Attack Vectors to Wireless ZigBee Network Communications - Analysis and Countermeasures

J.Markert[1], M.Massoth[2], K-P.Fischer-Hellmann[2], S.M.Furnell[1] and C.Bolan[1]

[1]Plymouth University, [2]Hochschule Darmstadt - University of Applied Sciences
e-mail: jurgen.markert@plymouth.ac.uk

Abstract

New communication technologies offer new opportunities for developers. Yet, they also bear new risks through potential attacks by an intruder. The purpose of this paper is to present the current state of work in the area concerning the security of wireless sensor networks, especially when using ZigBee standard communication protocols. The major findings from research on recent literature on the subject regard the improvement of the security features of these networks, based upon formal specification, simulation and tests. Another trend pursues the development of methods to detect intrusions or intrusion attempts conducted by an attacker against the wireless sensor network. Very little research has been done so far in the development of honeypots which offer analysis opportunities on specific attacks and interceptions of ZigBee networks. Honeypots are ideal for devising appropriate countermeasures.

Keywords

Wireless Sensor Network, ZigBee, Intrusion Detection System, Honeypot

1. Introduction

A new de facto standard has been established over the course of the last ten years to address the expected need for measurement solutions using wireless communications in the low and medium range of 30 meters and beyond. ZigBee has been designed on top of IEEE 802.15.4 to offer manufacturers all over the world a reliable standard for the upcoming need for team play functionality (IEEE 2006). Around a dozen of manufacturing companies worked together on the ZigBee drafts in order to establish a common operational platform for future technologies using low power communications in star and mesh networks (ZigBee-Alliance 2008).

There are some ZigBee-featured products already present in the market. Such solutions are already present in home automation, in home entertainment and in buildings for monitoring purposes. These wireless sensors would all communicate among each other directly or relayed over peered communication.

Whenever such a network is supposed to be established, it is necessary to deploy a larger amount of nodes than minimally required as a good practice to ensure a higher reliability of communication and interaction through redundancy (Cai et al. 2011). Such redundancies might be needed for several reasons: some of the nodes might run

out of batteries sooner than others, the signal strength of neighbouring nodes has deteriorated, other wireless communications are taking place on the frequency, interfering with the sensor network, natural radio activity has increased within a period of time (higher ambient noise), and stability of the network.

2. Motivation

ZigBee PRO 2007 defines mechanisms for authentication, encryption and trust centre functions on selected main components of the wireless net (ZigBee-Alliance 2008). But due to the increased computational effort and a higher amount of data transmitted, these improvements result in a higher power consumption.

The design of Wireless Sensor Networks relies on low power consumption through low computational need as well as a low power drain though low transmission powers. Any security mechanisms in these networks should therefore be lightweight. Researchers have focused on lightweight securing mechanisms to address this fundamental need for security together with power saving features.

It should be noted that there are several new attacks and ideas by developers regarding security flaws in the ZigBee field. The KillerBee API (Wright 2009) is a simple but powerful tool, and it is easy to build add ons on top of it. The KillerBee API and the tools provide a basis for further development. Results may be given back to the community. 15dot4 is a tool to listen to ZigBee and 802.15.4 communication (15dot4 project 2011), it provides an input device for the well known network monitoring tool Wireshark (Wireshark project 2011) to monitor and capture the network traffic in realtime. Both tools feature usage with state of the art development kits, e.g. the AVR Raven (AVR Raven 2008) and might be ported to other platforms.

Free projects like the Freakduino (Freakduino project 2011) make it easy to build ZigBee components based on the free development-kit Arduino (Arduino project 2006). These kits are cheap and powerful tools to work with, bringing ZigBee technology to everybody interested in working with and doing research on the technology.

3. Threats and attacks

Network communication, be it wired or wireless, always bears security flaws that must be dealt with. Several threats arise whenever a network is established. Developers are asked to protect communication in order to attain the classic information security requirements: confidentiality, integrity and availability.

As we have already seen in the design and implementation of the common wireless networks IEEE 802.11a/b/g/n, there is a need to provide security and reliability, in order to prevent data loss. The authentication and preservation of the integrity of data is a requirement in wireless data communication (Masica 2007).

3.1. Eavesdropping

Whenever a wireless communication is established, there is a way to eavesdrop and listen to the transmitted content (Cunha 2007) or to interfere with the communication by concurrently sending data on the same medium (DePetrillo 2009).

3.2. Obtaining Keys

The initial assignment and distribution of encryption keys in a sensor network is very peculiar. The keys in ZigBee networks can be assigned before placing the nodes. The keys can also be modified over the air (so called "over the air programming" OTAP) (Das 2009). Actual research states that it is possible to eavesdrop the key distribution in plain text, depending on the chosen implementation (Masica 2007).

3.3. Redirecting Communication

It is possible to redirect streams of data in a local area network in order to eavesdrop as an attacker, these techniques can also be used to launch a man-in-the-middle attack with the intent of intercepting or changing the transmitted data. An API has been written by Wright (2009) as a tool to effectively implement attacks to ZigBee networks.

3.4. Replay-Attacks

It has been researched how networks react to replay-attacks. In such a scenario, an outside party re-sends captured packets which had been previously transmitted in a network (Wright 2009). A variation is the so called “Garbage-Attack”, where a network is flooded with garbage data originating from a packet generator. This could also be done to test the reliability of a ZigBee network by applying advanced testing methods.

3.5. Summary

Unencrypted wireless networks can be attacked with the intent of compromising their confidentiality by applying the following techniques: sniffing (Cunha 2007) and man-in-the-middle attacks (BSI 2006),(Yüksel et al. 2008).

The integrity in ZigBee networks is targeted by e.g.:man-in-the-middle attacks and replay-attacks, but the nodes could also be compromised by a firmware-modification/replacement (Cai et al. 2011),(Goodspeed 2007a),(Goodspeed 2007b),(Großschädl 2006),(Gu & Noorani 2008),(Yang et al. 2008).

Availability is a problem in unencrypted wireless networks through: replay-attacks, flooding, denial of service attacks and selective forwarding (Deng et al. 2005),(Raymond & Midkiff 2008),(Karlof & Wagner 2003). Modifications to the devices and its firmware can also interfere with the availability.

Several concerns on security were targeted by the final release of ZigBee PRO in 2007 (ZigBee-Alliance 2008). Improvements were made regarding encryption and authentication and were added to the standard to address the threats (Yüksel et al. 2008).

4. Improvements

ZigBee PRO 2007 defines security mechanisms for authentication, encryption and trust centre functions.

The process of protecting a network from a successful attack is reachable by a process called hardening. It is the improvement of a technology with the reduction of attack vectors. This can for instance also be achieved with the application of methods for encryption. The intention is the improvement of the reliability and availability.

4.1. Encryption

The currently valid ZigBee-2007 standard requires, that AES 128-bit encryption (FIPS 2001) has to be provided with new hardware in order to comply with the ZigBee specification. The strength of the implementations of vendors may differ, especially regarding the protection of the shared secrets. It is assumed that AES-128 is currently unbreakable, but its implementation in hardware might contain flaws (Masica 2007).

Some possible research on these attack scenarios might focus on the challenge of extracting the encryption keys from the hardware by using off-the-shelf hardware or custom tools (DePetrillo 2009).

4.2. Network key distribution

Several problems were solved according to research conducted since the release of ZigBee PRO 2007, but a few problems remain. A flaw in the key distribution algorithm of ZigBee 2007 was formally proven in a publication by Yüksel et al. (2010).

A man-in-the-middle attack is a supplemental method for obtaining a network key to that of eavesdropping on the channel. The intended purpose of this approach is the acquisition or modification of a key. The possession of such a key enables further attacks. This would offer new ways of effectively exploiting the network. The modification of a valid network key of one node would probably lead to the loss of this node for the operator, rendering it unusable (Wright 2009).

4.3. Configuration

There are already guidelines for manufacturers regarding the many possibilities in the configuration and in the design of ZigBee networks. These have been written in part by governmental research departments. A document (BSI 2006) by the German

BSI (German governmental institute for standards and best practices in network security) discusses possible problems in ZigBee installations and provides advice for minimal requirements for the development of new products using ZigBee networks.

In a survey by Chen et al. 2009 around one-hundred references to security related research is presented (Chen et al. 2009). The most of them focus on the improvement of security in wireless sensor networks.

One out of the statements of the authors is very worth mentioning, they propose more research in the area of detection mechanisms, together with research in the area of corresponding countermeasures with the detection of an attack.

The intrusion detection shall be as early as possible, due to the fact, that an attacker will continue the work on the system until an attack is successful. Ignoring an attack completely is in general not advisable. Countermeasures like ignoring a part of the wireless sensor network for the time an attack takes place, helps to save some of the limited amount of battery power.

So the most important fact aside of the improvement of security features is the detection of attacks to the ZigBee network. So called intrusion detection systems (IDS) are well known in wired networks. They analyse network traffic by scanning patterns for anomalies.

5. Intrusion Detection Systems

The existence of various different interpretations of some terms used in this section necessitates their concise definition: An Intrusion Detection System (IDS) is, within the scope of information technology, an application with the purpose of monitoring network traffic for malicious activity. The application of policies leads to the reporting of detected violations to the operator of the system (Misic et al. 2005).

The surveillance of an area with the aid of ZigBee sensors, for example for troop movement observation or for perimeter breach detection is sometimes also called an intrusion detection system (Klues et al. 2005)(Wang et al. 2008). There is currently no known implementation of an available IDS implemented for a ZigBee network in the context of traditional network surveillance. Meshed networks do not have the structure and the associated problems of traditional wired networks (Zhang et al. 2003). An attack on the network is however theoretically possible according to current knowledge, resulting in long-term loss of information. It will remain unknown whether or what information has been compromised in the time before the discovery of an attack (Lee et al. 2008).

Research in the field of wireless LAN has emphasized the need of a technique called honeypot (Yek 2005). The determined reports on honeypots for wireless networks describe tools in a draft and prototype status, these results shall be the basis for a honeypot for ZigBee networks (Siles 2008).

5.1. IDS in ZigBee networks

The idea of an IDS and its proposed features should also be implemented in ZigBee networks. Such a detection entity should span different layers, starting from the physical and MAC layer and reaching up to the high ZigBee layers (Kaplantzis 2006).

A lot of research on this topic has been done before, starting from the detection of intrusion on the low physical layer (Bhuse & Gupta 2005). Bhuse and Gupta propose a detection based on anomalies in signal strength.

The detection of unusual traffic has been extensively researched for wireless LANs. The use of wavelets for fingerprinting normal behaviour compared to unusual traffic has been discussed by Hamdi et al. (2008).

Another proposed method employs a separate IDS which is not part of the network at all. The IDS will only detect a smaller amount of different attacks to the network in this scenario (Bhuse & Gupta 2005). Other research using nodes as part of the network have been proven to achieve a higher detection ratio (Hai et al. 2010).

The discussion by Hai et al. (2010) on the use of a single networking node did not yield satisfactory results in comparison to a single intrusion detection sensor in a wired network. This is due to the possible configuration of ZigBee nodes to form different topologies (Krontiris et al. 2009). These could be a star topology, or a meshed network. In meshed networks, each node in the network has only a few peers to communicate with. A single node can therefore only detect attackers within its direct communication range (Shin et al. 2010). This prevents the detection of attacks in other parts of the network which are not routed through this part of the meshed network. Islam et al. (2010) discuss a solution to this problem in their paper which focusses on hierarchical intrusion detection systems. Their assumed a routed tree topology, and implemented the detection mechanisms in the main routing nodes.

All this information considered as a whole shows that a lot of research has already been done in the field of securing ZigBee networks regarding integrity and confidentiality. Attacks regarding availability still remain a topic of further research.

6. Countermeasures and possible security solutions

The previous section featured possible attacks on ZigBee networks and their countermeasures.

Hardening a system to resist an attack will not stop the attack itself from taking place. It is difficult, if not impossible to prevent novel attack methods against the network.

The challenge presented by such a novel attack lies in the detection of the attack pattern. Only then will it be possible to develop new countermeasures and defence

mechanisms, possibly also leading to a new hardening plan of the whole system. The detection is the job of dedicated network sensors. A typical implementation of such a detection strategy is called a honeypot. A honeypot is a part of the network which appears to an attacker as a valuable point of interest. Yet, the honeypot has only one goal: to attract an attacker with the purpose of collecting information about new attacks on the network and to report the attack.

Our proposal emphasises the development of a ZigBee honeypot. Whenever a honeypot is attacked it records the attack and leads on the attacker to assume that it is actually attacking the initially targeted ZigBee network. This concept requires the detection of malicious parties as well as malicious network traffic (Prathapani et al. 2009).

A paper by Mostara and Navarra (2008) suggests assigning specific roles in wireless honeypots. The roles shall then change over the lifetime of the established network. Some of the nodes are normal routers and forward the traffic, others have sensing functionality and are part of a distributed honeypot. This approach seems to fit well in the context of ZigBee honeypots.

Observed attacks on a network could later also be analysed to devise countermeasures. The reactions may be passive and not interact with the attacker at all. Active reactions on the other hand could include countermeasures like alerting the rest of the network of the detection of an attack and flag a specific part of the network as not trustworthy, which should be ignored for routing purposes. The protecting nodes defend the working network through directed responses upon detection of potential intruders (Das 2009). A list of honeypots is provided by the agents to the clients at the time of network establishment. The clients are forbidden from using the honeypots for networking purposes since connections to these honeypots would be regarded as an attack.

The roles in this network will change over time following a predefined schedule in order to attain a lower false positive intrusion detection rate and to render these networks harder to attack. Kaplantzis (2006) merely describes a conceptual honeypot system without discussing an implementation under real-life conditions. Further development remains to be done. There is still a gap in the research of honeypots for ZigBee Networks.

Literary research on the state of actual research has evidenced the remaining need on these topics. Further research should be done especially in the field of availability of ZigBee networks, regarding honeypots, distributed honeypots and honeynets intended as defence mechanisms.

To be more precise, it is not feasible to blindly adopt features of honeypots for wired networks. The wireless aspect of ZigBee adds a lot of points to ponder. It is not recommended to simply migrate research from WiFi networks and their honeypots to ZigBee networks. There are other layers and protocols implemented in WiFi networks (IP, TCP, ICMP, HTTP). The securing mechanisms (WEP, WPA/WPA2,

SSL/TLS, SSH, IPsec) also differ too much to simply adopt research on honeypots from wireless networks directly to ZigBee networks.

The detection of new attacks and their methods is possible with honeypots. Once attackers engage the honeypots, the functional part of the network will be left with additional time to perform normally while preparing countermeasures. This should increase the reliability and availability, fulfilling the main purpose of honeypots. Unknown attacks can also be found and screened for reporting. The development of new countermeasures will only be possible with the detection of unprecedented attacks. The proposed honeypot concept for ZigBee networks will therefore feature new detection mechanisms and new countermeasures compared to traditional approaches.

The implementation of a honeypot for wireless sensor networks is a new way to deal with new attack scenarios in the field of ZigBee-featured communications. It deals with the expected upcoming increase of research interest in the area of ZigBee network security flaws and could also lead in part to a new kind of intrusion detection system within wireless sensor networks.

7. Summary

The level of security offered by ZigBee, along with its weaknesses, has been explored only in part to the present day. Merely a few people have been doing research in this area at all, and no one has ever adopted honeypot techniques to a ZigBee network. The intended research will explore hitherto unconsidered and unregarded aspects of security threats against ZigBee networks and new defence mechanisms with the use of honeypots for ZigBee.

8. References

15dot4 project, http://sourceforge.net/projects/dot4-tools/, 2010

Arduino project, http://www.arduino.cc, 2006

AVR Raven, http://www.atmel.com/dyn/products/tools_card.asp?tool_id=4291, 2008

Bhuse, V., Gupta, A., “Anomaly Intrusion Detection in Wireless Sensor Networks“, Western Michigan University, 2005

BSI, “Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte”, Bundesamt für Sicherheit in der Informationstechnik, 2006

Cai, H., Jia, X., Sha, M., “Critical Sensor Density for Partial Connectivity in Large Area Wireless Sensor Networks”, ACM, 2011

Chen, X., Makki, K., Yen, K., Pissinou, N., “Sensor Network Security: A Survey”, IEEE Communications Surveys & Tutorials, Vol. 11, 2009

Cunha, A., “On the use of IEEE 802.15.4/ZigBee as federating communication protocols for Wireless Sensor Networks” IPP Hurray Technical Report 1.0, 2007

Das, V.V., "Honeypot Scheme for Distributed Denial-of-Service", International Conference on Advanced Computer Control, 2009

Deng, J., Han, R., Mishra, S., "Defending against path-based DoS attacks in wireless sensor networks", ACM, 2005

DePetrillo, N., "Power Hungry People - Making Sense of New Critical Infrastructure Threats", http://proidea.maszyna.pl/CONFidence09/2/CONFidence2009_nick_de_petrillo.pdf, 2009

Djenouri, D., Badache, N., "A gradual solution to detect selfish nodes in mobile ad hoc networks", Inderscience Publishers, Vol. 4, 2010

Federal Information Processing Standards "Advanced Encryption Standard (AES)", Std. FIPS Pub197, 2001

Freakduino project, http://freaklabs.org/, 2011

Goodspeed, T., "Memory-constrained code injection" http://travisgoodspeed.blogspot.com, 2007

Goodspeed, T., "MSP430 buffer overflow exploit for wireless sensor nodes", http://travisgoodspeed.blogspot.com/, 2007

Großschädl, J., "TinySA: A security architecture for wireless sensor networks", Proceedings of the 2nd International Conference on Emerging Networking Experiments and Technologies, ACM, 2006

Gu, Q., Noorani, R., "Towards self-propagate mal-packets in sensor networks", WiSec '08: Proceedings of the first ACM conference on Wireless network security, ACM, 2008

Hai, T.H., Huh, E.-N., Jo, M., "A lightweight intrusion detection framework for wireless sensor networks", 2010

Hamdi, M., Meddeb-Makhlouf, A., Boudriga, N. "Multilayer Statistical Intrusion Detection in Wireless Networks" Hindawi Publishing Corporation, EURASIP Journal on Advances in Signal Processing, Vol. 2009, 2008

IEEE, Institute of Electrical and Electronics Engineers - IEEE 802.15.4-2006 IEEE Standard, http://standards.ieee.org/getieee802/802.15.html, 2006

Islam, S., Khan, R.H. Bappy, D.M., "A Hierarchical Intrusion Detection System in Wireless Sensor Networks", IJCSNS International Journal of Computer Science and Network Security, Vol.10, 2010

Kaplantzis, S., "Security Models for Wireless Sensor Networks", http://users.monash.edu.au/~skap3/transfer-final-rev.pdf, 2006

Karlof, C., Wagner, D., "Secure routing in wireless sensor networks: attacks and countermeasures", University of California at Berkeley, 2003

Klues, K., Hoffert, J., Orjih, O., "Configuring the IEEE 802.15.4 MAC Layer for Single-sink Wireless Sensor Network Applications", http://sing.stanford.edu/klueska/Black_Site/Publications_files/kluesConfig802154.pdf, 2005

Krontiris, I., Benenson, Z., Giannetsos, T., Freiling, F.C., Dimitriou, T., "Cooperative Intrusion Detection in Wireless Sensor Networks", EWSN, 2009

Lee, G., Lim, J., Kim, D.K., Yang, S. H., Yoon, M. H., “An Approach Mitigating Sybil Attack in Wireless Networks using ZigBee”, http://mobile.ajou.ac.kr/new/pubs/papers/2008/20080724_060856_70276.pdf, 2008

Masica, K., “Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments”, http://csrp.inl.gov/Documents/, 2007

Misic, V. B., Fung, J.,Misic, J., “MAC Layer Security of 802.15.4-Compliant Networks”, http://asc.di.fct.unl.pt/tasd/archivemod3/Misic05.pdf, 2005

Mostarda, L., Navarra, A., “Distributed Intrusion Detection Systems for Enhancing Security in Mobile Wireless Sensor Networks”, International Journal of Distributed Sensor Networks, Vol. 4, 2008

Prathapani, A., Santhananr, L., Agrawal, D.P., “Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks”, University of Cincinnati, 2009

Raymond, D.R., Midkiff, S.F.,"Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", IEEE Pervasive Computing, Vol. 7, 2008

Shin, S., Kwon, T., Jo, G.-Y., Park, Y., Rhy, H, “An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks”, IEEE Transactions on Industrial Informatics, Vol. 6, 2010

Siles, R., “HoneySpot: The Wireless Honeypot - Monitoring the Attacker’s Activities in Wireless Networks”, 2008

Wang, Y., Wang, X., Xie, B., Wang, D., Agrawal, D.P., “Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks” IEEE Transactions on mobile computing, Vol. 7, 2008

Wireshark project, www.wireshark.org, 2011

Wright, J., “Killerbee: Practical ZigBee Exploitation Framework”, http://www.willhackforsushi.com/presentations/toorcon11-wright.pdf, 2009

Yang, Y., Zhu, S., Cao, G., “Improving sensor network immunity under worm attacks: A software diversity approach”, MobiHoc '08: Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2008

Yek, S., “Blackhat fingerprinting of the wired and wireless honeynet”, http://scissec.scis.ecu.edu.au/proceedings/2005/forensics/yek1.pdf, 2005

Yüksel, E., Nielson, H. R., Nielson, F., “ZigBee-2007 Security Essentials”, Informatics and Mathematical Modelling, Technical University of Denmark, 2008

Yüksel, E., Nielson, H. R., Nielson, F., “A Secure Key Establishment Protocol for ZigBeeWireless Sensor Networks”, Oxford University Press, 2010

Zhang, Y., Lee, W., Huang, Y., “Intrusion detection techniques for mobile wireless networks”, http://www.cc.gt.atl.ga.us/~wenke/papers/winet03.pdf, 2003

ZigBee-Alliance, “Latest ZigBee Specification Including the Pro Feature Set”, http://zigbee.org/Products/DownloadZigBeeTechnicalDocuments.aspx, Std. 053 474r17, 2008