ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys

Pedram Radmand[1], Marc Domingo[2], Jaipal Singh[1], Joan Arnedo[2], Alex Talevski[2], Stig Petersen[3], Simon Carlsen[4]
[1]Digital Ecosystem and Business intelligence Institute, Curtin University of Technology, Perth, Australia
e-mail: pedram.radmand@postgrad.curtin.edu.au, {J.Singh, A.Talevski}@curtin.edu.au
[2]Estudis d'Informàtica, Multimèdia i Telecomunicació, UOC, Barcelona, Spain
e-mail: {mdomingopr, jarnedo}@uoc.edu
[3]SINTEF ICT, Trondheim, Norway
e-mail: stig.petersen@sintef.no
[4]$StatoilASA, Trondheim, Norway$
e-mail: SCAR@StatoilHydro.com

***Abstract*—Sensor networks have many applications in monitoring and controlling of environmental properties such as sound, acceleration, vibration and temperature. Due to limited resources in computation capability, memory and energy, they are vulnerable to many kinds of attacks. The ZigBee specification [1], based on the 802.15.4 standard [2], defines a set of layers specifically suited to sensor networks. These layers support secure messaging using symmetric cryptographic. This paper presents two different ways for grabbing the cryptographic key in ZigBee: remote attack and physical attack. It also surveys and categorizes some additional attacks which can be performed on ZigBee networks: eavesdropping, spoofing, replay and DoS attacks at different layers. From this analysis, it is shown that some vulnerabilities still in the existing security schema in ZigBee technology.**

I. Introduction

Wireless Sensor Networks (WSNs) comprise of a large number of spatially distributed autonomous devices that may collect data using a wireless medium. They may be used to cooperatively control and monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion and pollutants, at different locations. WSNs exhibit several unique properties as compared to their wired counterparts, such as large scale of deployment, mobility of nodes, temporary installations, redundancy and dynamic network topologies. However, each sensor node has constraints on its operational environment, energy, memory, computation speed and available bandwidth [3].

WSNs are generating significant interest in the industry area and moving into the wireless domain. This technology has the potential to be beneficial in many fields, such as oil and gas, military and medicine. Since information security is a very important factor for these industries, any WSN application requires secure communications. Due to the absence of physical protection, security in WSNs is extremely important [3]. Unfortunately, WSNs, and indeed all other wireless networks, are inherently and ultimately insecure, since their availability can be selectively and strategically modified by manipulating the radio environment.

This paper presents a survey on the existing security schema in the 802.15.4/ZigBee specification [1], focusing on vulnerabilities in this technology. We categorize and provide a detailed description of the different kinds of attacks in the related literature and as well as explaining how they may be actually executed by taking advantage of the current ZigBee specification weaknesses.

This paper is organized as follows. Section II provides an overview of the 802.15.4/ZigBee specification security. Section III explains the security assessment of this technology, which may be divided in attacks which require key compromise and attacks which do not. Finally, Section IV exposes the summary and conclusions of this paper.

II. ZigBee Security Features Overview

The ZigBee Alliance is a group of companies that develop and maintain the ZigBee standard. ZigBee is a specification for a suite of high level communication protocols built over IEEE 802.15.4. One important characteristic of ZigBee is that tries to be simpler and less expensive than other Wireless Personal Area Networks (WPAN) standards, such as Bluetooth and IrDA. The main focus of the ZigBee standard is applications that require low data rate, long battery life and security.

The main difference between ZigBee and other WPAN definitions is the kind of devices that can be deployed in the network, namely: Full Function Devices (FFD) and Reduced Function Device (RFD). An FFD can receive and send messages over the 802.15.4, whereas an RFD is usually a sensor which sleeps most of the time and only wakes up in order to send messages.

Being based on the IEEE 802.15.4 standard [4], ZigBee shares its low level layers specification, defined as the physical (PHY) and the Medium Access Control (MAC) layers. Basically, the former handles the bit rate and communication channel whereas the latter handles the access to the physical radio channel, manages the radio synchronization and provides

Option	Joiner required information	Description
1	No keys pre-configured	Master, Link or Network Key are transmitted unencrypted Over The Air (OTA)
2	Active Network Key	Since the device has joined the network, the active Network Key should not change.
3	Trust Center address and Link Key	The secure connection is built using the Link Key and the address between Trust Center and the End Device. Then the Network Key is sent securely from the Trust Center.
4	Trust Center Address and Master Key	The Link Key for the device is generated using the Master Key. The Network key is sent securely from the Trust Center

TABLE I
TRUST CENTER AUTHENTICATION CONFIGURATION OPTIONS

a reliable link between two nodes. As far as security is concerned, ZigBee shares the basic capabilities defined in IEEE 802.15.4, which operate at the MAC layer [5]. Unfortunately, these capabilities are partially constrained by the diverse range of potential applications which must be supported. They basically consist of maintaining an access control list (ACL) and using the Advanced Encryption Standard (AES) [6] to protect frame transmissions. Furthermore, both services are only optional and the IEEE 802.15.4 standard does not include key management and device authentication schemes, relying on final security policies defined by the higher layers.

However, the 802.15.4/ZigBee specification defines some particular additional security capabilities to avoid potential vulnerabilities such as message interception, modification and fabrication, as well as interruption of communication. The last specification of ZigBee at this date, redacted in 2007, defines two special security modes: Standard Security and High Security. The former is used in ordinary applications, while the latter, which is implemented in ZigBee PRO, provides higher security mechanisms at a cost in the demand on device resources. A general overview of such security features in ZigBee follows. Nevertheless, a more detailed description may be found in [7].

1) ZigBee Keys: ZigBee devices establish secure communications over the network by protecting messages through using symmetric keys. It should mention that the communication in the Standard Security mode in ZigBee is secured thought the Network Key, which is shared among all devices in the network, while the communication in High Security mode in ZigBee PRO is secured through employing three different keys: Link Key, Master Key, and Network Key. The Link Key is a 128 bit key that is shared between two nodes and is applied for securing unicast communications. The generation of the Link Keys is made using the Master Key, which is pre-installed at the factory, added by the final user in an out-of-band manner or sent from a Trust Center, a special device which other devices trust for the distribution of security keys. The Network Key is a 128 bit long key that is shared between devices in the network and is used to secure the broadcast communications.

2) Key Exchange: Symmetric-key Key Exchange (SKKE) is a new security mechanism in ZigBee PRO which is used to periodically update the Link Key. SKKE employs the Master Key to initialize a secure exchange, increasing the system's security.

3) Additional Security Layers: ZigBee basically provides security services at three different layers, MAC, Network (NWK) and Application Support (APS), in contrast with vanilla IEEE 802.15.4. On one hand, the NWK layer routes frames to their destination and discovers and maintains the routing table. On the other hand, the APS layer acts as an extension of the Application (APP) layer, which provides services to users, defines the role of devices and manages data reassembly.

At the MAC layer, ZigBee provides additional security to single hop messages using the AES encryption algorithm.

At the NWK layer, the Link and Network Keys are used to also provide privacy using AES encryption. Additionally, data integrity is also provided using a Message Integrity Code (MIC) security schema.

Finally, the APS sublayer performs the security functions of the APP layer. This security function is based on the Link and Network Keys. The APS sublayer adds an auxiliary header for carrying security information. At the APS layer, a MIC is also applied to determine the level of data integrity.

4) Network Join Mechanism: ZigBee defines three types of devices: ZigBee Coordinator (ZC), ZigBee Router (ZR), and ZigBee End Device (ZED). A ZC will initiate the network and accept join requests originating from ZRs or ZEDs. Only a ZC or other ZRs which already have joined the network can accept join requests and forward packets [8]. Joining and identifying each device to the network is a very important step. Once a device has joined the ZigBee network, before communications begin, a message is sent to the ZC or a Trust Center. At this stage, a decision is made about whether the device is authorized to join the network or not. This decision is based on the type of key and the configuration of the Trust Center [9]. As it is addressed in Table I there are four options to configure the Trust Center in ZigBee PRO, whereas only the two first options are available for the Trust Center configuration in ZigBee standard.

III. ZIGBEE SECURITY ASSESSMENT

In this section, we analyze the current capabilities of the ZigBee standard in order to assess the security level currently provided by the platform. We categorize the existing

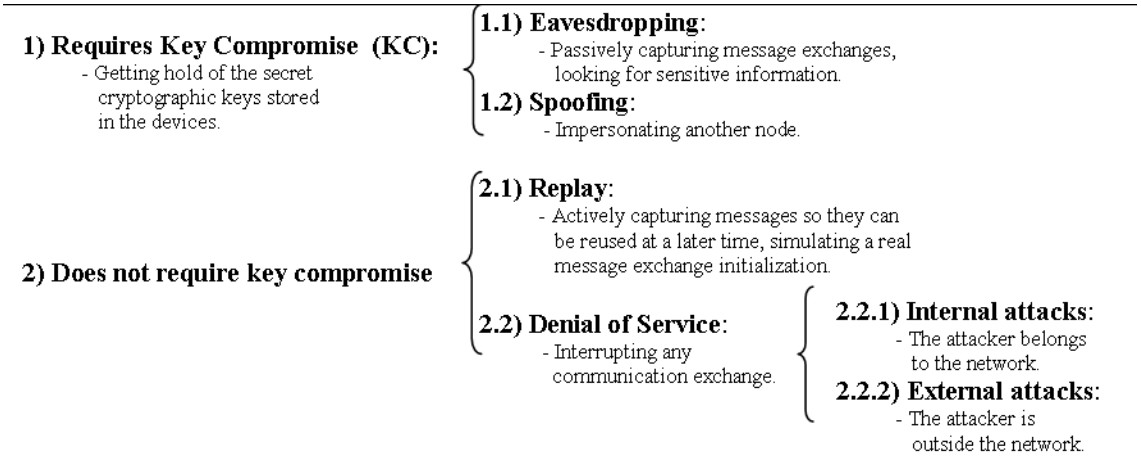

Fig. 1. Attack categories

vulnerabilities according to the following factors: constraints on performing a successful attack and the kind of disruption an attack may cause on the network. From our analysis, the existing vulnerabilities can be divided in two main categories: those which require knowledge of the ZigBee cryptographic keys (Link, Master or Network), and those which do not. Depending on this fact, the set of sub-scenarios varies, as shown in Figure 1.

A. Attacks Requiring Key Compromise

All unicast communications between ZigBee nodes are secured using a 128 bit Link Key shared between two devices at the APS layer. All broadcast communications are secured by a 128 bit Network Key shared among all devices in the network layer [9]. Therefore, a compromised key is a very important issue as far as security is concerned. Once an attacker gets hold of a key, he will be able to act at leisure within the network.

An attacker can obtain the Network Key through different methods such as remote attack or a physical attac [10]. In the former case, this feat may be achieved by intercepting the key during the out-of-band transmission or capturing plain text traffic sent from a ZigBee Coordinator. In the latter case, the physical device is stolen, extracting the information directly from its hardware.

Remote attacks rely on message interception and exploiting the out-of-band exchange key mechanisms, which may be executed through a social engineering attack. Hence, we focus on the much more complex physical attack rather than focus on the remote attack.

Physical attacks are feasible by dumping device firmware using existing available hardware [11]. ZigBee chips, typified by the CC2430 evaluation board from Texas Instruments, are vulnerable to local key extraction. Currently, there is no protection against an external access which tries to steal keys using unprotected data memory and exploiting flash memory.

Specifically, it is possible to attack micro-controllers and ZigBee radios by exploiting their Pseudo-Random Number Generator (PRNG). This attack is called *side-channel timing attack*, which is an attack against the MSP430 micro-controller by exploiting and programming of Joint Test Action Group (JTAG), a 4-wire Test Access Port (TAP) controller or a serial bootstrap loader (BSL) which resides in masked ROM [12]. The MSP430 is a low-power micro-controller popular in ZigBee/802.15.4 and found in many wireless sensor development kits.

The PRNG uses a 16-bit Linear Feedback Shift Register (LFSR), as shown in Figure 2, which can be advanced by writing to the RaNDom High (RNDH) register or overwritten by writing to the RaNDom Low (RNDL) register, to generate pseudorandom numbers. RNDH and RNDL are the High and Low bytes in a 16-bit Cyclic Redundancy Check (CRC) of the LFSR, used to calculate the CRC value of a sequence of bytes and read the 16-bit shift register in the LFSR. In other words, the 802.15.4 Low radio frequency randomizes the seed by mixing 32 values into the Random Number Generation (RNG), for i 0 to 8. Once the RNG has been seeded, it has an initially random 16-bit state [4].

This random number can be read by the CPU and used to generate random cryptographic keys. In fact, the state of this random number is initialized in the Hardware Abstraction Library (HAL) by feeding 32 bytes from the Analog Digital Converter (ADC), a device that converts continuous signals to discrete digital ones, into the RNDH register. The random values generated by the ADC are read from the Radio Frequency (RF) registers ADCTSTH and ADCTSTL, which correspond to ADC test high and low, respectively. Unfortunately, bytes from the ADCTSTH register are physically random, but poorly distributed [4]. This problem in ADCTSH has been inherited from one of the flaws in the PRNG.

There are two flaws in the PRNG: the pool is extremely small (16 bits) and it is not seeded with very much entropy. The first flaw is that the PRNG is not cryptographically secure because the pool is extremely small (16 bits). Nevertheless, even if the pool was much larger, it is still vulnerable because the LFSR is not a cryptographically-secure PRNG and attacker

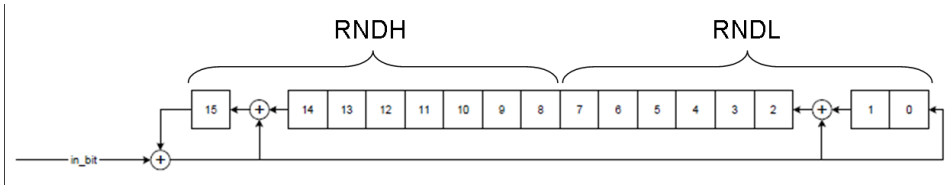

Fig. 2. The Random Number Generator structure

can recreate the LFSR taps and then generate any future sequence from it. The second problem is that it is seeded from a random source that has very little entropy. This could be exploited even if it was used in a cryptographically-secure PRNG. These problems are enough to make the system trivially insecure to a simple brute-force attack [13].

In order to prove both flaws in the PRNG, a dumping of a random byte sequence from the ZigBee evaluation was developed by Travis Goodspeed through employing GoodFET to debug the chip. GoodFET is an open-source Joint Test Action Group (JTAG) interface adapter [12]. It is based upon the TI MSP430 micro-controller and is provided with a USB bus adapter. The firmware was compiled with the Small Device C Compiler and flashed by the GoodFET. A quick Python script is then used by the GoodFET library to debug the target micro-controller and dump random values through the JTAG interface [13].

As a result, it was found that by exploiting the PRNG through its flaws and access to LFSR, which does not have high entropy, obtaining the key stored in the MSP430 micro-controller of ZigBee devices is achievable. From this security test, it may be concluded that it is feasible, even though not necessarily easy, to crack the cryptographic keystores in individual ZigBee devices. Once an attacker has gained hold of the cryptographic keys, he can easily perform eavesdropping and spoofing attacks.

1) Eavesdropping: In ZigBee, broadcast messages are encrypted using the Network Key, which is shared between all the devices in the network. Unfortunately, it is only necessary to compromise a single device in the network for the attacker to be able to compromise the entire network. By using this key the attacker is able to capture the content of broadcast messages in the network, and thus, this is one of the most important vulnerabilities in the ZigBee technology. This is a feasible feat, since an adversary may obtain the cryptographic keys remotely or physically, as mentioned in SectionIII-A.

In contrast, unicast communications are secured by an unique Link Key shared between two devices in the network. This means, if a device of the network is compromised by physical attack, an attacker is able to capture the content of all the direct unicast communication of the device.

In order to address this problem, a mechanism to protect the key exchange must be used. Also, the physical security of devices would be necessary to prevent this attack.

2) Spoofing: This attack is based on the same vulnerability mentioned in the previous one: all broadcast messages are encrypted using the same key, the Network Key. This allows attackers to impersonate the identity of any node in the broadcast messages, since there is no authentication check. Since this vulnerability only applies to broadcast messages, the risk of this vulnerability depends on the amount of broadcast data sent by each application.

In order to address this problem, a mechanism to secure the broadcast communications by enforcing an authentication process is proposed in [14], by using a modified one-way signature.

B. Attacks With Unrequired Key Compromise

Attacks which do not require for an attacker to gain access to the cryptographic keys stored in a ZigBee device are a bigger concern, since they can be performed remotely from the wireless space. It is not necessary to manipulate physical devices. The two existing main attacks which follow this condition are Replay and Denial of Service (DoS).

1) Replay attack: This kind of attack can apply to many applications. For example, in a server room where the temperature is controlled by ZigBee sensor and the data changed is only +1 or -1 degrees. By executing replay attack, the temperature can be changed by an adversary. It means, if an attacker, who implemented the Replay attack, sniff the sent packet from the ZigBee device to the Air Conditioning and replay it n-times, the temperature is added or decreased by n-degrees. This incorrect temperature can cause damage to servers.

ZigBee technology provides one mechanism to avoid replay attacks [15], called the *Frame Counter*, which has been added to the frame header at the Network layer. It consists of a counter that is employed in each transmission and is supposed to detect replicate data. Nevertheless, a replay attack has been successfully executed by Joshua Wright, a senior security analyst from InGuardian [16]. As he mentioned: ”802.15.4 has no replay protection and ZigBee has meager replay protection” and ”An attacker can replay any previously observed traffic until key rotation”.

In fact, at the moment, Joshua Wright is working in KillerBee, an open source collection of python tools intended for testing the security of ZigBee networks. One of this tools is *zbreplay*, that produces a straightforward and unintelligent

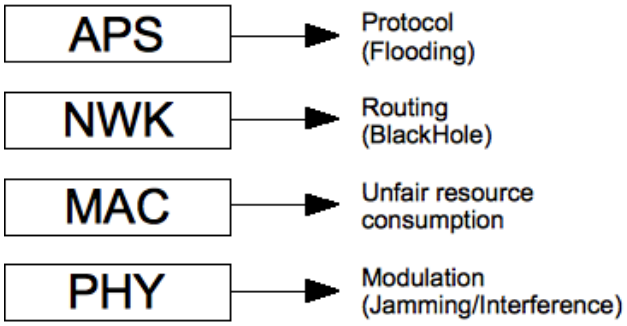

Fig. 3. Denial of Service attack

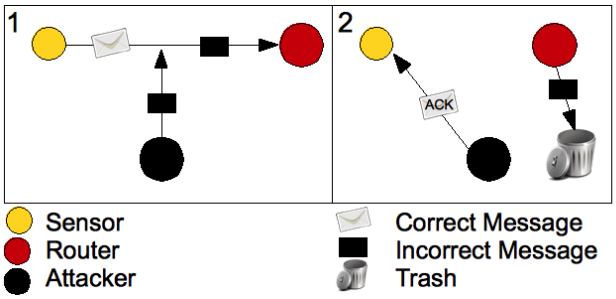

Fig. 4. ACK-MAC layer attack

replay attack from stored data streams.

2) DoS: A great deal of effort has been done by the ZigBee Alliance to be able to perform authentication and provide confidentiality to transmitted data. However, no effort has been done to avoid Denial of Service (DoS) attacks. This attack can be performed at several layers and depends on whether the attacker has joined the network, being part of it (an insider) or not (an outsider). [17], [18].

If the attacker is an insider, the DoS attack may be conducted at the PHY/MAC/NWK/APS layers, whereas if the attacker is an ousider, DoS may only be conducted at the PHY/MAC layers. Figure 3 classifies all possible DoS attack according to each layer.

The possibility to perform the DoS attack at several layers is important because more complex attacks will be more difficult to detecte, as an attacker always intends to be invisible.

Insider Attacks:

At the *APS* layer, DoS is performed by sending a great deal of messages to the device (flooding) 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 an 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.

Outsider Attacks:

At the *MAC* layer, ZigBee uses CSMA/CA [10] (if it is running in non-beacon mode) 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.

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 [18], [19]. This is since the transmitted signal loses energy as the distance increases. An algorithm to avoid the jamming attack has been proposed in [17].

Additionally, the MAC layer may also be interfered using an ACK attack, an optimized DoS attack that more difficult to be detected. Since ZigBee is built over the IEEE 802.15.4 stack, some of its vulnerabilities has been inherited. In ZigBee, the sender has the option to activate ACK by setting a flag inside of each message sent. If this flag is set, the receiver sends a new message containing an ACK answer. However, this message is not authenticated, so anyone may respond with an ACK message [20], [21]. The 802.15.4/ZigBee specification does not provide integrity and confidentiality protection for acknowledgment packets [21].

The scenario is shown in figure 4. There are three devices: the sensor (sender), the router (receiver) and an external device (attacker). (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.

IV. Conclusions

As ZigBee technology is generating significant interest in the industry area. Therefore, the security of this standard becomes extremely important in its successful deployment.

In this paper, we presented a survey of the existing vulnerabilities in the security services available in ZigBee. From our analysis, it has been identified that ZigBee is still vulnerable to some attacks, specially those related to capturing its cryptographic keys. The MSP430 micro-controller from TI is still vulnerable to key theft because of unprotected data memory. Based on these vulnerabilities, some attacks such as eavesdropping, spoofing are feasible. It can also be concluded that, even when keys are not compromised, some attacks are still possible, such as replay and DoS attacks at different layers.

Further research will include developing and implementing new mechanisms to protect against the different attacks analyzed in this paper. To avoid Eavesdropping and Spoofing attacks, secure distribution of the keys, physical security of devices as well as authentication and confidentiality in broadcast communications should be implemented. Additionally, even though a protection for frame freshness exists in the ZigBee standard, we plan on improving this schema to protect this technology against Replay attacks.

ACKNOWLEDGEMENTS

This work has been supported by the Spanish Ministry of Science and Innovation, the FEDER funds under the grants TSI2007-65406-C03-03 E-AEGIS, CONSOLIDER-INGENIO CSD2007-00004 ARES.

REFERENCES

[1] ZigBee Alliance, "ZigBee specification", 2007.
[2] IEEE 802.11, "Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications", 1999.
[3] Junqi Zhang and Vijay Varadharajan, "A new security scheme for Wireless Sensor Networks", in *GLOBECOM*, 2008, pp. 128–132.
[4] IEEE, "IEEE 802.15.4-2006 IEEE standard for information technology– telecommunications and information exchange between systems–local and metropolitan area networks– specific requirements part 15.4: Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)", 2006.
[5] Yang Xiao, Hsiao-Hwa Chen, Bo Sun, Ruhai Wang, and Sakshi Sethi, "MAC security and security overhead analysis in the IEEE 802.15.4 Wireless Sensor Networks", *EURASIP Journal on Wireless Communications and Networking*, vol. 2006, pp. 1–12, 2006.
[6] "NIST. AES: Advanced Encryption Standard", http://csrc.nist.gov/CryptoToolkit/aes/.
[7] Paolo Baronti, Prashant Pillai, Vince W. C. Chook, Stefano Chessa, Alberto Gotta, and Y. Fun Hu, "Wireless Sensor Networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", *Computer Communications*, vol. 30, no. 7, pp. 1655–1695, 2007.
[8] Tian-Wen Song and Chu-Sing Yang, "A connectivity improving mechanism for ZigBee Wireless Sensor Networks", *Embedded and Ubiquitous Computing, IEEE/IFIP International Conference on*, vol. 2, pp. 495 – 500, 2008.
[9] Kyunghwa Lee, Joohyun Lee, Bongduk Zhang, Jaeho Kim, and Yongtae Shin, "An enhanced Trust Center based authentication in ZigBee networks", in *Advances in Information Security and Assurance*, pp. 471–484. SpringerLink, 2009.
[10] "Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications", 1999.
[11] Joshua Wright, "Will hack for sushi - hacking and defending wireless", http://www.willhackforsushi.com/, 2009.
[12] Travis Goodspeed, "Extracting keys from second generation ZigBee chips", in *Black hat*, 2009.
[13] Nate Lawson, "Smart meter crypto flaw worse than thought", http://rdist.root.org/2010/01/11/smart-meter-crypto-flaw-worse-than-thought/, 2010.
[14] Ji-Tsong Shieh and Li chun Ko, "Implementation of a broadcast authentication mechanism in ZigBee", in *The 2nd Workshop on Wireless, Ad Hoc, and Sensor Networks (WASN)*, August 10, 2006 2006.
[15] ZigBee Alliance, "Understanding ZigBee RF4CE", July 2009 2009.
[16] Joshua Wright, "KillerBee: Practical ZigBee exploitation framework", in *ToorCon*, 2009.
[17] Rajani Muraleedharan and Lisa Ann Osadciw, "Jamming attack detection and countermeasures in Wireless Sensor Network using ant system", in *Proceedings of the SPIE*, Monday 17 April 2006 2006, vol. 6248.
[18] Peter Egli, "Susceptibility of wireless devices to denial of service attacks", Technical white paper, Netmodule AG, 2006.
[19] Jacob Brodsy and 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.
[20] Radosveta Sokullu, Ilker Korkmazy, Orhan Dagdevirenz, Anelia Mitsevax, and Neeli R.Prasad, "An investigation on IEEE 802.15.4 MAC layer attacks", in *Proceedings of The 10th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2007*, 2007.
[21] Naveen Sastry and David Wagner, "Security considerations for IEEE 802.15.4 networks", in *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*, New York, NY, USA, 2004, pp. 32–42, ACM.