AC 2008-2591: COMPARATIVE FRAMING ANALYSIS FOR TEACHING WIRELESS NETWORK MOBILITY

Robert MacDonald, Purdue University

Robert MacDonald is a graduate student with the College of Technology at Purdue University. He completed his undergraduate degree in 2006, obtaining his BS in Network Engineering Technology from Purdue University as well. Robert is expecting to complete his MS in December of 2008. His interests lie in advanced internetwork design, wireless networking, and applied network security. His thesis research is focused on the implementation of secure routing protocols.

Raheel Malik, Whirlpool Corp.

Raheel A. Malik is a senior analyst with the Information Security and Audit Compliance team at Whirlpool Corporation in Benton Harbor, MI. His responsibilities include penetration testing their network, conducting internal IT audits for Sarbanes-Oxley compliance, investigating computer-related security incidents, and providing security consulting for on-going projects. Raheel holds a Masters of Science degree specializing in Information Security and a Bachelors of Science degree, with distinction, in Telecommunications and Networking from Purdue University, West Lafayette, IN.

Anthony Smith, Purdue University

Anthony H. Smith is an assistant professor with the Computer and Information Technology Department at Purdue University. He has more than 15 years of experience in various technical roles, as well as 10 years experience with computer technologies including LAN, WAN and wireless network design and implementation. After graduating from Wittenberg University, Anthony spent several years in general management positions. He served in the U.S. Coast Guard for 5 years in a number of technical, management, and law enforcement roles. He left the Coast Guard to pursue a Masters in Technology at Purdue, which he received in 1994. Since then, Anthony's industrial experience includes both large corporate and small business environments serving in management and systems engineering roles. He has designed and consulted on numerous corporate and municipal networks, and has extensive application development and project management experience. Professor Smith currently teaches and conducts applied research in the areas of local and wide-area wireless network design, implementation and security. In addition, he has an active consultancy dedicated to local and wide area wireless networks, currently focused on wide-area wire-line replacement strategies.

James Goldman, Purdue University

Jim Goldman is Professor and Associate Department Head in the Department of Computer Technology at Purdue University where he founded the Telecommunications and Networking Technology (Network Engineering Technology) program. Jim has over 20 years of experience in telecommunications strategy, network engineering, and project management of regional, national, and global networking projects. Jim is a CISSP (Certified Information Systems Security Professional) with advanced training in computer forensics. He is certified by the U.S. National Security Agency in their InfoSec Assessment Methodology (IAM) and InfoSec Evaluation Methodology (IEM). He is an internationally published author with market leading textbooks in data communications and networking. Among Jim's areas of research and publication are municipal telecommunications strategy, information technology economics and investment strategy, network security investment strategy, steganography, and computer-aided image analysis.

Comparative Framing Analysis for Teaching Wireless Network Mobility

Abstract
As wireless networking in the enterprise has gained popularity within recent years, the demand for technical talent has increased in direct proportion to that demand. This has occurred partially due to the complexity of troubleshooting and security issues. Professional wireless networking certification programs have also become popular as a result of the financial incentives associated with this demand. Since the content taught in these professional certifications is an appropriate reflection of the challenges faced in the real world as reported by Fortune magazine, it is appropriate to align the content of undergraduate wireless networking courses with that of these professional certifications.

University professors have often taken the approach of teaching 802.11 wireless networks starting from the signal processing layer and immediately transitioning to the higher layers. This process bypasses the Media Access Control (MAC) layer in consequence. Understanding the MAC layer is of utmost importance for understanding wireless network security because it contains the management frames that control both authentication and encryption. Additionally, the potential impacts and effects of the distribution system implemented are glossed over.

In this paper, a new course module was created for undergraduates that builds on a laboratory framework developed previously. The previously developed framework focused on the 802.11 and 802.3 MAC layers and can be used to facilitate teaching troubleshooting and security concepts for wireless networking with the help of packet sniffers. These modules provided students with the hands-on experience of what is generally illustrated in only text for Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Virtual Private Networking (VPN) as well as troubleshooting skills. The new module is geared towards upper classmen and graduate students. This module focuses on the potential distribution systems for 802.11 WLANs, including a proprietary mesh protocol, wireless distribution system, and the classic wired network.

1. Introduction

The introduction of wireless networking has allowed people the freedom to access networks, including the Internet, from almost any location. This fact has been reflected, in part, by a surge in laptop sales over the recent years. Vice president of Gartner's worldwide computing platforms, Charles Smulders, states that "Consumers are flocking to notebooks because of lower prices, better performance, and an increased appreciation for wireless technologies."[5] The increased appreciation here stems from the transparently bridging technologies. According to an engineer at Qualcomm, "One of the fundamental design goals for 802.11 is to provide services that are consistent with the services of 802.3 networks. This makes the peculiarities of wireless communication irrelevant to higher layers of the protocol stack."[10] The most important differences, therefore, lie between the wireless and the wired networking bridge as all the higher layer protocols communicate transparently over them. The simplicity and mobility of wireless networks arises from the characteristics of its contention domain which requires little infrastructure while providing service up to 300 feet.[16] The contention domain works much like a wired Ethernet hub.[4] This is an inherent weakness of wireless networks that can be examined for

educational purposes. And though denial of service attacks will always haunt wireless networks including Wireless Local Area Networks (WLANs), other risks can be mitigated such as compromise of confidentiality and integrity through authentication, authorization and encryption mechanisms.[14]

Security over wireless networks has matured greatly since the original 802.11 standard was ratified. Privacy had been of great concern as the signals were originally broadcast over the shared medium sans encryption. The Wired Equivalent Privacy (WEP) encryption algorithm was introduced to overcome the initial privacy issues. Not only was it discovered to be flawed, but it was also only a one-factor authentication mechanism.[15] As wireless networks grew, key sharing became an increasing threat to privacy since authentication was bypassed in this process and getting authorized was as easy as asking someone for the key. Other algorithms / protocols / methods have been employed which currently guarantee privacy over a wireless link. These include the 802.1X port-based authentication framework, and Virtual Private Networking (VPN) which, when used together, provide enterprise level security for remote access users.[3]

In order to properly implement a secure enterprise wireless network, IT personnel need to be knowledgeable about wireless network configuration and security.[1] There exist technology- and vendor-specific certification programs that train personnel on the fundamental concepts of wireless networks and provide the skills needed by actual IT professionals for administration, security, and teaching purposes [11]. Educational institutions have also attempted to provide the skills in demand by employers today with the help of donated equipment from corporations and funding from government agencies for human resources.[7] They have attempted to teach the concepts through hands-on exercises for signal processing[13], observing network delay[12], and programming applications for providing services.[8] All of these exercises lack training in the fundamental concepts of authentication, authorization, and encryption which have stimulated the demand for IT talent in the first place, and conceived the evolution of the aforementioned security mechanisms which are implemented at the MAC layer through use of management frames.

In addition to the focus on authentication, authorization, and encryption, educational efforts in wireless networking must address the growing demand for mobility amongst wireless clients. Users want increasing portability beyond the range of a single access point, while sending and receiving latency-sensitive traffic without interruption. The original 802.11 standard established a basic framework for mobile clients moving between access points. However, many decisions about how to implement handoffs were left up to the vendors. The result is a handoff process which often fails or times out when attempting to handoff.

The traditional approach to connecting multiple 802.11 access points together was to wire each access point directly to a switch or other network device. Running cable to every access point in a large wireless network is unrealistic due to the cost and overhead of maintaining that infrastructure. Because of this, various wireless distribution technologies have become popular. The wireless distribution system (WDS) and proprietary wireless mesh protocols allow access points to be connected together without the need for laying network cables. However, the impact that these distribution systems have on the already weak roaming and handoff processes is unknown. In order to develop an educational module focused on teaching wireless client roaming

and mobility concepts to IT personnel, several experiments were conducted to establish the impact the distribution system has on the 802.11 handoff process. These experiments were then used to design course modules for upper classmen or graduate students, using Malik et al's model for wireless laboratory development.[24] The course module focused on analyzing and gaining an understanding of 802.11 frames over mesh and WDS.

Since there is an increase in demand for highly skilled IT personnel in the field of wireless networking [1], it is important to fulfill the demand as early on as possible in the undergraduate programs through improved hands-on exercises that heavily incorporate security practices. Students will be required to conduct framing analysis from different scenarios including authentication, authorization, encryption, roaming, and high traffic environments.

2. Methodology of the Study

When combined with the previous work of Malik et al., there were a total of six course modules developed. The first five modules were developed previously, and used as a framework for the development of a new module. These modules, presented in Table 1, attempt to put together the best elements from lessons learned by others. Students will be required to conduct framing analysis from different scenarios including authentication, authorization, encryption, roaming, and high traffic environments. Since the modules are intended to be used after the introductory labs, students will have the general knowledge of setting up the framework for collecting data samples.

Table 1: Modules created during this project

	Module	Comments / Outcome
1	Basic WEP Security	Wireless authentication using management frames.
2	WPA	Wireless authentication similar to WEP but this handshake is distinctly different.
3	VPN	Normal unencrypted wireless handshake followed by and end-to-end PPTP tunnel.
4	WPA with RADIUS	Authentication is a multi-step process which spans wireless and wired domains.
5	VoIP handshake	Normal flowing traffic can be observed as it travels across wireless and wired domains.
6	Client roaming and handoffs	Capture and analysis of 802.11 frames during client handoffs with three different distribution systems.

With a simple network topology, the basic wireless networking concepts will be communicated more efficiently to the students. The basic differences between management, control, and data frames can be witnessed and analyzed in unison with wired traffic.

Using this framework, it is easy to see how progress can be made for moving on to exploring the different kinds of authentication frames, association frames, probe request and response frames, and other subtypes as defined by the 802.11 MAC layer specification. Also as a result, it becomes easier to deduce how wireless networking threatens privacy requirements.

Since accurate analysis requires media isolation, 802.11a equipment can be used so that fewer errors occur and fewer findings are skewed due to collisions and other RF issues. Such isolation is not likely when using 802.11b or 802.11g equipment due to overlapping channels.

With this framework, the modules created provide exposure to 802.11 management, control and data frames as described in Table 1 previously. The first five modules in Table 1 are documented in further detail in Malik et al[24]. The five modules were well received by undergraduate students, and have been used effectively for two semesters (as of this writing). Undergraduates gained a better understanding of the 802.11 standard through a combination of hands-on laboratory work and traditional classroom instruction. With the success of the modules documented by Malik et al[24], a new module was created as an extension of the previous work.

In order to develop effective instructional modules focused on 802.11 client roaming, three different experiments were performed. The intention for this research was to design experiments to be replicated by undergraduate students in an isolated laboratory. For each of the three separate experiments, three different distribution systems were utilized: a wired infrastructure, a wireless distribution system (WDS), and a wireless mesh distribution system. The most traditional distribution system, a wired infrastructure is also the most popular implementation with 802.11 WLANs. The WDS implementation is easier to implement because there is no additional cabling required beyond power to the access points, but the distribution system must be configured manually by the administrator.

In order to replicate similar course modules, the instructor(s) must obtain the proper hardware and make it available for student use. Access points must support some kind of similar mesh protocol, as well as wireless distribution system protocols that can work in conjunction with 802.11 standards. Ideally, wireless access points utilized for this course module should support two separate radios. One radio should support 802.11a while the other supports 802.11b/g standards. In this manner, the distribution system can be separated from the client-access domain. A single unmanaged switch is also a minimum requirement for replication of this new course module. Finally, the instructor(s) should allocate at least three laptops per student or student team. One laptop will be used to roam between two access points, while the remaining two laptops are used to capture the 802.11 frames. Further information regarding the configuration and channel allocation is discussed later in this paper.

Finally, instructors must perform an assessment or wireless survey of the proposed laboratory space. Instructors must take into account the existing 802.11 WLANs present in the proposed laboratory space. With the limited number of 802.11b/g channels and varying numbers of students, care must be taken to ensure bandwidth is available. Sources of interference can ruin the effectiveness of this course module. Wireless handoffs are sensitive processes, and dropped frames can have dramatic impacts on the laboratory module. This module is intended to demonstrate to students how 802.11 handoffs don't always work the way they're supposed to, and how conventional wisdom regarding distribution systems does not always pan out.

It is recommended that instructors assign this course module to a small group of students, with no more than three people per group. If the available bandwidth is crowded with third party access points, instructors must attempt to stager when students can perform their packet captures.

Ideally, a set number of student groups would utilize all of the available bandwidth for their packet captures. Any remaining student groups should use the down time to analyze previously captured data or reconfigure their access points for further testing. These restrictions should be taken into account when defining enrollment limits for laboratory sections.

The mesh protocol utilized was proprietary and owned by Proxim. A dynamic protocol, the Proxim mesh distribution system identifies a "mesh portal" (the access point directly connected to the wired network) and "mesh access points" (802.11 access points that connect to one another and send outgoing traffic back to the portal). As of this writing, the IEEE is currently developing 802.11s, a set of standards defining wireless mesh distribution systems. These standards would greatly benefit this research, but are currently unfinished and a proprietary solution had to be utilized.

Proxim AP-4900M access points were utilized for this research. These models supported all three types of distribution systems (wired, WDS, and mesh) and are equipped with two separate radios. One of the radios was dedicated to 802.11b/g traffic, and one was dedicated to 802.11a traffic. There was no WEP/WPA security on any access points, and the AP was set to open authentication. The client utilized was a Dell Latitude D620, utilizing the built-in Intel PRO/Wireless 3945ABG 802.11a/b/g card with version 10.5.1.72 of the manufacturer's drivers. In each experiment, client handoffs were performed for both 802.11a and 802.11g. The wireless handoffs were captured with two separate laptops (both Dell Latitude D620s as well, with Atheros-based Cisco Aironet WLAN adapters), each running WildPackets' AiroPeek NX software. The handoff exchange was captured and analyzed. Also, in each experiment two access points were configured with the same SSID (the access points were in the same extended service set [ESS]). In the second experiment, a third access point was introduced. This third access point was not a part of the same ESS, and was deliberately configured to overlap channels with one of the other two access points. The third and final experiment involved the same two access points from the first experiment. However, this time both access points were configured to use the same channels for both 802.11a and 802.11b/g traffic. Table 2 summarizes the three separate experiments.

The Dell laptop used the default settings for the Intel PRO/Wireless drivers with one notable exception. The Intel drivers include a setting entitled "roaming aggressiveness." This setting controls when the client initiates the 802.11 handoff process. The default setting for roaming aggressiveness proved to be completely inadequate for this testing. The client would refuse to initiate the handoff process unless the signal strength with the associated access point became incredibly weak. By the time the client moved far enough away for the signal quality to drop appropriately, both access points had poor signal strength and the handoff process would usually time out. The conservative nature of this driver is understandable, given that most laptop users do not roam frequently between access points. However, for this experiment the "roaming aggressiveness" was set to the maximum value. This forced the client to handoff smoothly while walking between access points 'A' and 'B'.

Table 2: 802.11 Roaming/Handoff Experiments

Experiment #	Number of APs	SSIDs	Channels
1	2	One	Two different channels for both APs

2	3	Two	Two different with third AP overlapping one of the first two
3	2	One	Both APs on the same channel

3. Experiment Designs

3.1 Roaming Experiment #1: Wired, WDS, Mesh

The first experiment was designed to identify the impact the distribution system had on client handoffs between access points. In this experiment, two access points were utilized. Both access points were configured with IP addresses on the same subnet and within the same ESS. The access points were directly wired to a single unmanaged switch (both APs were in the same broadcast domain). Both APs had their transmit power set to 50% to limit cell sizes. See Figure 1 for the access point, sniffer, and client layout. During the experiment, the client connected to both the 802.11a and 802.11g networks and successfully roamed between access points. Client access channel allocation lists the channel allocation for both access points.

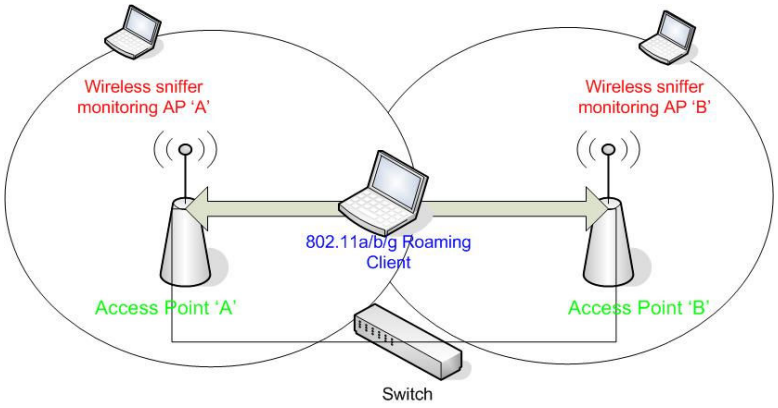


Figure 1: Roaming Experiment #1

Table 3: Client access channel allocation

802.11 Standard	Access Point 'A'	Access Point 'B'
802.11a	Channel 60 – 5.300GHz	Channel 52 – 5.260GHz
802.11g	Channel 6 – 2.437GHz	Channel 11 – 2.462GHz

After capturing several handoffs, the access points were reconfigured. The first change was disconnecting the access points from the switch. Both access points were configured for a wireless distribution system. In order to successfully configure a WDS, a radio had to be selected for the WDS and a radio had to be identified for client access. Whatever radio was selected for WDS had to share the same channel as the other access points in the WDS. In this experiment, the WDS was configured first on the 802.11a radios (using channel 60 at both ends). After capturing several handoffs, the WDS was reconfigured on the 802.11b/g radios and the 802.11a radios reset to the values in Table 3. Further handoffs were captured.

The final stage of the first experiment was very similar to the WDS distribution system. In the final stage, the proprietary mesh protocol was utilized. Proxim's mesh distribution system has the same channel allocation requirements as WDS (radios running the mesh protocol must be on the same channel)

3.2 Roaming Experiment #2: Third AP on overlapping channels

The second experiment was an exact duplication of the first experiment. However, for the second experiment, a third Proxim AP-4900M access point was configured and placed within close proximity to the previous two access points. See Figure 2 for the access point, client, and sniffer layout. The newly introduced access point 'C' was to deliberately introduce minor interference. AP 'C' was configured using the factory default settings, with a few exceptions. For the channel allocation, access point 'C' always utilized the same channels for both the 802.11b/g and 802.11a radios as access point 'B'. Additionally, the transmit power on both radios for access point 'C' were set to 50%.

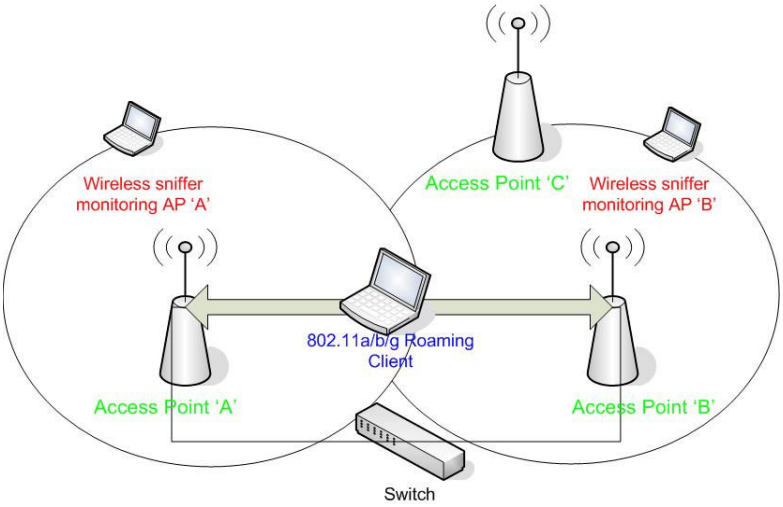


Figure 2: Roaming Experiment #2

3.3 Roaming Experiment #3 – Two APs on overlapping channels

The third and final experiment mimicked the first experiment. Only two access points were needed, the same access points 'A' and 'B' utilized previously. The only change was the channel allocation. In this experiment, both access points utilized channel 52 for the 802.11a radios, and channel 11 for the 802.11b/g radios.

4 802.11 Roaming

Due to the work performed by Mishra et al.[21] identifying the variability introduced by the client probing before initiating the handoff procedure, probe time was not counted in the handoff times. The desire was to study the most consistent part of the 802.11 handoffs, and note the impact of three different distribution systems on these handoffs. The impact of a third access point and co-channel interference was also measured. With that in mind, the handoff times were determined by measuring the time elapsed between the first authentication frame sent from the client to the AP and the reassociation response frame from the AP to the client finalizing the handoff procedure. For a detailed breakdown of the 802.11 handoff process, see Mishra et al.[21]

4.1 Roaming Experiment #1

The average handoff times (in milliseconds) associated with each of the three different types of distribution systems can be seen in Figure 3. The average handoff time and standard deviation for each distribution system and each 802.11 standard can be seen in Table 4: Experiment #1 Findings

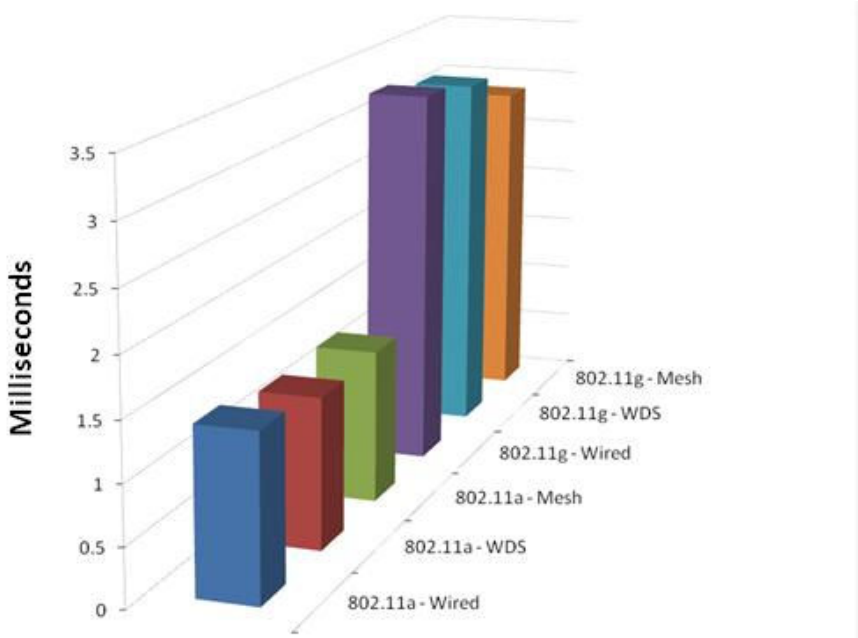


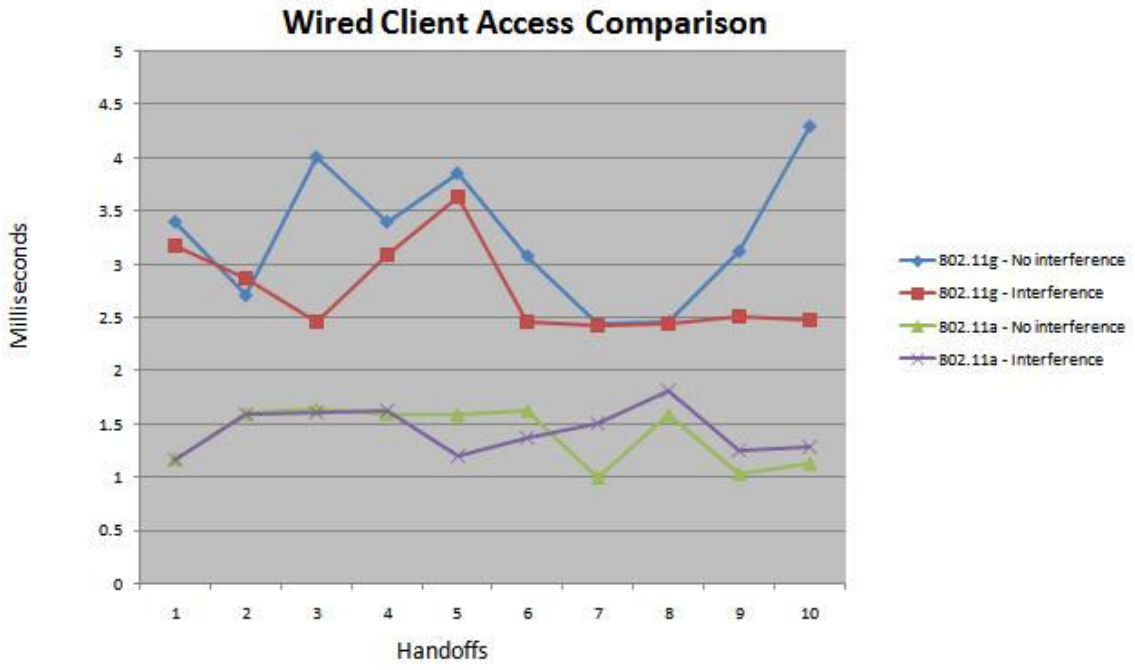
Figure 3: Experiment #1 - Average Handoff Times

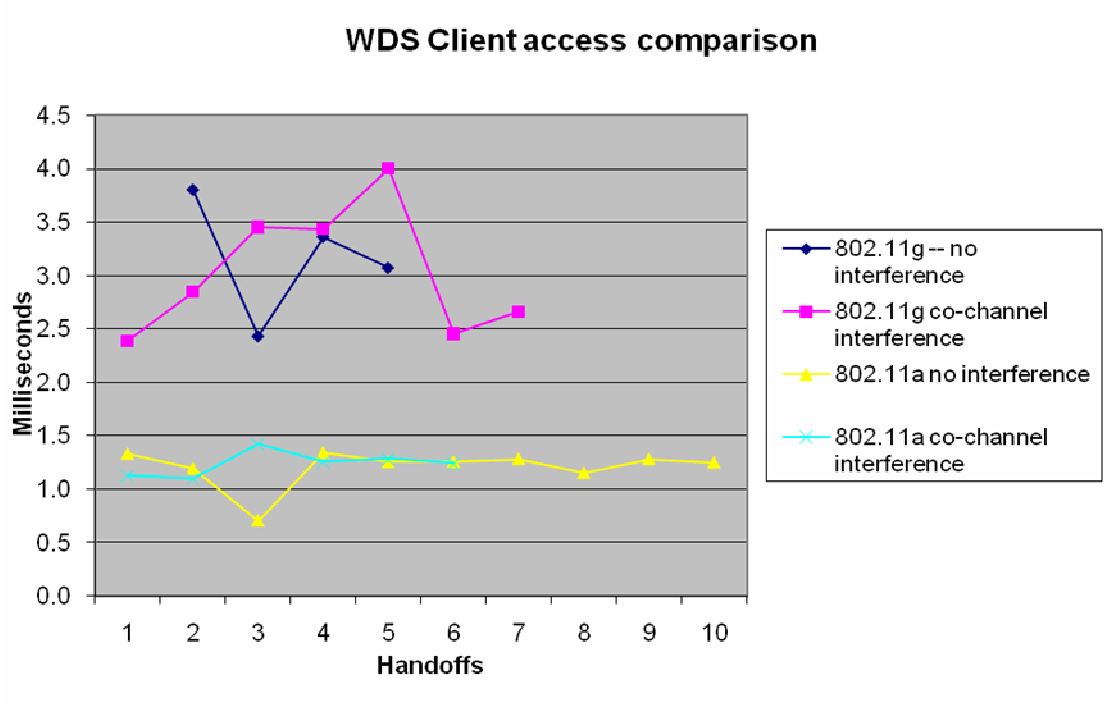
Table 4: Experiment #1 Findings

Distribution System	Number of Captured Handoffs	802.11a – Avg. Handoff Time (milliseconds)	802.11a – Standard Deviation (milliseconds)	802.11g – Avg. Handoff Time (milliseconds)	802.11g – Standard Deviation (milliseconds)
Wired	10	1.096	0.278	3.2788	0.64
WDS	10	1.285833	0.251	5.4442	5.113
Mesh	10	1.3148	0.136	2.8775	0.357

4.2 Roaming Experiment #2

The addition of a third access point had a minimal impact on the handoff times for both 802.11a and 802.11g radios. There were several clear outliers during this experiment, the result of the client or access point being forced to retransmit a frame during the handoff process. Since the retransmission of frames is built in to the 802.11 standards, these outliers are not surprising. Figure 4 illustrates the handoff timing both with interference from the third access point and without the third access point (values taken from experiment #1).


Wired Client Access Comparison
Milliseconds
Handoffs
802.11g - No interference
802.11g - Interference
802.11a - No interference
802.11a - Interference


WDS Client access comparison
Milliseconds
Handoffs
802.11g -- no interference
802.11g co-channel interference
802.11a no interference
802.11a co-channel interference

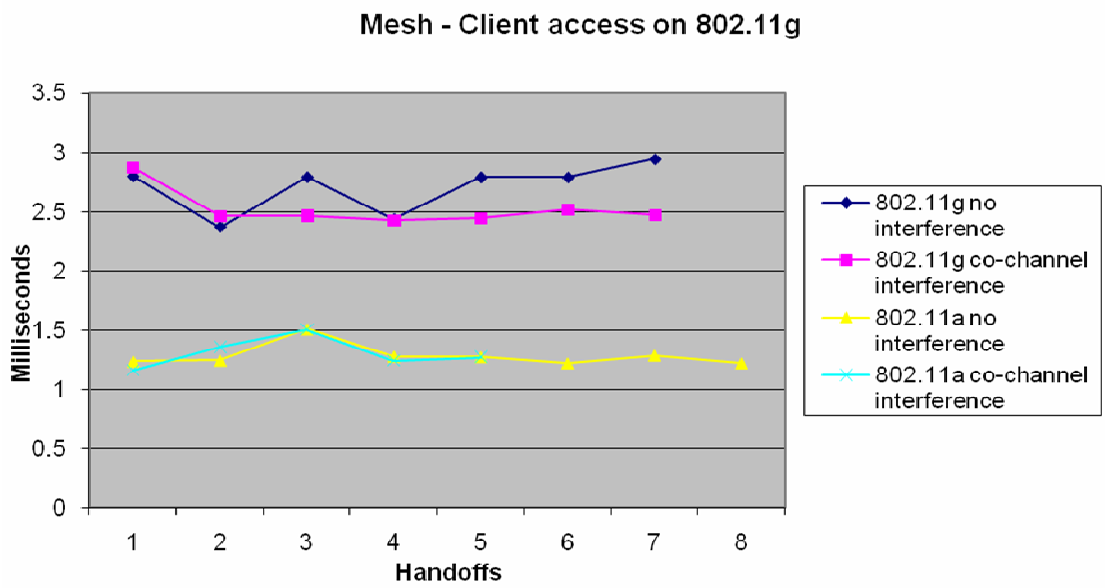


Figure 4: Experiment #2 Results

4.3 Roaming Experiment #3

The most surprising result from experiment #3 did not involve the data that was captured and analyzed. The most surprising result was the lack of data for 802.11a or 802.11g handoffs when the two access points were connected via a wireless distribution system. Figure 5 illustrates the handoff times for the wired distribution system as well as the times associated with the proprietary Proxim mesh protocol.

However, WDS proved to be a mystery. The client was able to successfully connect to both access points, and the client appeared to roam normally. A continuous connection was established throughout the entire experiment, and the client appeared in the respective access point's station table as being fully authenticated and associated. However, neither sniffer was able to see any authentication nor reassociation frames from either the client or the access points. Several attempts were made to contact WildPackets about the invisible frames without avail. The lack of WDS authentication and reassociation frames remains a mystery.

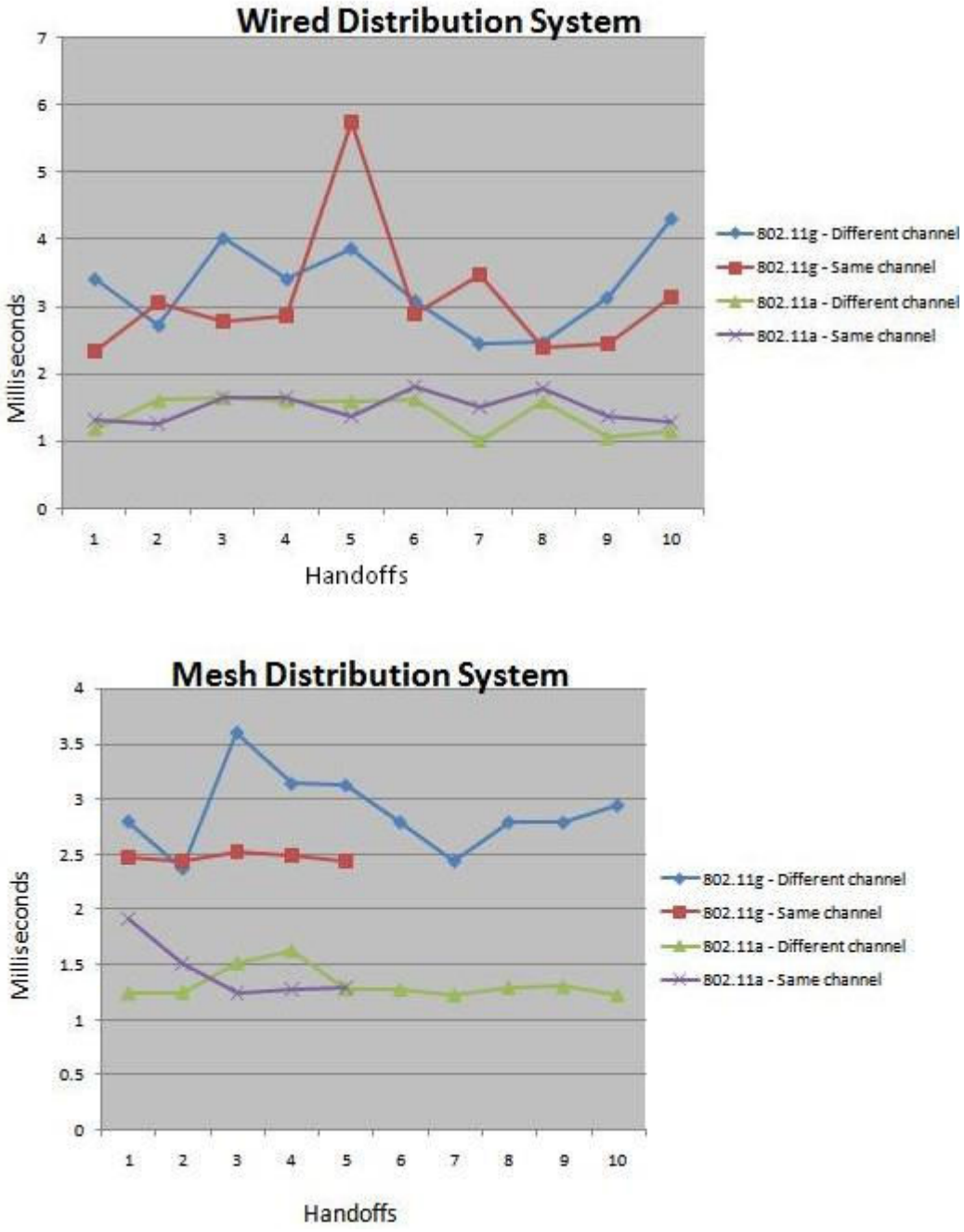


Figure 5: Experiment #3 Results

4.4 Results of Roaming Experiments

The most obvious conclusion drawn from the results listed was how superior the 802.11a handoffs were compared to its 802.11g counterpart. In every experiment, 802.11a produced faster handoffs than 802.11g. These findings were the same regardless of the distribution system or the degree of interference experienced during a handoff.

The second conclusion drawn from this research was not surprising. The wired distribution system was clearly superior to WDS and mesh when client access was running 802.11a. This

result is not surprising, because the wired distribution system is being compared against WDS and mesh running over 802.11g. However, what was unexpected was the mesh's performance when run over 802.11a. Combining mesh over 802.11a with client access on 802.11g, the average handoff time was faster compared to the wired distribution system. Additionally, mesh results had little variability. This is illustrated by the small standard deviation. Unfortunately, it is impossible to draw hard conclusions as to why the mesh protocol outperformed the WDS to such a degree. This is because of the proprietary nature of Proxim's mesh protocol. If the inner workings of the protocol were well documented, hard conclusions could be drawn.

Not surprisingly, both experiments #2 and #3 illustrated that interference does have a direct impact on the time required for a client to handoff between access points in an ESS. However, the interference isn't a show stopper, either. The client continued to function normally and complete successful handoffs in a timely manner when subjected to small degrees of interference. The system took a minor hit in terms of performance, but nothing that the end user would notice (a matter of microseconds). Bandwidth-intensive and/or low latency applications may be impacted by this extra handoff time, though.

Finally, co-locating 802.11 access points with the same channel do not provide any significant advantage regarding handoffs. At the same time, co-locating the same access points doesn't provide a significant disadvantage either. While the 802.11 handoff process is far from perfect, it is resilient.

5 Conclusions

These packet filtering modules helped observe actual authentication handshakes for WEP, WPA-PSK, VPN PPTP, and WPA Enterprise. The fifth module illustrated the handshake sequence for a SIP call. The sixth module documented the 802.11 handoff process and the potential impact imposed by various factors. All of these observations helped demonstrate the resilience of the 802.11-standard specification as most of these observations included retransmitted data packets alongside the normal management and control frames.

As described in the introduction, the need for training experts in wireless technologies without any programming experience can be satisfied using packet capturing as an educational tool because it adds value to the hands-on exercises they are already required to do for their curricula. These exercises make for a challenging undergraduate course module as they allow students to make decisions based upon their prior knowledge of networking and the lecture portion of their wireless networking course.

The characteristics of a contention domain become obvious as they begin to see retransmitted packets and the acknowledgments sent after each frame is transmitted over the air. Their knowledge is reflected in the analysis of their results which they conclude using the guiding questions provided in the lab phase description. They are required to respond with an analysis of how they came up with the models that were required for the exercises; this shows how much they understood the different parts of wireless networking such as the control, management, and data frames, as well as the physical layer components. The other two parts for analysis of results require them to respond with the business implications for each authentication method and the troubleshooting benefits of packet capturing.

The challenges facing wireless clients as they attempt to roam between access points have to be recognized by students. With user demand for mobility on the rise, it is imperative that students training in wireless networking be aware of the challenges posed by 802.11 roaming. By creating three unique experiments, students are able to replicate these experiments with minimal effort and witness the handoff process. Additionally, students must analyze the management frames during the exchange and draw conclusions about the impact of the distribution system and other variables. Students can then respond by proposing business solutions to potential challenges, and make educated decisions regarding implementation of large wireless networks.

As the techniques for teaching wireless networking continue to evolve, it is important to update and customize the course material / content to ensure that the latest techniques are being employed for teaching the subject matter. Also since these phases are portable, in that they can be conducted anywhere the basic technology required is available, the supply for wireless security professionals can be increased easily if other educational institutions incorporate them into their programs.

6 Implications for Further Research

Malik et al established a foundation for the further development of course modules focusing on the 802.11 MAC layer and frame analysis. This knowledge was utilized for the development of laboratory exercises for upperclassmen and graduate students focusing on wireless distribution systems, wireless mesh protocols, and their impact on handoff timing. With the modules in this paper providing foundational knowledge, other modules can be created to target more specific aspects of wireless networks such as traffic prioritization of the 802.11e standard, and the emerging standards such as 802.11r for fast roaming and 802.11s for mesh networking when they are finalized. The reasons they are not recommend for such modules prior to standardization is twofold: the packet analysis tools do not provide decoders for non-standard protocols, and non-standard protocols are often vendor-specific. Although decoders can be programmed and plugged into Airopeek and Packetyzer, the process of doing so would require students with prior programming experience; the modules presented in this paper are intended for courses whose prerequisites do not require such talent. These modules are also intended to be technology specific only and not vendor specific.

The roaming experiments developed for the final education module also leave several questions unanswered. Due to the costs associated with testing multiple brands of access points and clients, only Proxim AP-4900M access points and Dell Latitude laptops were available. Similar research could be done with a variety of platforms and APs, possibly with very different results. Additionally, the lack of data from the third experiment is troublesome. There is no clear answer to why two different laptops running WildPackets AiroPeek software could not detect any authentication or reassociation frames while utilizing WDS. The authors would very much like to see this issue resolved.

Packet sniffing and the consequent comparative analysis exercises can be used for a variety of other purposes. The most prominent example in this case would be for troubleshooting wireless networks only. There are a multitude of problems that can occur and cause service disruption. Troubleshooting-specific modules could potentially gain popularity as the reliance on wireless

networks continues to grow. Different modules could be created for a network whose performance is suffering from: a MAC address-spoofing client, a rogue AP falsely associating certain clients, virally-infected clients flooding the network, and signal jamming devices causing interference, among others. Modules that force examination and analysis of these real-world problems and allow students to troubleshoot them will undoubtedly provide invaluable experiential knowledge.

7 References

1. Danielsson, K. Employers to seek more security talent in '07 SearchSecurity.com: The web's best security-specific information resource for enterprise IT professionals, 2006.
2. De Santis, A. Il four way handshake Wireless Ethernet Universita Degli Studi Di Salerno, n.d.
3. Erten, Y.M. and Tomur, E. A layered security architecture for corporate 802.11 wireless networks. Wireless telecommunications symposium. 123-128.
4. Kapp, S. 802.11: leaving the wire behind. Internet Computing, IEEE, 6 (1). 82-85.
5. Krazit, T. PC sales exceed expectations: Increase in notebook sales is the key, researchers say PC World, 2003.
6. Microsoft. Understanding point-to-point tunneling protocol (PPTP) MSDN, 1997.
7. Midkiff, S.F. An experiential course in wireless networks and mobile systems. Pervasive Computing, IEEE, 4 (1). 9-13.
8. Midkiff, S.F., DaSilva, L.A. and Chen, I.-R. ECE/CS 4984: Wireless and mobile systems design Course materials, 2003.
9. Netgear. Wireless networking basics, Netgear, Santa Clara, 2005.
10. Noerenberg, J.W., II Bridging wireless protocols. Communications Magazine, IEEE, 39 (11). 90-97.
11. Planet3 Wireless. Introduction - CWNP career certifications, 2006.
12. Richards, B. and Stull, B. Teaching wireless networking with limited resources Proceedings of the 35th SIGCSE technical symposium on Computer science education, ACM Press, Norfolk, Virginia, USA, 2004.
13. Sarkar, N.I. Teaching computer networking fundamentals using practical laboratory exercises. IEEE Transactions on Education, 49 (2). 285-291.
14. Shin, M., Ma, J., Mishra, A. and Arbaugh, W.A. Wireless network security and interworking. Proceedings of IEEE, 94 (2). 455-466.
15. Snyder, J. Down and dirty with Wireless LAN security NetworkWorld, 2002.
16. Welch, D. Wireless security threat taxonomy. Information Assurance Workshop. 76-83.
17. WiFi Alliance. Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise WPA and WPA2 Implementation White Paper, 2005, 1-26.
18. Youssef, M.A. and Vasan, A. The ABC...I of 802.11 WLANs Crossroads: The ACM student magazine, 2003.
19. Kim, H. P. (2004). Selective Channel Scanning for Fast Handoff in Wireless LAN using Neighbor Graph. Proceedings of ITC-CSCC .
20. Liao, Y. a. (2006). Practical Schemes for Smooth MAC Layer Handoff in 802.11 Wireless Networks. Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks .
21. Mishra, A. S. (2003). An empirical analysis of the IEEE 802.11 MAC layer handoff process. ACM SIGCOMM Computer Communication Review .
22. Ramani, I. a. (2005). SyncScan: Practical Fast Handoff for 802.11 Infrastructure Network. Proceedings of IEEE Infocom .
23. Velayos, H. a. (2004). Techniques to reduce IEEE 802.11b handoff time. Proceedings of ICC .
24. Malik, R., Goldman, J., Hansen, R., and Smith, A. (2007). Laboratory Modules for Conducting Comparative Analysis of 802.11 Frames. Proceedings of SIGITE.