International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 8, No.2 (Mar-2019)

http://dx.doi.org/10.12785/ijcds/080202

Evaluating Security of Low-Power Internet of Things Networks

Ivan Vaccari[1], Enrico Cambiaso[1] and Maurizio Aiello[1]

[1] *National Research Council (CNR), IEIIT Institute, via De Marini, 6 - 16149 - Genova, Italy*

Received 5 Dec. 2018, Revised 3 Feb. 2019, Accepted 20 Feb. 2019, Published 1 Mar. 2019

Abstract: Internet of Things (IoT) is one of the most prominent technologies on the Internet. Simple objects gain the ability to store, process and exchange information among themselves or with external entities, by observing and controlling the environment. Thanks to the rapid development of this innovation, IoT opens possibilities to a huge number of objects and applications that promise to improve our daily life. The main scenarios of the development of IoT are home automation/domestic and Industrial IoT. According to such scenarios, several applications could be implemented: from smart thermostats, light bulbs, refrigerators, ovens, door window sensors to volumetric, flow, heat and connected data processing devices. Since this is a new phenomenon, it has not yet been studied and analyzed for its entirety, also due to the lack of a definitive standard that can provide an overview of these devices. The objective of this paper is to implement different well-known attacks against IoT networks, by adopting the ZigBee communication protocol to analyze devices and network security. For our aim, we have considered different scenarios involving an attacker aiming to dismantle the IoT network (jamming, flooding DoS), retrieve sensitive information (sniffing, brute force password crack) and to actively communicate on the network to impersonate legitimate nodes (replay). Such exploitation provides us the ability to analyze the effects of attacks designed to target common wireless networks, when they are perpetrated against IoT environments. Obtained results prove that IoT devices and networks (often embedded in sensitive environments such as hospitals or critical infrastructures) are vulnerable to several attacks.

Keywords: Internet of Things, ZigBee, Wireless Sensor Network, Cyber-attack, Cyber-Security, Network Security

1. Introduction

Internet of Things (IoT) is a recent and emerging phenomenon that allows common use devices to communicate on the Internet. Although IoT devices are not widely adopted yet, it is assumed that, by 2020, approximately 24 billion of IoT devices will be online [1]. Such devices provide the ability to automate daily life activities such as turning lights on automatically when the user reaches home, considering a domestic context, or to improve productivity, on an Industry 4.0 environment. Being a pervasive technology embedded on critical locations, the IoT phenomenon is often coupled with privacy issues: as such sensors often process sensitive information, security becomes a very important topic.

Considering the domestic context in particular, Internet of Things devices may communicate through standard networks, such as Wi-Fi or ethernet, or build a dedicated network to communicate with other sensors, called Wireless Sensor Network (WSN). In this regard, a real standard is not commonly adopted yet [2]. Currently, there are different protocols providing communication between sensors: some of them are based on pre-existing protocols (Wi-Fi, 6LowPan or LoRa), while others provide the creation of a new ad-hoc infrastructure (ZigBee, Z-wave).

Although different IoT protocols may be adopted, IoT devices are often exposed to security attacks, due to their limited functionalities (e.g. power consumption, computational capabilities). Therefore, the IoT security topic is extremely critical: let's thing for instance to a temperature sensor installed on a home environment. Although at first sight, security may not appear a crucial element (in case of data leak, people may think that the house temperature may not be relevant to an external user), it is actually a critical topic (a malicious external user accessing leaked data may derive that if the house temperature during daylight is lower/higher than a specific threshold, then nobody is in the house).

Being exchanged information extremely sensitive, due to the nature of IoT devices and networks, security of IoT systems is a topic to be investigated in deep. In this paper, we evaluate the security of the IoT networks. Wireless

E-mail: ivan.vaccari@ieiit.cnr.it, enrico.cambiaso@ieiit.cnr.it, maurizio.aiello@ieiit.cnr.it

cyber-attacks are investigated and implemented to verify if IoT networks are vulnerable to them. A set of cyber-attacks targeting non-IoT systems are selected and performed against a test ZigBee network, in order to evaluate the possibility to effectively target the network. We have analyzed in particular different scenarios associated to different threats. Such scenarios focus on network dismantling to make it inaccessible, through the execution of jamming and flooding DoS attacks, the recovery of sensitive information, through sniffing and brute force attacks, and the impersonation of a network node, by perpetrating a replay attack. The results we obtained provide a set of vulnerabilities on IoT networks based on threats affecting non-IoT systems, by providing researchers a starting point concerning the potential exposure of IoT networks and systems to cyber-threats.

The paper is structured as follows: Section 2 provides an overview of the ZigBee protocol. Section 3 presents instead the state of the art on IoT network security, by focusing in particular on the ZigBee protocol. Section 4 reports details on the attacks adopted during the tests, while an exhaustive description of the configured test network is provided in Section 5. Section 6 describes in details the executed attacks, while Section 7 analyzes protection approaches against the considered threats. Finally, Section 8 concludes the paper and reports possible future works on the topic.

2. THE ZIGBEE PROTOCOL

ZigBee is a wireless standard introduced by the ZigBee Alliance in 2004. It is based on the IEEE 802.15.4 standard, used in the Wireless Personal Area Networks (WPAN) context [3]. The communication protocol is implemented mainly for embedded system where the devices used in these networks required extremely low power consumption and low-rate transfers requirements [4]. ZigBee is able to minimize battery consumption (ZigBee Alliance officially declares at least 2 years of autonomy[1]) and to provide a communication rate up to 250 kbps, providing a coverage distance up to 1000 meters. Figure 1 shows the ZigBee stack protocol.

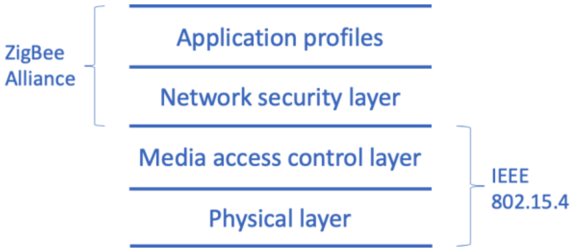


Figure 1 . A ZigBee stack protocol

The first two levels of the stack (positioned at the bottom of the stack in Figure 1) are based on the standard IEEE 802.15.4, instead the remaining two (positioned at the top of the stack in Figure 1) are implemented by the ZigBee Alliance.

The physical layer manages modulation and demodulation operations. ZigBee supports three separated frequencies and different number of channels:

- 2.4 GHz with support to 16 channels and providing a maximum communication rate of 250 kbps (used worldwide);
- 868 MHz with support to 1 channel and a maximum data rate of 20 kbps (used in Europe);
- 915 MHz with support to 10 channels and 40 kbps of communication rate (used in US).

Since they work on the same frequencies with different channels bandwidth size, in case of 2.4 GHz adoption, there may be interferences with existent Wi-Fi networks [5] in the same area. So, in case of communication problems, this interference must also be analyzed if there are a lot of wireless networks. The Media access control layer is implemented to ensure a reliable and secure communication, by using a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to manage access to the physical level [6].

The first layer implemented by ZigBee Alliance is the network security layer. It is implemented in order to manage commissioning of a new device, security handling and network topologies. Particularly, ZigBee supports three different network topologies:

- A star topology, where each node communicates only with a central node;
- A tree topology, where central nodes of different star networks are connected with a bus network;
- A mesh topology, where all the nodes are connected to each other.

Depending on the application to be implemented, the topologies depend on the applications that the network must implement. Between Among the different topologies of networks, the most interesting one is the mesh one, since it implements ad-hoc routing algorithms to autonomously restore the communication when a node is connected or disconnected from the network [7].

The last top layers implemented by ZigBee Alliance is the application profiles. Inside the Application profiles, there are three different sub-layers called Application Support SubLayer (APS), ZigBee Device Object (ZDO) and Application Framework (AF) It provides the user interface and it is composed of different elements:

- Application Support SubLayer (APS), managing the interfacing between the application layer and

[1] More information are available at the following address: https://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbeehomeautomation/

the network layer. Furthermore, it controls and analyses information sent and received by other layers to ensure proper packet transmission and encryption;

- ZigBee Device Objects (ZDO), an object implemented to initialize the APS and the network layer to manage commissioning and discovering of new nodes in the network;
- Application Framework (AF), containing and executing ‘application objects’ which define input and output of the APS, every objects are identified by an endpoint address from 1 to 254 (0 is reserved for ZigBee Device Object (ZDO), 255 for broadcast messages). These objects can be implemented by different manufacturers in order to develop a proprietary application. In order to enhance products interoperability, the ZigBee Alliance has created some standard Application Profiles in order to enhance products interconnection used by the developer to implement applications. The most common profiles are home automation, smart energy, light link and green power

A. ZigBee Node Types

ZigBee supports different kind of devices characterized by different functionalities:

- ZigBee end-device (ZED): it is implemented for the sensor installed in the interested area, it stays most of the time in sleep mode in order to reduce power consumption, and it is periodically powered up in order to send data on the network;
- ZigBee Router (ZR): an optional node used to route information on the network with role similar to a Wi-Fi router;
- ZigBee Coordinator (ZC): used to interface the ZigBee network with other platforms and to manage the configuration parameters of nodes and network.

ZigBee networks are always characterized by a single coordinator, different end-devices and an arbitrary number of routers.

B. ZigBee Security

As in any environment where information is exchanged, such as Wi-Fi [8] or ad-hoc wireless sensor network [9], communication security assumes a crucial role. The encryption algorithm used by ZigBee in order to encrypt packets is Advanced Encryption Standard (AES) with a 128-bit key. Such algorithm is used to guarantee confidentiality and authenticity [10].

ZigBee adopts three keys in order to protect the communication:

- Master Key: usually pre-installed on the device or shared out-of-band, it is adopted to retrieve the other keys, but never exchanged on the network;
- Network Key: a key shared by all the devices connected to the network. It is generated by the Trust Center and it can be sent on the network as plain text or in encrypted form, depending on the adopted security profile;
- Link Key: a key generated using the Master Key and adopted for communications between two different devices on the same network in order to exchange the Network Key encrypted.

By exploiting such keys, ZigBee implements two security profiles [11]:

- Standard Security profile: the basic security profile where packets are encrypted but the Network Key is shared in clear text. It is rarely adopted due its exposure to different attacks [12]–[14];
- High Security profile: it offers a higher level of security. The Network Key is shared in encrypted form, while the Link Key which is never exchanged on the network.

Using wireless communication, traffic exchanged on the network can easily be recovered from a malicious user [15]. If the communication is unencrypted, an attacker can access all packets exchanged on the network and retrieve sensitive data since they are recovered in clear text. Otherwise, if communications are encrypted, a malicious user can often only perform attacks external to the network, such as denial of service or jamming, since clear text data retrieval can be very difficult [6].

3. RELATED WORK

Cyber-security of IoT systems is a hot topic, since it is important to identify possible vulnerabilities and innovative threats on such systems, with the final aim to efficiently protect them. In order to detect possible vulnerabilities that could be exploited in an IoT network, especially considering the domestic context, scope of our work, it is important to consider security of wireless networks and the panorama of attacks affecting them. Concerning threats against the Wi-Fi protocol, one of the most popular wireless protocols, different taxonomies are proposed. [16] proposes a classification of Wi-Fi attacks by analyzing both threats and countermeasures. Instead, [17] introduces a taxonomy of attacks against Wireless Sensor Networks, by grouping attacks in function of the exploited layer of the ISO/OSI stack. WSN are also investigated in [18], [19], proposing attacks categorization and taxonomies. [20] proposes instead a categorization of wireless attacks in smart grid environments. A complete survey on the technical challenges, advances and future topics about WSN is proposed by [21] focused on security protocols and algorithms that are adopted in the wireless network. Most of the attacks mentioned in such taxonomies are implemented in our work, by analyzing their success against a ZigBee IoT network.

Unlike other network nodes, IoT devices have limited energetic and computational capabilities, hence, it is important to properly secure them, also guaranteeing low power consumption. This is a challenge investigated in literature and generally known as *green security* [22], and it also concerns the mobile context [23]. An interest research work analyses the impact of cyber-security algorithms from the power consumption point of view [10]. Authors compare well-known security algorithms in different contexts, in order to identify the most efficient algorithm to adopt.

Given the low power consumption and the limited capabilities of IoT devices, security-related features can not be implemented properly [24]. For this reason, a trending research topic concerns cyber-security aspects applied to IoT environments. In this regard, [25] considers hardware and software limitations of IoT systems, by creating a taxonomy of weaknesses of IoT devices and networks. Differently from the proposed work, no tests on real environments are proposed by the authors. Instead, [26] analyzes security of IoT networks by identifying crucial aspects related to common vulnerabilities, while [27], [28] focus on the security challenges to be addressed in the IoT field, also proposing protection solutions. Similarly, [29] focuses on security issues on environments such as healthcare, smart home or vehicles management. The mentioned vulnerabilities are used as a basis for the selection of the attacks considered in our work.

Internet of Things networks may adopt different communication protocols. A comparison between IoT network protocols is proposed in [30], including Wi-Fi, ZigBee, Z-Wave, Thread and Bluetooth LE. For our work, we focused on the ZigBee protocol, due to its wide adoption [31].

Other works focus on the execution of cyber-attacks on Internet of Things contexts. Concerning Wi-Fi IoT networks, efficiency of denial of service [32], flooding [33], sybil [34] and man-in-the-middle [35] attacks is investigated in literature. Our work is focused instead on the execution of some of these threats against ZigBee based IoT networks.

Concerning protection systems, [36] proposes an algorithm to analyze spatio-temporal data to detect attacks to IoT systems. [37] focuses instead on the identification of compromised nodes in IoT networks. Similarly, [38] introduces a technique to discover threats inside of a network. Instead, [39] proposes a data protection system using public key infrastructure (PKI) encryption in IoT networks, while [40] introduces an attack protection framework, by classifying possible threats, hence proposing ad-hoc mitigation activities. A survey of the state-of-the-art in Intrusion Detection Systems (IDS) is proposed by [41]. They analysed a set of well-know algorithms to detect threats on an IoT network. [42] proposed TermID which is a distributed network for intrusion detection system based on classification rule and swarm intelligence principles to detect an attack on execution on the network. [43] also compared a serious of machine learning and algorithms to detect threats on 802.11 protocol.

Because of the wide adoption of the ZigBee protocol [31], its interest in literature is focused not only to enhance the protocol [44]–[47], but also to improve ZigBee security. In this context, [48] makes use of received signal strength indication (RSSI) to detect running sybil attacks, while [49] implements a protection system to counter jamming attacks, and [50] introduces countermeasures against the sinkhole attack. Protection from attacks aiming at sensors battery draining is investigated in [12], while [51] proposes instead a protection system against DoS attacks, by evaluating its efficiency on networks adopting different protocols, including ZigBee. Instead, [52] focuses on the proposal of a novel rekeying system to protect a network from suspicious nodes and to prevent eavesdropping. [53] proposes a protection system against packet-in-packet attacks (also known as tunneling [54]). Nodes redistribution to counter non-patchable vulnerabilities exploitation in IoT networks is investigated in [55], while sniffing, replay, and network discovery attacks protection is provided in [15].

Other works focus on the proposal of innovative intrusion detection systems, designed to protect ZigBee based IoT networks. [56] introduces ABAS, an anomaly based protection system analyzing network traffic to classify anomalous behavior, while [57] makes use of machine learning algorithms to detect running attacks. [58] uses fuzzy methods based on a finite state machine to detect possible vulnerabilities. Instead, [59] makes use of noise filtering processing to protect a network from impulsive noise.

Concerning ZigBee attacks, ad-hoc security testing tools are proposed by [60], while [61] introduces the KillerBee framework, able to execute a wide range of attacks against ZigBee networks. Also, [62] introduces an innovative attack to ZigBee sensor devices, exploiting remote AT commands. Concerning the tools proposed in [60], due to hardware limitations, we do not adopted the proposed software for our tests. Conversely, our work makes use of the KillerBee framework to perpetrate a set of attacks against our test network.

By considering the literature on cyber-attacks on wireless networks, in our work we select a set of cyber-attacks in order to implement them and to perpetrate them against a ZigBee network, evaluating the success of the executed attacks. Our implementation makes use of already existent specific attack tools able to target ZigBee based systems, integrating them with ad-hoc implemented software. We focus in particular on the analysis and implementation of several well-known threats, to verify their effectiveness when they are perpetrated against IoT environments based on the ZigBee protocol. To the best of our knowledge, no other works on the topic is present. Hence, the results provided in our work will be valuable in order to evaluate the possibility to carry out cyber-attacks against ZigBee networks.

4. ATTACKS CLASSIFICATION

In this section, an overview of cyber-attacks implemented on the test network and the procedure adopted in the security test phases are reported. We select in this section the threats adopted during our tests. Such threats represent important attacks in the wireless security scenario [63].

Our selection is based on a multi-stage process. Such attack flow initially involves the execution of threats from outside of the network (hence, no network access is required). Particularly, jamming attacks are considered for this step. Hence, network access attacks are considered, by retrieving the authentication key through a brute force attack. Finally, once access to the network is provided, several attacks are executed, by starting with passive threats (network communications sniffing), to the execution of denial of service (DoS) attacks against specific nodes of the systems and, finally, to the execution of a replay attack, able to assess network security from active attacks. By executing such threats, a malicious node is potentially able to damage the network and make its services unusable, retrieve sensitive information exchanged on the network, or propagate malicious information/actions. With the aim to contextualize each considered attack, **TABLE 1** reports, for each threat, information on how the attack is performed (inside or outside of the network), the effects of the attack for the network, and the tools that we have adopted to perpetrate the attack (described in details in Section 5).

TABLE 1. SUMMARY OF ATTACKS

Attacks	Execution	Effects	Adopted tools
Jamming	Outside	Unaccessible network	RF explorer
Brute force	Outside	Unpermitted access to the network	Atmel RZ RAVEN USB Stick and TelosB mote
Sniffing	Inside	Retrieve sensitive information	Atmel RZ RAVEN USB Stick
Flooding	Inside	Unaccessible network	Atmel RZ RAVEN USB Stick and TelosB mote
Replay	Inside	Propagation of malicious packets	Atmel RZ RAVEN USB Stick and TelosB mote

By considering the ZigBee protocol in particular, scope of our work, we will now report a description of the considered threats.

A. Jamming

The main aim of a jamming attack is to produce a DoS attack on the targeted system, by working at the physical layer of the ISO/OSI stack. By using a directional module called jammer, specific electromagnetic waves tilting network devices are created and spread over the air. The aim of jamming attack is to deny the reception of communications from a network node, by interfering with the radio frequencies of the targeted system. In general, physical attacks are a crucial topic for security of computer networks [49], [64], since a malicious user may interrupt connectivity and system restore may not be immediate [65].

B. Brute force and dictionary

In computer science, a brute force attack consists in verifying all the theoretically possible solutions of a certain problem, until the correct one is found. In the cyber-security field, this approach is usually adopted to retrieve the secret key used by a service to implement access control, data decryption or device protection. In network security context, instead, the aim of a brute force attack is to detect the key/passphrase used to authenticate a node in the network, hence gaining access to the network like a legitimate node does [66]. Although a brute force attack is theoretically always able to retrieve the correct key, it may require extremely long execution times.

A variant of brute force attacks consists in text files containing several combinations of possible values. Such approach is commonly known as dictionary attack [67].

C. Sniffing

The aim of this attack, also known as eavesdropping, is to passively intercept data exchanged in a network. This threat can in general be executed either outside or inside of the network. This activity can be carried out both for legitimate purposes (for instance, to analyze communication issues or to detect intrusion attempts) and illicit purposes (fraudulent interception of sensitive information exchanged on the network) [68]. Usually, exchanged network packets directly transit from the sniffing node [69], although this is not always true (for instance, data propagated over the air or received through mirroring interface are received by both the recipient and the malicious user). Because of this, sniffing activities are sometimes confused with man-in-the-middle (mitm) ones, while sniffing should be considered an implementation of a mitm attack [70]. The difference between sniffing and man-in-the-middle is that mitm is adopted to alter received data before forwarding them to the intended recipient (active attack), while sniffing is a passive implementation of mitm.

D. *Flooding denial of service*

During a denial of service attack, resources of the targeted system are depleted by the attacker, until it is no longer able to communicate on the network [71]. In a distributed denial of service attack (DDoS), incoming traffic sent to the victim comes from many different sources. In case of DDoS, rather than a simple DoS, it is more difficult to stop the attack [72]. There are different categories of denial of service attacks, and several threats affecting all the layers of the ISO/OSI stack [73], [74]. An important category of DoS threats is represented by flooding attacks, targeting the system with high amount of packets, in order to consume its resources or induce it to a misbehavior [75]–[77].

Concerning DoS attacks against IoT systems, Mirai is maybe the most known attack. Mirai is a botnet that become popular after the October 21th 2016 attack against the DNS provider Dyn. The attack exploited vulnerabilities of several IoT devices to execute the global coordinated DDoS attack [78].

E. *Replay*

A replay attack occurs when an attacker copies a stream of messages between two parties and plays it back to one or more parties [79]. If the attack is not detected, the affected nodes process the flow as if the messages are legitimate. This misinterpretation may lead to negative consequences, such as the creation of redundant orders for an article on an online shopping system, or the re-elaboration of sensitive information that could create damage to the system. On IoT networks, a replay attack may lead to the opening of a secure lock, or to an interruption of a farm machine. In order to protect a network system from replay attacks, it is therefore crucial to distinguish whether the received packets are legitimate or whether they are sent from a malicious node to abuse the network [80].

5. TESTBED

In this section, we report the architecture of the test network we used to execute the different attacks in order to validate the success and the efficiency of the well-known threats against our ZigBee network. In order to perform the tests, we have configured a test ZigBee network, reported in Figure **2**.

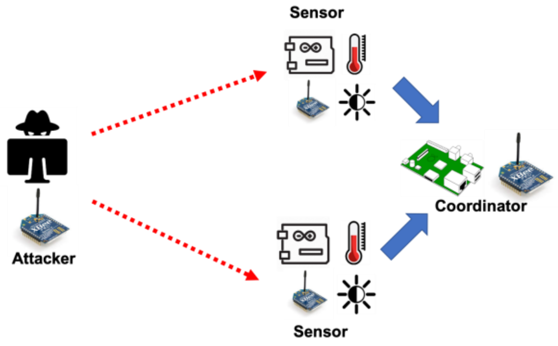


Figure 2. The considered test network

The network is implemented by using IoT sensors adopted to retrieve and propagate temperature information from the environment. Temperature data are sent from the sensor devices to the coordinator as single packets sent every 30 seconds. When they are not retrieving/sending data, devices are in sleep mode, to prevent battery drain. The network is composed by a coordinator node for packets management and two sensors for data retrieval and sending. In this configuration, sensors send packets composed by random temperature values, since the content of data exchanged in the network is not relevant for the scope of the scenario. The aim is to test security of the communication protocol and sensors.

According to the multi-step process reported in Section 4, we first execute both jamming and brute force attacks from outside of the network. Particularly, in order to execute a jamming attack, authentication is not required. Also concerning the brute force scenario, the aim is to retrieve the network key used to access the network. Hence, even in this case, the attacker is not connected on the network.

Subsequently, a malicious node is connected to the network in order to execute the attacks introduced in Section 4. For this purpose, we suppose that the attacker is able to connect to the network without forcing the access for the sniffing, flooding and replay attack. Although this may be unusual, a scenario such this one may be related, for instance, to a dissatisfied user working on the organization. This kind of attack is commonly known as insider threat [81].

We will now report technical details of the adopted test network.

A. *Adopted software and hardware*

Different devices are used in the test ZigBee network. According to Figure **2**, network components are composed by the following nodes:

- *Coordinator*, composed of a Raspberry PI 3[2] equipped with an XBee USB Board[3] and an XBee Series 2[4];
- *Sensors*, composed of an Arduino UNO R3[5], equipped with an XBee Shield[6] and an XBee Series 2;
- *Attacker*, composed of computer with specific network card for the ZigBee protocol.

The sensor and the coordinator nodes are connected to the network by using XBee Series 2 radio modules. Concerning the attacking node, jamming attacks were accomplished through the RF Explorer Signal Generator device[7], while the Atmel RZ RAVEN USB Stick[8] was used to accomplish packets interception, the XBee Serie 2 radio module was used to accomplish brute force, while the TelosB mote[9] sensor was used to accomplish flooding DoS and replay attack. For sniffing, flooding and replay threats, the KillerBee software framework was used.

The KillerBee framework[10] was created in 2009 by Joshua Wright and later purchased by the company Riverloopsecurity. It is a software library offering a set of security tools focused on the IEEE 802.15.4 protocol. The main features of KillerBee are the ability to intercept the communication between two devices and also allows to process, decrypt, create and modify packets and then send them on the ZigBee network [82].

6. Test Execution and Obtained Results

We have executed the attacks introduced in Section 4 against the test network described in Section 5.

By following the attacks previously introduced in Section 4, our tests perform the following steps:

A. Execution of a jamming attack against the targeted IoT network

B. Execution of a brute force attack, in order to retrieve the access key adopted by the targeted network for authentication purposes

C. Once the access to the network is provided, sniffing of the packets exchanged on the network

D. Interruption of legitimate accesses to the IoT network by flooding it

E. Execution of a replay attack in order to impersonate a legitimate network node

Concerning the executed activities, we will now report the results we obtained.

A. *Jamming results*

In order to analyze the effects of a jamming attack, we used the RF Explorer Spectrum Analyzer device[11], providing us the ability to analyze the radio waves present in the environment during the jamming attack.

The jamming device was used to generate radio waves at the specific frequency adopted by the network[12]. For instance, ZigBee channel 28 corresponds to a frequency of 2480 GHz.

We considered two different scenarios: in the first one, sensors were at a distance of 1 meter from each other. In the second one, such distance was equal to 5 meters. By taking the communication between two sensors, for each scenario, the device was first turned towards one of the two sensors (Jamming Case A), after which the test was performed by placing the jammer between the two sensors (Jamming Case B). For each test, communication involves the send of 100 packets between the two sensors. Such attack is almost instantaneous, as the RF explorer immediately begins the waves generation process that leads to the denial of service.

Packets exchanged by the sensors are analyzed through the Range Test software tool by X-CTU. The results of the tests are available in

and **Error! Reference source not found.**. The tables report information on the packets sent (Sent) and received (Received) from/by a node, packets lost (Lost) during the communication (for instance, two sensors physically distant one from the other), ad errors (Error) during the transmission (for instance, due to communication interruption).

[2] More information are available at the following address: https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

[3] More information are available at the following address: https://www.digikey.com/catalog/en/partgroup/xbee-usb-adapter-board-32400/15676

[4] More information are available at the following address: https://www.sparkfun.com/products/retired/10414

[5] More information are available at the following address: https://store.arduino.cc/arduino-uno-rev3

[6] More information are available at the following address: https://www.arduino.cc/en/Main/ArduinoXbeeShield

[7] More information are available at the following address: https://www.seeedstudio.com/RF-Explorer-Signal-Generator-RFE6GEN-p-2074.html

[8] More information are available at the following address: http://www.atmel.com/tools/RZUSBSTICK.aspx

[9] More information are available at the following address: https://telosbsensors.wordpress.com

[10] More information are available at the following address: https://github.com/riverloopsec/killerbee

[11] More information are available at the following address: http://rfexplorer.com

[12] Actually, during our tests, we noticed that, due to physical radio waves propagation characteristics, a frequency slightly lower/higher than the target one should be adopted.

TABLE 2 . INFORMATION RETRIEVED WITH THE JAMMER TURNED TOWARD ONE DEVICE (JAMMING CASE **A)**

Distance (m)	**1**	**5**
Frequency (GHz)	**2.479**	**2.479**
Power (dBm)	**-30/-40**	**-75/-85**
Sent	**100**	**100**
Received	**0**	**0**
Errors	**100**	**100**
Lost	**0**	**0**

TABLE 3 . INFORMATION RETRIEVED WITH THE JAMMER PLACED BETWEEN TWO COMMUNICATING DEVICES (JAMMING CASE B)

Distance (m)	**1**	**5**
Frequency (GHz)	**2.479**	**2.479**
Power (dBm)	**-30/-40**	**-75/-85**
Sent	**100**	**100**
Received	**56**	**47**
Errors	**43**	**51**
Lost	**1**	**2**

As expected, by analyzing the obtained results, it is possible to notice that the jamming attack is more efficient when the attacker is physically close to a device, since the generated waves have a greater power and can better overlap the (legitimate) waves generated by the devices. Also, results show that while the Jamming Case A leads to 0 received packets, during the Jamming Case B, about half of a packets are correctly received. We can therefore state that the Jamming Case A leads to a more successful attack.

B. Brute force/dictionary results

A brute force attack was used during our tests to recover the network key adopted by the test network. Although other protocols such as Wi-Fi have different brute force tools that even work offline [83], this is not the case of the ZigBee protocol.

Because of this, we executed a tool ad-hoc created, trying all possible key combinations until the valid one is found. Since the network key is represented as a 32 bit hexadecimal value, all possible combinations are 232, hence more than 4 billion. By assuming a test rate equal to 1 check every 10 second[13], more than 40 billion of seconds (more than 1000 years) would be needed in order to retrieve the correct network key. The time required to perpetrate the attack can be approximated as $t = k * \left(\frac{len(file)}{2}\right)$ where k represents the time needed to compute one key (in seconds).

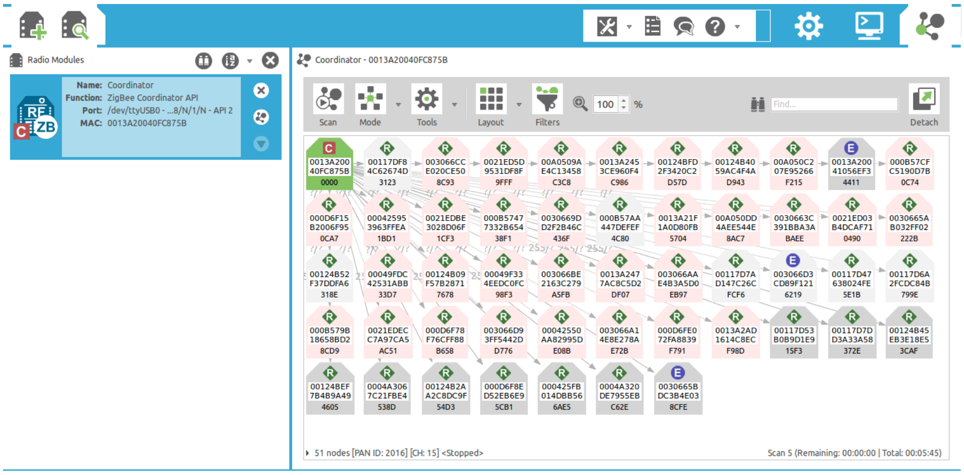
Therefore, a brute force attack against a ZigBee network system is not possible to implement in practice. Hence, for our tests, we executed a dictionary attack (see Section 4), by willingly including the correct network key in a dictionary file given in input to the attack script. As expected, in this case we obtained that the attack was successful and it was possible to access the network through the retrieved key. In this case, although as effect of the attack, one or more malicious nodes may join the network, the nodes are not directly affected by the attack.

C. Sniffing results

After the brute force and jamming attacks were executed and evaluated, we sniffed network packets exchanged on the network: our goal is to intercept the network traffic and retrieve useful information [84]. For our test network, end devices communicate with the coordinator by repeatedly sending packets every 30 seconds. Although, as previously mentioned, this attack can also be executed from inside of the network, for our tests, the attacker did not join the network. Intercepted packets are either encrypted or in clear text, in function of the network configuration. Through the *zbdump* and *zbwireshark* tools of KillerBee [85], we were able to store exchanged packets locally and analyze them. Once the packet sniffing phase was carried out, the package analysis phase was accomplished.

As reported in Section 2.B, three different security transmission modes are provided by the ZigBee protocol. For our tests, we analyzed all such security implementations. The first tested configuration concerns unencrypted communications. Since packets are transmitted in clear, it was possible to analyze the content of the data, including packets payload or sender/recipient addresses. The second tested configuration is relative to the exchange of the network key between the end devices and the coordinator in clear text, with subsequent encryption of the exchanged messages. In this case, if a malicious user sniffs the network key, e.g. when a node connects to the network, or after actively disconnecting an already connected node, all communications can be decrypted by the attacker.

[13] From our tests, this should be considered a very optimistic result.



Name: Coordinator
Function: ZigBee Coordinator API
Port: /dev/ttyUSB0 - ...8/N/1/N - API 2
MAC: 0013A20040FC875B

Coordinator - 0013A20040FC875B

C 0013A200 40FC875B 0000
R 00117DF8 4C62674D 3123
R 003066CC E020CE50 8C93
R 0021ED5D 9531DF8F 9FFF
R 00A0509A E4C13458 C3C8
R 0013A245 3CE960F4 C986
R 00124BFD 2F3420C2 D57D
R 00124B40 59AC4F4A D943
R 00A050C2 07E95266 F215
E 0013A200 41056EF3 4411
R 000B57CF C5190D7B 0C74

R 000D6F15 B2006F95 0CA7
R 00042595 3963FFEA 1BD1
R 0021EDBE 3028D06F 1CF3
R 000B5747 7332B654 38F1
R 0030669D D2F2B46C 436F
R 000B57AA 447DEFEF 4C80
R 0013A21F 1A0D80FB 5704
R 00A050DD 4AEE544E 8AC7
R 0030663C 391BBA3A BAEE
R 0021ED03 B4DCAF71 0490
R 0030665A B032FF02 222B

R 00124B52 F37DDFA6 318E
R 00049FDC 42531ABB 33D7
R 00124B09 F57B2871 7678
R 00049F33 4EEDC0FC 98F3
R 003066BE 2163C279 A5FB
R 0013A247 7AC8C5D2 DF07
R 003066AA E4B3A5D0 EB97
R 00117D7A D147C26C FCF6
E 003066D3 CD89F121 6219
R 00117D47 638024FE 5E1B
R 00117D6A 2FCDC84B 799E

R 000B579B 18658BD2 8CD9
R 0021EDEC C7A97CA5 AC51
R 000D6F78 F76CFF88 B658
R 003066D9 3FF5442D D776
R 00042550 AA82995D E08B
R 003066A1 4E8E278A E72B
R 000D6FE0 72FA8839 F791
R 0013A2AD 1614C8EC F98D
R 00117D53 B0B9D1E9 15F3
R 00117D7D D3A33A58 372E
R 00124B45 EB3E18E5 3CAF

R 00124BEF 7B4B9A49 4605
R 0004A306 7C21FBE4 538D
R 00124B2A A2C8DC9F 54D3
R 000D6F8E D52EB6E9 5CB1
R 000425FB 014DBB56 6AE5
R 0004A320 DE7955EB C62E
E 0030665B DC3B4E03 8CFE

51 nodes [PAN ID: 2016] [CH: 15] <Stopped>

Scan 5 (Remaining: 00:00:00 | Total: 00:05:45)

Figure 3. Denial of Service flood attack

The last configuration is the safest one and it involves encryption of both authentication and communications, hence making key recovery activities particularly difficult. Through physical access to the end device, an attacker may access the internal configuration to retrieve the link key and recover the network key.

For our tests, since we assume that the attacker is not able to physically access the network nodes, we obtained access to clear text data only on the first two configuration.

D. Flooding denial of service results

For our flooding DoS tests against the ZigBee protocol, we adopted the *zbassocflood* tool of the KillerBee framework, that is supposed to send network binding packets making the coordinator inactive, because too many active connections are generated [61]. After the execution of this attack, it is required to legitimate devices to access to the network again. Such access failed due to an authentication failure.

In particular, the executed attack works at the application layer of the ZigBee stack, generating random MAC addresses connected to the coordinator, in order to block connectivity of the entire network. **Error! Reference source not found.** shows the connections managed by the coordinator during a flooding attack. As shown in the figure, the attacker creates a high number of rogue nodes (related to different MAC addresses). By having a higher number of nodes to be part of the network, it is more difficult to provide network connectivity to other (legitimate) nodes. In the figure, nodes identified by an “E” icon are end devices, while nodes identified by a “R” icon are router nodes. Also, nodes with light background are executing the authentication phase. Instead, nodes with dark background are already authenticated on the network. The time required to the attacker to perform this attack depends on the number of nodes currently connected to the network, as the aim of the attack is to saturate the maximum number of nodes simultaneously connected to the network.

Under these conditions, a legitimate node is not able to connect to the network, since the coordinator is not able to manage additional connections.

E. Replay results

In order to execute a replay attack, it is needed to intercepts packets of interest first. Indeed, since the replay attack is based on a retransmission of packets exchanged on the network, the attacker has to sniff packets first. Hence, packets are sent on the network again. Figure **4** reports a scheme of the executed replay attack on the considered network. The aim of the attacker is to sniff exchanged packets until relevant information are found. At this point, packets can be replayed even instantly.

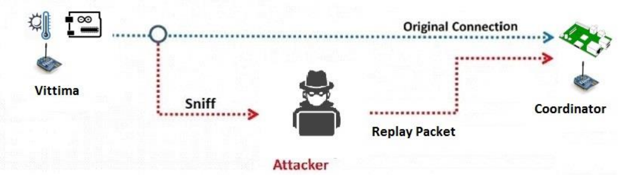


Figure 4. Architecture of the executed replay attack scenario

By referring to the test network, we captured packets relative to temperature data, sent by the sensor nodes to the coordinator. Hence, we replayed such packets, by sending them to the coordinator. For our tests, we only focus on packets including application payload data, since other packets may lead to an attack failure, due to the ZigBee protocol functioning. Once a packet is received, the coordinator processes it without verifying its authenticity. In our case, authenticity is the same of the original sender, since addresses are unchanged. After executing the attack, we noticed that the coordinator processes the packet as it is legitimately sent, hence making the attack successful and the network vulnerable to a replay attack. Therefore, we can state that the ZigBee protocol is vulnerable to a replay attack in our validation activities. Nevertheless, in function of the adopted hardware, a protection system may be implemented in this case at the application layer of the ZigBee stack, by providing additional security to the commands to avoid repetitions (e.g. by using temporary tokens).

7. Protection Approaches

In the previous sections of the paper, we have demonstrated how it is possible to successfully carry out cyber-attacks against IoT environments, in order to compromise security of the entire network. In the cyber-security context, it is nevertheless also important to investigate cyber-attacks and their efficiency, with the final aim to design and adopt proper protection techniques.

In particular, concerning the attacks previously considered, protection from jamming attacks is accomplished by adopting different strategies: [71] proposes a protection system based on a periodic check accomplished by the targeted nodes to analyze the status of the jamming attack. In order to reduce power consumption, a lower duty cycle is accomplished by the involved nodes. Instead, [51] introduces combines information on the received signal strength indicator (RSSI), the average time required to sense an idle channel (carrier sense time), and the packet delivery ratio, to apply statistical based algorithms for protection purposes. Finally, [86] proposes a jamming-resistant network that re-routes network packets when a jamming attack is detected, in order to isolate the jammed area and keep communications working.

Instead, concerning brute force attacks, our results show that the system is not vulnerable to such kind of threats, although it is vulnerable to dictionary-based attacks. An efficient protection system against dictionary based attacks is reported in [87], proposing an authentication approach which combines traditional password authentication methods with a challenge easy to answer by human users, but not by automated tools. In order to protect the system from such threats, it is also important to adopt strong authentication keys, as reported in [88], [89].

Regarding sniffing attacks, although sniffing can't be prevented in specific scenarios (e.g. a malicious node physically involved in the communication path), efficient protection systems are based on the encryption of the packets exchange in the network, as proposed in [90], or by implementing a policy-based approach to monitor and profile network users [91].

Finally, relatively to flooding denial of service attacks, they are typically mitigated through the bi-directionality verification of a link before starting to elaborate received messages [92]. In addition, such threats can be countered by using ad-hoc rules designed to drop packets received by unauthorized address [93].

Therefore, although we have proved that IoT environments are natively vulnerable to cyber-attacks, it should be considered that different protection approaches may be applied to protect a system from the mentioned threats. The effective implementation of such approaches is an interesting topic that may be addressed in future works. Particularly, the implementation of protection systems may be investigated to analyze efficiency and performance of the adopted countermeasures, when applied on low-power IoT environments, often characterized by limited resources.

8. Conclusion and Future Work

This paper focuses on Internet of Things (IoT) security. This aspect is crucial, not only due to the wide adoption that characterizes the IoT context, but also for the criticality of IoT sensors, often physically placed in sensitive locations or managing sensitive data. In addition, IoT sensor nodes are often equipped with hardware with limited capabilities (e.g. power, computation, etc.) [62]. Because of this, proper security function are rarely implemented [24], hence making IoT networks and sensors vulnerable to common attacks.

Considering the IoT context, in this paper we address security aspects of the ZigBee protocol, a prominent wireless protocol adopted in Internet of Things environments. After analyzing in detail the protocol and its functioning, we analyze the possibility to carry out specific cyber-threats against a ZigBee based system. We select valuable attacks with demonstrated efficiency in the wireless security context, describing in detail how they work and how it is possible to implement them. Selected threats include jamming and flooding DoS, key retrieval through brute force and dictionary techniques, network traffic eavesdropping, and replay attacks execution. Our aim is to perpetrate the same attacks against a ZigBee network, that represents the same characteristics of other wireless protocols such as Wi-Fi, by evaluating the possibility to perpetrate wireless cyber-attacks successfully. In order to assess the security of ZigBee based IoT networks, we designed a test network to be targeted with the selected threats. Hence, we implemented and perpetrated such attacks, in order to validate their efficiency on a real scenario.

Our results show that all the tested attacks are successful, although we found that specific approaches are less efficient than others. In particular, we prove that performance of jamming attacks depends on the direction of the jamming device. Also, we demonstrate that pure brute force attacks to get access to a ZigBee network can not be implemented, in favor of dictionary-based threats. In addition, we obtained that clear text packets interception may not be easy to implement on specific networks. These should be considered as barriers for an attacker which prefers a low cost/high result approach. Concerning instead the execution of flooding attacks, our results show that if an attacker is able to get into the network, it is possible to execute a successful attack, hence dismantling the entire network. Finally, replay attacks results prove that the protocol is natively vulnerable to this kind of threat. For each of the considered attack, we have analyzed the protection approaches that may be adopted to counter the investigated threats.

By extending this preliminary work on protection, future work may be focused on a deeper investigation of defense systems able to protect IoT systems from the adopted vulnerabilities. Similarly, further work on the topic may be directed on the proposal of improvements of the protocol in order to natively implement protection from replay attacks. Additional work on the topic may also be directed on the study of innovative threats targeting IoT systems, with the final aim of identifying protocol weaknesses and fix them. By following the green computing context, another possible extension of the work may be focused on the analysis of the energetic impact of attacks on the IoT network and nodes. Finally, future developments may also concern the execution of additional tests, considering different configuration parameters, both from the attacker (for instance, different distances concerning the execution of jamming attacks) and network side, additional attacks, or different IoT communications protocols such as LoRA, Z-Wave or other protocols for IoT network [30].

Acknowledgment

This work is supported by the following research projects:

- Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures (ANASTACIA), funded by the European Commission (Horizon 2020, call DS-01-2016) Grant Agreement Number 731558
- Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures (FINSEC), funded by the European Commission (Horizon 2020, call CIP-01-2016-2017) Grant Agreement Number 786727

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[2] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” Comput. networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[3] C. M. Ramya, M. Shanmugaraj, and R. Prabakaran, “Study on ZigBee technology,” in Electronics Computer Technology (ICECT), 2011 3rd International Conference on, 2011, vol. 6, pp. 297–301.

[4] A. Dementyev, S. Hodges, S. Taylor, and J. Smith, “Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario,” in Wireless Symposium (IWS), 2013 IEEE International, 2013, pp. 1–4.

[5] M. A. Sarijari, M. S. Abdullah, A. Lo, and R. A. Rashid, “Experimental studies of the ZigBee frequency agility mechanism in home area networks,” in Local Computer Networks Workshops (LCN Workshops), 2014 IEEE 39th Conference on, 2014, pp. 711–717.

[6] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, “Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards,” Comput. Commun., vol. 30, no. 7, pp. 1655–1695, 2007.

[7] J. Li, X. Zhu, N. Tang, and J. Sui, “Study on ZigBee network architecture and routing algorithm,” in Signal Processing Systems (ICSPS), 2010 2nd International Conference on, 2010, vol. 2, pp. V2-389-V2-393.

[8] S. Gold, “Cracking wireless networks,” Netw. Secur., vol. 2011, no. 11, pp. 14–18, 2011.

[9] E. Cayirci and C. Rong, Security in wireless ad hoc and sensor networks. John Wiley & Sons, 2008.

[10] L. Caviglione, M. Gaggero, E. Cambiaso, and M. Aiello, “Measuring the Energy Consumption of Cyber Security,” IEEE Commun. Mag., vol. 55, no. 7, pp. 58–63, 2017.

[11] G. Dini and M. Tiloca, “Considerations on security in zigbee networks,” in Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on, 2010, pp. 58–65.

[12] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, “Security threats in ZigBee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned,” in System Sciences (HICSS), 2013 46th Hawaii International Conference on, 2013, pp. 5132–5138.

[13] C. Alcaraz and J. Lopez, “A security analysis for wireless sensor mesh networks in highly critical systems,” IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev., vol. 40, no. 4, pp. 419–428, 2010.

[14] P. Radmand et al., “ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys,” in P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010 International Conference on, 2010, pp. 465–470.

[15] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, and P. Toivanen, “Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned,” in Hybrid Intelligent Systems (HIS), 2014 14th International Conference on, 2014, pp. 199–206.

[16] D. Welch and S. Lathrop, “Wireless security threat taxonomy,” in Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, 2003, pp. 76–83.

[17] M. R. Ahmed, X. Huang, and D. Sharma, “A taxonomy of internal attacks in wireless sensor network,” Mem., vol. 128, p. 48, 2012.

[18] D. G. Padmavathi and M. Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” arXiv Prepr. arXiv0909.0576, 2009.

[19] M.-L. Messai, “Classification of Attacks in Wireless Sensor Networks,” arXiv Prepr. arXiv1406.4516, 2014.

[20] Y. Liu, “Wireless sensor network applications in smart grid: recent trends and challenges,” Int. J. Distrib. Sens. Networks, vol. 8, no. 9, p. 492819, 2012.

[21] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” Proc. IEEE, pp. 1–39, 2016.

[22] L. Caviglione, A. Merlo, and M. Migliardi, “What is green security?,” in Information Assurance and Security (IAS), 2011 7th International Conference on, 2011, pp. 366–371.

[23] A. Merlo, M. Migliardi, and L. Caviglione, “A survey on energy-aware security mechanisms,” Pervasive Mob. Comput., vol. 24, pp. 77–90, 2015.

[24] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad hoc networks, vol. 10, no. 7, pp. 1497–1516, 2012.

[25] M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an analysis of security issues, challenges, and open problems in the internet of things,” in Services (SERVICES), 2015 IEEE World Congress on, 2015, pp. 21–28.

[26] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: a review,” in Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on, 2012, vol. 3, pp. 648–651.

[27] G. S. Matharu, P. Upadhyay, and L. Chaudhary, “The Internet of Things: challenges and security issues,” in Emerging Technologies (ICET), 2014 International Conference on, 2014, pp. 54–59.

[28] A. Balte, A. Kashid, and B. Patil, “Security Issues in Internet of Things (IoT): A Survey,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 4, 2015.

[29] J. S. Kumar and D. R. Patel, “A survey on internet of things: Security and privacy issues,” Int. J. Comput. Appl., vol. 90, no. 11, 2014.

[30] S. Pradeep, T. Kousalya, K. M. A. Suresh, and J. Edwin, “IoT AND ITS CONNECTIVITY CHALLENGES IN SMART HOME,” 2016.

[31] D. Geer, “Users make a Beeline for ZigBee sensor technology,” Computer (Long. Beach. Calif)., vol. 38, no. 12, pp. 16–19, 2005.

[32] Y. Lee, W. Lee, G. Shin, and K. Kim, “Assessing the Impact of DoS Attacks on IoT Gateway,” 2014.

[33] M. Sharma, “A SURVeY ON SECURITY ISSUES AND ATTACKS IN WIRELESS SENSOR NETWORK,” Int. J. Eng. Sci. Res. Technol., vol. 1, no. 5, pp. 563–567, 2016.

[34] K. Zhang, X. Liang, R. Lu, and X. Shen, “Sybil attacks and their defenses in the internet of things,” IEEE Internet Things J., vol. 1, no. 5, pp. 372–383, 2014.

[35] G. Fournier, P. Matoussowsky, and P. Cotret, “Hit the KeyJack: stealing data from your daily wireless devices incognito,” arXiv Prepr. arXiv1610.05212, 2016.

[36] K. Akkaya, I. Guvenc, R. Aygun, N. Pala, and A. Kadri, “IoT-based occupancy monitoring techniques for energy-efficient smart buildings,” in Wireless Communications and Networking Conference Workshops (WCNCW), 2015 IEEE, 2015, pp. 58–63.

[37] M. Taneja, “An analytics framework to detect compromised IoT devices using mobility behavior,” in ICT Convergence (ICTC), 2013 International Conference on, 2013, pp. 38–43.

[38] J. R. C. Nurse, A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese, “Smart insiders: exploring the threat from insiders using the internet-of-things,” in Secure Internet of Things (SIoT), 2015 International Workshop on, 2015, pp. 5–14.

[39] C. Doukas, I. Maglogiannis, V. Koufi, F. Malamateniou, and G. Vassilacopoulos, “Enabling data protection through PKI encryption in IoT m-Health devices,” in Bioinformatics and Bioengineering (BIBE), 2012 IEEE 12th International Conference on, 2012, pp. 25–29.

[40] Q. M. Ashraf and M. H. Habaebi, “Autonomic schemes for threat mitigation in Internet of Things,” J. Netw. Comput. Appl., vol. 49, pp. 112–127, 2015.

[41] I. Butun, S. D. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” IEEE Commun. Surv. tutorials, vol. 16, no. 1, pp. 266–282, 2014.

[42] C. Kolias, V. Kolias, and G. Kambourakis, “TermID: a distributed swarm intelligence-based approach for wireless intrusion detection,” Int. J. Inf. Secur., vol. 16, no. 4, pp. 401–416, 2017.

[43] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, “Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset,” IEEE Commun. Surv. Tutorials, vol. 18, no. 1, pp. 184–208, 2016.

[44] W. Li and J. Wei, “Design of Low-Power Consumption ZigBee Wireless Sensor Networks Nodes [J],” J. Chengdu Univ. (Natural Sci. Ed., vol. 3, p. 18, 2008.

[45] B. El Madani, A. P. Yao, and A. Lyhyaoui, “Combining Kalman filtering with ZigBee protocol to improve localization in wireless sensor network,” ISRN Sens. Networks, vol. 2013, 2013.

[46] B. Bakhache, K. Ahmad, and S. El Assad, “A new chaotic encryption algorithm to enhance the security of ZigBee and Wi-Fi networks,” Int. J. Intell. Comput. Res., vol. 2, no. 1/2/3/4, pp. 219–227, 2011.

[47] W. Razouk, G. V Crosby, and A. Sekkaki, “New security approach for zigbee weaknesses,” Procedia Comput. Sci., vol. 37, pp. 376–381, 2014.

[48] S. Marian and P. Mircea, “Sybil attack type detection in wireless sensor networks based on received signal strength indicator detection scheme,” in Applied Computational Intelligence and Informatics (SACI), 2015 IEEE 10th Jubilee International Symposium on, 2015, pp. 121–124.

[49] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: attack and defense strategies,” IEEE Netw., vol. 20, no. 3, pp. 41–47, 2006.

[50] K. Weekly and K. Pister, “Evaluating sinkhole defense techniques in RPL networks,” in Network Protocols (ICNP), 2012 20th IEEE International Conference on, 2012, pp. 1–6.

[51] D. R. Raymond and S. F. Midkiff, “Denial-of-service in wireless sensor networks: Attacks and defenses,” IEEE Pervasive Comput., vol. 7, no. 1, 2008.

[52] B. Ramsey and B. Mullins, “Defensive rekeying strategies for physical-layer-monitored low-rate wireless personal area networks,” in International Conference on Critical Infrastructure Protection, pp. 63–79.

[53] A. Biswas, A. Alkhalid, T. Kunz, and C.-H. Lung, “A lightweight defence against the packet in packet attack in ZigBee networks,” in Wireless Days (WD), 2012 IFIP, 2012, pp. 1–3.

[54] M. Aiello, M. Mongelli, E. Cambiaso, and G. Papaleo, “Profiling DNS tunneling attacks with PCA and mutual information,” Log. J. IGPL, vol. 24, no. 6, pp. 957–970, 2016.

[55] M. Ge, J. B. Hong, S. E. Yusuf, and D. S. Kim, “Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities,” Futur. Gener. Comput. Syst., 2017.

[56] B. Al Baalbaki, J. Pacheco, C. Tunc, S. Hariri, and Y. Al-Nashif, “Anomaly Behavior Analysis System for ZigBee in smart buildings,” in Computer Systems and Applications (AICCSA), 2015 IEEE/ACS 12th International Conference of, 2015, pp. 1–4.

[57] P. Jokar and V. Leung, “Intrusion Detection and Prevention for ZigBee-Based Home Area Networks in Smart Grids,” IEEE Trans. Smart Grid, 2016.

[58] B. Cui, S. Liang, S. Chen, B. Zhao, and X. Liang, “A novel fuzzing method for Zigbee based on finite state machine,” Int. J. Distrib. Sens. Networks, vol. 2014, 2014.

[59] J. Jia and J. Meng, “A novel approach for impulsive noise mitigation in ZigBee communication system,” in 2014 Global Information Infrastructure and Networking Symposium (GIIS), 2014, pp. 1–3.

[60] T. Zillner and S. Strobl, “ZigBee exploited: The good the bad and the ugly,” 2015.

[61] B. Stelte and G. D. Rodosek, “Thwarting attacks on ZigBee-Removal of the KillerBee stinger,” in Network and Service Management (CNSM), 2013 9th International Conference on, 2013, pp. 219–226.

[62] I. Vaccari, E. Cambiaso, and M. Aiello, “Remotely Exploiting at Command Attacks on ZigBee Networks,” Secur. Commun. Networks, vol. 2017, 2017.

[63] S. Hansman and R. Hunt, “A taxonomy of networks and computer attacks,” Comput. &amp; Secur., 2005.

[64] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, “Effects of denial-of-sleep attacks on wireless sensor network MAC protocols,” IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 367–380, 2009.

[65] R. Muraleedharan and L. A. Osadciw, “Jamming attack detection and countermeasures in wireless sensor network using ant system,” in Wireless Sensing and Processing, vol. 6248, p. 62480G.

[66] H. Berghel and J. Uecker, “WiFi attack vectors,” Commun. ACM, vol. 48, no. 8, pp. 21–28, 2005.

[67] J. D. Mireles, J.-H. Cho, and S. Xu, “Extracting attack narratives from traffic datasets,” in Cyber Conflict (CyCon US), International Conference on, pp. 1–6.

[68] B. S. Thakur and S. Chaudhary, “Content sniffing attack detection in client and server side: A survey,” Int. J. Adv. Comput. Res., vol. 3, no. 2, p. 7, 2013.

[69] N. Stojanovski and M. Gušev, “Analysis of Computer Networks Attacks,” 2007.

[70] Y. Yang et al., “Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems,” 2012.

[71] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” Computer (Long. Beach. Calif)., vol. 35, no. 10, pp. 54–62, 2002.

[72] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, “Distributed denial of service attacks,” in Systems, Man, and Cybernetics, 2000 IEEE International Conference on, 2000, vol. 3, pp. 2275–2280.

[73] A. D. Wood and J. A. Stankovic, “A taxonomy for denial-of-service attacks in wireless sensor networks,” Handb. Sens. networks Compact Wirel. wired Sens. Syst., pp. 739–763, 2004.

[74] E. Cambiaso, G. Papaleo, Istituto, G. Chiola, and M. Aiello, “Slow DoS attacks: definition and categorisation,” Int. J. Trust Manag. Comput. Commun., vol. 1, no. 3–4, pp. 300–319, 2013.

[75] J.-H. Son, H. Luo, and S.-W. Seo, “Authenticated flooding in large-scale sensor networks,” in Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on, 2005, p. 8 pp.-543.

[76] C. L. Schuba, I. V Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, “Analysis of a denial of service attack on TCP,” in Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on, 1997, pp. 208–223.

[77] L. Pawar, “Using APDA and RRDA Improving Flooding Impact in VANETs due to DDOS Attacks,” 2017.

[78] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer (Long. Beach. Calif)., vol. 50, no. 7, pp. 80–84, 2017.

[79] R. Pries, W. Yu, X. Fu, and W. Zhao, “A new replay attack against anonymous communication networks,” in IEEE International Conference on Communications, 2008.

[80] P. Syverson, “A taxonomy of replay attacks [cryptographic protocols],” in Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings, 1994, pp. 187–191.

[81] J. R. C. Nurse et al., “Understanding insider threat: A framework for characterising attacks,” in Security and Privacy Workshops (SPW), 2014 IEEE, 2014, pp. 214–228.

[82] J. Wright, “Killerbee: practical zigbee exploitation framework,” 11th ToorCon Conf. San Diego, 2009.

[83] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne, “Vulnerabilities of Wireless Security protocols (WEP and WPA2),” Int. J. Adv. Res. Comput. Eng. Technol., vol. 1, no. 2, p. pp: 34-38, 2012.

[84] H. Mouratidis, P. Giorgini, and G. Manson, “Using security attack scenarios to analyse security during information systems design,” 2004.

[85] C. Valli et al., “Eavesdropping on the smart grid,” 2012.

[86] D. Perrig, Adrian and Stankovic, John and Wagner, “Security in wireless sensor networks,” Commun. ACM, vol. 47, pp. 53–57, 2004.

[87] B. Pinkas and T. Sander, “Securing passwords against dictionary attacks,” in Proceedings of the 9th ACM conference on Computer and communications security - CCS ’02, 2002.

[88] T. Lin, Chun-Li and Sun, Hung-Min and Hwang, “Attacks and solutions on strong-password authentication,” IEICE Trans. Commun. Inst. Electron. Inf. Commun. Eng., vol. 84, pp. 2622–2627, 2001.

[89] D. P. Jablon, “Strong Password-Only Authenticated Key Exchange,” Can. Med. Assoc. J., 1996.

[90] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini, “A secure and quality-aware prototypical architecture for the Internet of Things,” Inf. Syst., 2016.

[91] L. Cai, S. Machiraju, and H. Chen, “Defending against sensor-sniffing attacks on mobile phones,” in Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds - MobiHeld ’09, 2009.

[92] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, SNPA 2003, 2003.

[93] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, “Denial-of-Service detection in 6LoWPAN based Internet of Things,” in International Conference on Wireless and Mobile Computing, Networking and Communications, 2013.

Ivan Vaccari: Computer engineer and Ph.D student in Computer Science. In 2017 he obtained his MSc Degree Cum Laude in Computer Engineering from the University of Genoa, Italy, with a thesis entitled “Study of security issues on ZigBee networks in reference to the Internet of Things phenomenon”. For this work, he received a price for the “Best project 2017” for IoT networks implementation offered by the multinational company ABB.

Enrico Cambiaso: graduated in Computer Science at the University of Genoa, Italy, in 2012, with a thesis entitled “Analysis of slow DoS attacks”. He is a PhD student at the University of Genoa and he collaborates with the Research National Council of Italy, working to the slow DoS field. His scientific interests are related to computer and network security, intrusion detection systems, covert channels and cloud computing.

Maurizio Aiello: graduated in 1994, worked as a free-lance consultant both for universities and research center and for private industries. From August 2001, he is responsible of CNR network infrastructure. He is a Teacher at the University of Genoa and University College of Dublin; students Coordinator, fellowships and EU projects in the computer security field. His research activities are on network security and protocols.