International Journal of Computer Networks and Communications Security

VOL. 4, NO. 12, DECEMBER 2016, 330–335
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

ZigBee Security Using Public Key Steganography

Iqra Hussain[1], Dr. Nitin Pandey[2] and Dr. Mukesh Chandra Negi[3]

[1, 2] Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida

[3] Delivery Manager, TechMahindra Ltd, A7, Sector 64, Noida

[1]iqrahussain4@gmail.com, [2]npandeyg@gmail.com, [3]mn00330419@techmahindra.com

ABSTRACT

ZigBee an IEEE 802.15.4 based specification is a low cost, low complexity and low power consumption wireless personal area network (WPAN) standard targeted at the wide development of long battery life devices in wireless control and monitoring applications. It finds a wide use in the industrial and physical operation and so it is majorly associated with M2M and IoT. The security on such WPAN's is a concern and has been gaining a lot of attention in recent years. The security techniques in use for such kind of networks over past years are cryptographic techniques. However, the techniques proposed so far have the major scope of improvement to come up with more secure data transfer. As in cryptography encrypted messages no matter how unbreakable, will arouse suspicion and can be sufficient for an attacker, who eavesdrops the network that something important has been detected. Therefore to preserve security in such networks we propose another way to secure data by using Public key Steganography, which is a technique that allows two parties to send hidden messages over a public channel in a way that an adversary cannot even detect that the hidden messages are being sent. So as cryptography protects the contents of a message alone, Steganography can be said to protect both, contents of the message and even hiding the fact that a secret message is being sent. Our sole aim is to propose a Public key Steganographic method that resists to steganalysis and hence we show that this solution can be an energy-efficient solution with a low latency to secure data transfer in wireless personal area networks.

Keywords: *ZigBee, IEEE 802.15.4, Public Key Steganography, Reserved Bits, Stego Object*.

1 INTRODUCTION

1.1 ZigBee

ZigBee is a wireless sensor and control network specification based on IEEE 802.14.5 wireless protocol and developed by the ZigBee Alliance. ZigBee was conceived in the year 1998, standardized in 2003 and later revised in 2006. ZigBee is a low cost, low complexity and low power consumption wireless personal area network (WPAN) standard which targets at the wide development of long battery life devices. ZigBee applications are used in home automation, industrial automation, health/medical care, smart grids etc. We can say that ZigBee finds an extensive use in the world of Internet of Things and M2M. In advance, ZigBee has more than a few benefits for instance self organizing, lower power consumption, depleted cost, smaller size of protocol stacks and larger addressing modes. ZigBee is the lone universal; standards-based wireless explanation that is capable of appropriately and reasonably be In charge of the extensive variety of devices to enhance contentment, security and convenience for clients. It is actually the technology of choice for world-leading service providers, installers and retailers who fetch the gains of the Internet of things into the Smart Home [4].

ZigBee consists of two categories of hardware devices such as the full functional device (FFD) and reduced function devices (RFD). FFD devices are competent to correspond with both FFD and RFD devices. Alternatively, RFD devices are capable to correspond merely with the FFD devices. Further the ZigBee network devices consist of three classes of devices, the coordinator, the router and the end devices. The ZigBee network protocol stack is based on Open System Interconnection (OSI). [4]

1.2 ZigBee Architecture

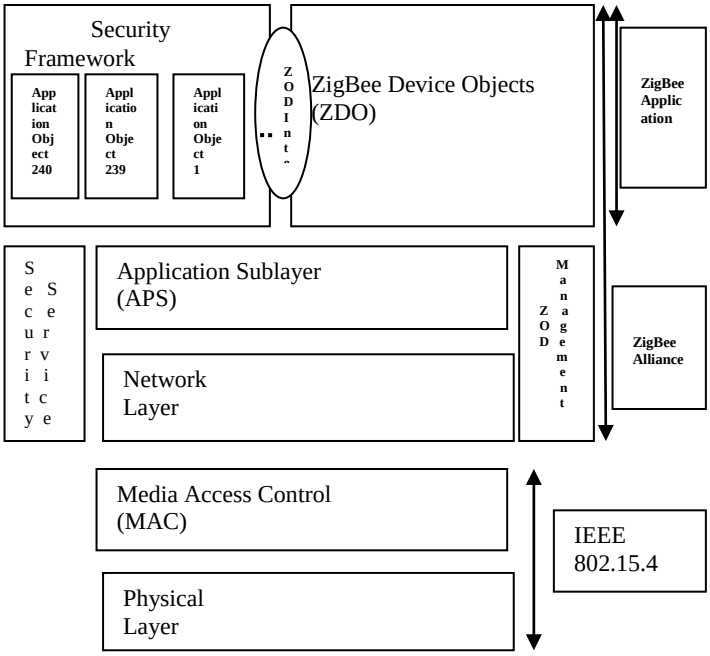

Fig. 1. the ZigBee Architectur

As shown in the Figure 1, the ZigBee Architecture is alienated into two major divisions, the IEEE 802.15.4 which incorporates the MAC layer and the physical layer. The further division is the ZigBee layers, which incorporate the network layer, the ZigBee Device Objects (ZDO), the Application Support Sublayer (APS) and the Security management. Every layer executes seperate operations. The Physical layer performs modulation and demodulation on outgoing and incoming signals correspondingly. It broadcasts and collects information from a source. The MAC layer accesses the network using carrier-sense multiple access, with collision avoidance (CSMA/CA), to transmit frames for synchronization and impart a reliable transmission. The network layer positioned between the MAC layer and the APS offers tasks such as starting a network, organization of end devices, joining or leaving a network, route detection, neighbor detection etc. The Application Support Sublayer (APS) offers services required for Application Objects (end points) and the ZDO to interface with the network layer for data and management services. The Application Objects\End Points describe input and output to the Application Support Sublayer. The ZigBee Device Objects carry out monitoring and management of Application Objects and execute by and large the device management jobs i.e. identify the class of devices in a network, whether it's a coordinator, a router or an end device.

1.3 Public Key Steganography

Steganography refers to the practice of transferring messages concealed in irreproachable appearing communications on top of a public channel so that an adversary eavesdropping on the channel cannot even detect the existence of the concealed messages [9].

The intend of steganography consists of embedding data such as text, movie, picture, etc described as the secret message, in
an alternative media or support [3]. The alternative media or support which incorporates the hidden data is specified as the cover object. And once the secret message is embedded in the cover message, the end result is called as the stego object. For example, we can hide a picture in an additional picture, and in this second picture, we cannot notice that the first picture is hidden within the first picture. When we talk about steganography, we pass on to the analogy of Alice and Bob [3]. Alice and Bob are in jail and are watched over by a warden, Wendy. If Alice desires to convey a message to Bob, this message ought to go through Wendy. If Wendy spots the message which includes the important information, for instance the hour of the escape. Wendy will by no means give that message to Bob. For that reason, Alice is supposed to discover a way out to hide information in the message devoid of Wendy noticing it. For instance, Alice will hide a message in an alternate message and if every other letter is read, the hidden message can be read; and if somehow Wendy reads this message, she will not be able to notice the hidden message. So in steganography, the above example states that the Steganographic technique should be kept secret and if Wendy understands the Steganographic method, she will know how to interpret the message and all the participants who are involved in the communication should be able to understand this technique to hide the data and as well as later read the data [3].

On the further part, public-key steganography permits participants to communicate steganographically with no prior swap of secrets. Like by means of public-key encryption, the correspondent of a message even requires to be familiar with the recipient's public key or else take part in a key exchange protocol. At the same time as it is true that if there is no global PKI, the use of public keys may provoke doubt, as seen in several circumstances it is the dispatcher of a message who is concerned in covering up his/her communication and there is no requirement for him/her to broadcast

any keys. A number of Steganographic methods set sights on to make use of specificities of communication protocols to conceal data or information and employ the communication layer fields as the cover objects. Making use of the Steganographic data in communication layer fields offers the conception of a hidden channel in the network. And merely the devices that are aware of in which fields the data or information is hidden can read or write data. It can even be possible to invisibly exchange data or information in the network if the network does is not aware about the Steganographic technique used.[11], [17] and [18] show various possibilities for hiding the data or information, using specificities of the protocols to generate hidden channels or the Steganographic channels. The mainly employed techniques constitute of using the reserved field bits of the protocols.

The paper proposes implementing the Public Key Steganography technique on the reserved field bits used to hide secret messages, in the layers of IEEE 802.14.5 to boost the overall ZigBee protocol security that is based on the similar IEEE 802.14.5 specification. The remainder of the paper is organized as follows: Section II will present the related work in regard of the proposition to hide information in the MAC layers of 802.15.4 [1], Section III will present the block diagram proposition of associating a Public Key with steganography to enforce security, Section IV will present the advantage of using this technique, Section V will present the implementation and section VI will present the conclusion of the paper.

2 RELATED WORK

This section illustrates the proposition of hiding information in the MAC layers of IEEE 802.14.5 protocol. This technique constitutes using the reserved field bits to hide data or information in them. IEEE 802.15.4 uses different forms of frames, depending on the type of data packet sent. The MAC layer of 802.14.5 uses 4 different types of data frames [3]:

1. *Data Frame*
2. *Beacon Frame*
3. *Acknowledgement Frame*
4. *MAC command Frame*

A. Data Frame

The structure of a MAC data frame is given in the Figure 2.

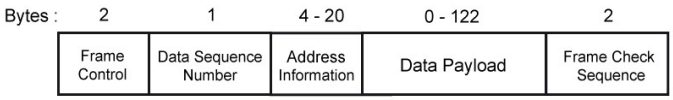

Fig. 2. MAC Data Frame Structure

In this field the Frame Control field and the Address Information field provide potential to hide data or information.

1) Frame Control Field

The structure of the Frame Control Field is given in Figure 3.

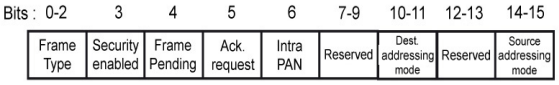

Fig. 3. Frame Control Field Structure

In the above given structure in Figure 3, we see that the 7-9 bits and 12-13 bits are reserved and can be used to encode a 3 bit and a 2 bit stego object respectively.

2) Address Information Field

The structure of the Address information Filed is given in the Figure 4.

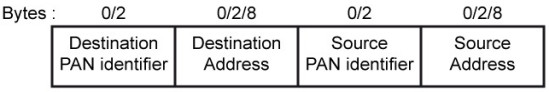

Fig. 4. Address Information Field Structure

The Source Address can be used to have a short 16 bits or an extended of 64 bits source address. This field can be used to hide data in a way, like if we specify a nonexistent source address and with this nonexistent source address, a stego object of size up to 64 bits can be hidden in it.

B. Beacon Frame

The structure of MAC beacon frame is given in the Figure 5.

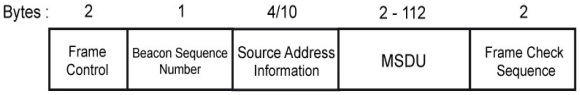

Fig. 5. MAC Beacon Frame Structure

The possibility for hiding information is similar here as in the Data Frame i.e. the frame control field and the source address information field can be employed to hide the stego object. The only distinction is that the source address information field here is limited to 10 bytes only.

C. Acknowledgement Frame

The structure of the Acknowledgement frame is given in the Figure 6.

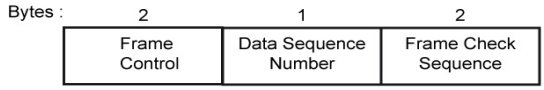

Fig. 6. MAC Acknowledgement Frame Structure

The potential for hiding data or information here is in the Frame Control field, similar to the field of MAC data frame.

D. Command Frame

The structure of the Command frame is given in the Figure 7.

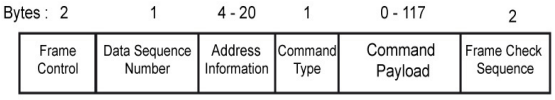

Fig. 7. MAC Command Frame Structure

The Frame Control field and Address Information field provide the same potential of hiding data in the command frame as in the MAC data frame.

3 OUR PROPOSITION

As already proposed that Steganography is possible in 802.15.4 protocol, [1] our proposition will be associating a Public Key with steganography to enhance security. As shown in the Figure 8, if two participants communicating with each other require sharing some sensitive information or a secret message in a network based on the ZigBee specification, the secret message can be hidden in the reserved field bits as discussed above in the related work [1]. But the fact remains that intruders can always try to make attempts to gain access to the sensitive information being transferred, and therefore the communication needs to be kept private so that no other third party is allowed to have access to this sensitive information. For that reason a Public Key can be associated with steganography to keep the communication more secure. Figure 8 shows a block representation of Public Key Steganography. We make an assumption that a sensitive information or data is required to be shared between two participants and no other third party should have access to this data or information. This secret message or sensitive information can be put in the reserved field bits of the MAC layer and associating a private key with it. Once this secret message is encrypted, the formed stego object passes through the channel to the other participant. And so the other participant receives the stego object and decrypts this stego object using a public key. Hence finally the sensitive information or data is delivered to the other participant in the communication. This technique provides a way out to keep the sensitive information being transferred hidden from the third parties who illegally try to gain access to this sensitive information or data.

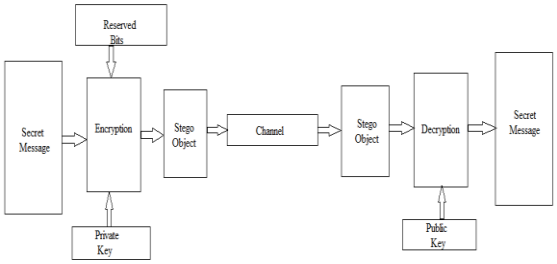

Fig. 8. shows a block representation of Public Key Steganography

4 ADVANTAGE

The technique Public Key Steganography discussed above has an advantage over cryptography and hence provides a better way out in maintaining the security of communications, i.e. to be further secure. As in cryptographic techniques encrypted messages no matter how unbreakable they will be, can provoke doubt or suspicion and can be adequate for an attacker, who eavesdrops the network that something significant has been detected. For that reason to preserve security in such networks we put forward another way out to secure data, using Public key Steganography, which is a technique that permits two participants to dispatch hidden messages over a public channel in a way that an adversary cannot even detect that the hidden messages are being sent. So as cryptography protects the contents of a message alone, Steganography can be said to protect both, contents of the message and even hiding the fact that a secret message is being sent. And once the fact is hidden that a secret message is being transferred in a communication network, there are very less chances of intrusions or any security attacks taking place along the communication.

5 IMPLEMENTATION

The technique finds an implementation in wireless personal area networks based on the protocol ZigBee. The technique provides a better, secure and a reliable way to secure sensitive information or data and hence can be implemented in the following:

1) It can be implemented in the ZigBee-GSM based home security monitoring and remote control system. [5].
2) It has an implementation in the remote lighting control system based on ZigBee technology and SoC solutions. [6]
3) It can even find implementations in the field of Design and implementation of ZigBee-RFID based vehicle tracking. [7]
4) The field of Design and smart home energy management systems based on ZigBee can employ the proposed technique to enhance security and reliability. [8]
5) The smart meters used presently that are developed with characteristics as in metering support, demand response and even the load control support, pricing support, text message support, security support etc can be developed on ZigBee based applications and further the technique can be implemented in these smart meters as well.
6) The ZigBee applications employing the technique can even find an implementation in several devices such as the smoke and heat sensors, the medical and scientific equipments, control units of home and industry and several other wireless communication devices.

6 CONCLUSION

The paper proposes a technique to keep the sensitive information being transferred over a network secure and reliable. The sole aim of this paper is to propose a method which enables to pass a secret message in the form of a stego object and even hiding the fact that a secret message is being transferred in the communication networks. And this can be achieved using the public key steganography technique.

7 REFERENCES

[1] Michael Backes, Christian Cachin, IBM Research, Zurich Research Laboratory, CH-8803R¨uschlikon, Switzerland, "Public-Key Steganography with Active Attacks".

[2] R. Anderson and F. Petitcolas, "On the limits of Steganography," IEEE Journal of Selected Areas in Communications vol. 16, pp. 474–481.

[3] Martins and Herv´e Guyennet Computer Science Department LIFC, University of Franche-Comte Beasancon," Steganography in MAC Layers of 802.15.4 Protocol for securing Wireless Sensor Networks".

[4] Z. Alliance, "In http://www.zigbee.org [access: July 12, 2010]."

[5] Ahmad, A.W. ; Hanyang Univ., Ansan, South Korea ; Jan, N. ; Iqbal, S.; Lee, C. "Implementation of ZigBee-GSM based home security monitoring and remote control system".

[6] Maoheng Sun; Sch. of Electron. & Inf. Eng., Tongji Univ., Shanghai; Qian Liu; Min Jiang, "An implementation of remote lighting control system based on ZigBee technology and SoC solution".

[7] Anuradha, P. ; Network Eng., Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Eng. Coll., Chennai, India ; Sendhilkumar, R., "Design and implementation of ZigBee-RFID based vehicle tracking".

[8] Dae-Man Han; Sch. of Comput. Sci. & Eng., Kongju Nat. Univ., Kongju, South Korea ; Jae-Hyun Lim, "Design and implementation of smart home energy management systems based on ZigBee".

[9] Nesir Rasool Mahmood Kufa University Education College Ali Abdul Azeez Mohammad Kufa University Education College Zahraa Nesir Rasool Kufa University Sciences College, '' Public Key Steganography''.

[10] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das "A Tutorial Review on Steganography", University of Calcutta, 2008.

[11] T. G. Handel and M. T. Sanford, II, "Hiding data in the OSI network model," in Proceedings of the First International Workshop on Information Hiding, (London, UK), pp. 23–38, Springer-Verlag.

[12] F´abio Borges, Renato Portugal, and Jauvane Oliveira "Steganography with Public-Key Cryptography for Videoconference", National Laboratory of Scientific Computing, 2007.

[13] Muthu Ramya.C, Shanmugaraj.M, Prabakaran.R, "STUDY ON ZIGBEE TECHNOLOGY".

[14] Bin Karnain, Md.Azmi; Bin Zakaria, Zahriladha, Information Science and Security (ICISS), 2015, " A Review on ZigBee Security Enhancement in Smart Home Environment".

[15] Mishra, M.; Tiwari, G.; Yadav, A.K., Recent Advances and Innovations in Engineering (ICRAIE), 2014, "Secret communication using Public Key steganography".

[16] Schurgot, M.R.; Shinberg, D.A.; Greenwald, L.G., World of Wireless, Mobile and Multimedia Networks, 2015 IEEE 16th International Symposium, "Experiments with security and privacy in IoT networks".

[17] Z. Trabelsi, H. El Sayed, L. Frikha, and T. Rabie, "A novel covert channel based on the ip header record route option,"Int. J. Adv. Media Commun., vol. 1, no. 4, pp. 328–350, 2007.

[18] S. J. Murdoch and S. Lewis, "Embedding covert channels into tcp/ip," in Information Hiding: 7th International Workshop, volume 3727 of LNCS, pp. 247–261, 2005.