ACTA SCIENTIFIC COMPUTER SCIENCES

Volume 2 Issue 4 April 2020

Research Article

Innovative Protection System Against Remote AT Command Attacks on ZigBee Networks

Ivan Vaccari*, Maurizio Aiello and Enrico Cambiaso

National Research Council (CNR), IEIIT Institute, Genova, Italy

***Corresponding Author:** Ivan Vaccari, National Research Council (CNR), IEIIT Institute, Genova, Italy.

Received: March 10, 2020

Published: March 20, 2020

Abstract

Internet of Things (IoT) is one of the most consolidated technologies adopted in the world. Being exchanged information extremely sensitive, due to the nature of IoT devices and networks, cyber security of IoT systems is a critical topic to be investigated in deep by studying protocols, devices and technologies in order to identify possible vulnerabilities and weakness. In this work, a threat against ZigBee called Remotely AT Command attack is studied and analyzed in order to develop an innovative protection system able to detect and mitigate the devices from this innovative threat. Also, the protection system implemented is tested and validated on a real network by using XBee module [1], a wireless module adopted to implement and instantiate ZigBee network.

The proposed protection system aims to verify if devices are able to communicate on the network when the attack is running. In this case, just before the sensor is ready to communicate on the network, an internal check is accomplished directly by the IoT device: if needed, an additional reconfiguration is accomplished, in order to restore connectivity of the node in order to mitigate the threat. The results of this work are very interesting since, if executed against real network, the Remote AT Command attack could create huge damage to companies. For this reason, the protection system implemented is an innovative result in terms of research achievement.

Keywords: Zigbee; AT Command; Cyber Threats; Protection Systems; Internet of Things; Cybersecurity; Network Security

Introduction

Nowadays, the Internet of Things (IoT) is a consolidated technology and it is currently adopted in many contexts and applications of different nature [2]. In the Internet of Things environment, simple objects are able to manage, process and communicate data of the surrounding environment and send them to other IoT devices or to more complex systems such as smartphone, robots, cars, machines of the new industrial era or critical infrastructures. In IoT world, people and objects can directly interact with each other, thanks to the spread of smartphones, tablets and other mobile devices that allow people to share information in real-time over the Internet from anywhere in very simple ways [3]. Thanks to the rapid developments in the underlying technologies, IoT offers enormous opportunities for a large number of new applications that promise to improve the quality of human life and to improve production benefit of companies by reducing costs. In recent years, IoT attracted researchers and professionals around the world due to the potential benefits that these technologies could bring [4]. IoT networks and devices are widely adopted in different scenarios such as home automation [5], industry 4.0 [6], healthcare [7], robotics [8], smart cities [9], cyber physical systems [10] or critical infrastructure [11]: with IoT devices and networks, it is possible to remotely control physical quantities such as temperatures and humidity or to control more complex systems such as smart light bulbs, robotics, health parameters, sensor networks and smart integrated systems. Given this freedom of implementation and applications, even at the level of technologies enabling the Internet of Things, many options are available to implement these networks as, currently, exist ad hoc IoT communication protocols or applications implemented on well-known standards. It is possible to implement IoT networks using standard protocols such as Wi-Fi or ad hoc protocols such as ZigBee or 6LowPAn based on user needs.

Otherwise, this rapid spread of IoT applications opens challenges related to the cyber security aspects on these devices and communication protocol [12]. As mentioned, the IoT applications cover different critical contexts where sensitive information are exchanged between devices and humans. Also, IoT networks are connected on the global internet so devices could be targets of cyber threats or adopted as attack vectors. For these reasons, cyber security about IoT devices and networks is a critical and trending topic.

An ad hoc communication protocol widely adopted for IoT applications is ZigBee, a protocol based on IEEE 802.15.4, with interesting features and requirements that have allowed its rapid diffusion in applications. For this reason, we decided in this work to focus on the development of an innovative protection systems for the ZigBee networks based on XBee module in order to protect

the devices from a specific zero-day attack called Remote AT Command attack [13], a cyber threat able to create potential damage to ZigBee networks and devices. The proposed work is contextualized in the IoT security topic, where we introduce a protection system against the innovative cyber threat able to protect the ZigBee networks implemented by using XBee module.

The remaining of the paper is structured as follows: Section 5 reports the related work on the topic. Section 6 introduces the innovative protection system, while Section 7 reports the testbed. Section 8 presents in detail the algorithm about the protection system. Executed tests and obtained results are reported in Section 9. Finally, Section 11 concludes the paper and reports further works on the topic.

Related work

Due to the rapid adoption of the ZigBee protocol related to the IoT applications spread, an important and critical topic is related to ZigBee networks protection in order to detect and mitigate cyber threats to reduce potential damage on networks and devices. Many security researchers and experts studied the protocol and identified several threats able to target such systems in order to implement protection systems about these vulnerabilities. Marian and Mircea [14] proposes an approach to detect sybil attacks by computing the location of a node and then classifying it as malicious or not. Weekly and Pister [15] introduces two countermeasures against sinkhole attack: the first, called rank verification, is based on one-way hash function and the second, instead called parent fail-over, is based on end-to-end acknowledgment scheme. Al Baalbaki., *et al.* [16] introduces an Anomaly Behavior Analysis System (ABAS) for the ZigBee protocol based on network traffic analysis in order to classify attack using information such as packets origin or destination. Jokar and Leung [17] implements a protection algorithm called HANIDPS based on machine learning in order to analyze network traffic to detect a running threat. Cui., *et al*. [18] adopts a fuzzing method implemented on finite state machines by injecting different testing cases into the system in order to detect vulnerabilities. Jia and Meng [19] implements a system using a noise filtering to protect against impulsive noise a ZigBee network. Zillner and Strobl [20] describes the applied security measures in ZigBee protocol with a focus on weakness and he proposes a software, called Sec Bee [21], to test security about ZigBee network using know vulnerabilities. Raymond., *et al.* [22] studies a deep and interesting approach to detect DoS attack and defense on ZigBee with related countermeasures available. Ramsey and Mullins [23] introduces a novel rekeying system in response to a suspected malicious node in a ZigBee network and an innovative obfuscation algorithm to prevent common wireless sniffer. Biswas., *et al.* [24] performs a study to protect ZigBee network against Packet-in-Packet attack by implementing a bit stuffing algorithm. Ge., *et al.* [25] works on a protection system in order to defense an IoT network by studying an approach to re-distribute nodes in order to reduce damage in the network. Regarding physical attack [26-29], perform different study about attack and defense against ZigBee regarding jamming threat by implementing a protection approach able to protect sensor from this physical attack. Instead [30] implements two countermeasures against physical attack aimed to discharge battery of sensors and to protect the exchange of the network key between end-device and coordiantor. Olawumi., *et al.* [31] proposes a protection system against sniffing, by installing the network key in the device avoid over-the-air exchange, for a replay attack, proposing that the encryption process can be integrated with timestamp mechanism, and against Network Discovery and Device Identification where they suggest to introduce in the network an intrusion detection and prevention system.

During our research work, we studied cyber security aspects of ZigBee by initially studying the protocol, thus analyzing the major threats affecting it, hence studying possible protection systems and approaches. During our study, we performed a deep study about cyber threats against ZigBee by analyzing well-known threats [32] and innovative zero-day attack exploiting specific packets adopted in the ZigBee network called Remote AT Command [13]. Remote AT Command attack is considered extremely innovative and particularly dangerous, since it allows malicious users to retrieve/forward sensitive information or manipulate nodes functionality in a ZigBee network. Our work focuses on the proposal of an innovative protection system against the Remote AT Command attack in order to protect ZigBee networks from the threat. In the next section, the protection system is reported and the obtained results described in detail.

Protection against remote AT command attack

In order to carry out a complete security analysis of the ZigBee protocol and to develop an efficient protection system, we studied the communication flows between devices and the packets adopted by the protocol to communicate on the network since ZigBee adopts specific network packets to exchange information, to authenticate devices or to manage network configuration. Among the different network message flows, we initially focused on packets sent from end-devices, which are IoT devices adopted to retrieve information on the field, to the coordinator, a single device for ZigBee network adopted to manage the entire network, as these packets contain data recovered from the environment and may contain sensitive data. After we analyze this communication flow without detect critical vulnerabilities, we focused on other information exchange flows and we noticed that Remote AT Command can be used to handle parameter configuration devices.

As discovered and analyzed, we implemented an attack on ZigBee networks, in particular against XBee module, that exploits this particular type of packets with the aim to disconnect a legitimate node from the network and make it not able to communicate [13]. This specific configuration packets are used by many devices, such as XBee [1], ESP8266 [33] or ETRX3 [34], to configure network

access parameters such as the network identifier, destination address or device identifier on the network.

The main objective of our work is to implement a protection security system able to protect devices from the Remote AT Command attack aimed to tamper the communication of a device on the network. In order to implement a ZigBee network sensor to simulate a real scenario, we focused on XBee modules. These modules are widely used around the world, especially in DIY implementations, as they are cheap, user can implement their custom applications without deep knowledge on IoT. On the other hand, these devices have many vulnerabilities and weakness, e.g. AT Command are automatically processed by the module without allowing a user to access the contents of these specific types of packets. The cyber threat implemented exploit this vulnerability by using Remote AT Command to attack all active nodes by scanning the network. In this way, all sensors in the network are exposed to malicious user's attack.

In order to implement an efficient defense protection system from Remote AT Command exploit, it is assumed that a malicious node have access to the sensor network and it execute the attack in order to disconnect legitimate nodes. IoT devices are mainly used to manage and process very sensitive information, a vulnerability known as the AT Command attack must be neutralized to allow normal and more secure communication.

Testbed

In this section, we report structure of the network implemented in order to test and validate the protection system from Remote AT Command threats to compare protected and unprotected sensors by monitoring network traffic of the test network. In order to perform tests, we implemented a ZigBee network by using XBee module in order to communicate through the IoT communication protocol. A schema is reported in figure 1.

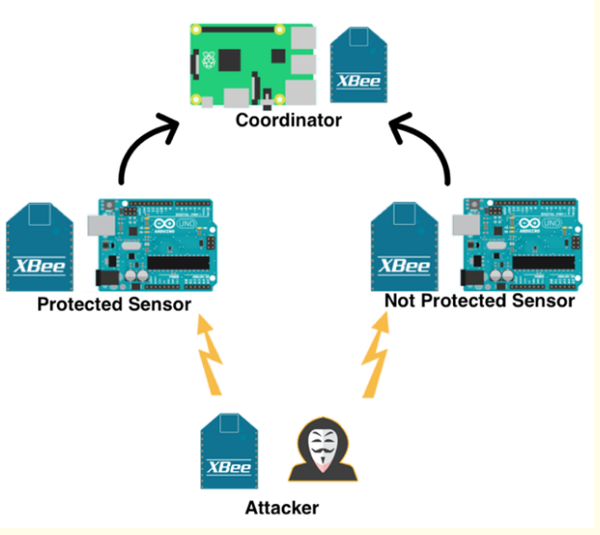

Figure 1: Testbed network.

The testbed network is composed of a ZigBee coordinator, two end-devices representing common sensors, and a malicious node connected to the ZigBee network. Two sensors are different since one sensor implements the innovative protection system against the Remote AT Command attack instead, the other sensor, implements simple logic to share data through the network so it is considered as vulnerable to the attack. As previously mentioned, the Remote AT command attack is able to scan the network in order to identify the end-device nodes and to execute the threat against these devices. In this scenario, the coordinator is not target by the attacker since potentially if the attack took effect, the whole ZigBee network is disconnected and, in this way, it would be very simple to detect the attack. On the other hand, in the event that a node is disconnected, mitigation can take some time from execution to detection of the attack as if the network is composed of a huge number of nodes, it can be difficult to identify the disconnected one.

By using the analyzed scenario, the aim is to evaluate if the device that implements the protection system is able to keep the connection on the network alive while the vulnerable node of the network should be disconnected.

Protection system algorithm and implementation

As previous mentioned, the attack using the AT Command implemented is able to target all end-devices by scanning devices connected to the network and sending Remote AT Command packets with a specific time interval. In order to test the innovative protection system, we performed a series of tests in order to evaluate efficiency and accuracy. Initially, an in-depth study was carried out on possible implementations about the protection system by analyzing hardware and software aspects of the components used to create the ZigBee network.

After this important and critical study, we identified possible protection system based on different implementation features and characteristics: (i) modifying XBee device firmware, (ii) disabling AT Command packets sent by other devices on each single sensor, (iii) software solution implemented at application layer of the network stack.

The first two solutions cannot be implemented as the manufacturer of the XBee module doesn't provide firmware to users (the firmware is not open source). Furthermore, is not possible to disable the AT Command packets on the modules as they are adopted to handle the network parameters. The most appropriate solution to implement a protection system on the device is a software implementation in the application layer of the ZigBee stack.

After deciding the approach to be adopted to implement the protection system, we started to define the main characteristics of the defense. In particular, the algorithm developed is based on the real-time analysis of the device's network configurations in order

to avoid modification or manipulation in order to keep the devices connected to the legitimate network.

The protection system proposed and implemented is based mainly on two functions:

- GET function: It is used to retrieve the current configuration of the XBee module;
- SET function: It is implemented to set new values of XBee parameters.

In the protected module is installed a configuration file containing a list of network parameters used to allow devices to access the network. The purpose of our tests is to demonstrate that two devices under the same attack, respectively an unprotected sensor and a protected one, have different effects: while the unprotected sensor has a sort of inability to communicate, this effect is not accomplished on the protected sensor since the protection system is able to protect the sensor from the attack and keep the connection alive. For our purpose, the attack performed reconfigures the end device by disconnecting it from the network. Therefore, we expect that the vulnerable device interrupts the communication with the coordinator, while the protected sensor continues to communicate on the network.

In order to better understand the proposed protection system, we describe how the GET and SET functions are structured in terms of timing and functionality, based on three main steps:

- Open AT mode: It requires 1 second for all functions, in official documentation it is 3 seconds[1];
- SET or GET parameter: In case of GET parameters, it requires 100 ms;
- Close AT mode:
  - Get function: 1 second;
  - Set function: In total restore implementation is set to 0 because after this step, no AT mode operation are required, instead in partial restore it is 1,2 seconds because is possible to execute AT command mode to manage other parameters.

After analyzing the protection system in detail and defining the timing of the algorithm, we performed tests to verify the efficacy and accuracy of the proposed protection system against an Remote AT Command attack. In order to obtain a complete view of the ZigBee network, we scheduled the malicious node to execute the attack with the following timelines: 10 seconds to network scanning, 5 second to send Remote AT Command packets and 30 seconds of delay.

Executed tests and obtained results

In this section we reported the executed tests and the obtained results in terms of timing and network traffic analysis as mentioned in the previous section related to the protection algorithms.

Time execution for end-device has been divided into different parts reported in table 1. "WakeUp" is the time required by the XBee device to initialize the connection with the coordinator. "Sleep" time is, instead, the timing where the XBee device is disconnect from the network in order to save battery and it is an arbitrary value. GET and SET functions timing are described in Section 8. Time results are reported in seconds.

Sketch	WakeUp (s)	Sleep (s)	GET function (s)	SET function (s)	Total (s)
Without defense	20	5	0	0	25
Total	20	5	5,3	1	31,3
Partial (3 parameters)	20	5	5,3	6,6	36,9
Partial (2 parameters)	20	5	5,3	4,4	34,7
Partial (1 parameters)	20	5	5,3	2,2	32,5

Table 1: Reconfiguration time.

In order to test and evaluate the protection system, we implemented two different protection system application that by testing the performance, execution of time and response times on the modules, then we have compared the results to verify the most efficient solution. The first protection system application is implemented with a specific logic: the protection system performs a GET function to know the actual value of the parameters, if they are different from the configuration file, the SET function restores all configuration values without worrying about what the parameter value actually changed.

Instead, the protection system application is different from the first one: after the GET function, the protection system restores the default values, contained in the configuration file, only for the parameters exploited by the Remote AT Command attack.

We tested these two versions of the protection system by comparing the obtained results in terms of time features and communication with a vulnerable device, a device without protection system installed. We measured these timelines on the end-devices: the vulnerable device sends data every 25 seconds, the communication interval of the protected device depends directly on the protection system since, in case of attack, it must carry out the mitigation phase by exploiting the SET function. For the device with total restore of network parameters, this time is constant, for the

[1]More information are available at: https://cdn.sparkfun.com/learn/materials/29/22ATCommands.pdf

device with partial restore it depends instead on the number of exploited parameters from the Remote AT Command attack. For this work, we assumed that an attacker could modify a maximum of 3 parameters. As shown in Table 1, the times required for the partial protection system are directly proportional with the parameter number exploited. In the case of a few parameters, it is efficient but when the number increases, it may be convenient to reconfigure all the parameters even if they are not modified. This is due to the fact that the protection system first performs a check if the parameter is modified and then sets it to the correct value, thus requiring a longer execution time than reconfiguring all the parameters.

After analyzing the response times of the network devices in the different configurations comparing vulnerable and protected sensor, a phase of collection and processing data obtained from network traffic analysis was carried out.

We analyzed ZigBee traffic by using a specific wireless module able to intercept ZigBee traffic, then we represent the traffic of each device of the network with a graph in order to compare and evaluate the obtained results. We analyzed a total time of 15 minutes divided in 3 phases: 5 minutes without attack, 5 minutes of execution Remote AT Command attack and 5 minutes after attack. The network traffic analysis results are reported in figure 2.

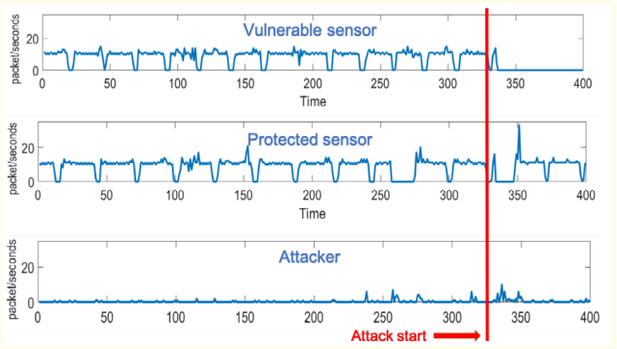

Figure 2: Network analysis of ZigBee network.

By analyzing Figure 2, the protection system developed is able to protect the devices from the Remote AT Command attack since, after the execution of the threat, the protected sensor is able to communicate again with the coordinator. Instead, the vulnerable sensor is disconnected from the network.

In the initial part of the time analysis, the one that goes from 0 to 300 seconds on the abscissa axis, all the sensors communicate on the network sending data regularly, the attack is then performed in the area between 300 and 350 seconds and then return to the initial state.

The graph of the protected sensor shows that, even in the attack phase, the protected device remains connected to the network and continues the communication with the coordinator. During the attack phase, a spike of packets since the protected sensor adopts AT Command to reconfigure the parameters exploited by the attacker by using the protection system implemented. The graph of the vulnerable sensor instead shows that, during the attacking time attacked, stop sending packets on the network.

Finally, Figure 2 shows a time interval from 0 to 400 seconds when in reality it should be 900. The last 500 seconds have been omitted since the graph is not relevant because the vulnerable sensor stops communicating while the protected sensor communicates nominally on the network

Conclusion and Future Work

This work focuses on Internet of Things (IoT) security, in particular on the ZigBee protocol and the XBee module. This aspect is crucial, not only for the wide adoption that characterizes the IoT context, but also for the criticality of the IoT sensors, often physically placed in sensitive positions or in the management of sensitive data. In addition, IoT sensors are often equipped with hardware with limited capacities (eg power supply, calculation, etc.). For this reason, adequate security functions are rarely implemented, thus making IoT networks and sensors vulnerable to common but also advanced attacks. Considering the IoT context, in this document we address the security aspects of the ZigBee protocol, a prominent wireless protocol adopted in Internet of Things environments. After analyzing the protocol and its operation in detail, we analyzed a specific attack called Remote AT Command against ZigBee. The proposed work presents an innovative protection system against the Remote AT Command attack inherent to the ZigBee protocol.

As previously described, the attack turns out to be very critical as it is able to disconnect XBee sensors from a legitimate network, thus causing a loss of sensitive data. For this reason, the proposed protection system is extremely important and innovative because, as demonstrated both in terms of network traffic and timing, it is able to protect XBee modules from this type of attack. Therefore, analyzing the results obtained, the times necessary for the protection system to identify and mitigate the attack are therefore appropriate because, during the attack, the protected module communicates every 30 - 40 seconds instead of the 25 seconds set. The protection system developed is therefore able to protect devices and provide added value to the network as it allows to increase the level of network security and to keep the connections protected from Remote AT Command attacks.

A possible future work inherent to this protection system will be to integrate it directly on the xbee sensors and to test the attachment and protection system on other ZigBee modules. Finally, another possible solution will be to allow users to manipulate AT Command packages because at the moment the XBee protocols allow this solution, in this way a user will be able to identify and implement his own application that can choose which AT Com-

mand packages to process. and which ones to discard to avoid such attacks. Another possible improvement of the protection system is related to the identification phase of the attack. At the moment the attack is identified by comparing the parameters installed in the configuration file and the parameters set on the XBee module. A possible improvement therefore concerns the identification phase in which Machine Learning algorithms and artificial intelligence can be applied to analyze the number of AT Command packets exchanged in the network proportional to the number of devices.

Finally, possible future developments could concern the evolution of the protection system to be able to detect other types of attack in the world to make it more useful to the entire IoT scenario and not only linked to a specific attack, considering different configuration parameters or investigate additional innovative attacks on different IoT communication protocols such as LoRA, Z-Wave or MQTT.

Acknowledgements

This work is supported by the following research projects: Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures (FINSEC), funded by the European Commission (Horizon 2020, call CIP01-2016-2017) Grant Agreement Number 786727.

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Bibliography

1. Piyare Rajeev and Seong-ro Lee. "Performance Analysis of XBee ZB Module Based Wireless Sensor Networks". *International Journal of Scientific and Engineering Research* (2013).

2. Kaur Kuljeet., *et al*. "A Big Data-Enabled Consolidated Framework for Energy Efficient Software Defined Data Centers in IoT Setups". *IEEE Transactions on Industrial Informatics* (2020).

3. Sisinni Emiliano., *et al*. "Industrial Internet of Things: Challenges, Opportunities, and Directions". *IEEE Transactions on Industrial Informatics* (2018).

4. Gupta Reetu and Rahul Gupta. "ABC of Internet of Things: Advancements, Benefits, Challenges, Enablers and Facilities of IoT". 2016 Symposium on Colossal Data Analysis and Networking, CDAN (2016).

5. Pavithra D and Ranjith Balakrishnan. "IoT Based Monitoring and Control System for Home Automation". Global Conference on Communication Technologie GCCT (2015).

6. Xu Li Da., *et al*. "Industry 4.0: State of the Art and Future Trends". *International Journal of Production Research* 56.8 (2018).

7. Catarinucci, Luca., *et al*. "An IoT-Aware Architecture for Smart Healthcare Systems". *IEEE Internet of Things Journal* (2015).

8. Grieco LA., *et al*. "IoT-Aided Robotics Applications: Technological Implications, Target Domains and Open Issues". *Computer Communications* 54 (2014): 32-47.

9. Latré Steven., *et al*. "City of Things: An Integrated and Multi-Technology Testbed for IoT Smart City Experiments". IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life, ISC2 2016 - Proceedings (2016).

10. Zhang Yingfeng., *et al*. "A Framework for Smart Production-Logistics Systems Based on CPS and Industrial IoT". *IEEE Transactions on Industrial Informatics* (2018).

11. Russell L., *et al*. "Agile IoT for Critical Infrastructure Resilience: Cross-Modal Sensing As Part of a Situational Awareness Approach". *IEEE Internet of Things Journal* (2018).

12. Celik Z Berkay., *et al*. "Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities". *ACM Computing Surveys* (2019).

13. Ivan Vaccari., *et al*. "Remotely Exploiting at Command Attacks on ZigBee Networks". *Security and Communication Networks* (2017).

14. Marian Salavat and Popa Mircea. "Sybil Attack Type Detection in Wireless Sensor Networks Based on Received Signal Strength Indicator Detection Scheme". Applied Computational Intelligence and Informatics (SACI), 2015 IEEE 10th Jubilee International Symposium On, IEEE (2015): 121-24.

15. Weekly Kevin and Kristofer Pister. "Evaluating Sinkhole Defense Techniques in RPL Networks". Network Protocols (ICNP), 2012 20th IEEE International Conference On, IEEE (2012): 1-6.

16. Al Baalbaki, Bilal., *et al*. "Anomaly Behavior Analysis System for ZigBee in Smart Buildings". Computer Systems and Applications (AICCSA), 2015 IEEE/ACS 12th International Conference Of, IEEE (2015): 1-4.

17. Jokar Paria and Victor Leung. "Intrusion Detection and Prevention for ZigBee-Based Home Area Networks in Smart Grids". *IEEE Transactions on Smart Grid* (2016).

18. Cui Baojiang., *et al*. "A Novel Fuzzing Method for Zigbee Based on Finite State Machine". *International Journal of Distributed Sensor Networks* (2014).

19. Jia Jia and Julian Meng. "A Novel Approach for Impulsive Noise Mitigation in ZigBee Communication System". 2014 Global Information Infrastructure and Networking Symposium (GIIS) IEEE (2014): 1-3.

20. Zillner Tobias and S Strobl. "ZigBee Exploited: The Good the Bad and the Ugly". (2015).

21. Deniz Emre and Refik Samet. "A New Model for Secure Joining to ZigBee 3.0 Networks in the Internet of Things". International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings (2019).

22. Raymond David R., *et al*. "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols". *IEEE Transactions on Vehicular Technology* 58.1 (2009): 367-380.

23. Ramsey Benjamin and Barry Mullins. "Defensive Rekeying Strategies for Physical-Layer-Monitored Low-Rate Wireless Personal Area Networks". International Conference on Critical Infrastructure Protection, Springer (2013): 63-79.

24. Biswas Anshuman., *et al*. "A Lightweight Defence against the Packet in Packet Attack in ZigBee Networks". Wireless Days (WD), 2012 IFIP, IEEE (2012): 1-3.

25. Ge Mengmeng., *et al*. "Proactive Defense Mechanisms for the Software-Defined Internet of Things with Non-Patchable Vulnerabilities". *Future Generation Computer Systems* 78 (2017): 568-582.

26. Xu Wenyuan., *et al*. "Jamming Sensor Networks: Attack and Defense Strategies". *IEEE Network* 20.3 (2006): 41-47.

27. Muraleedharan Rajani and Lisa Ann Osadciw. "Jamming Attack Detection and Countermeasures in Wireless Sensor Network Using Ant System". Wireless Sensing and Processing, International Society for Optics and Photonics (2006): 62480G.

28. Perrig Adrian., *et al*. "Security in Wireless Sensor Networks". *Communications of the ACM* 47 (2004): 53-57.

29. Chen Gonglong and Wei Dong. "JamCloak: Reactive Jamming Attack over Cross-Technology Communication Links". Proceedings - International Conference on Network Protocols ICNP (2018).

30. Vidgren Niko., *et al*. "Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned". System Sciences (HICSS), 2013 46th Hawaii International Conference On, IEEE (2013): 5132-5138.

31. Olawumi Olayemi., *et al*. "Three Practical Attacks against ZigBee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned". Hybrid Intelligent Systems (HIS), 2014 14th International Conference On, IEEE (2014): 199-206.

32. Vaccari Ivan., *et al*. "Evaluating Security of Low-Power Internet of Things Networks". *International Journal of Computing and Digital Systems* (2019).

33. Makhanya SP., *et al*. "A Smart Switch Control System Using ESP8266 Wi-Fi Module Integrated with an Android Application". Proceedings of 2019 the 7th International Conference on Smart Energy Grid Engineering, SEGE 2019 (2019).

34. Dictionary AT. Command. ETRX2 and ETRX3 Series ZigBee® Modules AT-Command Dictionary (2010).