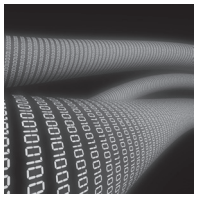

Archives of
Transport System
Telematics

Volume 4

Issue 2

May 2011

Safety mechanisms of ZigBee technology for safety-related industrial applications

T. ONDRAŠINA[a], M. FRANEKOVÁ[a]

[a]Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia

EMAIL: tomas.ondrasina@fel.uniza.sk

ABSTRACT

Authors describe the possibilities of a wireless technology used within safety-critical applications with orientation to selection the computationally safety cryptography techniques. Undetected corruption of data transmission can cause substantially considerable damages within equipments, environments or demands on human health and this is reason why systems have to be designed so that guarantee required Safety Integrity Level. For this reason the safety-related wire or wireless machines must have implemented a number of safety mechanisms located into special safety or security profiles. Nowadays, after acceptation of the new standard ISA 100.11a the barrier was broken towards the use of wireless machine-to-machine communications in standard and safety-related communication, too. ZigBee technology is very accepted standard which fulfils the requirements to the wireless industrial communication system.

The main part of the paper describes the possible attacks to ZigBee communications based on cryptography mechanisms with orientation to Denial-of-Service attack. The practical part contains the results of ZigBee sensor network testing in laboratory conditions with demonstration of error-control mechanisms of MESH topology and cryptoanalytic's attacks based on monitoring of traffic are mentioned as well.

KEYWORDS: safety industrial communication system, wireless technology, ZigBee, safety integrity level, confidentiality, device and data verification, AES standard, link key, network key, cryptoanalysis

1. Introduction

Developments of wireless networks record a very important role in many areas of control systems [1]. Wireless networks have become un-substitutable technology within intelligent transport systems where networks allow providing services which directly relate with the security of traffic flow as well as services that are connected with better knowing of car drivers by selection of various charges, adjoin in public communication networks. Wireless sensor networks became the new technologies used within technological level of control systems, too. Nowadays, after acceptation of new standard ISA 100.11a: "Wireless systems for industrial automation. Process Control and Related Applications" [2], the barrier towards the use wireless machine-to-machine communications in standard and safety-related communication was broken, too (with additional safety profile). The protocol ISA 100.11a was developed for very unfavourable operation conditions

which can occur in manufacturing area with requirements on robustness, resistance against interferences and network security. These requirements fulfil the wireless industrial communication system based on ZigBee technology too [3]. Today the following specifications of ZigBee technology are available: ZigBee 2004, ZigBee 2006, ZigBee 2007 and ZigBee RF4CF. Technology ZigBee was developed for purpose of effective data exchange between sensors. The advantage of ZigBee industrial network is possibility to use the large number of devices which cooperated with other devices within one network. Technology ZigBee is projected so that minimizes the consumption of energy. This allows the long lifetime of device in the case of accumulator source using. The additional advantage of ZigBee technology in comparison with another communication forms is that devices in network can direct the data with each other and can be mobile. Like that the devices do not need to be in direct range of device with which want to communicate. Technology is achieved to assure reliable transmission of data across very noise environments too. Version ZigBee 1. 1 represents the fundamental break in process development of this standard. Main modification in standard development is transfer from tree address structure to address allocation randomly with mechanism of address collision detection. This improvement increases the stability of network and creates the large scale of ZigBee applications. Next modification ZigBee 2007: for intelligent house applications and for commercial applications, which is signed as ZigBee PRO [4] and supports the additional functions as multicast communications, routing many-to-one and the high security with applying cryptography algorithm on the base of symmetric cryptography. In March 2009 consortium RF4CE (Radio Frequency for Consumer Electronics) arranged the cooperation with ZigBee Aliance and they created the standardized specification ZigBee RF4CE for remote control which is faster, reliable and offers the better free scope in devices operation and allows to apply advanced functions, e. g. bi--directional communications between device and remote control system.

Development of additional safety profiles within wireless industrial communications supports safety-related communication between safety-related devices generally in safety integrity level (SIL) 3 and by it increases the

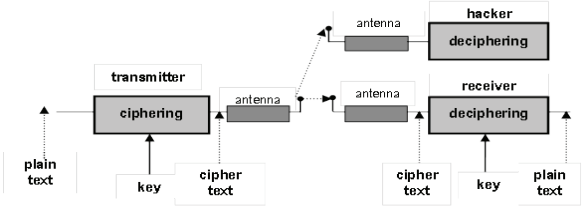

Fig. 1. Process of enciphering in ZigBee

applying the ZigBee technology within safety-critical control systems, too [5].

In the paper authors considered the safety mechanisms used within communication protocol with orientation to cryptography techniques on the base of theoretical and practical results.

2. Analyses of safety mechanisms of ZigBee

Before ZigBee technology applying it is necessary to remember that the transmitted messages in wireless network can be received by any device which is near of transmitter. Generally, two unintentional attacks are well known: attacker can keep the information by wiretapping of messages or can modify the message and repetitively send one from previous messages. The first attack we can eliminate by ciphering of all content of message which offers ZigBee standard IEEE 802.15.4 [6]. In standard the symmetric block cipher AES (Advanced Encryption Standard) is used [7]. The second attack can be eliminated by the auxiliary cryptography mechanism using so called MIC (Message Integrity Code) which is added to transmitted frame and which allows the receiver side to determine the modification of message. This process is known as data authentication.

One from major limitation of safety functions realizations within a wireless network is a problem of limited supply. The nodes are mostly powered by battery packs and they have limited power and the store size. If the attacker keeps the access to node which is not assured he/she can obtain the secret key from device memory. If unauthorized access was detected, the assured node can be able to delete secret information including the value of key.

2.1. Safety procedure of enciphering

The basic concept of the ciphering on the base of the symmetric cryptography system with the secret key used in ZigBee technology is illustrated in the Figure 1 [8].

The most sensitive part of this system is the secret key which is changing for every transmitted frame. The length of key determines the level of assurance. ZigBee support 128 bits key what is the computationally safety length today for brute force attack realization. The attacker (hacker) must test 3,4 $*10^{38}$ possible keys. The transmitter and the receiver use for ciphering and deciphering the same key. ZigBee supports several methods for key implementation and its sharing between two or more devices. Standard ZigBee uses two types of keys: link key and network key. Link key is sharing between two devices and can be used within unicast communication. Network key is common

for all networks and it is used within message transmission. Each assured ZigBee network contents one device called trust centre which the link and network keys distribute to another devices. Trust centre works in two modes of operation: commercial and residential. In commercial mode, e. g. some industrial application, the trust centre must store the list of devises, master keys and network keys. All received frames are checked if they are not duplicate frame. The size of memory increases within the commercial mode of operation dependence on number of devices in networks. Residential mode is determined for modest house applications.

2.2 Safety procedure of authentication

ZigBee standard supports two safety procedures: devices and data authentications. Device of authentications is realized after connection the new device to network. The new device must be able to receive the network key and set the right attributes in given time. Within the safety procedure of data authentications the receiver checks if data was not re-sequences or corrupted. Device authentication is realized by trust centre. The procedure of authentication is different for resistance and commercial modes of operations. In the commercial mode trust centre never sends the network key to new device across untrusted channel. The master key can be sent as en-secured if the new device does not have the same main key as trust centre. Then the new device keeps the master key of trust centre and the new device starts protocol for key distribution. The new device has the limited time for creating the link key (Aps Security Time Out Period). If within the limit of device does not keep the key the authentication procedure must start again. When the new link key is certified the trust centre sends the network key to the new device across trusted channel. The purpose of data authentication is to assure the data during transmission. This problem is solved by addition of MIC (Message Integrity Code) to every transmitted frame.

MIC works on the same principle as MAC (Message Authentication Code) [7] so called key hash function and uses the secret key to determination of code by fixed length. Algorithm of MIS is known for all sides the secret key is store only. If received and determined code MIC in received frame are the same data is identical. The level of assurance increases with the lengths of MIC code bits. ZigBee and IEEE 802.15.4 standards support three levels of safety according to bit lengths of MIC code: 32 bits, 64 bits and 128 bits.

The safety of MIC code is increasing in ZigBee with using the special protocol in which MIC is generated as CCM (Counter with Cipher block chaining Message authentication code). CCM is designated for using in connection with AES ciphering standard with block of plaintext 128 bits and key length 128 bits too.

The principle of AES-CCM mechanism within data authentication is illustrated in the Figure 2. Algorithm AES in CCM mode assures both the ciphering of data and generating the additional hash code MIC, which is transmitted with the ciphering frame. On the received side the receiver knows algorithm AES-CCM on the base which is generating the MIC and comparing with received code. CCM is marked as a special type of operation which combined the ciphering (service of confidentiality) and data authentications (service of integrity). CCM supports the possibilities of ciphering only or data authentication separately according to requirement safety level of application.

AES-CCM algorithm has three inputs: data, safety key and single-sweep value of NONCE (Number Used ONCE). In the Figure 3 CCM NONCE and auxiliary header of the frame are illustrated. NONCE is 13-octave string which uses the fields from auxiliary header: safety field, counter of frames and source address. AES-CCM uses NONCE as a part of its algorithm. The value of it is never equal for two messages, because the counter value

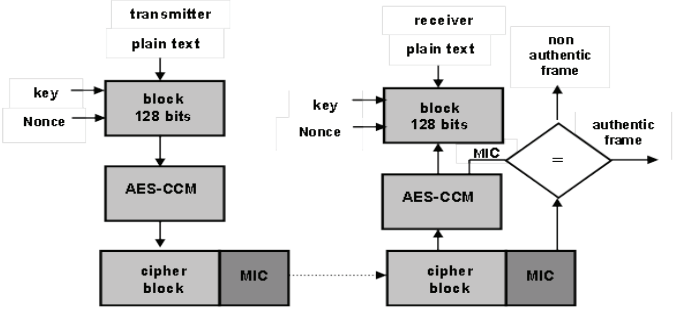

Fig. 2. Principle of AES-CCM

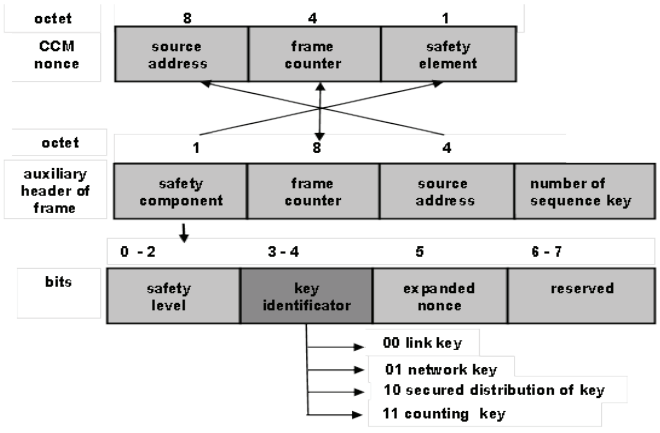

Fig. 3. Format of auxiliary header within CCB NONCE

is increasing about one for each transmitted frame. If attacker generates the same frame in this manner counter of frame helps identifier of duplicate frames. The format of the auxiliary frame is illustrated in the Figure 3 [9].

3. Denial of Service attack

Although the ZigBee technology belongs to relatively new wireless technologies in comparison with e. g. Wi-Fi several cryptography attacks against it are well known today. Very popular are the attacks which do not require for attacker to gain the access to the cryptographic keys stored in a ZigBee device and they can be performed remotely from the wireless space. During attack realisation it is not necessary to manipulate within physical level of devices. The main attack which follows this condition is Denial of Service (DoS).

This attack can be performed at several layers of communication protocol and depends on whether the attacker has joined the network, being part of it (an insider) or not (an outsider) [10], [11].

If the attacker is an insider, the DoS attack may be con-ducted at the physical (PHY), link (MAC), network (NWK) or application (APS) layers, whereas if the attacker is an outsider, DoS may be conducted at the PHY and MAC layers only. Figure 4 classifies the all possible DoS attacks according to communication layer.

Characteristics of insider attacks:

At the APS layer, DoS is performed by sending a great deal of messages to the device (flooding) with aim to interrupt message processing. In addition, this action exhausts the device resources, such as battery. This attack can be easily detected, since all the messages are sent from a specific device.

At the NWK layer, DoS is executed by modifying the default routing protocol. If the attacker, which is placed within the network, is a compromised router, it can stop forwarding messages between nodes, which leads to changes to the routing protocol. Fortunately, this DoS attack may be directly detected and avoided by the default routing protocol. The sensor can just start sending messages via another router, if possible.

Characteristics of outsider attacks:

At the MAC layer, ZigBee uses CSMA/CA method to guarantee that all the devices can communicate through the same communication channel. Once a device intends to transmit data, the communication channel should be listened during the specific time. If the channel is sensed idle, then the node is permitted to begin the transmission. However, if the channel is sensed as busy, the node defers its transmission for a random period of time. A DoS attack occurs if a device starts consuming bandwidth unfairly. For example, if the attacker starts continuously sending data over the communication channel, other devices cannot communicate to each other.

Fig. 4. Possibilities of DoS attack realisation in relation to communication layer of protocol

At the PHY layer, the DoS attack is performed by direct jamming of the channel. This attack can be executed through an outsider device by disrupting the signal of other devices by changing the Power Spectral Density (PSD). In fact, a jammer can never re-produce a signal nor it can pretend to be a receiver node. There are some parameters such as signal strength of a jammer as well as the location and its type which may influence the performance of the network.

To perform jamming, the attacker should be near to the device or use an adequate level of transmission power [11], [12]. This is since the transmitted signal loses energy as the distance increases.

4. Practical realisation

The testing scenario was realized in the laboratory conditions with the used of developed kit Texas Instrument CC2530ZDK.

The kit includes the following parts:

- 2X SmartRF05EB,
- 5X SmartRF05BB,
- 7X CC2530 evaluation modules,
- 7X antenna,
- 1X CC2531 USB key.

In practical construction of ZigBee network the following devices were applied: the sensor (sender), the router (receiver) and an external device (attacker). The cryptography attack based on DoS method to ZigBee network was realised in MAC layer and the process of realisation is described by Figure 5. For catching the frames the catching key - type CC2531USB Dongle was used.

Description of procedures within realised attack (see Figure 5):

(1) While the sensor is sending a message to the network, the attacker interferes and corrupts the transmitted data, so the receiver does not receive the complete message.

(2) To ensure that the sensor does not resend the message again, the attacker generates an ACK message and sends it back to the sensor (sender). Due to not checking the authentication, the sensor assumes that the message has been sent to the router.

ZigBee frames were catching via SW tool SmartRF Packet Sniffer from Texas Instruments, Inc. The structure of one catching frame number 19 (from 100 catching frames) is illustrated in the Figure 6.

Monitoring of ZigBee traffic via SW tools belongs among useful apparatus on the base which attacker can keep important information about time, large of transmitted message, security level, and destination address. Obtained data from large number of keeping frames can be applied within statistical evaluations of traffic and then within realisation of active attacks, e. g. DoS attack.

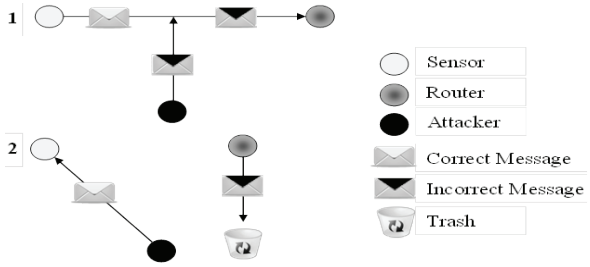

Fig. 5. ACK-MAC layer attack

Pnbr.	Time (us)	Length	Frame control field					Sequence number	Dest. PAN	Dest. Address	Beacon request	LQI	FCS
			Type	Sec	Pnd	Ack.req	PAN_compr						
RX	+79452												
19	=148005016	10	CMD	0	0	0	0	0x45	0xFFFF	0xFFFF		220	OK

Fig. 6. Example of catching frame during ZigBee traffic via SW tool SmartRF Packet Sniffer

5. Conclusion

Nowadays the security mechanisms are used as support for safety-related wireless machine too, which communicate across Wi-Fi, ZigBee and other wireless media [5]. In this case it is necessary to orient oneself to a safety computationally security cryptography mechanisms which are resistant against well-known cryptoanalytic attacks. Practical realisation of attacks methods in laboratory conditions is useful knowledge for designer of a safety-related system in process of selection of parameters of cryptography mechanism (the length of key, mode of operation or security level).

In safety-related wireless communications is necessary to choose the safety mechanisms according to standards relevant for the open transmission systems. Cryptography mechanisms provide different level of safety in compliance with the type of cryptography algorithm and length of its key. Under the results of realisation of one of most well known cryptanalytic attack to secure wireless communication we can observe that this system without implementation of additional security layer does not fulfil the requirements to safety-related communications. In this case the value of SIL 0 is necessary to increase to value of SIL 1 – 4 (by implementation of security communication profile).

Acknowledgement

This work has been supported by the European Regional Development Fund and the Ministry of Education of the Slovak Republic, within the project ITMS 26220220089 "New methods of measurement of physical dynamic parameter and interactions of motor vehicles, traffic flow and road".

Bibliography

[1] GALAJDA,P.-MARCHEVSKÝ,S.-GAMEC,J. GAMCOVÁ,M.-PILLÁR,S.: Infrastructure for Packet Based e-learning Services Provided Via Satellite. In: Acta Electrotechnica et Informatica, Vol.9, No.1, 2009, 74-80.

[2] ISA 100.11a: Wireless systems for industrial automation: Process Control and Related Applications. International Society of Automation. 2009.

[3] http://www.zigbee.org

[4] VOJÁČEK, A.: ZigBee PRO - new improved version of wireless ZigBee.: In: http://automatizace.hw.cz/

[5] MALM, T.- HÉRARD, J.- BOEGH, J.- KIVIPURO, M.: Validation of safety – related wireless machine control systems. Technical report TR 605. 2007. ISSN 0283-7234

[6] 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

[7] http://www.fips-197.com

[8] GISLASON, D. ZigBee Wireless Networking, Oxford: Newnes, Elsevier Inc, 2008. 448 s. ISBN: 978-0-7506-8597-9

[9] FARAHANI, S. ZigBee Wireless Networks and Transceivers, Oxford: Newnes, Elsevier Inc, 2008. 448 s. ISBN: 978-0-7506-8393-7

[10] MURALEEDHARAN, R. - OSADCIW, L., A.: Jamming attack detection and countermeasures in Wireless Sensor Network using ant system. In Proceedings of the SPIE, 2006.

[11] EGLI, P.: Susceptibility of wireless devices to denial of service attacks. Technical white paper, Netmodule AG, 2006.

[12] BRODSY, J. - McCONNELL, A.: 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.