NILE

BT 5.0 + ZB/Thread + NFC-A Standalone Module

ZigBee OTA upgrade client application note

Version 0.1

6141 Running Springs Rd
San Jose, CA 95135
www.ivativ.com

Email: info@ivativ.com
Ph: (408) 893 7812

Table of Contents

Table of Figures

1. Scope of the document

The following article shows how to securely upgrade ZigBee application OTA (over-the-air) using signed encrypted files. The process is tested with nRF nRF5_SDK_for_Thread_and_ ZigBee v3.2.0. This document explains the steps in DFU, keys generation, package preparation for a DFU.

2. Overview

2.1 Introduction

The ability to update the firmware of units already deployed in the field is a common requirement for many products. For example, it may be necessary to add new features into products after the first version has been launched.

Products that use ZigBee technology often designed to work with smart homes, bulbs or similar consumer electronic devices that are connected to the Internet. This makes it possible to implement OTA (Over-the-Air) firmware update capability without adding any extra cost or significant increase in the software complexity. The Internet of Things (IoT) also poses a challenge, because new types of devices and use cases are continually introduced, which can create unanticipated interoperability issues. For this reason, the ability to do OTA firmware updates is essential for any IoT device.

2.2 Security

Here we are using key, that key will be shared by the device and by the user. User need to add the key to his application which he is building. So when we do the update the device will check the key and accepts the incoming DFU request.

2.3 Reasons for firmware update

Firmware update needed for specific reasons like

For example, the ZigBee protocol under constant development, with different revisions of the protocol stack released over time. A revision may include new features, performance optimizations, and patches to bugs or interoperability issues. It may be desirable to use the OTA update procedures to change to the latest available stack revision, even if the user application itself remains unchanged.

2.4 ZigBee OTA process

Two entities participate in the ZigBee OTA Upgrade process

OTA Upgrade Client:

The OTA Upgrade Client runs on a target that is the device that is being upgraded, and is responsible for downloading and installing the new firmware. The OTA Upgrade Client incorporates a DFU controller that manages the DFU process. This means that each OTA target can be in a different state regarding the OTA process at a given point of time.

OTA Upgrade Server:

The OTA Upgrade Server is a server that provides a firmware image. The OTA Upgrade Server can be an example provided with this SDK, a standalone 3rd party device, or it can be instantiated as an nRF52840 DK in conjuction with the nrfutil utility.

Note: Assuming the reader of this document has been expertise in ZigBee. The reader should have hands on using the Nordic SDK for thread and ZigBee. The readers should have knowledge to install all the required tools by following the instructions in the link attached.

3. Requirements

3.1 Hardware requirements

- NILE DVK's – 3 Nos
- Windows PC
- Micro USB cables – 2 Nos

3.2 Software requirements

- nRF SDK
- nrfjprog tool
- nrfutil tool
- Jlink tool
- segger embedded studio
- micro-ecc

Note: All the tools and applications must be installed. Respective download links are attached herewith.

4. Test setup

Note: Assuming that the reader is well known with the nRF SDK and its applications. He should also know how to load image using the segger embedded studio. The PC should be installed with the nrfutil and nrfjprog tools.

Precondition: To test the ZigBee OTA Upgrade process, we need at least two NILE Development Kit boards. One of these boards will be an OTA Upgrade Server that distributes the new firmware. The others will play the role of OTA Upgrade Clients that are updated.

- Here the SDK refers to the nRF5_SDK_for_Thread and ZigBee v3.2.0
- Assume the 3 DK's named as
  - Client (OTA upgrade client)
  - Server (OTA upgrade server)
  - Router(coordinator)
- The client will be loaded with the MBR,bootloader, application
- The coordinator loads with the coordinator example
- The server does not need any firmware it's just act as a connectivity medium for DFU

Note: All the commands should be given from command line.

4.1 Procedure

1. After downloading the SDK for thread and ZigBee. Go to the path from command line SDK\examples\ZigBee\ota
2. Need to create keys for secure update. So follow the below commands from command line to generate the keys
   a. Create a private key:
      - **nrfutil keys generate priv.pem**
   b. Create a public key in code format and store it in a file named dfu_public_key.c:
      - **nrfutil keys display --key pk --format code priv.pem --out_file dfu_public_key.c**
   c. The generated keys will be in the path of SDK\examples\ZigBee\ota
   d. Copy the dfu_public_key.c file to SDK\examples\dfu\ by replace the existing file
3. Make sure that you are in the path of SDK\examples\ZigBee\ota
4. Build the bootloader by giving the command
   - **make -C bootloader\pca10056\blank\armgcc**
5. Prepare the ZigBee OTA upgrade client:
   a. Open the **main.c** file in the client folder. Add the following define in main.c
      - **#define OTA_UPGRADE_TEST_FILE_VERSION 0x01010101**
   b. Compile the ZigBee OTA upgrade client:
      - **make -C client\pca10056\blank\armgcc**
6. Make sure that you are in the SDK\examples\ZigBee\ota
7. Generate a bootloader settings hex file by using the command

- **nrfutil settings generate --family NRF52840 --application client\pca10056\blank\armgcc_build\nrf52840_xxaa.hex --application-version 0x01010101 --bootloader-version 1 --bl-settings-version 2 --app-boot-validation VALIDATE_ECDSA_P256_SHA256 --key-file priv.pem settings.hex**

8. Merge the client hex file and the bootloader settings file
    - **mergehex -m client\pca10056\blank\armgcc_build\nrf52840_xxaa.hex settings.hex -o dfu_client.hex**
9. You will observe the dfu_client.hex file in the SDK\examples\ZigBee\ota.
    a. Connect the Client DK to the PC and power on
    b. Erase the flash of the DK by using
        - **nrfjprog -f nrf52 --eraseall**
    c. Flash the MBR to the DK by using the below command
        - **nrfjprog -f nrf52 -r --program ..\..\..\components\softdevice\mbr\nrf52840\hex\mbr_nrf52_X.X.X.hex --chiperase**
    d. Flash the bootloader to the DK by using the below command
        - **nrfjprog -f nrf52 -r --program bootloader\pca10056\blank\armgcc_build\nrf52840_xxaa_mbr.hex**
    e. Led 2 will lit
    f. Flash the merged DFU client to the DK by using the below command
        - **nrfjprog -f nrf52 -r --program dfu_client.hex –sectorerase**
    g. Led 2 will off
10. Now prepare a package to load via OTA
    a. Modify the main.c file in the SDK\examples\ZigBee\ota\client. For example add the following line to the in main.c
        - **bsp_board_led_on(BSP_BOARD_LED_3);**
        - **bsp_board_led_on(BSP_BOARD_LED_1);**
    b. Increase the version. For example, change the **define OTA_UPGRADE_TEST_FILE_VERSION to 0x01020101.**
    c. Before compiling make sure that you are in the path of SDK\examples\ZigBee\ota
    d. Compile the modified client example
        - **make –C client\pca10056\blank\armgcc**
    e. Prepare a firmware package (in zip format) with the new firmware
        - **nrfutil pkg generate --hw-version 52 --sd-req 0x00 --application-version 0x01020101 --application client\pca10056\blank\armgcc_build\nrf52840_xxaa.hex --key-file priv.pem --app-boot-validation VALIDATE_ECDSA_P256_SHA256 app_dfu_package.zip --ZigBee True --ZigBee-manufacturer-id 123 --ZigBee-image-type 321 --ZigBee-comment good_image --ZigBee-ota-hw-version 52 --ZigBee-ota-fw-version 0x01020101**
    f. A image with the “007B-0141-01020101-good_image.ZigBee” will be generated in the path of SDK\examples\ZigBee\ota

Note: One can use any name in the place of the"good_image". It is the file name to represent the updated firmware package.

11. Prepare the ZigBee coordinator with the server DK
    a. Connect the server DK to the PC and erase the flash of server DK by using the following command
        - **nrfjprog -f nrf52 --eraseall**
    b. Load the application present in the path of **SDK\examples\ZigBee\light_control\light_coordinator\pca10056\blank\ses\ ZigBee_light_coordinator_pca10056.emProject**. Load that application using segger embedded studio.
    c. Now the server DK becomes the coordinator of the ZigBee network, As it seems that LED3 lit.
    d. The Router will become the coordinator of the network by LED3 lit.
    e. Power of the client. You see that coordinator will add the client into ZigBee network that can be observed by LED3 will lit on client.
    f. Do not power off coordinator and client DK's
12. Use **nrfutil** to run the DFU
    a. Connect the server DK to the PC. This board serves as the connectivity IC to the ZigBee network. This board does not require installation of any firmware. It will be flashed by nrfutil.
    b. Run the following command to start the DFU process over ZigBee, where 608123456 in the following command is the serial number of the ZigBee OTA Upgrade Server for the Development Kit, and 11 is the 802.15.4 channel number:
        - **nrfutil dfu ZigBee -f 007B-0141-01020101-good_image.ZigBee -snr 608123456 --channel 16**

        Note: If the DFU does not happen, try with the channel number 11. For more info go through this link
    c. The update take couple of minutes

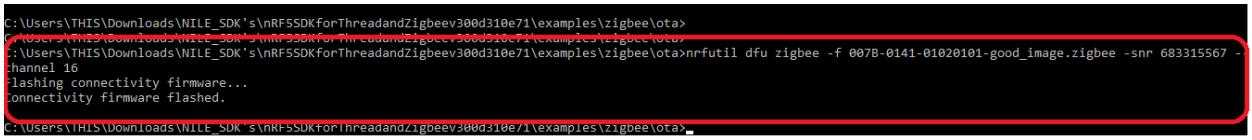

Figure 1: Status of OTA update

13. The status will be seen while starting the DFU process
14. While the DFU is happening, on server DK LED2 & LED3 will lit. And LED 4 will lit alternatively which says DFU is in progress.
15. This take nearly 20-30 minutes for update
16. Nothing we get when the DFU is in progress. We need to wait for the new application to load into the client and observed the difference.
17. After completion of DFU the device resets and runs the new application LED1 and LED3 will lit.
18. Thus the ZigBee OTA update is completed
19. Follow the below links in the chapter 6 for more info

5. Test reports

Observed that the ZigBee client is updated with the new application via OTA. With the help of ZigBee server.

6. References

Info center - https://infocenter.nordicsemi.com/index.jsp

Nordicsemi – https://www.nordicsemi.com/

Nrfutil - https://github.com/NordicSemiconductor/pc-nrfutil

Devzone: https://devzone.nordicsemi.com/nordic/short-range-guides/b/software-development-kit/posts/ZigBee-getting-started-device-upgrade-ota