World Wide Web (2021) 24:971–1001
https://doi.org/10.1007/s11280-020-00855-2

DDoS attacks in IoT networks: a comprehensive systematic literature review

Yahya Al-Hadhrami[1] · **Farookh Khadeer Hussain**[1]

Received: 10 December 2019 / Revised: 12 November 2020 / Accepted: 23 November 2020 /
Published online: 6 January 2021

Abstract

The Internet of Things (IoT) is a rapidly emerging technology in the consumer and industrial market. This technology has the potential to radically transform the consumer experience, as it will change our daily scenes, starting from the way we drink coffee to how smart objects interact with industrial applications. Such rapid development and deployment face multifarious challenges, including the sheer amount of data generated, network scale, network heterogeneity, as well as security and privacy concerns. In recent years, Distributed Denial-of-Service (DDoS) attacks in IoT networks are considered one of the growing challenges that need to be shed light on. DDoS attacks utilize the limited resources in IoT devices, such as storage limitation and network capacity, that cause this issue in the IoT application. This paper comprehensively reviews the attacks that can lead to DDoS, which eventually will cause serious damage to existing systems. Additionally, the paper investigates the available solutions used to counter these attacks and explore their limitations from the perspective of the constrained device. Furthermore, a detailed analysis of the existing solution placement was implemented, including heterogeneity and their performance for IoT based networks. Finally, the paper will reveal and discuss interesting research direction on the future IoT security and current trends.

Keywords IoT security · Trust · Intrusion detection system ++

This article belongs to the Topical Collection: *Special Issue on Intelligent Fog and Internet of Things (IoT)-Based Services*
Guest Editors: Farookh Hussain, Wenny Rahayu, and Makoto Takizawa

✉ Yahya Al-Hadhrami
yahya.s.al-hadhrami@student.uts.edu.au

Farookh Khadeer Hussain
farookh.hussain@uts.edu.au

[1] School of Computer Science, Centre for Artificial Intelligence, University of Technology Sydney, Broadway NSW 2007, Australia

1 Introduction

Technology is evolving rapidly, and devices become smaller and cheaper, not to mention the adaption of the always-connected model in toady's networks. This revolution makes every device able to communicate easily with each other and construct the future of the Internet. The new concept of the Internet future is known as the Internet of Things (IoT). IoT is an inter-network of numerous information-sensing objects and services such as infrared sensors, laser scanners, gas indicators, radio frequency identification devices (RFIDs), and global position systems (GPS) that can communicate and share information among themselves using the Internet as a backbone network [40]. These devices and gadgets have become well-connected to the Internet due to the drastic advancement in IP addressing schemes and reduced cost of micro-controllers and CPU power in the last few years. Nowadays, there are more than 20 billion devices connected to the Internet, and this number is expected to double in the next few years [20]. Meanwhile, IoT is not limited to household and everyday use applications. On the contrary, it spans a vast and diverse set of applications such as Smart Farming, Industrial automation, and smart metering. Today, IoT penetrating markets and industries that were never expected, from connected autonomous vehicles to smart cities. The demand for such technology is in its peak, causing manufacturers and IoT providers to rush product into the market to gain competitive advantage and security usually overlooked. As a result of such behavior, many IoT devices suffer from security flaws at different levels of implementation. The Mirai-bot that caused almost half of the Internet to break down was triggered due to inadequate security practice in these devices, causing one of the most significant DDoS attacks in the history of the Internet [32]. DDoS attacks are powerful attacks that can hinder the activities of the victim networkdevice, causing money waste, data, and sometimes even leads to higher risks in lives. Although, this sound on the extreme side of the problem, but from a security mindset it is possible to stop healthcare IoT system if such attack where triggered against hospitals and healthcare organizations. IoT devices and networks are prone to many types of attacks form message alteration and eavesdropping attacks to more complicated and sophisticated like the Sybil and node cloning attacks. Not to mention all of the security flaws extended from the classical Internet framework. Although some parts of the traditional network security model can be ported to the IoT ecosystems, many of the conventional security methods are not applicable in limited resources networks like the IoT. Due to the heterogeneous nature of such networks and the constraints and limitations associated with such devices, a new security model is crucial to tackles security issues at different levels of the IoT model. Undoubtedly, many other security issues and challenges exist, and before building a secure and robust IoT ecosystem, security-related questions such as the ones related to trust, privacy, confidentiality, and integrity must be answered. Therefore in this research, we aim to answer some of these questions and define existing attacks that affect the availability of the network, beside explore the existing countermeasures to counter such attacks.

The main contribution of this work can be summarized in threefold as follows: (a) we propose a comprehensive classification of the existing DDoS attack based on the existing literature; (b) we focus on the systematic approach used to extract all of the existing solutions for DDoS detection in IoT; (c) we report the limitations and weaknesses of the existing methods in the literature. We believe our work provides researchers and interested individuals with the stepping stone into understanding the full picture of the existing security issues in the IoT. The rest of the paper is organized as follows. Section 2 gives a brief overview of IoT and its associated security requirements. In Section 3, we shed light on the process used to conduct the research. Attacks categorization and definition are presented in Section 4. Comprehensive literature review and the limitation associated with it are presented in Section 5, While Section 6 discuses opportunities for further future research. Finally, Section 7 gives a clear conclusion of the study.

2 Background

IoT devices and platforms have been escalated over the last few years, and studies have shown that more than 20 billion devices will be connected to the Internet by the end of 2020. The unique aspect of the accelerated number of connected devices lies in the diversity of applications, ranging from a simple application like a coffee machine connected to the Internet to a very complicated mesh of sensors used for industrial purposes.

The accessibility and affordability of IoT devices do not come without consequences, security being one of the major challenges of such systems. Security suffers the most in this heterogeneous network of things, due to the lack of a standard architecture for the IoT network and devices, and the Different vendors have various architectures and protocols. Therefore, by trying to apply traditional security measurements, security will not deliver the expected result. Moreover, due to the constraints which are discussed in Section 5, conventional methods are not applicable due to their high computing needs and resource requirements. In this study, we focus on providing security solutions based on the systems that have been implemented in the context of IoT devices and networks.

2.1 Security requirements and goals

Different security protocols are required to achieve a solution. The most commonly used security and assurance model is the CIA triad model, which consists of three requirements:

1. **Confidentiality:** Ensuring sensitive data is protected from unauthorized entities either when the data is in transit or at rest. IoT devices can have sensitive applications, such as in the health care system, where personal information about the patient is critical and might be life-threatening. In such scenarios, confidentiality is crucial and must take it seriously.
2. **Integrity:** Data can be changed and altered when transmitted to the receiver, resulting in an unreliable service in the IoT system. Ensuring integrity between IoT devices is essential in most scenarios and applications. The alteration and modification of data while in transit can lead to serious negative implications, such as in the health sector where manipulating sensitive data, e.g. (blood pressure, heart rate, etc.), which are very sensitive data for both the patient and the doctor [1].
3. **Availability:** This is one of the most important security goals as it ensures that the IoT device is accessible at any time when needed. Attacks on availability, usually referred to as (DoS) attacks, are of great concern to any business or organization. Hence, it can deny access to devices and services, leading to great revenue losses from a business perspective. Therefore, IoT devices and networks must be robust and accessible, even when security threats and attacks are present.

These requirements, referred to as the CIA-triad, have been criticized in the literature as being insufficient against the new threats that emerge every day. To address these limitations, Abomhara et al. [1] proposed a new set of security requirements by analyzing and exploring a large set of security systems from the security assurance and requirement perspective. The study provided a new list of requirements called the IAS-octave. This list address adds the following five requirements to the CIA-triad:

4. **Audibility:** This is the process of ensuring that the system is monitoring all its services and actions comprehensively [1]. Audibility might not be applicable to all IoT applications, as it requires more computational resources and storage.
5. **Trustworthiness:** The ability of the system is to ensure the identity of the IoT devices and build trust between the system and third parties [1].
6. **Accountability:** Ensure that each entity in the IoT system is held responsible for its actions, which can prevent information misuse [1].
7. **Non-repudiation:** In some cases, the system is required to validate the occurrence of specific actions on a specific event [1]. In the IoT context, such property might not be considered important unless there is some kind of payment involved in the system [1].

In the remainder of this study, we use the IAS-octave model for security requirement evaluation.

2.2 Constraints and limitations:

Similar to other computer networks, IoT networks require various security protocols. However, the security measurements for IoT must meet certain criteria that might not apply to different networks due to its nature and resource constraints, which are listed as follows:

1. **Resource Limitations:** One of the challenges facing IoT devices is its limited resources such as CPU and memory, making it very difficult to implement a security solution that requires high processing capabilities. IoT devices are packed with minimal network protocols and minimal features that require less computing power to save energy and resources; therefore, implementing a complex and comprehensive security solution is a constant challenge for manufacturers and developers who need to minimize the number of features and design a simple yet efficient security solution.
2. **Privacy and Data Confidentiality:** In IoT, different applications have different privacy implications. The privacy level required for the healthcare application is different from the privacy level used for the city temperature sensors. This is not to say that we should neglect privacy concerns for some applications. On the contrary, we should harness security in IoT devices more where user privacy is involved. IoT devices have permeated to different aspects of lives such as smart vehicles and smart homes, which can provide sensitive user information like user location, health status, and user home preferences, all of which can raise serious privacy concerns. The key idea about privacy and confidentiality is that the data is kept private and only accessible to an authorized entity, which can be a human or machine. To achieve privacy and confidentiality, cryptography is mandatory and should be applied in a manner that does not affect the IoT devices' constraints and limitations.
3. **Authentication:** IoT devices generate a substantial amount of data every day. The data moving between entities must be securely transmitted, besides activating the data privacy authentication mechanism as a crucial process. Unfortunately, there are no common standards that are used by all vendors for authentication. Different vendors use different authentication protocols, which raise security concerns between different platforms since there is no standard method of authentication. Hence, the integration between these platforms is weak and can lead to security issues in the future [14].

4. **Service Availability:** Service availability on IoT networks is prone to many DoS attacks. Nodes can be compromised internally within the network or from outside intruders; this kind of attack can paralyze the whole IoT network and hinder all activities and services. Moreover, availability attacks usually try to consume all device resources, and since IoT devices in many cases are battery-powered, this might cause the device to drain all of its resources. To add more, ensuring the availability of a device or service is crucial since many applications are time and data-sensitive, such as in the healthcare system.
5. **Data Management Challenge:** IoT is all about data, and with the increases of data generated by sensors and devices, data centers face an architectural challenge in terms of how to cope with such data. Research has shown that the current data centers cannot handle such an increase in data [36]. IoT at the enterprise level generates a significant amount of big data that needs to be processed, analyzed, and stored in real-time, which in this case, will leave providers with security complications [51].

2.3 IoT stack

Different manufacturers have different architecture, and unfortunately, there is no standard architecture for IoT devices across different vendors. This research focuses on the three-layer architecture since it is the most common among researchers. Figure 1 shows the three

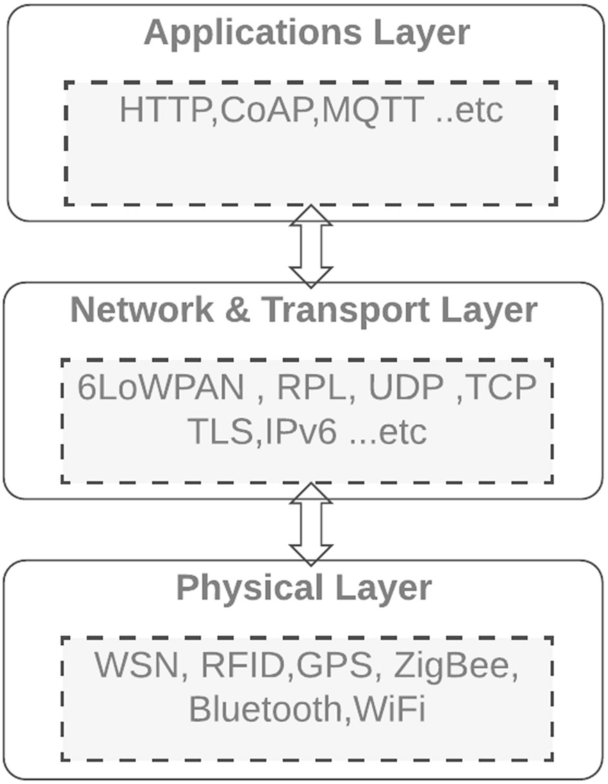

Figure 1 IoT three-layer architecture

layers with some examples of protocols at each level. Each layer is explained briefly as follows:

Physical layer This is responsible for data using sensors and actuators. This layer also takes the responsibility of handling node communication, including signal transmission and channel selection in wireless communication. Some examples of technologies that work in this layer are ZigBee, Bluetooth, and WiFi, 4G/LTE.

Network/adaptation layers This works as the middle-ware layer that exchanges data between the application layer and the physical layer. This layer also takes responsibility for routing the data between different nodes in the network. Moreover, when using the 6lowpan protocol, this layer maps the IPv6 address with the outside world. Some protocols that work ins this layer are RPL,6lowpan, IPv6, and TCP/UDP.

Application layer This is the high-level layer where data representation occurs and allows other protocols to access data in the IoT devices, such as HTTP COaP and MQTT. It is the interaction point between the user and the devices.

3 Research strategies

This study focuses on building a robust understanding of DDoS attacks in IoT, and explores the available solutions to counter such threats. We followed a systematic literature review process to build this comprehensive review.

Numerous review papers have been published in the area of IoT security; Therefore, we can form a general idea about the attacks that affect network availability and IoT devices. Table 1 shows the review papers that have been thoroughly investigated. Most of the studies have covered different aspects of IoT security, yet none specifically address DDoS attacks from the IoT perspective. Therefore, in this systematic literature review, we focus on building a knowledge base of DDoS attacks on IoT and their counter-measurement solution.

3.1 Keywords

We extracted the following relevant keywords as we are only focused on DoS and DDoS attacks. The attacks explored are further explained in Section 4 of this paper. To extract the relevant attacks related to our study, the following terms were extracted:

"IoT Security","DDoS attacks IoT","Selective Forwarding IoT" ,"Blackhole Attacks", "Jamming IoT", "6lowpan Attack","Flooding Attack".

3.2 Research questions

This study aims to answer the following research questions:

1. What attacks affect the IoT network and cause a denial of services/devices?
2. What are the solutions to counter such threats?
3. How does the proposed solution limit IoT devices, and what security goal does it address?
4. What solutions are mostly used to counter DDoS in IoT?
5. How can the available solutions be categorized?

Table 1 Survey paper comparison

Study	Attacks	Novel methods	IDS	Protocol	Trust	Authentication	DDoS specific	Multiple domain	Security goals	IoT architec-ture	Research method*
[21]	X	X	X	X	X	X	–	–	X	–	–
[33]	–	X	–	X	X	X	–	X	X	–	–
[63]	–	X	–	–	X	–	–	–	X	X	–
[38]	X	–	X	–	–	X	–	–	–	X	–
[53]	–	X	–	–	X	X	–	–	–	–	–
[43]	X	–	X	X	-	X	–	–	X	X	–
[54]	–	–	–	X	X	X	–	X	–	X	–
[12]	X	–	X	–	–	–	–	–	–	X	–
[37]	X	–	X	X	–	X	–	–	X	X	–
[5]	X	–	–	X	X	X	–	X	–	X	–

* - Research method criteria indicates whether the explored survey papers outlines precisely their research methodology they have followed. , **x** - yes , **-** no

Table 2 Databases

Database name	Address
IEEE	http://ieeexplore.ieee.org/
ACM	http://dl.acm.org/
Science Direct	http://www.sciencedirect.com/
Springer	http://link.springer.com/
Google Scholar	http://scholar.google.com/

3.3 Research filtration process

This section outlines our process for extracting relevant information to obtain data for our review framework. We have gone through the process of filtering the research found in the databases shown in Table 2, through these stages sequentially, as shown in Figure 2:

- The process starts by collecting the papers based on the defined keywords in Section 3.1 from different publishers and databases. Figure 3 shows the distribution of the databases.

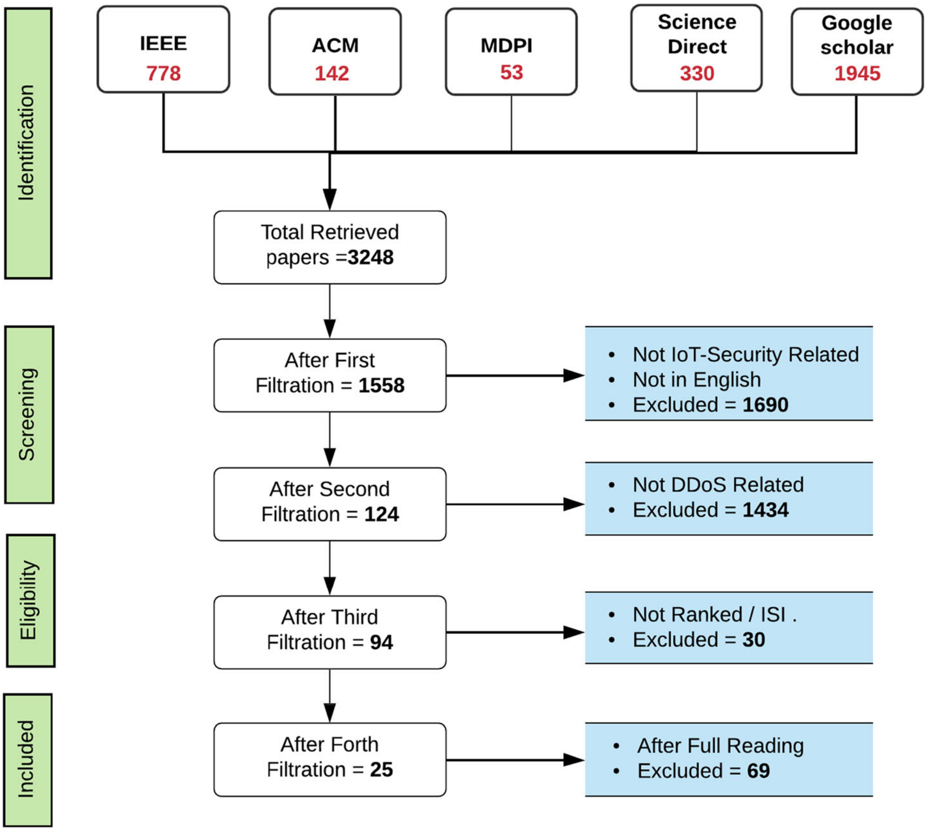

Figure 2 Literature review Filtration process

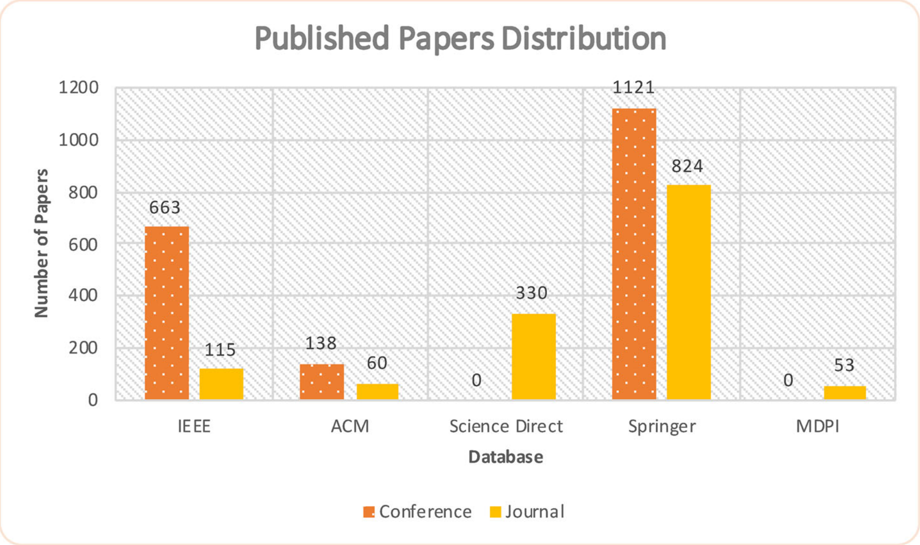

Figure 3 Paper distribution based on database

- The first filtration process is to filter the papers by reading the titles and excluding any paper that is not related to IoT security or is not published in English.
- The second stage of filtration is to filter any paper that is not related to IoT DDoS attacks. This process was done by reading the title and scanning the abstract if necessary.
- The third filtration stage is to verify that the filtered papers have been ranked or peer-reviewed. We used the CORE database provided by the Computing Research and Education Association of Australasia to check the conferences and journal ranking.
- The final stage is to read the papers in full and exclude any that are not specifically related to the domain of this research, which is DDoS attacks.

4 Security issues and attack classifications

In reviewing the literature, we identified the attacks responsible for DoS or DDoS attacks, both directly and indirectly. In this study, attack categorization is based on where the attack happens in the IoT three-layer architecture, which is highlighted in this section.

4.1 Perception layer attack

This layer is a low-level layer where data is acquired. Sometimes it is called the sensing layer since it acquires information from sensing devices such as RFID tags, sensors, or even GPS locations [68]. These devices are usually deployed in unmanned geographic locations where intruders obtaining physical access are not a challenge; therefore they are prone to security attacks as outlined in the following.

4.1.1 Jamming

Jamming attacks target the physical layer of the communication stack by interfering with network radio frequencies [28]. This kind of attack is carried out by occupying the same radio frequency channels in the network, which causes node frequency jamming [28]. This attack can be launched against the whole network, causing a large-scale DDoS, hence bringing the entire network down and disrupting all services provided by the network. Moreover, it can target specific network nodes by using a less powerful jamming source [8]. There are many countermeasures solutions against jamming attacks, and a typical defense mechanism is the frequency hopping spread spectrum (FHSS). FHSS is a technique used in signal transmitting by switching between different channels while transmitting. This technique prevents the attacker from knowing which channel is used for node communication.

4.1.2 Tampering

As previously mentioned, IoT devices sometimes are scattered in unmanned areas where devices are unattended; therefore, such devices are prone to tampering and modifications. An intruder can compromise a node by altering the programming code or injecting malicious code into it. The attacker can even go further and replace the entire node with another node created by the attacker, which later on can control it remotely and use it to launch different attacks like blackhole or selective forwarding attacks [8].

4.1.3 Battery exhaustion (Sleep deprivation)

Battery exhaustion can be achieved by varieties of attacks across the network stack. However, there is a common attack that targets the power saving mechanism in any node, which is called the sleep deprivation attack. It's launched by sending a useless control packet to the victim node, making it forget its sleep cycle until it exhausts and shuts down [7]. This attack is complicated to detect as it typically affects the normal procedure node executions (Table 3).

4.1.4 Unfairness

In IoT and WSN, there is a feature that allows nodes with low battery to have a higher priority in sending packets. Such feature can be misused by the intruder and impact battery health, through the process of making nodes with normal battery level sends priority messages, leading to unfairness in packet sending and disturb the network behavior [8].

4.1.5 Collision

Data collision occurs when two nodes transmit data at the same time when occupying the same channel [8]. A collision can alter part of the transmitted data, which can cause a checksum mismatch, causing the data to be invalid and ignored by the receiving node [65]. This can lead to the exhaustion of the node resource by forcing the node to retransmit data for every collided packet. Moreover, if this attack is launched on a large scale, it can lead to denial of service and exhaust the whole network [8].

Table 3 Attack summary

Attack	Effected Layer	Effect	Possible Solution	Effected SG
Jamming	PHY	Jamming wireless signal causing DOS	Frequency Hopping	A
Tampering	PHY	Code Modification Maliciously	Physical Security	ACI
Sleep deprivation	PHY	Exhaustion of battery power devices	Split Buffer Solution	A
Unfairness	PHY/MAC	Disturb priority packet sending	-	AI
Collision	PHY/MAC	Exhaustion of battery power devices	Authentication	AI
Buffer Reservation	ADP / 6LOWPAN	DOS using buffer reservation	split Buffer solution	AI
Selective Forwarding	NTW/RPL	DoS and disturbing Network Topology	Authentication, IDS	AIP
Blackhole	NTW/RPL	DoS and disturbing network topology	Authentication, IDS	A
Sinkhole	NTW/RPL	Disturbing network topology, Rank manipulation	Authentication, IDS,	AI
Sybil	NTW/RPL	Masquerading node Identity, compromise privacy	Unique Identifier , Authentication	AIP
Flooding	NTW,PHY,APP	Sending unlimited amount of packets	Authentication, IDS	A
Wormhole	NTW	Routing Distrust	Authentication, IDS	Ai
TCP Hijacking	APP	Stealing node identity using sequence number	Authentication, IDS	AI
6lowpan Fragmentation	ADP / 6lowpan	adding unknown fragment to packet structure	Authentication, IDS	AI

DD - DDoS attack, **Sh**-sinkhole attack, **SF**-Selective Forwarding , **BH**-Blackhole, **HF**-Hello Flood attack, **NTW/RPL** - Network Layer, **L**-Low,**M**-Medium , **H**-High, **D**-Distributed , **C**- Centralized, **U**-Undefined

4.2 Network

This layer of the IoT stack combines more than one feature including routing, adaption and fragmentation. Therefore, complex attacks can occur at this layer, from route manipulation to fragmentation, all of which can affect network resources availability. Attacks that affect network layer functionality are listed as follows:

4.2.1 Buffer reservation attack

This attack utilizes the fragmentation and reassembly functionality in the 6lowpan protocol. The core idea of this attack is to use a flaw in the buffer mechanism when handling fragmented packets. When the target node receives the first fragment of the packet, it reserves the entire buffer and waits for the other fragments to reassemble them. Attackers can utilize this flaw to send only one fragment and reserve the buffer for the maximum time allowed, which is defined by the 6lowpan protocol to around 60 seconds. Therefore, the intruder node can repeatedly send the first fragment to the receiving node and occupy the buffer for as long as it can, causing the victim node to be drained all of its resources [26].

4.2.2 Selective forwarding

This is one of the popular routing attacks which tries selectively to forward only very specific packets to the next node by dropping specific data of the packets. This attack can be extremely dangerous when it is combined with other attacks like the sinkhole attack, which can lead to DoS.

4.2.3 Blackhole

A blackhole attack is similar to a selective forwarding attack, but instead of forwarding specific packets, it actually drops all kinds of packets, coming from other nodes. This attack can disturb network topology by manipulating the ranking mechanism in the RPL protocol.

4.2.4 Sinkhole

In a sinkhole attack, the malicious node advertises itself as having a better rank than the parent nodes, causing the neighboring nodes to change their parent and alter the routing path. The nearby nodes change their route to the sink because of the better fake route provided by the malicious node. A sinkhole might not be effective when it is executed by itself, but it can be far more critical when it is combined with other attacks like the blackhole or selective forwarding attack.

4.2.5 Sybil

A Sybil attack is an attack on node identity. It can have many forms, but it is a common identity fabrication attack where the advisory node tries to advertise itself as a different node in the network by stealing or fabricating another node's identity.

4.2.6 Flooding

In a flooding attack, the attacker node sends an unlimited number of DIS messages to the victim node over a very short period of time, causing a dos attack and disabling the node services. This kind of attack can also lead to battery exhaustion due to consuming node resources.

4.2.7 Wormhole

A wormhole attack is a routing-based attack where the attacker uses one or more nodes to create a fake tunnel with a better rank than the normal route to the sink node. Therefore, instead of data transmitting through the legitimate node, it uses the fake tunnel to transmit data [6]. This attack can cause different kinds of disturbances to network communications, which include eavesdropping, selective dropping and DoS attack.

4.2.8 TCP Hijacking

The transport mechanism in IoT uses either UDP or TCP protocols to transport data to the application layer. When using the TCP protocol, it inherits all the available flaws and vulnerabilities, one of which is top session hijacking where the attacker tries to steal the client's identity because the attacker knows the sequence number and communication port [39]. Later, the attacker can launch DoS attacks on the victim and assume its identity to communicate with the server.

4.2.9 6lowpan fragmentation attack

In IoT, when using the IEEE 802.15.4 standard, the user is limited to an MTU of 127 bytes by using the 6LoWPAN fragmentation mechanism, which allows the transmission of IPv6/4 packets. The problem with 6loWPAN is that it does not provide any kind of authentication, which means an attacker can inject their own fragments among other fragments [48].

This next section of the research explores the available methods used to counter DDoS attacks in IoT.

5 Literature review

In examining the literature, this study has found the published studies can be categorized based on the type of solution proposed. Therefore, we divide the literature into four categories: intrusion detection system (IDS)-based solutions, protocol-based solutions, trust-based solutions and others.

5.1 Protocol-based solutions

Protocol-based solutions utilize the existing protocols to mitigate security flaws by enhancing the existing method or building new methods on top of the existing one. An example of such a solution is proposed in Glissa and Meddeb [19], which investigated the use of a chaining message authentication code and the advanced encryption standard to cipher the packet payload between entities. The authors termed this framework 6lowPSec, and it works under the MAC security sub-layer in the adaption layer. They evaluated the system against many attacks, one of which was denial-of-service attacks, as the authors stated the solution was able to counter such malicious activities. However, the performance of the system decreases when new nodes are added, causing the proposed model to take longer to process.

Wallgren et al. [64] presented a comprehensive analysis of IoT technologies and their new security capabilities that can be exploited by attackers. One of the highlights is the implementation and demonstration of well-known routing attacks against 6LoWPAN networks running RPL as a routing protocol, which they simulated using the Cooja simulator and the Contiki operating system. The following RPL attacks were used for testing: selective-forwarding attacks, sinkhole attacks, hello flood attacks and wormhole attacks. The testing results show that while the RPL protocol is vulnerable to different routing attacks, it has internal mechanisms to counter the hello flood attacks and mitigate the effects of sinkhole attacks. The authors claim to implement a solution that minimizes selective forwarding attacks by implementing a heartbeat protocol on top of the IPSEC function in the ipv6 protocol. The basic idea is to send ICMPv6 messages from the 6BR router to all nodes in the network and wait for the ICMPv6 echo reply from the nodes. This technique has been implemented such that it sends ICMPv6 messages in an interval time, hence it is called the heartbeat. The authors claim that this technique helps to identify which node has been filtered using the IPsec protocol, hence identifying any node which may have been the victim of the attack.

Bio-metrics play a major role in security, but few studies have focused on IoT applications. The work in Hossain et al. [23] presents four layers of bio-metric architecture to provide an end-to-end solution for secure communication. The proposed architecture focuses on authenticating communication by using bio-metric devices and pairing-based cryptography to secure the data in transit. The core idea is to use a three-level interaction between each layer to establish a communication channel between the layers. The system uses private key generator cryptography at each layer to ensure the secure transmission of biometric data. The authors claim that by encrypting the barometric data, the proposed protocol is resilient against masquerade and reply attacks. The problem with such a model is that it can introduce a communication overhead and heavy resource consumption on the end devices. Since bio-metric solutions have a large data footprint in comparison to other authentication solutions such as encryption, and solutions can be challenging for devices with limited resources.

Similarly Glissa and Meddeb [18] proposed a new security protocol to secure RPL networks and called it (SRPL). It uses a hash chaining authentication approach to validate the authenticity of each node. SRPL has three stages: the first stage is the initiation phase, where the node calculates the hash and the threshold values when the DODAG is created. The second stage is the verification stage, where parents check the validity of the child node by checking the hash and threshold values. The third stage is where the hash and threshold values are updated when any changes in the rank are signaled. To counter the selective forwarding attack Pu and Lim [49] proposed SCAD, a lightweight verification method that utilizes the map hash function that sends a frequent acknowledgment packet between the source node and the sink. To ensure secure communication between the source and destination, the author proposes placing a checkpoint node that piggybacks the connection packets with a unique random hashed number. This number serves as the ID between the checkpoint, source and destination nodes. Furthermore, to reduce packet delivery latency caused by the attack, the authors propose a timeout technique based on estimated single-hop transmissions. One of the limitations of this study is that it depends on a static link between nodes. However, in practical, real-world IoT scenarios, nodes change their communication link dynamically. Therefore, this method is not practical in dynamically changing topology.

A major challenge for the RPL protocol is countering insider attacks with limited resource devices. To enhance RPL resilience against attacks Heurtefeux et al. [22] introduced a new method that uses randomized route selection and data duplication techniques. Duplicating the data and sending them through randomized parent nodes ensures if one link is compromised, the data will reach the sink through the other randomized link. The author assumes the IoT network is dense and each node has multiple routing parents.

Another study that focuses on solving one limitation of the RPL protocol was proposed by Dvir and Buttyan [16] to address version number attack. The proposed method utilizes hash chains to authenticate the rank exchange between nodes. However, this method was later criticized by Perrey et al. [46] as it is still susceptible to forgery and reply attacks. Therefore Perrey et al. [46] proposed an enhancement to VeRA by using an encryption chain instead of a MaC hash chain. The encryption chain for every node is calculated by the root/sink node. Also, the authors proposed a new method called TRAIL to authenticate the topology in the network. This method is used to prevent topology inconsistency in RPL networks.

Another method that uses cryptography was proposed by Hossain et al. [24] to counter 6Lowpan fragmentation attack. Each joining node is assigned a temporary address by the border router (BR) and then selects its parent node based on its location in the network. To ensure safe communication, the method uses the ECQV implicit certificate-based cryptography which is computed by the BR and assigned an encrypted CGA-ipv6 address, dropping the temporary address. The new address is used as a secure channel between the nodes in the network. The method proposed by Gara et al. [17] is based on a statistical model where they use the sequential probability test [47] to estimate the dropped packet between the node and the sink. This is achieved by sending a hello packet using a dynamic adaptive threshold. If the dropped packet rate exceeds the predefined threshold, this indicates the node is malicious and will be blocked from the network. This method is used to detect a selective forwarding attack.

5.1.1 Protocol-based solutions discussion

In protocol-based solutions, few methods have explored the different aspects of integrating new protocols into the system. By thoroughly investigating the methods in the literature, we have defined the following limitations:

- **Cross-layer:** as can be seen from Table 4, only one study has designed a solution addressing multiple layers attacks on IoT architecture. The study proposed by Hossain et al. [23] used bio-metric solutions to provide a more secure architecture for data communication. However, the study fails to report the performance with respect to IoT limitations. The biometric data has a large footprint compared to encryption/authorization solutions. It might be more secure in terms of the uniqueness of biometric features, but we do not see this solution as feasible for constrained devices with the framework proposed. Other studies have not reported any cross-layer integration.
- **Evaluations:** most studies focus on simulation-based evaluation without introducing any real-world elements, such as noise and signal distribution objects, which can affect the result when deployed in real-world scenarios. The study proposed by Wallgren et al.

Table 4 Protocol-based solutions

Study	Attacks	Layer	Method	Performance	Placement	Description
[19]	SH,SF,BH,SY	NTWRPL	Authentication / Encryption	H	C	hash chaining authentication approach.
[64]	SF,SH,HF,WH,CID	NTWRPL	Specification	L	C	Lightweight Heartbeat, RBL & IDS
[23]	MQ,RP	Cross Layers	Bio-metric based Encryption /authentication	~M	C/D	Bio-metric Authetcation and encypayion.
[18]	*	NTWRPL	Authentication / Encryption		C	Hashing approach and private key
[49]	SF	NTWRPL	Authentication		C	Hashing and Map Function
[22]	SF,BH	NTWRPL	Data and route Duplication		C	data redundancy
[24]	FM	NTWRPL	Encryption		C	encrypted CGA-IPV6
[16]	FM	NTWRPL	Hashing		C	Hash chaining for secure RPL Rank
[46]	DI	NTWRPL	Encryption		C	encrypted chain

DD - DDoS attack, **Sh**-sinkhole attack, **SF**-Selective Forwarding , **BH**-Blackhole, **HF**-Hello Flood attack, **NTW/RPL** - Network Layer, **L**-Low,**M**-Medium , **H**-High, **D**-Distributed , **C**- Centralized, **U**-Undefined

[64] provides a comprehensive evaluation of the heartbeat protocol proposed, but does not report how such solutions will perform in real- world scenarios [52].

- **Heterogeneity:** from Table 4 we can see that none of the studies addresses the heterogeneous nature of the IoT network, although the architecture bio-metric proposed by Hossain et al. [23] is a cross-layer solution but the authors do not explore the idea of supporting multiple technologies to address heterogeneity problems.

5.2 Trust-based solution

IoT devices and networks are designed to create business value by connecting different kinds of devices and objects, no matter what resources are available in the end devices. This is why many devices with low memory and computing power are a part of this ecosystem. Therefore, when designing any trust management system (TMS), constraints and limitations related to such an ecosystem should be taken into consideration.

Many architectures for trust management are available in the literature. In this survey, we focus on the trust architecture that is based on a three-layer architecture [4].

The trust-based mechanism proposed by Khan and Herrmann [31] is based on a trust value calculated using the subjective logic approach by Jøsang [29] and is evaluated using the opinion triangle (OP). OP evaluates trust-based approaches on three attributes: trust, distrust, and uncertainty. In contrast to the traditional method where only two attributes are considered, this method explores the grey area where further analysis is required by using uncertainty attributes. To calculate trust, the authors assume the node is in a promiscuous mode which allows them to hear a neighbour's node traffic. If the trust value of the neighbour's node is low, this means that the node is distrustful and the monitoring node will prohibit data from being transmitted through it. The authors suggested using this technique to counter the selective forwarding attack, sinkhole attack, and version number attack.

The work done by Airehrour et al. [3] focuses on a trust-based solution to counter a blackhole attack in RPL networks. Essentially, a trust value for each node is calculated based on the number of packets sent and delivered through the parent node. The proposed mechanism also calculates what is called the feedback value between nodes, which is the ratio of packets a node is able to successfully forward. Utilizing the feedback value, a blackhole attacker can be detected by monitoring the number of packets it dropped, hence giving a low feedback value. The proposed model has two assumptions: the first is every node in the network will be able to overhear their neighbour's nodes and the transmitted packets. The second assumption is that the blackhole attacker will start dropping every packet it receives over time. This approach has some limitations, as it does not mention how the trust value is utilized to prevent a blackhole attack. Secondly, it assumes that all of the nodes are in promiscuous mode, which can minimize the lifespan of battery-powered devices.

Another study that utilizes the use of promiscuous nodes to detect blackhole attack is proposed by Ahmed and Ko [2]. This technique utilizes the promiscuous nature of nodes to overhear the neighbour's node traffic and determine if the node is misbehaving or not. A local decision process uses a specific threshold to determine if any node is suspicious or not. To further investigate the suspicious node, a verification process is called, which uses two types of messages: the received Request (RREQ) and the received Result(RRES) messages. The RREQ initiated by the verification node and it carries a request asking the root node if the forwarding packet was received or not. The RREQ messages are sent through an alternative path so that it will not be affected by the attacker node.

The root then will send RRES, which refers to whether the forwarding message was received or not. If the message was not received, the attacker node will be flagged to the blacklist and broadcast to the whole network to avoid the attacker node.

In this study, the author fails to mention how to calculate the misbehaving node, and there is not enough information about the misbehaving threshold. Moreover, the study does not mention what happens if there is no alternative route to the root node.

A study that tries to solve the problem of IoT heterogeneity was proposed by Alaba et al. [5]. The authors proposed a context-aware trust management system that uses a dynamic trust score based on the node context and its status and proposes the use of different trust calculating functions for different node services. The centralized design of the system may help in reducing network overhead but can lead to a single point of failure if the system fails. However, the author does not explain how the system will scale in a large dense network [13].

5.2.1 Trust based solution discussion

Based on the aforementioned studies, Table 5 provides a comprehensive summary of the explored trust studies. As can be seen, most of the studies affect the network layer, which is referred to as communication trust in the trust management framework. The observation in this context is that the trust evaluation schema in each study is limited, but most of the studies fail to address the limitations associated with IoT devices.

IoT limitations Although some of the proposed solutions achieve a good results in terms of trustworthiness and accuracy, they fail to adapt to IoT limitations and constraints, since these solutions require an extensive amount of CPU and memory power which is not applicable in the context of limited resource devices. At a glance these studies by Medjek [41] and Zheng et al. [68] appear to have good results in terms of trust accuracy; however, they fail to report the system solution from the IoT device's perspective.

Cross layer As can be seen in the summary table, most of the studies focus on communication layer trust-based solutions and ignore multiple-layer adaptation. All of the studies reviewed focus on one-layer solution and ignore the trust issues that appear at a different layer of the ecosystem. Designing a cross-layer solution is crucial to handle security breaches at a different layer of the IoT architecture.

This shows that the literature still lacks a reliable and scalable trust management framework that can take into account the limitations associated with IoT networks.

Evaluation The studies focused mostly on simulation-based evaluation without taking into consideration real-world elements, such as noise which is usually an essential factor when deploying a solution in the real world.

5.3 Intrusion detection based solutions

The intrusion detection system (IDS) has been used for sometime in different network applications. The main purpose of IDSs is to detect any suspicious activity against the targeted network. There are various approaches in IDS systems, which can be classified into four categories:

Table 5 Trust-based solutions summary

Study	Targeted attacks	Layers	Trust measurement method	Evaluation		Placement	Info collection	
				Performance	Scalability		Indirect	Direct
[11]	SH	NTW/RPL	Trust-based	–	–	H/N	–	x
[31]	SF,SH,VN	NTW/RPL	Trust Value	–	x	H	–	–
[3]	BH	NTW/RPL	Trust	x	–	H/N	x	x
[41]	SY	NTW/RPL	Trust Based -IDS	–	–	H/N	–	x
[2]	SD	NTW/Any	Message based	x	x	H/N	–	–
[5]	SD	NTW/Any	Message based	x	x	H/N	–	–

DD - DDoS , **Sh**-sinkhole , **SF**-Selective Forwarding , **BH**-Blackhole, **HF**-Hello Flood, **NTW/RPL** - Network Layer, **L**-Low,**M**-Medium , **H**-High, **D**- Distributed , **C**-Centralized, **U**-Undefined

- Signature-based approach: The system detects an attack by comparing the signature of the activity against a pre-installed set of signatures in the IDS database. If there is a mismatch in the signature, the system raises the alarm.
- Anomaly-based approach: In this approach, the IDS is trained to detect any anomalies in the network by analysing their behavior and if any activity exceeds a specific threshold, this indicates that an attack has happened.
- Specification-based approach: In a specification-based approach, the IDS checks network activity against a set of predefined rules and settings. This approach detects misbehaving intruders when their activity does not have the same specification as defined in the system. This approach is sometimes called the rule-based approach.
- Hybrid-based approach: This approach combines more than one approach to maximise the advantages of each and minimize the drawbacks.

A good example of a signature-based IDS is the architecture proposed by Kasinathan et al. [30]. It integrates an IDS into a network that has been developed within the EU FP7 project Ebbits. The goal of this proposed architecture is to detect threats on a 6LoWPAN network. The authors studied and analyzed DOS attacks in IP-based WSNs and proposed a solution involving a signature-based IDS that uses a predefined source of signatures and patterns collected prior to implementing the solution. The authors used probes in the edge of the network to sniff packets that go through the entire network and analyse each packet to look for any suspicious behavior, which is later on sent to SenacIntrture IDS for further analysis.

Likewise, Lee and Lee [36] uses the same approach, which is dependent on the specification-based approach, but the main focus of their study is to build an IDS that addresses routing attacks in an RPL network using a semi-auto profiling technique. This technique was used to gather and formulate a set of rules that is integrated into the IDS agent. The placement of the IDS was chosen carefully by the authors to eliminate any kind of network resource overuse. Therefore, they placed the IDS as a cluster head agent as they assume the network is a cluster-based network.

Raza et al. [50] uses a hybrid technology combining the signature-based approach and anomaly-detection approach. This approach utilizes the limited resources consumption of the signature-based approach and when combined with the accuracy of the anomaly detection technique, it produces better results. The basic idea of Svelte is to implement the IDS in a distributed approach, which is later installed across every node and is also implemented in the 6BR router. To fix network inconsistency, the authors developed a 6Mapper on top of the RPL protocol. The main function of the 6Mapper is to fix the network inconsistency caused by either hackers from within the network who send incorrect information to its neighbours, or due to the loss nature of an IoT network which can cause inconsistency. Raza et al. [50] used the Contiki OS RPL implementation to develop the 6Mapper on top of the system.

In addition to the 6Mapper, the authors developed a mini- firewall to detect any global attacks coming from outside by distributing the mini firewall across all the constrained nodes in the network, with the main module installed in the 6BR router. The authors claim that this helps minimize the overhead in the network.

La et al. [34] proposed a monitoring tool for attack inspection and detection which uses a deep packet inspection approach to investigate network traffic and identifies any misbehavior based on a set of rules defined in an XML file.

In the method proposed by Yaseen et al. [66], fog computing is used to counter selective forwarding attacks in sensing networks. The core idea is to build an intrusion detection system in fog computers at the edge of the network. The author proposed the use of watch-dog nodes that monitor any suspicious node while on the move. The watch-dog nodes maintain the received packet and the sent packet by the monitored node. These values are forwarded to the fog node for further processing, where the fog node decides whether the monitored node is malicious or not, based on a specific threshold. Unfortunately, the authors do not mention how to calculate the threshold and the study lacks details about the approach.

The “Kalis” IDS architecture proposed by Midi et al. [42] utilizes a knowledge-driven intrusion detection system to counter hello flood and smurf attacks, where the IDS observes the network traffic to extract specific features and feeds them to what is called knowledge-base storage. Using the knowledge gained about the specific node, the system identifies the malicious node and triggers the specific detection mechanism. However, the study does not explore how the feature process is executed and what kind of features are collected for the knowledge base database.

Another hybrid method that uses an anomaly and specification detection mechanism is proposed by Bostani and Sheikhan [9]. The placement of this IDS is distributed between the router and the sink node in the network, where the specification-based agent works as a general inspection tool for all of the nodes in the network. In case of a suspected attack, the router forwards this information to the sink node for further processing. Using anomaly-based detection, the root node extracts specific features from the communication data and analyzes them for any malicious activity. The process is then passed to a voting system that learns by analyzing the network behaviors. This IDS is used to counter selective forwarding and sinkhole attack.

5.3.1 Intrusion detection based solutions discussion

Based on the aforementioned literature in the context of IDSs in IoT, the following observations can be made:

IDS methods Although there are variations of IDS placement choice in the literature, most of it does not identify both the negative and positive sides behind choosing such placements. The hybrid method has shown good results when it comes to attack accuracy and fast response, but none of the studies have thoroughly investigated the scalability and performance of such methods in real-world scenarios. By examining the literature, we find that the only hybrid IDS that provides enough details for an evaluation and testing scenario is the one proposed by Raza et al. [50] as it tries to address the limitations introduced by specification and anomaly detection when they work separately. One weakness of the proposed system as a result of not disclosing any details on how the system will evaluate a different kind of attacks or protocols, and although the author claims there is a possibility of expanding the system, no detailed information is provided.

IDS placement There are three types of IDS placements: distributed, where the IDS is installed across the network; centralized, where all data processing and attack detection happens on a single node that has more resources the other nodes in the network, and hybrid, where it tries to overcome the limitations of the centralized and distributed approach by organizing the network into a group of clusters. Each cluster has a root node that interacts with the main IDS component, which is usually installed in the 6br router. Although there are a variety of placement strategies, most of these studies fail to point out the performance trade-off of each placement. Cervantes et al. [11] presented how distributed placement methods can help detect sinkhole attacks more efficiently, but the authors offer no details about how the placement of the IDS helps in achieving good results in attack detection.

IDS heterogeneity problem In the literature, most of the studies discussed the 6lowpand protocol and building an IDS on top of the 6lowpan protocols is often proposed. This can be easily explained due to the standardization by the ITTF organization, where the 6lowpan and the RPL protocol is adopted by most IoT manufacturing companies. A problem arises when the IoT network is combined with different kinds of protocols and technologies like the Z-Wave, zEEgbee and BLE, as this can cause a miscommunication problem that needs to be addressed when designing any IDS. The heterogeneity nature of IoT networks allows different manufacturers and organizations to form the IoT network; therefore, designing a solution that takes this aspect into consideration is crucial.

IDS targeted attacks None of the explored studies focus on realizing the concept of attack detection. Most of the studies concentrate on very specific attacks like blackhole attacks or sinkhole attacks, however, most of these attacks can be combined to have a more disastrous effect. None of the studies explored in this literature review investigated the idea of integrated attacks that work collectively to maliciously affect the system. Another limitation observed in the literature is the limited number of studies that focus on physical and application-layer attacks. The majority of the studies retrieved focused more on attacks on the network and adaptation layer. A cross-layer solution will help address this limitation.

IDS dataset limitations As can be seen from the summary presented in Table 6, all of the studies used the DARPA, and KDD datasets to evaluate and test the proposed solutions. The limitations of the DArapa and the kdd datasets, namely their biased nature there are many duplicated records, outdated, and are not designed specifically for use in IoT networks. Moreover, these datasets use a totally different set of protocols and attack emulation that are not supported by most IoT network architectures.

5.4 Other solutions

Shrivastava et al. [56] proposed a technique that combines the return-oriented programming ROP approach with code checking to provide extra security against malicious code tampering in IoT devices. It aims to protect the most critical part of the code by including a two-level module (ROP and Checksumming) in the tamper resistance section of the program. Such a technique adds an extra level of difficulty in terms of a tampering attack since the attacker has to bypass two modules to establish a successful attack, therefore increasing the cost of exploitation. This approach has some limitations from the user access perspective, although the authors stated no additional performance is compromised when using these techniques. The authors do not state how the approach will affect battery-powered devices (since most IoT devices are battery powered).

Another method that utilizes the use of the ROP technique is presented by Hota et al. [25]. The authors proposed a model that assumes a hostile user has access privileges to control the entire run environment of the program. The proposed model uses the Genetic Algorithm to choose the best devices with the minimum execution time to optimize the ROP chain.

Namvar et al. [44] introduced an anti-jamming approach for OFDM-based IoT devices by utilizing a game-theory technique. The proposed approach uses the Colonel Blotto game to establish an interaction between the jammer and the IoT controller. The IoT controller defends the network against jamming attacks by intelligently distributing the attack power across sub-carriers, which causes the bit error rate (BER) to decrease, therefore reducing the effect of the attack. The authors demonstrate the effectiveness of such an approach in maintaining healthy network performance and a good BER through simulation.

Table 6 Intrusion detection solution summary

Study	Attacks	Layer	Method	Performance	Placement	Brief	Dataset
[30]	DD	NTW/RPL	Signature-based	L	D	Complicated DOS attacks,	KDD
[61]	SH	NTW/RPL	Specification	L	C	Leader Node Selection,	KDD
[35]	SH	NTW/RPL	Specification	L	C	semi-auto profiling technique	KDD
[50]	SH,SF,BH	NTW/RPL	Hybrid(Specification / Signature)	L	C	Fixing network inconsistency	KDD
[34]	SF	NTW/RPL	IDS	M	D	Deep packet Inspection , Misbehavior	KDD
[67]	SF	NTW/RPL	Anomaly	M	D	Anomaly Based solution	KDD
[55]	HF,SY	NTW/RPL	Encryption	U	D	two ray prorogation model	KDD
[57]	DD	NTW/RPL	Specification	L	D	Identify DDoS attacks before targeting network,	KDD
[42]	HF,SM	NTW/RPL	IDS	*	D	knowledge-drive IDS	KDD
[27]	HF,BH	NTW/RPL	Authentication	U	D	Signature-based	KDD
[58]	SH	NTWr/RPL	Packet Inspection	H	D	Based on IR value, packet Received , Packet Sent	KDD
[9]	SH,SF	NTWr/RPL	Specification& Anomaly H	D	packet Received , Packet Sent	-	

DD - DDoS , **Sh**-sinkhole , **SF**-Selective Forwarding , **BH**-Blackhole, **HF**-Hello Flood , **NTW/RPL** - Network Layer, **L**-Low,**M**-Medium , **H**-High, **D**- Distributed , **C**-Centralized, **U**-Undefined

Similarly, Tang et al. [62] explored the hierarchical security game approach to form a competitive relationship that tricks the jammer into taking action after the legitimate node start transmission, a to stop what is called reactive jamming. By utilizing such techniques, the study forces the victim node to take action first, hence minimizing the effect of the jamming attack. To achieve this level of protection, the authors suggest that the legitimate user determines its transmitting power (since the attacker uses the transmitting power to launch the attack) to trade-off between the signal-to-noise ratio and the probability of being detected and jammed.

5.4.1 Other solutions discussion

The method proposed in this section varies between detecting tampering and jamming attacks. Although some might consider these attacks outside the scope of this survey, we have found that these attacks can serve as the starting point to launch complicated attacks that affect the availability of the network. The study by Shrivastava et al. [56] uses the ROP code checksumming method to protect IoT devices from code tampering. However, the study does not mention how to implement this solution on different platforms to adapt to the heterogeneity of the IoT network. Another study that uses the ROP method the one was proposed by Hota et al. [25], but it might not be applicable to many IoT architectures since it assumes the user has access permission to control the entire run environment. This can limit the application of such techniques.

6 Comprehensive discussion

After examining the literature, we have created a comprehensive table examining each proposed solution, and their limitations and the following issues are identified:

- **Limited evaluation parameters:** As can be seen from Table 7, only a limited number of studies cover the four aspects of the evaluation process. When designing any solution for IoT, it is important to take these parameters into consideration. For example, network overhead can cause the system to drain the energy resources of the IoT device. Therefore, analyzing every aspect of the system from the perspective of energy, computing, and network resources is essential when designing a security solution for IoT. Although some studies have good accuracy in terms of their attack detection results, they have failed to report the performance evaluation from resource perspectives, such as the solution proposed by Raza et al. [50] and the solution proposed by Hota et al. [25].
- **Scalability :** Scalability is crucial when it comes to measuring how the new system is performing in a large dynamic network, where nodes frequently join and leave the network. To minimize performance degradation when new nodes are added to the network and to increase the scalability of the system, several studies show that grouping nodes into clusters can help in some scenarios [60]. To address the scalability issues, Midi et al. [42] proposed the addition of new IDS nodes across the network. The larger the network, the more IDS nodes the network will require. Unfortunately, most of the studies in this survey do not explain how their system scales when a large number of nodes are introduced to the network.
- **Heterogeneity** IoT networks are different from the others because of the heterogeneous nature of the network. IoT networks comprise different devices from different

Table 7 Overview of IoT solution

Study	Solution	Attacks	Performance				Evaluation		Scalability	Heterogeneity	New Data	Attacks	IoT
			E	C	N	M	S	R					
[19]	Protocol	SH,SF,BH,SY	x	x		–	x	-	x	-	-	-	-
[64]	Protocol	SF,SH,HF,WH,CID	x	x	–	–	–	–	x	–	–	x	–
[23]	Protocol	MQ,RP	–	–		–	–	x	–	x	x	x	–
[18]	Protocol	DD	–	–	–	–	–	–	–	–	–	–	
[49]	Protocol	SF	–	–	–	–	–	–		–	–	–	–
[22]	Protocol	MQ,RP	–	–		–	–	x	–	x	x	x	–
[24]	Protocol	FM	–	–		–	–	x	–	x	x	x	–
[17]	Protocol	SF	–	–		–	–	x	–	x	–	–	–
[16]	Protocol	VN	–	–		–	–	x	–	x	–	–	–
[46]	Protocol	VN,DI	–	–		–	–	x–	–	x	–	–	–
[3]	Trust	SH	–	–	x	–	–	–	x	–	x	–	–
[31]	Trust	SD	–	–		–	–	–	x	–	–	x	x
[2]	Trust	SD	x	x	x	x	–	–	x	–	x	–	x
[5]	Trust	*	x	x	x	x	–	–	x	–	x	–	x
[30]	IDS	DD,UDP flooding	–	–	x	–	–	x	–	–	–	–	–
[35]	IDS	SH	x	–	–	–	–	–	x	–	x	–	x
[50]	IDS	SH,SF,BH	x	–	x	x	x	–	x	–	–	–	x
[34]	IDS	*	–	–	x	–	–	–	x	–	x	–	–
[66]	IDS	SF	–	x	x	–	–	–	x	–	–	–	–
[42]	IDS	HF,SM	–	x	–	x	–	x	–	–	x	–	–
[58]	IDS	SH,SF	–	–	–	–	–	–	–	–	–	–	–

Table 7 (continued)

Study	Solution	Attacks	Performance				Evaluation		Scalability	Heterogeneity	New Data	Attacks	IoT
			E	C	N	M	S	R					
[9]	IDS	SH,SF	–	–	–	–	–	–	–	–	–	–	–
[44]	Other	JM	x	x	–	–	x	2	–	x	–	–	–
[56]	Other	JM	–	x	–	–	–	2	–	–	–	–	–
[62]	Other	TM	–	–	–	–	–	–	x	–	–	–	–
[25]	Other	TM	–	x	–	–	–	–	–	–	–	–	–

- Unsupported , **x** - Supported, **E**-Energy, **C**-cpu , **N**-Network , **M**-Memory , **S**-Simulation , **R**-Real-world Scenario , **DD** - DDoS , **Sh**-sinkhole , **SF**-Selective Forwarding , **BH**-Blackhole , **HF**-Hello Flood ,**DI**-DoDAG inconsistency , **SD**-Sleep Deprivation , **CID** -Clone ID , **MQ**-Masquerade , **WH**-Wormhole , **SM**-Smurf , **VN**-Version Number , **JM**- Jamming , **TM** -Tampering , **P**- Partially manufacturers running various applications and operating systems. Under this level of complexity, the security solutions should be interoperable in such ecosystems. The study by Hossain et al. [23] addresses this issue. However, limited information exists on how the system functions under different environments. Other studies reviewed in this paper do not address this issue, whereas most of the proposed systems focus on a very specific set of protocols and environments.

- **Datasets** Anomaly detection IDS requires a good dataset to produce a good unbiased result in the training and testing phase. Therefore, choosing the right dataset for the system is crucial. Hossain et al. [23] and Mahmoud et al. [40] used the KDD dataset [59]; however, as discussed in Section 5.3, it is an outdated dataset and has been criticized on many occasions [10, 15, 45]. Furthermore, the KDD and DArapa datasets were created in a very different environment and with different protocols to those used in IoT networks today. Therefore, building a dataset that uses appropriate protocols and architecture is a vital element in building a reliable framework for any anomaly detection solution. A common protocol used in the IoT network is RPL for routing, 6lowpan for adaption, and MQTT and COAP for a top-layer application interface. Hence, creating a dataset with these protocols is crucial to produce an accurate and relevant result.
- **Multi layer solution** Another critical observation from Table 7 is that limited studies focus on building a solution that covers more than one layer of the IoT architecture. The only study that proposed a multi-layer solution is the one proposed by Hossain et al. [23], where the authors use a biometric solution on a different layer. Although, in theory, this can increase attack prevention, it is not practical due to the network overhead and performance. Most solutions focus on network and topology layer attacks, such as sinkhole and blackhole attacks, as can be seen in Figure 4. Where the solution distribution shows, the majority of research focused on network and physical layer, with less research conducted on top layer attacks such as COAP and MQTT-related denial-of-services attacks. Therefore, there a huge research opportunity in this specific area.

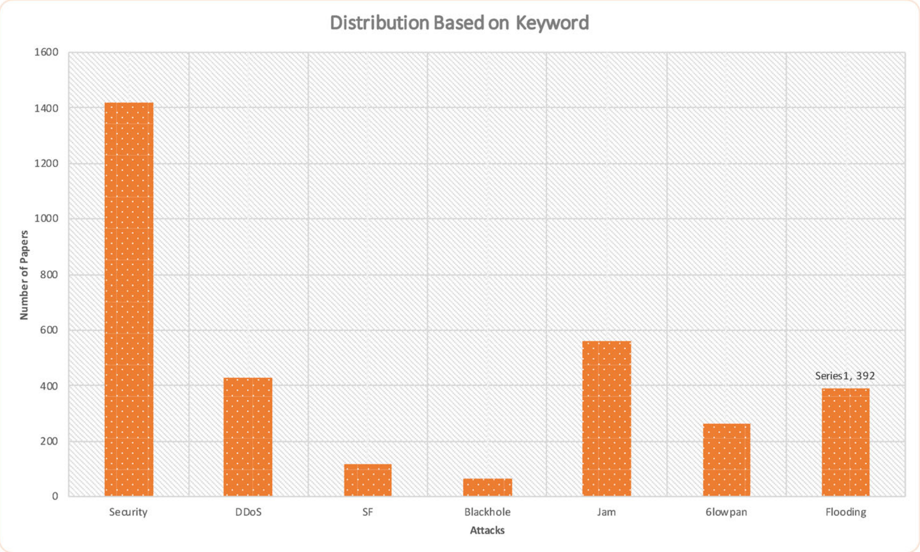

Figure 4 Paper distribution based on keywords

6.1 Trends and future directions

Due to the heterogenetic nature of IoT and other reasons, there are still some challenges that need to be addressed from a security point of view. In this section, the study focuses on some of the hot trends in the security area that can help to provide solutions for IoT. AI has significant momentum in the research community across different applications, as AI and machine learning have shown promising results in security applications across a broad spectrum of applications. Although there are some applications in IoT and big data analytics for either data extraction and data forecasting, there is a limited application in the context of IoT security, specifically utilizing AI and machine learning for attack detection. Therefore, there is a crucial need for AI applications that focus on attack detection and have the ability to adapt to new attacks that emerge every day. Another hot research area that can provide solutions to the constrained nature of IoT network is fog computing. If integrated with the IoT network and AI solutions, this can revolutionize the way we look at the IoT network since the nature of an AI solution is resource hungry and cannot be adapted directly to IoT devices due to resource constraints. Therefore, moving heavy computational tasks to the edge of the network will solve many issues with the current security models that require high computational power and an extensive amount of resources.

7 Conclusion

Security is a key element in determining how IoT networks and devices will help shape our future. One of IoT's biggest security challenges is how to detect DDoS attacks without compromising the limitations associated with IoT devices. This systematic literature review has presented a comprehensive survey of the current DDoS attack detection approach and identified the attacks associated with DDoS that affect the availability of the network. In addition to exploring the limitations associated with the detection approach, the study identifies aspects that should be taken into consideration when designing IoT security solutions. Finally, the study evaluates the proposed solutions to DDOS attacks in terms of practicality in real-world scenarios.

Acknowledgments This work was supported by the University of Technology Sydney and the Centre for Artificial Intelligence in UTS. The authors are thankful for the funding entities.

References

1. Abomhara, M. et al.: Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J. Cyber. Secur. Mob. **4**(1), 65–88 (2015)
2. Ahmed, F., Ko, Y.-B.: Mitigation of black hole attacks in routing protocol for low power and lossy networks. Secur. Commun. Netw. **9**(18), 5143–5154 (2016)
3. Airehrour, D., Gutierrez, J., Ray, S.K.: A lightweight trust design for iot routing. In: 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 552–557. IEEE (2016)
4. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutorials **17**(4), 2347–2376 (2015)
5. Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F.: Internet of things security: A survey. J. Netw. Comput. Appl. **88**, 10–28 (2017)

6. Amish, P., Vaghela, V.B.: Detection and prevention of wormhole attack in wireless sensor network using aomdv protocol. Procedia Comput. Sci. **79**, 700–707 (2016)
7. Bhattasali, T., Chaki, R., Sanyal, S.: Sleep deprivation attack detection in wireless sensor network. arXiv:1203.0231 (2012)
8. Borgohain, T., Kumar, U., Sanyal, S.: Survey of security and privacy issues of internet of things. arXiv:1501.02211 (2015)
9. Bostani, H., Sheikhan, M.: Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach. Comput. Commun. **98**, 52–71 (2017)
10. Brown, C., Cowperthwaite, A., Hijazi, A., Somayaji, A.: Analysis of the 1999 darpa/lincoln laboratory ids evaluation data with netadhict. In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1–7. IEEE (2009)
11. Cervantes, C., Poplade, D., Nogueira, M., Santos, A.: Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606–611. IEEE (2015)
12. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P.: Network intrusion detection for iot security based on learning techniques. IEEE Communications Surveys & Tutorials (2019)
13. Chen, R., Bao, F., Guo, J.: Trust-based service management for social internet of things systems. IEEE Trans. Depend. Sec. Comput. **13**(6), 684–696 (2015)
14. Conti, M., Dehghantanha, A., Franke, K., Watson, S.: Internet of things security and forensics: Challenges and opportunities. Elsevier (2018)
15. Creech, G., Hu, J.: Generation of a new ids test dataset: Time to retire the kdd collection. In: 2013 IEEE Wireless Communications and Networking Conference (WCNC), pp. 4487–4492. IEEE (2013)
16. Dvir, A., Buttyan, L., et al.: Vera-version number and rank authentication in rpl. In: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 709–714. IEEE (2011)
17. Gara, F., Saad, L.B., Ayed, R.B.: An intrusion detection system for selective forwarding attack in ipv6-based mobile wsns. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 276–281. IEEE (2017)
18. Glissa, G., Meddeb, A.: 6lowpan multi-layered security protocol based on ieee 802.15. 4 security features. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 264–269. IEEE (2017)
19. Glissa, G., Meddeb, A.: 6lowpsec: An end-to-end security protocol for 6lowpan. Ad Hoc Netw. **82**, 100–112 (2019)
20. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (iot): A vision, architectural elements, and future directions. Fut. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
21. Hassan, W.H. et al.: Current research on internet of things (iot) security: A survey. Comput. Netw. **148**, 283–294 (2019)
22. Heurtefeux, K., Erdene-Ochir, O., Mohsin, N., Menouar, H.: Enhancing rpl resilience against routing layer insider attacks. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, pp. 802–807. IEEE (2015)
23. Hossain, M.S., Muhammad, G., Rahman, S.M.M., Abdul, W., Alelaiwi, A., Alamri, A.: Toward end-to-end biomet rics-based security for iot infrastructure. IEEE Wirel. Commun. **23**(5), 44–51 (2016)
24. Hossain, M., Karim, Y., Hasan, R.: Secupan: A security scheme to mitigate fragmentation-based network attacks in 6lowpan. In: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, pp. 307–318. ACM (2018)
25. Hota, C., Shrivastava, R.K., Shipra, S.: Tamper-resistant code using optimal rop gadgets for iot devices. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 570–575. IEEE (2017)
26. Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., Wehrle, K.: 6lowpan fragmentation attacks and mitigation mechanisms. In: Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, pp. 55–66. ACM (2013)
27. Ioulianou, P., Vasilakis, V., Moscholios, I., Logothetis, M.: A signature-based intrusion detection system for the internet of things. Information and Communication Technology Form (2018)
28. Jan, M.A., Khan, M.: Denial of service attacks and their countermeasures in wsn. IRACST–Int. J. Comput. Netw. Wirel. Commun. (IJCNWC) **3** (2013)
29. Jøsang, A.: A logic for uncertain probabilities. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. **9**(3), 279–311 (June 2001). https://doi.org/10.1142/S0218488501000831
30. Kasinathan, P., Pastrone, C., Spirito, M.A., Vinkovits, M.: Denial-of-service detection in 6lowpan based internet of things. In: 2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob), pp. 600–607. IEEE (2013)

31. Khan, Z.A., Herrmann, P.: A trust based distributed intrusion detection mechanism for internet of things. In: 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), pp. 1169–1176. IEEE (2017)
32. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: Ddos in the iot: Mirai and other botnets. Computer **50**(7), 80–84 (2017)
33. Kouicem, D.E., Bouabdallah, A., Lakhlef, H.: Internet of things security: A top-down survey. Comput. Netw. **141**, 199–221 (2018)
34. La, V.H., Fuentes, R., Cavalli, A.R.: A novel monitoring solution for 6lowpan-based wireless sensor networks. In: 2016 22nd Asia-Pacific Conference on Communications (APCC), pp. 230–237. IEEE (2016)
35. Le, A., Loo, J., Chai, K., Aiash, M.: A specification-based ids for detecting attacks on rpl-based network topology. Information **7**(2), 25 (2016)
36. Lee, I., Lee, K.: The internet of things (iot): Applications, investments, and challenges for enterprises. Bus. Horiz. **58**(4), 431–440 (2015)
37. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **4**(5), 1125–1142 (2017)
38. Lu, Y., DaXu, L.: Internet of things (iot) cybersecurity research: a review of current research topics. IEEE Internet Things J. (2018)
39. Lyu, M., Sherratt, D., Sivanathan, A., Gharakheili, H.H., Radford, A., Sivaraman, V.: Quantifying the reflective ddos attack capability of household iot devices. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 46–51. ACM (2017)
40. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of things (iot) security: Current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336–341. IEEE (2015)
41. Medjek, F., Tandjaoui, D., Romdhani, I., Djedjig, N.: A trust-based intrusion detection system for mobile rpl based networks. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 735–742. IEEE (2017)
42. Midi, D., Rullo, A., Mudgerikar, A., Bertino, E.: Kalis—a system for knowledge-driven adaptable intrusion detection for the internet of things. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 656–666. IEEE (2017)
43. Mosenia, A., Jha, N.K.: A comprehensive study of security of internet-of-things. IEEE Trans. Emerg. Top. Comput. **5**(4), 586–602 (2017)
44. Namvar, N., Saad, W., Bahadori, N., Kelley, B.: Jamming in the internet of things: A game-theoretic perspective. In: 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2016)
45. Owezarski, P.: A database of anomalous traffic for assessing profile based ids. In: International Workshop on Traffic Monitoring and Analysis, pp. 59–72. Springer (2010)
46. Perrey, H., Landsmann, M., Ugus, O., Schmidt, T.C., Wählisch, M.: Trail: Topology authentication in rpl. arXiv:1312.0984 (2013)
47. Pihl, R.L.: The sequential probability ratio test. History **9**, 1 (1998)
48. Pongle, P., Chavan, G.: A survey: Attacks on rpl and 6lowpan in iot. In: 2015 International Conference on Pervasive Computing (ICPC), pp. 1–6. IEEE (2015)
49. Pu, C., Lim, S.: A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: design, analysis, and evaluation. IEEE Syst. J. **12**(1), 834–842 (2016)
50. Raza, S., Wallgren, L., Voigt, T.: Svelte: Real-time intrusion detection in the internet of things. Ad hoc Netw. **11**(8), 2661–2674 (2013)
51. Rivera, J., vander Meulen, R.: Gartner says the internet of things will transform the data center. Retrieved August 5, 2014 (2014)
52. Sehgal, A., Mayzaud, A., Badonnel, R., Chrisment, I., Schönwälder, J.: Addressing dodag inconsistency attacks in rpl networks. In: 2014 Global Information Infrastructure and Networking Symposium (GIIS), pp. 1–8. IEEE (2014)
53. Sfar, A.R., Natalizio, E., Challal, Y., Chtourou, Z.: A roadmap for security challenges in the internet of things. Digit. Commun. Netw. **4**(2), 118–137 (2018)
54. Sha, K., Wei, W., Yang, T.A., Wang, Z., Shi, W.: On security challenges and open issues in internet of things. Futur. Gener. Comput. Syst. **83**, 326–337 (2018)
55. Sherasiya, T., Upadhyay, H.: Intrusion detection system for internet of things. Int. J. Adv. Res. Innov. Ideas Educ.(IJARIIE) **2**(3) (2016)
56. Shrivastava, R., Hota, C., Shrivastava, P.: Protection against code exploitation using rop and checksumming in iot environment. In: 2017 5th International Conference on Information and Communication Technology (ICoIC7), pp. 1–6. IEEE (2017)

57. Sonar, K., Upadhyay, H.: An approach to secure internet of things against ddos. Proceedings of International Conference on ICT for Sustainable Development, pp. 367–376. Springer (2016)
58. Stephen, R., Arockiam, L.: Intrusion detection system to detect sinkhole attack on rpl protocol in internet of things. Int. J. Electr. Electron. Comput. Sci. **4**(4), 16–20 (2017)
59. Stolfo, S.J. et al.: Kdd cup 1999 dataset. UCI KDD repository. http://kdd.ics.uci.edu (1999)
60. Sung, Y., Lee, S., Lee, M.: A multi-hop clustering mechanism for scalable iot networks. Sensors **18**(4), 961 (2018)
61. Surendar, M., Umamakeswari, A.: Indres: An intrusion detection and response system for internet of things with 6lowpan. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1903–1908. IEEE (2016)
62. Tang, X., Ren, P., Han, Z.: Jamming mitigation via hierarchical security game for iot communications. IEEE Access **6**, 5766–5779 (2018)
63. Tewari, A., Gupta, B.B.: Security, privacy and trust of different layers in internet-of-things (iots) framework. Futur. Gener. Comput. Syst. (2018)
64. Wallgren, L., Raza, S., Voigt, T.: Routing attacks and countermeasures in the rpl-based internet of things. Int. J. Distrib. Sens. Netw. **9**(8), 794326 (2013)
65. Wang, Y., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutorials **8**(2), 2–23 (2006). https://doi.org/10.1109/COMST.2006.315852
66. Yaseen, Q., Albalas, F., Jararwah, Y., Al-Ayyoub, M.: Leveraging fog computing and software defined systems for selective forwarding attacks detection in mobile wireless sensor networks. Trans. Emerg. Telecommun. Technol. **29**(4), e3183 (2018)
67. Yaseen, Q., AlBalas, F., Jararweh, Y., Al-Ayyoub, M.: A fog computing based system for selective forwarding detection in mobile wireless sensor networks. In: 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W), pp. 256–262. IEEE (2016)
68. Zheng, L., Zhang, H., Han, W., Zhou, X., He, J., Zhang, Z., Gu, Y., Wang, J., et al.: Technologies, applications, and governance in the internet of things. Internet of things-Global technological and societal trends. From smart environments and spaces to green ICT (2011)

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.