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] Dept. of Electrical and Electronic Engineering, Islamic University, Kushtia, Bangladesh ; smsr.aece@gmail.com, h.2011.kabir@gmail.com
[2] Dept. of Mechanical Engineering, University of Utah, Salt Lake City, Utah, USA ; halim.miah@utah.edu
* Correspondence: h.2011.kabir@gmail.com; Tel.: +88-071-62205, Ext. 2270

Abstract: Internet of Things (IoT) opens new horizons by enabling automated procedures without human interaction using IP connectivity. IoT deals with devices, called things which are represented as any item from our daily life that is 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 have been the main concern for the research community. In this paper, different security-threats of Zigbee networks in 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 environment. Our proposed SIF can predict and protect 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 several potential security attacks efficiently enabling more secure way of intelligent monitoring.

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) becomes an important topic amongst technology enthusiasts and industry. IoT constitutes of physical devices such as refrigerators, cars, buildings, health monitoring systems and many others those are embedded with sensors, actuators, radio frequency identification (RFID), 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]. Bluetooth, Zigbee, Z-Wave, 6LoWPAN, WiFi, 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 2016-2020 [2]. Seeing the fast growth of IoT usage, and Zigbee communication specifically has sparked our attention to investigate the securities concerns that the IoT industry faces.

Securing IoT systems in communication technology have been concerned of many researchers and private companies. Symantec has reported that 52% of health apps -many of which connected to wearable devices did not have so much as a privacy policy in place, and 20% personal information, logins, and passwords over the wire in clear text [3]. In May of 2014, more than 90 people from 19 different countries in connection with "creepware" have been arrested by the FBI and the police using Internet-connected webcams to spy on people [4]. Many researchers have also found that many cars, hospitals, oil grids and energy grids those are connected to an IoT 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 that it is susceptible to [6-11]. Despite the fact that Zigbee protocol could be hacked in many different ways, researchers have agreed that solving the problem of security in IoT does not only depend on securing the IoT devices and their communication technology, but on securing the IoT system as whole and developing a full solution IoT framework that involve 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 not transmitted over the air, and Zigbee devices physical location should be secured at all-time. Olawumi et al. [18] suggest that the Standard Security level (sending the network key unencrypted over air) should be removed all together from the Zigbee protocol. Also default configurations of keys or a fall back default keys should not be allowed by the manufacturers. The 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 [19,20]. Cache et al. [21] suggested that replay attacks could be avoided by configuring the Zigbee protocol in a way that it can confirm that the sequence number of the newly received packet is at least one number greater than the sequence number of the previously received one. DoS attacks are very common in the attacks related to IoT in general. Insiders' attacks can happen at the Application Layer (APS) 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 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 basically has a complete control of almost everything in the network. Outsiders' attacks can happen at the medium access layer; Zigbee uses CSMA/CA (if it is running in non-beacon mode). An attacker can send data continuously over the channel. Insider DoS attacks can be prevented by not allowing unauthenticated devices to join the network and also by enabling security in the network. DoS attacks can be also avoided by placing a device that detects external signals interference close to the Zigbee network. Cache et al. [21] suggested tracking the energy depletion of the Zigbee devices, since a DoS attack will deplete the power of the devices much faster than normal. Another, mitigation is to maintain a list of the misbehaving nodes, and if the victim node observes messages with bogus security headers, it will add the sender node to the blacklist and inform the network. Based on all the above researches in securing IoT systems, it is obvious that additional security measures could be added to better secure Zigbee communication in IoT.

This research paper 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 IoT platform. Our proposed SIF is able to configure Zigbee devices in IoT framework in a secured manner instead of default configuration, predict various potential malicious Zigbee network threats: Flooding attack, Physical attack, overcome Flooding and notify system administrator in real time while there is any Physical attack and Flooding. 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 setup the time period that they should be notified of any suspicious activities that occurs,

iii) configuring and securing Zigbee devices communication instead of using default configuration, iv) predicting potential malicious attack, 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/un-authorized office staffs in the office and notify the activities to the administrator which allows 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. Once security is enabled in the network, all data packages are encrypted with the network encryption key. Security at the network layer applies to all packages transmitted and is encrypted and decrypted on 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 [18].
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 attacks categories in Zigbee protocol.

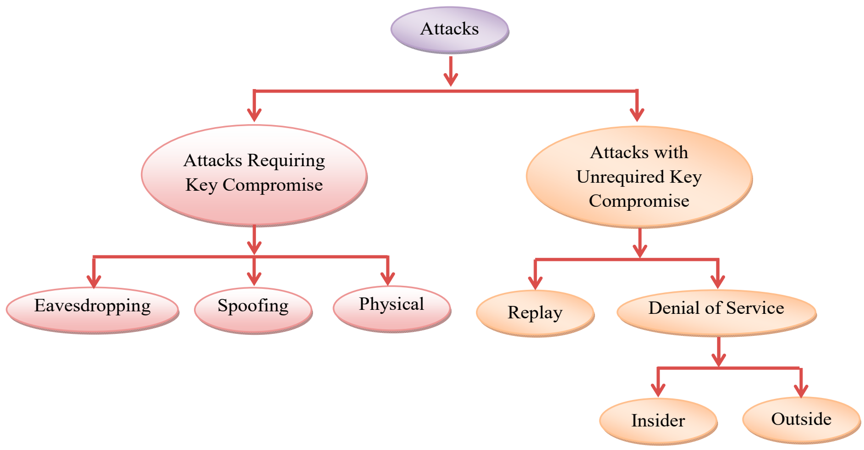


Figure 1. Attacks categories in Zigbee protocol.

Zigbee network or link key can be obtained by a physical attack [22,23]. The keys can be extracted from Zigbee devices' flash memory once a physical access is achieved. Also when a device is removed from the network, Zigbee does not invalidate the keys and generate new ones and that allow tempering the whole network. Several researchers gained physical access to the Zigbee device have extracted the firmware and found the encryption from there. Two practical attacks against ZigBee security were proposed by Niko Vidgren et.al. [17]. Millions of IoT devices use the same cryptographic secrets key; SEC have analyzed more than 4,000 IoT devices in the market from over 70 vendors and extracted the encryption keys from the firmware, and have found that most of the devices use the same keys. The number of unique keys was 580, and out of these 230 were actively used .

Using Replay attacks an attacker can sniff a packet, or record packets traffic in a network and send it back at a later time to cause a malicious attack. Zigbee alliance had put 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 if the attacker has joined the network (insider attack) or not (outsider 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's an outsider the DoS could happen only at the physical and medium access control layers. Figure 2 shows the attacks at several OSI layers.

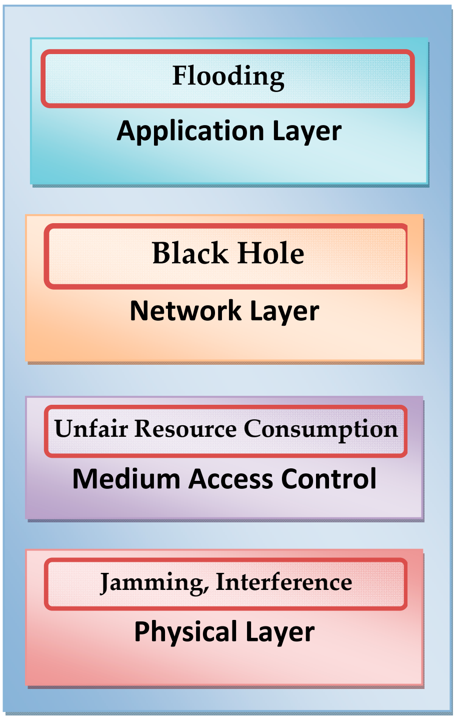


Figure 2. Denial of Service (DoS) attacks at the OSI Layers of Zigbee protocol.

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

We have proposed a Security Improvement Framework (SIF) using Zigbee protocol for securing Zigbee network in the IoT framework. Figure 3 shows the proposed Security Improvement Framework (SIF) whereas Table 1 shows the proposed alleviation method used in the SIF to resolve various Zigbee network threats.

Physical layer of this framework does modulation and demodulation operations upon transmitting and receiving signals respectively. The physical layer works on a frequency bank of 868.3 MHz with the data rate of 20 Kbps. Medium Access Control (MAC) layer is responsible for reliable transmission of data by accessing different networks with the carrier sense multiple access collision avoidance (CSMA)/ carrier detection (CD). Network layer takes care of all network related operations such as network setup, end device connection and disconnection to network, routing, device configurations, etc. We have used KY AES Encryption in security management instead of default key configuration.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 July 2018 doi:10.20944/preprints201807.0227.v1

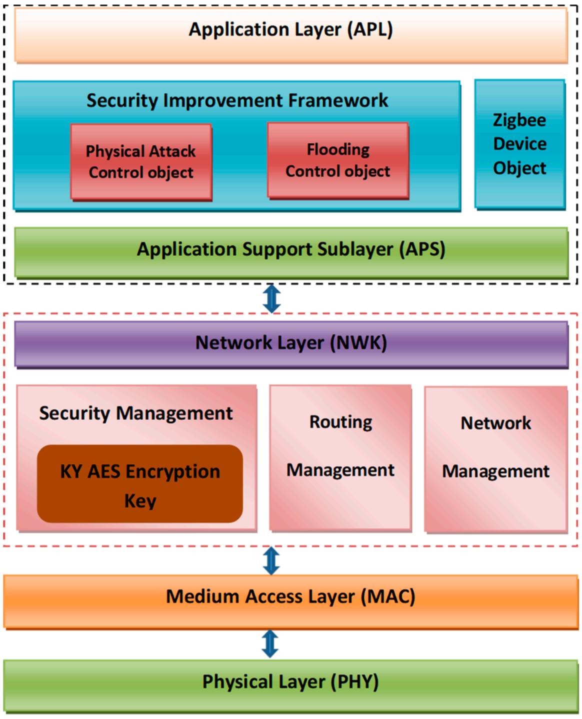


Figure 3. Proposed Security Improvement Framework (SIF) of Zigbee network in the IoT platform.

Table1. Proposed alleviation method used in the Security Improvement Framework (SIF).

Threats	Proposed Method
Physical	KY AES Encryption Key and Pulse Beat
Flooding	KY AES Encryption Key and Application Framework Security

Application support sublayer is used to provide interface between the network layer and various data, management services. These services are providing with the help of application objects and Zigbee device objects. Zigbee Device Objects (ZDO) are used to perform the various management tasks. This includes security management, network management and binding management. It is also useful to define the types of devices which are used in the network. ZDO provides an interface between application layer objects and 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 two modules Physical Attack Control Object and Flooding Control Object in Application Framework which can detect and protect Physical attack and Flooding attack.

3.1 Physical Attack Control Object

Securing the Zigbee network by only securing devices configurations is not sufficient. So removing a node from the Zigbee network is not detected by the network and specifically by the coordinator, and does not generate and send a new network key to the other devices that are still in network. Detecting the absence of a node in the network is crucial to prevent any stolen Zigbee device to be reused thus to re-join and compromise 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. In addition to this configuration, the PAN ID of the network also set to the Zigbee devices and has specified the channel mask that the network should operate on.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 July 2018 doi:10.20944/preprints201807.0227.v1

The flowchart to detect Physical attack is shown in Figure 4. The "Pulse Beat" is an encrypted message sent by the sender repeatedly every 200ms to indicate its presence to the receiver; in case of the receiver does not receive any message in the period of 2 seconds 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, and the secure configuration of the Zigbee devices, we have also encrypted all the data that being transmitted at the application layers. If the "Pulse Beat" message is valid then receiver will make an "HttpRequest" to the web application that will show the admin "No Physical attack". Figure 5 shows data flow between 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 200ms. The receiver in its turn will decrypt the "Pulse Beat" message. When the sender becomes unavailable or receiver does not receive any "Pulse Beat" signal from the sender within 2 seconds the receiver that will make an "HttpRequest" to the web application that will show the admin "Physical attack".

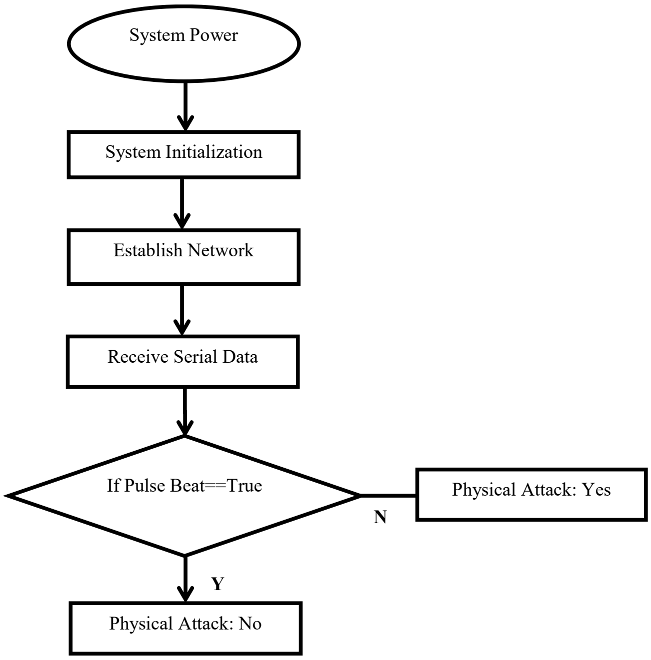


Figure 4. Flowchart to detect Physical attack in the proposed Security Improvement Framework (SIF).

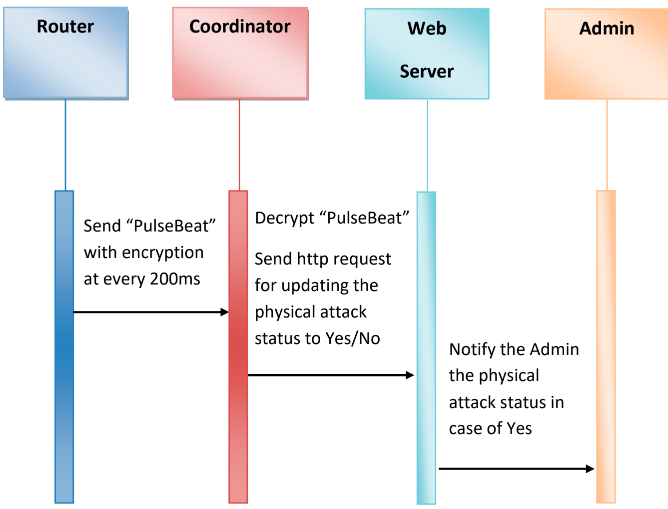


Figure 5. Data flow between Router, Coordinator, Webserver and Admin to detect physical attack in the proposed Security Improvement Framework (SIF).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 July 2018 doi:10.20944/preprints201807.0227.v1

3.2 Flooding Control Object

Insiders' attacks can happen at the Application Layer (APS) by flooding the network with messages. An attacker can send a bunch of messages without any delays which causes the whole network to freeze. To prevent flooding attack, the coordinator is used as trust center and linked key and network encryption key are configured. An algorithm is presented to prevent the flooding attack. Receiving data are counted simultaneously at a predefined delay of 200ms. If receiving data number exceeds the default value then flooding occurs and it discards the receiving data. Functional algorithm of this module is presented by flowchart in Figure 6. In case of detecting flooding effect, the status message is notified to Admin using web application. To detect and prevent the flooding attack the flooding control object considered the Data flow between Router, Coordinator, Webserver and Administrator as shown in Figure 7.

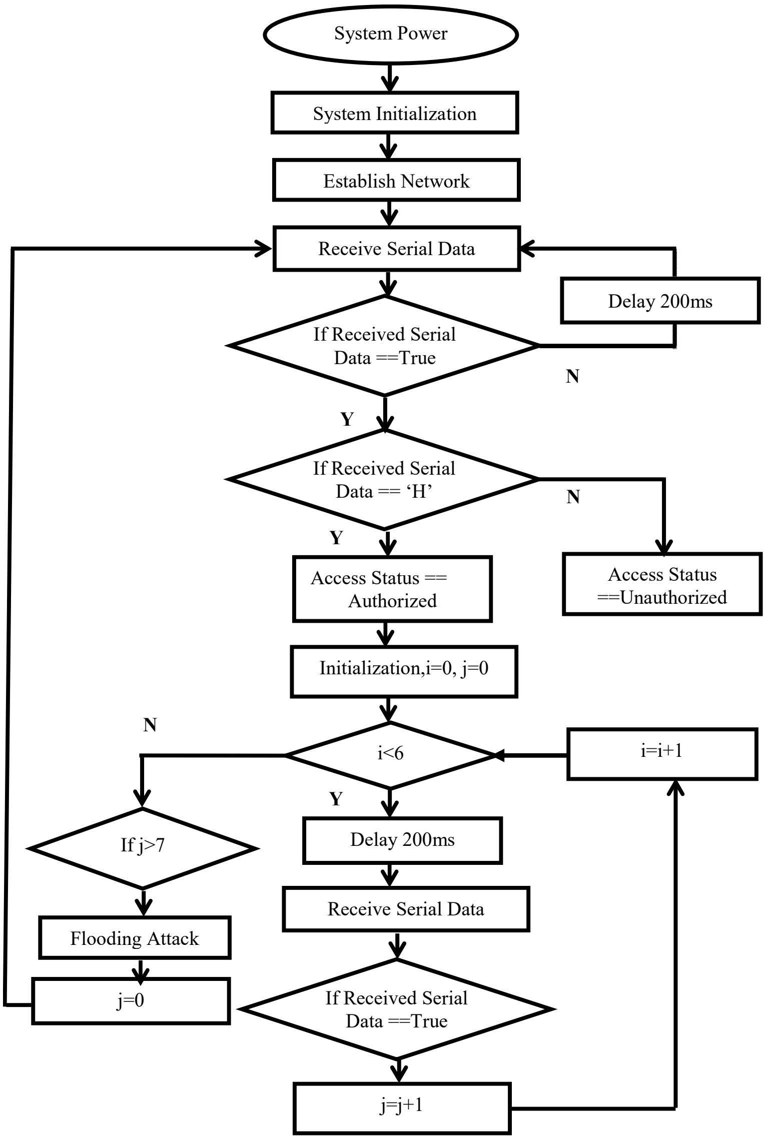


Figure 6. Flowchart to Prevent Flooding Attack in the proposed Security Improvement Framework (SIF).

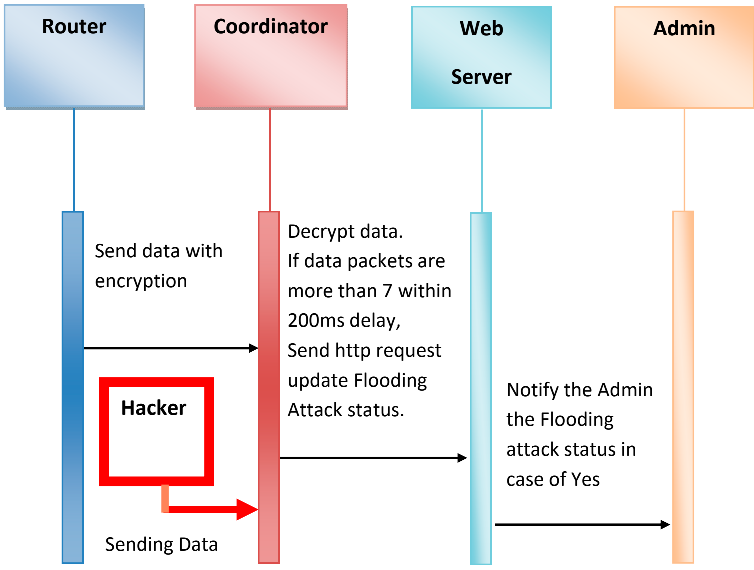
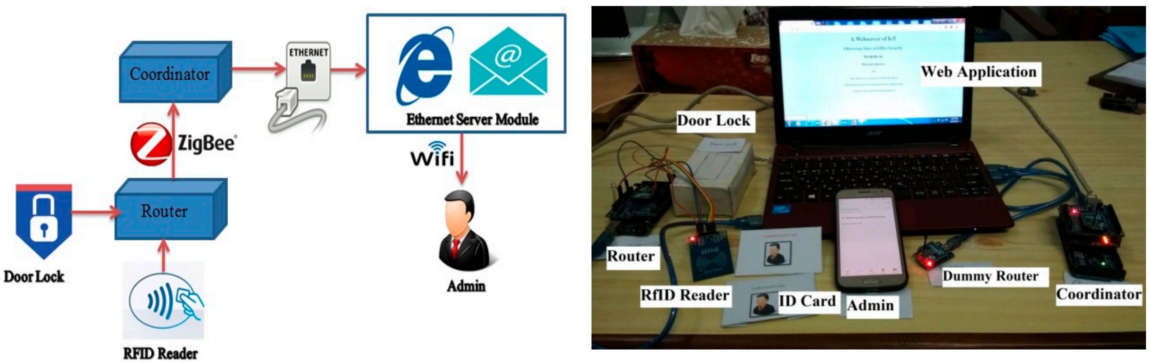


Figure 7. Data flow between Router, Coordinator, Webserver and Admin to detect Flooding attack in the proposed Security Improvement Framework (SIF).

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 as shown in Figure 8. Office area is separated into different location and employees have restriction to enter specific area. All employees must use their RF Identity card to enter any office area. When any employee wants to enter any office area she/he will touch his card on the RF card reader. Readers include Zigbee communication module which is called router for our research. Router send reading information to central controller which is called as Coordinator. If any employee wanted to enter his/her permitted office area, then the coordinator sends permission to unlock the door. On the other hand if any employee wanted to enter his/her prohibited office area, then the coordinator sends deny permission and notify the administrator through email. Moreover if any hacker tries to attack the system then the framework detects and protects such attempts effectively. The proposed algorithm of an office security system is also presented in Table 2.



(a) (b)

Figure 8. (a) Block diagram of the office security system using proposed Security Improvement Framework (SIF) using Zigbee protocol; (b) photograph of the testbed for implementing the proposed SIF.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 July 2018 doi:10.20944/preprints201807.0227.v1

Table 2. Algorithm used in the proposed Security Improvement Framework (SIF) using Zigbee protocol implemented in the 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)	For i=1 to 20 do	
(21)	Data=data+1;	
(22)	Delay ==200ms;	
(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 notifying Flooding attack */
(27)	End	
(28)	End	
(29)	End	
(30)	If R_data == 'H' then	
(31)	A_status==Authorized;	
(32)	D_state==Open;	
(33)	Update Web(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*/
(40)	Send Email(Admin);	/* Send email to Admin notifying unauthorized access */
(41)	End	
(42)	End	

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 July 2018 doi:10.20944/preprints201807.0227.v1

4.1 Evaluation of the proposed Security ImprovementFramework (SIF)

In this office security system, employs used their Identity card to enter the office premises and individual's room. Router which reads Identity card send the information to coordinator at 500ms delay. If any Hacker tries to do flooding attack then this system can detect the flooding attack and can protect it. To evaluate the flooding probability of the office security system we have send bunch of messages from router to coordinator. Coordinator reads the messages at 200ms delay and counts the messages which are coming simultaneously. We have plotted flooding probability curves for office security system with respect to the number of messages at constant message-receiving delays of 200ms as shown in Figure 9 (a). From this plot it is assumed that for number of messages greater than 7, Flooding probability is 1. If the Security Improvement Framework (SIM) gets more than 7 messages simultaneously at receiving delay of 200ms then it decided flooding occurs. Moreover another flooding probability curve also plotted with respect to message receiving delays at constant number of message received i.e., 7 as shown in Figure 9(b). This plot also shows that for 200ms delay at constant number of 7 messages, it detects the Flooding.

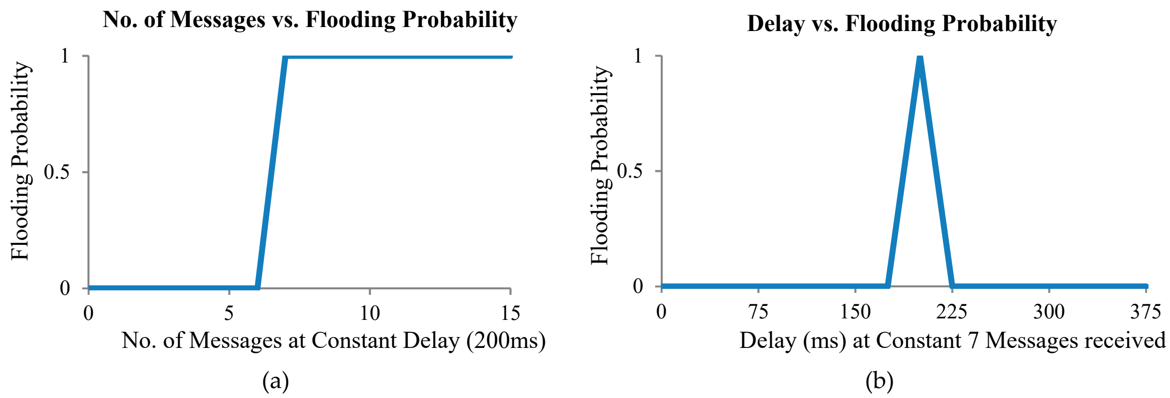


Figure 9. The Flooding Probability Curve with respect to (a) No. of Messages at Constant Delay and (b) Delay at Constant Messages.

To confirm the presence in the network, the router is sending an encrypted "Pulse Beat" signal to the receiver every 200ms. The coordinator in its turn decrypted the "Pulse Beat" message. When the router becomes hacked or coordinator does not receive any "Pulse Beat" signal from the router within 2 seconds the coordinator makes an "Http Request" to the web application that shows status (Physical attack Yes/No) to the admin. We have turned off router several times and checked the status signal. All the times the system can detect physical attack successfully.

5. Conclusion

The importance of security of Zigbee protocol in IoT is the main focus of this research. In this research, the security threats of Zigbee have reviewed based on some common IoT real world attacks such as message flooding, reply attack, etc. Experiments of those attacks have been performed to find out the 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 message is encrypted and decrypted with Advanced Encryption Standard (AES) 128-bit key. This framework is implemented in an office security system. If any employee wanted to enter his/her prohibited office area, then the coordinator sends deny permission and notify the administrator through email. Moreover if any hacker tries to attack the system then IoT framework detects and protects such attempts effectively negates the use of the manufacturers default configuration. In future, we will try to adopt system recovery in case of potential security attack.

Author Contributions: Conceptualization, M. Humayun Kabir; Funding acquisition, Miah Abdul Halim; Methodology, S M Sohel Rana; Software, M. Humayun Kabir; Supervision, M. Humayun Kabir; Validation, S M Sohel Rana; Writing – original draft, S M Sohel Rana; Writing – review & editing, Miah Abdul Halim and M. Humayun Kabir.

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

References

1. J. Gubby; R. Buyya; S. Marusic; M. Palaniswami, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. In Technical Report CLOUDS-TR-2012-2, *Cloud Computing and Distributed Systems Laboratory*, The University of Melbourne, 29 June, 2012.
2. R. Milman, 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.
4. R. Khan;S. U. Khan; R. Zaheer; S. Khan, 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. A. Al-Fuqaha; M. Guizani; M. Aledhari; M. Ayyash, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. Vol.17, pp. 2347–2376, 2015.
6. B. Ali; A. I. Awad, Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes, Sensors, Vol.18, 2018.
7. A. Betzler; C. Gomez; I. Demirkol; J. Paradells, A Holistic Approach to ZigBee Performance Enhancement for Home Automation Networks, Sensors, Vol. 14, 2014.
8. P. Radmand; M. Domingo; J. Singh; J. Arnedo; A. Talevski; S. Petersen; S. Carlsen, Zigbee/Zigbee PRO security assessment based on compromised cryptographic keys. International Conference on P2P, Parallel, Grid, Cloud and Internet Computing 2010, Available online:https://espace.curtin.edu.au/bitstream/handle/20.500.11937/11224/154187_154187.pdf?sequence=2 (accesses on 20 May 2018)
9. O. Olawumi; K. Haataja; M. Asikainen; N. Vidgren; P. Toivanen, Three Practical Attacks AgainstZigbee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned, in IEEE 14th International Conference on Hybrid Intelligent Systems (HIS2014), At Kuwai. DOI: 10.1109/HIS.2014.7086198
10. I. S. Kocher; C.-O. Chow; H. Ishii; T. A. Zia, Threat Models and Security Issues in Wireless Sensor Networks, International Journal of Computer Theory and Engineering, Vol. 5, No. 5, October 2013.
11. J. Brodsy; Anthony McConnell, Jamming and Interference Induced Denial-of-Service Attacks on IEEE 802.15.4-based Wireless Networks, Tech. Rep., Digital Bond's SCADA Security Scientific Symposium, 2009
12. Securing the Internet of Things: A Proposed Framework, In CISCO, Available online: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html (accesses on 20 May 2018)
13. I. B. Pasquier; A. A. El Kalam1; A. A. Ouahman; M. De Montfort, A Security Framework for Internet of Things. Springer International Publishing, 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/ (accesses on 20 May 2018).
16. J. Durech; M. Franekova, Security attacks to Zigbee technology and their practical realization. In IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI 2014).
17. N. Vidgren; K. Haataja1; J. L. Patino-Andres; J. J. Ramırez-Sanchis; P. Toivanen, Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned, 46th Hawaii International Conference on System Sciences, 2013.
18. O. Olawumi; K. Haataja; M. Asikainen; N. Vidgren; P. Toivanen, Three Practical Attacks AgainstZigbee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned. In

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 July 2018 doi:10.20944/preprints201807.0227.v1

IEEE 14th International Conference on Hybrid Intelligent Systems (HIS2014), At Kuwait. DOI: 10.1109/HIS.2014.7086198

19. N. Vidgren; K. Haataja; J. L. Patino-Andres; J. J. Ramirez-Sanchis; P. Toivanen,Security threats in Zigbee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned. In System Sciences (HICSS),46th Hawaii International Conference on, 2013, pp. 5132-5138.
20. I. B.Pasquier; A. A. El Kalam1; A. A. Ouahman; M. De Montfort, A Security Framework for Internet of Things.Springer International Publishing , Switzerland, 2015.
21. J. Cache; J. Wright; V. Liu, Hacking Exposed Wireless: Wireless Security Secrets and Solutions. McGraw-Hill, Second Edition, Jul. 2010.
22. Kyunghwa Lee;Joohyun Lee;Bongduk Zhang; Jaeho Kim;Yongtae Shin, An enhanced Trust Center based authentication in Zigbee networks, *Advances in Information Security and Assurance*,SpringerLink, pp. 471–484, 2009.
23. G. Dini; M. Tiloca, Considerations on Security in Zigbee Networks.In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2010, pp. 58–65.