Research and Analysis for Vulnerability of ZigBee Communication

sangheon lee, Information & Intelligence System Lab, Sungkyunkwan University  
Juyeon kang, Mobile Electronics Lab, Sungkyunkwan University   
JinHyuck park, Network Computing Lab, Sungkyunkwan University

ZigBee is a proximity network that is widely used in IoT and Smart Grid applications. Like other sensor networks, ZigBee security is also the most important issue. However, ZigBee networks designed for low power and low cost cannot use high security protocols that require many computations. This report shows the vulnerability of ZigBee network through packet analysis of ZigBee and possibility of stealing security information.

KEYWORDS

ZigBee, ZigBee Network, ZigBee Security, Packet Sniffer, Wireless Network

1 INTRODUCTION

Since ZigBee has been known to the world in 2005, low-power, low-cost and wireless mesh networks have become an attractive sensor network for battery-powered products. ZigBee chips typically integrate radio and microcontrollers and have a relatively low latency. ZigBee originally supports star, tree, and mesh networks. Based on the 802.15.4 standard with low battery consumption, ZigBee works and is now being used as the standard for home automation and smart grid.

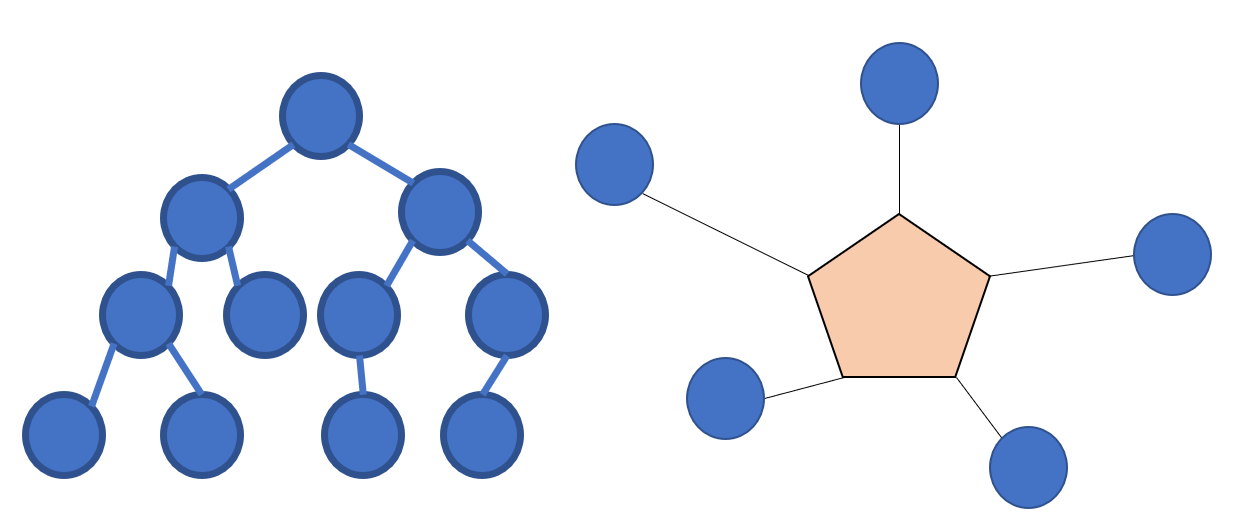


Fig. 1. Structure of Network. Tree(left) and Star(right).

However, ZigBee also has security problems with most wireless communication methods. In the case of general wireless communication, ZigBee, which is designed to operate on low power condition, is too hard to maintain high level security protocol. However, it is difficult to use the above security protocol because of power consumption.

In this paper, we research the configuration and security of ZigBee and analysis the vulnerability of ZigBee security by packet sniffing between ZigBee communication using a ZigBee packet sniffer program. Chapter 2 explains ZigBee and ZigBee network configuration, and Chapter 3 covers ZigBee security. Chapter 4 explains the experiment implemented in this paper, Chapter 5 analyzes the experimental results, and Chapter 6 concludes the paper.

2 ZIGBEE

2.1 ZigBee

ZigBee is an [IEEE 802.15.4](https://en.wikipedia.org/wiki/IEEE_802.15.4)-based [specification](https://en.wikipedia.org/wiki/Specification_(technical_standard)) for a suite of high-level communication protocols. ZigBee use 16 channels in IEEE 802.15.4 and create [personal area networks](https://en.wikipedia.org/wiki/Personal_area_network) with small, low-power [digital radios](https://en.wikipedia.org/wiki/Digital_radio), such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Hence, ZigBee is a low-power, low data rate, and close proximity (i.e., personal area) [wireless ad hoc network](https://en.wikipedia.org/wiki/Wireless_ad_hoc_network).

The technology defined by the ZigBee specification is intended to be simpler and less expensive than other [wireless personal area networks](https://en.wikipedia.org/wiki/Wireless_personal_area_network) (WPANs), such as [Bluetooth](https://en.wikipedia.org/wiki/Bluetooth) or more general wireless networking such as [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi). Applications include wireless light switches, [home energy monitors](https://en.wikipedia.org/wiki/Home_energy_monitor), traffic management systems, and other consumer and industrial equipment that requires short-range low-rate wireless data transfer.

Its low power consumption limits transmission distances to 10–100 meters [line-of-sight](https://en.wikipedia.org/wiki/Line-of-sight_propagation), depending on power output and environmental characteristics.[[1]](https://en.wikipedia.org/wiki/Zigbee#cite_note-specs-1) ZigBee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. ZigBee is typically used in low data rate applications that require long battery life and secure networking (ZigBee networks are secured by 128 bit [symmetric encryption](https://en.wikipedia.org/wiki/Symmetric-key_algorithm) keys.) ZigBee has a defined rate of 250 Kbit/s, best suited for intermittent data transmissions from a sensor or input device.



Fig. 2. ZigBee Module

2.2  ZigBee Network Configuration

ZigBee network consists of ZC (ZigBee Coordinator), ZR (ZigBee Router) and ZED (ZigBee End Device) depending on the role. ZC exists only one in the ZigBee network and is responsible for managing the information on all devices in the network and communicating with other ZigBee networks. ZC uses the FFD (Full-function Device), that can be used in any ZigBee network with all the functions of managing information, controlling the network, and collecting data. ZR is usually FFD, which collects and communicates the data of a small ZED within the ZigBee network. It is less expensive than ZC because it uses less memory due to less functionality. ZED is responsible for measuring and transmitting data to the devices at the bottom of the ZigBee network. ZED uses RFD (Reduced-functioning Device), but RFD has limited performance and can only perform certain roles such as collecting data within ZigBee network or sending data unilaterally. ZED can communicate with ZR or ZC, and because it does not require a large function, it has a merit that it is advantageous for network configuration because the terminal cost is low.[2][3]

The configuration of the ZigBee network is shown in Fig. 3 and the Trust Center (TC), which exists within ZC, is responsible for the management of all devices in the network. The TC manages all the keys on the ZigBee network and updates them regularly. The new key is encrypted and broadcast with the existing key.

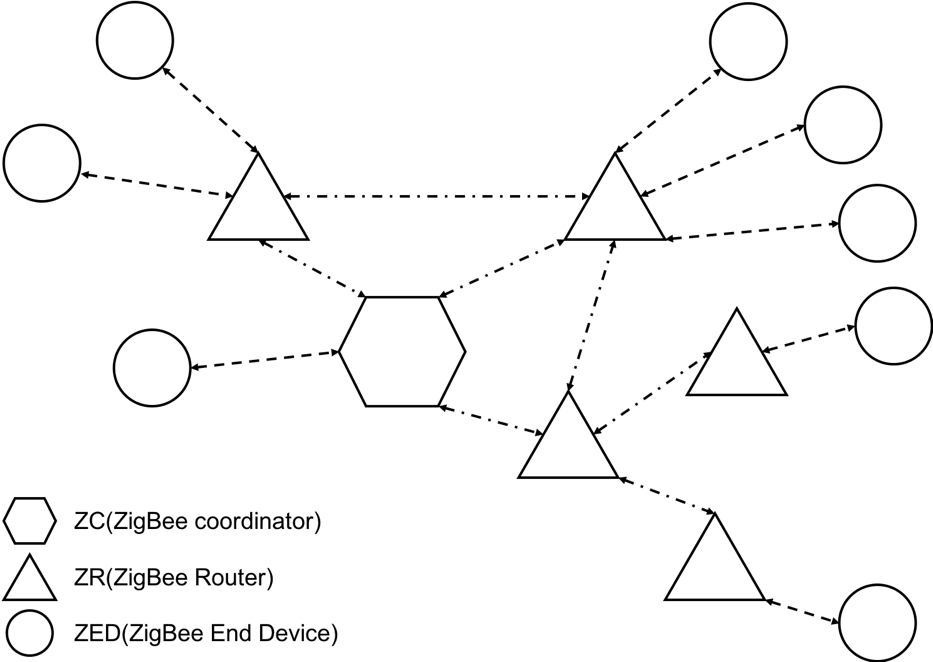


Fig. 3. ZigBee Network

ZigBee is based on the PHY (Physical) layer and the MAC (Medium Access Control) layer, which are two layers defined in 802.15.4 as shown in Fig. 4. In addition, it consists of two ZigBee layers: NWK (Network layer) and APL (Application layer) defined by the ZigBee Alliance.[4]  
 ZigBee runs the application object in this structure. Among ZigBee's layers, APL includes two internal layers that serve as ancillary, one that is ZDO (ZigBee Device Object) and the other is APS (Application Support Sublayer). SSP (Security service providers) that provide security services exist separately and provide security services to APS and NWK.

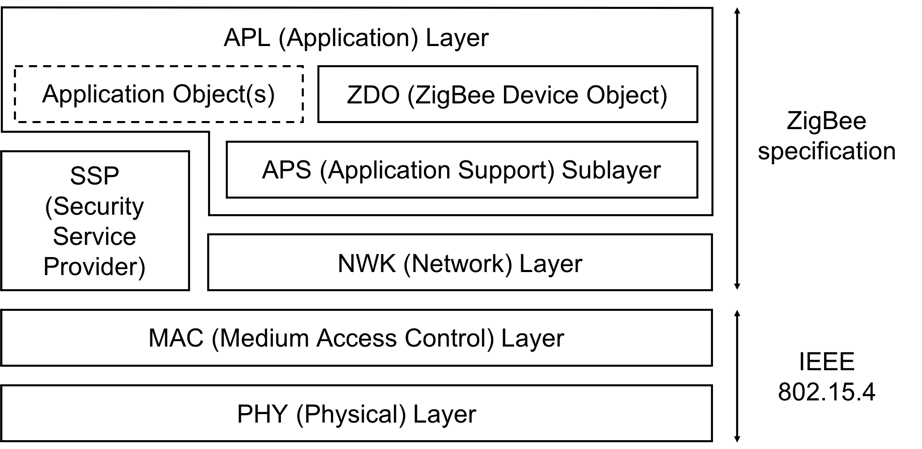


Fig. 4. ZigBee Stack Architecture

Each layer of ZigBee has a different role. First, PHY is a layer that has the basic function of wireless communication. PHY is responsible for transmitting data according to established communication settings.  
Second, MAC is responsible for data transfer between neighboring devices and supports the security services defined in 802.15.4.[5] Third, NWK is responsible for new subscription and address allocation to ZigBee network and routing to transmit frames. Fourth, the APS is responsible for framing the application object and linking it to a lower layer while the program is operating. Fifth, ZDO is responsible for determining information and policies of devices. Finally, the SSP provides security services used within ZigBee. The layer in need of security will be provided with services from the SSP to encrypt its own frame, which will be certified by the APS and ZigBee networks for application objects. As mentioned above, ZigBee has created and installed a relatively efficient security feature, since strong security protocols are not available.

3 ZIGBEE SECURITY

3.1   Security Model

The ZigBee standard supports three security modes: Residential Security Model (RSM), Standard Security Model (SSM) and High Security Model (HSM). Residential security model was first supported in the ZigBee 2006 standard. This level of security requires that a network key be shared among devices. Standard security model adds optional security enhancements over residential security model, including an APS layer link key. High security model adds entity authentication, and other features not widely supported. ZigBee ZB modules primarily support standard security model.

Open Trust Model is used for ZigBee encryption. Open Trust Model is a concept that guarantees reliability between all layers and all programs in each device. Each device guarantees only its own reliability, so it cannot know what encryption process the other device is going through. Since the internal reliability is guaranteed, only the threat in the transmission process to the outside can be considered.

In this basic environment, ZigBee uses the 128-bit symmetric key block cipher (AES-128) to provide encryption of keys and CCM \* algorithm to apply selective services on integrity and confidentiality. The CCM \* algorithm is a technique that provides comprehensive encryption and authentication procedures using 128-bit block encryption. ZigBee uses the AES-CCM \* method, which is an extension of AES-CCM provided by IEEE 802.15.4, and can provide encryption and authentication functions, respectively. It can also provide encryption and authentication functions at one time as needed.

The currently used security mode can be confirmed from the field value of the frame. First, the basic frame structure is shown in Fig. 5.[6]



Fig. 5. ZigBee Frame

When the security mode starts to be used, a supplementary header (Auxiliary Header) or MIC (Message Integrity Code) is added as needed. The reason for using MIC is to guarantee the integrity of header and auxiliary header and payload in each layer without modulation in transmission process. Fig. 6 shows the form of the frame with the content added according to the layer. Above shows NWK frame, and below shows APS frame.[6]

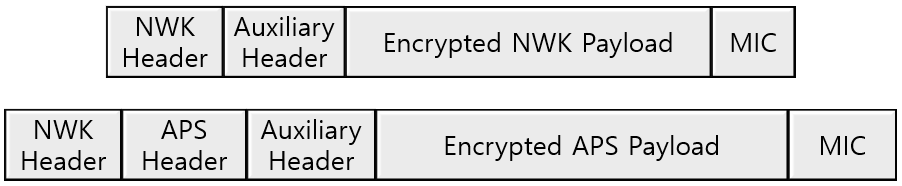


Fig. 6. ZigBee Frame with Auxiliary Header and MIC

3.2   Key configuration

TC maintains and manages the Master key, Link key, and NK, which are the encryption keys in the ZigBee network that it manages.

Master key (MK) acts as a secret key that must be initially shared between two devices in Symmetric Key Establishment Procedure (SKKE) for Link Key Generation. In particular, the key shared between the TC and the node is referred to as TC-MK (Trust Center Master Key), and the key shared between the devices is referred to as AP-MK (Application Layer Master Key).

Link key (LK) is used to encrypt messages sent to unicast between application layers of two devices. In particular, the key shared with TC is called TC-LK (Trust Center Link Key), and the key shared between devices is called AP-LK (Application Layer Link Key).

Network Key is a key for security of NWK, which is shared by all devices in the network. SSNK (Standard Security Network Key), which is the NK used in SSM, is transmitted without encryption, but HSNK (High Security Network Key), which is the NK when operating as HSM, is encrypted and transmitted.

3.3   Key exchange process

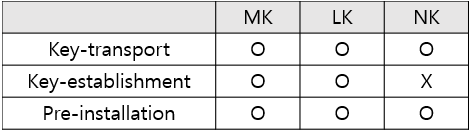
ZigBee devices must perform encryption operations using these three kinds of keys within the set security mode, and each key can be obtained through different methods. There are three ways to get a key in a ZigBee network.

First method is Key-transport, which receives keys from other ZigBee devices (ZC (TC), ZR) using wireless communication. It is the most commonly used method in the network, but if the eavesdropping is done in the delivery process, the key may be exposed, so encryption in the delivery process is required.

Second method is Key-establishment, in which the two devices first verify the mutual authenticity and then generate a new key with the data exchanged in the verification process. Verification of authenticity is performed by using a previously set key, and a new key is calculated by mixing the additional information generated during the verification process. ZigBee uses the method that derive LK using MK.

Third method is Pre-installation, which pre-installs the available keys on the network in the ZigBee device. The key is injected during the production process, or the key is injected by the administrator at the time of installation. In this method, a default key is injected. Table. 1 shows the cases in which each of the keys can be obtained in the methods described above.[7]

Table 1. How to acquire by the key type



3.4   Vulnerability of ZigBee Security

The security architecture of ZigBee has several problems. The most fundamental problem is limited performance. ZigBee environments do not have the strong security mechanisms that currently available. Most devices of ZigBee have very limited performance. Therefore, ZigBee has a limited number of security mechanisms to choose from and is exposed to many threats because it only can be encrypted under a certain level.

Also, there are a total of 16 channels used for communication between ZigBee, and a small number of channels can be a security vulnerability.

4  EXPERIMENTAL ENVIRONMENT AND EXPERIMENT METHOD

To communicate with each ZigBee, the frequency to communicate must be set to the same communication channel using a program called XCTU. XCTU is a free multi-platform application designed to enable developers to interact with Digi RF modules through a simple-to-use graphical interface. It includes new tools that make it easy to set-up, configure and test ZigBee RF modules. When setting ZigBee using XCTU, it is necessary to connect ZigBee module and then set it through Arduino. Fig. 9. Shows the design for connecting the ZigBee module to Arduino. Connect pin 1 of the ZigBee module to the 3.3V pin of the Arduino and pin 2 and pin 3 to the RX pin and TX pin of the Arduino, respectively. Finally, connect pin 10 to GND pin in Arduino then, the ZigBee module is ready configure through Arduino.

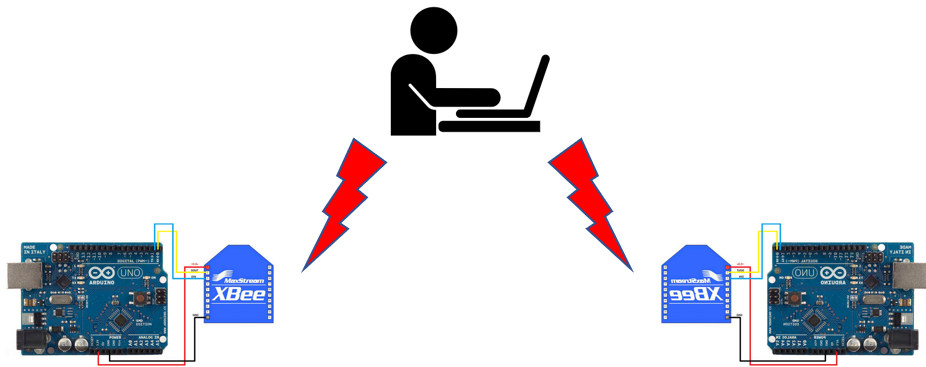


Fig 8. Communication between two ZigBees using XCTU

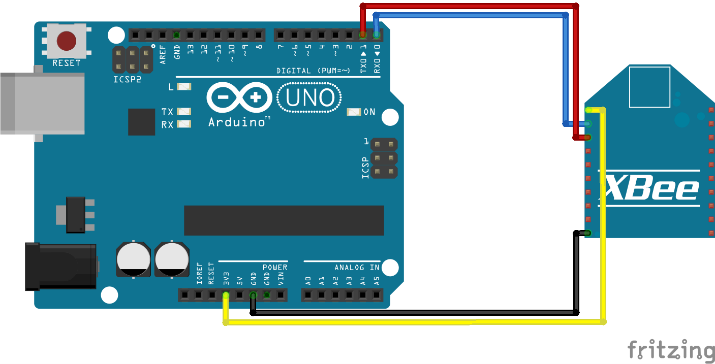


Fig. 9. Schematic for connecting the ZigBee module to the Arduino

Fig. 10. Shows the initial screen when the XCTU program is executed. After connecting the Arduino connected to the ZigBee module, click the + button on the upper right of the screen, and the list of the ZigBee module connected to the current computer is displayed. Click O the ZigBee module you want to configure and will see a screen where can configure the ZigBee module.

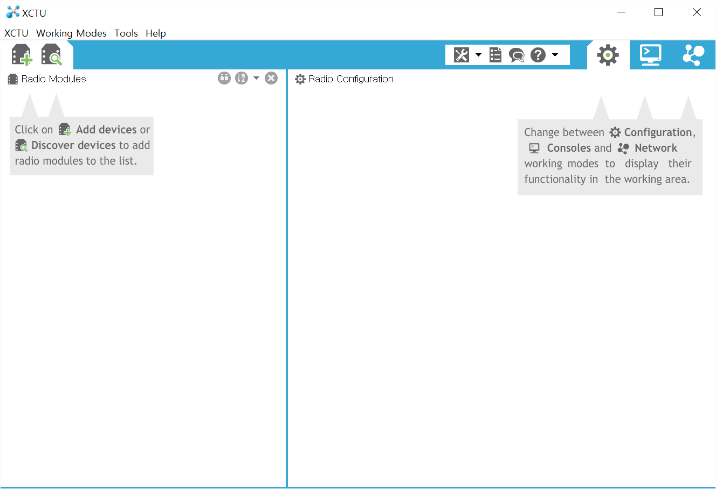


Fig. 10. Initial screen of XCTU

In the setting screen, set the ZigBee channel and the PAN ID to be communicated equally, and set the DH and DL to the same as those of the relative ZigBee SH and SL. Finally, ZigBee is all set to communicate.

5 EVALUATION AND ANALYSIS

To test the security of ZigBee, we constructed the following experimental environment. Using the Arduino UNO with Atmega328, the status of data transmission and reception between two ZigBees is confirmed by the Serial Monitor. Configuration and test utility software, XCTU, was used for ZigBee configuration. Assume that the attacker knows the communication channel between two ZigBees in the middle. We use Sniffer module and Packet Sniffer program to sniff packets between two ZigBees as shown in Fig. 11 and 12. The experimental results are as follows.

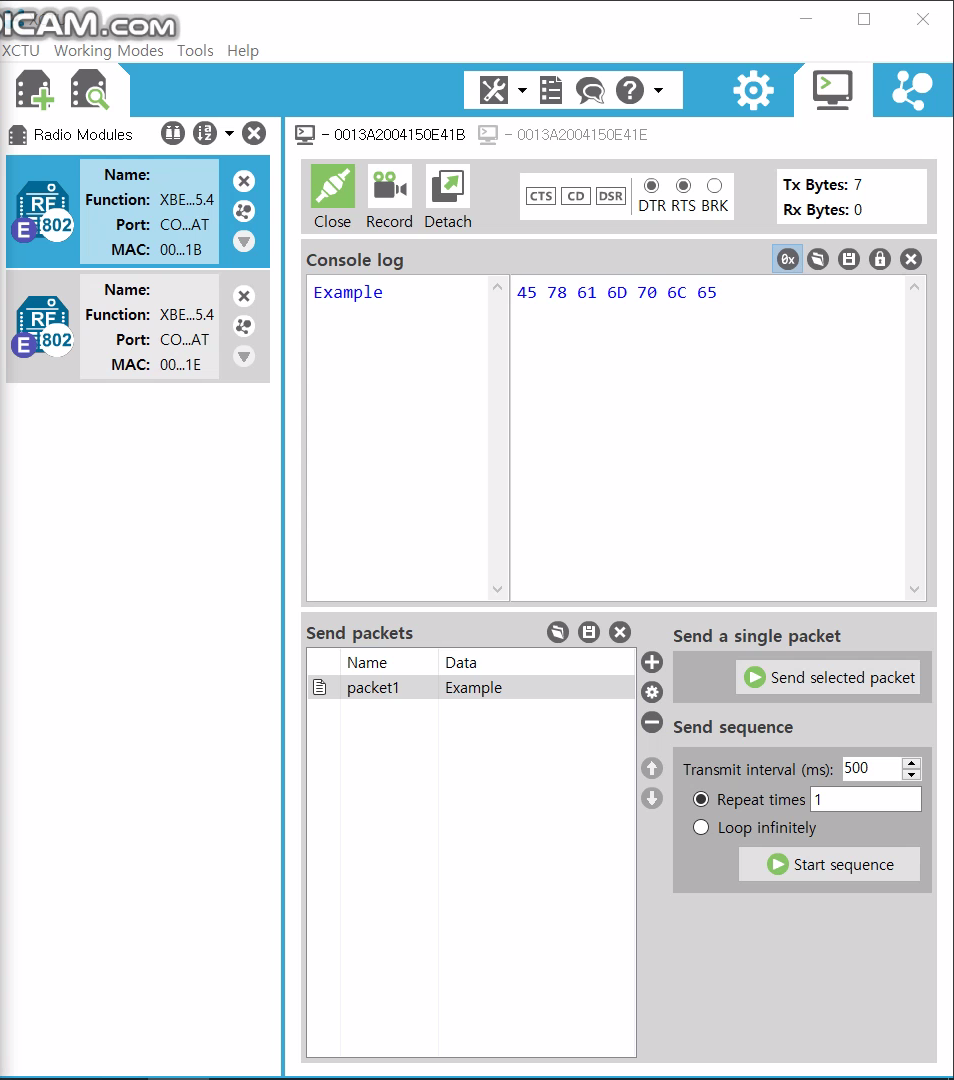


Fig. 11. ZigBee Packet Sniff

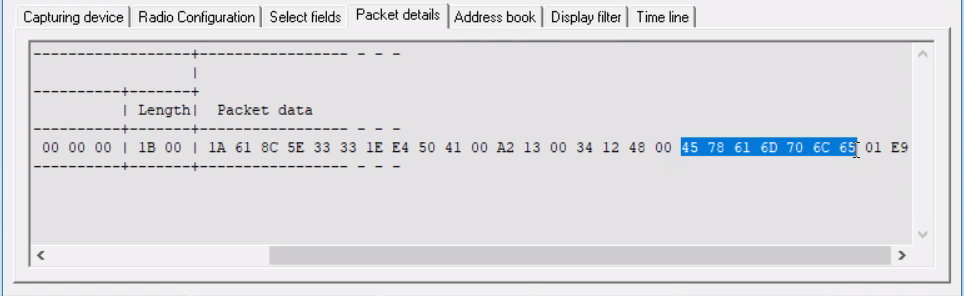


Fig. 12. ZigBee Packet Sniff

Since connecting both ZigBee addresses and channels using XCTU, we can find that the HEX value of the ‘Example’ (45 78 61 6D 70 6C 65) appears in the Sniff program when the data is sent. Knowing only the information of the channels used to communicate between two ZigBees, messages can read with a simple sniffer. Since the number of channels used for ZigBee communication is a total of 16 (from 2405MHz, channel 11 to 2480MHz, channel 26) if the attacker does not know the information of the channel used for communication between two ZigBees, the communication channel information can be easily derived through a brute-force attack.

6 CONCLUSIONS

ZigBee is used in various fields because it has excellent cost and performance according to the construction range among the near range sensor networks. Especially in the smart grid. However, as the risk of hacking of smart grid and the damage caused by hacking are expected recently, security of ZigBee is also becoming a big problem. Because ZigBee runs at low power and low cost, it cannot use highly reliable encryption or security protocols. Therefore, ZigBee needs a cryptographic protocol that can be implemented even at low power.

Also, a total of 16 channels are used for communication between ZigBee, and a small number of channels is a security vulnerability. By using more channels, the attacker must make it difficult for the brute-force attack to find information on the channel.

REFERENCES

|  |  |
| --- | --- |
| [1] | Shahnaz Saleem and Sana Ullah and Kyung Sup Kwak, “A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks", "Sensors 2011- Volume 11", Issue 2, January 2011 |
| [2] | ZigBee Alliance, “ZigBee Specification- r17", part 1.1.4, January 2008. |
| [3] | ZigBee Alliance, “ZigBee Specification- r17", part 1.4, January 2008. |
| [4] | Ender Yüksel and Hanne Riis Nielson and Flemming Nielson, "ZigBee-2007 Security Essentials", "Proceedings of The 13th Nordic Workshop on Secure IT SystemsNordSec 2008", pp. 65-66 , October 2008. |
| [5] | IEEE Std. 802.15.4-2006, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)", IEEE , part 5.4-5.5 , September 2006. |
| [6] | Shahin Farahani, "ZIGBEE WIRELESS NETWORKS AND TRANSCEIVERS", ELSEVIER , part 3.4-3.6 , 2008. |
| [7] | Ender Yüksel and Hanne Riis Nielson and Flemming Nielson, "ZigBee-2007 Security Essentials", "Proceedings of The 13th Nordic Workshop on Secure IT SystemsNordSec 2008", pp. 67-68 , October 2008. |
|  |  |