CS 490 / ECE 492: Embedded Systems Security

Zigbee Personal Area Networks #08

Total Points: 100

Assigned Date : Monday, April 11, 2016
Due Date : Monday, April 18, 2016 @ 11:59:59 a.m. [**Group assignment**]

1 IEEE 802.15.4 Wireless

The IEEE 802.15.4 standard defines a low level wireless protocol for personal area networks. A number of vendors have built wireless technologies on top of this standard, ie. Zigbee (mostly consumer level), WirelessHART (mostly industrial) to improve configuration, reliability, and security. The protocol has use cases similar to the nrf24L01 radios, ie. low power, close range, intermittent communication between embedded devices. It can use either the 900 MHz (in U.S) or 2.4 GHz (worldwide/US) spectrum. Similarly, it has two topologies, peer-to-peer, where two radios communicate directly, and mesh network, where communication can flow from any devices participating.

Zigbee especially is considered as an enabling technology for the Internet-of-Things (IoT). Many "smart" devices utilize Zigbee for much of the low level communication between device and a "hub", sometimes called an IoT gateway. Zigbee does have the advantage of supporting built in, 128-bit symmetric key encryption for security. However, issues of key storage and distribution can still be problematic (ie. is the key hard coded in the firmware? How can new devices be trusted to participate in the mesh? Are devices with the key implicitly trusted?)

Regardless, we would like for you to gain some experience with the protocol. For this lab, we would like for you to construct an IoT gateway using your BeagleBone Black and some Digi Xbee radios. We are using Digi XBee Series 1 radios that have a range of about 100 ft. The datasheet for them is here: `https://www.sparkfun.com/datasheets/Wireless/Zigbee/XBee-Datasheet.pdf`. The XBee radios use UART for communication between the device and a host. Connect the Xbee radio to your BeagleBone as following:

- VCC to a 3.3 V supply (either P9_3 or P9_4)
- GND to digital ground (either P9_1 or P9_2 or any other GND)
- DOUT (TX) on the Xbee breakout board goes to RXD (P9_11) of UART4 on the BeagleBone
- DIN (RX) on the Xbee goes to TXD (P9_13) of UART4 on the BeagleBone

You will most likely have to load the overlay for UART4 to be active, but once it is, you can connect to it using /dev/ttyO4 as the serial device. Use minicom (or any serial port program) to talk to the device, which by default uses 9600 baud, 8 bit, no parity, 1 stopbit, no hardware flow control, no software flow control as the serial parameters. If you are connected, you should be able to type "+++" in minicom and see a response of OK.

Partner with another group in lab. Use the web interface you already have configured (You can plug the BBB directly into the router if that helps). When someone goes to your web interface, you should, through the Xbee radios, be able to control your partner group's motor or read their temperature sensor. Your communication should be encrypted. Think carefully about how you store the key, you will be required to explain the adavantages/disadvantages of your key management.

Deliverables

The due date of this assignment is **Monday, April 18, 2016 @ 11:59:59 a.m.** A dropbox will be opened for submission on Moodle before the due date. You are required to detail your findings in a report. All reports must be in **PDF** format. No exceptions.

- [**50 points**] A group demo of your work. We will again ask you questions on what you've done and how you've done it.

- [**45 points**] A group report with the followings:
  - Motivation and objective of the experiment.
  - A detailed methodology of your experiment. You must be able explain the commands, tools, procedures you've used. Don't simply list the commands. We want you to explain what you've done and why you did it. Screenshots highly recommended.
  - A detailed testing plan and test results.
  - Justification of your observations. You must be able to justify and/or argue why (or why not) your method worked.
  - Final conclusions.
- [**5 points**] An individual report. Use this report to explain your individual contributions towards the experiment. This is a separate writing on your own. In essence, both members of the group will write their own individual report and make their own submission; you are only required to submit one group report. You can use the individual report to explain/mention/complain about your teammate's contributions to the project as well.