IoT

Device (ZigBee) Security Study

April 2020

hkpc 生產力局

HKCERT

Disclaimer

The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Productivity Council (HKPC) reserve the right to amend the document from time to time without prior notice.

While we have made every attempt to ensure that the information contained in this document is obtained from reliable sources, HKCERT is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The information contained in this document is intended to provide general information and for reference only. Reliance or use of this information shall be at the reader's own risk. Nothing herein shall to any extent substitute for the independent investigations and the sound technical and business judgment of the reader. In no event will HKCERT, HKPC or its partners, employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on the information in this document, or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Table of Contents

1. Background

Industries all over the world are keeping up with the trend of Internet of Things (IoT), by developing and applying products with built-in IoT-related function. Examples can be found in smart-home facilities, industrial automation and medical automation, etc. Although Wi-Fi and Bluetooth are the common wireless technologies and give good performance, they are power-costly for needing to be attached with batteries with larger capacities or even plugged with A/C electricity when operating.

As a result, achieving low-power consumption is one of the key goals in IoT product development. To this end, wireless technologies with low-power consumption have been deployed such as Bluetooth Low Energy (BLE), LoRa and ZigBee. Among those mentioned, ZigBee has been commonly used for end-user products as the simplicity of the setup makes it more marketable.

Therefore, HKCERT has conducted security testing of some ZigBee devices, aiming to illustrate the relevant security issues arising from the test results and raise the security awareness of ZigBee device developers and general users.

This security study report on ZigBee technologies is to introduce and promote security awareness for developers and general users who are considering to develop IoT devices with ZigBee for wireless communication. The report focuses more on letting the audience well-informed of the ZigBee wireless technology and the security features that are suitable to be incorporated in ZigBee IoT solutions.

2. Study in ZigBee Technology

2.1 Introduction of ZigBee

ZigBee technology is mostly built-in with products that operate with simple actions, for example, motion sensors, temperature detectors, electricity plugs, etc. ZigBee is designed for simple network request and response packets to be transferred to achieve a simple data reading or command action on a ZigBee device. Hence, ZigBee technology has a heavy presence in home appliance, from wireless remote-controlling light bulbs to door locks. Also, it is used in healthcare products, mostly in the form of sensors such as body parameter measuring sensor, etc. While industrial products require high-level operating commands, ZigBee would only be covering up the area of their sensors and switches of the power plug with simple network packets completing the operation of the devices.

2.1.1 Network Architecture in ZigBee

ZigBee is based on the wireless networking standard of IEEE 802.15.4. It is popular in use for in its low power and low data rate as it is basically used for two-way communication between sensors and control systems. ZigBee has a similar communication coverage range as Bluetooth and Wi-Fi, covering up to 100 meters indoor. The major difference is that Bluetooth and Wi-Fi are high data rate communications standards supporting the transfer of complex structure. Also, ZigBee focuses on simple data packets for communication as to obtain a low data rate and low power communication environment. As a result, it is more suitable for an appliance to implement ZigBee network technology when they require low power or long battery life. The table below shows the comparisons of basic technical specifications between ZigBee, Wi-Fi and Bluetooth technologies:

	ZigBee	**Wi-Fi**	**Bluetooth**
Distance Coverage	10-100 meters	50-100 meters	10-100 meters
Network Topology	Ad-hoc, Star, Cluster, and Mesh	Point-to-hub	Ad-hoc, very small networks
Frequency Band	868 MHz, 2.4 GHz	2.4 and 5 GHz	2.4 GHz
Complexity	Low	High	High
Power Consumption	Very low	High	Medium
Max Number of Nodes	65000	2007	8

The above table illustrates the difference between ZigBee, Wi-Fi and Bluetooth technologies. It indicates that ZigBee has the advantages of low power consumption, supporting various network topologies, and high number of nodes.

The other significant difference is the support of several types of ZigBee network topologies, namely the Star Network, Cluster Tree Network and Mesh Network.

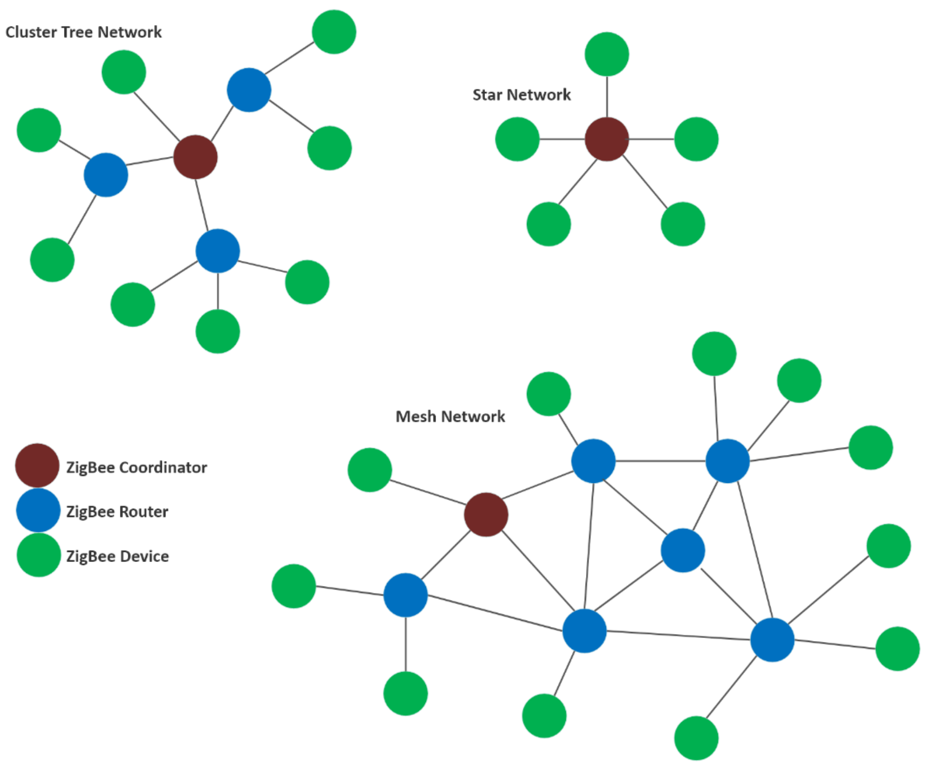

Fig 2.1.1.1 ZigBee Network Topologies

2.1.1.1 Star Network

The Star Network topology is the simplest topology that involves only a ZigBee Coordinator (ZC) and ZigBee End Device (ZED). The ZC acts as the central device which initiates and manages devices within the network. This topology is commonly used in applications for Home Automation, in which the distance coverage between ZC and ZED is far enough for the coverage requirement in a home environment.

2.1.1.2 Cluster Tree Network

The Cluster Tree Network topology deploys additional ZigBee Router (ZR) between ZigBee Coordinator (ZC) and ZigBee End Device (ZED). With the help of ZR, the distance coverage can be further extended. For example, when ZC and ZED are physically situated beyond 100 meters, they can still communicate by replaying through the ZR. This topology is commonly used in Industrial Automation applications since a large number of ZEDs can be deployed across multiple industrial workshop environments beyond the restriction of distance.

2.1.1.3 Mesh Network

The Mesh Network topology deploys multiple ZigBee Router (ZR) between ZigBee Coordinator (ZC) and ZigBee End Device (ZED). Each ZR can communicate with one another, and thus, the distance coverage can be further extended. For example, when ZC and ZED is physically situated beyond 100 meters, they can still communicate by relaying through several ZRs. This topology is commonly used in Smart Grid application because of the massive number of ZEDs can be deployed across multiple regions in the city, which carried out communication in a massive area.

2.1.2 ZigBee Standard

ZigBee standard was introduced and developed by ZigBee Alliance upon its establishment in 2002 as a non-profit organisation. Many major companies have implemented their products with ZigBee communication standards since it does not require a patent to implement the protocol.

ZigBee Alliance has announced the technical specifications of ZigBee for manufacturers to follow, allowing cross communication of products with other brands. Wireless networking standard IEEE 802.15.4-2011 has been standardised for ZigBee. Current version which is ZigBee 3.0 requiring the products to follow the specifications of ZigBee Pro 2015 (R21) or newer, while ZigBee Pro 2017 (R22) has been introduced to support two ISM frequency bands (868 MHz and 2.4GHz) simultaneously.

In 2012, ZigBee Alliance launched the ZigBee Certified programme for the certification of products that conform to its standards. This involves defining various types of certifications and related policies, including requirements for certification and testing programs and leveraging engineers' and business people's expertise to ensure only quality products earn ZigBee Certified product status.

2.2 ZigBee Application

ZigBee technologies have been widely used in Home Automation, Industrial Automation, Smart Grid Monitoring, etc. They are used in broad purposes such as sensing, monitoring, tracking and tagging objects, which are the means of collecting data. Besides, ZigBee has also been used for different automation controls. To facilitate the description of ZigBee security study on different application, we categorised the application use cases as below:

1. Sensors for Data Analysis

   Various sensors can be deployed into ZigBee networks to collect environmental parameters, such as temperatures, humidity, pressure and moisture, etc. Within the use cases in Home Automation, a central web portal is mostly provided for consumers to monitor the temperature and humidity in different areas in the Smart Home environment. Within Industrial Automation, automation in manufacturing and production industries have been keeping in development where a communication link keeps monitoring various critical parameters and equipment.

2. Sensors for Automated Decision and Control

   An example can be found in Home Automation that ZigBee temperature sensors getting real-time room temperature to carry out automated control of air-conditioning in home area. While for Industrial Automation, sensors detecting the moisture of the area helps to automate control watering in industrial applications.

3. Electricity Relay and Switching Control

   Examples can be found in home appliances such as lighting control systems for turning the lights on or off. While within Industrial Automation there are also ZigBee electricity switching control turning machines on or off.

4. Direct Mechanical Control

   Some ZigBee is used for direct mechanical control, such as door lock in home automation application, and robotic actuator control in industrial application. Since the network packets of ZigBee are aimed for simplicity, single action will be done within this field, such as perform open and close actions of a ZigBee door lock.

5. Critical Infrastructure

   ZigBee has also been used for Smart Grid Monitoring. For example, it can be used to effectively manage power grids, such that users with ZigBee equipment can easily detect faults precisely. Sensors which monitor temperature, pressure, etc. are examples in Smart Grid Monitoring using ZigBee technology.

There are many other purposes of usages in which manufacturers have included the use of ZigBee in their products, such as for outdoor asset GPS tracking. ZigBee's low-latency and low power consumption has reduced the communication cost and significantly enhanced the overall control process. Besides, ZigBee can be implemented within other remote operations in smart metering including energy consumption response, pricing support, security over power theft, etc.

3. Security Study in ZigBee Technology

3.1 Security Features in ZigBee Network Architecture

As ZigBee taking part in one of the wireless technologies with low-power consumptions, they can only carry small network packets which do not allow high-end security appliance to be implemented. Most of the security within ZigBee technology has been done in pairing and networking sections which include encryption. ZigBee Alliance has announced security standards for manufacturers to develop ZigBee products with wise security standard attached.

3.1.1 Security Models and Device Pairing

Taking towards the security features within ZigBee networking environment, ZigBee provides security services based on IEEE 802.15.4, such as secure key establishment, secure key transportation, frame protection via symmetric cryptography, and secure device management. These security services have been done when pairing and networking in ZigBee devices.

There are two different types of security models that ZigBee network is supporting, Centralised Security Model and Distributed Security Model.

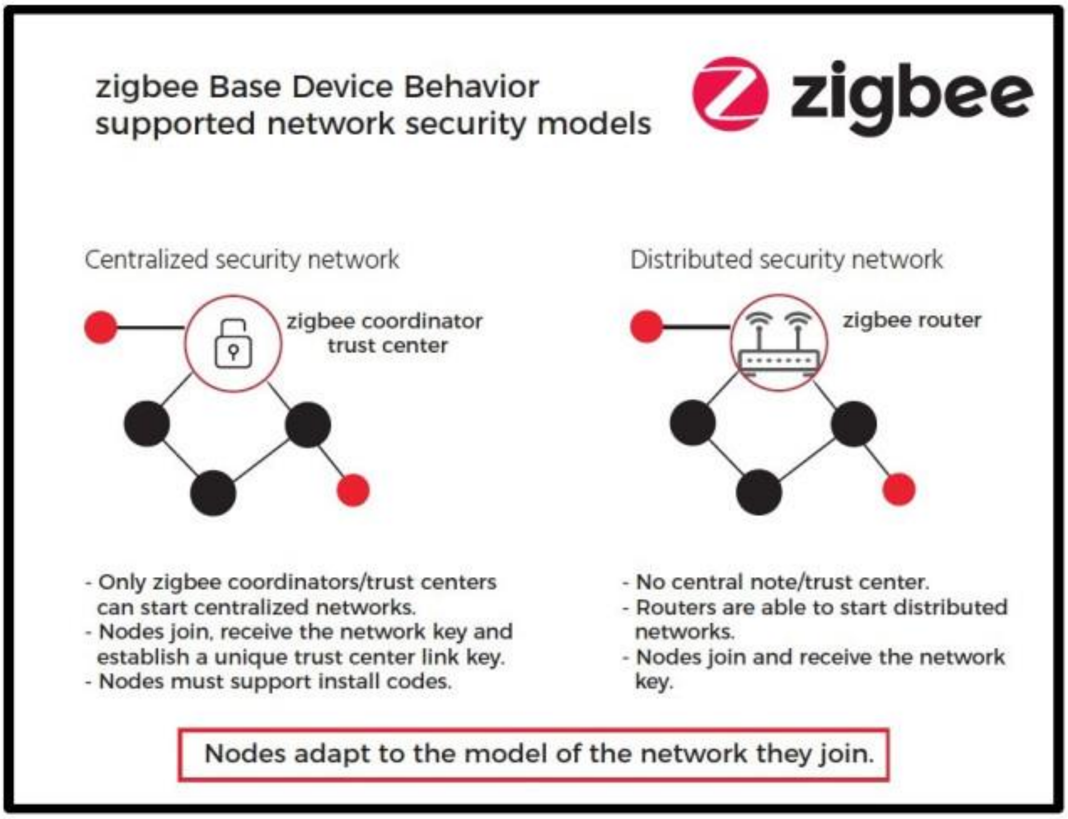

Fig 3.1.1.1 ZigBee Supported Network Security Models[1]

The security of ZigBee network mostly relies on the network keys and the link keys when implementing both Centralise Security Model and Distributed Security Model. The 128-bit network key is used to

[1] Source: Zigbee Alliance (https://zigbeealliance.org/)

secure broadcast communication, which shared among all devices in the network. The 128-bit link key is used to secure unicast communication on Application Layer, which is shared between the two communicating devices.

ZigBee network with Centralised Security Model is that to let the ZigBee Coordinator be the Trust Centre, it forms a centralised network, handling configurations and authentications once the devices are joining the network. The Trust Centre is used to establish a unique Trust Centre Link Key for each device on the network, as well as to determine the network key. All devices must be pre-configured with the Trust Centre Link Key, in order to encrypt the network key when passing it from the Trust Centre to the device that has newly joined.

ZigBee network with Distributed Security Model is operating by ZigBee Routers and end devices. The ZigBee Router can form a distributed security network when it cannot find any existing network. With the network key that the ZigBee Router can be issuing by itself, all the ZigBee Routers and end devices must be pre-configured with a link key that is used to encrypt the network key when passing it from a router parent to a newly joined node.

3.1.2 Encryption

3.1.2.1 Encryption Standard

While IEEE 802.15.4 provides robustness against interference from other networks and uses AES (Advanced Encryption Standard) with a 128-bit key length, developers have an option to implement ZigBee devices to transmit and receive network frames which protected with the security suite. AES-CCM, which is supported to be implemented within ZigBee network, is a minor variation of AES (Advanced Encryption Standard) with a modified CCM mode (Counter with CBC-MAC). The CCM is referred to as a generic mode of operation that combines the data encryption, data authentication, and data integrity. Comparing to the Wi-Fi technology, Wi-Fi Protected Access 2 (WPA2) is the current adoption of encryption method being used within Wi-Fi networks. It also uses AES-based encryption mode and mandatory support for CCM Mode Protocol (CCMP) with a 128-bit key length. As mentioned above, this shows that the encryption standard in ZigBee technology has a similar encryption strength in current wireless technology.

3.1.2.2 Replay Attack Protection

The ZigBee network deploys replay attack protection by using 32-bit frame counter, which is incremented at every packet transmission. In normal operation, a node first verifies the frame counter value before the packet is accepted. If it finds the frame counter invalid, it drops the invalid packets and thus prevents against replay attack, in which attackers try to attack the network wirelessly by simply replaying a captured packet in the ZigBee network.

3.1.2.3 Encryption on Network Layer

Within the Network Layer as part of the node authentication process during network joining, the Trust Centre sends an encryption key to the joining device, which is the Network Key. This randomly generated key is common to all nodes of the same network, while nodes must use this key at the network layer to encrypt or decrypt the general protocol maintenance data which they are exchanging. In some applications, this key is also used for encryption or decryption of user data.

When distributed to a new node, the network key itself is encrypted with pre-configured key that is known to the Trust Centre and the node. This pre-configured key is not used again by the node but maybe used by the Trust Centre to authenticate other joining nodes.

3.1.2.4 Encryption on Application Layer

On top of network layer encryption, one node can form end-to-end encrypted communication with another node in the application layer. A unique key named application key or link key has been used for two nodes, which to perform encryption or decryption of communications carried between them. This key provides application level security, which is additional to that provided by the network layer, and to offer two tiers of security.

Besides, the encryption on application layer has also been used in the initial device pairing process. Initially, a joining node may have configured with a pre-configured link key for communications with the Trust Centre, to securely transport the network key from the Trust Centre to the node. If link key security is enabled for the network, this unique link key will subsequently be used to secure communications with the Trust Centre. In addition, it will be used by the device to rejoin the network later if needed.

The newly authenticated device may also need to communicate with another device in the network using application layer encryption, which requires a unique link key to secure the messages that they are exchanging. Once a network node has established a secured link with the Trust Centre, the Trust Centre can act as a broker to provide this unique link key for communication between the other two nodes. The link key is usually a random key generated by the Trust Centre, but since to let different manufacturers to implement their ZigBee products obtain communications between different brands, “ZigbeeAlliance09” as a common pre-configured link key has been introduced.

3.1.2.5 Installation Code Keys

Installation Code Key is an alternative to pre-configured link key as mentioned in section 3.1.2.2. Pre-configured link key facilitates devices to join the network easily without much user interaction. Installation code key needs user interaction or manual configuration on both Trust Centre ends and device ends in the ZigBee network, such that a ZigBee device can use the installation code key in pairing with the Trust Centre successfully.

This provides additional security for the initial exchange of the network key at the moment of pairing process.

3.1.2.6 Encryption with Certificate-Based Key

Certificate-based Key Encryption is that the ZigBee application profiles employ Certificate-Based Key Establishment (CBKE) to derive a unique key to secure communication. Every device within the network requires to store a certificate issued by a trusted certification authority. The certificate is possible to generate a public key and other security elements. The CBKE method provides a mechanism to safely identify a device and to allow it to start the communication. The CBKE procedure involves the following steps:

1. Exchange static data (certificate validation) and ephemeral data
2. Generate the key
3. Derive a Message Authentication Code (MAC) key and key data

4. Confirm the key using the MAC

For the 2nd and 3rd steps, the key establishment procedure refers to the Elliptic Curve Menezes-Qu-Vanstone (ECMQV) key agreement scheme and a key derivation function respectively. The Trust Centre and the authenticating device share a new link key that will be used to protect data communications between them at the end of this process.

3.2 Security Standards from ZigBee Alliance

While the technical specifications from ZigBee Alliance allow manufacturers to implement ZigBee network environment in the choice of Centralised Security Model or Distributed Security Model, “ZigbeeAlliance09” has been introduced by ZigBee Alliance to be the default value of the Trust Centre Link Key.

“ZigbeeAlliance09” can be used as the pre-configured link key for manufacturers who want their devices to be compatible to other certified devices from other manufacturers. The devices have to implement the standard interfaces and practices of this profile.

The pre-configured global link key is used to encrypt the network key when it is passed from the Trust Centre to the end devices. By using “ZigbeeAlliance09” as the default global Trust Centre Link Key, this allows nodes from different manufacturers to join the ZigBee network.

4. Security Analysis in ZigBee Technology

4.1 Security Features and Analysis

There are various security features mentioned from the previous sections which being optional to developers when implementing their products. This section further analyses the security considerations in implementing different security features available in ZigBee technology. Different levels of security configuration will be introduced according to the security requirements of application use cases.

4.1.1 Security Configuration

As to let product developers having the options of what security features can be included into their products, various of security configurations can be implemented into different sectors in ZigBee products to enhance their security levels:

A. Trust Centre Link Key in Zigbee Communication

   As the Trust Centre Link Key is the encryption key within the Application Layer in ZigBee communication, the following is the usage of the Trust Centre Link Key:

   a. Used in initial pairing to exchange of network key from hub to device
   b. Sending or receiving Application Support (APS) security messages

B. Network Key in Zigbee Communication

   The Network Key is the encryption key within the Network Layer for ZigBee communication:

   a. Used between the ZigBee communication between hub to device
   b. All devices use the same network key at one time

C. Security Control of the Smart Hub

   As ZigBee smart hub usually holds better performance power than the end-devices and as the role of Trust Centre, the following adjustments can be done to level up the security of the whole ZigBee network:

   a. Administration of the smart hub
   b. Management of connected devices (add or remove devices)
   c. Trust Centre Link Key updates

D. Security Control of Device Pairing

   To prevent the devices to be compromised during pairing and initialisation stage, the following functionalities can be implemented to avoid the chances to be compromised:

   a. Pairing recognition control
   b. Communication initialisation
   c. Key exchange management

E. Device connection management

   The followings can be implemented to avoid and block the unauthorised ZigBee devices entering the network environment:

   a. Connection timeout adjustment
   b. Device status update period

4.1.2 Recommended Security Configuration

The security requirements for different application use cases can vary. Some smart home products may only use ZigBee network for collecting data from sensors. It may not require high security level while maintaining a low product cost. On the other hand, applications involving critical infrastructure control system may require very high security level due to its impact on the society.

As such, different design considerations based on the five categories of use cases as mentioned in section 2.2 are analysed to make recommendations on their suitable security configurations.

The table below shows the application considerations and recommended security configurations of ZigBee devices sorted by use cases:

<table>
<tr><th>Use cases</th><th>Product Design Considerations</th><th>Suitable Security Configuration</th></tr>
<tr><td>1. Sensors for Data Analysis</td><td rowspan="2">• The interoperability between different brands of sensors is the major requirement in this use case.
• The simplicity of the deployment process is the primary consideration in the product design for large-scale data collection.
• Incorrect sensor data may cause an impact on decision making and automated control.
• The integrity of sensor data is the primary consideration in this use case.
• Appropriate security configuration is required in the product design.</td><td rowspan="2">A) Trust Centre Link Key:
• Use ZigBee Alliance default key for interoperability and ease of user installation process.
B) Network Key:
• Randomly generated at initial setup
C) Smart Hub Security Control:
• Provide administration on Smart Hub security control with account authentication (e.g. two-factor authentication)
• Provide status monitoring of Smart Hub to facilitate the monitoring of connected devices
D) Device Pairing Control:
• Enter pairing mode with user interaction only
• Automatic stop pairing mode if the operation reached a timeout limit.
E) Device Connection Management:
• Event log or notification available on changes of device connection status</td></tr>
<tr><td>2. Sensor with Automated Decision and Control</td></tr>
</table>

<table>
<tr><th>Use cases</th><th>Product Design Considerations</th><th>Suitable Security Configuration</th></tr>
<tr><td>3. Electricity Relay and Switching Control</td><td rowspan="2">Electricity switching controls usually require accurate action and timing.
The unavailability of switching control may cause severe impact to applications such as industrial production line
Appropriate security configuration is required in the product design.
Malfunction of mechanical control may cause direct harm to physical safety.
High level of security configuration is required in the product design.</td><td rowspan="2">A) Trust Centre Link Key:
Use proprietary pre-configured link key which is not well-known by users
Or use Installation Code Key for device joining or pairing with user interaction
B) Network Key:
Randomly generated
Perform rolling update of network key regularly
C) Smart Hub Security Control:
Provide central administration portal on Smart Hub with account authentication (e.g. two-factor authentication)
Provide status monitoring of Smart Hub to facilitate the monitoring of connected devices
Setup whitelist and blacklist of the device connection
D) Device Pairing Control:
Enter pairing mode with user interaction only
Automatic stop pairing mode if the operation reached a timeout limit.
Provide a means to validate the pairing of correct devices with user interaction (e.g. validate the S/N on the device hardware and on the admin portal)
E) Device Connection Management:
Event log or notification available on changes of device connection status
Regular polling of control device status
Provide administrative disable and stop device operation on admin portal.</td></tr>
<tr><td>4. Direct Mechanical Control</td></tr>
</table>

Use cases	Product Design Considerations	Suitable Security Configuration
5. Critical Infrastructure	• Critical infrastructure may cause a severe impact on society as a whole. • The maximum level of security configuration is required in the product design.	A) Trust Centre Link Key: • Use Certificate-Based Key • Adopt security configuration in ZigBee Smart Energy B) Network Key: • Randomly generated • Perform rolling update of network key more frequently C) Smart Hub Security Control: • Provide central administration portal on Smart Hub with account authentication (e.g. two-factor authentication) • Provide status monitoring of Smart Hub to facilitate the monitoring of connected devices • Setup whitelist and blacklist of the device connection • Provide adequate physical control depending on installation environment. D) Device Pairing Control: • Enter pairing mode with user interaction only • Automatic stop pairing mode if the operation reached a timeout limit. • Provide a means to validate the pairing of correct devices with user interaction (e.g. validate the S/N on the device hardware and on the admin portal) E) Device Connection Management: • Event log or notification available on changes of device connection status • Regular polling of control device status • Provide administrative disable and stop device operation on admin portal.

Use cases	Product Design Considerations	Suitable Security Configuration
		• Anomaly detection and alerting on device connection and traffic log.

4.2 Testing and Findings in Smart-Home Scenario

To facilitate the investigation, a ZigBee smart-home environment has been set up to provide the scenarios for verifying the findings of the above security issues. The setup environment includes a variety of ZigBee devices, including a ZigBee hub, a ZigBee multi-purpose sensor, a ZigBee motion sensor, a ZigBee lightbulb and a ZigBee-integrated door lock. While the ZigBee multi-purpose sensor includes magnetic switch sensing and temperature sensing functionality, a simulated ZigBee smart-home environment has been created to test a few scenarios that may lead to security risks. Below Diagram shows the setup of the smart-home environment:

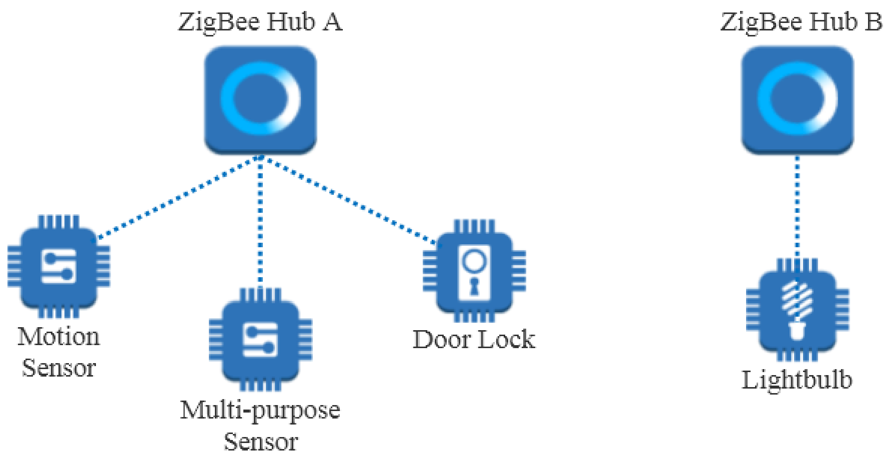

Fig 4.3.1 Testing Environment Setup

4.2.1 Attacker to Discover the ZigBee Smart-Home Environment

As the attacker needs to have some ideas of the network within the ZigBee smart-home environment, packet sniffing is the first step to get numerous of network packets and analyse the actions that have been made. A packet sniffing test was conducted by using ZigBee sniffer as a tool, starting from the ZigBee devices pairing to the ZigBee hub, and monitoring of the traffic packets continued once they were in operation. The detailed findings of packet sniffing test are attached within Appendix 7.1.

Since the plan was to discover the network key at the beginning, the "ZigbeeAlliance09" key was inputted as the default link key values. As the devices were exactly using "ZigbeeAlliance09" as the Trust Centre Link Key, they were decrypted and the network key was discovered by looking up the transport key command traffic packets.

Once the network key was confirmed to be that within the ZigBee communication, the network packets were made readable to human with the help of packet viewer. As some sample ZigBee packets had been attached within Appendix 7.1, the sensors were sending their status back to the hub, with temperature data being carried in the network packet, and commands to lock or unlock have been sent to the ZigBee door lock.

The findings mentioned above shows that "ZigbeeAlliance09" key has been commonly used for manufacturers developing their products. However, it is not hard to understand what the network packets the ZigBee devices are transmitting once the key is known. The findings mentioned above may lead attackers to perform denial of services (DoS) or packet replay attacks, since the network packets within this ZigBee network environment setup are possible to be read by an unauthorised person.

4.2.2 Attacker to Paralyse the ZigBee Smart-Home Environment

The first test showed that the attackers would be gain a basic understanding of the network communication by the performance of packet sniffing. We assumed the attackers would perform further actions to try to compromise or take down the network, while performing denial of services (DoS) attack will be the first attempt to paralyse the ZigBee smart-home network. Flooding packets would be one of the testing that were performed to find out if it may trigger denial of services within the ZigBee network, estimating the security level that the ZigBee network environment is holding. Screen captures of the steps and findings within the flooding packet process are attached within Appendix 7.2.

The completion of packet sniffing process mentioned in Section 4.3.1 offered a better understanding of the body of a ZigBee packet for its network environment. Several flooding attacks towards the ZigBee Hub were performed to observe if it would be possible to make the ZigBee Hub crashe from too many connected stations.

PAN ID Conflict Flooding, Spoofed Orphan Notification Flooding and Associate Request Flooding were attempted. While the ZigBee hub was able to receive flooding packets, it ignored them, reflecting that those flooding attack attempts did not cause DoS towards the ZigBee hub.

4.2.3 Attacker to Hijack the ZigBee Smart-Home Devices

Rather than sending flooding packets to trigger denial of services within ZigBee network environment, attackers would try to perform packet replay, which is an advanced technique to fake the ZigBee devices with incorrect network instructions. Packet replay requires further understandings of the network communication that to specify what series of network packets are needed to be modified and transmit, successfully hijacking the device's environment. Screen captures of the steps and findings within the packet replay process are attached within Appendix 7.3.

Further to packet sniffing and flooding attack attempts described in Section 4.2.1 and 4.2.2, attackers might want to control the devices within the ZigBee network as well, to compromise or hijack the devices to perform malicious actions. Packet replay will be a simple hijacking technique to collect original packets and replay it in unexpected times.

With the help of the ZigBee packet replay program and module, some sniffing actions had been done within the devices in the ZigBee smart-home environment, such as switching on and off of the lightbulb, opening and closing the door lock, positive and negative movement of the sensors, etc. With the network packets being collected during Packing Sniffing test in Section 4.2.1, the exact ZigBee packets that proceeding commands with the lightbulb control from the ZigBee hub were filtered. The mentioned packets by ZigBee replay module had been replayed to test if it was able to perform replay attacks towards the ZigBee devices.

Although the replay attack was successfully performed within the ZigBee network, the light bulb neglected the replay network packet and was not executed the attack command. It might be due to other safeguards in message authentication control (e.g. message sequence number), which deterred the attacker from performing the replay attack successfully.

5. Recommendations

Having summarised the security issue that would be encountered when having a ZigBee network, the Study would provide recommendations to general users and product developers.

5.1 General Users

- Purchase ZigBee devices from official channels. Before purchasing, search for information like whether the ZigBee device has security vulnerability, and whether the vendor provides firmware update in official website, etc;
- Purchase ZigBee devices that are certified with technical specifications from ZigBee Alliance;
- Turn on the device only when in use and connect the device immediately after it is turned on. And turn off the device when it is idle;
- Check and update the device firmware regularly; and
- Enable higher security feature options whenever the products provides.

5.2 Product Developers

- Adopt the suitable security configurations as mentioned in section 4.1.2 according to the application use cases;
- Develop ZigBee devices by following the technical specifications announced by ZigBee Alliance.
- Timely rollout of updates to fix ZigBee products' vulnerabilities;
- Regular rolling update of the network keys; and
- Implement ZigBee products that requires high security assurance with the ZigBee Smart Energy profile which includes Key Establishment Cluster and certificates issued by certification authorities.

6. Summary

- Given the simplicity of ZigBee network architecture, general users and developers should be aware of the use of the ZigBee devices.
- ZigBee wireless technology has in place several security features built-in (e.g. encryption) to achieve a certain level of security in wireless communication. But developers need review their application use cases and adopt suitable security configurations available in the ZigBee standard.
- Due to the simple setup of ZigBee enabled products, there are fewer security configuration options available to general users or consumers. Therefore, developers play a vital role in product development to ensure the security of their ZigBee products.
- This security study on ZigBee IoT devices may not cover all aspects in the ZigBee IoT solution, e.g. cloud platform, mobile application, physical device security, etc. Developers are recommended to go through the HKCERT "IoT Security Best Practice Guidelines" to improve the security on different security layers of their ZigBee products during development stage.

7. Appendix

7.1 Discovery on the ZigBee Smart-Home Environment Security Test

From the beginning, we need to use the ZigBee channel scanner tool to verify which channel is the ZigBee network is holding the communications since there are various channels which could be chosen by the ZigBee devices for communications. Channel 20 and channel 24 had been found which responding from the ZigBee chancel scanner tool, by the meanings that the two ZigBee hubs were using channel 20 and chancel 24 for network communication respectively.

```
Setting channel to 16.
Transmitting beacon request.
Setting channel to 17.
Transmitting beacon request.
Setting channel to 18.
Transmitting beacon request.
Setting channel to 19.
Transmitting beacon request.
Setting channel to 20.
Transmitting beacon request.
Received frame.
Received frame is not a beacon (FCF=4188).
Received frame.
Received frame is not a beacon (FCF=4188).
Setting channel to 21.
Transmitting beacon request.
Setting channel to 22.
Transmitting beacon request.
Setting channel to 23.
Transmitting beacon request.
Setting channel to 24.
Transmitting beacon request.
# DEBUG Clearing overflow
# DEBUG Clearing overflow
# DEBUG Clearing overflow
# DEBUG Clearing overflow
# DEBUG Clearing overflow
Received frame.
Received frame is not a beacon (FCF=0200).
# DEBUG Clearing overflow
Received frame.
Received frame is not a beacon (FCF=0200).
# DEBUG Clearing overflow
# DEBUG Clearing overflow
# DEBUG Clearing overflow
# DEBUG Clearing overflow
# DEBUG Clearing overflow
# DEBUG Clearing overflow
Setting channel to 25.
Transmitting beacon request.
Setting channel to 26.
Transmitting beacon request.
```

Fig 7.1.1 Detecting ZigBee Channels In Use

After observation and from the results shown on the above, channel 20 and 24 were being used for the communication for network environment of ZigBee Hub A and B. The packet sniffing process began by tuning the ZigBee sniffer to channel 24 in the following tests.

Sniffing the Network Key

As it is known that the encrypted network key would be sent from ZigBee Hub to devices during the pairing process, we had then successfully sniffed some ZigBee pairing packets and loaded into the packet viewer for packets analysis. One packet noted as "APS: Command" had been sent from the ZigBee Hub to the end-devices within the pairing mode. Since the packets had been encrypted, the data of the packets are unreadable, and we were only able to review the encrypted data as below:

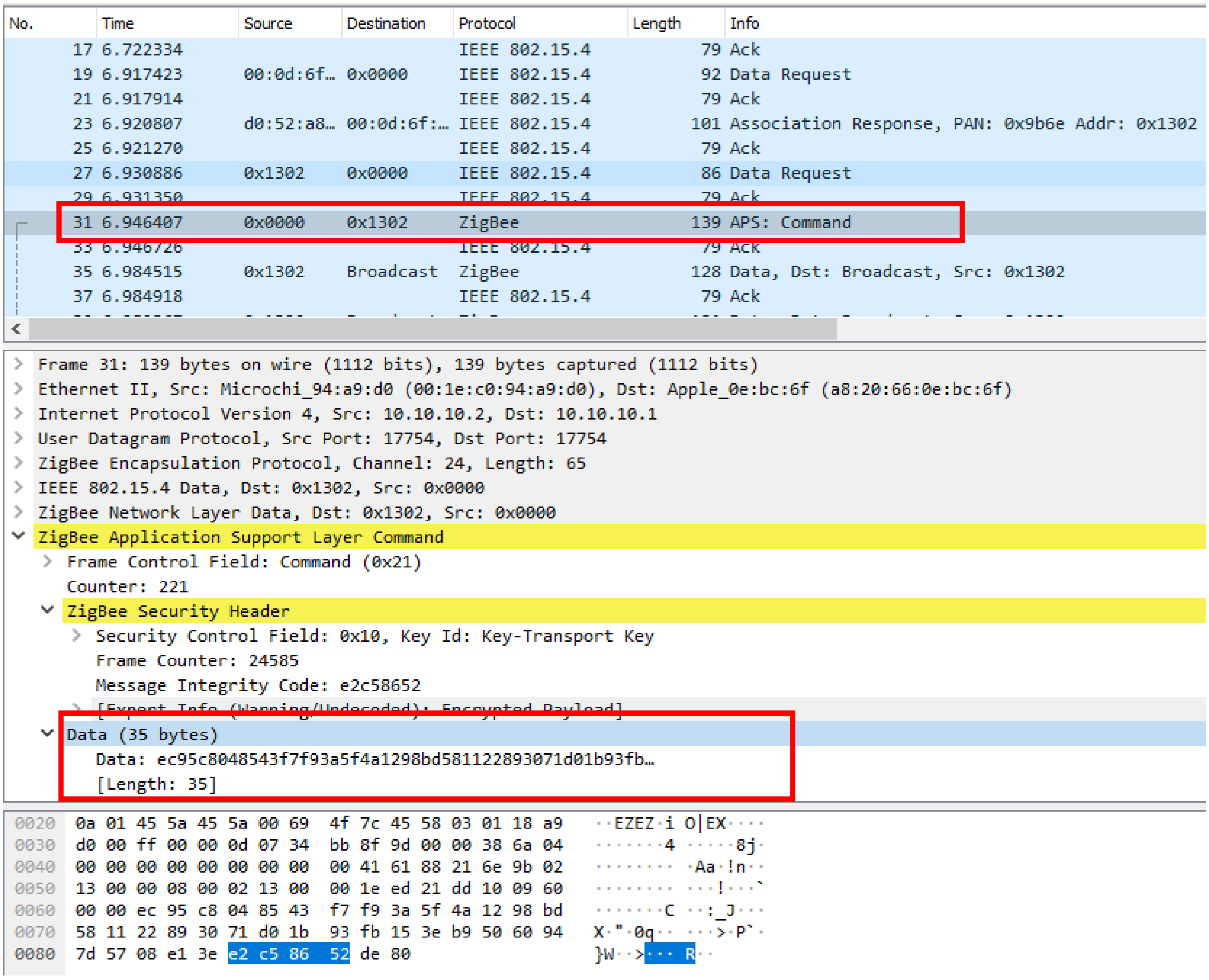

Fig 7.1.2 Sniffing ZigBee packet during the pairing process

As ZigBee Alliance had promoted the "ZigbeeAlliance09" to be the default Link Key to the public. We had tried to input the "ZigbeeAlliance09" (Value: 5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39) to be the Trust Centre Link within transport key command packet viewer to obtain the Network Key.

As the fact that the ZigBee Hub and the end-devices were using the "ZigbeeAlliance09" as the Trust Centre Link Key, we had found a packet which sending from the ZigBee Hub to the ZigBee device that containing the information Network Key, which is [2aba5474cae8f6d1e7b3ce6797df25af].

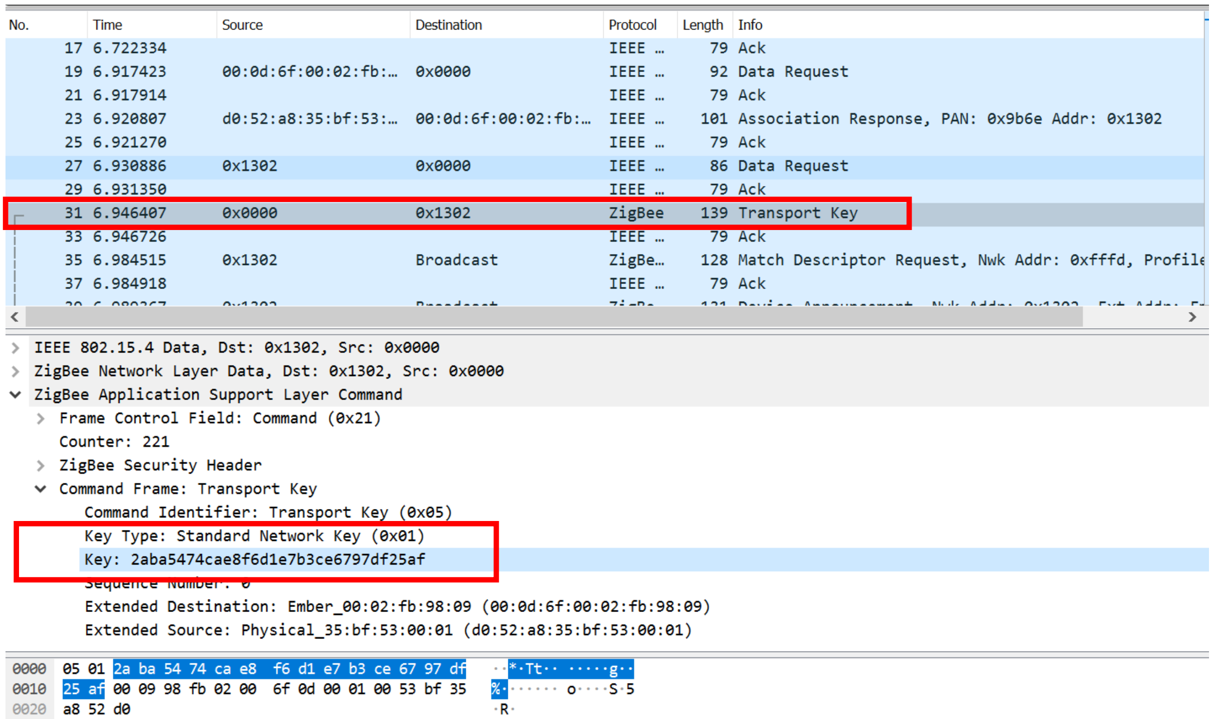

Fig 7.1.3 Decrypted packet showing the Network Key of Smart Hub A in plaintext

To obtain a fully readable network packets' history, the Network Key which obtained from the previous step was inputted into packet viewer.

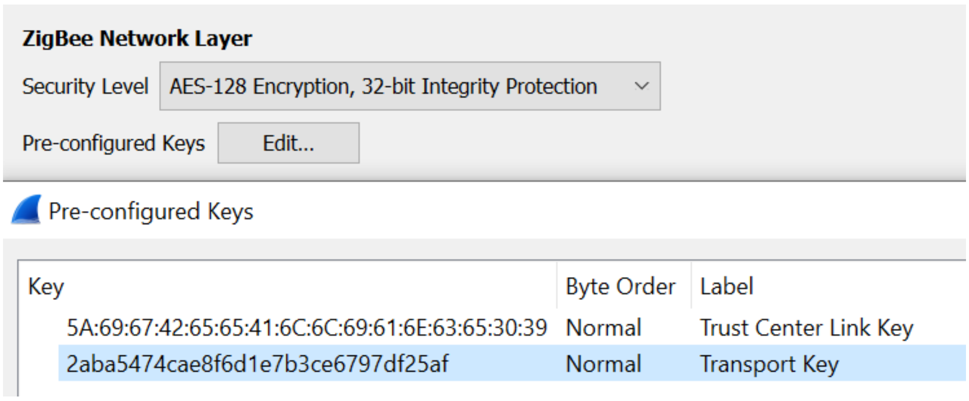

Fig 7.1.4 Configure Network Key in packet viewer

Decrypted ZigBee communications content

After the Trust Centre Link Key and the Network Key had been input into packet viewer, we were able to read the data within the ZigBee packets and analyse what actions that the ZigBee devices and the ZigBee Hub had been performed.

The ZigBee packet captured below showing the multi-purpose sensor was sending "Zone Status Change Notification" to the ZigBee Hub A. The network packet had described "Alarm 1" stored the value of 1 which meant that it was opened or alarmed, as it actually meant that door sensor had been opened within the multi-purpose sensor.

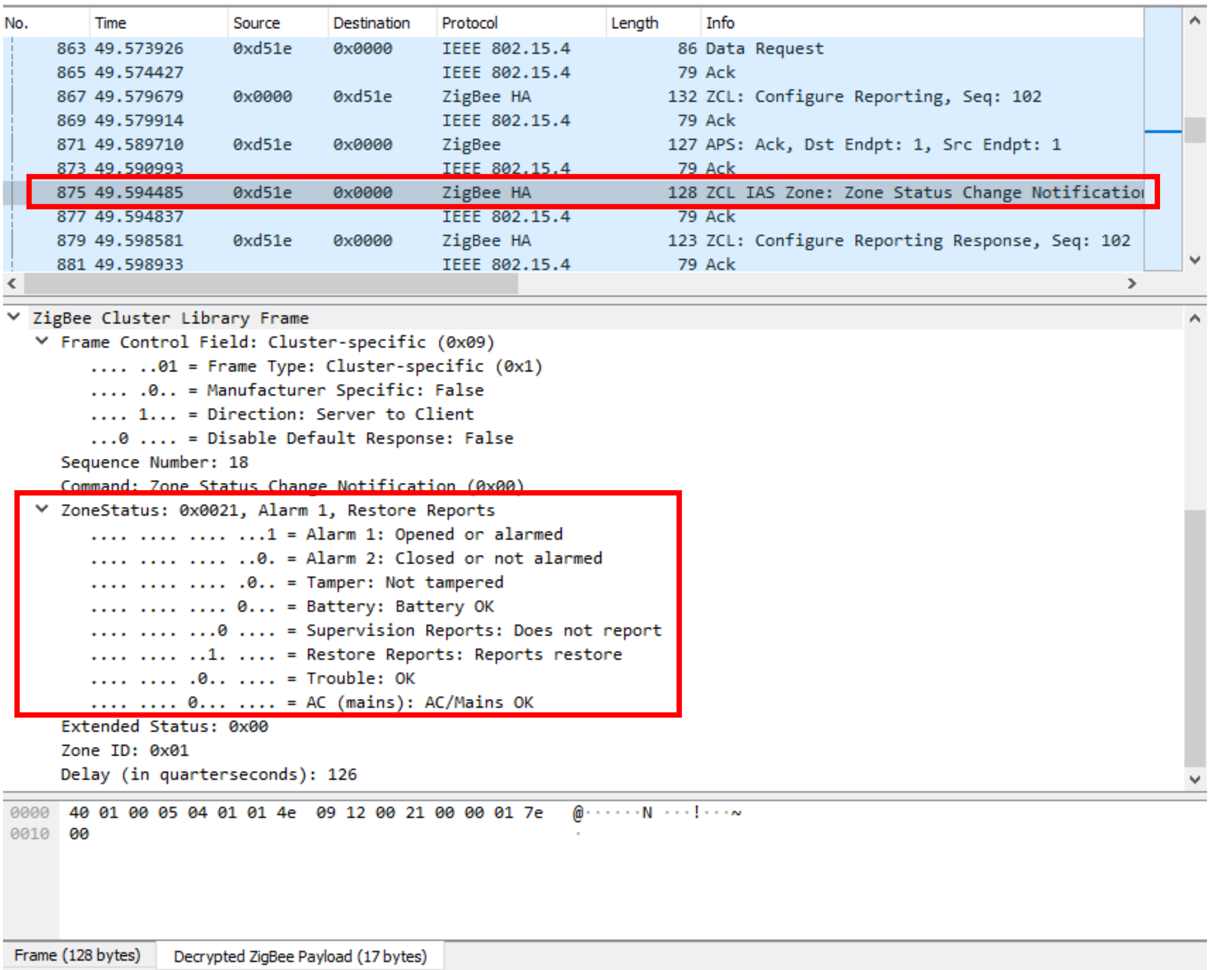

Fig 7.1.5 Decrypted packet content showing the door sensor status

One example shown below is the ZigBee packet which fetching a “Read Attributes” request from the ZigBee hub to the multi-purpose sensor. We can see that the packet was readable and showing its cluster described as “Temperature Measurement”.

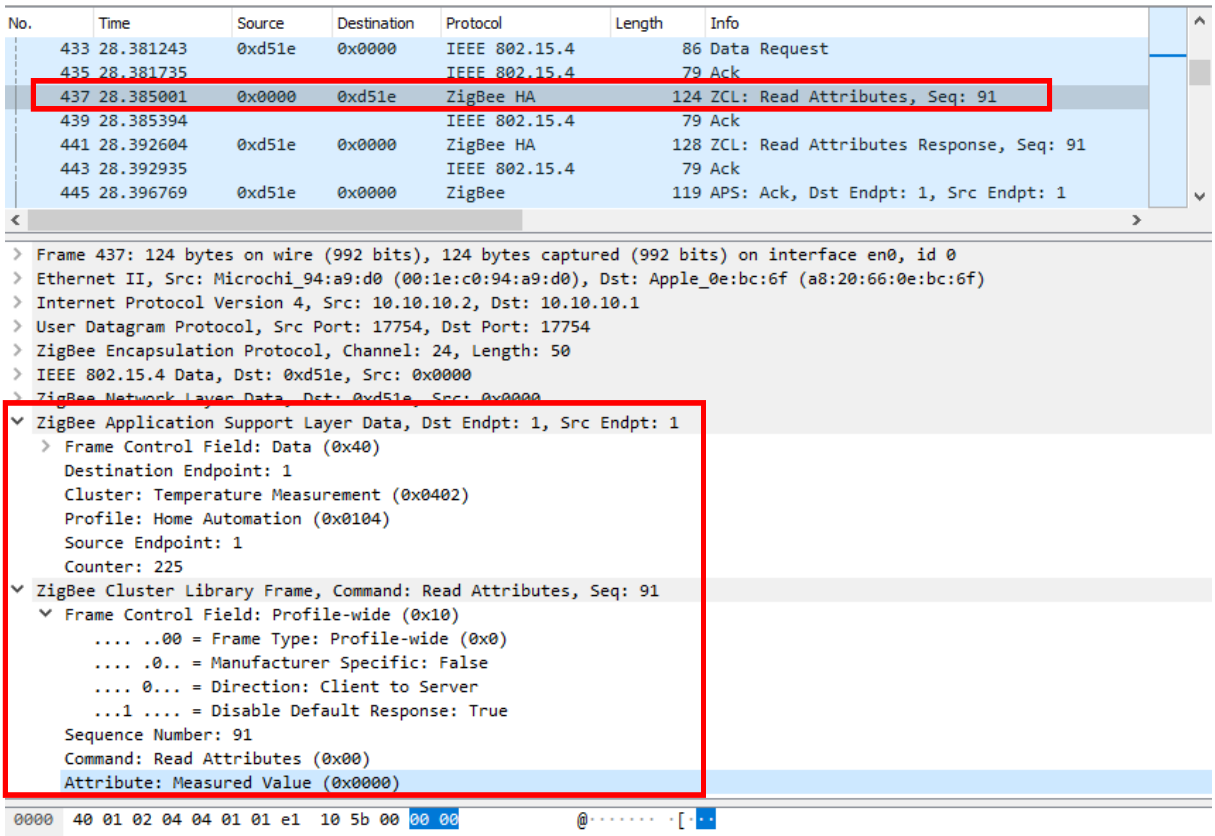

Fig 7.1.6 Read Attributes packet content showing the request for temperature sensor

Another packet had been sent from the multi-purpose sensor to the ZigBee hub, which is the "Read Attributes Response". As we had explored within the packet, the packet had carried out a string "23.38 [°C]" which alike temperature that readable by human.

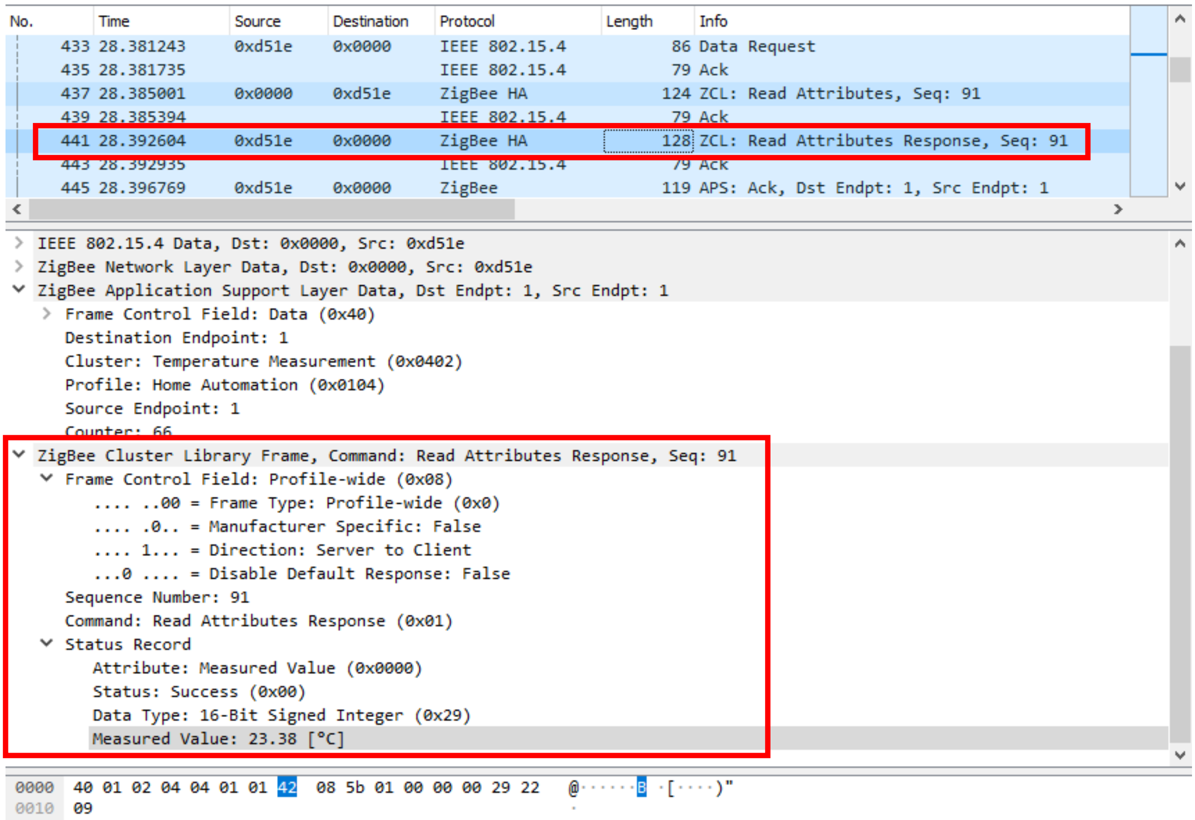

Fig 7.1.7 Read Attributes Response packet content showing the temperature value

Moving to the ZigBee Hub B environment, the packet sniffer was switched to channel 20. And the network key was obtained by inputting the “ZigbeeAlliance09” as the Trust Centre Link Key into the packet viewer, with [563aac7453f9ade238c57b9af6348579] being the value of the network key.

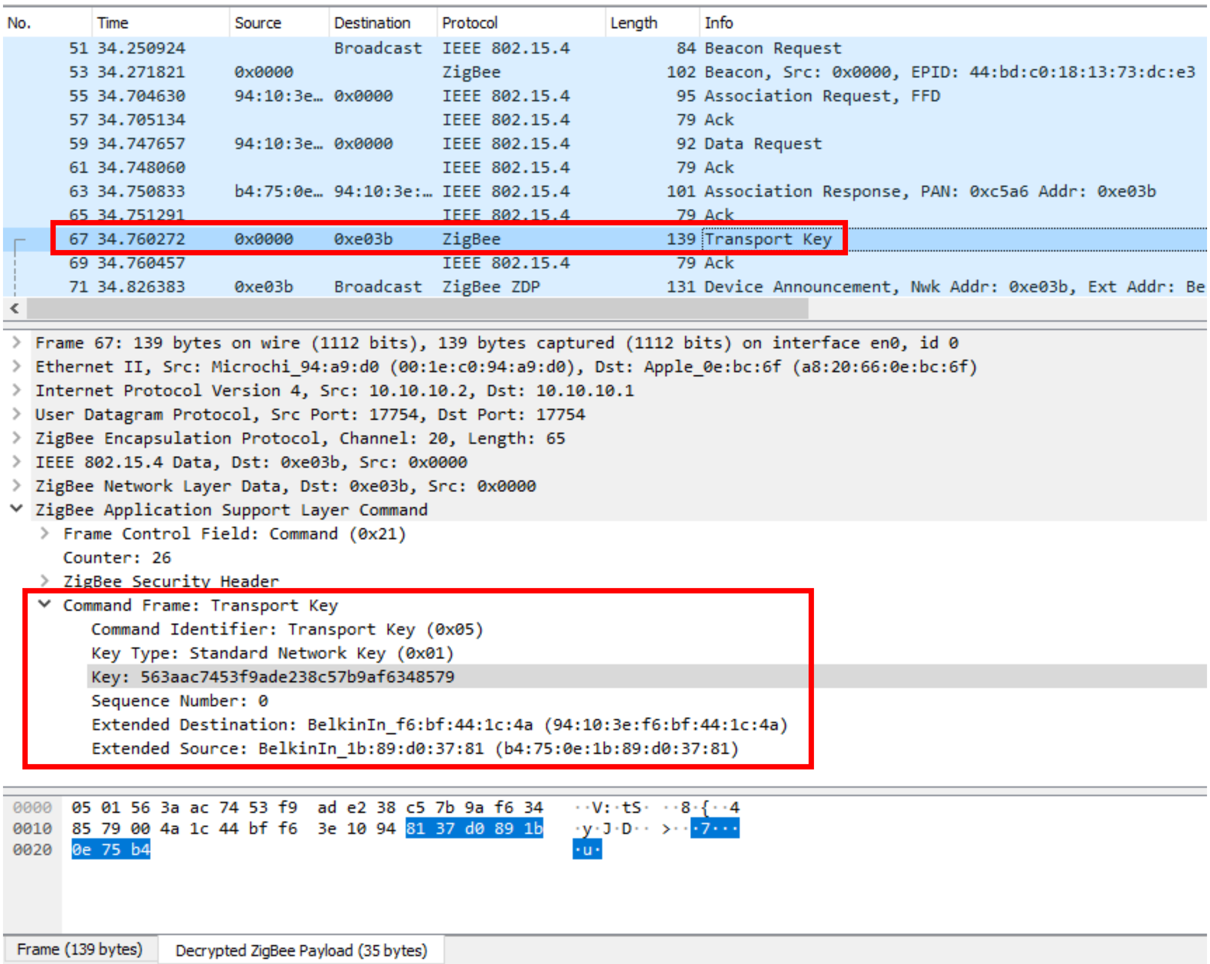

Fig 7.1.8 Decrypted packet showing the Network Key of Smart Hub B in plaintext

After the Network Key had been obtained, the Network Key was inputted into the packet viewer. Some packets noted as “ZCL OnOff: Off” or “ZCL OnOff: On” were found. Investigation into those packets revealed the commands “On (0x01)” and “Off (0x00)”, which was referring to ZigBee lightbulb to switching on or off.

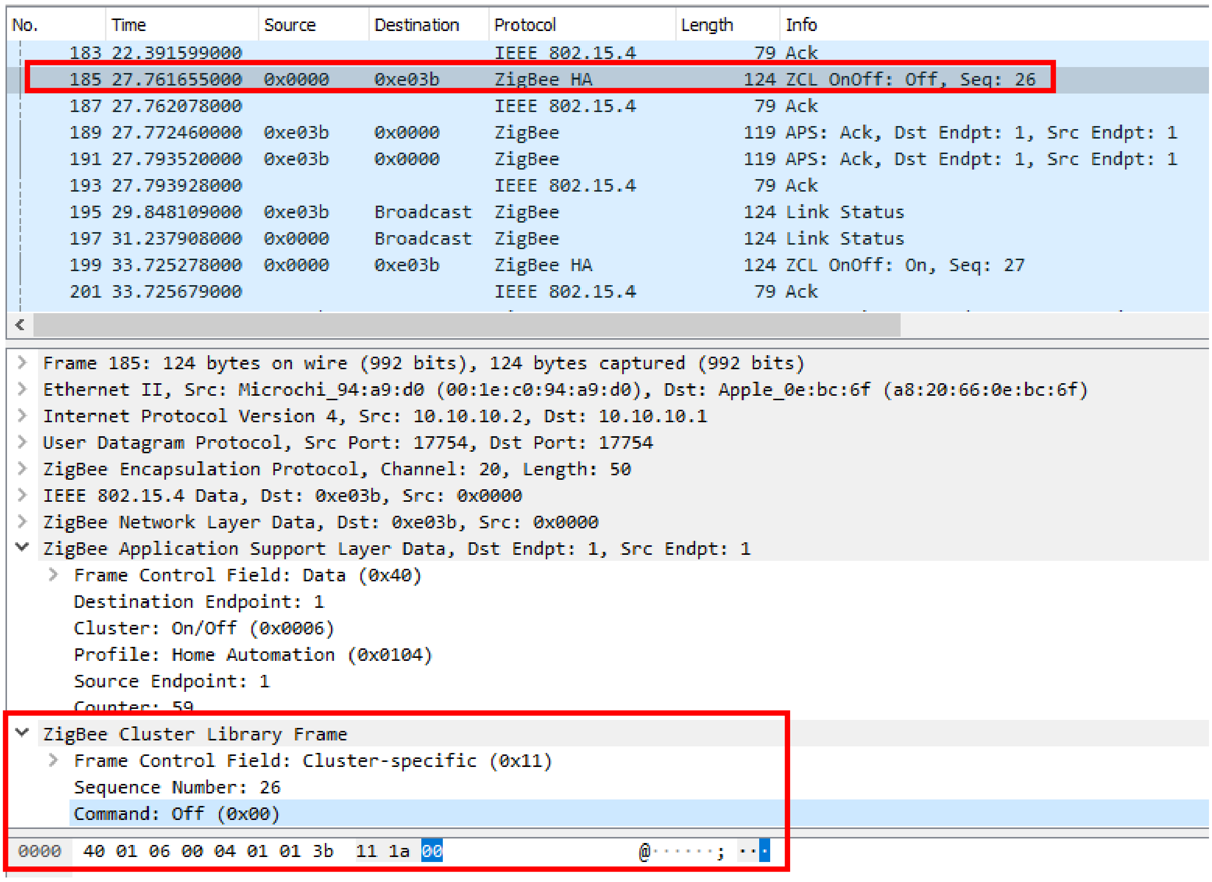

Fig 7.1.9 Decrypted packet showing the ZigBee lightbulb switch OFF command

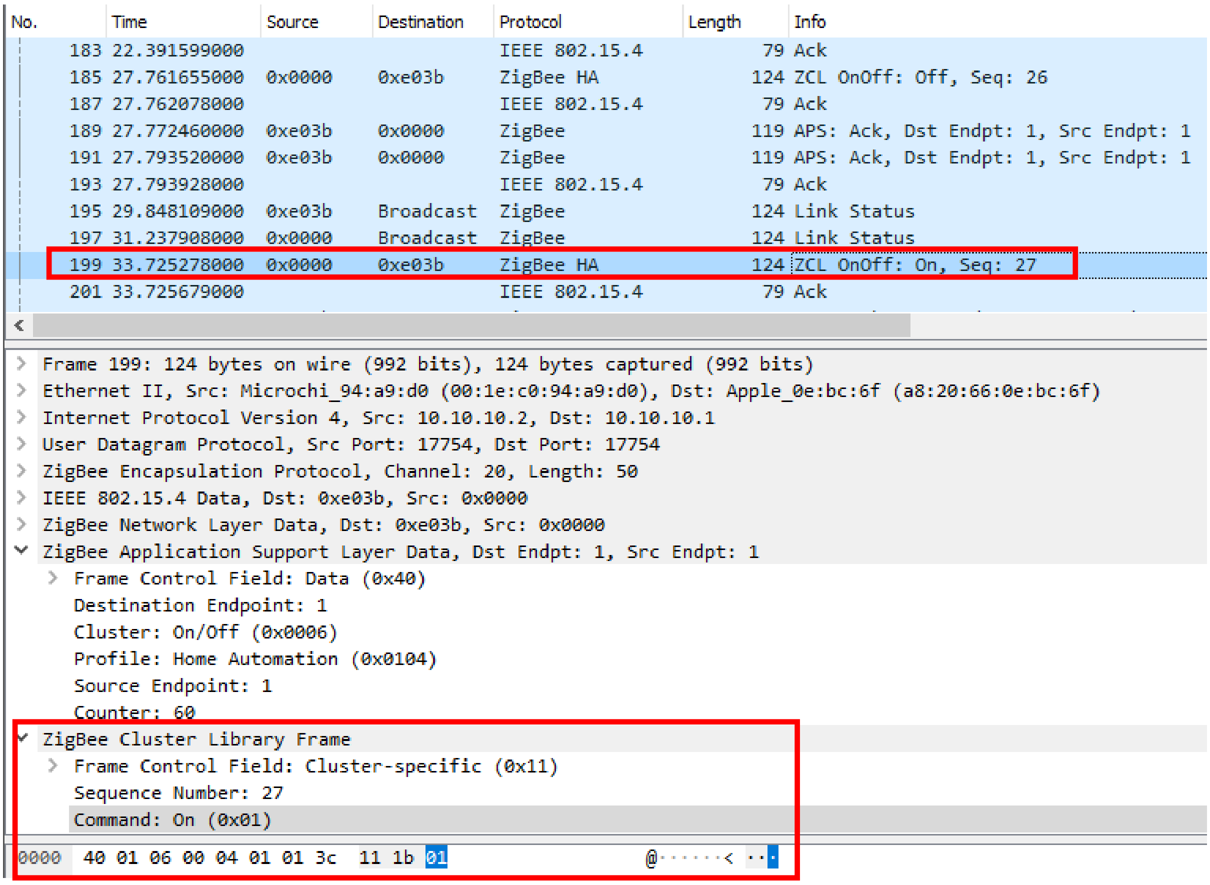

Fig 7.1.10 Decrypted packet showing the ZigBee lightbulb switch ON command

7.2 Paralyse the ZigBee Smart-Home Environment Security Testing

Once the flow of the network packets within the ZigBee smart-home environment created by the two ZigBee hubs were understood, further testing were conducted to find out if the ZigBee networks could be paralysed. Denial of Services (DoS) attacks had been performed to the ZigBee network to test if the ZigBee devices with different purposes would be unable to work normally.

1st DoS attack attempt: PAN ID Conflict Flooding

The first Denial of Service (DoS) attack attempt against ZigBee network is to generate a large amount of packet with a specific PAN ID. This might mislead the ZigBee Hub that the same PAN ID was being occupied and conflicted with the one in use. This situation might cause the devices and coordinators not functioning normally.

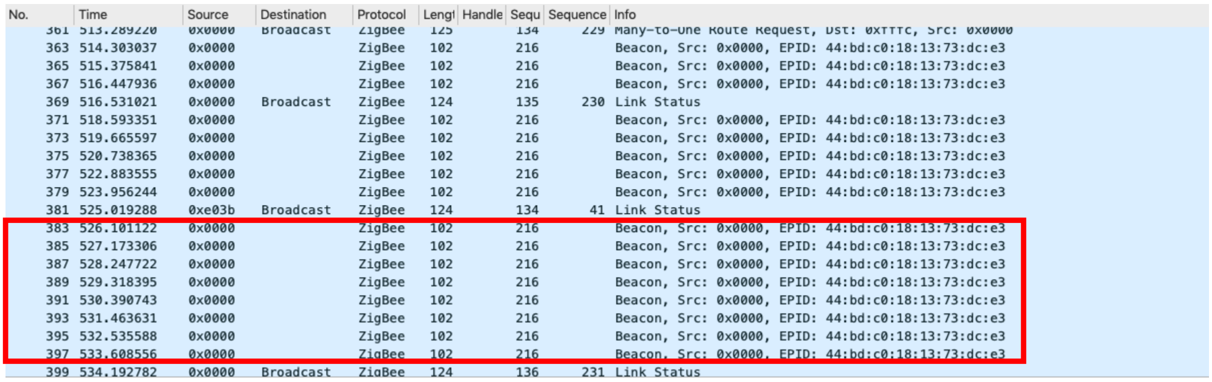

Fig 7.2.1 Generation of PAN ID conflict flooding

After the generation of PAN ID conflict flooding, it is observed that the product functionalities in the testing ZigBee Smart-Home Environment were not affected.

2nd DoS attack attempt: Spoofed Orphan notification

The second DoS attack attempt against ZigBee network is to spoof an orphan notification packet originated from the target device to the ZigBee hub, such that it might cause ZigBee hub to recognise the target device disassociated from the network.

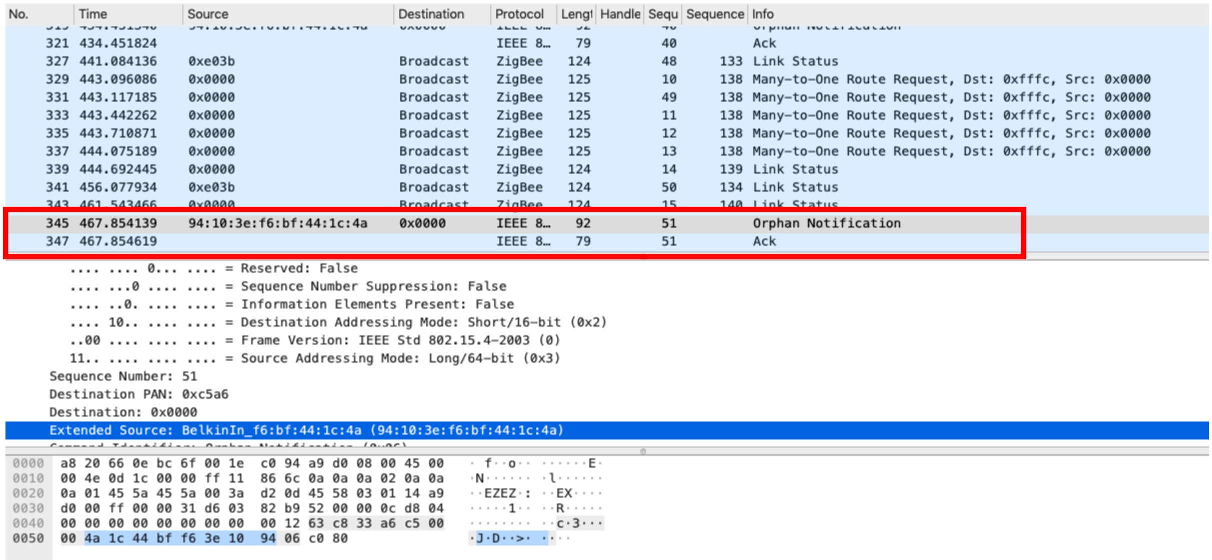

Fig 7.2.2 Spoofed Orphan Notification

After the generation of spoofed orphan notification packet, it is observed that the product functionalities in the testing ZigBee Smart-Home Environment were not affected.

3rd DoS attack attempt: Associate Request Flooding

The third DoS attack against ZigBee network is to generate a large amount of device association request packet to the ZigBee Hub. This might cause the ZigBee Hub not functioning normally by exhausting its system resources in handling the associate request.

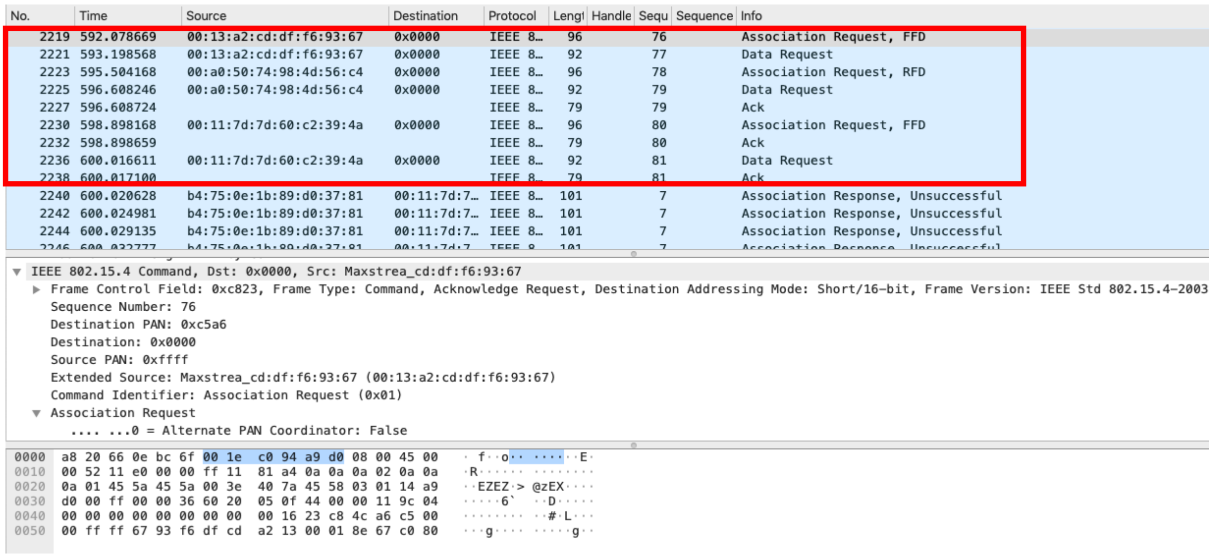

Fig 7.2.3 Generation of Association Request Flooding

After the generation of association request flooding packets, it is observed that the ZigBee Hub could correctly respond to those association requests and its functionalities were not affected.

7.3 Hijack the ZigBee Smart-Home Devices Security Testing

Moreover, other tests were undertaken to find out if the ZigBee networks could be hijacked or compromised. Replay attacks had been performed within the ZigBee network to test if it is possible to fake the ZigBee devices with unauthorised commands.

Replay attacks had been performed into separated into two steps:

<u>Step 1: Sniffing the control command network packets</u>

By sniffing the normal network environment within the ZigBee network, the exact packet of the control command to switch on the light bulb was obtained.

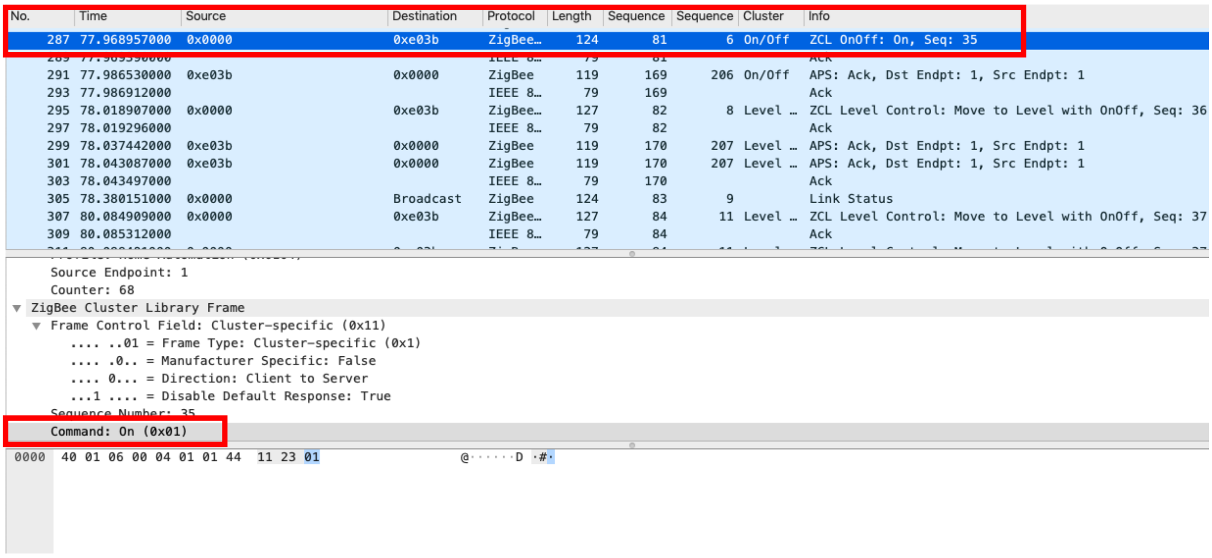

Fig 7.3.1 Obtaining exact packet of switch ON control command

Step 2: Implements a replay attack

From the previous step, we obtained the network packet to replay. The packet was loaded to a network packet crafting tools and send the exact same packet directly via ZigBee penetration testing wireless module.

```
>>> replaypkt[0]
<Dot15d4FCS  fcf_reserved_1=0 fcf_panidcompress=True fcf_ackreq=True fcf_pending=False fcf_security=False fcf_frametype=Data fcf_srcaddrmode=Short fcf_framever=0 fcf_destaddrmode=Short fcf_reserved_2=0 seqnum=81 |<Dot15d4Data  dest_panid=0xc5a6 dest_addr=0xe03b src_addr=0x0 |<ZigbeeNWK  discover_route=0 proto_version=2 frametype=data flags=security+source_route destination=0xe03b source=0x00 radius=30 seqnum=6 relay_count=0 relay_index=0 relays=[] |<ZigbeeSecurityHeader  reserved1= extended_nonce=1 key_type=network_key nwk_seclevel=None fc=0x1a9d source=b4:75:0e:1b:89:d0:37:81 key_seqnum=0 data='\xda\xd9\x90\xc6\xff\xa8\xe1\xa9x\xdfp\x93\x991\x8a' |>>>>
>>>
```

Fig 7.3.2 The details of the replay network packet

```
>>> kbdecrypt(replaypkt[0],"563aac7453f9ade238c57b9af6348579".decode('hex'))
<ZigbeeAppDataPayload  frame_control=ack_req delivery_mode=unicast aps_frametype=data dst_endpoint=1 cluster=on_off profile=HA_Home_Automation src_endpoint=1 counter=68 |<ZigbeeClusterLibrary  reserved=0 disable_default_response=1 direction=0 manufacturer_specific=0 zcl_frametype=1 transaction_sequence=35 command_identifier=read_attributes_response |>>
>>>
```

Fig 7.3.3 Decrypted payload details of the replay network packet

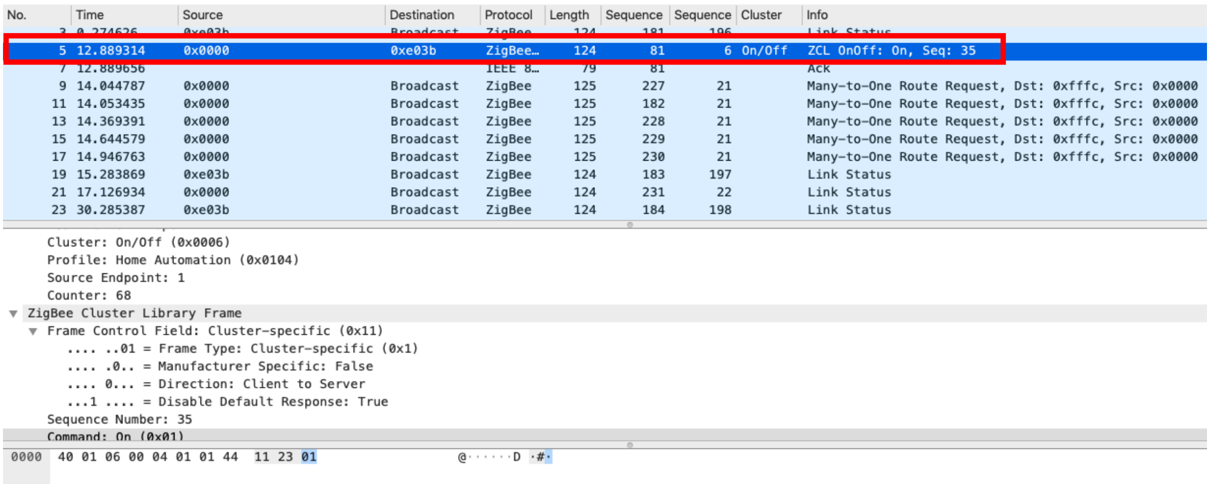

Fig 7.3.4 Replayed network packet as shown from the network sniffer

Although the replayed network packet was successfully sent into the ZigBee network, the light bulb neglected the replay network packet and was not executed the attack command to switch ON.

As mentioned in section 3.1.2.1 Replay Attack Protection, the ZigBee network communication has replay attack protection feature that prevented replay attack. Further attempted was made to craft another attack payload content based on previous replay network packet and change the network packet attributes, trying to bypass the replay attack protection by observing the current sequence number and predicting the next sequence number to launch the attack. In the testing, attempt was also made to change the transaction sequence from the original 35 to 74 based on prediction guess.

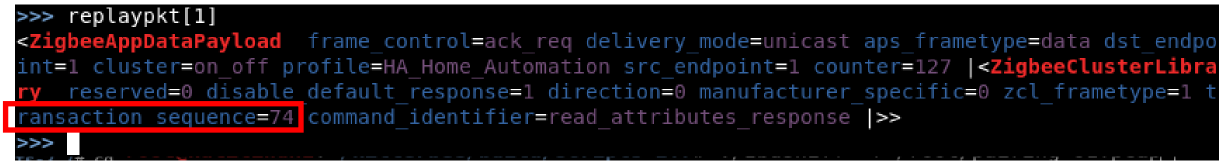

Fig 7.3.5 Crafting attack payload with modifying different packet parameters

After changing the transaction sequence attribute, the payload was then encrypted and encapsulated into a complete ZigBee network packet using the network key obtained in section 7.1. Other network packet sequence numbers (e.g. setting seqnum attribute to 58) were modified by prediction guess. Then the complete crafted attack network packet is shown below.

Fig 7.3.6 Crafting complete attack packet with modifying different attributes

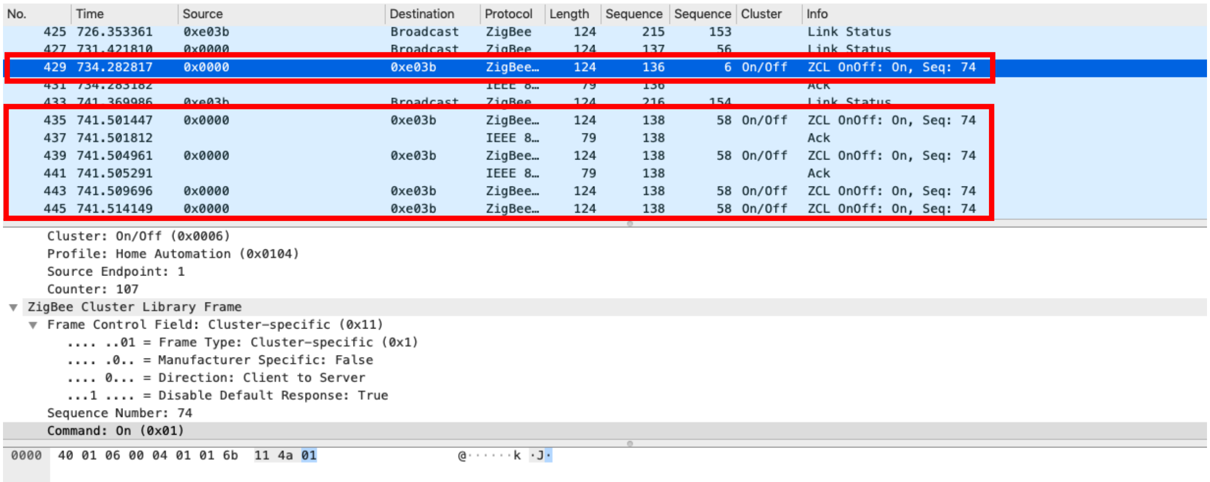

Fig 7.3.7 Sending crafting attack packet with modification of different attributes

Although the crafted attack network packet was successfully sent into the ZigBee network, the light bulb neglected the replay network packet and was not executed the attack command to switch ON.

From the above, the replay attack and unauthorized command injection attempts were not successful and caused no impact to the testing ZigBee smart-home devices.

7.4 IoT Security Best Practice Guidelines Self-Verification Checklist

As the various testing had been done from the above sections, a self-assessment checklist was conducted for the ZigBee smart-home environment setup, abstracting from HKCERT "IoT Security Best Practice Guidelines". Section 4.2.4.1 Wireless Security of the self-assessment checklist in "IoT Security Best Practice Guidelines" has included as below:

Self-Verification Checklists	Assessment Result
- Encryption is enabled in all wireless communications.	Yes. The communications between ZigBee devices have been encrypted with network key, and the exchange of network key from the beginning has been encrypted with the link key.
- Data is encrypted in application layer before transmission through wireless protocols without encryption features.	Yes. The ZigBee devices share the network key for encryption and decryption of data which being transmitted or received.
- Due to limited device computation power, content in wireless data stream is still secured from trivial eavesdropping with alternative encryption methods.	Yes. The network encryption standard in ZigBee technology are commonly supported within ZigBee hardware module, which is independent to the device computation power.
- User interaction is required in initial pairing process to avoid unintended pairing to unauthorised remote party.	Yes. There is pairing mode which is required to be enabled when pairing the ZigBee device into the network.
- Default wireless passphrase is only used once during initial pairing process and enforced to be changed for proceeding to normal service.	Yes. The pre-shared link key used only during the exchange of network key during the pairing process and a network key is randomly generated for the proceeding to normal operation in ZigBee network.

7.5 List of Reference Publications

No.	Publisher	Publication Name	Release Date
1	Cognosec	ZigBee Exploited – The good, the bad and the ugly https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/11/20081735/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf	Aug 2015
2	HKCERT	IoT Security Best Practice Guidelines https://www.hkcert.org/my_url/en/guideline/20011401	Jan 2020
3	Kudelski Security	ZigBee Security: Basics https://research.kudelskisecurity.com/2017/11/01/zigbee-security-basics-part-1/	Nov 2017

		https://research.kudelskisecurity.com/2017/11/08/zigbee-security-basics-part-2/ https://research.kudelskisecurity.com/2017/11/21/zigbee-security-basics-part-3/	
4	MIT	Security Analysis of Zigbee https://courses.csail.mit.edu/6.857/2017/project/17.pdf	May 2017
5	NXP	Maximising Security in ZigBee Networks https://www.nxp.com/docs/en/supporting-information/MAXSECZBNETART.pdf	Jan 2017
6	Silicon Labs	AN1233: Zigbee Security https://www.silabs.com/documents/public/application-notes/an1233-zigbee-security.pdf	Dec 2019
7	ZigBee Alliance	ZigBee Specification https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf	Aug 2015