A Survey on Key Management of ZigBee Network

Zavosh Abdollahzadeh Davani
Advance Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
adzavosh2@live.utm.my

Azizah Abdul Manaf
Advance Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
azizah07@ic.utm.my

Abstract— **ZigBee is short distance, low complexity, and low power consumption wireless personal area network. As ZigBee has several applications in industry and healthcare, its security in the recent years has been attracting a lot of attention. This paper is a survey on key management of ZigBee network and model that proposed for enhancing key management of it. And also at the end, it suggests another way to enhancing the security of ZigBee network.**

Keywords—ZigBee Network ; Security; Key Management; Steganography

I. INTRODUCTION

ZigBee is a wireless personal area network, which is based on IEEE 802.15.4 wireless protocol [1]. First time in 2004 Alliance defined the ZigBee network and in 2006 it released the second stack of the ZigBee network, which was defined as ZigBee 2006. In 2007 it improved ZigBee 2006 and introduced it as ZigBee Pro. ZigBee is a short distance, low complexity, low data rate, and two way technology which has been developed recently and oriented to Wireless Sensor Network (WSN) [2]. Furthermore, it has several advantages such as self organization, lower power consumption, low cost, smaller size of protocol stacks, and larger addressing space [1].

ZigBee consist of two types hardware device such as full function device (FFD) and reduced function device (RFD). FFD devices are able to communicate with both FFD and RFD devices. In other hand, RFD devices are able to communicate just with FFD devices. ZigBee network devices include PAN Coordinator, Router as FFD devices and End devices as RFD devices [3]. ZigBee network protocol stack is based on Open System Interconnection (OSI). ZigBee network protocol is built on IEEE 802.15.4 standard, which consist Physical (PHY), and Media Access Control (MAC) layers. ZigBee network defines the Network (NW) layer and Application layer (APL) [4]. And it also has several applications in military, industry, smart grid, health care, and home automation for monitoring, controlling information, and transmits it in a safe and secure way [5]. Therefore, security issues in ZigBee have attracted a lot of attention and in the recent years there are several key management models have been proposed for enhancing security of it.

This paper is a survey on key management of ZigBee network and models that proposed for enhancing security of it. The remainder of this paper is organized as follows: section II is summary of ZigBee network security, section III is security vulnerabilities of ZigBee network, section IV is related work, section V is comparison of proposed model, section VI is suggestion and future work, and section VII is concluded.

II. SECURITY OF ZIGBEE NETWORK

ZigBee security mechanism applies some features such as Data Encryption, Sequential Freshness, Frame Integrity Checking Function, and Entity Authentication Service [6].

Data Encryption in ZigBee applies a symmetric cipher to protect data from being read by the parties without cryptographic key. ZigBee adopts AES-128 CCM* encryption algorithm, CCM* is a modification of CCM and it includes all of the features of CCM. It offers encryption only and integrity only capabilities. These extra capabilities simplify security by eliminating the need for CTR and CBC-MAC modes. ZigBee security unlike other MAC layer security modes that require a different key for every security level, by using CCM* enables the security mechanism to use a single key for all CCM* security levels. With the use of CCM* throughout the ZigBee stack, the MAC, Network, and Application layers can reuse the same key [7]. Sequential Freshness applies an ordered sequence number for each packet and rejects each frame that has been replayed. The Frame Integrity Checking function use Message Integrity Code (MIC) in the each data frame to protect data from modifying by those parties, which do not have cryptography key. And Entity Authentication Service provides a secure means for a device to synchronize information with another device while simultaneously providing authentically based on a shared key [6].

ZigBee Pro, which specified as ZigBee-2007 has two security modes such as Standard Security mode, which is compatible with the residential security of ZigBee-2006, and High Security mode, which is compatible with the commercial security of ZigBee-2006. The High Security mode includes three keys, which are Master Key (MK), Link Key (LK), and Network Key (NK). In other hand, Standard Security mode has two keys, which are Link Key (LK) and Network Key (NK) [8].

MK is pre produce or transmitted in each node and it is used to generate the LK and shared between network nodes. The LK is a unique and optional key that shared between ZigBee devices and it is used to secure unicast communication between the Application layers of devices. In addition, the NK

provided by the Coordinator and shared between all ZigBee devices to encrypt the communication at network level and used to secure initialization and distribution of Frame Counters between network devices [7].

ZigBee defines Trust Center (TC) in the network, which is not a device but it is a security application that responsible for authenticate devices which request to join in the network, maintain and distribute encryption keys, and enable end-to-end security between devices [9].

III. SECURITY VULNERABILITIES OF ZIGBEE NETWORK

As the ZigBee network is the new technology in WSN, still it has some vulnerability in key management and information transmission. Some of the vulnerabilities of ZigBee network are mentioned as below:

First vulnerability of ZigBee network is key distribution. Key distribution of ZigBee network is a challenging issue since it is vulnerable in transferring MK, LK, and NK. In ZigBee network MK is preinstalled in each node or transferring to each node in the unsecure way. [10].

The second vulnerability of ZigBee network is number of cryptography keys in large-scale network. ZigBee in network with n nodes using the symmetric key cryptosystem and it must generate and store n keys for distributing in the large-scale network. The problem is managing and maintaining the large number of symmetric keys by ZigBee network in large-scale network.

The third vulnerability of ZigBee network is its peer-to-peer communication. Current ZigBee key management use LK based on Application Layer for peer-to-peer communication. The vulnerability of this communication is poor key authentication and integrity of information [5].

The fourth vulnerability of ZigBee network is a node that leaves the network. When any node leaves the network, MK and LK are stored in it and the ZigBee network does not have any mechanism for destroying these keys in disjoined node. Therefore, an attacker is able to use these keys to put the ZigBee network at the risk.

The fifth vulnerability of ZigBee network is cryptography nonce. The important part of the nonce (n) is 32 bits frame counter that has an important role in the ZigBee network since it applies in the ZigBee network to protecting ZigBee against replay attack. In the ZigBee network, devices such as Sensors, Power Strip, and the Controller should save the nonce in their memory since they are restarting and going to sleep for saving the energy and they need to save the nonce for further transmission. When the Power Strip loses the association to the Coordinator for a certain amount of time such as four minutes, it resets its frame counter to zero and starts a new association [11]. This power cycle cusses the devices to reproduce the same cipher texts (CT) such as:

$$(I)\ CT_1 = [PT_1 \text{ XOR } E_{key}(n)]$$
$$(II)\ CT_2 = [PT_2 \text{ XOR } E_{key}(n)]$$

In the ZigBee these cipher texts are network packets and they are equal in keys and nonce. According to [12] in XOR Reinvented key attack when two CT_1 and CT_2 produced with the different plain texts (PT) and same Encryption Key (E_{Key}) and same nonce, an attacker is able to use bypass the key problem to obtain the [PT_1 XOR PT_2] through computing [CT_1 XOR CT_2]. The Mathematical proof of this problem is shown as a below:

$$(III)\ \text{Assumption: } CT1 \text{ XOR } CT2 = PT1 \text{ XOR } PT2$$
$$(IV) = (PT1 \text{ XOR } E_{key}(n)) \text{ XOR } (PT2 \text{ XOR } E_{key}(n))$$
$$(V) = PT1 \text{ XOR } PT2 \text{ XOR } (E_{key}(n) \text{ XOR } E_{key}(n))$$
$$(VI) = PT1 \text{ XOR } PT2 \text{ XOR } (0 \text{ XOR } 0)$$
$$(VII) = PT1 \text{ XOR } PT2$$

In this level adversary is able to use frequency analysis to obtain one of the plain text and after that he or she is able to produce the key according to the following method:

$$(VIII)\ E_{key} = CT \text{ XOR } PT = (PT \text{ XOR } E_{key}) \text{ XOR } PT = E_{key}$$

Therefore, the adversary by comparison of several cipher texts could be found which bytes in the clear text have changed and able to guess about the plain text. Since the plain text is different in the cipher text and after that they are able to generate the key.

IV. RELATED WORK

Since the security of ZigBee network is critical issue and has several vulnerabilities that described in last section, in recent years there are several models are proposed for enhancing it and make it more secure and reliable. These models are as follows:

Zhang and Chen [13] have been proposed the improvement key management mechanism for enhancing security feature of the ZigBee network such as confidentiality in the large-scale node. Zhang's model is based on LEAP algorithms that is energy efficient and ensures that messages transferred are not fragmented, which would increase packet losses in transmission. Rossi, Omana, Giaffreda, and Metra [14] have been proposed the new protocol for Wireless Sensor Network (WSN) that solve the security vulnerability of the ZigBee network in peer to peer communication. Their model guarantees the authentication and integrity of massage and Acknowledgment (ACK) by means of a Message Authentication Code (MAC) and encrypted the ACK by AES in the communication. Its stack consist of Tx-ID and Rx-ID, Payload, Message type (Msg- type), #seq, MAC of the MSG or ACK. In their model, MAC of the MSG or ACK has been generated by encrypting the first part of the message using AES algorithm (Tx_ID, Rx_ID, Msg-type, #seq and Payload). Li, Jia, and Xue [6] proposed a security mechanism in Application Layer of ZigBee network that use a simple way to encrypt and integrity checking the data packet of MSG type. In this model it uses the Application framework (AF) frame format with MSG frame type. Chen, Zhang, Tian, and Fu [15] have been proposed identity based authentication key management for enhancing the integrity and confidentiality of

the ZigBee network in large scale. Their model uses both identity based authentication method and certificate based authentication method to realize secure, fast, low cost and scalable authentication between nodes that belong to the same cluster and different clusters. Dini and Tiloca [16] have been proposed Home Certification Authority (HCA) for vulnerability of the ZigBee network in devices that leaving the network and has yet stored NK and LK in the their memory. HCA used to identify each device that joins to the network since the adversary is not able to use the old LK and NK for communicate to other devices. Al-alak, Ahmed, Abdullah, and Subramiam [17] have been proposed Multiple Key Protocol (MKP) for ZigBee that is based on AES-128 CCM* and ECC cryptography algorithm. Since the AES-128 CCM* in ZigBee network has a vulnerability into the key distribution, therefore this model used AES-128 CCM* and ECC for enhancing the security system of ZigBee WSN in term of confidentiality and integrity as well as defense against replay attack. Since of vulnerability of ZigBee network in terms of the number of keys for sharing key between full mesh network and limited services for home automation, Seo and Kim [18] have been proposed key management mechanism for ZigBee network. This model is applied in the home automation, which allows users to design home network and control home appliances depending on their use. Seo's model is applied Attribute Based Proxy Re-encryption (ABPRE) for security of ZigBee network and provides services to authorize user such as visitors. Seo, Kim, and H. Kim [19] have been proposed another model that is an application of attributes-based cryptography mechanism for ZigBee network. Seo's model using attributes and offers various services, reduces the number of key, reduces the key space, increasing security and reduces the waste of power consumption of ZigBee network. Sun and Qian [5] have been introduced the security model based on Advanced Encryption Standard (AES) algorithm for security application of ZigBee that support Application Sub Layer (APS). This model introduced a MSG frame on the APS that includes transmission sequence (8 bits), length (8 bits), and data. The symmetric encryption algorithm use AEC CBC for XOR between initialized vector and plain text. Seshabhattar, Yenigalla, Krier, and Engels [20] have been proposed the authentication key establishment based on Hummingbird (HB) key establishment on the ZigBee network for secure key agreement between an initiator and a responder device in ZigBee network that called Hummingbird Key Establishment (HBKE). Kim, H. Kim, and Chung [9] have been proposed the novel security mechanism based on Elliptical Curve Identity Cryptography (ECIC) for ZigBee network. In this model the traffic concentrated on the trust center is diminished, and the key establishment time is reduced, therefore it cussed reducing the overall energy consumption of the sensor network and improve the network efficiency. Kwon and Kim [21] have been proposed the Efficient Group Key Management for ZigBee network for enhancing the key storage and key distribution of ZigBee network. Choi, Yun, Chae, and Kim [10] proposed a Key Management mechanism to enhancing vulnerability of ZigBee key management in network key distribution. The proposed model is based on Elliptic Curve Diffie- Hellman (ECDH) and SubMAC for Wireless Sensor and ZigBee Network.

V. COMPARISON OF MODELS

As this paper mentioned security of ZigBee network has several vulnerabilities in key management and key distribution and in effort to enhance these vulnerabilities some models have been proposed in the recent years. Table I show the result of analysis these models and it classified proposed models by scope that they are trying to enhance it.

TABLE I. Comparison of Proposed Model

No	Article	Problem	Solution	Enhanced Scope
1	An Improved Key Management of ZigBee Protocol [13]	Vulnerability in Large Sensor Network	Proposed Key Management mechanism based on LEAP	Master Key, Link Key, and Network Key
2	Secure communication protocol for wireless sensor networks [14]	Vulnerability of ACK Authenticity And Data Authentication	Proposed protocol based on Message Authentication Code (MAC) and encryption ACK of packet by AES	Link Key
3	Application and analysis of zigBee security services specification [6]	Complexity and high power mechanism	Propose application Frame work base on data integrity	Link Key
4	An identity-based authentication protocol for clustered ZigBee network [15]	Integrity and Confidentiality of ZigBee network in large scale	Propose Identity based Authentication method and Certificate based Authentication method	Link Key, and Network Key
5	Considerations on security in ZigBee networks [16]	Vulnerability in devices that leaving the network	Proposed Home Certification Authority (HCA).	Link Key
6	AES and ECC Mixed for ZigBee Wireless Sensor Security [17]	Vulnerability in key distribution	Proposed Multiple Key Protocol based on AES-128 CCM* and ECC	Master Key, Link Key, and Network Key
7	Zigbee security for visitors in home automation using attribute based proxy re-encryption [18]	Confidentiality data in home automation, Authentication home user	Proposed Attribute Based Proxy Re-encryption (ABPRE) model	Master Key, Link Key, and Network Key
8	ZigBee security for Home automation using attribute-based cryptography [19]	Vulnerability in key distribution	Proposed an application of attributed-based cryptography mechanism	Master Key, Link Key, and Network Key

No	Article	Problem	Solution	Enhanced Scope
9	Study and Application of Security Based on ZigBee Standard [5]	Vulnerability of ZigBee security in application layer	Proposed model that introduced a MSG frame on the APS	Link Key
10	Hummingbird key establishment protocol for low-power ZigBee [20]	Vulnerability in Authentication	Proposed the key management based on Hummingbird	Master Key, Link Key, and Network Key
11	A novel elliptical curve ID cryptography protocol for multi˜ hop ZigBee sensor networks [9]	Vulnerability in Key distribution of new joining node	Proposed the novel security mechanism based on Elliptical Curve Identity Cryptography	Link Key, and Network Key
12	Efficient group key management of ZigBee network for home automation [21]	Vulnerability in key storage and key distribution	Proposed the Efficient Group Key Management	Master Key, Link Key, and Network Key
13	An enhanced key management using ZigBee Pro for wireless sensor networks [10]	Vulnerability in key distribution	Proposed a Key Management based on Elliptic Curve Diffie Hellman and SubMAC	Network Key

As you can see in table I there are several models have been proposed for enhancing vulnerabilities that described in security vulnerabilities of ZigBee network section except vulnerability of nonce that cause to occur XOR Reinvented Key attack. Since XOR Reinvented Key attack just occurs in real world application of ZigBee network not simulation of this network, it still exist and able to put security of ZigBee network at risk.

VI. SUGGESTION AND FUTURE WORK

As mentioned security of ZigBee network is a critical issue and it needs to transfer information in a secure way. Thus, to achieve this goal there are several cryptography models have been proposed for enhancing security of ZigBee network.

Another way to transferring information in a secure way is stenography. Steganography unlike cryptography hide information in a way that no one is able to predict there is any hidden information behind the data. On the other hand, cryptography focus on encrypting contains of message in a way which attract the attention of someone that there is secret information is encrypted and attempt to decrypt information [22].

Furthermore, encryption algorithm consumes some resources such as memory, power and CPU process for encryption and decryption algorithms in WSN. To avoid this situation, Martins and Guyennet [23] proposed another way by using steganography for secure transmission data in WSN. This model uses steganography algorithm to hide data in MAC layer of IEEE 802.15.4 protocol. In the MAC layer of IEEE 802.15.4 packet frame has different type based on the kind of packet that has been sent, and it has been classified in four types such as Data frame, Beacon frame, Acknowledgment frame and MAC command frame. This model is costs less energy for transferring messages in a secure way than the cryptography use AES-128 for encrypting information.

VII. CONCLUSION

This paper first introduced the ZigBee network and security mechanism that is applied to the ZigBee network. After that summarized ZigBee security vulnerabilities and models that proposed for enhancing these vulnerabilities and then comparing these models with each other. In the final it suggests another way for the security of ZigBee network, which is able to transferring information in the most secure way through the network. And also, it can be applied as future work for enhancing security of ZigBee network.

REFERENCES

[1] Z. Yan and Z. Jiaxing, "Design and implementation of Zigbee based wireless sensor network for remote SpO2 monitor," 2010, pp. V2-278-V2-281.

[2] G. Wang, J. Zhang, W. Li, D. Cui, and Y. Jing, "A forest fire monitoring system based on GPRS and ZigBee wireless sensor network," 2010, pp. 1859-1862.

[3] H. Guozhen, "Key technologies analysis of ZigBee network layer," 2010, pp. V7-560-V7-563.

[4] C. Ramya, M. Shanmugaraj, and R. Prabakaran, "Study on ZigBee technology," in *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, 2011, pp. 297-301.

[5] M. Sun and Y. Qian, "Study and Application of Security Based on ZigBee Standard," in *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on*, 2011, pp. 508-511.

[6] H. Li, Z. Jia, and X. Xue, "Application and analysis of zigbee security services specification," in *Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on*, 2010, pp. 494-497.

[7] E. Yüksel, H. R. Nielson, and F. Nielson, "Zigbee-2007 security essentials," in *Proc. 13th Nordic Workshop on Secure IT-systems*, 2008, pp. 65-82.

[8] C. Alcaraz and J. Lopez, "A security analysis for wireless sensor mesh networks in highly critical systems," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on,* vol. 40, pp. 419-428, 2010.

[9] H. Kim, C. H. Kim, and J. M. Chung, "A novel elliptical curve ID cryptography protocol for multi□hop ZigBee sensor networks," *Wireless Communications and Mobile Computing,* vol. 12, pp. 145-157, 2012.

[10] K. Choi, M. Yun, K. Chae, and M. Kim, "An enhanced key management using ZigBee Pro for wireless sensor networks," 2012, pp. 399-403.

[11] R. Meyer, "Security issues and vulnerability assessment of Zigbee enabled home area network implementations," California State University, 2012.

[12] C. Forler, S. Lucks, and J. Wenzel, "Designing the API for a Cryptographic Library," *Reliable Software Technologies–Ada-Europe 2012,* pp. 75-88, 2012.

[13] B. Zhang and L. Chen, "An Improved Key Management of ZigBee Protocol," 2010, pp. 416-418.

[14] D. Rossi, M. Omana, D. Giaffreda, and C. Metra, "Secure communication protocol for wireless sensor networks," 2010, pp. 17-20.

[15] W. Chen, X. Zhang, D. Tian, and Z. Fu, "An identity-based authentication protocol for clustered ZigBee network," *Advanced Intelligent Computing Theories and Applications. With Aspects of Artificial Intelligence,* pp. 503-510, 2010.

[16] G. Dini and M. Tiloca, "Considerations on security in ZigBee networks," 2010, pp. 58-65

[17] S. Al-alak, Z. Ahmed, A. Abdullah, and S. Subramiam, "AES and ECC Mixed for ZigBee Wireless Sensor Security," *computing,* vol. 1, p. 5, 2011.

[18] H. Seo and H. Kim, "Zigbee security for visitors in home automation using attribute based proxy re-encryption," 2011, pp. 304-307.

[19] H. Seo, C. S. Kim, and H. Kim, "ZigBee security for Home automation using attribute-based cryptography," in *Consumer Electronics (ICCE), 2011 IEEE International Conference on*, 2011, pp. 367-368.

[20] S. Seshabhattar, P. Yenigalla, P. Krier, and D. Engels, "Hummingbird key establishment protocol for low-power ZigBee," in *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, 2011, pp. 447-451.

[21] Y. Kwon and H. Kim, "Efficient group key management of ZigBeenetwork for home automation," in *Consumer Electronics (ICCE), 2012 IEEE International Conference on*, 2012, pp. 378-379.

[22] A. H. Lashkari, A. A. Manaf, M. Masrom, and S. M. Daud, "A Survey on Image Steganography Algorithms and Evaluation," in *Digital Information Processing and Communications*, ed: Springer, 2011, pp. 406-418.

[23] D. Martins and H. Guyennet, "Steganography in {MAC} Layers of 802.15. 4 Protocol for securing Wireless Sensor Networks," in *IWNS 2010, 2nd IEEE Int. Workshop on Network Steganography*, 2010.