■ ECE/CS 4984: Wireless Networks and Mobile Systems ■
At-home Exercise 2 (E2)

Part I – Objectives and Lab Materials

Objective:

The objectives of this at-home exercise are to:

- Introduce you to the operation of a wireless LAN in infrastructure mode.
- Illustrate the effect of distance to the access point on throughput.
- Study the effect of co-channel interference on the performance of 802.11b.

After completing the assignment, the student should be able to:

- Set up an infrastructure network consisting of multiple nodes and an access point.
- Measure the throughput and evaluate the range of the wireless devices.

Hardware to be used in this lab assignment:

- Dell Notebook
- Compaq iPAQ
- Xircom 802.11b Ethernet adapters
- Intel Wireless gateway.

Software to be used in this lab assignment:

- Client-server throughput measurement tool developed by Agnes Tan (Documentation included in the folder: C:\WMSD\Tools\Agnes)
- vxUtil on iPAQ

Part II – At-home lab assignment

You are expected to perform the following tasks:

- Reading Assignment- A document describing the throughput measurement tool before starting on the experiments, available on the course website and in C:\WMSD\Tools\Agnes.

In class, we set up an infrastructure network using IEEE 802.11a. Similarly, you will set up an infrastructure network using IEEE 802.11b. The first step is to configure the Intel wireless gateway.

- Configuration of the 802.11b wireless gateway

    1. The process is similar to configuring the 802.11a access point as shown in class. Connect the Ethernet card to the Intel wireless gateway using the red cross-over cable. Enter 192.0.2.2 as the IP address for the 10/100 Ethernet card on the notebook. Open Internet Explorer and enter the default IP address 192.0.2.1 for the Intel wireless gateway in the address bar. When the

configuration pages appear, click on "Setup Wizard" tab. A pop-up window will appear asking for username and password. The username is "Intel" with "I" in upper case and the default password is "Intel". Click on the wireless settings tab and enter SSID as "wmsd*groupnumber*" where *groupnumber* is the number assigned to you.

Note: You may need to reset the configuration of the Intel wireless gateway using the following procedure: with the power on, use a paper clip or similar object to press and hold the RESET button down for five seconds and release it. After about one minute, the gateway complete the reset procedure. The status light flashes during the reset.

2. Under the "Wireless Setting" tab, set the encryption algorithm to 40-bit and set the WEP key to "ABCDEF4984." Save the current changes by clicking on the Save/Next button and proceed to Function Settings. Use RF channel 11 for the access point.

3. Under "Function Settings" select the "Use the access point as a wireless router and access point" option and enter the internal IP, as *198.69.groupnumber.1*.This IP address is the internal LAN address of the access point. Only the internal nodes associated with the access point know it. Note down the LAN MAC address of the access point. This can be obtained by viewing the "Device Information" tab.

4. Dynamic Host Configuration Protocol allows automatic assigning of IP addresses to the clients from a DHCP-enabled server. Enable the *DHCP* server setting under the "Advanced Settings" tab and enter the valid range of IP addresses (*198.69.groupnumber.2-198.69.groupnumber.50*) that will be used by the wireless gateway to allocate to the clients. Save and restart the gateway by clicking on the Save and Restart button.

5. While the access point is restarting, change the IP address assigned to the 10/100 Ethernet card from 192.0.2.2 to *198.69.groupnumber.2* and the subnet mask to 255.255.0.0. The default gateway address can be set to 198.69.*groupnumber*.1.

6. After the access point has restarted, the configuration window will reappear on the screen. Check whether the settings have changed. If the changes made are successful, remove the red cross-cable and insert the Xircom WLAN card.

- In order for the Xircom card to continue being associated with the access point, it will need to have encryption enabled; the SSID also needs to be changed. Insert the Xircom WLAN card to the card slots. Open the Xircom Client utility on the notebook and select menu Commands> Edit Properties. Change the first SSID to "wmsd*groupnumber*." WEP can be enabled on the card by clicking on the "Network security tab" and checking the "Enable WEP" option.

- In order to set the WEP key, open the Xircom Client Encryption Manager. Enter password as Xircom. Click on Commands>Enter WEP key and set the WEP key 1 to "ABCDEF4984." The WEP key is fixed for all sessions with the access point. Check the "persistent" button in the client manager.
- Check whether the card is associated with the access point by checking the IP address obtained. The IP address in Windows can be checked by using the *ipconfig* command. Type *ipconfig /?* in the command window to display the options associated with the command. Use *ipconfig* command and report the IP address obtained by the card.

After setting up the access point, you will evaluate network performance by measuring the link throughput using a client-server utility.

- You must first configure the iPAQ to enable it to communicate with the wireless access point. Read the document iPAQ.pdf (available on the Blackboard course web site).
- With the iPAQ connected to the notebook and a connection established with Active Sync, copy the IEEE 802.11b driver file (CWESA11xxPPC30v150.cab) from C:\WMSD\iPAQ to My computer>Mobile Device>My Pocket PC folder on your notebook.
- To install the driver, go to Start>Programs>File Explorer>My device on the iPAQ and double click on the CWESA11xxPPC30v150.cab file. This will install both the Xircom client utility and the driver.
- Insert the iPAQ into the dual cardbus sleeve and insert the Xircom WLAN card in one of the slots.
- To set up the card, go to Start>Programs>Xircom and click on the Xircom client utility. Enter the SSID as wmsd*groupnumber* and set the Infrastructure mode field to "Yes." Set the WEP field to "Enabled." Set the transmission power to 1mW.
- In order to set the WEP key, open the Xircom Client Encryption Manager on the iPAQ. Enter the password as "Xircom". Click on Commands>Enter WEP key and set the WEP key 1 to "ABCDEF4984." The WEP key is fixed for all sessions with the access point. Check the "persistent" button in the client manager.
- Remove your Xircom card from the card sleeve and re-insert it for the settings to take effect.
- Set up an infrastructure network consisting of the notebook, iPAQ and the Intel Wireless Gateway. Check whether the network has been set-up by noting the IP addresses assigned to the nodes. On the iPAQ, the IP address obtained can be determined by using the vxUtil.

- To install vxUtil on the iPAQ, start Microsoft ActiveSync program, select the menu Tools->Add/Remove Programs. Make sure that "Cambridge vxUtil" is checked and click the OK button. To use the utility on iPAQ, go to Start>Programs>Communication. Click on vxUtil to start the utility. The utility can be used to initiate a ping session, start a traceroute operation or to obtain the IP address of the iPAQ. Use the Info function located at the bottom of the iPAQ screen to obtain the IP address of the iPAQ.
- After the network has been set up, copy the throughput measurement client from C:\WMSD\iPAQ\Agnes\client.exe to My computer>Mobile Device>My Pocket PC folder. Start the throughput measurement client application on the iPAQ and the server on the notebook. Go to Start>Programs>File Explorer>client on the iPAQ to start the client. The server can be started by going to My computer>C:\>WMSD>Tools>Agnes>server on your notebook. Ensure that the transmission power for the cards on both nodes is set at 1mW.
- Configure the client to transmit 5,000,000(5 million) bytes of UDP data to the server by clicking on the configure button of the client. Enter the IP address of the server in the host field. Select UDP protocol and set the total number of bytes to send as 5,000,000 bytes. Note down the received throughput at the iPAQ and the number of packets lost. Perform this procedure three times and report the average throughput obtained. Also report the signal strength at the iPAQ for the duration of the connection. The signal strength at the iPAQ can be observed by viewing the Xircom Link Status meter in Start>Programs>Xircom. Capture a snapshot of the server window that lists the throughput values for each instance. Include this snapshot along with your results in the lab report.
- Repeat the same with 10,000,000(10 million) bytes of UDP traffic and note the difference in throughput. Take a screenshot of the server window on your notebook and include it in your lab report.
- Now change the location of the iPAQ by moving to another room or behind some walls and repeat the above two steps of transferring data. Monitor the signal strength and report whether there is any change in the number of packets received. Capture a screenshot of the throughput values as reported at the server (notebook) for the three different readings and include it in your report.

Since 802.11b operates in the 2.4GHz unlicensed ISM frequency band, there are other potential sources of interference such as Microwave ovens. These devices interfere with the 802.11b signals leading to

attenuation of the signal strength thereby causing packet losses. We will determine quantitatively the interference of a microwave oven with the operation of a WLAN.

- Now move to a location in your current environment such that there exists a microwave oven in the path between the client and the server. Turn the microwave device 'on' and start transmitting 5,000,000 bytes of UDP data from the client to the server and note down the throughput and the number of packets lost. Repeat the transfer two more times and note down the average throughput and number of packets lost.
- Perform this procedure for different channels of operation for 802.11b. To change the channel of operation select the appropriate channel from the access point configuration page. Select a different channel of operation and repeat the procedure of data transfer of 5 Million bytes as in the above step. Note the average throughput and the number of packets lost, if any. Perform this for channels 7, 9, and 11 and note the channel/frequency at which you observe more packet losses.

Part III – Report

This report will include both in-class and take-home aspects of this lab assignment.

You must turn in a report containing the following:

Part I – Pre-lab Assignment

1. *iperf* throughput measuring tool
    (a) What are the options available in iperf that can be used to configure the server and the client to tune a TCP connection?

Part II – In-class experiments

1. Experiments with IEEE 802.11a
    (a) Report the throughput obtained with the traffic exchange done using iperf. Show any calculations you performed in to obtain this throughput.
    (b) Report the number of packets lost during the data transfer.
2. Setup of an ad-hoc network with IEEE 802.11b
    (a) Include the snap shot of the ping output collected during the in-class lab exercise.

Part III – Take-home experiments

1. Experiments in setting up the 802.11b access point

(a) What is the MAC address of your access point? Is it possible to change the MAC address by reconfiguring the access point?

(b) Provide the output of the ipconfig command, including the IP address obtained by the laptop.

2. Experiments with UDP data transfer

(a) Report the average throughput and average packet loss in the data transfer(s), with line of sight with the access point. Also report the signal strength for the duration of the connection. Include all relevant snapshots.

(b) Repeat part (a) with walls or partitions between the client and the access point. Include relevant snapshots.

(c) Repeat part (a) with interference caused by a microwave oven. Report for your results for multiple choices of frequency.

Part IV – General Conclusions

This is the free-form portion of your report. Provide a summary of lessons learned in this lab, general observations on how each of the tools illustrated by the experiments can be used to configure and assess performance of the network, any unexpected results obtained, etc. Feel free to suggest improvements to the experiments performed in this lab.