SY488A Lab III

Wireless Communication

(Communicate, Intercept/Decode, Attack)

Introduction: This multipart lab will use a programmable radio module to communicate between computers, intercept and decode wireless communications and then attack a vulnerable industrial control network. The deliverable for this lab is filled in answer sheets.

Background: Today we'll be setting up small programmable radio modules called XBees (http://www.digi.com/xbee/). Parts 1-4 will focus on initial setup and communication test, followed by an exercise involving receipt and analysis of a message with Hamming encoding.

Students will be working in pairs. Each will need a laptop. Once software installation is complete, the instructor will provide each student with an XBee kit.

Part 1: Software Installation

Before we can use the Xbee wireless nodes for communication, we have to set up some software. DO NOT PLUG YOUR XBEE INTO THE USB PORT PRIOR TO INSTALLING THE SOFTWARE AND USB DRIVERS.

1.Installing X-CTU Software

X-CTU is freeware which provides a nice graphical interface for our Xbee wireless nodes. If you have not already installed the software prior to class, you will need to do the following:

- Copy the two installer files located on the course website to your Desktop. (You can also download the X-CTU software from http://www.digi.com/xctu.)
- Double-click on the XCTU installer file and follow the prompts to install the software on your computer.

2.Installing USB Drivers

Now we'll install the USB drivers for our XBee.

- Right-click on the other installer file (Install-Parallax-USB-Drivers-v2.08.24.exe) that you copied over from the course website and select "Run as Administrator".
- A window will pop up during installation and automatically close when the process is complete.

3.Setting up your XBee

- Once you've completed the software installation, your instructor will provide you with one Xbee kit, which consists of an XBee Module (Assembled) and a USB cable.
- Carefully take the packaging of your XBee kit.
- Now plug your USB connector (Xbee cable and connectors) into your laptop.
- The XBee USB interface board is a "plug-and-play" device that should be detected by the PC automatically. The USB drivers should automatically install and a notification will

appear in the lower right portion of your screen indicating success or failure (i.e. "Your device is ready to use.")

- If the USB drivers fail to install, and you had successfully installed the parallax drivers, please ask your instructor or tech to help you.

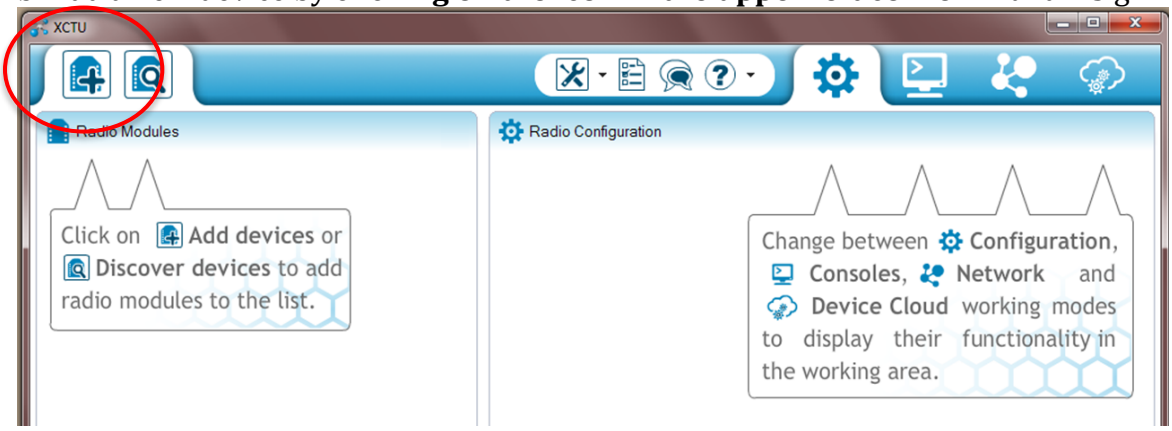
Part 2: Test Communications Link and Establish a Network

1.You will need to establish a connection with the X-CTU software:

a. Double-click the X-CTU shortcut on your desktop. The initial screen should look like the figure below.

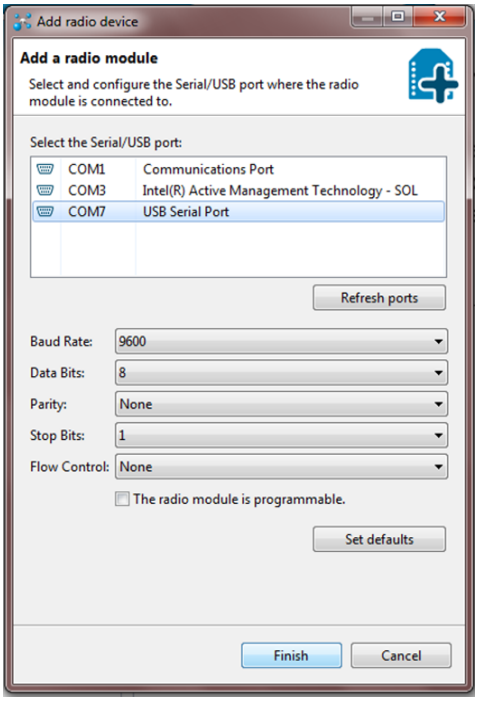
NOTE: If at any time in this set-up process you get a pop-up that says "Windows Firewall has blocked some portions of this program", just click on Cancel and keep going.

b. Add a new device by **clicking on the icon in the upper left corner** with a + sign.



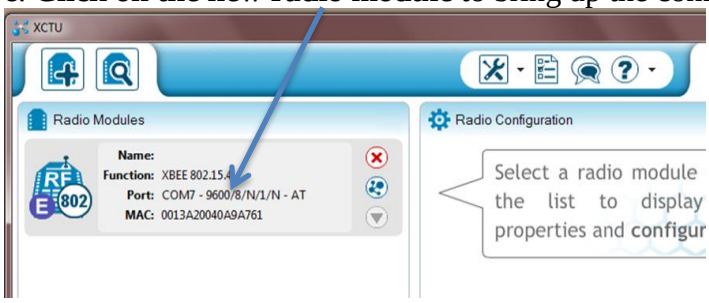
c. This will bring up a popup like the figure shown to the right. **Select the COM port that says "USB Serial Port". Verify** that the baud rate and data settings match the internal settings of the devices:

- Baud Rate: 9600
- Data Bits: 8
- Parity: NONE
- Stop Bits: 1
- Flow Control: NONE

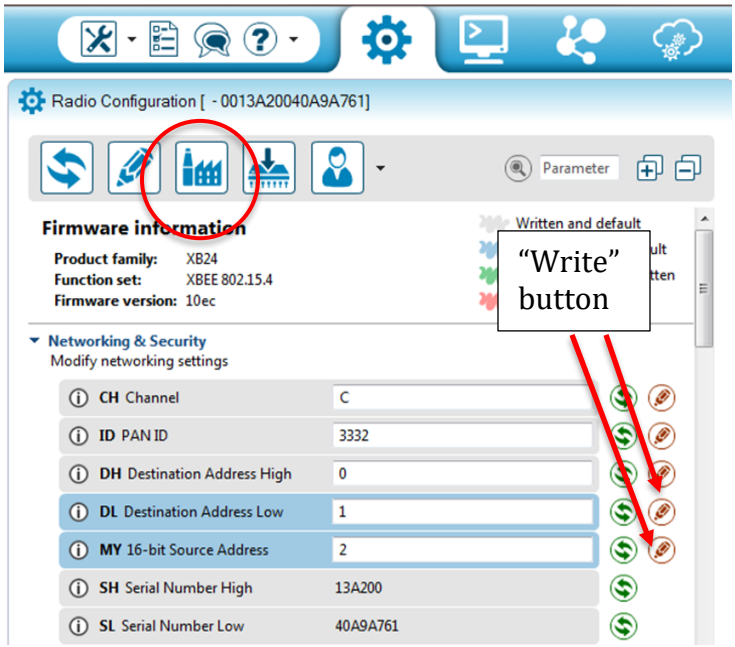


d. **Click Finish** to add the radio module. A pop-up will be displayed showing status and some basic information. If the Communication with the modem is OK, you will see a display like the figure below, with the XBee's port, MAC address, etc.

e. **Click on the new radio module** to bring up the configuration screen.



f. You should see the configuration interface shown in the figure to the right. First, **reset the XBee to its factory default settings** by clicking on the third icon from the left (circled in the figure).



g. Your instructor will assign each pair of partners one of the following number pairs. **Circle the pair** that you have been assigned:
1,2; 3,4; 5,6; 7,8; 9,10; 11,12; 13,14; 15,16; 17,18; 19,20; 21,22; 23,24;
Your partner will take one of the numbers in the pair, and you will take the other. Write them here:
My address: _____
Partner's address:_____

h. To set your XBee up to communicate with your partner, we will need to change the following fields:
- **DL** – Destination Address Low (i.e. the address of the node you want to send to).
- **MY** – 16-bit Source Address (i.e. the address you want to assign to your own node).
In the **DL** field, type your partner's address (from the pair of numbers you selected). In the **MY** field, type your address.

i. Note that no changes are actually made to the XBee until we tell the software to implement the changes we just made. **Implement the changes by clicking on the "Write" button to the right of the DL field and to the right of the MY field.** (The Write button looks like a pencil or screwdriver (circled in the figure above). You can always check whether your changes have taken effect, by clicking on the "Read settings icon" which looks like this: 

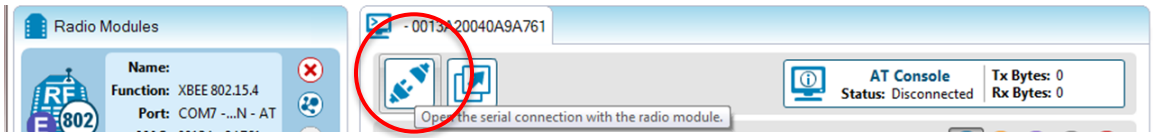
Note that you will be on the same Personal Area Network ID as your partner and all of your classmates, and you all will also be on the same channel (C), which means you will be using the same frequencies.

Part 3. Communicate

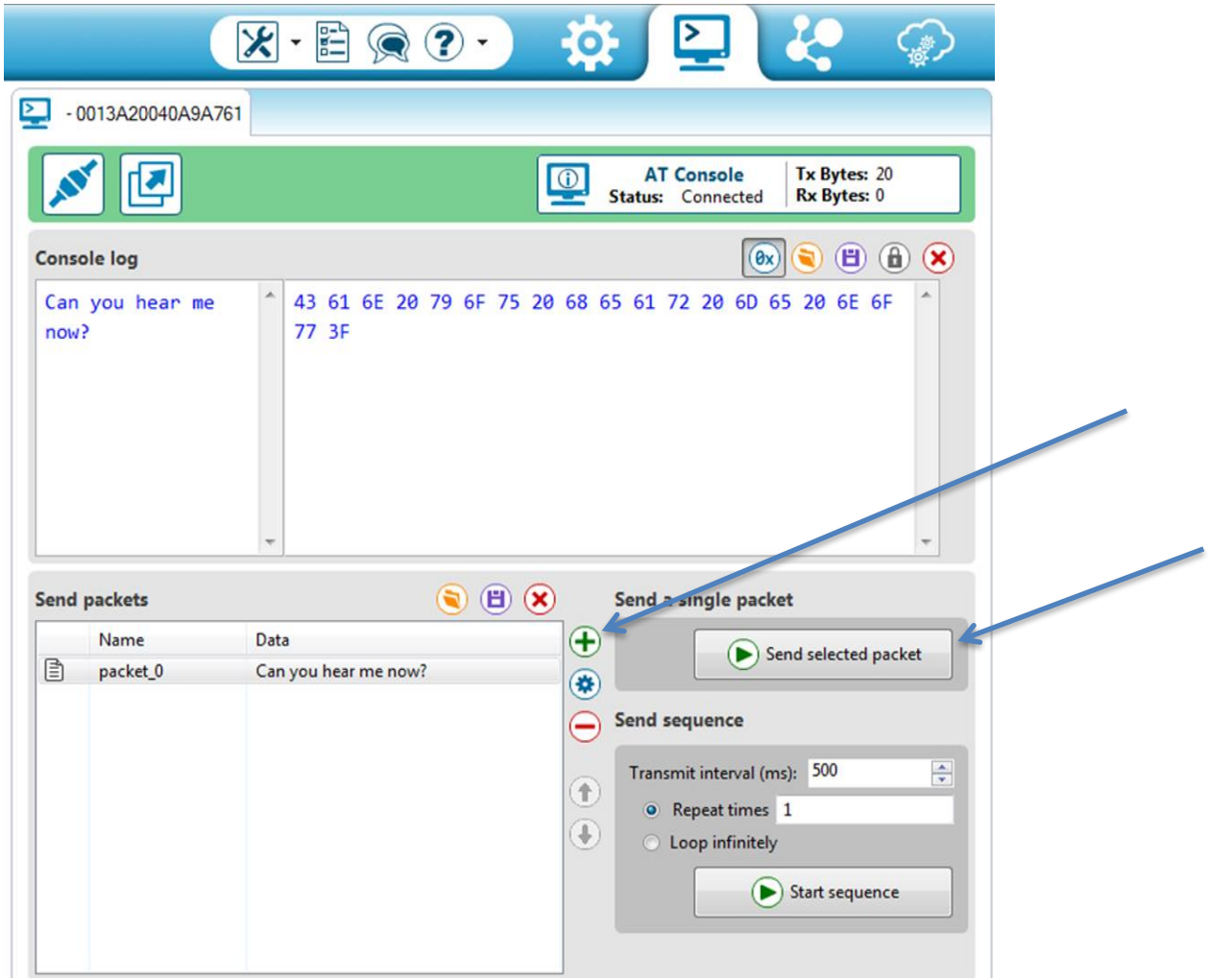
1. Transmit and receive data from point to point

a. **Select the Terminal tab** at the top of the screen, which looks like the figure to the right. In the upper right, you should see that the Console status says "Disconnected".

b. Establish a serial connection with the radio module by **clicking on the icon that looks like an electrical plug**, circled in the figure below. You should see the Status change to "Connected".



c. **Create a message** to send to your partner by clicking on the plus sign in the bottom portion of the screen. This will bring up a field that allows you to write a message in ASCII or in Hex. Once complete, you can send the message to your partner by **clicking on "Send Selected Packet".**



d. **Demonstrate to your instructor or lab tech**, and have them sign off on your answer sheet (**Question 1**).

Part 4. Intercept and Decode

Remember that *wireless communication is inherently insecure*. Your instructor is also using an XBee with ID 29, and they are trying to send a secret message to their fellow instructor with ID 30. Your goal is to intercept and decode that message.

Question 2. Based on the information above, circle the correct item in each of the bold pairs in the following sentence: "To configure your XBee to eavesdrop on the instructor's transmissions, you should set your **DL/MY** field to read **29/30**."

1. Configuring the XBee for eavesdropping.

a. **Disconnect your serial connection** by clicking on the same icon you clicked on earlier to establish the connection (i.e. the one that looks like a plug).

b. **Go back to the configuration page** by clicking on the icon that looks like a gear at the top of the page.

c. **Implement the changes from your answer to question 2**, and make sure you write them to the XBee by clicking on the Write icon next to each field that you modify.

2. Intercepting and decoding the message.

a. Go back to the **terminal page**, and **reconnect the serial connection** that you disconnected in the first step of the previous section.

b. You should see a 3-letter message being transmitted by your instructor, which repeats every few seconds.

FOR THE FOLLOWING QUESTIONS, SHOW YOUR WORK ON YOUR ANSWER SHEET.

Question 3. What is the ASCII message that your instructor is sending? _____

Question 4. What is the binary representation of the message your instructor is sending?

Question 5. Suppose your instructor is actually attempting to send 19 bits of message data and wants to use Hamming encoding. How many Hamming bits will he/she need?

Question 6. It turns out that your instructor is using Hamming encoding. Based on the methods you learned in the lecture today, determine whether there was a bit error in the transmission. If so, what is the bit position of the bit with the error? Verify your answer with instructor before proceeding.

Question 7. Once you correct any bit errors found in Question 6, what would be the original 19-bit binary message which the instructor was trying to send?

Question 8. Suppose you found out that the first three bits (i.e. the most significant bits) of the 19-bit binary message were just a preamble, and the last 16 bits were the real ASCII message. What was the ASCII message the instructor was sending?

Question 9. Send your instructor a message with your name followed by the two-letter ASCII message you intercepted from him/her.