyber-security related defense strategies devised for IoT. All these sections revealed that devising a "one-fits-all" security solution to defend the WSNs and IoT against cyber-attacks is non-trivial. Therefore in this section, we provide partial possible candidate solutions from the literature that are targeting security of some specific features of the WSNs, especially IoT. These solutions can be categorized as follows; key distribution, trust management, data confidentiality, segmented attack discovery, location privacy, hierarchical intrusion detection, redundant data infusion.

5.1 Key Distribution

In order to enhance the security of WSNs against attacks, one should consider increasing the effectivity and flexibility of the key distribution scheme being used. When using encryption throughout WSNs; one of the critical issues is how to properly distribute the secret keys among sensor nodes when needed. Besides, revocation of the existing nodes and addition of new nodes are other challenges to be introduced while designing key management for WSNs. More interested readers would refer to [11], [90], [91], [92] for further detailed discussions regarding key distribution and key management in WSNs.

5.2 Trust Management

Trust management is a very powerful concept to be used in detecting misbehaving sensor nodes in WSNs. After one of these nodes is detected by the trust evaluation, neighbors of this node can simply stop communicating with it. They can block the node by removing it from all routing tables, dropping all packets destined to/from it and stopping collaborating with it. By following this idea of using "trust management" to cope with attacks towards WSNs, many security methodologies and protocols are proposed in the literature. However, the proposed protocols introduced un-tolerable communication and/or computation overheads and unfortunately presented limited endurance against Sybil-attacks, DoS-attacks, and collusion-attacks. For instance, in the trust management scheme of [12], the trust evaluation of sensor nodes depends on the previous behavioral pieces of evidence or the referrals from the neighboring nodes. However, predicting future trust of a sensor node depending on its historical course of trust is just ignored. To enhance accuracy and efficacy of trust evaluation, more trust metrics should be included, i.e. packet-loss, hop-count, radio transmission range, energy consumption rate, data link latency, path-quality, etc.

As mentioned above and also in [162], application of trust mechanisms seem to be the future of WSNs in order to secure the sensor network from attackers. Secure routing along with secure data aggregation techniques are being devised for WSNs, especially based upon the trust metrics of the nodes. An example would be the "Trust-Aware Secure Routing Framework in Wireless Sensor Networks" presented by Duan *et al.* [163], which employs the combination of trust and QoS metrics in terms of routing related metrics in an effort to provide an optimized and qualified routing algorithm for WSNs.

In [164], Xiang *et al.* presented "Addition Encouragement, Multiplication Punishment (AEMP)" trust model in which each node in the network can calculate communication trust values of all its neighbors. An enhanced version of the AEMP trust model can be devised for WSNs in order to fight against the increasing number of attack scenarios.

Secure and efficient data transmission as shown in [165] would be another solution avenue to prevent attacks against WSNs. Encryption prevents eavesdropping and impersonation attacks but it brings an extra computational load to the sensor nodes, which in most cases have strict power constraints.

ActiveTrust of [103] is also another promising security solution for WSNs, in which trusted routing is achieved through an active detection route protocol. In ActiveTrust, basically the location and behavior of an attacker, along with the node related trust, could be gathered and utilized for avoiding blackholes while in process of real-data route construction. This provides "blackhole" free paths for the real-data traffic and improves network lifetime as well as network QoS drastically.

5.3 Data Aggregation

In WSNs, owing to the limited energy sources and computation power, data aggregation among sensor nodes is achieved at the aggregating-node and generally, this is executed by using simple methodologies like as data-averaging. Nonetheless, data-aggregation is not robust against node-compromisation attacks. Hence not only sensor nodes are generally deployed in unattended environments, but they also lack tamper-proof hardware; they are very vulnerable to those mentioned attacks. Therefore, the inclusion of trustworthiness to data management and reputing mechanisms of nodes has prime importance for sensor networks as well as IoT. Secure data aggregation techniques such as Iterative Filtering (this algorithm is an appealing alternative for sensor networks hence it solves both problems 1) data aggregation, 2) assessment of data-trustworthiness; by employing a unique iterative method [166]), would be used in WSNs and IoT in order to cope with the vulnerabilities mentioned above.

Therefore, a unique way of providing security to WSNs and IoT would be "secure data aggregation". In the specific applications where average sensed data is of the interest, for example, the average temperature of a crop field, this method may be used efficiently. Data can be averaged at some "aggregation points" and these aggregation points might communicate each other in a more secure way by implementing ways of Secret Key Cryptography (SKC). This way, more attention can be paid to this specific data gathering points and hence more secure data dissemination can be achieved.

5.4 Hierarchical Security Solution

Another promising technique to cope with attacks against WSNs would be hierarchical security solutions:

Butun *et al.* [114]'s hierarchical IDS provides two different paths of detecting intruders through watchdog and majority voting mechanisms. Multi-level cluster heads and subordinate nodes are being watched and recorded separately, and at a specific threshold level, intruders have revoked from the network accordingly.

In Wu *et al.* [167]'s hierarchical security framework, authors employed dynamic adaptive chance discovery mechanism to detect unknown attacks. With this unified framework, low-level attack-detection is executed in sensor nodes with simple rules, and high-level attack-detection is executed in sinks and at the base-station with complex rules. Besides, software-defined networking and network function virtualization technologies are used to perform attack mitigation when any type of attack is detected.

5.5 Traffic Shaping

Independent Link Padding (ILP) is a network traffic shaping methodology proposed by Apthorpe *et al.* [147] in an effort to protect smart home IoT systems from network sniffing (eavesdropping) attacks. The proposed ILP scheme is promising in protecting privacies of the house habitants from unintended eyes. ILP works in a sense to shape the traffic without violating pre-determined data rate and schedule of the regular network traffic so that it does not cause disturbance or loss for the data communication activities of the smart home IoT devices. In essence, the result of the ILP procedure ends up with a constant flow of information in which regular and meaningful data packets are padded with redundant data so that no useful information can be interpolated from the data traffic. By this way, the privacy of the smart home users is assured against passive information gathering (sniffing or eavesdropping) attack. ILP methodology improves the privacy of the IoT users, however, it causes bandwidth of the network to be wasted by introducing extra load and causing unnecessary traffic.

5.6 Patch management

Patch management possesses a very significant role in industrial networks and IIoT, in which timely patching firmware of the critical devices has prime importance, such as the ones in SCADA networks, that are deployed over critical infrastructures and factories [168]. As mentioned in [169], patching vulnerabilities of the IoT is also very important as in the case of many computer networks, however, owing to their low-cost components, i.e. things of IoT consists of very cheap embedded devices most of which do not have upgradeable firmware, this is quite impossible.

5.7 Automated fingerprinting

In order to prevent node replication attacks and variants towards IoT, an automated fingerprinting technique can be used. In this technique, several messages emanating from legitimate devices can be characterized, such as periodic status update messages, firmware update messages, patch update messages, device initiation messages, etc. Any behavior, out of this fingerprint can be evaluated as a suspicious act or an attack.

6 Conclusion

The IoT is a large-scale complex architectural design consisting of a variety of heterogeneous devices, therefore scalability, transparency, and reliability are most prominent issues to be solved. Security-related initiatives need to consider these issues in the first place. Besides, not only should a higher architectural security design be conceptualized, but low-level security also needs to be addressed. This can be achieved by designing lightweight security protocols and cryptography algorithms that are tailored according to the specific needs of the resource-constrained devices of the IoT.

From the discussions made throughout this paper, it can be deduced that the heterogeneity of the devices in IoT ecosystem along with its scalability causes several implications, in terms of security. Although some of the new vulnerabilities can be discovered on time, related security patches cannot be installed to the end devices in a timely manner due to the mentioned IoT network implications above. Therefore IDS techniques become more important for IoT systems, as some of them are even efficient against zero-day-attacks. If the necessary IDS techniques require high processing power, gateway devices can be employed for this purpose.

As a conclusion, security must be a key component when designing protocols for WSNs as well as IoT. Without a

TABLE 4
List of abbreviations.

Abbreviation	Explanation
ARP	Address Resolution Protocol
CIA	Confidentiality, Integrity, Availability
CoAP	Constrained Application Protocol
CoAPs	CoAP in secure mode (by using DTLS)
CPS	Cyber Physical System
CPHS	Cyber Physical Human System
CTS	Clear to Send
DODAG	Destination Oriented Directed Acyclic Graph
DIO	DODAG Information Object
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
ID	Identity
IDS	Intrusion Detection System
ILP	Independent Link Padding
IoT	Internet of Things
IPS	Intrusion Prevention System
ISP	Internet Service Provider
MAC	Medium Access Control
MANET	Mobile Ad-Hoc Network
MEMS	Micro Electro Mechanical Systems
MQTT	Message Queue Telemetry Transport
OSI	Open Systems Interconnection
PKC	Public Key Cryptography
PUF	Physical Unclonable Function
PZ	Promiscuous Zone
RPL	Routing Protocol for Low-power and lossy networks
RREQ	Route Request
RREP	Route Reply
RTS	Request to Send
SDN	Software Defined Networking
SKC	Secret Key Cryptography
TLS	Transport Layer Security
TSCH	Time Slotted Channel Hopping
VPN	Virtual Private Network
WSN	Wireless Sensor Network
6LowPAN	Internet protocol devised for the IoT for the usage with IPv6
6TiSCH	IPv6 over the TSCH mode

proper assessment of possible threats and inclusion of related preventive measures, these networks will be vulnerable to attacks. Future researchers working on WSNs and IoT need to consider security to a higher extent while designing their routing, key distribution, trust management, and finally data aggregation schemes over MAC, networking, transport, and application layers.This paper has compiled all known types of security attacks towards WSNs in IoT context together with a description and evaluation of the defending strategies against each type of attack. Authors hope that this article will shed light on the researchers working in the field of WSNs and IoT, by leading them to produce more robust and secure network solutions.

APPENDIX A
ABBREVIATIONS AND ACRONYMS

List of abbreviations are listed in Table 4.

REFERENCES

[1] I. Butun, "Prevention and detection of intrusions in wireless sensor networks," *Ph.D. Dissertation, University of South Florida*, 2013.

[2] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[3] V. Friedman. (2018) On the edge: Solving the challenges of edge computing in the era of iot. [Online]. Available: https://data-economy.com/on-the-edge-solving-the-challenges-of-edge-computing-in-the-era-of-iot/

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[5] M. Kocakulak and I. Butun, "An overview of wireless sensor networks towards internet of things," in *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017, pp. 1–6.

[6] S. Fang, L. Da Xu, Y. Zhu, J. Ahati, H. Pei, J. Yan, Z. Liu *et al.*, "An integrated system for regional environmental monitoring and management based on internet of things." *IEEE Trans. Industrial Informatics*, vol. 10, no. 2, pp. 1596–1605, 2014.

[7] M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*. IEEE, 2014, pp. 1–8.

[8] P. Gope and T. Hwang, "Bsn-care: A secure iot-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.

[9] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[10] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in wireless sensor networks: a survey," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1022–1034, 2012.

[11] C.-Y. Chen and H.-C. Chao, "A survey of key distribution in wireless sensor networks," *Security and Communication Networks*, vol. 7, no. 12, pp. 2495–2508, 2014.

[12] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 602–617, 2014.

[13] A. G. Finogeev and A. A. Finogeev, "Information attacks and security in wireless sensor networks of industrial scada systems," *Journal of Industrial Information Integration*, vol. 5, pp. 6–16, 2017.

[14] G. Padmavathi and M. D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *IJCSIS*, pp. 117–125, 2009.

[15] A.-S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges," in *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, vol. 2. IEEE, 2006, pp. 6–pp.

[16] K. Shabana, N. Fida, F. Khan, S. R. Jan, and M. U. Rehman, "Security issues and attacks in wireless sensor networks," *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, vol. 5, no. 7, pp. pp–81, 2016.

[17] S. Bartariya and A. Rastogi, "Security in wireless sensor networks: Attacks and solutions," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 3, 2016.

[18] K. Sharma and M. Ghose, "Wireless sensor networks: An overview on its security threats," *IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs*, pp. 42–45, 2010.

[19] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," *arXiv preprint arXiv:1501.02211*, 2015.

[20] I. Butun, N. Pereira, and M. Gidlund, "Analysis of lorawan v1.1 security," in *Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects*. ACM, 2018, p. 5.

[21] ——, "Security risk analysis of lorawan and future directions," *Future Internet*, vol. 11, no. 1, p. 3, 2019.

[22] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, "Formal security analysis of lorawan," *Computer Networks*, 2018.

[23] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, "A survey of lorawan for iot: From technology to application," *Sensors*, vol. 18, no. 11, p. 3995, 2018.

[24] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on lpwa technology: Lora and nb-iot," *Ict Express*, vol. 3, no. 1, pp. 14–21, 2017.

[25] I. Butun, "Privacy and trust relations in internet of things from the user point of view," in *Computing and Communication Work-*

shop and Conference (CCWC), 2017 IEEE 7th Annual. IEEE, 2017, pp. 1–5.

[26] R. Chen, J. Guo, and F. Bao, "Trust management for soa-based iot and its application to service composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, 2016.

[27] D. Ott, C. Vishik, D. Grawrock, and A. Rajan, "Trust evidence for iot: Trust establishment from servers to sensors," in *ISSE 2015*. Springer, 2015, pp. 121–131.

[28] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.

[29] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.

[30] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," Tech. Rep., 2014.

[31] K. Hartke, "Observing resources in the constrained application protocol (coap)," Tech. Rep., 2015.

[32] A. Banks and R. Gupta, "Mqtt version 3.1. 1," *OASIS standard*, vol. 29, 2014.

[33] T. Yokotani and Y. Sasaki, "Comparison with http and mqtt on required network resources for iot," in *Control, Electronics, Renewable Energy and Communications (ICCEREC), 2016 International Conference on*. IEEE, 2016, pp. 1–6.

[34] A. Brandt, E. Baccelli, R. Cragie, and P. van der Stok, "Applicability statement: The use of the routing protocol for low-power and lossy networks (rpl) protocol suite in home automation and building control," Tech. Rep., 2016.

[35] T. Zhang and X. Li, "Evaluating and analyzing the performance of rpl in contiki," in *Proceedings of the first international workshop on Mobile sensing, computing and communication*. ACM, 2014, pp. 19–24.

[36] V. P. Nikshepa and U. K. K. Shenoy, "6lowpanperformance analysis on low power networks," in *International Conference on Computer Networks and Communication Technologies: ICCNCT 2018*, vol. 15. Springer, 2018, p. 145.

[37] A. Fabre, K. Martinez, G. M. Bragg, P. J. Basford, J. Hart, S. Bader, and O. M. Bragg, "Deploying a 6lowpan, coap, low power, wireless sensor network," in *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*. ACM, 2016, pp. 362–363.

[38] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6tisch: deterministic ip-enabled industrial internet (of things)," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 36–41, 2014.

[39] T. Watteyne, P. Tuset-Peiro, X. Vilajosana, S. Pollin, and B. Krishnamachari, "Teaching communication technologies and standards for the industrial iot? use 6tisch!" *IEEE Communications Magazine*, vol. 55, no. 5, pp. 132–137, 2017.

[40] T. Chang, T. Watteyne, K. Pister, and Q. Wang, "Adaptive synchronization in multi-hop tsch networks," *Computer Networks*, vol. 76, pp. 165–176, 2015.

[41] T. Watteyne, M. Palattella, and L. Grieco, "Using ieee 802.15. 4e time-slotted channel hopping (tsch) in the internet of things (iot): Problem statement," Tech. Rep., 2015.

[42] S. Jeschke, C. Brecher, H. Song, and D. Rawat, "Industrial internet of things: Foundations, principles and applications," *Cham, Switzerland: Springer*, pp. 1–715, 2017.

[43] S. Forsström, I. Butun, M. Eldefrawy, U. Jennehag, and M. Gidlund, "Challenges of securing the industrial internet of things value chain," in *2018 Workshop on Metrology for Industry 4.0 and IoT*. IEEE, 2018, pp. 218–223.

[44] H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, *Cyber-physical systems: foundations, principles and applications*. Morgan Kaufmann, 2016.

[45] Y. Zhang, L. Sun, H. Song, and X. Cao, "Ubiquitous wsn for healthcare: Recent advances and future prospects," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 311–318, 2014.

[46] K. Xu, X. Wang, W. Wei, H. Song, and B. Mao, "Toward software defined smart home," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 116–122, 2016.

[47] S. Rani, S. H. Ahmed, R. Talwar, J. Malhotra, and H. Song, "Iomt: A reliable cross layer protocol for internet of multimedia things," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 832–839, 2017.

[48] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of things and big data analytics for smart and connected communities," *IEEE access*, vol. 4, pp. 766–773, 2016.

[49] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1143–1155, 2017.

[50] Q. Xu, P. Ren, H. Song, and Q. Du, "Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1924–1933, 2017.

[51] J. Zhu, Y. Song, D. Jiang, and H. Song, "A new deep-q-learning-based transmission scheduling mechanism for the cognitive internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2375–2385, 2018.

[52] I. Butun, A. Sari, and P. Österberg, "Security implications of fog computing on the internet of things," *arXiv preprint arXiv:1809.10492*, 2018.

[53] H. Song, G. A. Fink, and S. Jeschke, *Security and Privacy in Cyber-physical Systems: Foundations, Principles, and Applications*. John Wiley & Sons, 2017.

[54] H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke, *Smart cities: foundations, principles, and applications*. John Wiley & Sons, 2017.

[55] Y. Sun and H. Song, *Secure and Trustworthy Transportation Cyber-Physical Systems*. Springer, 2017.

[56] W. Li, H. Song, and F. Zeng, "Policy-based secure and trustworthy sensing for internet of things in smart cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 716–723, 2018.

[57] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[58] Y.-a. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*. ACM, 2003, pp. 135–147.

[59] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.

[60] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, 2008.

[61] E. Çayirci and C. Rong, "Security attacks in ad hoc, sensor and mesh networks," *Security in Wireless Ad Hoc and Sensor Networks*, pp. 105–120, 2009.

[62] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," *Ad Hoc Networks*, vol. 3, no. 1, pp. 69–89, 2005.

[63] W. Znaidi, M. Minier, and J.-P. Babau, "An ontology for attacks in wireless sensor networks," Ph.D. dissertation, INRIA, 2008.

[64] F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ubiquitous computing," *Computer*, vol. 35, no. 4, pp. 22–26, 2002.

[65] S. M. Sajjad and M. Yousaf, "Security analysis of ieee 802.15. 4 mac in the context of internet of things (iot)," in *Information Assurance and Cyber Security (CIACS), 2014 Conference on*. IEEE, 2014, pp. 9–14.

[66] Y. Liu, Y. Li, and H. Man, "Mac layer anomaly detection in ad hoc networks," in *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*. IEEE, 2005, pp. 402–409.

[67] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE wireless communications*, vol. 11, no. 1, pp. 38–47, 2004.

[68] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3. IEEE, 2003, pp. 1976–1986.

[69] M. Conti, R. Di Pietro, and A. Spognardi, "Clone wars: Distributed detection of clone attacks in mobile wsns," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 654–669, 2014.

[70] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Security and Privacy, 2005 IEEE Symposium on*. IEEE, 2005, pp. 49–63.

[71] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the 2nd ACM workshop on Wireless security*. ACM, 2003, pp. 30–40.

[72] T. Winter, "Rpl: Ipv6 routing protocol for low-power and lossy networks," 2012, by Internet Engineering Task Force (IETF).

[73] P. Pongle and G. Chavan, "A survey: Attacks on rpl and 6lowpan in iot," in *Pervasive Computing (ICPC), Int. Conf. on*. IEEE, 2015, pp. 1–6.

[74] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (iot): Taxonomy of security attacks," in *Electronic Design (ICED), 2016 3rd International Conference on*. IEEE, 2016, pp. 321–326.

[75] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "A study of rpl dodag version attacks," in *IFIP international conference on autonomous infrastructure, management and security*. Springer, 2014, pp. 92–104.

[76] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6lowpan fragmentation attacks and mitigation mechanisms," in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, 2013, pp. 55–66.

[77] H. P. Gupta, S. Rao, A. K. Yadav, and T. Dutta, "Geographic routing in clustered wireless sensor networks among obstacles," *IEEE Sensors Journal*, vol. 15, no. 5, pp. 2984–2992, 2015.

[78] I. I. technology, "Message queuing telemetry transport (mqtt) v3.1.1," *International Organization for Standardization*, vol. 20922, no. 2016, 2016.

[79] M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure mqtt for internet of things (iot)," in *Communication systems and network technologies (CSNT), 2015 fifth international conference on*. IEEE, 2015, pp. 746–751.

[80] B. Frank, Z. Shelby, K. Hartke, and C. Bormann, "Constrained application protocol (coap)," in *IETF-draft*. IETF, 2011.

[81] R. A. Rahman and B. Shah, "Security analysis of iot protocols: A focus in coap," in *Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on*. IEEE, 2016, pp. 1–7.

[82] J. Deng, R. Han, and S. Mishra, "Defending against path-based dos attacks in wireless sensor networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2005, pp. 89–96.

[83] S. Ghildiyal, A. K. Mishra, A. Gupta, and N. Garg, "Analysis of denial of service (dos) attacks in wireless sensor networks," *IJRET: International Journal of Research in Engineering and Technology*, vol. 3, pp. 2319–1163, 2014.

[84] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.

[85] J. Deng, R. Han, and S. Mishra, "A performance evaluation of intrusion-tolerant routing in wireless sensor networks," in *Information Processing in Sensor Networks*. Springer, 2003, pp. 552–552.

[86] R. Di Pietro, L. V. Mancini, Y. W. Law, S. Etalle, and P. Havinga, "Lkhw: A directed diffusion-based secure multicast scheme for wireless sensor networks," in *Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on*. IEEE, 2003, pp. 397–406.

[87] M. Tubaishat, J. Yin, B. Panja, and S. Madria, "A secure hierarchical model for sensor network," *ACM Sigmod Record*, vol. 33, no. 1, pp. 7–13, 2004.

[88] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*. ACM, 2004, pp. 162–175.

[89] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. B. Srivastava, "On communication security in wireless ad-hoc sensor networks," in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on*. IEEE, 2002, pp. 139–144.

[90] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 2, pp. 228–258, 2005.

[91] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*. IEEE, 2003, pp. 197–213.

[92] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*. ACM, 2002, pp. 41–47.

[93] A. Agah and S. K. Das, "Preventing dos attacks in wireless sensor networks: A repeated game theory approach." *IJ Network Security*, vol. 5, no. 2, pp. 145–153, 2007.

[94] R. Muraleedharan and L. A. Osadciw, "Cross layer denial of service attacks in wireless sensor network using swarm intelligence," in *Information Sciences and Systems, 2006 40th Annual Conference on*. IEEE, 2006, pp. 1653–1658.

[95] A. D. Wood, J. A. Stankovic, and S. H. Son, "Jam: A jammed-area mapping service for sensor networks," in *Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE*. IEEE, 2003, pp. 286–297.

[96] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-based antijamming techniques in sensor networks," *IEEE transactions on Mobile Computing*, vol. 6, no. 1, 2007.

[97] N. Accettura and G. Piro, "Optimal and secure protocols in the ietf 6tisch communication stack," in *Industrial electronics (ISIE), 2014 IEEE 23rd international symposium on*. IEEE, 2014, pp. 1469–1474.

[98] Z. Karakehayov, "Using reward to detect team black-hole attacks in wireless sensor networks," *Wksp. Real-World Wireless Sensor Networks*, pp. 20–21, 2005.

[99] S. N. Krishnan and P. Srinivasan, "A qos parameter based solution for black hole denial of service attack in wireless sensor networks," *Indian Journal of Science and Technology*, vol. 9, no. 38, 2016.

[100] A. Prathapani, L. Santhanam, and D. P. Agrawal, "Intelligent honeypot agent for blackhole attack detection in wireless mesh networks," in *Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on*. IEEE, 2009, pp. 753–758.

[101] M. Tiwari, K. V. Arya, R. Choudhari, and K. S. Choudhary, "Designing intrusion detection to detect black hole and selective forwarding attack in wsn based on local information," in *Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on*. IEEE, 2009, pp. 824–828.

[102] M. Medadian, M. H. Yektaie, and A. M. Rahmani, "Combat with black hole attack in aodv routing protocol in manet," in *Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on*. IEEE, 2009, pp. 1–5.

[103] Y. Liu, M. Dong, K. Ota, and A. Liu, "Activetrust: secure and trustable routing in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013–2027, 2016.

[104] M. Wazid, A. Katal, R. S. Sachan, R. Goudar, and D. Singh, "Detection and prevention mechanism for blackhole attack in wireless sensor network," in *Communications and Signal Processing (ICCSP), 2013 International Conference on*. IEEE, 2013, pp. 576–581.

[105] S. Misra, K. Bhattarai, and G. Xue, "Bambi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks," in *Communications (ICC), International Conference on*. IEEE, 2011, pp. 1–5.

[106] A. Amouri, L. G. Jaimes, R. Manthena, S. D. Morgera, and I. J. Vergara-Laurens, "A simple scheme for pseudo clustering algorithm for cross layer intrusion detection in manet," in *Communications (LATINCOM), 2015 7th IEEE Latin-American Conference on*. IEEE, 2015, pp. 1–6.

[107] M. A. Hamid, M. Rashid, and C. S. Hong, "Routing security in sensor network: Hello flood attack and defense," *IEEE ICNEWS*, pp. 2–4, 2006.

[108] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE Journal on selected areas in communications*, vol. 24, no. 2, pp. 247–260, 2006.

[109] M.-j. Duan and J. Xu, "An efficient location-based compromise-tolerant key management scheme for sensor networks," *Information Processing Letters*, vol. 111, no. 11, pp. 503–507, 2011.

[110] H. Choi, S. Zhu, and T. F. La Porta, "Set: Detecting node clones in sensor networks," in *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*. IEEE, 2007, pp. 341–350.

[111] R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1246–1258, 2007.

[112] K. Xing, F. Liu, X. Cheng, and D. H. Du, "Real-time detection of clone attacks in wireless sensor networks," in *Distributed Computing Systems. ICDCS'08. The 28th Int. Conf. on*. IEEE, 2008, pp. 3–10.

[113] J.-W. Ho, M. Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 1773–1781.

[114] I. Butun, I.-H. Ra, and R. Sankar, "An intrusion detection system

based on multi-level clustering for hierarchical wireless sensor networks," *Sensors*, vol. 15, no. 11, pp. 28 960–28 978, 2015.

[115] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*. IEEE, 2007, pp. 257–267.

[116] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2007, pp. 80–89.

[117] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in *Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on*. IEEE, 2009, pp. 284–293.

[118] Z. Li and G. Gong, "Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks," in *Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on*. IEEE, 2009, pp. 1030–1035.

[119] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*. IEEE, 2006, pp. 8–pp.

[120] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, pp. 11–25, 2001.

[121] T. H. Hai and E.-N. Huh, "Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge," in *Network Computing and Applications, 2008. NCA'08. Seventh IEEE International Symposium on*. IEEE, 2008, pp. 325–331.

[122] J. Brown and X. Du, "Detection of selective forwarding attacks in heterogeneous sensor networks," in *Communications, 2008. ICC'08. IEEE International Conference on*. IEEE, 2008, pp. 1583–1587.

[123] G. Wang, W. Zhang, G. Cao, and T. La Porta, "On supporting distributed collaboration in sensor networks," in *Military Communications Conference, 2003. MILCOM'03. 2003 IEEE*, vol. 2. IEEE, 2003, pp. 752–757.

[124] E. C. Ngai, J. Liu, and M. R. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," in *Communications, 2006. ICC'06. IEEE International Conference on*, vol. 8. IEEE, 2006, pp. 3383–3389.

[125] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 644–653, 2014.

[126] F.-J. Zhang, L.-D. Zhai, J.-C. Yang, and X. Cui, "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks," *Procedia Computer Science*, vol. 31, pp. 711–720, 2014.

[127] L. Teng and Y. Zhang, "Sera: a secure routing algorithm against sinkhole attacks for mobile wireless sensor networks," in *Computer Modeling and Simulation, 2010. ICCMS'10. Second International Conference on*, vol. 4. IEEE, 2010, pp. 79–82.

[128] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, 2004, pp. 259–268.

[129] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Detecting sybil attacks in wireless sensor networks using uwb ranging-based information," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7560–7572, 2015.

[130] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks." in *NDSS*, 2004, pp. 241–245.

[131] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 51–60.

[132] R. Z. El Kaissi, A. Kayssi, A. Chehab, and Z. Dawy, "Dawwsen: A defense mechanism against wormhole attacks in wireless sensor networks," Ph.D. dissertation, American University of Beirut, Department of Electrical and Computer Engineering, 2005.

[133] G. Glissa and A. Meddeb, "6lowpsec: An end-to-end security protocol for 6lowpan," *Ad Hoc Networks*, 2018.

[134] H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, and M. Wählisch, "Trail: Topology authentication in rpl," *arXiv preprint arXiv:1312.0984*, 2013.

[135] A. Dvir, L. Buttyan *et al.*, "Vera-version number and rank authentication in rpl," in *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*. IEEE, 2011, pp. 709–714.

[136] T. Aura, P. Nikander, and J. Leiwo, "Dos-resistant authentication with client puzzles," in *International workshop on security protocols*. Springer, 2000, pp. 170–177.

[137] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2014 IEEE 10th International Conference on*. IEEE, 2014, pp. 165–172.

[138] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[139] S. Song, H.-K. Choi, and J.-Y. Kim, "A secure and lightweight approach for routing optimization in mobile ipv6," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 7, 2009.

[140] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 839–850, 2005.

[141] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on*. IEEE, 2000, pp. 10–pp.

[142] I. Butun, I.-h. Ra, and R. Sankar, "Pcac: power-and connectivity-aware clustering for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, p. 83, 2015.

[143] A. Balte, A. Kashid, and B. Patil, "Security issues in internet of things (iot): A survey," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 4, 2015.

[144] S. Li and L. Da Xu, *Securing the internet of things*. Syngress, 2017.

[145] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial iot devices," in *Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific*. IEEE, 2016, pp. 519–524.

[146] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home iot devices," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 11th Int. Conf. on*. IEEE, 2015, pp. 163–167.

[147] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic," *arXiv preprint arXiv:1708.05044*, 2017.

[148] Radware. (2018) A quick history of iot botnets. [Online]. Available: https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/

[149] S. Chaudhary, "Privacy and security issues in internet of things," *International Education and Research Journal*, vol. 3, no. 5, 2017.

[150] C. Osborne. (2018) Meet torii, a new iot botnet far more sophisticated than mirai variants. [Online]. Available: https://www.zdnet.com/article/meet-torii-a-new-iot-botnet-far-more-sophisticated-than-mirai/

[151] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[152] S. A. Kumar, B. Bhargava, R. Macêdo, and G. Mani, "Securing iot-based cyber-physical human systems against collaborative attacks," in *Internet of Things (ICIOT), 2017 IEEE International Congress on*. IEEE, 2017, pp. 9–16.

[153] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of iot systems: Design challenges and opportunities," in *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*. IEEE Press, 2014, pp. 417–423.

[154] M. R. Schurgot, D. A. Shinberg, and L. G. Greenwald, "Experiments with security and privacy in iot networks," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 16th International Symposium on a*. IEEE, 2015, pp. 1–6.

[155] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*. IEEE, 2017, pp. 618–623.

[156] S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in iot using sdn," in *Telecommunication Networks and Applications Conference (ITNAC), 2017 27th International*. IEEE, 2017, pp. 1–6.

[157] J. Pacheco and S. Hariri, "Iot security framework for smart cyber infrastructures," in *Foundations and Applications of Self* Systems, IEEE International Workshops on*. IEEE, 2016, pp. 242–247.
[158] T. Abera, N. Asokan, L. Davi, F. Koushanfar, A. Paverd, A.-R. Sadeghi, and G. Tsudik, "Things, trouble, trust: on building trust in iot systems," in *Proceedings of the 53rd Annual Design Automation Conference*. ACM, 2016, p. 121.
[159] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," in *Sequences II*. Springer, 1993, pp. 329–334.
[160] J. E. McDonald, "The tokenization of industrial cryptocurrency mining," *Ormeus Coin, white paper*, pp. 1–21, 2018.
[161] F. A. von Hayek, *Denationalisation of Money: An Analysis of the Theory and Practice of Current Currencies*. Institute of economic affairs, 1976.
[162] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.
[163] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "Tsrf: A trust-aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.
[164] G. Xiang, Q. Jianlin, and W. Jin, "Research on trust model of sensor nodes in wsns," *Procedia Engineering*, vol. 29, pp. 909–913, 2012.
[165] H. Lu, J. Li, and M. Guizani, "Secure and efficient data transmission for cluster-based wireless sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 25, no. 3, pp. 750–761, 2014.
[166] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 98–110, 2015.
[167] J. Wu, K. Ota, M. Dong, and C. Li, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, vol. 4, pp. 416–424, 2016.
[168] M. Al-Faruque, I. Butun, L. Dalloro, H. Ludwig, J. Claus, and R. Frohlich, "Networking elements as a patch distribution platform for distributed automation and control domains," 2012, patents, U.S. Patent WO2012177597 A1.
[169] W. Stallings and L. Brown, *Computer Security: Principles and Practice, Global Edition*. Pearson Education Limited, 2018.

PLACE PHOTO HERE

Ismail Butun (M'09) received his B.Sc. and M.Sc. degrees in Electrical and Electronics Engineering from Hacettepe University, his M.Sc. and Ph.D. degrees in Electrical Engineering from the University of South Florida. He worked as an Assistant Professor in years between 2015 and 2016. Since 2017, he has been working as a post-doctoral fellow for various universities (University of Delaware, Mid Sweden University, Chalmers University of Technology). He has more than 30 publications in peer-reviewed scientific international journals and conference proceedings, along with an H-index of 11. He is a well recognized academic reviewer by IEEE, ACM, and Springer, who served for 32 various scientific journals and conferences in the review process of more than 80 articles. He is an editor of Springer Nature. His research interests include but not limited to; computer networks, wireless communications, WSNs, IoT, cyber-physical systems, cryptography, network security, and intrusion detection.

PLACE PHOTO HERE

Patrik Österberg (M'05) received his M.Sc. degree in Electrical Engineering from Mid Sweden University, Sundsvall, Sweden, in 2000, the degree of Licentiate of Technology in Teleinformatics from the Royal Institute of Technology, Stockholm, Sweden, in 2005, and the Ph.D. degree in Computer and System Science from Mid Sweden University in 2008. During 2007, he worked as a development engineer at Acreo AB in Hudiksvall, Sweden, and from 2008 to 2010, he was employed as researcher at Interactive TV Arena KB in Gävle, Sweden. Since 2008, he is an Assistant Professor at Mid Sweden University and from 2013, he is also the head of the Department of Information System and Technology.

PLACE PHOTO HERE

Houbing Song (M'12–SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in August 2012, and the M.S. degree in civil engineering from the University of Texas, El Paso, TX, in December 2006. In August 2017, he joined the Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us). He served on the faculty of West Virginia University from August 2012 to August 2017. In 2007 he was an Engineering Research Associate with the Texas A&M Transportation Institute. He serves as an Associate Technical Editor for IEEE Communications Magazine. He is the editor of four books, including Smart Cities: Foundations, Principles and Applications, Hoboken, NJ: Wiley, 2017, Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, Chichester, UK: Wiley-IEEE Press, 2017, Cyber-Physical Systems: Foundations, Principles and Applications, Boston, MA: Academic Press, 2016, and Industrial Internet of Things: Cybermanufacturing Systems, Cham, Switzerland: Springer, 2016. He is the author of more than 100 articles. His research interests include cyber-physical systems, cybersecurity and privacy, internet of things, edge computing, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. Dr. Song is a senior member of ACM. Dr. Song was a recipient of the prestigious Air Force Research Laboratory's Information Directorate (AFRL/RI) Visiting Faculty Research Fellowship in 2018, and the very first recipient of the Golden Bear Scholar Award, the highest campus-wide recognition for research excellence at West Virginia University Institute of Technology (WVU Tech), in 2016.