applied sciences

MDPI

Article

Design and Implementation of a Security Improvement Framework of Zigbee Network for Intelligent Monitoring in IoT Platform

S M Sohel Rana [1], Miah Abdul Halim [2] and M. Humayun Kabir [1,*]

[1] Department of Electrical and Electronic Engineering, Islamic University, Kushtia 7003, Bangladesh; smsr.aece@gmail.com

[2] Department of Mechanical Engineering, University of Utah, Salt Lake City, UT 84112, USA; halim.miah@utah.edu

* Correspondence: h.2011.kabir@gmail.com; Tel.: +880-716-2205 (ext. 2270)

Received: 8 November 2018; Accepted: 16 November 2018; Published: 20 November 2018

Abstract: Internet of Things (IoT) opens new horizons by enabling automated procedures without human interaction using IP connectivity. IoT deals with devices, called things, represented as any items from our daily life that are enhanced with computing or communication facilities. Among various mobile communications, Zigbee communication is broadly used in controlling or monitoring applications due to its low data rate and low power consumption. Securing IoT systems has been the main concern for the research community. In this paper, different security threats of Zigbee networks in the IoT platform have been addressed to predict the potential security threats of Zigbee protocol and a Security Improvement Framework (SIF) has been designed for intelligent monitoring in an office/corporate environment. Our proposed SIF can predict and protect against various potential malicious attacks in the Zigbee network and respond accordingly through a notification to the system administrator. This framework (SIF) is designed to make automated decisions immediately based on real-time data which are defined by the system administrator. Finally, the designed SIF has been implemented in an office security system as a case study for real-time monitoring. This office security system is evaluated based on the capacity of detecting potential security attacks. The evaluation results show that the proposed SIF is capable of detecting and protecting against several potential security attacks efficiently, enabling a more secure way of intelligent monitoring in the IoT platform.

Keywords: real-time intelligent monitoring; Zigbee protocol; internet of things (IoT), office security system; security threats

1. 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 "creepware" 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 cyberattacks [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 Unrequired 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 Unrequired 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 in Zigbee Protocol and the Alleviation Method

Zigbee security is applied to the Network and Application layers where packages are encrypted with 128-bit Advanced Encryption Standard (AES). Data is encrypted by using a network encryption key and possibly a link encryption key. Devices have to have the same keys to be able to communicate among each other in the network. The network layer security is implemented by using a network key to secure broadcast communication by encrypting the APS layer and application data. If security is enabled in the network, all data packages will encrypt with the network encryption key. Security at the network layer applies to all packages transmitted and is encrypted and decrypted in each node of the network; however, this security does not apply to the medium access layer communication, such as beacon messages. Application layer security is implemented by using a shared link key to secure the unicast communication between the source and the destination devices to encrypt application data [9]. Considering the importance of the security in IoT devices, the security threats in Zigbee communication protocol and the mitigation methods have been researched and proven by many researchers. We have divided security threats of Zigbee protocol into two categories: (1) Attacks Requiring Key Compromise, and (2) Attacks with Unrequired Key Compromise. In each of these categories, we go over scenarios and methods that could expose Zigbee to malicious attacks, and we suggest mitigation methods for each one of them. Figure 1 shows various attack categories in Zigbee protocol.

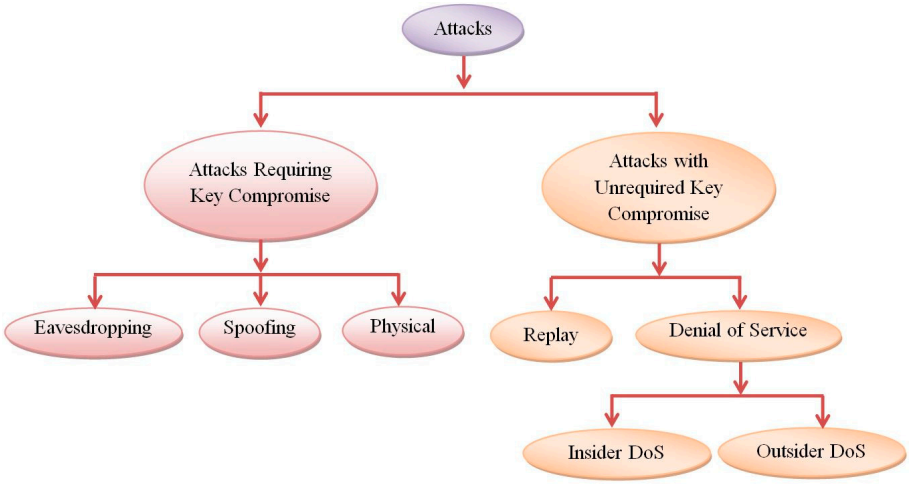


Figure 1. Attack categories in Zigbee protocol.

Network key or link key in Zigbee protocol can be obtained by a Physical Attack [20,21]. The keys can be extracted from Zigbee devices' flash memory while a physical access is achieved. Also, when a device is removed from the network, Zigbee does not invalidate the keys. It generates new ones that

allow tempering the whole network. Several researchers gained physical access to the Zigbee devices and have extracted the firmware which contains the encryption keys. Two practical attacks against Zigbee security were demonstrated by N. Vidgren et al. [17].

Using Replay Attacks, an attacker can sniff a packet or record packet traffic in a network and send it back at a later time to cause a malicious attack. Zigbee alliance had put in a good effort to achieve authenticity and confidentiality to the communicated packets; though, Denial of Service (DoS) is still an issue and no effort has been done in this area. Multiple stack layers could be affected by this type of attack and that depends on whether the attacker has joined the network (insider DoS attack) or not (outsider DoS attack). If the attacker has joined the network, the DoS may be conducted at the physical, medium access control, network, and application layers, but in case it is an outsider, the DoS could happen only at the physical and medium access control layers. Figure 2 shows the attacks at several OSI (Open Systems Interconnection) layers.

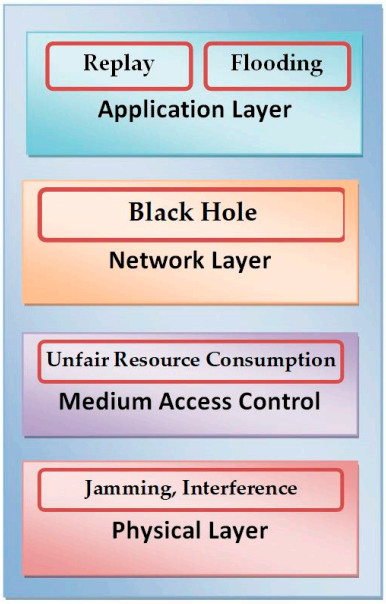


Figure 2. Denial of Service (DoS) attacks at the OSI layers of Zigbee protocol.

We have proposed three alleviation methods which can detect Physical Attack and protect from Replay Attacks and Flooding Attacks efficiently as compared with the current Zigbee protocols. Table 1 shows the proposed alleviation method used in the Security Improvement Framework (SIF) to resolve various Zigbee network threats. Those three security solutions will be discussed in Section 3.

Table 1. Proposed alleviation methods used in the Security Improvement Framework (SIF).

Threats	Proposed Method
Physical	Algorithm-1 (KY AES Encryption Key and Physical Control Object)
Replay	Algorithm-2 (KY AES Encryption Key and Replay Control Object)
Flooding	Algorithm-3 (KY AES Encryption Key and Flooding Control Object)

3. Proposed Security Improvement Framework (SIF) Using Zigbee Protocol

We have proposed a Security Improvement Framework (SIF) using Zigbee protocol for securing the Zigbee network in the IoT framework. Figure 3 shows the block diagram of the proposed SIF. The physical layer of this Security Improvement Framework (SIF) is based on IEEE 802.15.4 standard. It is the closest layer to the hardware which controls and communicates with the radio transceiver directly. It handles all tasks involving the access to the Zigbee hardware, including initialization of the hardware, channel selection, link quality estimation, energy detection measurement, and clear channel

assessment to assist the channel selection. This layer does modulation and demodulation operations upon transmitting and receiving signals, respectively. It supports three frequency bands, 2.45 GHz band that uses 16 channels, 915 MHz band that uses 10 channels, and 868 MHz band that uses only 1 channel. All frequency bands use Direct Spread Spectrum Sequencing (DSSS) access mode.

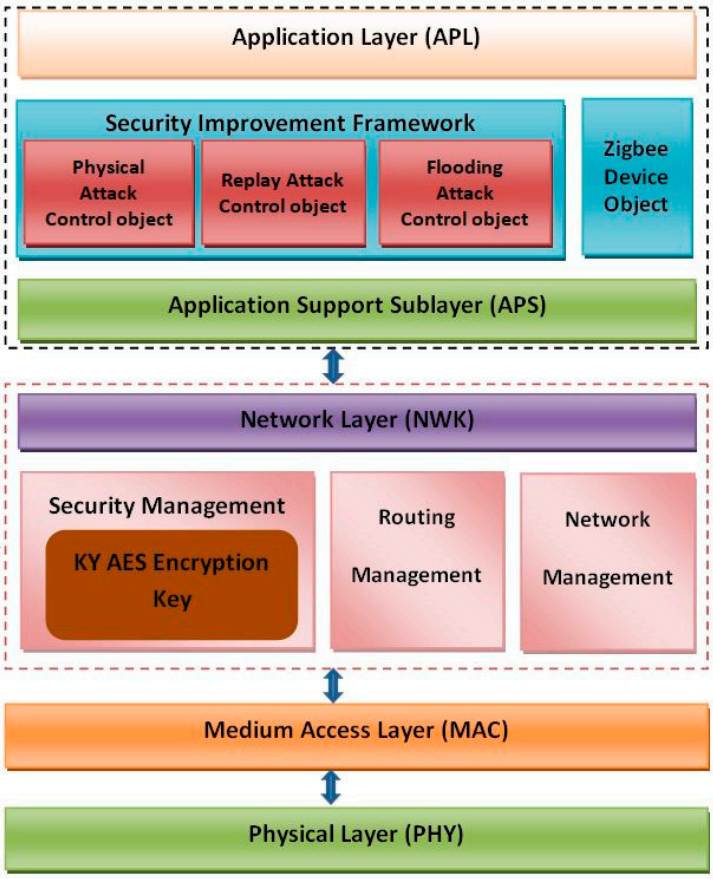


Figure 3. Proposed Security Improvement Framework (SIF) of Zigbee network in the IoT platform.

The Medium Access Control (MAC) layer provides an interface between physical layer and network layer. This layer is responsible for reliable transmission of data by accessing different networks with the carrier sense multiple access collision avoidance/carrier detection (CSMA/CD). This provides two services: MAC data services and MAC management service interfacing to the MAC sublayer management entity (MLME) service access point, called MLMESAP. The MAC data service enables the transmission and reception of MAC Protocol Data Units (MPDUs) across the PHY data service. Network layer interfaces between application layer and MAC Layer. Network layer takes care of all network-related operations such as network setup, end device connection and disconnection to network, routing, device configurations, and so on. It supports three network topologies: star network, tree network, and mesh network. We have used KY AES Encryption in security management instead of default key configuration provided by the manufacturer.

The application support sublayer is used to provide an interface between the network layer and various data management services. These services are provided with the help of application objects and Zigbee device objects. Zigbee Device Objects (ZDOs) are used to perform various management tasks including security management, network management, and binding management. They are also useful to define the types of devices used in the network. ZDO provides an interface between application layer objects and the APS layer in Zigbee devices. It is responsible for detecting, initiating, and binding other devices to the network. Security Service includes methods for key establishment, key transport, frame protection, and device management. We have proposed three modules: Physical Attack Control

Object, Replay Attack Control Object, and Flooding Control Objects in Application Framework which can detect and protect from Physical, Replay, and Flooding Attacks.

3.1. Physical Attack Control Object

Securing the Zigbee network by only securing devices' configurations is not sufficient. Therefore, removing a node from the Zigbee network is not detected by the network, specifically by the coordinator, and does not generate and send a new network key to the other devices that are still in the network. Detecting the absence of a node in the network is crucial to prevent any stolen Zigbee device from being reused, and from thus rejoining and compromising the network. To prevent any potential Physical Attack of Zigbee devices, Physical Attack Control Object is implemented. This module produces a "Pulse Beat" between the coordinator and the end devices that will notify the user/admin in case the coordinator does not receive any signal from the end devices. The Pulse Beat implementation is added to cover the lack of detection of missing nodes in the network by the Zigbee protocol.

The pseudocodes used to detect Physical Attack is shown in Table 2. The Pulse Beat is an encrypted message sent by the sender repeatedly every 200 ms to indicate its presence to the receiver; in case the receiver does not receive any message in the period of 2 s, it will notify the user. Implementing the Pulse Beat will not only warn the user about a possible malfunctioning of the sender but also about its nonexistence in the network, and will prevent any possible future network attacks. In addition to the Pulse Beat implementation, we have also encrypted all the data that is to be transmitted at the application layers. If the Pulse Beat message is valid, then the receiver will make an "HttpRequest" to the web application that will show the admin "No Physical Attack". Figure 4 shows the sequence diagram of Router, Coordinator, Webserver, and Admin to detect Physical Attack in the proposed SIF. To confirm its presences in the network, the sender will send an encrypted Pulse Beat signal to the receiver every 200 ms. The receiver, in its turn, will decrypt the Pulse Beat message. When the sender becomes unavailable or the receiver does not receive any Pulse Beat signal within 2 s, the receiver will make an HttpRequest to the web application that will show the admin "Physical attack".

Table 2. Pseudocodes used to detect Physical Attack in the proposed SIF using Zigbee protocol.

Algorithm: Physical_Attack_Detect (T_data, R_data, P)	
Data: Transmitting data=T_data, Receiving data=R_data, Pulse_bit=P, **Result:** Physical Attack=P_attack.	
(1)	Start
(2)	Connection==Serial Communication();/*Check serial communication between router and coordinator*/
(3)	If connection==Fail
(4)	Return Start; /*Step 1*/
(5)	End
(6)	If connection==True then
(7)	T_data==Encrypt(data); /*AES 128 bit encryption*/
(8)	If R_data=='P' OR 'H' OR 'L' then /*128 bit decryption*/
(9)	P_attack==No;
(10)	Update Web(P_attack);/*Update web page with no Physical attack data*/
(11)	Send Email(Admin); /*Send email to Admin notifying no Physical attack*/
(12)	Else
(13)	P_attack==Yes;
(14)	Update Web(P_attack);/*Update web page with Physical attack data*/
(15)	Send Email(Admin); /*Send email to Admin notifying Physical attack*/
(16)	End
(17)	End

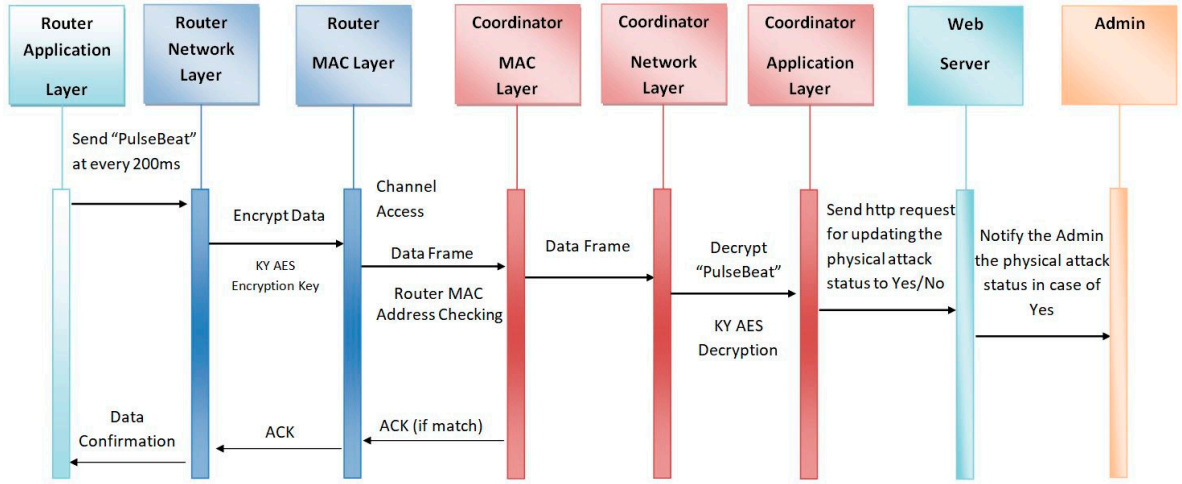


Figure 4. Sequence diagram of Router, Coordinator, Webserver, and Admin to detect Physical Attack in the proposed Security Improvement Framework (SIF).

3.2. Replay Attack Control Object

Replay attack could easily happen in a Zigbee network where security is not enabled, which leads to a Zigbee network operating without any encryption, authentication, or a frame counter. In this case, an attacker can sniff the packet using another Zigbee device connected to a computer and capture the packets transmitted. Since authentication and frame counter are disabled in the network, an attacker can replay the same packets, or even change the data contained in that packet, and send it using any Zigbee device, causing an unaccepted behavior in the network. In the Replay Attack Control Object, pseudocodes are used to detect and protect Replay Attack, as presented in Table 3.

Table 3. Pseudocodes used to protect Replay Attack in the proposed SIF using Zigbee protocol.

Algorithm: Replay_Attack_Protect (T_data, R_data, H, L)	
Data: Transmitting data=T_data, Receiving data=R_data, Authorize bit=H, Unauthorized bit=L. **Result:** Replay_attack=R_attack.	
(1)	Start
(2)	Connection==Serial Communication();/*Check serial communication between router and coordinator*/
(3)	If connection==Fail
(4)	Return Start; /*Step 1*/
(5)	End
(6)	If connection==True then
(7)	T_data==Encrypt(data); /*AES 128 bit encryption*/
(8)	If R_data==‘H’ OR ‘L’ then /*128 bit decryption*/
(9)	If R_data==‘H’ OR ‘L’
(10)	Initialization i, data;
(11)	Fori=1 to 10 do
(12)	Data=data+1;
(13)	Delay==200 ms;
(14)	If Data>7
(15)	R_Attack==Yes;
(16)	Update Web(R_attack);/*Update web page with Replay_attack data*/
(17)	Send Email(Admin); /*Send email to Admin notifyingReplay_attack*/

Table 3. *Cont.*

(18)	Return Start;	/*Step 1*/
(19)	End	
(20)	End	
(21)	End	

3.3. Flooding Control Object

Insider DoS Attacks can happen at the Application Layer (APL) by flooding the network with messages. An attacker may send a bunch of messages without any delays which might cause the whole network to freeze. To prevent Flooding Attack, the coordinator is used as trust center. In addition, linked encryption key and network encryption key are also configured. An algorithm is presented to prevent the Flooding Attack. Receiving data are counted simultaneously at a predefined delay of 200 ms. If receiving data number exceeds the default value, then flooding occurs and it discards the receiving data. The pseudocodes of this module is presented in Table 4. In case of detecting flooding effect, the Admin is notified by status message using web application. To detect and prevent the Flooding Attack, the Flooding Control Object considers the sequence diagram between Router, Coordinator, Webserver, and Administrator as shown in Figure 5.

Table 4. Pseudocodes used to prevent Flooding attack in the proposed SIF using Zigbee protocol.

Algorithm: Flooding_attack_protect (T_data, R_data, P, H, L)		
Data: Transmitting data=T_data, Receiving data=R_data, Authorize bit=H, Unauthorized bit=L. **Result:** Flooding_attack=F_attack.		
(1)	Start	
(2)	Connection==Serial Communication();/*Check serial communication between router and coordinator*/	
(3)	If connection==Fail	
(4)	Return Start;	/*Step 1*/
(5)	End	
(6)	If connection==True then	
(7)	T_data==Encrypt(data); /*AES 128 bit encryption*/	
(8)	If R_data==‘H’ OR ‘L’ then	/*128 bit decryption*/
(9)	Initialization I, data;	
(10)	Fori=1 to 20 do	
(11)	Data=data+1;	
(12)	Delay==200 ms;	
(13)	If Data>7	
(14)	F_Attack==Yes;	
(15)	Update Web(F_attack);/*Update web page with Flooding attack data*/	
(16)	Send Email(Admin); /*Send email to Admin notifyingFlooding attack*/	
(17)	Return Start;	/*Step 1*/
(18)	End	
(19)	End	
(20)	End	
(21)	End	

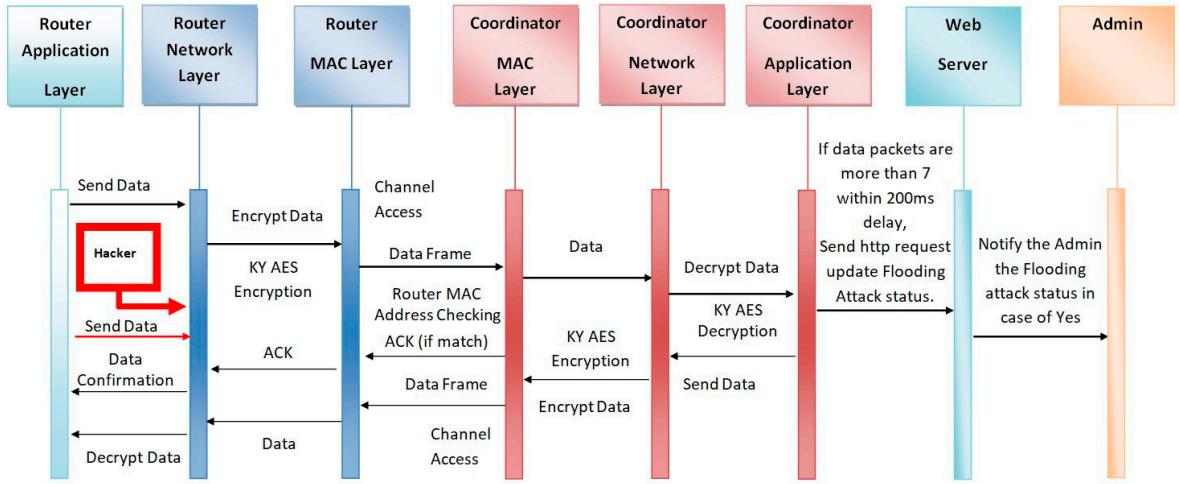
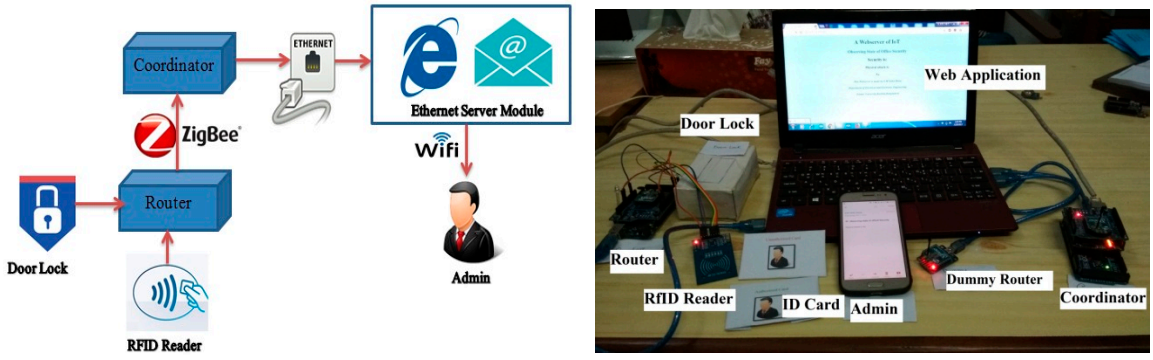


Figure 5. Sequence diagram of Router, Coordinator, Webserver, and Admin to detect Flooding Attack in the proposed Security Improvement Framework (SIF).

4. Implementation of the Proposed Security Improvement Framework (SIF)

The proposed Security Improvement Framework (SIF) using Zigbee protocol in the IoT platform is implemented in an office security system for intelligent monitoring. The office security system testbed is shown in Figure 6. The office area is separated into different locations and employees have restrictions for entering specific areas. All employees must use their RF identity card to enter any office area. When any employee wants to enter any office area, he/she will touch his card on the RF card reader. Readers include the Zigbee communication module which is called Router. Router sends reading information to central controller which is called Coordinator. If any employee wants to enter his/her permitted office area, the coordinator sends permission to unlock the door. On the other hand, if the employee wants to enter a prohibited office area for him/her, the coordinator sends denial of permission and notifies the administrator through email. Moreover, if a hacker tries to attack the system, then the framework detects and protects from such attempts effectively in the same way. The pseudocodes used for the proposed office security system is presented in Table 5.



(**a**) (**b**)

Figure 6. (**a**) Block diagram of the office security system using proposed Security Improvement Framework (SIF); (**b**) photograph of the testbed for implementing the proposed SIF.

Table 5. Pseudocodes used in the proposed Security Improvement Framework (SIF) using Zigbee protocol implemented in an office security system.

Algorithm: Office Security System (T_data, R_data, P, H, L)	
Data: Transmitting data=T_data, Receiving data=R_data, Pulse_bit=P, Authorize bit=H, Unauthorized bit=L. **Result:** Physical attack=P_attack, Flooding_attack=F_attack, Access status=A_status, Door state=D_state.	
(1)	Start
(2)	Connection==Serial Communication();/*Check serial communication between router and coordinator*/
(3)	If connection==Fail
(4)	Return Start; /*Step 1*/
(5)	End
(6)	If connection==True then
(7)	T_data==Encrypt(data); /*AES 128 bit encryption*/
(8)	If R_data=='P' OR 'H' OR 'L' then /*128 bit decryption*/
(9)	P_attack==No;
(10)	Update Web(P_attack);/*Update web page with no Physical attack data*/
(11)	Send Email(Admin); /*Send email to Admin notifying no Physical attack*/
(12)	Else
(13)	P_attack==Yes;
(14)	Update Web(P_attack);/*Update web page with Physical attack data*/
(15)	Send Email(Admin); /* Send email to Admin notifying Physical attack*/
(16)	End
(17)	End
(18)	If R_data=='H' OR 'L'
(19)	Initialization i, data;
(20)	Fori=1 to 20 do
(21)	Data=data+1;
(22)	Delay==200 ms;
(23)	If Data>7
(24)	F_Attack==Yes;
(25)	Update Web(F_attack);/*Update web page with Flooding attack data*/
(26)	Send Email(Admin); /*Send email to Admin notifyingFlooding attack*/
(27)	End
(28)	End
(29)	End
(30)	If R_data=='H' then
(31)	A_status==Authorized;
(32)	D_state==Open;
(33)	UpdateWeb(D_state);/*Update web page with Door state data*/
(34)	Send Email(Admin); /*Send email to Admin notifying authorized access*/
(35)	End
(36)	If R_data=='L' then
(37)	A_status==Un-authorized;
(38)	Door==Lock;
(39)	Update Web(D_state);/*Update web page with Door state data*/

Table 5. *Cont.*

(40)	Send Email(Admin); /*Send email to Admin notifying unauthorized access */
(41)	End
(42)	End

5. Quality of Protection (QoP) in the Proposed Security Improvement Framework (SIF)

We have used Quality of Protection (QoP) as quantitative metrics to assess the security features and performance of the proposed framework. Security is a key enabler of large-scale deployments of Zigbee protocol and is envisioned to provide better security than existing network solutions. In order to accomplish this goal, Zigbee security needs to be addressed in a comprehensive way to meet service provider and customer needs. By examining potential security threats to Zigbee protocols, a set of security solutions is proposed. QoP focuses the impacts of security mechanisms on system performance which demonstrate the relationship between the security policies and system performance quantitatively. The proposed solutions are based on the application layer and utilize the KY AES Encryption Key at the network layer to overcome different types of security threats in Zigbee protocols. The solutions are presented in Table 6.

Table 6. Security solutions in the proposed Security Improvement Framework (SIF).

Security Solutions	Description	Used Layer in Zigbee protocol
Algorithm-1	Physical Attack Detection	Network Layer and Application
Algorithm-2	Replay Attack Prevention	Network Layer and Application
Algorithm-3	Flooding Attack Prevention	Network Layer and Application

Five main security parameters are considered as the QoP parameters: authentication, confidentiality, data integrity, availability, and privacy, which are the fundamental features to offer secure and reliable services in SIF [22]. Table 7 gives the relationship between all the security solutions and the five security parameters.

Table 7. Mapping table of security solution with security parameter.

	Authentication (s_1)	Confidentiality (s_2)	Data Integrity (s_3)	Availability (s_4)	Privacy (s_5)
KY AES Encryption Key	√	-	-	-	√
Physical Attack Detection	-	-	-	√	√
Replay Attack Prevention	√	√	-	-	√
Flooding Attack Prevention	√	√	√	-	√

Security policy is considered as a combination of several solutions. We have proposed four security policies $P = \{P_1, P_2, P_3, P_4\}$, as shown in Table 8.

Table 8. Security policy description.

Security Policy	Description
P_1	KY AES Encryption Key
P_2	Algorithm-1
P_3	Algorithm-1 + Algorithm-2
P_4	Algorithm-1 + Algorithm-2 + Algorithm-3

To reflect the strength of protection of each security policy in the proposed SIF, a Cumulate QoP Reward (CQR) function is defined based on the number of QoP parameters each mechanism

covered. According to Table 7, if $P_r = \{p_1, p_2, \ldots \ldots, p_n\} \subseteq P$, $r = 1, 2, \ldots, 4$ is a set of security policies, then $S = \{s_1, s_2, s_3, s_4, s_5\}$ is a set of security dimension. Therefore, the Cumulative Reward Function (CRF) is presented as

$$CRF(P_r) = \sum_{i=1}^{n} \{\omega(p_i, s_1) + \omega(p_i, s_2) + \omega(p_i, s_3) + \omega(p_i, s_4) + \omega(p_i, s_5)\} \quad (1)$$

According to the definition of CRF, an effective QoP model is determined by the predefined numeric reward matrix $\omega(P_i, s_j)$ which is usually chosen in an empirical way based on the characteristics of security mechanisms. A simple reference matrix of numeric rewards of all the security mechanisms and algorithms on the five dimensions is tabulated in Table 9. The numeric values provide enough flexibility to adjust according to service sensitivity and user security needs, for example, if service is sensitive in Privacy, then numeric reward of Privacy will be much higher [23]. In most cases, the values are equal to 1 if p_i provides benefits to s_j, otherwise 0. Physical Attack Detection provides a guarantee about availability and all other security policies are independent of availability, therefore, its numerical value is set to 2.

Table 9. Numeric reward matrix.

	Authentication (s_1)	**Confidentiality (s_2)**	**Data Integrity (s_3)**	**Availability (s_4)**	**Privacy (s_5)**
KY AES Encryption Key	1	0	0	0	1
Physical Attack Detection	0	0	0	2	1
Replay Attack Prevention	1	1	0	0	1
Flooding Attack Prevention	1	1	1	0	1

Using Equation (1), we have calculated the CRF of each security solution presented in Table 10. Considering CRF values of P_4 as 100%, results are normalized. After normalizing, we got the QoP partition of seven security levels, which reflects strength of protection of each security solution in the proposed SIF.

Table 10. QoP partition based on Cumulative Reward Function (CRF).

	P_1	P_2	P_3	P_4
CRF	2	5	8	12
Normalized (%)	16.66	41.65	66.67	100
QoP Partition	Low (<50%)		Medium (50–80%)	High (>80%)

The results of the security analysis using the QoP model allow us to define clear distinctions on the strength of protection of each security policy in the SIF security solution. Among three proposed Security Policies (P_2, P_3, P_4), P_4 performs best. Security Policy P_4 includes solutions of three potential security threats (Physical, Replay, and Flooding Attacks). Existing Security Policy KY AES Encryption Key, P_1 in present Zigbee protocol, shows the lowest performance among the proposed Security Policies.

6. Evaluation of the Proposed Security Improvement Framework (SIF)

In this office security system, employees used their identity card to enter the office premises and individual's room. The router that reads the identity card sends the information to the coordinator at 500 ms delay. If any hacker tries to do a Flooding Attack, then this system can detect and protect against it. To evaluate the flooding probability of the office security system, we have sent a bunch of messages from router to coordinator. Coordinator reads the messages at 200 ms delay and counts the messages which are coming simultaneously. We have plotted flooding probability curves for the office security system with respect to the number of messages and delays, as shown in Figure 7. This plot indicates that for a number of messages greater than 7, flooding probability is 1. If the Security Improvement

Framework (SIM) gets more than 7 messages simultaneously at a receiving delay of 200 ms, then it decides flooding occurs.

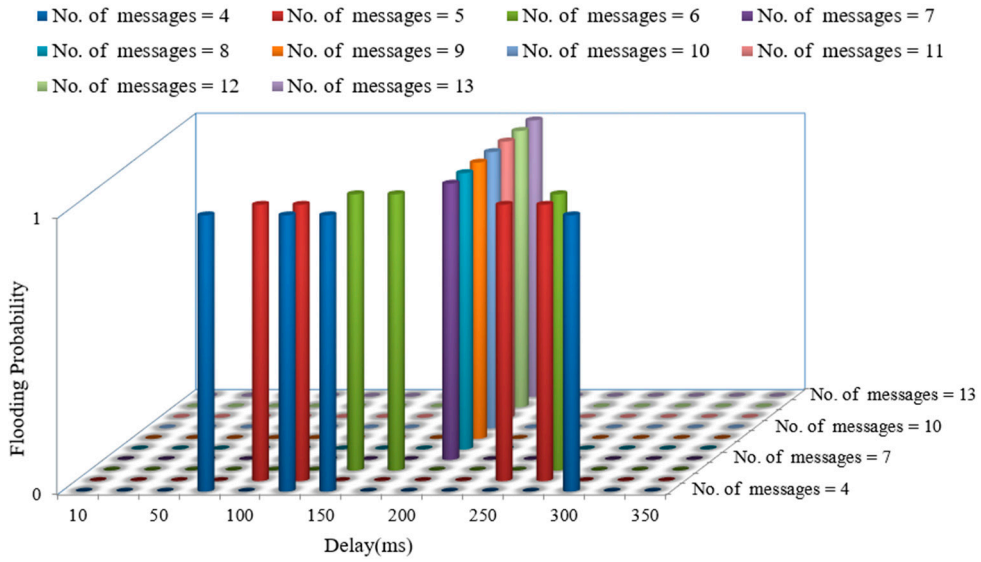


Figure 7. The Flooding Probability curve with respect to number of messages and delays.

To confirm the presence of the router itself in the network, it sends an encrypted Pulse Beat signal to the coordinator every 200 ms. The coordinator, in its turn, decrypts the Pulse Beat message. When the router becomes hacked or the coordinator does not receive any Pulse Beat signal from the router within 2 s, the coordinator makes an Http Request to the web application that shows Physical Attack status (Yes/No) to the admin. We turned the router off several times and checked the status signal. Every time, the system was able to detect the Physical Attack successfully.

Security solutions always have negative impacts on network performance and users' Quality of Service (QoS) guarantees. Security solutions need to transport users' certification to verify identity and to encrypt data for confidentiality. These increase transmission delays, which results in lowering system throughput and quality of service. Moreover, complex security mechanisms always add to the cost of performance much more, especially in resource restrictions. Therefore, in order to provide multilevel security service in the SIF to the users, it is insufficient to take security benefits into consideration only; adequately analyzing the impact of all the security policies on performance quantitatively is also necessary. The average signaling delay for each security policy is shown in Figure 8. It is observed that, in general, performance degrades as security policies provide more benefits. Maximum Signaling Delay is 1200 ms, which satisfies the real-time applications.

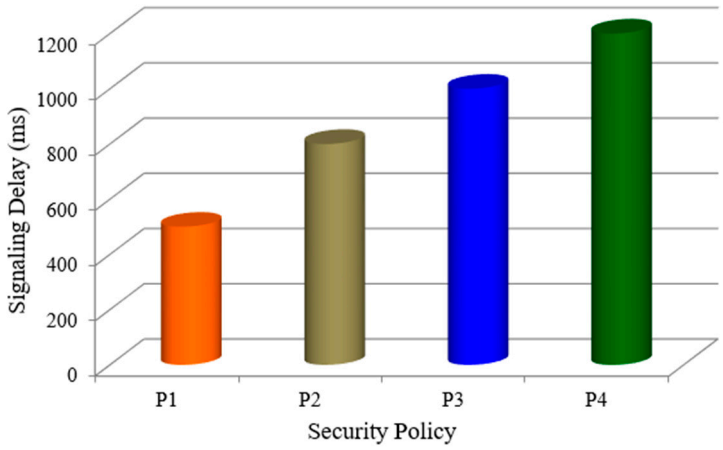


Figure 8. Signaling delay in each security policy of the proposed SIF.

Among three proposed Security Policies (P_2, P_3, P_4), P_4 performs more signaling delays than the others. Security Policy P_4 includes solutions of three potential security threats (Physical, Replay, and Flooding Attacks). Therefore, it requires more time to send the signal. Although existing Security policy P_1 in the present Zigbee protocol shows the lowest signaling delay, Quantitative metrics (QoP) are lower than others, as presented in Section 5.

7. Conclusions

The importance of security of Zigbee protocol in IoT is the main focus of this research. In this research, the security threats of Zigbee are discussed based on some common IoT real-world attacks such as message flooding, Replay Attack, and so on. Experiments of those attacks have been performed to find out a way to prevent them. We have designed Security Improvement Framework (SIF) including all the proposed algorithms to prevent several potential security attacks. The developed IoT framework utilized multiple layers of defense to predict and prevent potential malicious attacks. The framework can solve the problem of failing to detect a missing node in the Zigbee protocol by keeping a communication signal between any pair of communicating nodes in the network. Instead of using default device configuration, a secure device configuration is used. Moreover, messages are encrypted and decrypted with Advanced Encryption Standard (AES) 128-bit key. We have used Quality of Protection (QoP) as quantitative metrics to assess the security features and performance of the proposed framework. Results indicate that this framework can more effectively protect against security threats than the existing Zigbee protocol. This framework is implemented in an office security system. If an employee wants to enter his/her prohibited office area, the coordinator sends denial of permission and notifies the administrator through email. Moreover, if any hacker tries to attack the system, then IoT framework detects and protects against such attempts effectively.

Author Contributions: Conceptualization, M.H.K.; Funding acquisition, M.A.H.; Methodology, S.M.S.R.; Software, M.H.K.; Supervision, M.H.K.; Validation, S.M.S.R.; Writing—original draft, S.M.S.R.; Writing—review & editing, M.A.H. and M.H.K.

Funding: This research was supported by the fellowship from ICT division, Ministry of Posts, Telecommunications and Information Technology, Bangladesh. No. 56.00.0000.028.33.094.18-178, Date 03.05.2018.

Conflicts of Interest: The authors declare no conflict of interests.

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/ (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. [CrossRef]
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. [CrossRef]
6. Ali, B.; Awad, D.A.I. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* **2018**, *18*, 817. [CrossRef] [PubMed]
7. Betzler, A.; Gomez, C.; Demirkol, I.; Paradells, J. A Holistic Approach to Zigbee Performance Enhancement forHome Automation Networks. *Sensors* **2014**, *14*, 14932–14970. [CrossRef] [PubMed]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef] [PubMed]
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. [CrossRef]
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.