Development of a Security Enhancement Framework for Intelligent Monitoring on IoT Platform

[1]Vinod Kumar Singh, Research Scholar, Rama University Uttar Pradesh, Kanpur
[2]Hari Om Sharan, Professor, Rama University Uttar Pradesh, Kanpur
[2]C.S. Raghuvanshi, Professor, Rama University Uttar Pradesh, Kanpur

vksinghaa@gmail.com

ABSTRACT:

Through the use of IP connectivity, the Internet of Things (IoT) offers up new possibilities for automated processes. Things, or devices, are everything from our daily lives that have been upgraded with computing or communication capabilities and are the focus of the Internet of Things. Because Zigbee communication uses a modest data rate and little power compared to other mobile communications, it is frequently employed in controlling or monitoring applications. The research community has focused mostly on securing IoT systems. In order to foresee prospective security threats to the Zigbee protocol, various security threats to Zigbee networks in the IoT platform have been addressed in this article. A Security Improvement Framework (SIF) has also been created for intelligent monitoring in an office or corporate setting. Our suggested SIF can foresee and defend against a variety of potential harmful attacks in the Zigbee network and react accordingly by notifying the system administrator. On the basis of real-time data that the system administrator defines, this framework (SIF) is intended to make automatic decisions right away. As a case study for real-time monitoring, the planned SIF has finally been integrated in a workplace security system. This workplace security system is rated according on its ability to identify potential security threats. According to the evaluation findings, the suggested SIF may effectively identify and defend against a variety of potential security intrusions, enabling more secure intelligent monitoring on the IoT platform.

Keywords: Internet of Things, Communication Protocol, Security System, Security Threats, Encryption, Access Control

DOI Number: 10.14704/nq.2022.20.13.NQ88435 **NeuroQuantology2022;20(13): 3537-3546**

INTRODUCTION:

In recent years, Internet of Things (IoT) has become an important topic amongst technology enthusiasts and industries. IoT comprises physical devices such as refrigerators, cars, buildings, health monitoring systems, and many others which are embedded with sensors, actuators, radio frequency identification (RFID) tags, and software. These things are connected to a network (Internet) that enables them to exchange and collect data. IoT has stepped out from its infancy and is on the path of transforming our current understanding of a static Internet to a fully integrated dynamic future Internet [1]. Zigbee, Z-Wave, 6LoWPAN, Wi-Fi, GSM/3G/4G/LTE, LoRa, Neul, and Sigfox are all communication technologies used in IoT. Currently, Zigbee is the most used technology in home automation and smart lighting. Zigbee is expected to capture 34% volume share of the home automation and 29% of the smart lighting markets by 2021 with Compound Annual Growth Rate (GACR) of 26% during the period of 2016–2020 [2]. Seeing the fast growth of IoT usage, and Zigbee communication specifically, has sparked the attention of research communities to investigate the security concerns that the IoT industry faces.

Securing IoT systems in communication technology has been the concern of many researchers and private companies. Symantec has reported that 52% of health apps connected to wearable devices do not have a privacy policy in place, and 20% of personal information, logins, and passwords are in clear texts [3]. In May 2014, more than 90 people from 19 different countries in connection with “creep ware” were arrested by the FBI and the police for using internet-connected webcams to spy on people [4]. Many researchers have also found that many cars, hospitals, oil grids, and energy grids connected to an IoT system are vulnerable to cyber attacks [5]. As for Zigbee security concerns, much research and many experiments have been conducted to better understand the security threats to which it is susceptible [6 – 11]. Despite the fact that Zigbee protocol could be hacked in many different ways, researchers have agreed that solving the security issues in IoT does not only depend on securing the IoT devices and their communication technology, but also on securing the IoT system as a whole and developing a full solution IoT framework that involves multiple layers of security [12 – 17].

The security threats of Zigbee protocol can be divided into Attacks Requiring Key Compromise and Attacks with Unrequited Key Compromise. In order to prevent the acquisition of Zigbee keys by an attacker, the keys must be preloaded out-of-band and cannot be transmitted over the air, and Zigbee devices’ physical location should be secured at all times. Olawumi et al. [18] suggest that the Standard Security level (sending the network key unencrypted over air) should be removed altogether from the Zigbee protocol. Also, default configurations of keys or fallback default keys should not be allowed by the manufacturers. Two existing main attacks of Unrequited Key Compromise are Replay and Denial of Service (DoS). The Frame counter has been added to the frame header at the Network Layer to avoid Replay Attacks [13, 17]. Cache et al. [18] suggested that Replay Attacks could be avoided by configuring the Zigbee protocol in a way to confirm that the sequence number of the newly received packet is at least one number greater than that received previously. DoS Attacks are very common in the attacks related to IoT in general. DoS Attacks can be divided into Insider DoS Attacks and Outsider DoS Attacks. Insider DoS Attacks can happen at the Application Layer (APL) by flooding the network with messages. For example, an attacker can send a load of messages without any delays, which causes the whole network to freeze. Also, Insider DoS Attacks can happen at the Network Layer (NWK) by stopping the forwarded transmission of data between devices that can alter the routing protocol. Once an attacker joins the network, he/she basically has complete control of almost everything in the network. Insider DoS Attacks can be prevented by not allowing unauthenticated devices to join the network and also by enabling security in the network. Outsider DoS Attacks can happen at the medium access layer. An attacker can send data continuously over the channel which denies any other devices to communicate to each other. DoS Attacks can also be avoided by placing a device that detects external signal interference close to the Zigbee network. Cache et al. [18] also suggested tracking the energy depletion of the Zigbee devices, since a DoS Attack depletes the power of the devices much faster than normal. Another strategy is mitigation by maintaining a list of the misbehaving nodes; if the victim node observes messages with bogus security headers, it will add the sender node to the blacklist and inform the network. To address the illegitimate sessions with consumer devices using Wi-Fi, J. Han et al. [19] proposed a novel Security-enhanced Push Button Configuration (SePBC) scheme with which one can uncover suspicious or malicious devices. Based on the above-mentioned research works in securing IoT systems, it is obvious that additional security measures could be added to better secure Zigbee communication in IoT.

This work focuses on various potential attacks in Zigbee protocol and analysis of potential security threats in Zigbee communication protocol. Based on the analysis, we have designed and implemented a Security Improvement Framework (SIF) of Zigbee network that could efficiently solve several potential security concerns for intelligent monitoring in the IoT platform. Our proposed SIF is able to configure Zigbee devices in the IoT framework in a secured manner (instead of default configuration), predict various potential malicious Zigbee network threats (Replay Attack, Flooding Attack, Physical Attack, etc.), overcome Replay and Flooding Attacks, and notify system administrators in real time while there is any Physical and/or Flooding Attacks. It works on the basis of (i) setting up multiple layers of defense, where multiple layers of security could be used to defend a particular risk by using additional encryption to the data transmitted among Zigbee devices; (ii) educating consumers about privacy and data security by giving them the autonomy to track (in real time) any motion activities detected around them and set up the time period that they should be notified of any suspicious activities that occurs; (iii) configuring and securing Zigbee communication devices, instead of using default configuration; (iv) predicting potential malicious attacks by detecting the absence of a Zigbee node in the network and responding accordingly through a notification to the user and to the systems management team. The proposed SIF has also been implemented in an office security system (that consists of RFID cards as things of IoT) to detect the authorized/unauthorized office staff in the office and notify the administrator of the activities, which allow the administrator to monitor those activities in real time through a suitable web application.

2. SECURITY THREATS AND THE METHOD OF ALLEGATION

When packages are encrypted using the 128-bit Advanced Encryption Standard, Zigbee security is applied to the Network and Application layers (AES). A network encryption key and, perhaps, a link encryption key are used to encrypt data. To be able to connect with one another in the network, devices must have the same keys. By encrypting the APS layer and application data, network layer security is provided by utilizing a network key to protect broadcast transmission. All data packages will be encrypted with the network encryption key if security is enabled on the network. All packages delivered are subject to network layer security, which is encrypted and decoded in each network node; however, medium access layer communication, such as beacon messages, is not covered by this security. Utilizing a shared link key to encrypt application data during unicast communication between the source and destination devices is how application layer security is achieved [9]. Given the significance of security for Internet of Things (IoT) devices, numerous researchers have investigated and validated the security risks associated with the Zigbee communication protocol as well as mitigation techniques. Zigbee protocol security threats are classified into two categories: (1) attacks that need key compromise and (2) attacks that do not. We discuss potential scenarios and techniques that could expose Zigbee to malicious attacks in each of these categories, and we offer mitigation strategies for each of them. Zigbee protocol is illustrated in Figure 1 with numerous attack categories.

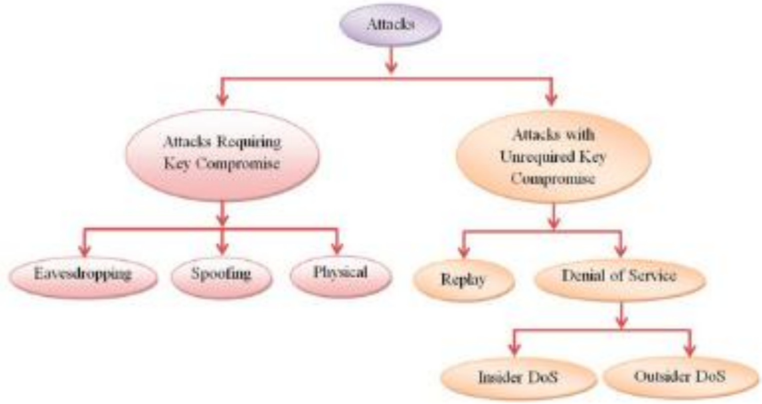

Figure 1. Types of Attack

A physical attack can be used to retrieve the network key or link key in the Zigbee protocol [20, 21]. The flash memory of Zigbee devices can be physically accessed in order to extract the keys. Additionally, Zigbee does not render the keys useless when a device is disconnected from the network. It creates fresh ones that enable network wide balancing. The software, which contains the encryption keys, was recovered from the Zigbee devices by a number of researchers who physically accessed the devices. N. Vidgren et al. [17] showed two real-world assaults against Zigbee security.

An attacker can sniff a packet or record packet traffic in a network using replay attacks, and then send it back at a later date to launch a malicious attack. However, Denial of Service (DoS) is still a problem and no effort has been made in this area. Zigbee alliance had made good efforts to accomplish authenticity and confidentiality to the transmitted packets. Depending on whether the attacker entered the network (an insider DoS attack), multiple stack layers may be impacted by this type of assault (outsider DoS attack). The physical, medium access control, network, and application layers are all susceptible to DoS attacks if the attacker has joined the network; however, if the attacker is an outsider, only the physical and medium access control layers are susceptible. The assaults at various OSI (Open Systems Interconnection) layers are depicted in Figure 2.

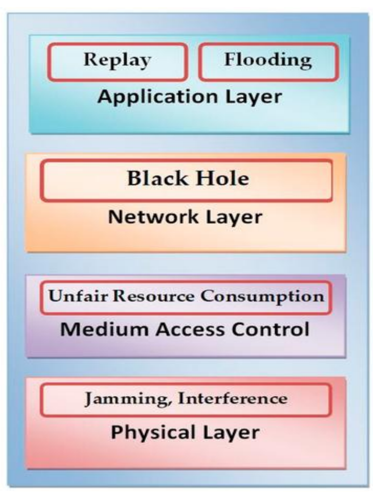

Figure 2. Denial of Service (DoS) attacks at the OSI layers

In contrast to the present Zigbee protocols, we have suggested three relief approaches that can identify Physical Attacks and effectively defend against Replay Attacks and Flooding Attacks.

3. PROPOSED SECURITY IMPROVEMENT FRAMEWORK (SIF)

In order to secure the Zigbee network within the IoT framework, we have suggested a Security Improvement Framework (SIF) utilizing the Zigbee protocol. The proposed SIF's block diagram is shown in Figure 3. This Security Improvement Framework (SIF physical)'s layer is based on the IEEE 802.15.4 standard. It is the layer that is most directly connected to the hardware that controls and interacts with the radio transceiver. It manages all operations involving access to the Zigbee hardware, including hardware initialization, channel selection, estimation of connection quality, measurement of energy detection, and clear channel assessment to aid in channel selection. This layer modulates and demodulates signals as they are sent and received, accordingly. It supports the 2.45 GHz band, which has 16 channels, the 915 MHz band, which has 10 channels, and the 868 MHz band, which has just one channel. Direct Spread Spectrum Sequencing (DSSS) access technique is used across all frequency bands.

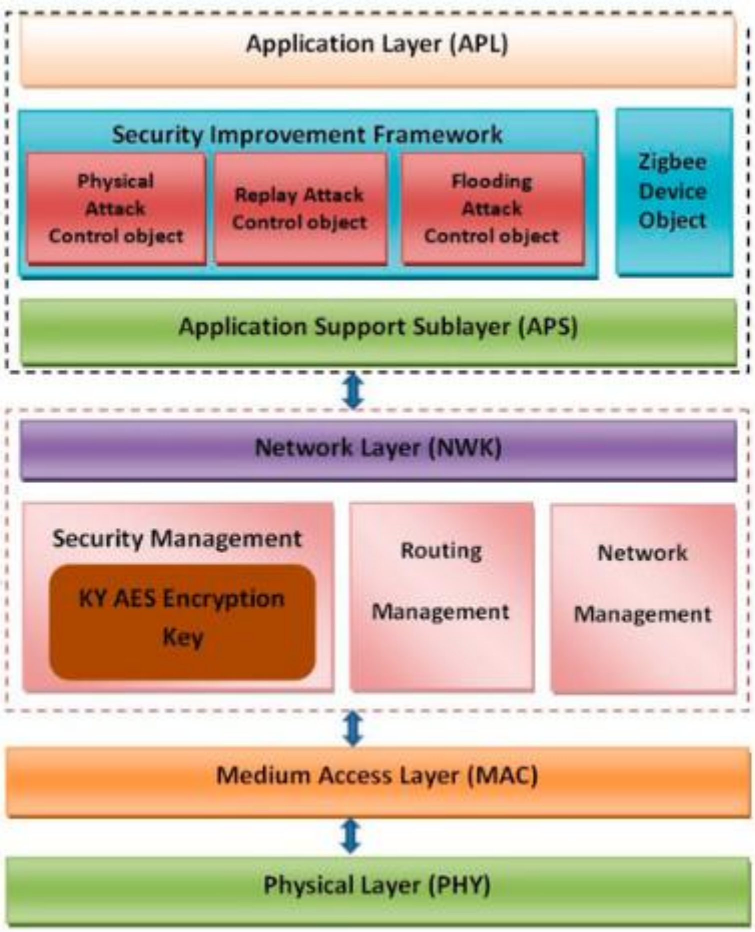

Figure 3. Proposed Security Improvement Framework (SIF) in the IoT platform

An interface between the physical layer and the network layer is provided by the Medium Access Control (MAC) layer. This layer is in charge of ensuring secure data transmission by connecting to various networks using CSMA/CD (carrier sense multiple access collision avoidance/carrier detection). This offers two services: MAC data services and MAC management services that interface with the MLMESAP service access point for the MAC sub layer management entity (MLME). MAC Protocol Data Units (MPDUs) can be sent and received over the PHY data service thanks to the MAC data service. Application layer and MAC Layer are interfaced by the network layer. All network-related tasks, such as network configuration, end device connection and disconnection from the network, routing, device configurations, and so forth, are handled by the network layer. It supports the star network, tree network, and mesh network topologies. In place of the manufacturer's recommended default key configuration, we have used KY AES Encryption for security management.

The network layer and various data management services are interfaced through the application support sub layer. Zigbee device objects and application objects are used to provide these services. Various management tasks, such as security management, network management, and binding management, are carried out by Zigbee Device Objects (ZDOs). They are helpful in defining the different kinds of network-connected devices. In Zigbee devices, ZDO acts as an interface between the APS layer and application layer objects. It is in charge of locating, starting, and connecting additional devices to the network. Methods for key creation, key transfer, frame security, and device management are all included in the Security Service. Three modules that can identify and defend against Physical, Replay, and Flooding Attacks have been proposed: Physical Attack Control Object, Replay Attack Control Object, and Flooding Control Objects in Application Framework.

3.1. PHYSICAL ATTACK CONTROL OBJECT

It is insufficient to secure the Zigbee network by merely securing device configurations. As a result, the coordinator of the Zigbee network is not alerted when a node is removed from it, and the other devices still connected to the network are not sent a new network key. To stop any stolen Zigbee device from being reused, rejoining the network, and posing a security risk, it is essential to identify the absence of a node in the network. Physical Attack Control Object is used to stop any potential physical attacks on Zigbee devices. In the event that the coordinator does not receive a signal from the end devices, this module creates a "Pulse Beat" between the coordinator and the end devices that will alert the user or administrator. To address the Zigbee protocol's inability to identify absent nodes in the network, the Pulse Beat implementation has been included.

The Pulse Beat is an encrypted message that is transmitted periodically by the sender every 200 ms to let the receiver know it is there. If the receiver doesn't receive a message within 2 s, it will alert the user. Implementing the Pulse Beat will stop any potential future network attacks by alerting the user to both the sender's potential fault and its absence from the network. We have encrypted all of the data that will be transferred at the application levels in addition to the Pulse Beat implementation. The receiver will send a "Http Request" to the web application, which will show the admin "No Physical Attack" if the Pulse Beat message is valid. The flow chart for the proposed SIF's Router, Coordinator, Web server, and Admin to identify Physical Attack is shown in Figure 4. Every 200 ms, the sender will send a Pulse Beat signal that is encrypted to the receiver to communicate its existence in the network. The Pulse Beat message will be decrypted by the receiver in turn. The receiver sends an HTTP request to the web application that displays the admin "Physical attack" when the transmitter is no longer available or when there isn't any Pulse Beat signal for 2 seconds.

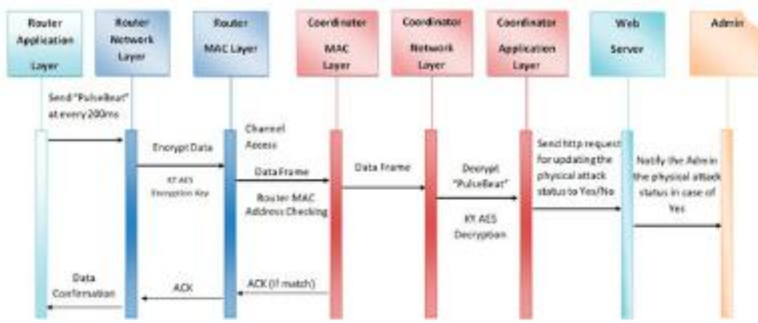

Figure 4. Router, Coordinator, Webserver, and Admin in the Proposed Security Improvement Framework's Sequence Diagram to Detect Physical Attack (SIF).

3.2. REPLAY ATTACK CONTROL OBJECT

When security is not set, replay attacks are simply possible, which results in a Zigbee network operating without any frame counters, encryption, or authentication. An attacker in this situation could sniff the packet using a different Zigbee device linked to a computer and intercept the transmitted packets. Since authentication and frame counters are disabled in the network, an attacker can send the identical packets using any Zigbee device, replay them, or even change the data they carry. This would cause an unacceptable behavior in the network. Pseudo codes are employed in the Replay Attack Control Object to recognize and prevent Replay Attack.

3.3. FLOODING CONTROL OBJECT

At the Application Layer (APL), insider DoS attacks can take place by sending a lot of messages over the network. Without any delays, an attacker may send a large number of messages, possibly bringing down the entire network. By acting as a trust centre, the coordinator can stop flooding attacks. Additionally, a network encryption key is configured, as well as a connected encryption key. The Flooding Attack is prevented via an algorithm that is described. Receiving data are counted concurrently with a 200 ms delay. The receiving data is discarded if the number of received data exceeds the preset value due to flooding. When flooding effect is detected, the administrator is notified via a web application status message.

4. THE PROPOSED SECURITY IMPROVEMENT FRAMEWORK'S INSTALLATION (SIF)

An office security system is equipped with the proposed Security Improvement Framework (SIF) for intelligent monitoring using the Zigbee protocol on the IoT platform. Employees are not permitted to enter certain areas of the office due to its division into different areas. To enter any office space, employees must present their RF identity cards. Any employee may enter any office space by touching his or her card to the RF card reader. Readers are equipped with the Router Zigbee connection module. The coordinator, a central controller, receives reading data from the router. In order to unlock the door, the coordinator must receive a request from an employee who wants to enter the designated office space. On the other side, if an employee requests access to a restricted office space, the coordinator will deny the request and email the administrator to let them know. Additionally, the framework successfully identifies and defends against such efforts if a hacker tries to attack the system.

5. QUALITY OF PROTECTION (QOP) IN THE PROPOSED SECURITY IMPROVEMENT FRAMEWORK (SIF)

We have evaluated the security attributes and functionality of the suggested architecture using quantitative measurements called Quality of Protection (QoP). Large-scale Zigbee deployments are made possible by security, which is expected to be more secure than current network options. To meet the objectives of service providers and customers, Zigbee security must be handled comprehensively in order to achieve this goal. A collection of security solutions are suggested after looking at potential security risks to Zigbee protocols. As a way to quantitatively show the connection between security policies and system performance, QoP focuses on the effects of security mechanisms on system performance. To address various security risks in Zigbee protocols, the suggested solutions are based on the application layer and make use of the KY AES Encryption Key at the network layer.

6. EVALUATION OF THE PROPOSED SECURITY IMPROVEMENT FRAMEWORK (SIF)

Employees had to enter the workplace and each person's room using their identity card as part of the office security system. With a 500 ms delay, the router that reads the identity card transfers the data to the coordinator. This system is capable of spotting and defending against any attempts by hackers to conduct a flooding attack. We sent a number of signals from router to coordinator to assess the likelihood of the office security system flooding. The coordinator counts the messages that are arriving simultaneously while reading the messages with a 200 ms delay. In relation to message volume and delay, we have plotted flooding likelihood curves for the office security system. This graphic shows that the flooding chance is 1 for message counts larger than 7. Flooding is deemed to have occurred if the Security Improvement Framework (SIM) receives more than 7 messages at once with a 200 ms reception delay.

Every 200 ms, the router transmits an encrypted Pulse Beat signal to the coordinator to verify its own presence in the network. The coordinator decrypts the Pulse Beat message in turn. The coordinator sends an HTTP request to the web application that displays the physical attack status (Yes/No) to the admin when the router is compromised or when it fails to provide the coordinator a Pulse Beat signal within 2 seconds of receiving one. We repeatedly turned the router off while monitoring the signal strength. The system consistently detected the Physical Attack with success.

Quality of Service (QoS) guarantees for users and network performance are always negatively impacted by security solutions. Users' certificates must be transported by security solutions in order to confirm users' identities and encrypt data for confidentiality. These cause longer transmission delays, which decrease system throughput and service quality. Furthermore, complicated security features always raise the price of performance significantly, especially when there are resource limitations. As a result, considering security advantages alone is insufficient to provide customers with multilevel security service in the SIF; additionally required is a thorough quantitative analysis of the effects of all security measures on performance. Performance is seen to generally decline as security policies offer greater advantages. 1200 ms is the maximum signaling delay, which is sufficient for real-time applications.

7. CONCLUSION

This study's major objective is to highlight the value of Zigbee protocol security in the Internet of Things. Message flooding, replay attacks, and other popular IoT real-world assaults are used in this study to discuss the security dangers to Zigbee. To learn how to stop them, those attacks have been the subject of experiments. To guard against a variety of potential security breaches, we have developed the Security Improvement Framework (SIF), which incorporates all the suggested methods. Multiple layers of defense were used in the designed IoT framework to foresee and stop potential harmful assaults. By maintaining a communication signal between any two communicating nodes in the network, the framework can address the issue of the Zigbee protocol failing to notice a missing node. A secure device configuration is utilized rather than the usual device setup. Messages are also encrypted and decoded using a 128-bit Advanced Encryption Standard (AES) key. We have evaluated the security attributes and functionality of the suggested architecture using quantitative measurements called Quality of Protection (QoP). Results show that this framework is a more effective security threat defense than the current Zigbee protocol. A security system for offices uses this foundation. The coordinator sends an email denying permission and notifying the administrator if an employee attempts to enter their restricted office space. Additionally, the IoT framework effectively identifies and defends against any hacker attempts to attack the system.

References:

1. Gubby, J.; Buyya, R.; Marusic, S.; Palaniswami, M. *Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions*; Technical Report CLOUDS-TR-2012-2; Cloud Computing and Distributed Systems Laboratory, The University of Melbourne: Melbourne, Australia, 29 June 2012.
2. Milman, R.; Bluetooth and Zigbee to Dominate Wireless IoT Connectivity. Internet of Business. Available online: [https://internetofbusiness.com/iotdriving- wireless-connectivity/](https://internetofbusiness.com/iotdriving-wireless-connectivity/) (accessed on 20 May 2018).
3. Nurse, J.R.C.; Creese, S.; Roure, D.D. Security Risk Assessment in Internet of Things Systems. *IT Prof.* **2017**, *19*, 20–26.
4. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, India, 17–19 December 2012; pp. 257–260.
5. Al-Fuqaha, A.; Guizani, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376.
6. Ali, B.; Awad, D.A.I. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* **2018**, *18*, 817.
7. Betzler, A.; Gomez, C.; Demirkol, I.; Paradells, J. A Holistic Approach to Zigbee Performance Enhancement forHome Automation Networks. *Sensors* **2014**, *14*, 14932–14970.
8. Radmand, P.; Domingo, M.; Singh, J.; Arnedo, J.; Talevski, A.; Petersen, S.; Carlsen, S. Zigbee/Zigbee PRO security assessment based on compromised cryptographic keys. In Proceedings of the International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Krakow, Poland, 4–6 November 2010.

9. Olawumi, O.; Haataja, K.; Asikainen, M.; Vidgren, N.; Toivanen, P. Three Practical Attacks Against Zigbee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned. In Proceedings of the IEEE 14th International Conference on Hybrid Intelligent Systems (HIS2014), Hawally, Kuwait, 14–16 December 2014.
10. Kocher, I.S.; Chow, C.-O.; Ishii, H.; Zia, T.A. Threat Models and Security Issues in Wireless Sensor Networks. *Int. J. Comput. Theory Eng.* **2013**, *5*, 5.
11. Brodsy, J.; McConnell, A. Jamming and Interference Induced Denial-of-Service Attacks on IEEE 802.15.4-Based Wireless Networks. In Proceedings of the Digital Bond's SCADA Security Scientific Symposium, Miami Beach, FL, USA, 21–22 January 2009.
12. CISCO. Securing the Internet of Things: A Proposed Framework. Available online: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html (accessed on 20 May 2018).
13. Pasquier, I.B.; Kalam, A.A.E.; Ouahman, A.A.; Montfort, M.D. *A Security Framework for Internet of Things*; Springer International Publishing: Basel, Switzerland, 2015.
14. Wu, T.; Zhao, G. A Novel Risk Assessment Model for Privacy Security in Internet of Things. *Wuhan Univ. J. Nat. Sci.* **2014**, *19*, 398–404.
15. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 2006. Available online: https://ieeexplore.ieee.org/document/4040999/ (accessed on 20 May 2018).
16. Durech, J.; Franekova, M. Security attacks to Zigbee technology and their practical realization. In Proceedings of the IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI 2014), Herl'any, Slovakia, 23–25 January 2014.
17. Vidgren, N.; Haataja, K.; Patino-Andres, J.L.; Ramırez-Sanchis, J.J.; Toivanen, P. Security Threats in Zigbee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned. In Proceedings of the 46th Hawaii International Conference on System Sciences, Wailea, HI, USA, 7–10 January 2013.
18. Cache, J.; Wright, J.; Liu, V. *Hacking Exposed Wireless: Wireless Security Secrets and Solutions*, 2nd ed.; McGraw-Hill: New York, NY, USA, 2010.
19. Han, J.; Park, T. Security-Enhanced Push Button Configuration for Home Smart Control. *Sensors* **2017**, *17*, 1334.
20. Lee, K.; Lee, J.; Zhang, B.; Kim, J.; Shin, Y. An enhanced Trust Center based authentication in Zigbee networks, Advances in Information Security and Assurance. In Proceedings of the International Conference on Information Security and Assurance, Seoul, Korea, 25–27 June 2009; pp. 471–484.
21. Dini, G.; Tiloca, M. Considerations on Security in Zigbee Networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Newport Beach, CA, USA, 7–9 June 2010; pp. 58–65.
22. Luo, A.; Lin, C.; Wang, K.; Lei, L.; Liu, C. Quality of protection analysis and performance modeling in IP multimedia subsystem. *Comput. Commun.* **2009**, *32*, 1336–1345.
23. Chigan, C.; Ye, Y.; Li, L. Balancing security against performance in wireless Ad Hoc and sensor networks. In Proceedings of the IEEE 60th Vehicular Technology Conference (VTC 2004), Los Angeles, CA, USA, 26–29 September 2004; pp. 4735–4739.