Security attacks to ZigBee technology and their practical realization

Ing. Ján Ďurech*, prof. Ing. Mária Franeková, PhD.*
* University of Žilina/Department of Control and Information Systems, Žilina, Slovakia
jan.durech@fel.uniza.sk; maria.franekova@fel.uniza.sk

In the paper the authors deal with problems of security mechanism in ZigBee network and their analysis and testing in laboratory condition. The realization part is focused on network design with application orientated to smart house, description of network communication, and testing security mechanism of ZigBee network. Authors realised several attacks and proposed recommendations to avoid the attacks. The network is created by modules of the company Texas Instrument.

I. INTRODUCTION

The last two decades wireless networks are getting very popular. Intensive research is being done in wireless networks, which is focused on new technologies in the field of sensor systems, methods of control, energy management in order to improve people's comfort or reducing installation cost for devices. The big advantage of wireless networks is their easy reorganization, possibility of additional connection of many devices and good price.

From large group of wireless networks, the market pushed ZigBee technology, which is based on minimizing of power consumption of nodes in order to achieve longer lifetime of devices, when battery source is used.

The ZigBee standard developed by the ZigBee Alliance [1] is communication technology based on the standard IEEE 802.15.4. ZigBee is not designed for transferring large amount of data, but is designed for home applications and in industry applications. As is shown in fig.1, IEEE 802.15.4 standard defines the physical and MAC layer, ZigBee defines network and application layer. The ZigBee Alliance was formed in 2002 as a nonprofit organization. In 2003 standard IEEE 802.15.4 (later modified in 2006) was released, which was adopted by ZigBee Alliance and in 14. December it has released the first ZigBee 1.0 specification [2].

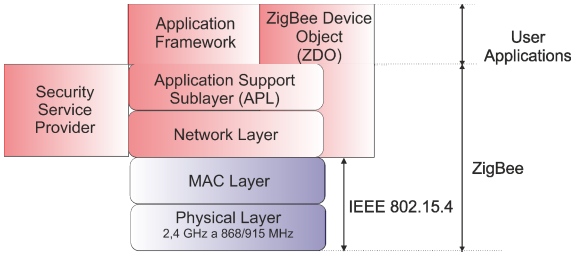

Figure 1. Reference model of ZigBee network.

Even though the ZigBee technology uses from the point of security algorithms computationally security mechanisms, which will be described in the next chapter, when the algorithms are not used correctly, it is possible to break up the communication very soon. If the ZigBee technology would be used in safety-related application within control systems in industry [3] with SIL 3 (Safety Integrity Level) it is necessary to realize detailed safety analyses of security mechanism [4], [5].

II. SECURITY SERVICES OF ZIGBEE NETWORK

By using of the wireless networks the question of their security become more actual. In a wireless networks we need to deal with two challenges. The first challenge is error-free transmission of data and the integrity check, the second challenge is to secure data against their capture and to avoid attacks against network. For error-free data transmission standard IEEE 802.15.4 uses FCS (Frame Check Sequence), which is creating checksum of framework. FCS is used for data integrity, which may be corrupted due to noise. For the integrity check standard ZigBee used MIC (Message Integrity Code), which ensures data authentication. For the purpose of data confidentiality the encryption standard AES (Advanced Encryption Standard) is used.

ZigBee standard supports the following security mechanisms:

- Data encryption.
- Data verification and devices verification.
- Protection against duplicate frames.

A. Frame Check Sequence – FCS

Standard IEEE 802.15.4 uses 16-bits FCS control field based on CRC (Cyclic Redundancy Check). It is a detection technique, which is used to detect potential errors in incoming packet. Concept of CRC is based on the remainder of a polynomial division, which is calculated from MAC header and payload. Recipient is calculated own FCS and when it is equal with received FCS, frame is considered as error-free. According to IEEE 802.15.4 generating FSP checksum and its check runs according to the following steps:

- On the transmitter site is created polynomial $M(x)$ from MAC header and MAC payload.
- Polynomial $M(x)$ is multiplied by the highest power of generating irreducible polynomial $g(x)$, which is defined as $g(x)= x^{16} + x^{12} + x^5 + 1$.
- Thus obtained polynomial is divided by $g(x)$, thereby creating remainder of dividing $r(x)$ is added to the MAC footer.
- Receiving side to start again dividing received polynomial, corresponding received data, agreed by generator polynomial $g(x)$.

978-1-4799-3442-3/14/$31.00 ©2014 IEEE

- If the division is without remainder in the incoming packet error was not detected, when division is with remainder packet was corrupted while transmitting.

According to knowledge of channel coding theory, e. g. in [6], CRC code with applying generator polynomial 16^{th} order, should be able to detect in the packet simple error and also a burst of errors corresponding generating polynomial degree. Described CRC code is used by link layer to detect errors in received packet. Mathematical principles of safety analyses of cyclic CRC code are possible to see e. g. in [7]. To verification of data, whose integrity could be disturbed knowingly, ZigBee standard uses message authentication code MIC (Message Integrity Code).

B. Data confidentiality

The IEEE 802.15.4 standard supports the AES (Advanced Encryption Standard) in order to maintain the data confidentiality. The AES algorithm is 128-bit block cipher which supports three key lengths (128, 256, 512 bits) announced by NIST (National Institute of Standards and Technology), which is also used by the ZigBee standard with key length of 128-bits. Nowadays scientists believe the AES as computationally safety cipher. Mathematical principles of AES are based on confusion a diffusion which is realized in 10 rounds (for length of key 128 bits).

Process of encryption is realized within nine rounds by the four identical operations:

- *Add round key* – to add the key of actual round.
- *Substite bytes* – to realize substitutions of bytes from state array using S-box.
- *Shift rows* – to realize permutation of rows by cyclic shift of bytes in rows according to define rule.
- *Mix columns* – to realize substitution of bytes in state array matrix using arithmetic of Galois field GF(2^8).

Tenth round includes three operation only because operation Mix columns is drop out.

In detail these four operations are described in [8].

Security of AES algorithm is possible to increase using CBC (Cipher Block Chaining Mode) [9] in which is realized chaining of encrypted blocks and the first cipher text block is random by IV (initial value).

One of the main limitations in implementing security features in a ZigBee network is limited resources. The nodes are mainly battery powered and have limited computational power and memory size. ZigBee is targeted for low-cost applications and the hardware in the nodes might not be tamper resistant. If an intruder gets access to a node from an operating network that has no tamper resistance, the actual key could be obtained simply from the device memory [10]. Fig.2 shows the basic concept of encryption in ZigBee network based on symmetric encryption scheme with private key

C. Data authentication

Data integrity is achieved by authentication code messages MIC. Message authentication code is a function that by a secret key produces an output fixed-length value that serves as the authenticator. The cryptographic checksum MIC is a block of bits of constant length which is attached to the original message. If MIC provided by the transmitter is equal with MIC calculated by the receiver, the data will be considered as authentic. The level of data authenticity is increased by increasing the number of bits in the MIC. The ZigBee and IEEE 802.15.4 standards support 32-bit, 64-bit, and 128-bit MIC options.

Note: The MIC is also referred to as Message Authentication Code (MAC*), but the ZigBee and IEEE 802.15.4 standard documents use MIC instead of MAC to avoid confusion with the Message Authentication Code (MAC*) and the Medium Access Control (MAC).

The MIC in ZigBee is generated using the enhanced Counter with Cipher Block Chaining Message Authentication Code (CCM*) protocol. The CCM* is defined to be used in conjunction with 128-bit AES and shares the same security key with AES. The responsibility of the AES-CCM* is to encrypt the data and generate an associated MIC, which is sent to the receiver along with the frame. On the transmitter side, the plaintext in the form of 128-bit blocks of data enters the AES-CCM*. The receiver uses the AES-CCM* to decrypt the data and generate its own MIC from the received frame to be compared with the received MIC. The CCM* is referred to as a generic mode of operation that combines the encryption and data authentication.

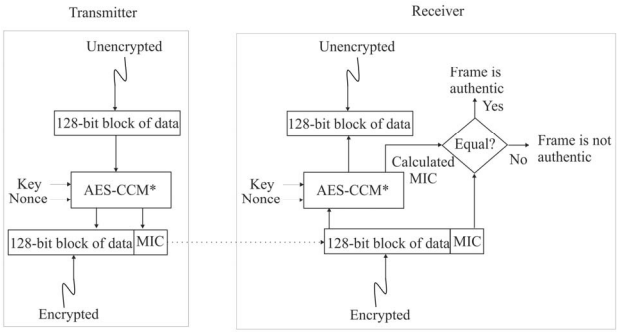

Figure 2. Encryption scheme in ZigBee network.

Three elements enter in the block AES-CCM*: data, security key and NONCE (Number used ONCE). NONCE is 13-octet string using the source address fields of auxiliary header, security control and the frame counter. AUS-CCM* uses the NONCE as part of algorithm. By adding frame counter to the NONCE, which is incremented every time a new frame is transmitted, encryption of two identical messages will always result in two different results. The use of the NONCE ensures freshness of received frame. When intruder without knowledge of security key capture secured message and after a time simply resend the exact message, this retransmitted message will have all the correct security features of a valid message, but frame counter will indicate that the frame was received preciously. In this way, the frame counter helps identify and prevent processing of duplicate frames. This is referred to as checking the frame freshness. If the intruding device changes the frame counter associated with the frame before retransmitting the frame, the receiver device will notice this unauthorized modification when it compares the calculated and received MICs [10]

When we assume that the only part A and B own a secret key, and if the calculate value of MIC is equal to

received value of MIC, we can derive the following conclusions:

- The addressee B can be sure that message has not been modified. If the intruder has changed the message and not changed value of MIC, than comparing the received MIC values and calculated MIC values is detected mismatch. Since the intruder does not know the secret key, is unable to identify and associate the correct value of the MIC to changed message.
- The addressee B can be sure that message comes from the declared subject A, since only subject A own secret key, which allows to generate the correct value of MIC.

Authentication code MIC is very similar to encryption, but difference is that MIC is not reversible, therefore decryption cannot be realized.

III. Design of ZigBee Wireless Network for Controlling Smart Houses

For practical application we used development kit CC2530ZDK [11] from Texas Instruments. Creation of our network is based on proposal of appropriate hardware accessories, programming of applications in C language for each device, compilation and uploading into the devices.

In our application (illustrated in fig.3) we have one control unit which is remote control of whole network. Control unit is communicating with coordinator. Coordinator takes care about entire network. When control unit send command to coordinator, coordinator takes care for solved of this command. Coordinator is only unit which is communicating with sensor and end devices. In our application we are controlling lighting, heating, computer and coffee maker.

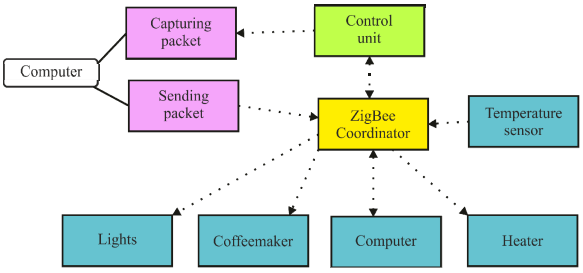

Figure 3. Concept of realized ZigBee network.

Software realization of all devices was made in program IAR Embedded Workbench. As converter between ZigBee boards and power devices we are using power switch described in [12]. After we turn on network we were observing noise in 2,4 GHz band. On fig.4, blue part is noise from another devices transmitting in 2,4GHz band. The green part is transmission off ZigBee signal [15].

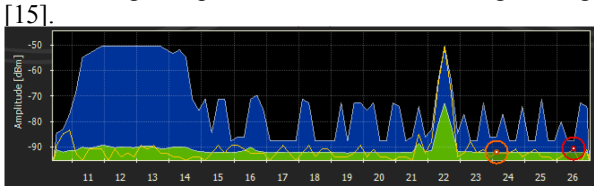

Figure 4. Spectrum of 2.4 GHz band.

IV. Results of Attacks Realizations to ZigBee Network

When we build our network we start to test security of network and we were trying to hack the network. At first experiment our network was in mode - unsecured. When intruder get access to unsecure network, he can easily capture packet and than he is able to get access to entire network. Intruder must to know source address, destination address and PAN ID for sending packet. Than he can send captured packet witch increased sequence number, or he can generate own packet.

We used program SmartRF Studio 7 to capture and resend packet. Capturing was made via special ZigBee USB key, which can be used after connecting to computer for purpose of communication computer with ZigBee network, connecting external devices or capturing packet. Sending unencrypted packet is shown in fig. 5. Because network was unsecured we have captured the packet between control unit and coordinator and then we were easily resending packed with increased sequence number. We were immediately able to control light. If we captured more packets, or start generate own packets it is very probable we could take control of entire network. To avoid this attack the network should be secured.

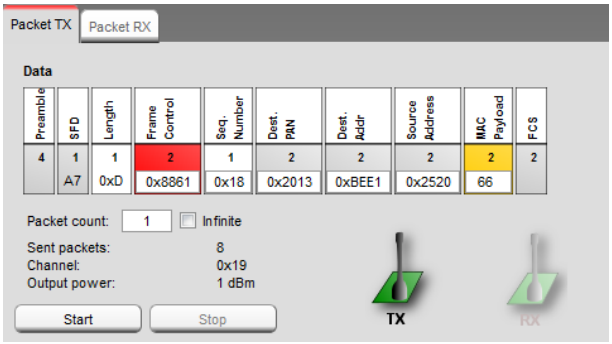

Figure 5. Example of sending unencrypted data.

A. Physical attack

Development kit CC2530ZDK which was used support in order to secure ZigBee network the 128 bit AES encryption with 64 bit MIC for data authentication. Big advantage of this type of security is that encryption the same plaintext two times will result in two different cipher-text because the sequence number in NONCE is used in encryption. This is known as semantic security. Breaking so secure network other than brute force attack is almost impossible. ZigBee network have one disadvantage that all passwords are stored unencrypted in storage. If intruder get physical access to the device, he can copy device memory to computer, in which can he find the key.

We made this physical attack with one device which has USB enter. We had easily plug device to computer and then we had copy all device memory to the computer. In this memory we had found the unencrypted key: c0c1c2c3c4c5c6c7c8c9cacbcccdcecf (see fig. 6). Position of key is always in same place in same microchip. In other brand of chip key may be in different place, but intruder can easily find out where it is. To avoid to this attack devices should be in tamper resistant box and when the violation is recorded device should delete its memory.

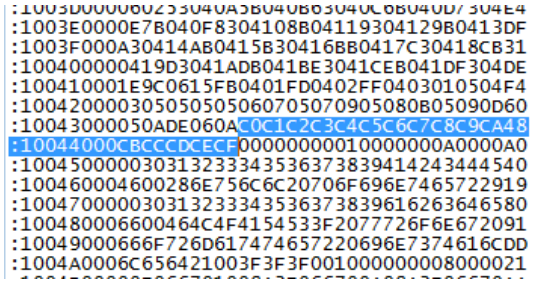

Figure 6. Key kept from memory of equipment.

B. *Same-NONCE attack*

Encrypting the same two plaintext two times will always result in two different cipher-texts, because in encryption is also used sequence number of frame. If for any reason device sent two consecutive messages m1 and m2 with same NONCE eavesdropper will have two different encrypted data c1 a c2 encrypted with same key and using XOR operation (1), "listening" device will be able to recover partial information about the original text using the formula:

$$c_1 \oplus c2 = [m_1 \oplus E(key, nonce)] \oplus [m_2 \oplus E(key, nonce)] = m_1 \oplus m_2 \quad (1)$$

This attack is known as the same-nonce attack. One of the occasions on which a same-nonce attack can happen is after the power failure that results in a clear of accumulator. If the last nonce states are unknown after the power failure, the system might reset the nonce states to a default value. This reset action increases the chance of reusing the same nonce with a key that has been used before the power failure [10].

We did this attack while we controlled lights, when every time after sending one message we reset device taking out the battery. The result of XOR original transmitted data was: 66h ⊕ 67h=01.

We used XOR operation also for captured encrypted data:

0600000000C515E5F9DF5193C558
⊕0600000000C485107A5FBADA5151 =
0000 000000 **01** 90f58380eb499409,

where we can see in the result the original data 01 after XOR operation.

If intruder knew more dates, he can easily calculate missing dates. To avoid this attack it would be necessary to store the nonce states in a nonvolatile memory and to recover them after each power failure.

C. *Denial of Service (DoS) attack*

DoS attack causes a node to reject all received messages [10]. Attack is an attempt to prevent legitimate users to use the network. Basic types of attacks are: overload the bandwidth or overload the processor. We made attack for overload the processor.

In realization this attack we were using program SmartRF Studio 7. First step of attack was capture of a packet. Then we were resending this packet at speed 30 packets for second. Our network is using acknowledgment of packet, i.e. the coordinator must send an acknowledgment packet to every frame, even if packet is discarded in upper layers when received, because it is a duplicate frame. After 250s of attack and 7442 sent packets coordinator stop reacting. To avoid this attack the change of transmitted channel after received hundred duplicate packets would be needed.

D. *Replay attack*

Secured networks are using trust center, which take cares about keys. Secured networks do not using one key all time, but they are using several keys and they continuously changed the key. Simple networks which are not using trust center and all time are using same key are vulnerable against resented old captured packet. For intruder is enough to capture data with higher sequence number and after the time when sequence number is reset retransmit the packet.

We realized this attack also by using program SmartRF Studio 7. We captured encrypted packet for control of light. After the time when we were monitoring communication and sequence number were reset, we resent this packet and ZigBee coordinator processed this packet. We were able to turn on light. To avoid this attack the trust center in network or several keys in network should be used.

V. Conclusions

ZigBee technology offers large solution for monitoring, control of different devices within application of smart house. Big advantage of ZigBee is compatibility with other devices and supporting energy efficient communications with sufficient assuring.

In the paper secure mechanism of ZigBee network based on ciphering and verification techniques and assuring of data integrity were described. In the laboratory conditions were realized four cryptography attacks to networks and were described the recommendations how to prevent them. The obtained results have their foundation in the future work focused on applying ZigBee technology in safety – related applications with requirement to increase of the safety integrity level (e. g. safety-related control and communication systems in industry), when it is necessary to proceed according to general norm IEC 61508 or norm valid for industry applications. In security critical applications, the cryptography mechanisms are recommended to use for reducing of masquerade effect. Cryptography mechanisms provide different level of safety in compliance with the type of cryptography algorithm and the length of its key. According to results of cryptanalytic attacks realization against the standard wireless ZigBee communication we can observe that this system without implementation of added safety layer does not fulfil the requirements to safety-related communications [13], [14]. In spite of this applying of ZigBee technology without additional safety layer is very wide in COTS (Commercial Off the Shelf) technology where we may include applications within smart buildings.

Acknowledgment

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 024ŽU-4/2012: Modernization of technology and education methods orientated to area of cryptography for safety critical applications.

REFERENCES

[1] ZigBee Alliance: [online]. In: http://www.zigbee.org

[2] IEEE 802.15.4: Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE Computer Society, 2006. ISBN 0-7381-4996-9

[3] T. Malm, J. Hérard, J. Boegh, M. Kivipuro: Validation of safety-related wireless machine control systems. NT Technical report TR 605, Oslo, Norway, 2007. ISSN 0283-7234

[4] M. Franeková: Safety and security profiles of industry networks used in safety - critical applications. In: Problemy transportu – Transport Problems. International Scientific Journal. Volume 3, Issue 4, Part 1, p. 25-32, Gliwice, 2008, Poland, ISSN 1896-0596

[5] T. Ondrašina, M. Franeková.: Attacks to cryptography protocols of wireless industrial communication systems. In: International scientific journal Advanced in Electrical and Electronic Engineering. ČR. Section: Information and Communication Technologies and services, Vol. 8, No. 3, September 2010, p. 77-82. ISBN 1804-3119

[6] Ľ. Muzikářová, M. Franeková, P. Holečko, M. Hrnčár: Theory of Information and Signals. In: English. EDIS, ŽU in Žilina, 2008, ISBN 978-80-8070-992-1

[7] M. Franeková: Mathematical apparatus for safety evaluation of cryptography and safety codes used in safety-related communication system. In: Modern transport telematics: 11th international conference on transport systems telematics, TST 2011, Katowice-Ustrón, Poland, October 2011, selected papers: Springer-Verlag. Berlin Heidelberg, series CCIS 104 - Communications in Computer and Information Science, p 126-135, ISBN 978-3-642-24659-3

[8] NIST FIPS PUB 197: AES standard, 2001.In: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[9] NIST SP 800-38A: Recommendation for block cipher modes of operation. 2001

[10] S. Farahani: ZigBee wireless networks and transceivers, Oxford: Newness, Elsevier Inc, 2008. ISBN: 978-0-7506-8393-7

[11] Texas Instruments: CC2530 ZigBee Development Kit User's Guide, In: http://focus.ti.com/lit/ug/swru209b/swru209b.pdf

[12] J. Ďurech: Applying ZigBee network in smart house. In Slovak. Diploma thesis, ŽU in Žilina, 2012

[13] T. Ondrašina, M. Franeková: Safety mechanisms of ZigBee technology for safety-related industrial applications. In: Journal Archives of Transport System Telematics, Volume 4, Issue 2. May 2011, Poland, p. 43-47, ISSN 1899-8208

[14] I. Zolotová, I. Landryová: Knowledge model integrated in SCADA/HMI system for failure process prediction. In: WSEAS Transactions on Circuits and Systems. Vol. 4, no. 4 (2005), p. 309-318. - ISSN 1109-2734

[15] T. Ondrašina: Safety mechanism of wireless networks for industrial automation. In Slovak. PhD thesis, ŽU in Žilina, 2011.