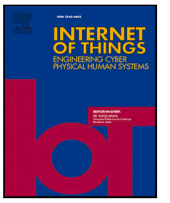
Internet of Things 22 (2023) 100791

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot



Review article

IoT Zigbee device security: A comprehensive review

Alireza Zohourian [a,*], Sajjad Dadkhah [a], Euclides Carlos Pinto Neto [a], Hassan Mahdikhani [a], Priscilla Kyei Danso [a], Heather Molyneaux [b], Ali A. Ghorbani [a]

[a] University of New Brunswick, Fredericton, New Brunswick, Canada
[b] National Research Council Canada, Ottawa, Ontario, Canada

ARTICLE INFO

Keywords:
Zigbee security
Vulnerability
Attack
Countermeasure
Internet of Things (IoT)

ABSTRACT

Zigbee is a well-known wireless network communications protocol designed specifically for low-cost, low-power, low-rate IoT devices, networks and applications. It has become one of the most famous IoT solutions for its smart home devices and appliances. Like every other technology, Zigbee is susceptible to different security vulnerabilities, regardless of all its inherent security considerations. In this survey, we comprehensively study the security of Zigbee with a focus on vulnerabilities, attacks and countermeasures throughout its evolution. We analyze the recent surveys that deal with Zigbee security and compare them based on different criteria. We also review papers that develop security assessment with regard to vulnerabilities, attacks and countermeasures in Zigbee networks. More importantly, we propose a classification scheme for these attacks and conduct a procedural review on the attacks to see how different vulnerabilities will lead to various attacks and how they can be counteracted. More importantly, we propose an attack chain study scheme to see how different vulnerabilities will lead to various attack that open new possibilities for other severe attacks. Finally, we conduct an evaluation study to see how the reader can use the reviewed papers for further future research in terms of vulnerability assessment, attack implementation and development, and countermeasure evaluation in Zigbee networks.

1. Introduction

The Internet of Things (IoT) has become one of the top trends in the academia and the industry and has been experiencing a proliferation in users, devices and applications [1,2]. Users include almost every person, business and organization from the private sector, the public sector and the government. The devices in the IoT ecosystem range from small sensors and actuators to smart cameras and vehicles with numerous applications (e.g., smart home, smart healthcare and smart industry) [3]. As such, this heterogeneous environment with such complexity demands various technologies and solutions to meet the needs of different services.

The Internet of Things (IoT) has been evolving rapidly, with emerging trends poised to revolutionize various sectors and improve our daily lives. One significant trend is edge computing, which pushes data processing closer to the devices themselves, enhancing response times and reducing bandwidth requirements [4]. Another trend gaining momentum is the rise of smart cities, where IoT technologies are leveraged to optimize urban infrastructure, traffic management, energy consumption, and waste management [5]. Furthermore, the integration of artificial intelligence (AI) and machine learning (ML) with IoT enables more sophisticated data analysis, leading to improved decision-making and automation [6]. Moreover, another trending topic is disaster management, where

* Corresponding author.
E-mail addresses: alireza.zohourian@unb.ca (A. Zohourian), sdadkhah@unb.ca (S. Dadkhah), e.neto@unb.ca (E.C.P. Neto), hmahdikh@unb.ca (H. Mahdikhani), priscilla.danso@unb.ca (P.K. Danso), heather.molyneaux@nrc-cnrc.gc.ca (H. Molyneaux), ghorbani@unb.ca (A.A. Ghorbani).

https://doi.org/10.1016/j.iot.2023.100791
Received 1 February 2023; Received in revised form 27 March 2023; Accepted 14 April 2023
Available online 2 May 2023

IoT technology plays a critical role in early warning systems, real-time monitoring, and post-disaster recovery [7]. More importantly, the non-wearable IoT-based smart ambient behavior observation system is an emerging IoT trend that involves using unobtrusive sensors and devices in the environment to monitor and analyze human behavior, enabling personalized services and improved well-being without the need for wearable devices [8]. Lastly, the increasing focus on security and privacy has led to advancements in blockchain-based solutions to safeguard sensitive data and ensure secure communication among IoT devices [9]. These IoT trends demonstrate the potential for transformative innovations that can reshape industries and enhance our quality of life.

The Internet of Things (IoT) encompasses a vast array of applications, each with distinct requirements pertaining to factors such as power consumption, transaction rates, and data transmission [10]. As an illustration, consider a scenario where a remote monitoring system requires a battery-operated temperature sensor to gather and transmit data about the surrounding environment upon request. Traditional communication protocols, such as Wi-Fi or Bluetooth, tend to have significant computational overhead, which can result in rapid battery drainage and may be unsuitable for these specific use cases. In light of these challenges, the development and adoption of lightweight protocols have become essential for ensuring the longevity and efficiency of IoT devices. These protocols offer several advantages, including lower transmission rates, reduced computational overhead, and optimized power consumption. Consequently, they are better suited for resource-constrained environments or situations where devices need to conserve energy for extended periods.

To address such demands, several IoT solutions have been proposed; Zigbee [10] and Z-Wave [11] for short range applications, LoRaWAN [12] and Sigfox [13] as wide area networks, and LTE-M [14] and NB-IoT [15] as cellular networks. Zigbee and Z-Wave are well-known protocols for Personal Area Networks (PAN) [16] mainly used in smart home applications and have been attracting a lot of attention from individuals and companies. LoRaWAN and Sigfox are well-known Low-Power Wide Area Networks (LPWAN) [17] for many different applications such as logistics and monitoring. LTE-M and NB-IoT are well-known cellular technologies suitable for enabling global IoT connectivity.

Moreover, Zigbee has become famous for its smart home solutions, such as smart lighting, and has been supported by large companies and vendors. It is a low-power low-rate network communications protocol built upon IEEE 802.15.4 [18] which is the standard introduced by IEEE for low-rate networks and constitutes the Physical (PHY) and Medium Access Control (MAC) layers of the Zigbee technology. Moreover, Zigbee has become more and more open to the public which enabled researchers to analyze its inherent capabilities and characteristics. Specifically, many cybersecurity researchers have studied Zigbee's underlying security mechanisms to find potential vulnerabilities and assess their exploitability.

Above all, Zigbee is no exception to security weaknesses and many works have proposed different strategies to assess the security of Zigbee networks. However, there are very few works that review the security of Zigbee, as one of the trends in IoT, in-depth. Therefore, it is paramount to study this topic in a systematic way and identify the challenges that this technology has faced since its genesis to enable the reader to obtain a broad outlook on this line of research. Therefore, The primary objective of this study is to provide the first in-depth analysis of Zigbee security with a focus on vulnerabilities, attacks and countermeasures. To accomplish this, we give a review of the recent survey papers about Zigbee security and compare them based on several criteria. Moreover, we extensively review the vulnerabilities exploited, attacks developed and countermeasures proposed on the Zigbee networks and devices.

The main contributions of this paper include:

- Conduct an extensive review of the literature related to Zigbee Security;
- Conduct a comprehensive study of the security assessment of Zigbee networks;
- Present a classification scheme to study the attacks in Zigbee;
- Conduct a procedural review of the attacks in Zigbee using Vulnerability-Attack-Countermeasure (VAC) sequences;
- Propose a novel attack chain study scheme based on the classification criteria and review process;
- Evaluation of Zigbee attack papers for future research development;
- Analyzed the open challenges and future work in Zigbee security assessment.

This survey outlines most of the works on the security of Zigbee and the rest of it is structured as follows: In Section 2, we will review and compare the survey papers in regard to Zigbee Security. In Section 3, an overview of the Zigbee technology is introduced in terms of the protocol stack, network topology and security measures. Sections 4–6 are the main contributions of this work which involve the classification of Zigbee attacks, a procedural review of the attack papers and a complementary analysis of attack chains. In Section 7, we conduct an evaluation study of the security assessment procedures proposed in papers for future research development. The study comes to a conclusion in Section 8, which also discusses open challenges and potential future paths for the security analysis of Zigbee networks. Fig. 1 shows an overview of the organization of this work.

2. Literature review

In this section, we first provide a temporal study of the publications about Zigbee. Then, we review the surveys that discuss Zigbee security, analyze their approach and compare their contributions. These related works are divided into two groups:

1. **Multi-protocol Surveys.** These surveys [19–31] analyze the security of not only Zigbee but many other common protocols in IoT. They do not focus on one specific protocol but include Zigbee as part of their study. However, we were concerned with how they analyzed these protocols in terms of security, especially Zigbee.
2. **Zigbee-specific Surveys.** In these surveys [32–39], the authors have addressed the security of Zigbee directly and provided insightful discussions. This group is of great importance since our focus is on the security of Zigbee networks solely.

These groups of papers are reviewed briefly and then compared in detail in Table 1.

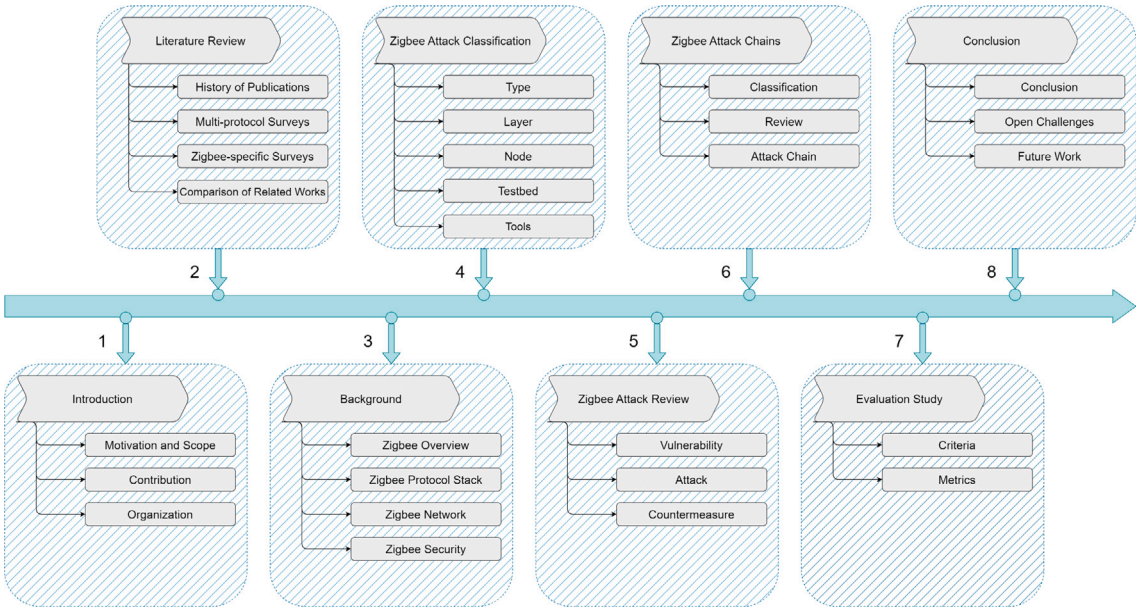


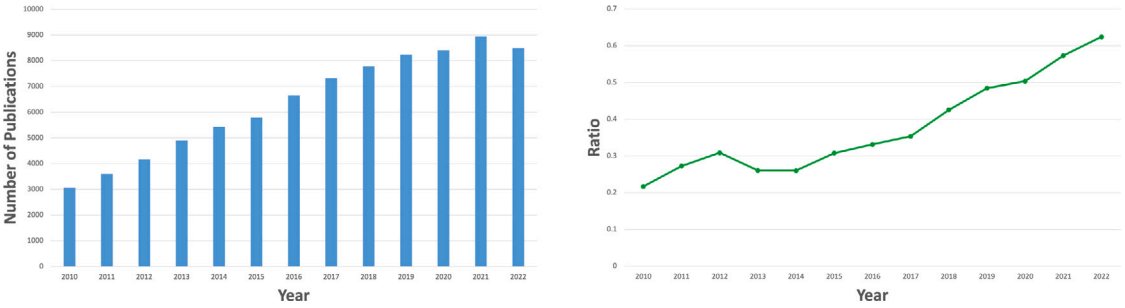
Fig. 1. Organization of the paper.

Table 1
Comparison of Survey Papers Regarding Security Analysis of Zigbee.
(✓: Included, ●: Adequately Analyzed, ◐: Partially Analyzed, ○: Not Analyzed)

Group	Publication	Focus	Comparison	Classification	Solutions	Relational Study	Vulnerabilities	Attacks	Countermeasures
Multi-protocol	[19]	Functionalities and Security Features			✓		◐	◐	◐
	[20]	Security Trends			✓		○	◐	◐
	[21]	Jamming Attacks	✓				○	◐	◐
	[22]	Security Issues	✓	✓	✓		●	●	○
	[23]	Attacks and Defenses		✓	✓	✓	◐	●	●
	[24]	Security Features			✓		◐	◐	◐
	[25]	IoT Security					○	○	○
	[26]	Technologies and Protocols					○	○	○
	[27]	Vulnerabilities and Exploitations	✓	✓			●	●	●
	[28]	Layer Security			✓		◐	○	○
	[29]	Protocol Security			✓		◐	◐	○
	[30]	Security Overview			✓		○	○	○
	[31]	Protocol Security			✓		◐	◐	○
Zigbee-specific	[32]	Weaknesses and Suggestions					◐	○	◐
	[33]	Routing Layer Intrusions					○	◐	○
	[34]	Zigbee Vulnerabilities		✓	✓		◐	●	○
	[35]	Zigbee Topology					○	○	○
	[36]	Zigbee Concepts					○	○	○
	[37]	General Overview			✓		◐	○	○
	[38]	Key Management			✓		◐	○	◐
	[39]	Zigbee and IEEE 802.15.4			✓		◐	●	○
	This Work	Attack Classification	✓	✓	✓	✓	●	●	●

2.1. History of publications

In this section, we provide a temporal study of the number of publications about Zigbee security since 2010. The reason to conduct such a study is to provide the reader with an overview of the number of publications throughout the past decade to realize what the trend of Zigbee security looks like in academia.



(a) Zigbee Security Publications. (b) Zigbee Security Publications Ratio.

Fig. 2. Temporal study of Zigbee publications.

To this end, we used google scholar to find the number of publications about Zigbee security using the phrase "Zigbee security". This gave us the number of publications that are concerned with Zigbee and Security in some context. We assume that the word "security" is an all-encompassing and general word to conduct this study.

Fig. 2 demonstrates the results of this analysis. Figure Fig. 2(a) shows the total number of such publications for each year and Fig. 2(b) shows the ratio of these numbers to all papers that include the word Zigbee. Both figures show an increasing pattern that implies the growing interest of academics in Zigbee security. This is true because Zigbee is one of many IoT protocols, most of which are not open source and this lets the researchers explore this protocol's security and try to find its vulnerabilities and propose countermeasures.

2.2. Multi-protocol surveys

Regarding Zigbee, the majority of these works provide an overview of the technology with respect to the protocol stack layer, network topology and security design. This is followed by assessing the security of Zigbee from different perspectives (e.g., attack classification, layer security, etc.).

Rizzardi et al. [19] overview the Zigbee specification extensively, analyze its security regarding four pillars of security, namely, Authentication, Confidentiality, Integrity and Authorization, and detail the existing and proposed security solutions for these pillars.

Lata et al. [20] outline some of the most important attacks on Zigbee with a focus on the network layer and refer to solutions to each of these attacks.

Pirayesh et al. [21] start by giving a primer on Zigbee communication with a focus on the Physical layer and transmitter–receiver structure of Zigbee. Then, the authors focus on different delicately designed jamming attacks and elaborates on the attack scenarios. Finally, they present the proposed anti-jamming techniques to mitigate various jamming attacks discussed earlier.

Tournier et al. [22] thoroughly recognize Zigbee through their generic IoT stack and overview the protocol, routing and security mechanisms. They, then, summarize the Zigbee attacks with a focus on three criteria: packet security, protocol security and system security. For each criterion, they outline the most prevalent attacks ranging from simple passive attacks to more complex active attacks.

Lounis et al. [23] present a generic attack taxonomy of IoT protocols and summarize the Zigbee attacks and defense strategies through the lens of this taxonomy. The authors categorize the attacks in five classes: Fabrication, Interception, Modification, Interruption and Domination. They also provide detailed attack-defense trees and include the related attacks in each attack class.

Kambourakis et al. [24] review the protocol considering its unique characteristics, and special node types and extensively analyzes its innate security measures in different versions of Zigbee. This is followed by a comprehensive summary of all the unique attacks on Zigbee in the literature, an explanation of the attack scenarios and a few possible countermeasures proposed.

Mrabet et al. [25] propose an IoT architecture in which Zigbee is implied as a component in the network layer.

Yugha et al. [26] examine and discuss several unresolved problems in the field of IoT security and protocol use. The survey's primary contribution is to emphasize the current state of research and simulation tools utilized for IoT layer protocol analysis.

Neshenko et al. [27] focus on IoT vulnerabilities and offer a distinct taxonomy that clarifies IoT weaknesses, corresponding attack vectors, effects on many different security principles, attacks that exploit such flaws, corresponding mitigation Schemes, and presently provided operational cybersecurity capacities to deduce and evaluate such vulnerabilities.

Burhan et al. [28] give a general introduction of various IoT layered designs and attacks on security from a layered perspective. After that, they analyze the techniques that offer fixes for these problems along with their drawbacks. They finally propose a new, safe, layered IoT architecture to address these problems.

Marksteiner et al. [29] give a summary of IoT application areas and go over the key wireless standards in IoT for smart homes, namely Zigbee. Finally, they discuss the security attributes of the aforementioned protocols, contrast them, and offer recommendations on which protocols are better suited for a secured smart home.

Datta et al. [30] explain the IoT architecture, protocols used, security concerns, and applications based upon smart cities for IoT.

Krejvci et al. [31] provide a security analysis of four popular IoT protocols, including Zigbee. Then, they go over several protocol flaws and how they have changed in terms of security.

2.3. Zigbee-specific surveys

According to our knowledge, most survey papers on Zigbee only give an overview of the inherent security measures and do not analyze the security from different viewpoints such as layer security, node security, vulnerability assessment, etc. Following, we will give a brief summary of these works.

Gupta et al. [32] enumerate major Zigbee vulnerabilities and propose several countermeasures to mitigate them.

Sidhu et al. [33] discuss about the research on how to develop attacks in test environments or simulated scenarios in order to properly capture the effects of attacks and to provide prompt intrusion detection for wireless sensor networks with limited resources.

Khanji et al. [34] categorize Zigbee threats based on four criteria; Layer, Method, Target and Member. They further subdivide these criteria into existing attacks. Based on layer, the authors consider Physical, MAC, Network and Transport layer attacks and provide details and examples of such attacks. They categorize the attacks into passive and active attacks in terms of method. Regarding target, the paper discusses sink, source and neighbor attacks and elaborates on their scenarios. Finally, the authors discuss the attacks in which the malicious device is or is not a part of the network. This is followed by a summary of methods to encounter the Zigbee security flaws.

Kumar et al. [35] present Zigbee networking topology, its types, architecture and its application.

Varghese et al. [36] describe some fundamental Zigbee principles and how they relate to networking security. Additionally, they provide a list of the principal producers of Zigbee transceivers, an essential element in any attack.

Aju et al. [37] they provide a comprehensive overview of Zigbee as a wireless sensor network-based technology, outlining its topology and use cases while also highlighting some of its limitations such as security and privacy concerns.

Davani et al. [38] enumerate Zigbee vulnerabilities comprehensively and explain one of the main attacks in Zigbee, the Same-Nonce Attack based on a shortcoming in the cryptography. They further conduct an elaborate study of all the related works each of which has proposed a countermeasure for one of the vulnerabilities in Zigbee.

Baronti et al. [39] examine many perspectives on the use of IEEE 802.15.4 in Zigbee with an emphasis on energy efficiency, networking, data management, and security in wireless sensor networks, particularly Zigbee.

2.4. Comparison of related works

In this section, we analyze and compare the reviewed survey papers based on different criteria. We first identified the **focus** of the papers in terms of Zigbee and its security. We, then, see if the work in question has done a comparison with earlier reviews and demonstrated their contribution. One of our main concerns was to see if the publications have provided a **classification** on all the attacks proposed against Zigbee networks. As a minimum requirement of Zigbee security analysis, we considered the elaboration of native Zigbee security **solution**s in each publication. Finally, we were interested to see if any of the authors have conducted a **relational review** to see how the **vulnerabilities** lead to attacks, how these **attacks** can lead to other complicated ones, and what **countermeasures** have been proposed to mitigate them. Table 1 shows an overview of this comparison.

3. Background

We will provide a broad outlook of Zigbee in this part. We introduce Zigbee with regard to applications, various devices and native properties. After that, we explain the Zigbee protocol stack as a network communications protocol. Zigbee networking concepts such as node types and IDs, and the native security mechanisms such as encryption keys are also presented.

3.1. Zigbee overview

3.1.1. Definition

Zigbee is a technology for low-cost, short-range IoT applications that consume little power and have low transmission rates and is developed and maintained by Connectivity Standard Standards Alliance (CSA), formerly known as Zigbee Alliance [40]. Zigbee is also a wireless network communications protocol sitting on top of the IEEE 802.15.4 standard and is designed for short-range applications to create a Low-Power Wireless Personal Area Network (LR-WPAN) [41].

3.1.2. Applications

Devices using Zigbee technology are designed for applications requiring little data transmission and power consumption (e.g., sensory data). Therefore, they are expected to survive on batteries up to several years. Moreover, one of the considerations in the design of Zigbee devices is to be low-cost and affordable. Some of the use cases of Zigbee devices are home automation, smart industry, healthcare, monitoring, etc.

3.1.3. Devices

Zigbee devices come in a wide variety, ranging from sensors and actuators to smart plugs and light bulbs. Based on different applications, one can find various Zigbee devices to meet their needs. For home security for instance, there are motions sensors, door/window sensors, and smart alarms and sirens. For automation purposes, there are several smart devices, such as bulbs, switches, plugs and dimmers.

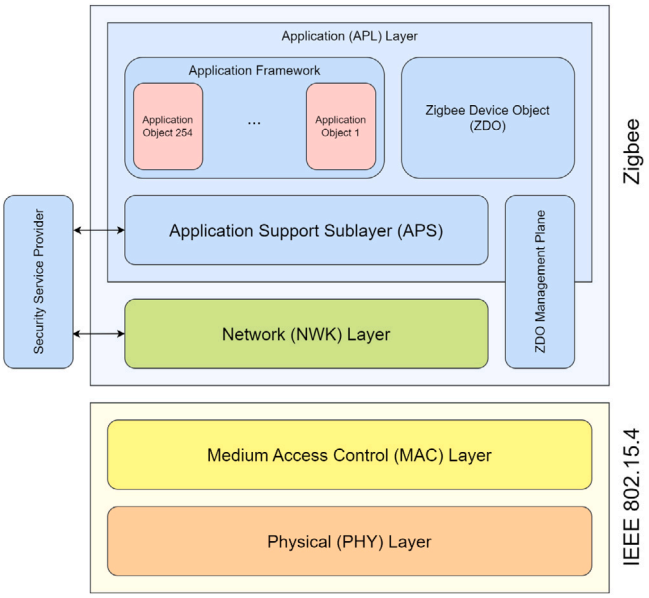


Fig. 3. Overview of the Zigbee protocol stack.

3.1.4. Characteristics

Zigbee is a mesh network of at most 65,536 nodes that operates on 868 Mhz (Europe), 915 Mhz (Americas) and 2.4 GHz (Global) radio bands, has a maximum rate of 250 kbps and depending on power output and environmental factors, it can enable transmission over a distance of no more than 100 m and a range of 1 km in Sub-Ghz bands. Zigbee is considered to have low cost and power consumption [42].

3.2. Zigbee protocol stack

The layers that make up the Zigbee stack architecture are a collection of building blocks each of which provides the layer above with a certain set of services. The service of transmitting data is provided by a data entity, while all other services are provided by another entity for management. A Service Access Point (SAP) is used by each entity that enables a service to provide an interface to the layer above it, and each SAP handles a variety of service basics to provide the necessary functionality [43].

The physical (PHY) layer and the medium access control (MAC) sub-layer are the two underlying layers that are specified by the IEEE 802.15.4 standard. By offering the network (NWK) layer and the framework for the application layer, the Zigbee Alliance builds up on this building block. Zigbee Device Objects (ZDO) and the application support sub-layer (APS) make up the application layer framework [41]. The framework is used by manufacturer-defined application objects, which also share security and APS services with the ZDO. Fig. 3 shows an overview of the layered stack structure of the Zigbee protocol.

3.2.1. Physical (PHY) layer

The PHY layer of the Zigbee protocol [44] works in the 868/915 MHz and 2.4 GHz frequency bands. Both the 915 MHz band, which is utilized in nations like the United States and Australia, and the 868 MHz European band are covered by the PHY layer that has a low frequency. The higher frequency PHY layer is largely in use all around the world.

Depending on the underlying MAC/PHY, the MAC layer [45] regulates how devices can access the radio channel using one of CSMA-CA or LBT mechanism. Additionally, it might be in charge of synchronization, beacon frame transmission, and transmission mechanism reliability.

3.2.2. Network (NWK) layer

The IEEE 802.15.4 MAC layer requires the capabilities that the network layer [43] must supply, as well as an appropriate service interface for the application layer. The NWK layer theoretically consists of two services that offer the required capability to interface with the application layer. These two services are provided by the data service and the management service.

The NWK Layer Management Entity (NLME) [46] supports services related to management through its corresponding SAP, the NLME-SAP, while the NWK Layer Data Entity (NLDE) [46] takes care of data transfer services with the help of its related SAP, the NLDE-SAP. Some administration duties are carried out by the NLME via the NLDE, and it also maintains the Network Information Base (NIB), a database of controlled items [47].

For an application to transmit application layer data units among the devices in the network, the NLDE offers a data service. The actual devices need to be connected to the same network. A management service must be made available by the NLME for an application to communicate with the stack.

3.2.3. Application (APL) layer

The APS, the ZDO (which includes the plane for ZDO administration), and the manufacturer-defined application objects make up the Zigbee application layer [48].

Using a consistent collection of services that are utilized by both the objects related to ZDO and the manufacturer-defined application, the APS [49] provides an interface between the NWK and the APL.

The domain on which the objects for application are organized on Zigbee devices is called the application framework [50] in Zigbee. Application profiles are arrangements on message structures, communication types, and processing techniques that let programmers use application entities that are located on different devices to create an interoperable, distributed application. Applications can transmit commands, query for data, and handle commands and data thanks to these application profiles. A cluster identifier connected to data going into or out of the device is used to identify clusters. Within the confines of a specific application profile, cluster identifiers are exclusive.

The Zigbee Device Object (ZDO) offers an interface for connection between application objects, device profiles, and APS [51]. It is situated between the application framework and the APS. It complies with the common needs of all applications using the stack of Zigbee protocol. The ZDO is in charge of the following tasks:

- Setting up the Security Service Provider (SSP), NWK layer, and the APS.
- Putting together configuration data from the end applications in order to decide and put into practice the discovery and the management of security, network, and binding.

In the application framework layer, the ZDO provides public interfaces to the application objects so they can control device and network functions.

3.3. Zigbee network

3.3.1. Node types

There are three main types of nodes in Zigbee networks, due to the presence of which the topology of the network might change:

- It is the **Zigbee Coordinator (ZC)** who starts and runs the network. To put it another way, the ZC is an IEEE 802.15.4 Personal Area Network coordinator in charge of integrating and removing devices from its PAN and has to be a Full-Function Device (FFD). [52].
- **Zigbee Routers (ZRs)** route the traffic in a network of Zigbee devices. A ZR is also an FFD that is not the ZC but has the ability to handle associations and route communications between devices.
- **Zigbee End Devices (ZEDs)** that send/receive data/commands to ZRs or the ZC. In other words, a ZED is any Reduced-Function Device (RFD) [53] or FFD which is not the ZC and a ZR.

3.3.2. Network topology

There are three network topologies that are supported by the Zigbee NWK: the star, tree, and mesh topologies. A single device, the ZC in this case, manages and maintains the inner workings of the network in a star topology. All the other devices, in this case ZRs and ZEDS, speak with the ZC directly. The ZC in tree and mesh topologies is responsible for establishing the network and selecting the crucial parameters for the network, although ZRs can be used to extend the range of the network. In tree network topologies, ZRs employ a routing approach that is hierarchical in order to move messages that carry data and controls throughout the network. Full peer-to-peer (P2P) conversation is possible with mesh network architectures. Fig. 4 shows a mesh network of one ZC, three ZRs and six ZEDs connected to the internet through the gateway.

3.3.3. Node IDs

Both a 64-bit and also a 16-bit address are used by every device in a Zigbee network. Each physical device has a 64-bit address that is specific to it. It is given during the manufacturing process and is also referred to as the MAC address or extended address [54]. A manufacturer-specific Organizationally Unique Identifier (OUI) [55], that is allotted by the IEEE, is present in the first three bytes of the extended address. When a device enters a Zigbee network, it is given a 16-bit address. This address is sometimes known as the network address because of this. The coordinator is given a reserved short address of 0×0000. The ZC or a ZR sends a randomly generated address to all other devices, enabling the join [56].

The source and destination short addresses are used to send every transmission over Zigbee. Zigbee devices also employ these short addresses in their routing tables to choose the best path for network packets via the network. The short address is dynamic, hence it cannot be used to reliably identify and specify a device. The extended destination address is frequently used in network packet transmissions to ensure that packets are delivered to the right location in order to overcome this issue. If the short address is not known, the Zigbee stack can find it before sending data to a distant device [48].

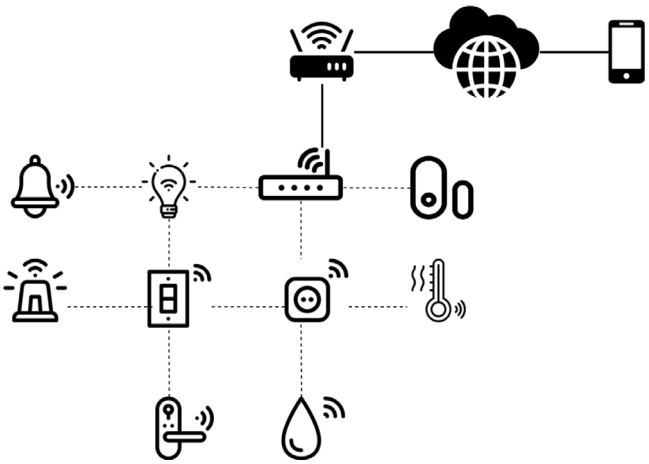


Fig. 4. A sample mesh network of Zigbee devices.

3.3.4. Network IDs

Personal Area Networks (PAN) are the name given to Zigbee networks. Each Zigbee network is identified by a distinct PAN Identifier (PAN ID) shared by every device connected to that network. Zigbee devices can either find adjacent networks and choose a PAN ID to attach, or they are preloaded with a PAN ID to connect [50].

All radio frequency transmissions of data among devices in a Zigbee network use the 16-bit PAN ID as an addressing field for the MAC layer. However, because this PAN ID has only has 16 bits and therefore 65,535 possible addressing combinations, it is possible for different Zigbee networks in close proximity to one another to hold the same PAN ID. The Zigbee Alliance developed another PAN ID that has 64 bits in order to eliminate any 16-bit PAN ID conflicts [44].

This extended PAN ID (EPID), commonly known as the 64-bit PAN ID, is designed to be a singular value with no duplicates. When a coordinator establishes a network, it has two options: it can choose a random EPID or one that has been preconfigured. When joining a network, devices utilize the EPID; if a device is already preconfigured with an EPID, it will only connect to a network with that same EPID. Otherwise, when a device joins a network, it could get into any detectable PAN and acquire the EPID from the network [57]. The EPID is present in all beacons inside a Zigbee network and is used to resolve conflicts between 16-bit PAN IDs.

Both an EPID and a PAN ID are supported by the Zigbee protocol. A network is uniquely identified by using both Identifiers. The network identifiers of devices connected to the same Zigbee network must match. If several Zigbee networks are active nearby, each one should have a different PAN ID.

3.4. Zigbee security

3.4.1. Security design

Zigbee security is built on an open trust paradigm in which all programmes running on a single device and various communication stack tiers trust one another [58]. Each layer can reuse keys to reduce costs on storage, since security can be built on the open trust paradigm. Additionally, end-to-end security is offered so that only source and destination devices can retrieve communications that are secured by a shared key. This makes it possible for message routing to and from the two devices using a shared common key to not depend on trust issues.

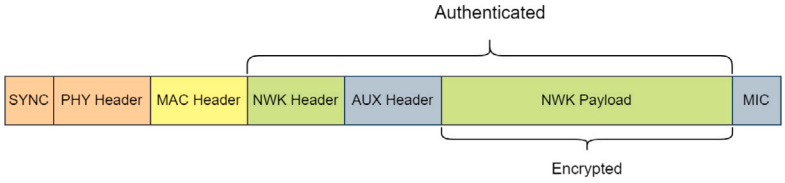
3.4.2. Security architecture

Security components are present in the protocol stack at two different tiers in the Zigbee security architecture. The secure transportation of each layer's particular frame is the responsibility of the NWK and APS layers. The APS additionally offers functionalities for the maintenance and creation of security connections [59].

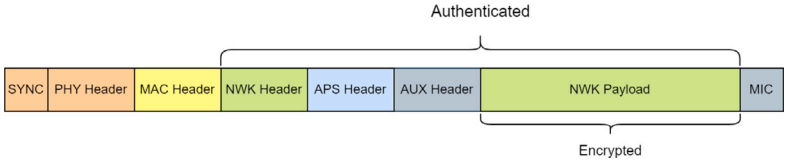
The frame-protection function must be used by Zigbee whenever a frame coming from the NWK layer has to be protected. The processing operations required to safely transmit outbound frames and securely receive inbound frames are handled by the NWK layer. By initiating necessary keys, initializing counters for frames, and establishing the security level, upper layers manage the security processing operations [60]. Fig. 5(a) shows the security of NWK in a Zigbee packet.

The APS handles security through a frame-protection mechanism in the APS layer while a frame coming from the APL must be safeguarded. The actions required for securely transmitting outgoing packets, securely receiving incoming packets, and reliably creating and managing keys for cryptographic calculations are handled by the APS layer. By sending primitives to the APS layer, upper levels handle the administration of cryptographic keys [61]. Fig. 5(b) shows the security of APS in a Zigbee packet.

Zigbee defines a role for a Trust Center (TC) as the device in a network on which other devices trust to disperse keys for the goal of managing the configuration of the network and, potentially, end-to-end applications. Each centralized security network



(a) NWK Packet Security.



(b) APS Packet Security.

Fig. 5. Packet formation of NWK and APS layer security.

must contain exactly one Trust Center, which every member of the network must acknowledge as legitimate [62]. Network security policies must be established, updated, and maintained by the Trust Center. All routers in a distributed security network can serve as the TC and disperse keys for making the network secure. Since there is not a single trust center in the network, this decentralized trust center role is utilized for the disperse of the network key but not the distribution of the Trust Center Link Key (TCLK) [62].

3.4.3. Security keys

Two security keys, namely link key and network key, are used to secure a network of Zigbee devices. A 128-bit network key that is commonly shared by all network devices is used to safeguard broadcast communications and any network layer communications, whereas a 128-bit link key common between two devices secures communications that are unicast and happen between APL peer entities [63].

The acquisition of a network key is done by a device through key transport and the acquisition of link keys are handled through the key-transport mechanism or pre-installation code keys (e.g., during factory production). Key-transport is a method for securely transmitting a key to and from one or multiple devices [64].

Although there is only one kind of network key, it can be applied to both centralized and distributed security architectures. The distribution of a network key is governed by the security model. Global and unique trust center link keys are the two different sorts. The kind of trust center link key that the local device is using will dictate how it responds to different trust center communications (like the commands in the APS), considering whether or not to apply encryption at the APS level. Additionally, the transmissions of data between the TC and the suitable peer device may be secured using a TCLK. An application link key is a cryptographic key for securing the communication of two devices, neither of which is the trust center [65].

4. Zigbee attacks classification

This section presents classification criteria for attacks on the Zigbee networks. Fig. 6 outlines the proposed attack classification scheme.

We classify these attacks based on the following criteria:

- **Type:** Attackers seek different goals when exploiting vulnerabilities of the Zigbee networks. Based on these goals, the main types of attacks in Zigbee networks are reconnaissance, device manipulation, denial of service and network control, concisely explained as follows:
  - **Reconnaissance:** In this class, the attacker's objective is to gather knowledge that can be used against the targeted network and leverage this information to make new attacks possible.
  - **Device Manipulation:** In order to alter a device's typical behavior, this kind of attack requires inserting malicious packets into the network.
  - **Denial of Service (DoS):** A DoS attack is concerned with preventing a device from working properly and gaining the advantage of doing further harm.
  - **Network Control:** In a network control attack the adversary seeks to gain control over a device or a part of the network to achieve their malicious goals.
- **Layer:** The attacks on the Zigbee networks target different layers of the protocol stack. Therefore, we analyzed the attacks to see if they are targeting the IEEE or the Zigbee part of the stack. The reader might be interested to know which solution is responsible for each attack.

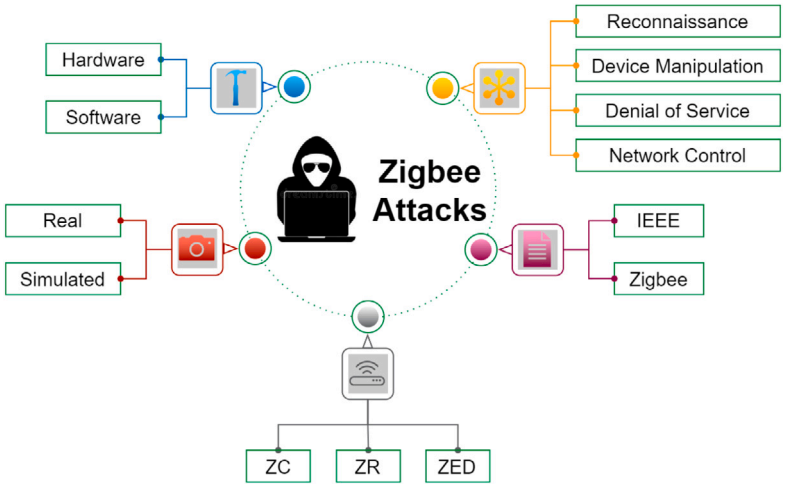


Fig. 6. Criteria for the classification of Zigbee attacks.

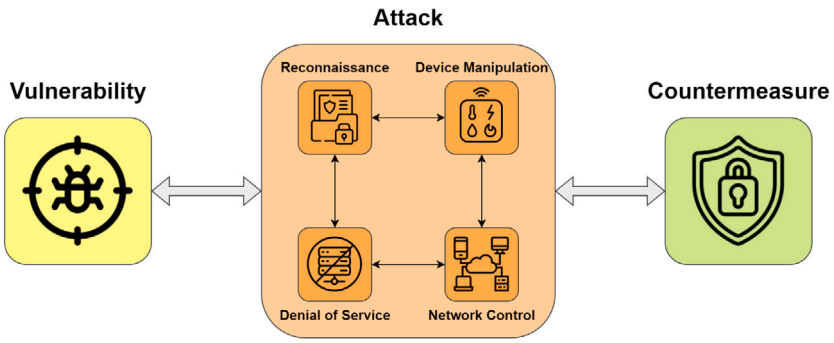


Fig. 7. Overview of the Attacks Review Scheme.

- **Node:** Many of these attacks are intended to gain an advantage from specific node types such as the ZC, the ZRs and the ZEDs. This can help the reader understand which node types are being targeted more frequently.
- **Devices:** The publications that propose any of these attacks have implemented them in two different ways; some use real devices and others have used simulated devices. It is of great importance to realize which attacks have been performed on real devices, as their nature is much different than that of simulated devices.
- **Tools:** In order to conduct these attacks, authors have used different **software** and **hardware** tools to conduct their attacks. The reader might be interested in learning the tools needed to implement the attacks for future experimentation.

Table 2 presents a comprehensive overview of all the attacks based on the proposed classification.

5. Zigbee attacks review

In this section, we conduct a procedural review of the attacks that enables us to interpret each attack as a Vulnerability-Attack-Countermeasure (VAC) sequence. This review is procedural in the sense that relates the existing vulnerabilities to specific attacks and then connects them to the proposed countermeasures if any, so the reader obtains a deep understanding of what vulnerability leads to which attack, and how that attack can be addressed. To this end, we will specify each attack as a VAC sequence and to obtain a good understanding of what has made an attack possible, how it is conducted and what solutions have been proposed to mitigate it, the attacks are explained based on the following procedure:

Fig. 7 shows an overview of the attacks review scheme.

- **Vulnerability:** Every attack begins with a security flaw that can be used to carry out the attack.
- **Attack:** Every attack requires certain conditions and follows a specific procedure to become feasible and effective.
- **Countermeasure:** Several attacks can be detected or mitigated by enabling different countermeasures in the right place.

Table 3 shows the review of the attacks based on vulnerabilities, attacks and countermeasures specified by VAC sequences.

Table 2
Overview of the attacks on Zigbee networks based on the classification scheme.
(RC: Reconnaissance, DM: Device Manipulation, DoS: Denial of Service, NC: Network Control)

Pub.	Type	Attack name	Layer	Node	Testbed	Software tools	Hardware tools
[66]	RC	Key Leakage	Zigbee	ZC/ZED	Real	Ubiqua Protocol Analyzer	CC2531 CC2538
	DoS	Communication Interruption	Zigbee	ZED			
	DoS	Disconnection	Zigbee	ZED			
	DoS	Truncated Packet	Zigbee	ZR/ZED			
	DM	Improper Integrity Check	Zigbee	All			
[67]	RC	Zigbee Signal Eavesdropping	Zigbee	All	Real	Wireshark	USRP-N210 CC26 × 2R
	DM	Zigbee Signal Emulation	Zigbee	All			
[68]	DoS	Capacity Exploitation	Zigbee	ZC/ZED	Real	ZigHomer	ATUSB
	DoS	Offline Attack	Zigbee	ZED			
	RC	Network Key Leakage Attack	Zigbee	ZC/ZED			
	NC	Hijacking Attack	Zigbee	ZED			
[69]	RC	Device and Event Identification	Both	All	Real	N/A	CC2531
	RC	Device Identification	Zigbee	All			
[70]	DoS	Low-rate DoS Attack (LDoS)	IEEE	ZC/ZR	Simulated	Python	N/A
[71]	RC	User Privacy Breaches	Zigbee	ZR/ZED	Simulated	Z3Sec, ProVerif	USRP210 ApiMote, RPi
	RC	Fake Device Injection	Zigbee	All			
[72]	DM	Replay Attack	IEEE	Node	Both	KillerBee	ApiMote
[73]	RC	Active Node Identification	IEEE	ZC/ZR	Real	Zigator, GNU Radio	USRP N210, ATUSB
	RC	Passive Node Identification	Zigbee	All			
	RC	Hardware Device Identification	IEEE	All			
	RC	Legacy Device Identification	Zigbee	ZED			
	RC	Network Command Identification	Zigbee	All			
	RC	Network Key Extraction	Zigbee	ZC			
	DoS	PANID Conflict Attack	Both	ZR/ZED			
[74]	RC	Network Key Extraction	Zigbee	ZC	Real	Z3Sec Scapy-radio	USRP B200
	RC	Active Device Scan	IEEE	All			
	DM	ACK Spoofing	Both	All			
	DM	Identify-Action Attack	Zigbee	ZR/ZED			
	DoS	Reset to Factory-New Attack	Zigbee	ZR/ZED			
	DoS	Permanent Disconnect Attack	Zigbee	ZR/ZED			
	NC	Hijack Attack	Zigbee	ZR/ZED			
[75]	DM	Correlation Power Analysis Attack	Zigbee	ZR/ZED	Real	Python	CC2531EMK
	NC	Takeover Attack	Zigbee	ZR/ZED			
[65]	RC	Key Sniffing	IEEE	ZC	Real	KillerBee	Atmel Raven RZUSB
	DM	Replay Attack	IEEE	ZR/ZED			
	DoS	Association Flooding	Zigbee	ZR/ZED			
	RC	Device Spoofing	Zigbee	ZR/ZED			
[76]	RC	Same-Nonce Attack	IEEE	ZED	Simulated	NS-3	ATmega128L CC2420
	DoS	Ghost-in-Zigbee	IEEE	ZED			
	DoS	High Computational Load	IEEE	ZR/ZED			
	DoS	MAC Misbehavior	IEEE	ZR/ZED			
	DoS	Post-Depletion Replay	IEEE	ZED			
	DM	Replay Attack	IEEE	ZED			
[77]	NC	Wormhole Attack	Zigbee	All	Simulated	NS-2	N/A
[78]	NC	Sinkhole Attack	Zigbee	ZR	Simulated	N/A	N/A
[79]	NC	Sybil Attack	Zigbee	ZR/ZED	N/A	N/A	N/A
[80]	RC	Same-Nonce Attack	IEEE	ZED	Simulated	IAR Embedded Workbench, SmartRF Studio 7	CC2530ZDK
	RC	Physical Attack	IEEE	All			
	DoS	Bandwidth/Processor Overload	IEEE	ZED			
	DM	Replay Attack	IEEE	ZED			
[81]	RC	Network Discovery	IEEE	ZC/ZR	Simulated	AVR Studio, KillerBee	JTAGICE mkII, RZ Raven
	RC	Interception of Packets	Zigbee	All			
	DM	Replay Attack	IEEE	ZED			
[82]	RC	Zigbee Network Key Sniffing Attack	Zigbee	ZC	Simulated	KillerBee	CC2531
	DoS	Zigbee End-Device Sabotage Attack	IEEE	ZED			
[83]	DoS	Association Flooding Attack	Zigbee	ZR/ZED	Simulated	KillerBee, Avrora	XBow MicaZ, TelosB, CC2420
	DM	Replay Attack	IEEE	ZED			
[84]	DM	Packet-in-Packet Attack	IEEE	All	Simulated	KillerBee, Z-Monitor	TelosB, GoodFET

Table 3
Review of the Attacks based on Vulnerabilities, Attacks and Countermeasures.
(RC: Reconnaissance, DM: Device Manipulation, DoS: Denial of Service, NC: Network Control)

Pub.	VAC#	Type	VAC name	Vulnerability (V)	Attack (A)	Countermeasure (C)
[66]	VAC01	DoS	Communication Interruption	Negative effects with a combination of clusters, attributes and commands in the Zigbee Cluster Library (ZCL)	Suppress communication from Zigbee devices	Standardize the processing of packets with attributes, commands or clusters that are not defined
	VAC02	DoS	Disconnection	NWK and APS commands for routing and control services	Make the target to disconnect from the network	1-Controller and device use network status command to check connection status 2-Controller checks device information regularly
	VAC03	RC	Key Leakage	Security information transmission controlled by the APS layer	Make vulnerable devices give away security information such as network key	Consider a distinct security key and put key management load on controller
	VAC04	DM	Improper Integrity Check	Improper integrity check in the NWK layer	Manipulate packet integrity code to put target in abnormal state	Redefine the authentication code with more flexible lengths
	VAC05	DoS	Truncated Packet	Incomplete payload of truncated packets with NWK layer	Delay data transmission by making response lagging on target	Standardize the minimum NWK packet length threshold
[67]	VAC06	RC	Signal Eavesdropping	Wireless nature of the Zigbee protocol	Eavesdrop on the communication between devices	
	VAC07	DM	Signal Emulation	Lack of verification of sequence numbers and frame counters	Generate a signal that is similar to the eavesdropped one	Mislead WiFi attacker to emulate imperfect signal
[68]	VAC08	DoS	Capacity Exploitation	Due to trust center rejoin process, unencrypted rejoin request packet is accepted by parent node	Create multiple phantom nodes that send trust center rejoin requests to legitimate parent node and make unauthorized connections	
	VAC09	DoS	Offline Attack	Inconsistent recognition of device properties	Cause inconsistency problem and disable normal communication between legitimate nodes	
	VAC10	RC	Network Key Leakage Attack	Accepting publicly available link keys	Send rejoin request to TC and sniff relies from parent node	
	VAC11	NC	Hijacking Attack	V10	Hijack the end device by connecting it to a phantom device	
[69]	VAC12	RC	Mapping the Network	Unencrypted Network Header	Infer the number and type of nodes from the header fields	
	VAC13	RC	Device and Event Identification	Traffic burst generated by user event includes functionality APL command	Infer the APL command in traffic burst generated from user event to identify device or event from encrypted wireless packets	1-Mandate using chipset manufacturer's identifier to hide their identity 2-Payload length obfuscation
	VAC14	RC	Device Identification	Periodic report patterns of the device's network traffic	Generate fingerprint for devices from periodic patterns to identify events	1-ZC or ZRs transmit decoy packets at random intervals 2-Generate similar periodic pattern for all devices
[70]	VAC15	DoS	Low-rate DoS with Sink Node	Buffer management, indirect transmission and insecure rejoin	Send attack packets to a malicious sink node to fill up the ZR's buffer	Change buffer management algorithm
	VAC16	DoS	Low rate DoS without Sink Node	V15	Send attack packets to the target device to overwhelm the ZR's buffer	Use Random Drop on Full Algorithm

(*continued on next page*)

6. Zigbee attack chain study

Many of the attacks proposed in the literature do not have a simple step to follow and execute. There are several attacks that can only be conducted with certain initialization. In other words, each vulnerability leads to an attack that will in turn lead to another attack with another vulnerability. We study these sequential attack dependencies – attack chains – to have a graphical overview of the flow of each attack. This study will help the reader understand how to perform attacks in a sequence to open new windows to other vulnerabilities and attacks. To this end, we use the insights gained from the two previous sections – classification and review – to demonstrate these attack chains in Fig. 8. In this figure, there are three levels of attack, each of which depend on a vulnerability and the previous attack, if applicable. Each level of attack starts with a vulnerability that will lead to an attack with one of the four attack types we have identified in Section 4.

Table 3 (*continued*).

Pub.	VAC#	Type	VAC name	Vulnerability (V)	Attack (A)	Countermeasure (C)
[71]	VAC17	RC	User Privacy Leakage	Using a single common NWK key to encrypt all network traffic	Decrypt every message transmitted inside the target network with the common key and access the data	1-Minimize use of network key 2-Introduce link keys for certain coordinator-device communications 3-Use Elliptic Curve Diffie–Hellman (ECDH)-based schemes during the join procedure
	VAC18	NC	User Device Control	V17	Impersonate the coordinator and use the NWK key to send packets to target devices	C17
	VAC19	RC	Fake Device Injection	1-ZC does not authenticate joining devices 2-TCLK is publicly available	Use an impersonated device to connect to the network	Improve the installation code mechanism by introducing asymmetric encryption scheme
[72]	VAC20	DM	Replay Attack	Weak message authentication mechanisms against replay attacks	Remove noise from the captured replay packet to deceive the device and get past the integrity check	
[73]	VAC21	RC	Active Node Identification	1-Only ZRs and the ZC reply to Beacon Requests 2-Lack of security services in the MAC layer	Identify all ZRs that are within communication range by injecting a Beacon Request	
	VAC22	RC	Passive Node Identification	1-A ZED periodically transmits Data Requests to its parent node to poll for pending frames 2-The NWK header is not encrypted	Identify node types based on their relationship with Data Requests	
	VAC23	RC	Hardware Device Identification	1-Publicly available list of verified Zigbee devices 2-Lists of supported devices by hub vendors	Identify the hardware device from its OUI as a keyword to query on the available registries	
	VAC24	RC	Legacy Device Identification	Many legacy devices do not handle end-device timeout request/response	Make ZEDs rejoin their network in order to observe the End Device Timeout Requests/Responses	
	VAC25	RC	Network Command Identification	Unencrypted IEEE 802154 header fields	Identify the network commands using the proposed decision tree	
	VAC26	DoS	Key-Transport Attack	Insecure transportation of the insufficiently protected network key to the new devices	Extract the NWK key by intercepting the packets of touchlink commissioning	
[74]	VAC27	RC	Active Device Scan	The 2.4 GHz ISM band's channels 11 through 26 used by Zigbee	Search for the devices in the proximity of the attacker's device	
	VAC28	DM	ACK Spoofing	If devices do not receive an ACK during a specified time window, they leave the communication	Impersonate an existing Zigbee device by sending the 64-bit source identifier of the scan request to that of the device being spoofed	
	VAC29	DM	Identify-Action Attack	The touchlink commissioning process enables the device to identify itself using an identify action defined in advance	Send an identify request to the target device who starts its identify action for a specific window of time	
	VAC30	DoS	Reset to Factory-New Attack	Lack of proper frame protection mechanisms	The attacker resets the configuration of a device to the state of the factory	
	VAC31	DoS	Permanent Disconnect Attack	Lack of proper frame protection mechanisms	Change the wireless channel by sending an NWK update request making the device leave the network	
	VAC32	NC	Hijack Attack	Lack of proper frame protection mechanisms	Force the target device to use a network key selected by the attacker	
	VAC33	RC	Network Key Extraction	Leakage of the touchlink preconfigured link key	Extract the current network key by eavesdropping on the request/response packets of a primary touchlink commissioning	

(*continued on next page*)

Table 3 (*continued*).

Pub.	VAC#	Type	VAC name	Vulnerability (V)	Attack (A)	Countermeasure (C)
[75]	VAC34	DM	Persistence of Code Execution	Safeguard the firmware update procedure using a single cryptographic key that is shared by many devices	Create a valid malicious software update	1-Using unique keys per bulb 2-Using asymmetric cryptography for the software verification
	VAC35	DM	Breaking Cryptographic Bootloader	The hardware is susceptible to side-channel analysis	Using Differential Power Analysis (DPA) and Correlation Power Analysis to break the AES hardware accelerator	Make sure the loss of a key from one device does not affect the entire network
	VAC36	NC	Takeover Attack	Implementation errors of procedures designed to impede the take-over attack from long distances away from the network	Make the target device undergo a factory reset and join the malicious network	Negative testing in the Zigbee certification process
[65]	VAC37	RC	Key Sniffing	V26	A26	Out-of-band key loading method
	VAC38	DoS	Association Flooding	Lack of proper DoS protection mechanisms	Induce an encrypted Network Key transport without requiring the owner to be adding a new device	Secure network admission
	VAC39	DM	Replay Attack	Lack of proper frame protection mechanisms	Injecting previously encrypted and transmitted messages on the network to induce devices to perform commands	
	VAC40	RC	Device Spoofing	Lack of proper frame protection mechanisms	Impersonate a device with a known address and broadcast requests to join the network to induce a key-transport	Dynamic device ID rotation
[76]	VAC41	DoS	Ghost-in-Zigbee	Unencrypted MAC header fields	Send several bogus messages to involve the receiver with superfluous security calculations to consume a large amount of power, leading to the battery depletion of the recipient	1-Develop neighbor monitoring-based techniques and attacker localization 2-Add another layer of a challenge-response process
	VAC42	DoS	High Computational Load	V41	Send a number of fake messages to rapidly empty the energy of the target device and therefore, stop the device from providing services	
	VAC43	DoS	MAC Misbehavior	The inherent characteristics of the IEEE 802.15.4 CSMA/CA protocol with regard to sensing the channels and its contention-based access	Continuously send the crafted traffic to the target device in the proximity of the device to deprive the device of accessing the channel	
	VAC44	DoS	Post-Depletion Replay	Possibility of a replay attack after 2^{32} frames due to the adoption of a 4-Byte counter	Replay packets with a frame counter larger than the current amount so that messages from legitimate devices will be rejected	
	VAC45	DM	Replay Attack	In case no certain controls are put in place, the node will end up with an empty ACL table with all the nonces or counters reset after a battery depletion attack	Replay intercepted packets after the frame counter reset	
	VAC46	RC	Loss of Confidentiality	Messages destined for the devices in the next hop are encrypted by XORing the plaintext with the encryption key	The XOR of two captured ciphertexts will lead to the XOR of the corresponding plaintexts	
[77]	VAC47	NC	Wormhole Attack	Inherent properties of the Wireless Sensor Networks (WSN)	The attacking nodes create a false realization that two devices at different parts of the network are connected via a few neighbors, thus luring the traffic of the network to their fake route	Optimized watchdog trust system
[79]	VAC48	NC	Sybil Attack	Inherent properties of the Wireless Sensor Networks (WSN)	The attacking device illegally asserts multiple identities and it creates many unreal identities	Address and distance validation of nodes in the trust center

(*continued on next page*)

Table 3 (*continued*).

Pub.	VAC#	Type	VAC name	Vulnerability (V)	Attack (A)	Countermeasure (C)
[78]	VAC49	NC	Sinkhole Attack	Inherent properties of the Wireless Sensor Networks (WSN)	The attacking device in the network starts sending false data about its routing properties, pretending to have a really good path to the ZC	
[80]	VAC50	RC	Physical Attack	Passwords are saved unencrypted in memory	Get access to the device physically and extract a copy of its memory to find the key	1-Put devices in tamper resistant boxes 2-Auto-delete of the memory by the device after detection of an attempt to attack
	VAC51	RC	Same-Nonce Attack	V46	A46	Store the nonce states in nonvolatile memory and recover them after each power failure
	VAC52	DoS	DoS Attack	Lack of proper DoS protection mechanisms	Resend intercepted packets at a rate of 30 packets per second After 250 s and 7442 frames of attack, the coordinator stops reacting	The change of transmission channel after receiving a hundred duplicate packets
	VAC53	DM	Replay Attack	Sequence numbers are reset to zero after a specific number	Intercept packets with a larger sequence number and replay it after a sequence number reset	Use a trust center or several keys
[81]	VAC54	RC	Network Discovery	ZEDs will send a beacon request on the channel for network discovery In response, ZC and ZRs will respond by disclosing network configuration information	Zigbee networks in proximity and all configuration details of their legitimate devices can be found	
	VAC55	RC	Interception of Packets	Many Zigbee networks do not provide encryption at all	The attacker listens to the network traffic and abuses the captured information for further hostile purposes	
	VAC56	DM	Replay Attack	Lack of proper replay protection mechanisms	Retransmit the frames with a pre-specified delay without acknowledgment, thereby preserving the true integrity of the packets	Integrate timestamping mechanism to the encryption process
[82]	VAC57	DoS	End-Device Sabotage Attack	Reliance of ZEDs on a parent device to stay awake and retrieve messages	Cause power failures to the devices due to the pre-defined polling rate and the energy leakage during each wake-up	
	VAC58	RC	Network Key Sniffing	If choosing the Standard Security mode, the TC transmits the current NWK key unencrypted wirelessly toward the devices when they try to connect to the network	Sniff the traffic during commissioning and intercept the network key	Remove standard security from Zigbee specification
[83]	VAC59	DoS	Association Flooding Attack	Unencrypted MAC header fields	Flood the ZC with fake association packets from non-existent devices	
	VAC60	DM	Replay Attack	Lack of proper replay protection mechanisms	If an adversary sends many packets with high-numbered counters to a victim device, other devices utilizing the replay protection scheme will drop the correct packets with small counters from other devices	Wireless Sensor Network (WSN) Intrusion Detection System (IDS)
[84]	VAC61	DM	Packet-in-Packet Attack	Inherent properties of the PHY layer	When bit errors randomly occur in communication, the attacker is able to exploit them to transmit managed frames when they happen in a specific way	Byte Stuffing

7. Evaluation study for future research development

One of the concerns that the authors had during paper reviews was to conduct a study on how each attack proposed in a paper can be implemented for further development of Zigbee vulnerability assessments for future research. Therefore, in this part, we outline the evaluation study of the reviewed works. To this end, we propose three criteria to analyze the security assessment procedures introduced. The overview of the evaluation is shown in Fig. 9.

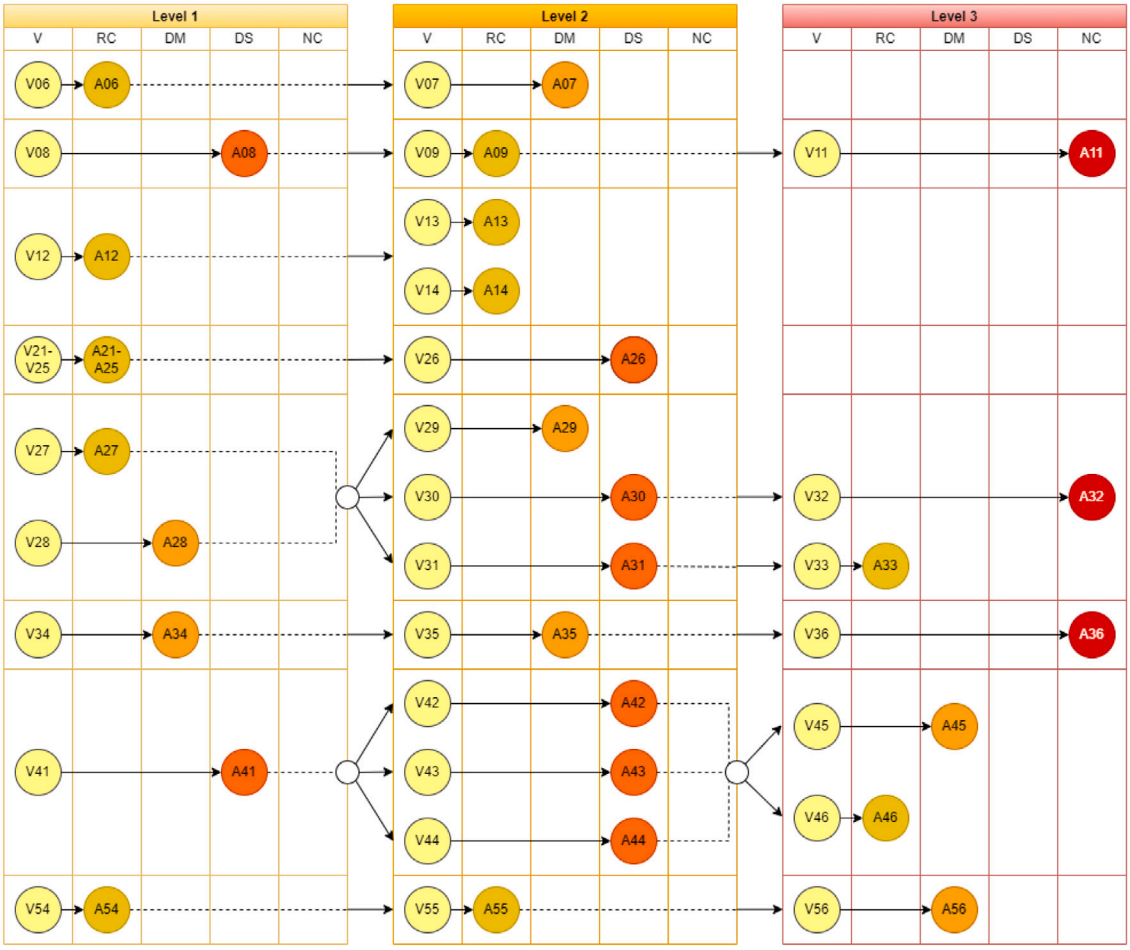


Fig. 8. Overview of the Zigbee Attack Chain Study.

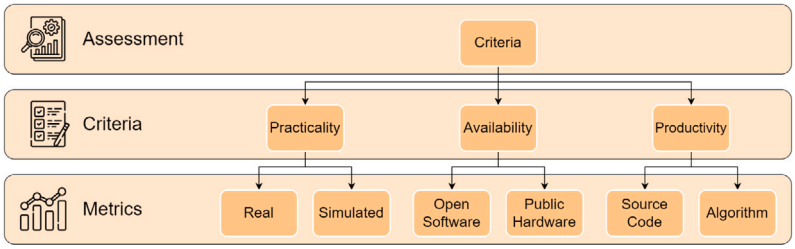


Fig. 9. Overview of the Evaluation Criteria and Metrics.

7.1. Evaluation criteria and metrics

After analyzing the Zigbee attack papers extensively, we found several criteria and metrics to be important in terms of the future development of the proposed attacks. We analyzed the papers based on metrics related to implementation, evaluation and Contribution. A detailed explanation of these metrics is as follows:

- **Practicality:** This criterion refers to how much the implementation is close to a real-world scenario. Some works implemented their approach on real devices and some on simulated devices. For this criteria, we consider the following two metrics: Real and Simulated.
- **Availability:** Availability deals with whether the authors have used software and/or hardware tools that are open-source and/or publicly available, leading to the two following metrics: Open Software and Public Hardware.

Table 4
Evaluation criteria.

Criteria	Metric
Practicality	Uses real devices Uses simulated devices Does not implement the attack(s) proposed
Availability	Uses open-source software Uses publicly-available hardware Does not use any of the above
Productivity	Provides software, tools, source-code, etc. Provides algorithm, pseudo-code, flowchart etc. Does not provide any of the above

Table 5
Results of evaluation study.

Publication	Practicality		Availability		Productivity	
	Real	Simulated	Open software	Public hardware	Source code	Algorithm
Wang et al. [66]	✓		✓	✓		✓
Zhang et al. [67]	✓		✓	✓		✓
Wang et al. [68]	✓		✓	✓	✓	
Shafqat et al. [69]	✓			✓		✓
Okada et al. [70]		✓				
Wang et al. [71]		✓	✓	✓		
Wara et al. [72]	✓		✓	✓		
Akestoridis et al. [73]	✓		✓	✓	✓	
Morgner et al. [74]	✓		✓	✓	✓	
Ronen et al. [75]	✓		✓	✓	✓	
Fan et al. [65]	✓		✓	✓		
Cao et al. [76]		✓	✓	✓		
Jegan et al. [77]		✓	✓			
Coppolino et al. [78]		✓				
Thaur et al. [79]						
Vdurech et al. [80]		✓	✓	✓		
Olawumi et al. [81]		✓	✓	✓		
Vidgren et al. [82]		✓	✓	✓		
Stelte et al. [83]		✓	✓	✓		✓
Biswas et al. [84]		✓	✓	✓		

- **Productivity:** This criterion is concerned with the fact that the paper has provided software, source-code, pseudo-code, algorithm, etc. and includes two metrics: Source Code and Algorithm.

We summarize the criteria and metrics for our evaluation study in Table 4.

Finally, we analyze the papers based on the proposed metrics. Table 5 shows an overview of the reviewed papers signifying how each paper can be used for further research development.

8. Conclusion, open challenges and future work

The internet of things has become a game changer in many applications from normal everyday use cases to critical situations. Zigbee, as one of the most prominent IoT protocols, has been adopted in many applications that require low-rate transmissions. The security of this technology has been under extensive study in academia and this, in turn, has helped mitigate many security vulnerabilities in Zigbee devices and networks. In this survey, we extensively analyzed papers in which the authors found vulnerabilities and exploited them to conduct different attacks and proposed different countermeasures to mitigate them.

Zigbee networks, widely used in IoT applications, face significant security challenges, particularly regarding key management. Inherent weaknesses in the protocol create opportunities for attackers to exploit vulnerabilities and execute damaging attacks. A primary issue lies in the extraction of encryption keys, which can further expose the network to a variety of malicious activities; a passive eavesdropper can potentially extract the network key by intercepting and analyzing transmitted data. This is usually achieved by monitoring and recording communication between devices without detection. The eavesdropper captures the initial key exchange that takes place when a new device joins the network. During this process, the network key is encrypted using the trust center's link key or the default global trust center link key before being transmitted to the new device. An attacker with knowledge of the default key can easily decrypt the network key, gaining unauthorized access to the network and its data. Once an attacker has successfully extracted the network key, they can perform a variety of attacks, including eavesdropping on all communications, injecting malicious data packets, and launching denial-of-service (DoS) attacks. These actions can significantly compromise the network's confidentiality, integrity, and availability. As such, developing robust strategies to mitigate these vulnerabilities is crucial for ensuring the security and integrity of Zigbee networks, regardless of the existing security measures in place.

One of the commonly exploited vulnerabilities in Zigbee networks is the susceptibility to denial-of-service (DoS) attacks, which can lead to battery depletion and render devices vulnerable to other damaging attacks. Among these DoS attacks, the PANID (Personal Area Network Identifier) conflict attack and battery depletion attack are particularly noteworthy. In a PANID conflict attack, an attacker impersonates the Zigbee network coordinator and sends a beacon frame with the same PANID as the target network but with a different extended PANID. This causes confusion among the devices in the network, forcing them to either join the fake network or continuously search for the legitimate coordinator, ultimately leading to a disrupted network operation. The battery-powered devices in the network may also experience rapid power depletion as they continuously search for the original network, rendering them non-operational. A battery depletion attack, on the other hand, specifically targets the battery life of devices in the network. The attacker floods the network with a large number of data packets, forcing devices to expend energy processing these packets. This not only disrupts the normal functioning of the network but also drains the battery of the targeted devices at a faster rate. Once a device's battery is depleted, it can no longer perform its intended functions or participate in network communications, leaving it susceptible to further attacks. Investigating detection and mitigation strategies against such attacks would be a valuable direction for future research in order to enhance the security and resilience of Zigbee networks.

The observant reader may notice that contemporary devices have become significantly more secure than their predecessors, thanks to advancements in security measures. However, there remain two crucial challenges that warrant attention. Firstly, many manufacturers opt for the bare minimum security measures in order to reduce production costs, which inadvertently leaves devices more susceptible to attacks, irrespective of the actual security capabilities of the Zigbee protocol. Secondly, a substantial number of legacy devices already in use predate the implementation of certain security measures, making them prone to exploitation due to outdated or vulnerable firmware update mechanisms. Given these concerns, addressing the security of vulnerable devices in the network, whether they are legacy devices or those with minimal security measures, presents a valuable research opportunity. One potential approach involves developing and implementing network-wide security policies that enforce mandatory security updates and promote the use of robust security features across all devices, regardless of their age or inherent security capabilities. This would entail designing secure firmware update mechanisms that can seamlessly patch vulnerabilities in both legacy and newer devices.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article

Acknowledgments

The authors would like to thank the Canadian Institute for Cybersecurity (CIC) for financial and educational support. This project was also supported partly by collaborative research funding from the National Research Council of Canada's Artificial Intelligence for Logistics Program.

References

[1] M. Safi, S. Dadkhah, F. Shoeleh, H. Mahdikhani, H. Molyneaux, A.A. Ghorbani, A survey on IoT profiling, fingerprinting, and identification, ACM Trans. Internet Things (2022).
[2] S. Dadkhah, H. Mahdikhani, P.K. Danso, A. Zohourian, K.A. Truong, A.A. Ghorbani, Towards the development of a realistic multidimensional IoT profiling dataset, in: 2022 19th Annual International Conference on Privacy, Security & Trust, PST, IEEE, 2022, pp. 1–11.
[3] A. Khanna, S. Kaur, Internet of things (IoT), applications and challenges: a comprehensive review, Wirel. Pers. Commun. 114 (2) (2020) 1687–1762.
[4] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646.
[5] V. Albino, U. Berardi, R.M. Dangelico, Smart cities: Definitions, dimensions, performance, and initiatives, J. Urban Technol. 22 (1) (2015) 3–21.
[6] A. Vij, S. Vijendra, A. Jain, S. Bajaj, A. Bassi, A. Sharma, IoT and machine learning approaches for automation of farm irrigation system, Procedia Comput. Sci. 167 (2020) 1250–1257.
[7] A. Adeel, M. Gogate, S. Farooq, C. Ieracitano, K. Dashtipour, H. Larijani, A. Hussain, A survey on the role of wireless sensor networks and IoT in disaster management, Geol. Disaster Monit. Based Sensor Netw. (2019) 57–66.
[8] M. Irfan, H. Jawad, B.B. Felix, S.F. Abbasi, A. Nawaz, S. Akbarzadeh, M. Awais, L. Chen, T. Westerlund, W. Chen, Non-wearable IoT-based smart ambient behavior observation system, IEEE Sens. J. 21 (18) (2021) 20857–20869.
[9] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190.
[10] S. Safaric, K. Malaric, ZigBee wireless standard, in: Proceedings ELMAR 2006, IEEE, 2006, pp. 259–262.
[11] C. Paetz, Z-Wave Essentials, eBook Partnership, 2017.
[12] J. Haxhibeqiri, E. De Poorter, I. Moerman, J. Hoebeke, A survey of LoRaWAN for IoT: From technology to application, Sensors 18 (11) (2018) 3995.
[13] A. Lavric, A.I. Petrariu, V. Popa, SigFox communication protocol: The new era of IoT? in: 2019 International Conference on Sensing and Instrumentation in IoT Era, ISSI, IEEE, 2019, pp. 1–4.
[14] S.R. Borkar, Long-term evolution for machines (LTE-M), in: LPWAN Technologies for IoT and M2M Applications, Elsevier, 2020, pp. 145–166.
[15] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, A. Ghosh, NB-IoT system for M2M communication, in: 2016 IEEE Wireless Communications and Networking Conference, IEEE, 2016, pp. 1–5.
[16] T.G. Zimmerman, Personal area networks: Near-field intrabody communication, IBM Syst. J. 35 (3.4) (1996) 609–617.
[17] K. Mekki, E. Bajic, F. Chaxel, F. Meyer, A comparative study of LPWAN technologies for large-scale IoT deployment, ICT Express 5 (1) (2019) 1–7.

[18] D. De Guglielmo, S. Brienza, G. Anastasi, IEEE 802.15. 4e: A survey, Comput. Commun. 88 (2016) 1–24.
[19] A. Rizzardi, S. Sicari, A. Coen-Porisini, Analysis on functionalities and security features of Internet of Things related protocols, Wirel. Netw. (2022) 1–31.
[20] N. Lata, R. Kumar, Communication technologies, smart home solution and security trends in internet of things, J. Algebraic Stat. 13 (1) (2022) 42–61.
[21] H. Pirayesh, H. Zeng, Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey, IEEE Commun. Surv. Tutor. (2022).
[22] J. Tournier, F. Lesueur, F. Le Mouël, L. Guyon, H. Ben-Hassine, A survey of IoT protocols and their security issues through the lens of a generic IoT stack, Internet Things 16 (2021) 100264.
[23] K. Lounis, M. Zulkernine, Attacks and defenses in short-range wireless technologies for IoT, IEEE Access 8 (2020) 88892–88932.
[24] G. Kambourakis, C. Kolias, D. Geneiatakis, G. Karopoulos, G.M. Makrakis, I. Kounelis, A state-of-the-art review on the security of mainstream IoT wireless PAN protocol stacks, Symmetry 12 (4) (2020) 579.
[25] H. Mrabet, S. Belguith, A. Alhomoud, A. Jemai, A survey of IoT security based on a layered architecture of sensing and data analysis, Sensors 20 (13) (2020) 3625.
[26] R. Yugha, S. Chithra, A survey on technologies and security protocols: Reference for future generation IoT, J. Netw. Comput. Appl. 169 (2020) 102763.
[27] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2702–2733.
[28] M. Burhan, R.A. Rehman, B. Khan, B.-S. Kim, IoT elements, layered architectures and security issues: A comprehensive survey, Sensors 18 (9) (2018) 2796.
[29] S. Marksteiner, V.J.E. Jiménez, H. Valiant, H. Zeiner, An overview of wireless IoT protocol security in the smart home domain, in: 2017 Internet of Things Business Models, Users, and Networks, IEEE, 2017, pp. 1–8.
[30] P. Datta, B. Sharma, A survey on IoT architectures, protocols, security and smart city based applications, in: 2017 8th International Conference on Computing, Communication and Networking Technologies, ICCCNT, IEEE, 2017, pp. 1–5.
[31] R. Krejčí, O. Hujňák, M. Švepeš, Security survey of the IoT wireless protocols, in: 2017 25th Telecommunication Forum, TELFOR, IEEE, 2017, pp. 1–4.
[32] M. Gupta, S. Singh, A survey on the zigbee protocol, it's security in internet of things (iot) and comparison of zigbee with bluetooth and wi-fi, in: Applications of Artificial Intelligence in Engineering, Springer, 2021, pp. 473–482.
[33] N. Sidhu, M. Sachdeva, A comprehensive study of routing layer intrusions in zigbee based wireless sensor networks, Int. J. Adv. Sci. Technol. 29 (3) (2020) 514–524.
[34] S. Khanji, F. Iqbal, P. Hung, ZigBee security vulnerabilities: Exploration and evaluating, in: 2019 10th International Conference on Information and Communication Systems, ICICS, IEEE, 2019, pp. 52–57.
[35] T. Kumar, P. Mane, ZigBee topology: A survey, in: 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies, ICCICCT, IEEE, 2016, pp. 164–166.
[36] J.M. Varghese, K. Nibi, V.T. Varghese, S. Rao, A survey of the state of the art in ZigBee, Int. J. Cybern. Inf. 4 (2) (2015) 145–155.
[37] O.G. Aju, A survey of zigbee wireless sensor network technology: Topology, applications and challenges, Int. J. Comput. Appl. 130 (9) (2015) 47–55.
[38] Z.A. Davani, A.A. Manaf, A survey on key management of ZigBee network, in: Proceedings of the International Conference on E-Technologies and Business on the Web (EBW'2013), Bangkok, Thailand, Citeseer, 2013, pp. 7–9.
[39] P. Baronti, P. Pillai, V.W. Chook, S. Chessa, A. Gotta, Y.F. Hu, Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards, Comput. Commun. 30 (7) (2007) 1655–1695.
[40] Z. Alliance, Zigbee alliance, WPAN Industry Group, 2010, http://www.zigbee.org/, the Industry Group Responsible for the ZigBee Standard and Certification.
[41] C.M. Ramya, M. Shanmugaraj, R. Prabakaran, Study on ZigBee technology, in: 2011 3rd International Conference on Electronics Computer Technology, 6, IEEE, 2011, pp. 297–301.
[42] N.A. Somani, Y. Patel, Zigbee: A low power wireless technology for industrial applications, Int. J. Control Theory Comput. Modell. 2 (3) (2012) 27–33.
[43] P. Li, J. Li, L. Nie, B. Wang, Research and application of zigbee protocol stack, in: 2010 International Conference on Measuring Technology and Mechatronics Automation, Vol. 2, IEEE, 2010, pp. 1031–1034.
[44] S.C. Ergen, ZigBee/IEEE 802.15. 4 Summary, Vol. 10, No. 17, UC Berkeley, 2004, p. 11, September.
[45] M. Zhou, Z.-l. Nie, Analysis and design of ZigBee MAC layers protocol, in: 2010 International Conference on Future Information Technology and Management Engineering, Vol. 2, IEEE, 2010, pp. 211–215.
[46] W. Wang, G. He, J. Wan, Research on Zigbee wireless communication technology, in: 2011 International Conference on Electrical and Control Engineering, IEEE, 2011, pp. 1245–1249.
[47] W.-C. Park, M.-H. Yoon, The implementation of indoor location system to control ZigBee home network, in: 2006 SICE-ICASE International Joint Conference, IEEE, 2006, pp. 2158–2161.
[48] R.-C. Wang, R.-S. Chang, H.-C. Chao, Internetworking between ZigBee/802.15. 4 and IPv6/802.3 network, SIGCOMM Data Commun. Festiv. (2007).
[49] O. Hersent, D. Boswarthick, O. Elloumi, Zigbee, Wiley Telecom, 2012.
[50] A. Tomar, Introduction to ZigBee technology, Glob. Technol. Centre 1 (2011) 1–24.
[51] S. Ondrej, B. Zdenek, F. Petr, H. Ondrej, Zigbee technology and device design, in: International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, ICNICONSMCL'06, IEEE, 2006, p. 129.
[52] P. Dhillon, H. Sadawarti, A review paper on zigbee (ieee 802.15. 4) standard, Int. J. Eng. Res. Technol. 3 (2014).
[53] Z. Xiaojing, L. Yuanguai, Zigbee implementation in intelligent agriculture based on internet of things, in: 2nd International Conference on Electronic & Mechanical Engineering and Information Technology, Atlantis Press, 2012, pp. 1842–1846.
[54] I. Poole, What exactly is ZigBee? Commun. Eng. 2 (4) (2004) 44–45.
[55] F. Ijaz, A.A. Siddiqui, B.K. Im, C. Lee, Remote management and control system for LED based plant factory using ZigBee and Internet, in: 2012 14th International Conference on Advanced Communication Technology, ICACT, IEEE, 2012, pp. 942–946.
[56] M.-S. Pan, H.-W. Fang, Y.-C. Liu, Y.-C. Tseng, Address assignment and routing schemes for ZigBee-based long-thin wireless sensor networks, in: VTC Spring 2008-IEEE Vehicular Technology Conference, IEEE, 2008, pp. 173–177.
[57] F. Sadikin, T. Van Deursen, S. Kumar, A ZigBee intrusion detection system for IoT using secure and efficient data collection, Internet Things 12 (2020) 100306.
[58] T. Zillner, S. Strobl, ZigBee exploited: The good, the bad and the ugly, 2015, Black Hat–2015. Available Online: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf. (Accessed 21 March 2018).
[59] E. Yüksel, H.R. Nielson, F. Nielson, Zigbee-2007 security essentials, in: Proc. 13th Nordic Workshop on Secure IT-Systems, 2008, pp. 65–82.
[60] H. Li, Z. Jia, X. Xue, Application and analysis of ZigBee security services specification, in: 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Vol. 2, IEEE, 2010, pp. 494–497.
[61] M. Qianqian, B. Kejin, Security analysis for wireless networks based on ZigBee, in: 2009 International Forum on Information Technology and Applications, Vol. 1, IEEE, 2009, pp. 158–160.
[62] J. Sun, X. Zhang, Study of ZigBee wireless mesh networks, in: 2009 Ninth International Conference on Hybrid Intelligent Systems, Vol. 2, IEEE, 2009, pp. 264–267.
[63] P. Radmand, M. Domingo, J. Singh, J. Arnedo, A. Talevski, S. Petersen, S. Carlsen, ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys, in: 2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, IEEE, 2010, pp. 465–470.

[64] K. Choi, M. Yun, K. Chae, M. Kim, An enhanced key management using ZigBee Pro for wireless sensor networks, in: The International Conference on Information Network 2012, IEEE, 2012, pp. 399–403.
[65] X. Fan, F. Susan, W. Long, S. Li, Security analysis of zigbee, MWR InfoSecur. 2017 (2017) 1–18.
[66] X. Wang, S. Hao, Don't kick over the beehive: attacks and security analysis on zigbee, in: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, 2022, pp. 2857–2870.
[67] X. Zhang, S. Yu, H. Zhou, P. Huang, L. Guo, M. Li, Signal emulation attack and defense for smart home IoT, IEEE Trans. Dependable Secure Comput. (2022).
[68] J. Wang, Z. Li, M. Sun, J.C. Lui, Zigbee's network rejoin procedure for IoT systems: vulnerabilities and implications, in: Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses, 2022, pp. 292–307.
[69] N. Shafqat, D.J. Dubois, D. Choffnes, A. Schulman, D. Bharadia, A. Ranganathan, Zleaks: Passive inference attacks on zigbee based smart homes, in: International Conference on Applied Cryptography and Network Security, Springer, 2022, pp. 105–125.
[70] S. Okada, D. Miyamoto, Y. Sekiya, H. Nakamura, New ldos attack in zigbee network and its possible countermeasures, in: 2021 IEEE International Conference on Smart Computing, SMARTCOMP, IEEE, 2021, pp. 246–251.
[71] W. Wang, F. Cicala, S.R. Hussain, E. Bertino, N. Li, Analyzing the attack landscape of Zigbee-enabled IoT systems and reinstating users' privacy, in: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2020, pp. 133–143.
[72] M.S. Wara, Q. Yu, New replay attacks on zigbee devices for internet-of-things (iot) applications, in: 2020 IEEE International Conference on Embedded Software and Systems, ICESS, IEEE, 2020, pp. 1–6.
[73] D.-G. Akestoridis, M. Harishankar, M. Weber, P. Tague, Zigator: Analyzing the security of zigbee-enabled smart homes, in: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2020, pp. 77–88.
[74] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, F. Armknecht, Insecure to the touch: attacking ZigBee 3.0 via touchlink commissioning, in: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2017, pp. 230–240.
[75] E. Ronen, A. Shamir, A.-O. Weingarten, C. O'Flynn, IoT goes nuclear: Creating a ZigBee chain reaction, in: 2017 IEEE Symposium on Security and Privacy, SP, IEEE, 2017, pp. 195–212.
[76] X. Cao, D.M. Shila, Y. Cheng, Z. Yang, Y. Zhou, J. Chen, Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks, IEEE Internet Things J. 3 (5) (2016) 816–829.
[77] G. Jegan, P. Samundiswary, Wormhole attack detection in zigbee wireless sensor networks using intrusion detection system, Indian J. Sci. Technol. 9 (45) (2016) 1–10.
[78] L. Coppolino, V. D'Alessandro, S. D'Antonio, L. Levy, L. Romano, My smart home is under attack, in: 2015 IEEE 18th International Conference on Computational Science and Engineering, IEEE, 2015, pp. 145–151.
[79] P. Thakur, R. Patel, N. Patel, A proposed framework for protection of identity based attack in ZigBee, in: 2015 Fifth International Conference on Communication Systems and Network Technologies, IEEE, 2015, pp. 628–632.
[80] J. Ďurech, M. Franeková, Security attacks to ZigBee technology and their practical realization, in: 2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics, SAMI, IEEE, 2014, pp. 345–349.
[81] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, P. Toivanen, Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned, in: 2014 14th International Conference on Hybrid Intelligent Systems, IEEE, 2014, pp. 199–206.
[82] N. Vidgren, K. Haataja, J.L. Patino-Andres, J.J. Ramirez-Sanchis, P. Toivanen, Security threats in ZigBee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned, in: 2013 46th Hawaii International Conference on System Sciences, IEEE, 2013, pp. 5132–5138.
[83] B. Stelte, G.D. Rodosek, Thwarting attacks on ZigBee-Removal of the KillerBee stinger, in: Proceedings of the 9th International Conference on Network and Service Management, CNSM 2013, IEEE, 2013, pp. 219–226.
[84] A. Biswas, A. Alkhalid, T. Kunz, C.-H. Lung, A lightweight defence against the packet in packet attack in ZigBee networks, in: 2012 IFIP Wireless Days, IEEE, 2012, pp. 1–3.