802.11 Wireless Networks: Incorporating Hands-On Learning Experience into the Undergraduate Classroom

Mira Yun, Charlie Wiseman, Leonidas Deligiannidis

Wentworth Institute of Technology
Department of Computer Science and Networking
550 Huntington Avenue
Boston, MA 02115, USA
{yunm, wisemanc, deligiannidisl}@wit.edu

Abstract

Wireless networking and communication systems are already fundamental in typical day-to-day use of the Internet. This usage is continuing to increase as newer wireless technologies such as 4G LTE, WiMAX, and 802.11s gain traction. As such, it is vital that current students learn both the theoretical concepts and the practical details of wireless networking. This paper describes a course that gives students that opportunity. Moreover, this course is targeted at undergraduates in computer science and computer networking whereas most wireless courses are only taught at the graduate level and often in computer or electrical engineering departments. Details are included on teaching methods for concepts in wireless technology through example lab assignments. Although the course will continue to evolve as new wireless standards emerge, we believe that the course provides a solid basis for teaching the theory and practice of wireless communication systems.

Keywords – IEEE 802.11 Wireless Networks, undergraduate computer science and networking education, hands-on experience.

1. INTRODUCTION

Wireless and mobile Internet-enabled devices such as laptops, smartphones, and tablets are becoming increasingly popular and affordable. With their promise of “anywhere, anytime” access to the Internet, wireless technology has become a crucial component in communication and networking systems and technology.The advantages of wireless and mobile technologies are more evident than ever, with various wireless technologies including 4G Long Term Evolution (LTE), WiFi, Bluetooth, Near Field Communication (NFC), Global Positioning System (GPS) and 802.16 Worldwide Interoperability for Microwave Access (WiMAX) being continually developed and deployed [1]–[3]. With its growing popularity, wireless technology supports various emerging applications in the fields of medicine, on-line education, military operations, industrial management, home automation and many others [4]-[7].

In response to the increasing demand for wireless networking skills in almost all industries, it is crucial to teach and provide our students with the knowledge to understand the state of the art in wireless technologies and applications, to help identify the current trends and challenges, and eventually to excel in their careers. Despite the popularity of the topic and increasing industry demand, courses or laboratories on wireless and mobile networks are not frequently offered at the undergraduate level; this is mainly due to the fact that the topic is relatively new and that it requires greater research. Unlike graduate students, teaching a wireless course to undergraduate students is a difficult task because the study requires the students to have strong knowledge in both technical implementation and theoretical concepts. The nature of the subject, which tends to be dry and heavily based on theory, makes the materials covered in class difficult to digest for many undergraduate students. Thus, introducing hands-on learning activities into the course study can dramatically improve the quality of the classroom experience by allowing students to engage with the topic in a practical manner [8]-[14]. As one of the leading undergraduate polytechnic institutes, the Computer Science and Networking Department at Wentworth Institute of Technology (WIT), Boston, sees the importance of active participation and has developed a hands-on wireless networks course for undergraduate students [15].

In this paper, we will provide an overview of this hands-on 802.11 wireless networks course for undergraduate juniors and seniors with specific examples of assignments and projects.

2. TEACHING WIRELESS NETWORKS

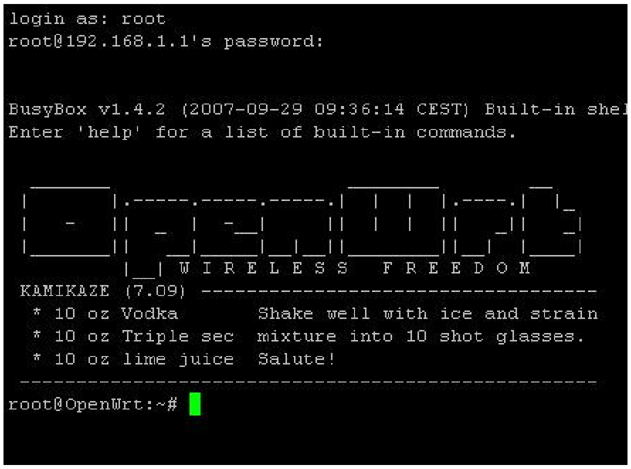
Teaching engineering and computer networking courses is a demanding task and continuous research has been made to develop effective teaching methods [8]-[14]. Although many diverse methods have been proposed, they all agree that incorporating hands-on learning experiences into these engineering courses significantly enhances student learning about engineering and networking [16][17]. However, it is difficult to provide practical demonstrations or hands on learning materials for engineering students at the undergraduate level. In response to this problem, Sarkar and Craig [8] presented several interesting Wi-Fi project ideas including infrared remote control, Wi-Fi Antenna, and Ad Hoc Networks to provide the students of wireless communication and networking with a hands-on learning experience. Guzelgoz and Arslan [9] presented eight fundamental wireless communication experiments including waveforms, modulation, synchronization, and channel impact in wireless communications for electrical engineering education. In extension of these efforts, several wireless laboratories for education and research have been developed to enhance student learning about wireless communications and networking technology. Most of these wireless laboratories focus on providing low cost and commercially available systems and devices to students. Linn [10] used a Xilinx Spartan-3 A Starter Kit board [18]. Chenard, Zilic, and Prokic [11] used the microprocessor system kit McGumps [19] [20] to setup a wireless and mobile embedded laboratory. However, these wireless laboratories were designed for engineering students and did not cover the same concepts and material required in computer science and networking. For example, they focused on the physical transmission of wireless signals and waveforms rather than communication protocols and security concerns.

Furthermore, as new wireless technologies and networks continue to be developed and updated, building a new experimental environment for each system and network is expensive and difficult. Thus, Wang and Jiang [12] used Network Simulator (NS)-3, a free software simulation platform, as an effective means of wireless local area network teaching. Instead of relying solely on existing free software such as NS-2[21], OPNET[22], and QualNet (formerly GloMoSim) [23], Sanguino et al. [13] developed a new educational wireless network simulator, WiFiSiM, devoted to the study and evaluation of wireless networks. Momeni and Kharrazi [14] presented a combined approach with both software simulations and physical network topologies.

It is interesting to note however that none of these previous endeavors are targeted at undergraduate computer networking students. In this paper, several Wi-Fi experiments for computer networking students are introduced. These experiments are designed with commercially available Linksys WRT54G series routers [24], which cost less than $50 USD, and other various software tools including aircrack-ng [25], InSSIDer [26], and Wireshark [27].

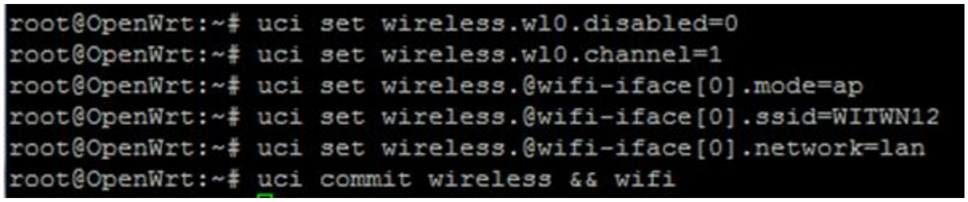
3. 802.11 WIRELESS EXPERIMENTS

The 802.11 Wireless Networks course is a four-credit course with 3 hours lecture and 2 hours lab weekly designed for junior or senior level undergraduate students. Theoretical aspects including the fundamental principles, architecture, and standards of modern WiFi communication systems are discussed during the lecture session. The principles of wireless communications are covered including basic terms and concepts, modulation, spread spectrum, multiplexing, antenna, Orthogonal Frequency Division Multiplexing (OFDM), and Code Division Multiple Access (CDMA). Based on these fundamentals, IEEE 802.11 a/b/g/n wireless standards are discussed in detail. This course also addresses the physical layer medium access control (MAC) protocols and their security protocols including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and 802.11i (WPA2). Various experiments from a single wireless access point (AP) to an advanced wireless distribution system (WDS) are conducted in order to strengthen student comprehension of the theoretical material. The major experiments are described in the following sections.



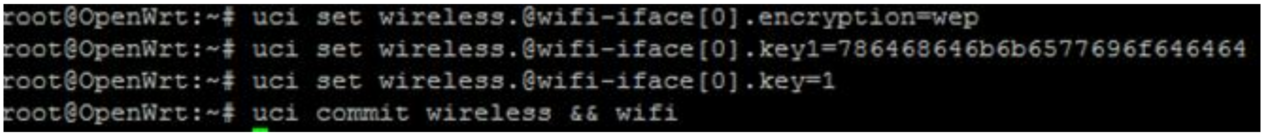
```
login as: root
root@192.168.1.1's password:


BusyBox v1.4.2 (2007-09-29 09:36:14 CEST) Built-in shel
Enter 'help' for a list of built-in commands.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 KAMIKAZE (7.09) -----------------------------------
  * 10 oz Vodka       Shake well with ice and strain
  * 10 oz Triple sec  mixture into 10 shot glasses.
  * 10 oz lime juice  Salute!
 ---------------------------------------------------
root@OpenWrt:~# 
```

Figure 1. OpenWRT Login Page



```
root@OpenWrt:~# uci set wireless.wl0.disabled=0
root@OpenWrt:~# uci set wireless.wl0.channel=1
root@OpenWrt:~# uci set wireless.@wifi-iface[0].mode=ap
root@OpenWrt:~# uci set wireless.@wifi-iface[0].ssid=WITWN12
root@OpenWrt:~# uci set wireless.@wifi-iface[0].network=lan
root@OpenWrt:~# uci commit wireless && wifi
```

Figure 2. UCI Commands for Wireless Network



```
root@OpenWrt:~# uci set wireless.@wifi-iface[0].encryption=wep
root@OpenWrt:~# uci set wireless.@wifi-iface[0].key1=786468646b6b6577696f646464
root@OpenWrt:~# uci set wireless.@wifi-iface[0].key=1
root@OpenWrt:~# uci commit wireless && wifi
```

Figure 3. UCI Commands for WEP Encryption Setup

3.1. Basic Wireless Network Setup

Many wireless routers actually run the Linux operating system with a custom web interface that allows users to do configuration with a minimum of technical know-how. OpenWRT [28] is essentially an open source Linux distribution for embedded devices, designed to fit into a small memory foot print. It was originally developed specifically for the Linksys WRT54G series routers; however, many other devices are supported today. Most of these compatible devices use the same Broadcom processor, but some other processors are also used. The idea behind OpenWRT was to open up functionality that was not originally available and also to provide a Linux frame work for customizing your device to do far more than it was originally designed to do. In order to explore various functionalities of off-the-shelf wireless APs, the course uses Linksys WRT54G series routers running the third party firmware from OpenWRT.

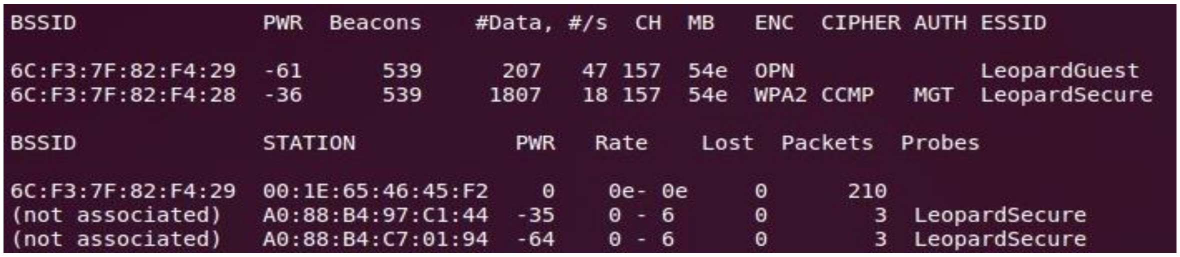
After installing OpenWRT on the WRT54G router, it is possible to connect to it via Secure Shell (SSH) or the web. Figure 1 shows logging on to the router with the root account and password through the SSH command `ssh root@192.168.1.1`.

Students first learn how to set up a wireless network by configuring wireless parameters on OpenWRT. Wireless specific (Layers 1 and 2) configurations are stored in `/etc/config/wireless`. Layer 3 parameters are stored in `/etc/config/network`. Students can manually modify these two configuration files using the vi editor [29]. Because there is no syntax checking inside vi, however, the Unified Configuration Interface (UCI) command [30] is used to set various parameters inside these two files directly. Figure 2 shows how to enable Wi-Fi networking, place the AP on a particular channel, and set the customized service set identification (SSID, i.e. the public name of a wireless network) by using uci commands.

Next, the security schemes are set up through additional command line configuration. Figure 3 shows how to configure WEP encryption with UCI commands. As per the standard, up to four WEP keys can be configured. The procedure is well documented in [31].

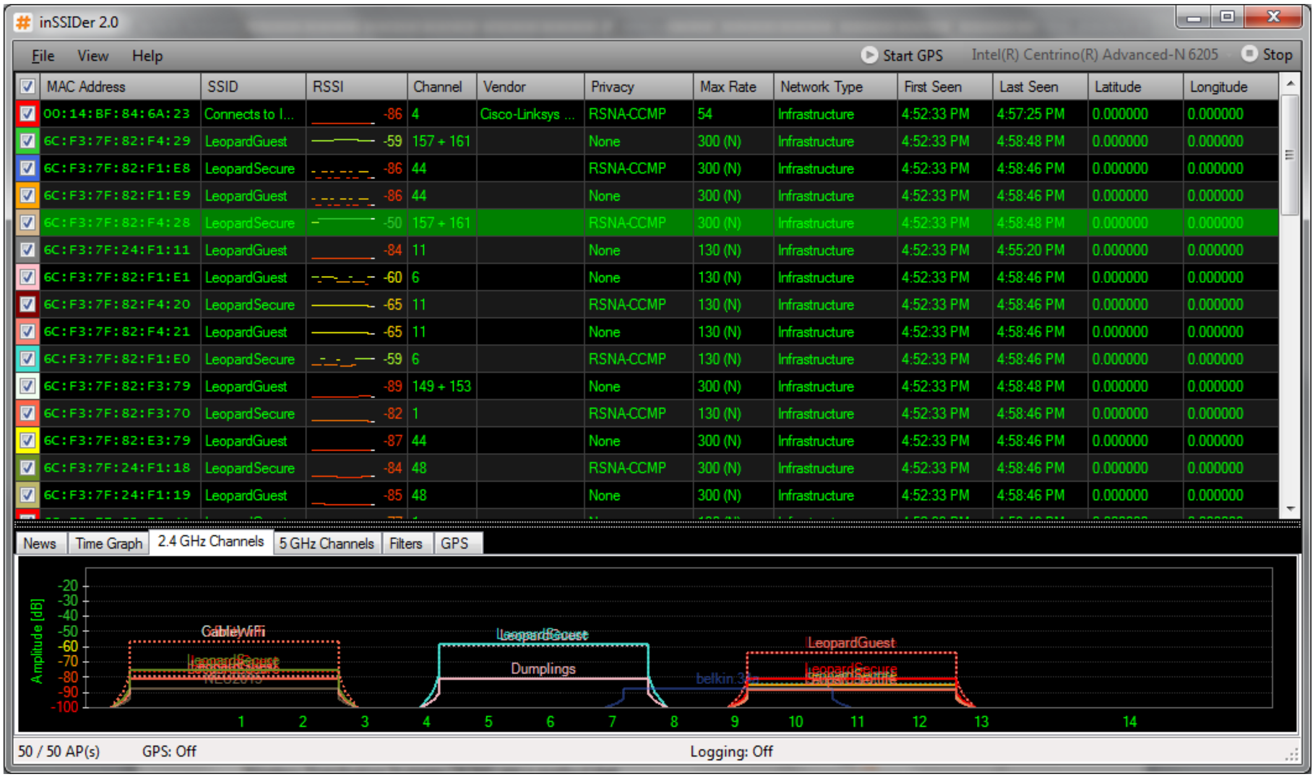
After all configuration is completed, students are asked to check the `/etc/config/wireless` file to verify that all changes have taken place. There are several methods and tools to get more detailed wireless information. Through one of the wireless scanning tools, students are able to verify that their wireless network is set up and functioning correctly. Figure 4 uses airodump-ng [25], a Linux based wireless packet capture tool. Figure 5 shows the scanning result of InSSIDer [26], a Windows based WiFi scanning software suite.

Finally, students move to the more advanced wireless network parameters such as antenna adjustment, rudimentary penetration testing, MAC filter setup, etc [28].



```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

6C:F3:7F:82:F4:29  -61      539      207   47 157  54e  OPN              LeopardGuest
6C:F3:7F:82:F4:28  -36      539     1807   18 157  54e  WPA2 CCMP   MGT  LeopardSecure

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

6C:F3:7F:82:F4:29  00:1E:65:46:45:F2    0    0e- 0e     0      210
(not associated)   A0:88:B4:97:C1:44  -35    0 - 6      0        3  LeopardSecure
(not associated)   A0:88:B4:C7:01:94  -64    0 - 6      0        3  LeopardSecure
```

Figure 4. Linux Method: airodump-ng



☑	MAC Address	SSID	RSSI	Channel	Vendor	Privacy	Max Rate	Network Type	First Seen	Last Seen	Latitude	Longitude
☑	00:14:BF:84:6A:23	Connects to I...	-86	4	Cisco-Linksys ...	RSNA-CCMP	54	Infrastructure	4:52:33 PM	4:57:25 PM	0.000000	0.000000
☑	6C:F3:7F:82:F4:29	LeopardGuest	-59	157 + 161		None	300 (N)	Infrastructure	4:52:33 PM	4:58:48 PM	0.000000	0.000000
☑	6C:F3:7F:82:F1:E8	LeopardSecure	-86	44		RSNA-CCMP	300 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000
☑	6C:F3:7F:82:F1:E9	LeopardGuest	-86	44		None	300 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000
☑	6C:F3:7F:82:F4:28	LeopardSecure	-50	157 + 161		RSNA-CCMP	300 (N)	Infrastructure	4:52:33 PM	4:58:48 PM	0.000000	0.000000
☑	6C:F3:7F:24:F1:11	LeopardGuest	-84	11		None	130 (N)	Infrastructure	4:52:33 PM	4:55:20 PM	0.000000	0.000000
☑	6C:F3:7F:82:F1:E1	LeopardGuest	-60	6		None	130 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000
☑	6C:F3:7F:82:F4:20	LeopardSecure	-65	11		RSNA-CCMP	130 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000
☑	6C:F3:7F:82:F4:21	LeopardGuest	-65	11		None	130 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000
☑	6C:F3:7F:82:F1:E0	LeopardSecure	-59	6		RSNA-CCMP	130 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000
☑	6C:F3:7F:82:F3:79	LeopardGuest	-89	149 + 153		None	300 (N)	Infrastructure	4:52:33 PM	4:58:48 PM	0.000000	0.000000
☑	6C:F3:7F:82:F3:70	LeopardSecure	-82	1		RSNA-CCMP	130 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000
☑	6C:F3:7F:82:E3:79	LeopardGuest	-87	44		None	300 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000
☑	6C:F3:7F:24:F1:18	LeopardSecure	-84	48		RSNA-CCMP	300 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000
☑	6C:F3:7F:24:F1:19	LeopardGuest	-85	48		None	300 (N)	Infrastructure	4:52:33 PM	4:58:46 PM	0.000000	0.000000

Figure 5. Windows Method: InSSIDer

3.2. Wireless Distribution System

Wireless Distribution Systems (WDS) are one way to enable the wireless interconnection of APs (or routers) in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple APs without the need for a wired backbone to link them together, as it has been traditionally required. In WDS, an AP (or router) can be either a main, relay, or remote AP as shown in Figure 6. A main AP is typically connected to the Internet. A relay AP relays data from remote APs, wireless clients or other relay APs to either a main or another relay AP. A remote AP accepts connections from wireless clients and passes them on to the relay or main APs.

WDS can be used to provide two modes of wireless AP-to-AP connectivity:

1) *Bridge mode*: wireless bridging in which WDS APs communicate only with each other and do not allow wireless clients or stations to access them.
2) *Repeater mode*: wireless repeating in which APs communicate with each other and with wireless stations. Repeater mode is more advanced than bridge mode.

All APs in a WDS must be configured to use the same radio channel, and share WEP keys or WPA keys if they are used. They can be configured to use different SSIDs. WDS also requires that every AP be configured to forward to others in the system.

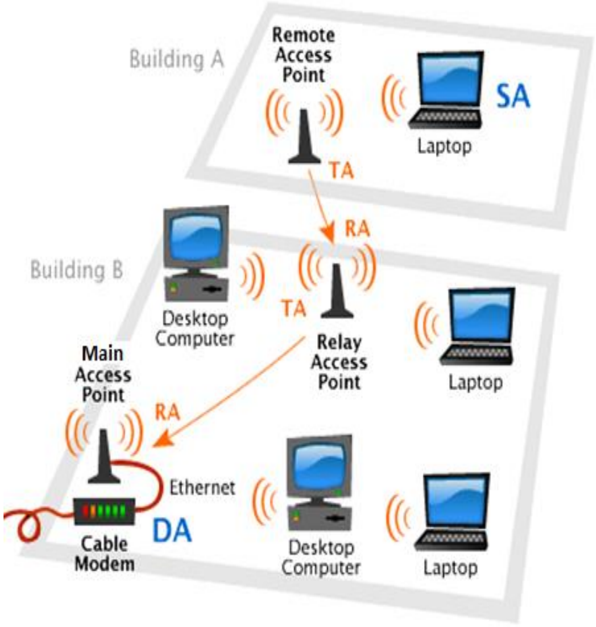
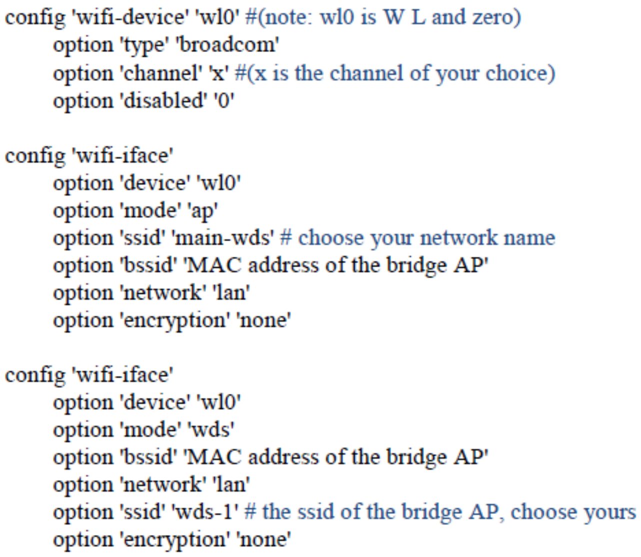


Figure 6. Wireless Distribution System



```
config 'wifi-device' 'wl0' #(note: wl0 is W L and zero)
       option 'type' 'broadcom'
       option 'channel' 'x' #(x is the channel of your choice)
       option 'disabled' '0'

config 'wifi-iface'
       option 'device' 'wl0'
       option 'mode' 'ap'
       option 'ssid' 'main-wds' # choose your network name
       option 'bssid' 'MAC address of the bridge AP'
       option 'network' 'lan'
       option 'encryption' 'none'

config 'wifi-iface'
       option 'device' 'wl0'
       option 'mode' 'wds'
       option 'bssid' 'MAC address of the bridge AP'
       option 'network' 'lan'
       option 'ssid' 'wds-1' # the ssid of the bridge AP, choose yours
       option 'encryption' 'none'
```

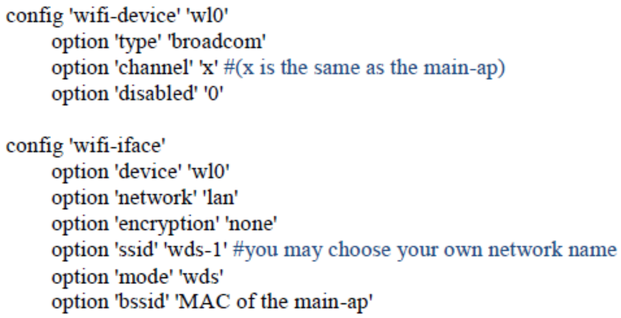
Figure 7. Main AP Wireless Configuration

3.4.1 Setup Bridge Mode

In this section, we illustrate a detailed example of how to set up a WDS in bridge mode with two or more APs. From two APs, we choose one AP as the main AP and name it as "`main-ap`". The other AP will be a wireless bridge in the WDS mode and is named as "`wds-1`". Of course students may name their APs in their preferred manner, perhaps including their username, so that they can be distinguished easily in the classroom.

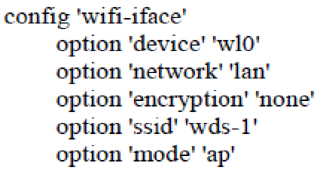
Here are the steps:

1) Open a new terminal and SSH to 192.168.1.1. Log on to each AP and get the MAC address (a.k.a, basic service set identification (BSSID)) of each router using the command: `ifconfig wl0`.
2) **Configure the Main AP:** Wireless specific configurations are stored in `/etc/config/wireless`. Backup the existing wireless configuration file and then modify the wireless file as shown in Figure 7.
3) **Configure the Bridge AP:** Change the IP address of the bridging AP (`wds-1`) to 192.168.1.2 (it can be any IP that is not 192.168.1.1). Go the `/etc/config` directory and edit the file named `network` to update the IP address (192.168.1.2).
4) Go to the `/etc/init.d` directory and disable the domain name system (DNS) and firewall services through the `rm dnsmasq` and `rm firewall` commands.
5) Go to the `/etc/config` directory and edit the file named `dhcp`. Remove all the lines that match these two entries: `config dhcp lan` and `config dhcp wan`.



```
config 'wifi-device' 'wl0'
       option 'type' 'broadcom'
       option 'channel' 'x' #(x is the same as the main-ap)
       option 'disabled' '0'

config 'wifi-iface'
       option 'device' 'wl0'
       option 'network' 'lan'
       option 'encryption' 'none'
       option 'ssid' 'wds-1' #you may choose your own network name
       option 'mode' 'wds'
       option 'bssid' 'MAC of the main-ap'
```

Figure 8. Bridge AP Wireless Configurations



```
config 'wifi-iface'
       option 'device' 'wl0'
       option 'network' 'lan'
       option 'encryption' 'none'
       option 'ssid' 'wds-1'
       option 'mode' 'ap'
```

Figure 9. Repeater AP Wireless Configurations

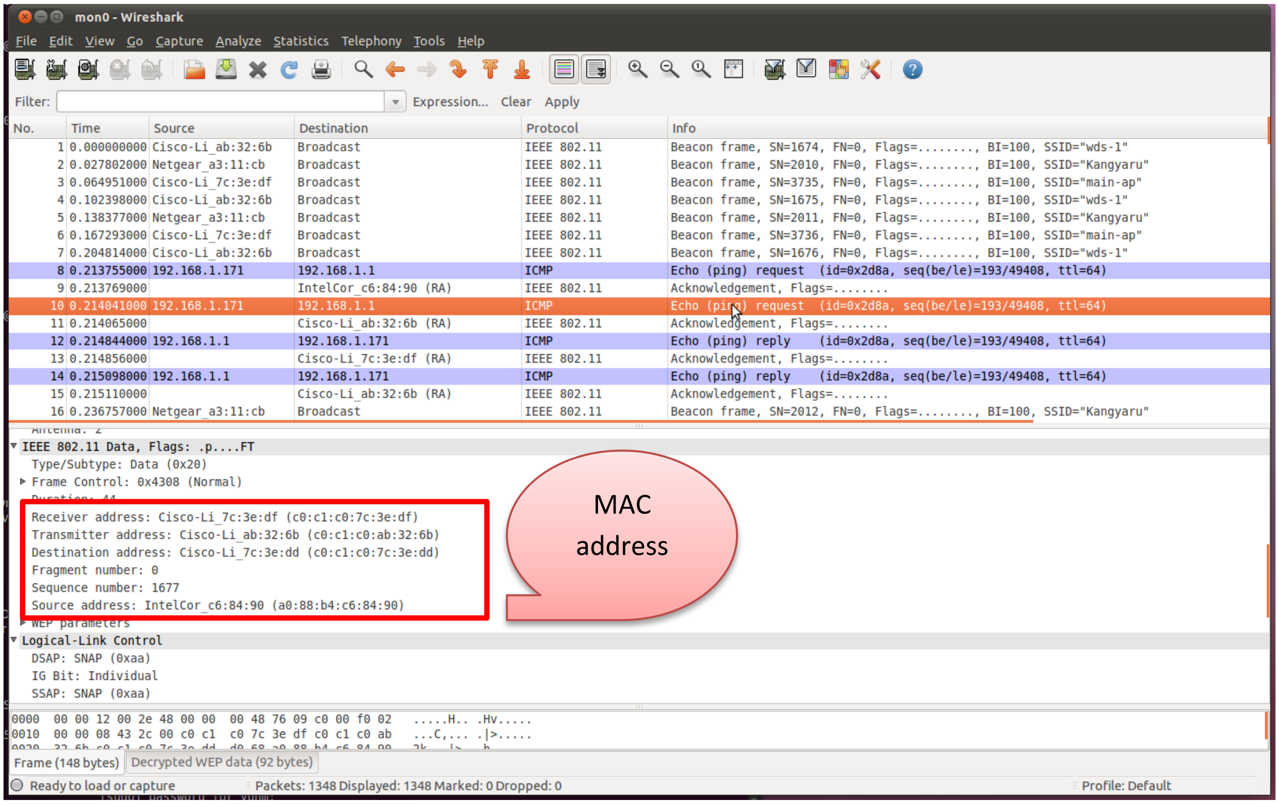
6) Backup the `/etc/config/wireless` file and then modify the wireless file as shown in Figure 8.

After rebooting each router, students need to verify their setup. If students connect a laptop (say laptop-a) to `main-ap` wirelessly and another laptop (say laptop-b) to the bridge AP using a network cable (the laptop needs to use DHCP instead of static IP), then laptop-b should obtain an IP address even though the bridge AP does not offer dynamic host configuration protocol (DHCP) services.

3.4.2 Setup Repeater Mode

In order to setup repeater mode, the bridge AP should be tuned into a relay AP (repeater mode). As shown in Figure 9, an extra `wifi-iface` configuration should be appended into the bridge AP wireless file in `/etc/config/wireless`. Nothing needs to be changed on `main-ap`.

After rebooting the router, students need to verify their setup. If students connect a laptop (say laptop-a) to `main-ap` wirelessly and another laptop (say laptop-b) to the relay AP (`wds-1`) wirelessly (the laptop needs to use DHCP instead of static IP), then laptop-b should obtain an IP address. If students ping laptop-a from laptop-b, students can capture the ping request and reply frame pair (between the two laptops) by using a packet capturing tool such as Wireshark [30]. Figure 10 shows an example of a ping request frame to check how four MAC addresses (receiver, transmitter, destination, and source) are set in the WDS mode.


mon0 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply
MAC address
Frame (148 bytes)
Decrypted WEP data (92 bytes)

```
No.  Time        Source             Destination             Protocol     Info
   1 0.000000000 Cisco-Li_ab:32:6b  Broadcast               IEEE 802.11  Beacon frame, SN=1674, FN=0, Flags=........, BI=100, SSID="wds-1"
   2 0.027802000 Netgear_a3:11:cb   Broadcast               IEEE 802.11  Beacon frame, SN=2010, FN=0, Flags=........, BI=100, SSID="Kangyaru"
   3 0.064951000 Cisco-Li_7c:3e:df  Broadcast               IEEE 802.11  Beacon frame, SN=3735, FN=0, Flags=........, BI=100, SSID="main-ap"
   4 0.102398000 Cisco-Li_ab:32:6b  Broadcast               IEEE 802.11  Beacon frame, SN=1675, FN=0, Flags=........, BI=100, SSID="wds-1"
   5 0.138377000 Netgear_a3:11:cb   Broadcast               IEEE 802.11  Beacon frame, SN=2011, FN=0, Flags=........, BI=100, SSID="Kangyaru"
   6 0.167293000 Cisco-Li_7c:3e:df  Broadcast               IEEE 802.11  Beacon frame, SN=3736, FN=0, Flags=........, BI=100, SSID="main-ap"
   7 0.204814000 Cisco-Li_ab:32:6b  Broadcast               IEEE 802.11  Beacon frame, SN=1676, FN=0, Flags=........, BI=100, SSID="wds-1"
   8 0.213755000 192.168.1.171      192.168.1.1             ICMP         Echo (ping) request  (id=0x2d8a, seq(be/le)=193/49408, ttl=64)
   9 0.213769000                    IntelCor_c6:84:90 (RA)  IEEE 802.11  Acknowledgement, Flags=........
  10 0.214041000 192.168.1.171      192.168.1.1             ICMP         Echo (ping) request  (id=0x2d8a, seq(be/le)=193/49408, ttl=64)
  11 0.214065000                    Cisco-Li_ab:32:6b (RA)  IEEE 802.11  Acknowledgement, Flags=........
  12 0.214844000 192.168.1.1        192.168.1.171           ICMP         Echo (ping) reply    (id=0x2d8a, seq(be/le)=193/49408, ttl=64)
  13 0.214856000                    Cisco-Li_7c:3e:df (RA)  IEEE 802.11  Acknowledgement, Flags=........
  14 0.215098000 192.168.1.1        192.168.1.171           ICMP         Echo (ping) reply    (id=0x2d8a, seq(be/le)=193/49408, ttl=64)
  15 0.215110000                    Cisco-Li_ab:32:6b (RA)  IEEE 802.11  Acknowledgement, Flags=........
  16 0.236757000 Netgear_a3:11:cb   Broadcast               IEEE 802.11  Beacon frame, SN=2012, FN=0, Flags=........, BI=100, SSID="Kangyaru"
```

```
  Antenna: 2
▼ IEEE 802.11 Data, Flags: .p....FT
    Type/Subtype: Data (0x20)
  ▶ Frame Control: 0x4308 (Normal)
    Duration: 44
    Receiver address: Cisco-Li_7c:3e:df (c0:c1:c0:7c:3e:df)
    Transmitter address: Cisco-Li_ab:32:6b (c0:c1:c0:ab:32:6b)
    Destination address: Cisco-Li_7c:3e:dd (c0:c1:c0:7c:3e:dd)
    Fragment number: 0
    Sequence number: 1677
    Source address: IntelCor_c6:84:90 (a0:88:b4:c6:84:90)
  ▶ WEP parameters
▼ Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
```

```
0000   00 00 12 00 2e 48 00 00  00 48 76 09 c0 00 f0 02   .....H.. .Hv.....
0010   00 00 08 43 2c 00 c0 c1  c0 7c 3e df c0 c1 c0 ab   ...C,... .|>.....
```

```
Ready to load or capture    Packets: 1348 Displayed: 1348 Marked: 0 Dropped: 0    Profile: Default
```

Figure 10. Wireshark Example: Ping Request Frame

4. CONCLUSION AND FUTURE WORK

The novelty of this work lies in developing a course targeted for undergraduates in computer science and computer networking. Most wireless courses are only taught at the graduate level and often in computer or electrical engineering departments. Through the combined hardware and software experiments, students become engaged in the topic and learn the material from a practical perspective. Course evaluation based on student feedback shows a high level of enthusiasm and engagement among the students in the wireless course. Most importantly, the students learned about current state of the art IEEE 802.11 wireless technologies in depth due to the strong hands-on learning nature of the course. In addition, this course addressed the physical layer specification and the medium access control protocols as well as their advanced applications such as WDS. In the future, the course will include wireless security experiments. Current wireless security protocols including WEP, WPA, and 802.11i can be circumvented due to a flaw that exists in the authentication procedure [32]-[34]. Providing students with an opportunity to see how these standards can be cracked and broken will enable them to build practical experience with current security issues and become more engaged in the topic of wireless security.

REFERENCES

[1] Yi, L.; Kai Miao; Liu, A., "A comparative study of WiMAX and LTE as the next generation mobile enterprise network," Advanced Communication Technology (ICACT), 2011 13th International Conference on, vol., no., pp.654,658, 13-16 Feb. 2011

[2] Michahelles, F.; Thiesse, Frederic; Schmidt, A.; Williams, J.R., "Pervasive RFID and Near Field Communication Technology," Pervasive Computing, IEEE , vol.6, no.3, pp.94,96, c3, July-Sept. 2007

[3] Want, R., "Near field communication," Pervasive Computing, IEEE , vol.10, no.3, pp.4,7, July-September 2011

[4] Tang Yu-liang; Luo Yu; Huang Lian-fen; Guo Jian; Lei Ying, "Wireless sensor network for on-line structural health monitoring," Computer Science & Education (ICCSE), 2012 7th International Conference on , vol., no., pp.386,389, 14-17 July 2012

[5] Yuksekkaya, B.; Kayalar, A.A.; Tosun, M.B.; Ozcan, M.K.; Alkar, A.Z., "A GSM, internet and speech controlled wireless interactive home automation system," Consumer Electronics, IEEE Transactions on , vol.52, no.3, pp.837,843, Aug. 2006

[6] Danielle Bragg, Mira Yun, Haya Bragg, and Hyeong-Ah Choi, "Intelligent Transmission of Patient Sensor Data in Wireless Hospital Networks", Proc. AMIA(American Medical Informatics Association) 2012 symposium, Chicago, Nov 2012

[7] Mira Yun, Danielle Bragg, Amrinder Arora, and Hyeong-Ah Choi, "Battle Event Detection using Sensor Networks and Distributed Query Processing", Proc. INFOCOM Workshops 2011, IEEE, CPNS 2011, Shanghai, China, April 2011

[8] Sarkar, N.I.; Craig, T.M., "Teaching wireless communication and networking fundamentals using Wi-Fi projects," Education, IEEE Transactions on , vol.49, no.1, pp.98,104, Feb. 2006

[9] Güzelgöz, S.; Arslan, H., "A Wireless Communications Systems Laboratory Course," Education, IEEE Transactions on , vol.53, no.4, pp.532,541, Nov. 2010

[10] Linn, Y., "An Ultra Low Cost Wireless Communications Laboratory for Education and Research," Education, IEEE Transactions on , vol.55, no.2, pp.169,179, May 2012

[11] Chenard, J-S; Zilic, Z.; Prokic, M., "A Laboratory Setup and Teaching Methodology for Wireless and Mobile Embedded Systems," Education, IEEE Transactions on , vol.51, no.3, pp.378,384, Aug. 2008

[12] Anbao Wang; WenRong Jiang, "Teaching Wireless Local Area Network Course Based on NS-3," Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on , vol., no., pp.1,4, 18-20 Jan. 2009

[13] Mateo Sanguino, T. J.; Serrano Lopez, C.; Marquez Hernandez, F. A., "WiFiSiM: An Educational Tool for the Study and Design of Wireless Networks," Education, IEEE Transactions on , vol.PP, no.99, pp.1,1, 2012

[14] Momeni, B.; Kharrazi, M., "Improving a Computer Networks Course Using the Partov Simulation Engine," Education, IEEE Transactions on , vol.55, no.3, pp.436,443, Aug. 2012

[15] Leonidas Deligiannidis, Charlie Wiseman, Mira Yun, and Tom Goulding, "Network Security Course: A Demonstration of Project-Based Learning", In Proc. of the 2012 International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS'12), pp.28-34, July 16-19 2012, Las Vegas NV, USA.

[16] M.F. Young, “Instructional design for situated learning,” Educ. Technol., vol 41, pp. 43-58, 1993

[17] J.R. Anderson, L. M. Reder, and H.A. Simon, “Situated learning and education,” in Educ. Res., 1996, vol. 25, pp. 5-11.

[18] Spartan 3 A Starter Kit HW-SPAR3A-SK-UNI-G. Xilinx Inc., San Jose, CA, May 2009 [Online]. Avaiable: http://www.xilinx.com

[19] J.-S. Chenard, U. Khalid, M. Prokic, R. Zhang, K.-L. Lim, A. Chattopadhyay, and Z. Zilic, “Expandable and robust laboratory for microprocessor systems,” in Proc. IEEE Int. Conf. Microelectronic Systems Education, Anaheim, CA, Jun. 2005, pp. 65–66.

[20] Z. Zilic, J.-S. Chenard, and M. Prokic, “A laboratory for wireless and mobile embedded systems,” in Proc. IEEE Int. Conf. Microelectronic Systems Education, San Diego, CA, Jun. 2007, pp. 103–104.

[21] T. Issariyakul and E. Hossain, Introduction to Network Simulator NS2. New York: Springer, 2008.

[22] G. Flores Lucio, M. Paredes-Farrera, E. Jammeh, M. Fleury, and M. J. Reed, “OPNET modeler and Ns-2: Comparing the accuracy of network simulators for packet-level analysis using a network testbed,” in Proc. 3rd WEAS ICOSMO, 2003, vol. 2, pp. 700–707.

[23] X. Zeng, R. Bagrodia, and M. Gerla, “GloMoSim: A library for parallel simulation of large-scale wireless networks,” inProc. 12th PADS, 1998, pp. 154–161.

[24] Cisco-Linksys WRT54G Wireless-G Router, Aug 2044, http://www.linuxjournal.com/article/7322

[25] Aircrack-ng, http://www.aircrack-ng.org/

[26] InSSIDer, http://www.metageek.net/products/inssider/

[27] Wireshark, http://www.wireshark.org/

[28] OpenWRT, https://openwrt.org/

[29] The Open Group (1997). "vi — screen-oriented (visual) display editor", Version 2, http://pubs.opengroup.org/onlinepubs/007908799/xcu/vi.html

[30] UCI, http://wiki.openwrt.org/doc/techref/uci

[31] OpenWRT Basic Configuration, http://wiki.openwrt.org/doc/howto/basic.config

[32] Boland, H.; Mousavi, H.; "Security issues of the IEEE 802.11b wireless LAN," Electrical and Computer Engineering, 2004. Canadian Conference on , vol.1, no., pp. 333- 336 Vol.1, 2-5 May 2004.

[33] Hal Berghel and Jacob Uecker, “WiFi attack vectors”. Commun. ACM 48, August 2005

[34] Scott R. Fluhrer, Itsik Mantin, and Adi Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”, In Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography (SAC '01), Serge Vaudenay and Amr M. Youssef (Eds.). Springer-Verlag, London, UK, 1-24.