ENHANCING THE IN-CLASSROOM TEACHING/LEARNING EXPERIENCE USING WIRELESS TECHNOLOGY

Adegbile Adewunmi[1], Catherine Rosenberg[2], Adeoluwa Sun-Basorun[3], Simon G. M. Koo[4]

Abstract *- The widespread use of wireless technologies in our everyday lives has made their application to electronic-learning (e-learning) environments, such as the classroom, imminent. However, there are several security and authentication issues that must be addressed before wireless devices can be used in any teaching scenarios including those requiring examination/testing. This paper addresses some of the issues that currently hinder (and complicate) the introduction of such devices to the classroom. We discuss and propose solutions to the challenges of providing a secure, non-distracting, web-based wireless environment suitable for both class lectures and quizzing scenarios. We present a novel system which, regardless of class size, authoritatively determines who is logging on to utilize an e-learning application and whether a student is accessing the application from the classroom or otherwise. The system also allows for the instructor to monitor the ways students use their wireless devices, an issue critical to maintaining integrity especially in quizzing situations. In addition to being secure, we propose a system flexible enough to allow an instructor to selectively control Internet, intranet or Virtual LAN (VLAN) resources students have access to. Our proposed system provides a secure and easily adaptable environment that allows for the development of secure e-learning applications which will significantly enhance the classroom experience for both instructors and students.*

Index Terms – E-learning, VLAN, Wireless Applications.

INTRODUCTION

With college class sizes growing, and college campuses becoming increasingly diverse in terms of the student body and faculty, effective communication between instructors and their students is becoming quite challenging. The increasing diversity of the student body means instructors must tailor their lessons to effectively reach students from very different academic backgrounds. Larger class sizes make it difficult for instructors to give their students the personal attention they need. Students, notably international students, wary of their spoken English skills, and the more reserved students can be hesitant to ask questions in large class settings. This changing nature of the classroom environment is also making it difficult for instructors to gauge how effectively students comprehend the material being presented. There is an on-going effort in schools at all levels to improve the in-class experience for both students and instructors. Educators are increasingly realizing the potential of wireless technology to revolutionize the classroom environment.

The Internet has been used as an educational tool for quite a while. E-learning applications have however, typically been geared towards distant learning. Wireless networks introduce an exciting new potential to the growing relationship between technology and education. They allow e-learning applications to be introduced directly into the classroom, significantly enhancing the in-class experience for instructors and students alike. The classroom could become a much better learning and teaching environment if students and teachers could bring in their laptops, handhelds or PDAs and use them to enhance communication. Instructors could incorporate multimedia demonstrations into their lectures and receive real-time feedback from their students using quizzes or surveys. Students could anonymously pose questions to the professor, collaborate with other students in or out of the same physical classroom, easily review materials from previous lectures and use their Internet access for further research.

Running wires in small classrooms, not to mention large ones, to allow for the use of laptops is not economical and in many cases physically impossible (in particular if the instructor can rearrange the classroom furniture). This is why wireless networks can significantly change the classroom experience as in a matter of minutes a traditional classroom could offer the same benefits that could previously only be provided by a computer laboratory. In addition, as students and instructors can bring in their own devices, the classroom is not limited to serving specific purposes as computers laboratories sometimes are. A classroom could be used by computer science students taking an in-class programming quiz, an activity that probably requires restricting Internet access, and the very next period could be used by biology students researching on birds, which could require full-blown Internet access.

Once the initial setup of the network is done, there are no additional costs (monetary or time) incurred to use a classroom for a different purpose. The potential impact of such benefits on the classroom experience, and the increasing affordability of handheld computers and laptops have encouraged the deployment of wireless networks on

[1-4] School of Electrical and Computer Engineering and Center for Wireless Systems and Applications, Purdue University, West Lafayette IN 47907
{adewunmi, cath, adebash, koo}@ecn.purdue.edu

0-7803-7444-4/03/$17.00 © 2003 IEEE **November 5-8, 2003, Boulder, CO**
33rd ASEE/IEEE Frontiers in Education Conference

many campuses as was recently done at Purdue University, West Lafayette IN.

A large-scale introduction of e-learning applications into the classroom environment has been slowed considerably by the challenges encountered in setting up a secure, easily adaptable wireless network. Wireless networks are inherently less secure than their wired counterparts, as anyone with a wireless device can potentially use the network. Wireless devices can also communicate with each other "locally" without using the larger router-based infrastructure making it possible for a student to pass information to another student in the class or even in a close-by room without the network knowing it. Instructors must be confident that real-time quizzing applications for instance, do not result in a loss of integrity by giving students an avenue to cheat without being easily detected.

In addition, there is a fine line between wireless technology being a learning enhancer and a distraction to students in the classroom. Some teachers may not be comfortable with students having full Internet access during class, giving them an opportunity to surf the Web, chat, check e-mail or participate in non-class related activities. Others teachers may want to encourage activities requiring full Internet access, while some might want to restrict access to only few specified sites. The underlying wireless network must be flexible enough to support a variety of teaching styles and must be able to switch quickly from one style to another to meet the needs of instructors.

Most of the work done in the e-learning area is focused on creating educational applications that are easy-to-use for both students and instructors. The next section cites some of these works. Our work focuses on making Purdue Air Link (PAL) a wireless network that will allow for secure implementation of e-learning applications. Before highlighting the major networking problems that must be resolved, we present the PAL architecture on which our solutions are based. After highlighting the problems we present our platform-independent, network-based solutions to these problems. We end with our conclusions and avenues for future research.

RELATED WORKS

In [2] the authors tackled the question of whether mobile and wireless technologies add any value to higher education. Based on their experimentation with wireless devices in an Electrical Engineering class, they concluded that such technologies could significantly improve the learning experience. Their e-learning application allowed for the quizzing of students on their understanding of the material helping the instructor to tailor her lectures to meet students' needs. Similar work was reported in [1] as part of Project Numina. Laptops and handhelds were used to run similar software applications to collect responses from the students on various quizzes posed by the instructor. In the case of Project Numina however, instructors were able to plot the results of the quiz as charts or graphs which could also be made available to the students. Working with online collaboration software, the authors in [3] reported success in utilizing wireless devices in the classroom ([4] presented similar conclusions as a result of work done at SCALE (Sloan Center for ALN Environments) at UIUC).

All these works have focused on developing e-learning applications with little to no concern for the security of the underlying network. As most of these experiments have been run in controlled environments, this is not surprising. With results showing that there are tremendous benefits in integrating wireless technology into the classroom, we have focused on the design of mechanisms that will make an open network such as PAL (discussed below) a secure and flexible platform, allowing for the large scale deployment of various e-learning applications at Purdue University.

THE PURDUE AIR LINK (PAL) NETWORK

Purdue Air Link (PAL) is a campus-wide wireless network access service provided by ITaP (Information Technology at Purdue) at Purdue University. Upon the completion of the project in May 2003, over eighty buildings in the West Lafayette campus will have wireless connectivity. PAL partitions physical areas into interconnected cells, and adopts Wi-Fi compliant IEEE 802.11b technology to provide wireless access to the cells in infrastructure mode (each cell is served by a base station called an Access Point (AP)). The configuration of PAL is VPN (Virtual Private Network) based and is shown in Figure 1.

In PAL network, users are assigned private IP (Internet Protocol) addresses through a DHCP (Dynamic Host Configuration Protocol) server logically located inside the VPN, and these private IP addresses are valid only in one VLAN (Virtual Local Area Network) area. Once a device leaves a VLAN coverage (say coverage A) to move to another VLAN coverage (say B), it needs to get another private IP address reflecting that it is in VLAN B and the old IP address of the mobile device while it was in VLAN A is released to be used by other mobile devices within VLAN A's coverage area. PAL does not use IP masquerading or other similar techniques to provide Internet access to users, instead, a VPN box (Figure 1) is put at the edge of the VPN to provide a private-to-real IP addresses mapping.

All the traffic that runs across the VPN destined for the Purdue Intranet or the Internet will pass through the VPN box, and all the IP packet headers will be modified by the VPN box to provide real-to-private IP mapping (the reverse for the traffic sent to mobile devices). This configuration scales better than a simple subnet solution because there is a much larger range of private IP addresses available (PAL uses class A private IP addresses). It is also more scalable since adding new VLANs will not increase the local traffic on the existing VLANs. Note that users must provide a Purdue account username and password to the system before the VPN box will perform any mapping services for them.

The system will check this username and password pair with the user authentication server located in the Purdue Intranet, and once the user is authenticated, the VPN box will perform the private-to-real-IP mapping and the reverse mapping throughout the session. Furthermore, IPSec [5] is deployed to provide better security. In order to use PAL, a mobile user must install the PAL VPN client software on the mobile device. The client establishes an IPSec tunnel between the device and the VPN box, a requirement for any data transfer to take place.

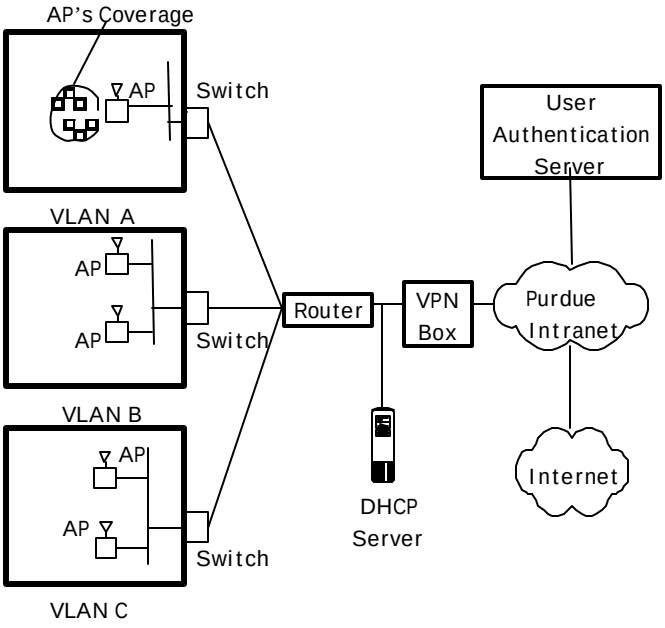

FIGURE 1
THE PURDUE AIR LINK (PAL) NETWORK

PROBLEM DEFINITION

Introducing wireless technology into a classroom environment brings up two major issues; the control of *local computer resources* and the control of *network resources*. Using a personal wireless device in the classroom allows students to go from class to class taking advantage of e-learning applications without much hassle. It also brings up the problem of what applications a student should be using during class. Instructors could be wary (and for good reason) that students will abuse the opportunity to bring in their own devices by playing games or writing papers for other classes for example.

Although our work has focused mainly on the problem of network resources, we realize that local resource issues could hamper the use of e-learning applications in test scenarios for example. Instructors must be satisfied their students will not use any forbidden resources (such as an electronic encyclopedia), and that any violators will be caught.

While wireless technology can significantly enhance the in-class experience for students and instructors alike, we must be careful that it is being used as a tool to supplement the instructor's efforts and not taking away any of the instructor's control of the classroom. Understanding that different instructors have different teaching styles and thus require different network resources for their classrooms is critical.

In addition an instructor could require different resources for different lectures, for example full Internet access for in-class research on a subject for one lecture but Intranet access only to access course notes for a another lecture. One instructor could require students be present in class while another might not care that students get access to the same information out of class. The underlying wireless network must be flexible enough to meet these challenges. The network resources problem can be split into three sub problems: flexible Internet/Intranet access, undesirable ad-hoc networks and the next room problem.

Internet/Intranet Access

Any Purdue student or staff with appropriate hardware is authorized to use PAL, allowing access to Internet and Intranet resources almost anywhere on the campus. The Internet/Intranet problem involves restricting the access of students using wireless devices in class to network resources. This must be done in a flexible manner and should depend on the instructor's criteria. A variety of wireless environments are necessary to teach the various classes at Purdue. Certain instructors could require their students to have Internet/Intranet access but might want to prevent them from checking their e-mail. Other instructors might allow access to Intranet resources only. Still other instructors might want to restrict all Internet/Intranet access.

Our solution will involve the design of mechanisms to be added to PAL to make it flexible enough to meet all such requirements. Instructors should be able to change their requirements at any time during the class period, i.e. PAL should not require prior specification of such requirements. Such flexibility allows instructors to modify the format of their lectures on the fly. An instructor allowing access to all network resources might decide to give a quiz during class, a situation that might require no Internet/Intranet access. In addition, our changes to PAL must restrict access of students only when they are in their classrooms. Students out of the classroom should have full access to all network resources.

Undesirable Ad-hoc Networks

Students operating their laptops or PDA's in ad-hoc mode can form a network without using the PAL infrastructure. Students could communicate illegally with other wireless devices within range be the device in or out of the classroom. This is unacceptable in most testing or quizzing situations and could be undesirable even during certain lectures. Once again we point out that our additions to the PAL network must be flexible enough to allow students to

form ad-hoc networks if the instructor permits it. Based on the Purdue Air Link (PAL) network setup, we have come up with a solution that can prevent such communication if the instructor so desires.

The Next Room Problem

Monitoring class attendance could be critical in using the wireless network for testing and quizzing situations especially for large class sizes. It could also be used simply for assigning attendance points. The next room problem results from the fact that a one-to-one mapping of a classroom to an AP does not necessarily exist. One AP could cover several small classrooms while a large classroom may require several APs to be properly covered. Given such configuration possibilities a student not in a classroom but still within range of one of the classroom APs (say in the next room) could be wrongly assumed to be in class. In addition to this, since it is possible for one AP to cover multiple classrooms probably having different requirements, the solution must be AP independent.

SOLUTIONS

Internet/Intranet Access

To solve the Internet/Intranet problem, we introduce the notion of a "FireClass" server. This server has a physical or logical connection with the VPN box and will be responsible for filtering all in-class traffic (Figure 2). At the beginning of a class period, the instructor and the students present in the classroom will login to the FireClass server specifying a class identifier e.g. ECE 495R. Anyone without a valid Purdue account will be unable to access FireClass, as logging on to PAL is a prerequisite for connecting to the server. Upon logging on to FireClass, the server can associate either a MAC address or private IP address with each student or instructor in a class. As a result different wireless devices can be used for different classes and even for different class periods of the same class.

FireClass decides on the legality of the traffic or network access for a particular class based on criteria specified by the instructor. In order to have as flexible a system as possible, instructors must be able to change such criteria relatively easily, but more importantly should be able to make the change whenever they want. Based on specified criteria, FireClass informs the VPN box on what constitutes illegal traffic for a particular user, and the VPN box disallows (i.e., filters and discards) such traffic. The astute observer would realize that the VPN box could be programmed to do the job of FireClass. The reason we do not take this approach is that instructors will have access to FireClass making it a possible security risk. Having a different server to do the work of FireClass ensures that if FireClass is compromised, the network will work without any problems.

Flexibility of our system demands that different instructors should be able to define allowable traffic differently. It could be as simple as all Internet traffic from students registered as being in-class being blocked or as complicated as allowing only specific application level protocols to be used [by students] or specific destination addresses to be reachable [by students]. FireClass is a network solution allowing wireless devices, regardless of platform, secure and flexible use of e-learning applications on PAL.

Undesirable Ad-hoc Networks

To prevent students from forming undesirable ad-hoc networks, the students will be required to login to FireClass as soon as they are in class forcing their wireless devices to operate in infrastructure mode. As laptops or PDAs cannot operate in both infrastructure and ad-hoc modes simultaneously, FireClass can be used to notify the instructor either immediately or at a later time as to when a student logs out of the server. Immediate notification, gives an instructor an opportunity to check that the student is not illegally forming an ad-hoc network as opposed to being disconnected from FireClass for other reasons.

A somewhat related problem of controlling local communication across an AP is nullified by the fact that PAL runs on IPSec in a tunneling mode. With a different network configuration, devices on the same AP aware of each other's IP addresses could send information directly to one another without involving the VPN box. As a result of the tunnel between each wireless device and the VPN box in the PAL configuration, all traffic regardless of its destination passes through the VPN box. This ensures that FireClass has a chance to decide on the "legality" of the traffic, ensuring that no illegal communication takes place.

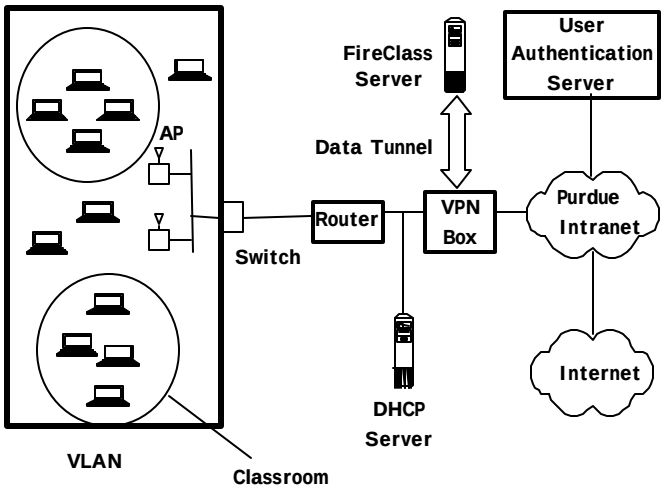

FIGURE 2
FIRECLASS ON THE PAL NETWORK

The Next Room Problem

Monitoring attendance can only be successfully accomplished once the next room problem is solved. Such a solution ensures that only students physically in class [as compared to login in from a remote location] are considered present. To tackle the next room problem we propose using a Password of the Day in addition to a Monitor application (responsible for keeping track of students physically in class) on FireClass. After login into FireClass, a student can attempt to login into Monitor. The instructor will have an application which allows for specifying the Password of the Day and how much time the students have to enter the password for Monitor.

Once the setup is complete, a pop-up window appears on the students' devices requiring them to enter the password of the day. Only students who are in class and can hear the instructor say or write the password will be able to provide the correct password in time. Students entering the correct password are marked present (by Monitor) and after the time specified by the instructor, Monitor stops accepting passwords. Students out of class but under coverage of the classroom AP(s) will have no knowledge of the password.

A location discovery mechanism like the one on PAL [6] could help limit the number of illegal login attempts to Monitor. Each class would have an AP or a number of APs associated with it. Any attempt to login to Monitor from a device not connected to one of the specified APs is blocked. If wireless devices are the only ones used in class, another level of security can be added to Monitor's implementation. Wireless devices unlike their wired counterparts have private IP addresses, as their IP addresses are not fixed. Consequently the VPN box can differentiate between the two, allowing Monitor to deny any login attempts from wired devices. Once again our solution applies regardless of the platform on the wireless devices being used. Figure 3 summarizes the Password of the Day and Monitor solution.

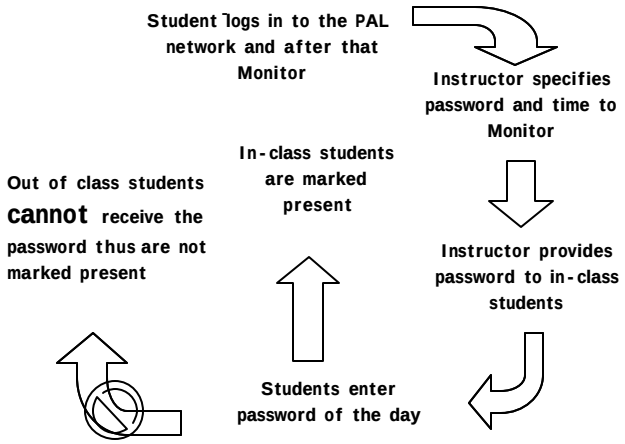

FIGURE 3
PASSWORD OF THE DAY AND MONITOR IMPLEMENTATION

CONCLUSION

Previous work on bringing wireless technology to the classroom has focused on developing e-learning applications without much concern for the security of the underlying network. Our work focuses on providing network dependent, platform independent solutions to the challenges that must be met to provide a secure network for e-learning applications.

One major challenge is how to control what type of access students have to Internet/Intranet resources. Diversity in teaching styles of instructors and class material demands a flexible solution. Full Internet access could be required for some of the class period for say research purpose, but may be undesirable for a quiz at the end of the class. Our FireClass server allows for such flexibility, giving instructors the opportunity to change the students' level of Internet/Intranet access whenever they see fit while ensuring that students do not violate their access permissions. FireClass also takes care of the problem of students forming undesirable ad-hoc networks.

Finally we solve the next room problem, presenting a solution that ensures that only students in class are considered present. Even students with wireless devices covered by the same AP(s) as that of the classroom, but are not in class will not be mistaken for being in class.

We have presented solutions to the major challenges of implementing a flexible, platform-independent, network dependent secure wireless network to facilitate the growing relationship between education and wireless technology. Our work will help inspire the necessary confidence in educators to take advantage of the various e-learning applications available to them.

ACKNOWLEDGEMENTS

This work has been supported in part by the 21st Century funded Indiana Center for Wireless Communications and Networking. The Authors would also like to thank John Campbell and Ed. Evans from ITaP for useful discussions and Hewlett Packard for their support

REFERENCES

[1] Shotsberger, P, G, Vetter, R, "Teaching and learning in the wireless classroom", *Computer*, Vol, No 34, March 2001, pp 110-111.

[2] Holmes, A, Schmidt, K, J, "Do mobile and wireless technologies add value to higher education", In Proceedin gs of Frontiers in Education (FIE), Boston MA. Vol, No 1, November 2002, pp 455-458.

[3] Griffioen, J, Seales, W, B, Lumpp, J, E, "Teaching in realtime wireless classrooms", In Proceedings of Frontiers in Education (FIE), Tempe AZ, Vol, No 2, November 1998, pp 748-753.

[4] Oakley, B, II, "The Virtual Classroom: At the cutting edge of higher education", In Proceedings of Frontiers in Education (FIE), Salt Lake City UT, Vol, No 1, November 1996, pp 135-139.

[5] Kent, S, Atkinson, B, "Security Architecture for the Internet Protocol", RFC 2401, Nov 1998.

[6] Koo, S. G. M., Rosenberg, C., Chan, H. -H., and Lee, Y. C., "Location Discovery in Enterprise-based Wireless Networks: Implementation and Applications", In Proceedings of the 2nd IEEE Workshop on Applications and Services in Wireless Networks (ASWN 2002), Paris, France, Jul 3-5, 2002.