SY310 – Lab III – Second Half (Wireless Cyber Attack with XBees)

R

Objectives:

1) To give the student an idea of what type of system data can be viewed and modified within a wireless networked control system.

2) To demonstrate the source and function of control system data.

Scenario: A power plant uses a networked controller to adjust a cooling system. The temperature must remain between 220 °F and 240 °F. If the plant temperature drops below 220 degrees, the cooling system stops functioning and the plant goes off line. If the temperature rises above 240 degrees, the cooling system overheats and the damage occurs.

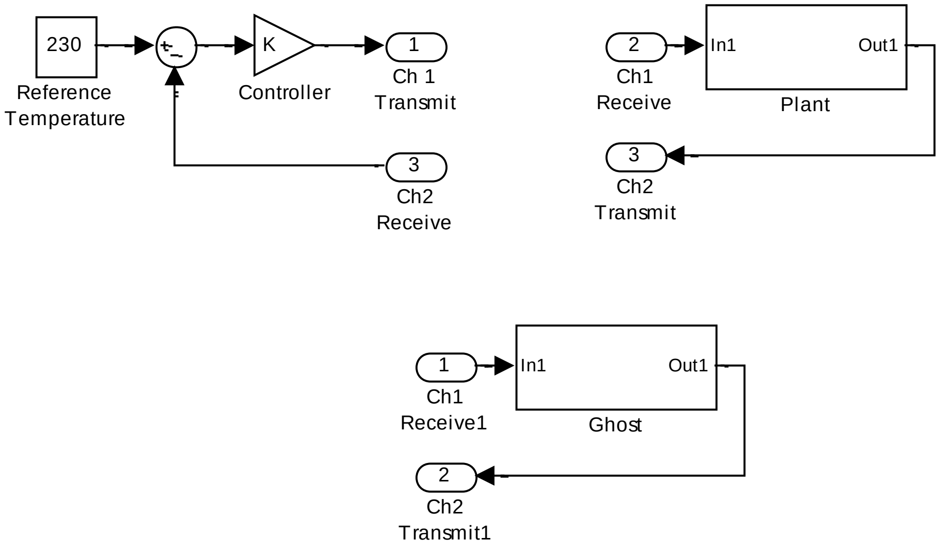


Figure 1. Communications architecture between the controller, the plant (on the same laptop) and the ghost (on an external laptop). Each communication module shown represents an XBee. .

A control systems schematic of the system is given in Fig. 1. The cooling system in this power plant is controlled by hydraulic valve. The controller simply turns the coolant flow on and off. If the coolant flow is left on too long, the plant temperature will drop below 220 °F and the plant will shut down. If the coolant flow is left off too long, the plant temperature will rise above 240 °F overheating the plant and cause it to go critical. There is a sensor located within the plant which transmits the temperature on "channel 2". Upon receiving the temperature, the controller sends a simple command of 'O' for open on "channel 1" to turn on the cooling, and 'C' for closed to turn it off. The control system law within the controller computes the proper coolant flow timing in order to maintain a desired temperature of 230 °F.

This is a partner lab:
One student will have 2 XBees communicating on one laptop (controller and plant).
The other student will have 1 XBee on another laptop (ghost).

Hardware and software used: This exercise will use **one MatLab** program and **two XBees** (wireless communication devices) to form a power plant control system on **one laptop**. One part of the MatLab program will function as the controller and the other part will function as the plant (cooling system). Each part of the software will present a graph (Figure 1 and 2) displaying the temperature they perceive the power plant to have. The XBees will provide a "two-channel" network that allows the two pieces of the program to communicate. The goal of the exercise is for the student to investigate the communications that take place on the network and explore potential cyber-attacks which could make the power plant overheat and go critical. To achieve this goal, the student will use a **third XBee** (ghost) and a terminal (X-CTU) program on **another laptop** to hack the system and introduce errant commands and measurements.

Fig. 2 shows the physical configuration of the system. The two parts of the MATLAB program, the controller and the plant (i.e. the cooling system), are embedded in the given hardware and will not be changed by the students. Reminder instructions on how to use the terminal program are provided in the appendix and will be most useful to ensure the XBees communicate with each other.

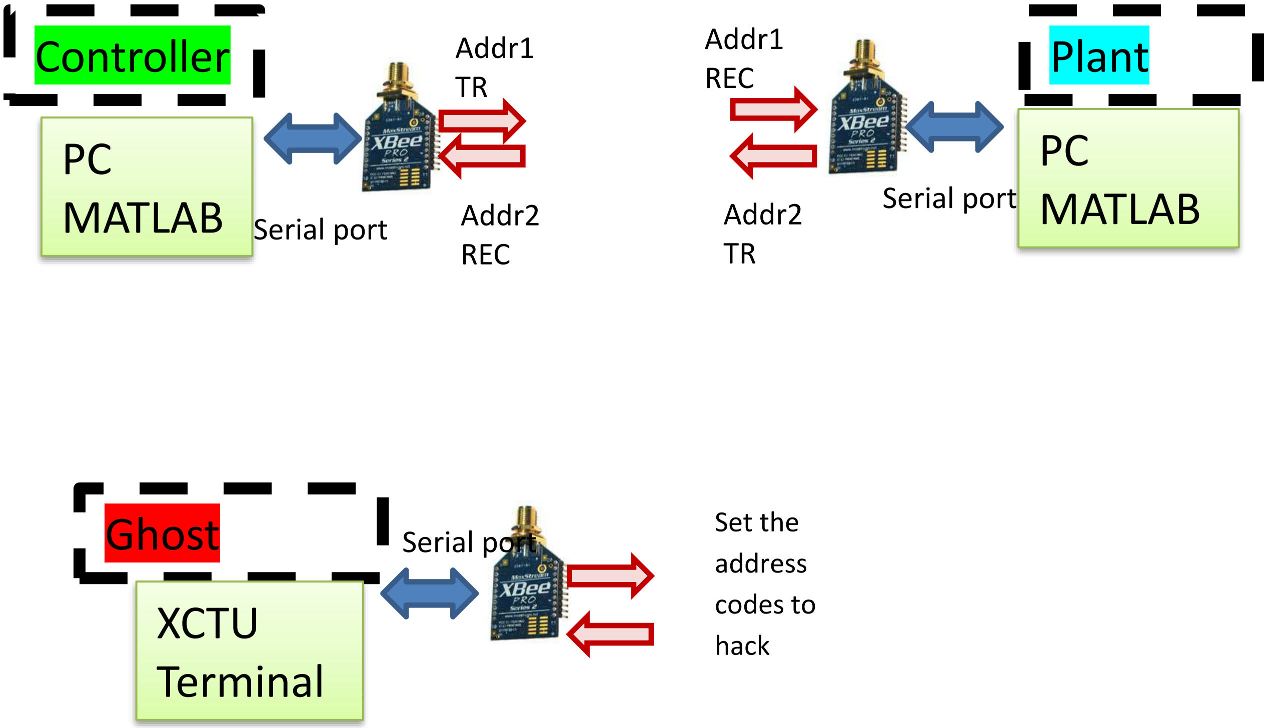
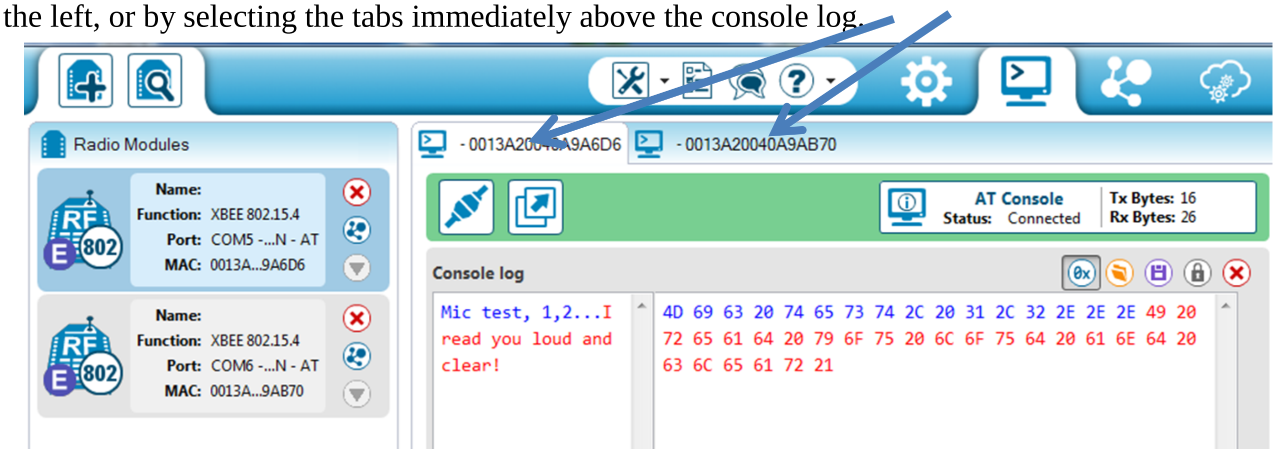


Figure 2. Physical architecture of the controller and the plant XBees(on one laptop), and the ghost XBee(on a second laptop)

<u>Procedures: (Both partners should be involved in every part of the lab, regardless of which laptop is being used for which part)</u>

Part 1: Set up Laptops and XBees, check communication, and configure the Power Plant
We'll first set up Laptop #1 with the controller and plant XBees, and then set up Laptop #2 with the ghost XBee.

1) Your instructor will provide three XBee's and assign two addresses to each team. **You decide** which address you want to assign to the controller XBee and the plant XBee and write them below. (You'll fill in the COM port numbers later.) Note that the ghost XBee will spend it's whole time impersonating other nodes, so we don't need to assign it a unique address.
controller XBee address: ______ and COM port:________
plant XBee address:_______ and COM port:________
2) Start XCTU and **follow the procedures from SX23** to connect one XBees on Laptop #1.
   a. Configure this XBee to be the controller XBee, i.e. set the MY address to be the controller address you assigned above, and DL to be the plant.
   b. In the section of the XCTU interface that shows the Radio Modules, note the COM number that is listed at the beginning of the Port assignment (i.e. "COM5-…"). Write the COM number in the space above.
3) Connect a second XBee to another USB port on Laptop #2, and follow steps (a) and (b) above to configure the plant XBee with the proper MY and DL addresses. As before, note the COM port and fill in the blank above.
4) Click on the terminal tab at the top of the XCTU interface. This will provide you with a terminal interface for each of the XBees, and you can switch between them by either clicking on the radio module icons on the left, or by selecting the tabs immediately above the console log.



```
Mic test, 1,2...I    4D 69 63 20 74 65 73 74 2C 20 31 2C 32 2E 2E 2E 49 20
read you loud and    72 65 61 64 20 79 6F 75 20 6C 6F 75 64 20 61 6E 64 20
clear!               63 6C 65 61 72 21
```

5) Write some test messages in each terminal to ensure that you can communicate between the controller XBee and the plant XBee. (Refer to **the procedures from SX23** if you don't remember how to do this.)
6) On Laptop #2, use XCTU to configure the ghost XBee with the same addresses as the controller (i.e. the ghost XBee is impersonating the controller.) Make sure that the ghost receives any information sent by the plant XBee and that anything the ghost sends is received by the plant. **Important: You cannot change the XBee address information while other XBees are transmitting data.**
7) Change the ghost addresses to impersonate the plant, and make sure that the ghost can send and receive with the controller.

8) After you convince yourself that you could assume the identity of either the plant or the controller, make sure you **close both of their COM ports** by clicking on the disconnect icon (i.e. the one that looks like a power plug). Leave the ghost XBee connected and configured as the plant.
9) On Laptop #1 (i.e. the laptop with two XBees), copy the MATLAB program **PowerPlantupdatedApr2015.m** from U:\Cyber2\EC312\SX24 to a location on your computer.
10) Open **PowerPlantupdatedApr2015.m** with MATLAB, and **edit lines 4 and 5** to reflect the appropriate COM port numbers that you noted in step 1. Then save the file.

Part 2: Eavesdrop on plant- controller communications to formulate first attack strategy.

In order to formulate our cyber attack strategy, we first need to gather some information. We can do that by configuring the ghost to passively listen in on the communication between the controller and plant. Since we already have the ghost configured to impersonate the plant, we'll start out with that.

Question 1: Circle the correct item in each of the bold pairs in the following sentence: "When the ghost is configured to impersonate the plant (i.e. the cooling system), it should expect to receive (**temperature data/controller commands)** and have the ability to send (**temperature data/controller commands)**".

1) On Laptop #1, execute the MATLAB program you previously saved by clicking the Play button.
2) You will see **two plots on top of each other** (move them to see both), Figure 1 is the controller's view of temperature and its response, Figure 2 is the actual temperature sensed by the plant.
   a) If you need to stop the MATLAB program prematurely, type Ctrl-C in the command window. If you do this, you will have to **restart MATLAB before you can run the file again. Also, if you receive MATLAB errors, first check to make sure your X-CTU COM ports are closed on Laptop #1.**

Question 2: Briefly describe the behavior of the power plant cooling system as observed from the MATLAB graphs that are displayed.

3) On Laptop #2, the ghost should be receiving information in the XCTU terminal based on its eavesdropping. Use this info to answer the following question.

Question 3: What type of data/information is the ghost receiving? Approximately how often does new data arrive? What two bytes (i.e. four Hex digits) are included at the end of each transmission?

Part 3: Perform Attack #1 to cause the plant to overheat and go critical.

Question 4: Based on your answer to questions 2 and 3, describe how the ghost could execute a cyber attack to cause the plant to overheat and go critical.

Question 5: Implement the attack you described in your answer to question 4. *Note: You may find it helpful to use the "Send Sequence" option rather than trying to send single packets.* When you have achieved critical reactor overheating, **show your instructor the results and have them sign off on your answer sheet.**

Part 4: Eavesdrop on controller- plant communications to formulate second attack strategy.

1) Adjust your ghost XBee transmit/receive addresses to match those of the XBee connected to the controller. You have now taken on its identity.

Question 6: Circle the correct item in each of the bold pairs in the following sentence: "When the ghost is configured to impersonate the controller, it should expect to receive (**temperature data/controller commands)** and have the ability to send (**temperature data/controller commands)**".

2) On Laptop #2, the ghost should be receiving information in the XCTU terminal based on its eavesdropping. Use this info to answer the following question.

Question 7: What type of data/information is the ghost receiving? Approximately how often does new data arrive? What two bytes (i.e. four Hex digits) are included at the end of each transmission?

Part 5: Perform Attack #2 to cause the plant to overheat and go critical.

Question 8: Based on your answer to questions 7, describe how the ghost could execute a new cyber attack to cause the plant to overheat and go critical.

Question 9: Implement the attack you described in your answer to question 8. When you have achieved critical reactor overheating, **show your instructor the results and have them sign off on your answer sheet.**

Part 6: Understanding questions

Question 10: Which of the IEEE standards does XBee communication fall under?

Question 11: In both of your cyber attacks, an XBee was receiving communication from two other XBees at the same time (i.e. from the ghost and from either the controller or the plant, depending on who was being attacked) and there are bound to be collisions between packets. Use Google to find out how XBee handles collisions between nodes. (Note: Your answer to Question 10 may help.) **Provide both the name and a short description of the approach for handling collisions.**