UNWIRING BUSINESS NETWORKS:
SECURITY AND PERFORMANCE ISSUES OF WIRELESS NETWORKS

Tiki Suarez, Florida Agricultural & Mechanical University, tiki.suarez@famu.edu

ABSTRACT

The focus of this paper is to describe and evaluate the security hazards and risks involved with wireless LANs within a business environment, present performance issues that must be addressed and introduce a new protocol, Intelligent Wireless Management (IWM) to enhance network performance. Performance evaluation is based on the results of experiments conducted using the network simulator (ns).

Keywords: wireless, networking, security, performance, intelligent, simulation

INTRODUCTION

The current widespread use of business and industry mobile communications has encouraged research in wireless networks, specifically the 802.1X standard, with how to secure its transmissions and improve performance. Recent wireless networking initiatives are aimed to make wireless local area networks (WLANs) even more ubiquitous, faster to connect and easier to employ. However, this freedom and flexibility comes with a price. Wireless networks such as these are completely insecure if used in a common mode of operation [2]. Furthermore, although the performance gap of wired and wireless networks is closing considerably, overall performance of wireless networks using standard transmission protocols is oftentimes less than its wired counterparts [3]. The main reason is that wireless link transmissions are often lossy (error-prone) and quite bursty and furthermore, protocols presently used to transport data were created for wired networks [1].

This paper examines and addresses the obstacles of wireless networking security, presents performance issues and briefly introduces a new protocol, Intelligent Wireless Management (IWM) to enhance network performance.

The remainder of the paper is organized as follows: Section 2 presents an overview of wireless networks. Security hazards and risks are presented in Section 3. A discussion of performance issues follows in Section 4. An introduction of Intelligent Wireless Management along with performance evaluation results are displayed in Section 5. Conclusions follow in Section 6.

WIRELESS NETWORKS

Wireless local area networking (WLAN), and more specifically 802.11 networks, has revolutionized the way business organizations, institutions and homeowners connect to their computers. The benefit of increased productivity through mobility encourages these entities to install wireless access to their existing fixed Ethernet network. In addition, WLANs are increasingly being deployed over hot spots such as hospitals, hotels, airports, cafes and other areas from which individuals can have untethered public access to the Internet. The deployment of wireless communications is even desirable for business field devices such as industrial automation and process control, where wiring might not be feasible and/or not cost-effective.

802.11 refers to a family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for WLAN technology [7]. 802.11 specifies an over-the-air interface between a wireless client (also known as a wireless node) and a based station located within a limited physical area. There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.

The 802.11b standard, often referred to as Wireless Fidelity (Wi-Fi), operates in the 2.4 GHz range offering data speeds up to 11 megabits per second (with a fallback to 5.5, 2 and 1 Mbps). Newer standards are promising five times the speed. The most recent draft standard, 802.11g, was approved by the IEEE Standards Board on June 12, 2003 [12]. Publication is scheduled to occur in July 2003. 802.11g offers wireless transmission over relatively short distances at up to 54 megabits per second (Mbps) compared with the 11 megabits per second of the 802.11b standard. Like 802.11b, 802.11g operates in the 2.4 GHz range and is thus compatible with it. Figure 1 shows the technology that is used to create a WLAN.

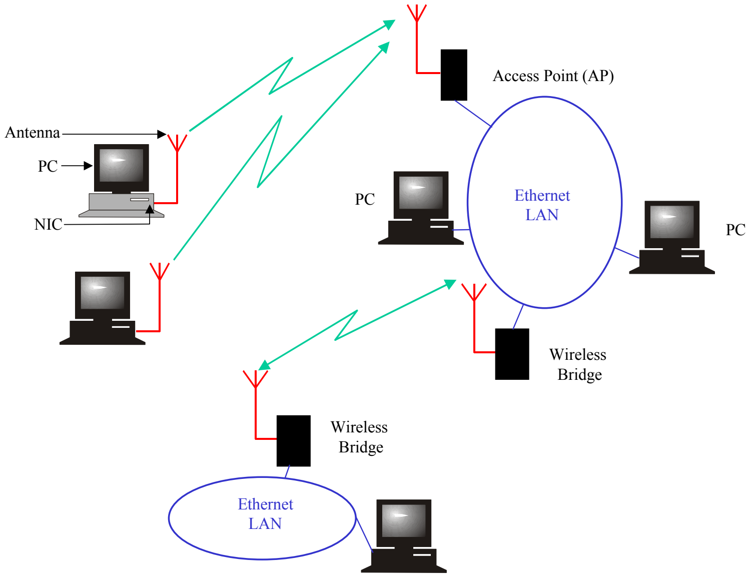

Figure 1: Building Blocks in WLAN

Since WLANs provide the transmitted data to anyone with a receiver that is in radio range, one must consider WLAN traffic as being delivered to unauthorized users. With the use of directional antennas, an unauthorized user desiring to eavesdrop on transmissions can be quite far away. This user also has the ability to inject or forge packets onto the network. Unless adequately protected, Wi-Fi wireless LANs are susceptible to access from the outside, some of whom have used the access as a free Internet connection.

SECURITY HAZARDS AND RISKS

Wireless networking has raised some very distinct and compelling issues. The most crucial issue is security. In the common mode of operation, wireless LANs are open to hackers trying to access sensitive information or spoil the operation of the network. Most wireless LANs do not implement any form of reliable security, enabling access to just about anyone. This section explores the IEEE 802.11 standard data confidentiality mechanism, its problems, and discusses both short-term and long-term solutions.

The data confidentiality mechanism for the IEEE 802.11 standard is known as Wireless Equivalent Privacy (WEP) [5]. WEP is based on protecting the transmitted data over the RF medium using the RC4 encryption algorithm and a shared key. When enabled, WEP only protects the data packet information by encrypting the body of each frame. This is supposed to keep hackers from viewing sensitive data such as e-mails, user names, passwords and proprietary documents. However, WEP does not protect the physical layer header and other stations on the network can listen to the control data needed to manage the network. WEP also uses a single shared key common to all users of a WLAN and this common key is often stored in software-accessible storage on each devices. Hackers can fairly easily decode WEP-encrypted information after monitoring an active network for only a few hours. Consequently, networks can not depend on WEP for protecting sensitive information.

The IEEE 802.11 Task Group i (TGi) is developing the new WLAN security protocols [8]. The short-term data link security protocol solution is named Temporal Key Integrity Protocol (TKIP). TKIP works on top of WEP, offering stronger security than WEP, and increased assurance that data will not be compromised. It incorporates a rapid re-keying protocol that changes the encryption key about every 10,000 packets. Installation requires firmware and driver upgrades. TKIP, intended only as an interim solution, wraps WEP in three new elements:

- A per-packet key mixing function to prevent attacks,
- A message integrity code, called Michael to defeat forgeries [4], and
- A packet sequencing discipline, to defeat replay attacks, thus fixing the known flaws of WEP.

The long-term data link security protocol solution is named Counter-Mode-CBC-MAC (CCMP) [6]. As with TKIP, CCMP addresses all know WEP deficiencies. In addition, CCMP provides freedom from limitations associated with currently-deployed hardware. CCMP utilizes the Advanced Encryption System (AES) encryption algorithm [8]. AES encryption is more robust than RC4 and enables interoperability with the older devices, but only by using weaker security technologies. Table 1 displays a comparison of security protocol features.

	WEP	*TKIP*	*CCMP*
Encryption Algorithm **Cipher Key Size(s)**	RC4 40- or 104-bit encryption	RC4 128-bit encryption, 64-bit authentication	AES 128-bit
Key Lifetime Per-packet key	24-bit wrapping IV concatenate IV to base key	48-bit IV TKIP mixing function	48-bit IV Not needed
Integrity Packet Header	CRC-32 None	Michael Enforce IV seq.	CCM Enforce IV seq.

Table 1: Comparison of security protocol features

PERFORMANCE ISSUES

Despite suffering from well-documented security problems, large corporations have rolled out and are continuing to roll out 802.11-based LANs. As these networks operate in the unlicensed 2.4-GHz band, they are subject to interference in both indoor and outdoor topologies. Performance is shown to depend not only on transmission rate and transmit power but on the product's response to multipath and obstructions in the environment along with the radio propagation path. This section describes several performance issues still plaguing both indoor and outdoor WLAN deployment.

Interference

If the performance of WLANs is suboptimal, the problem may be the result of high network utilization or possibly interference due to external Radio Frequency (RF) sources. For 2.4 GHz wireless LANs, there are several sources of interfering signals, including microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

RF signal dispersion for indoor wireless areas is often highly disturbed [12]. This is usually due to reflection, diffraction and scattering of the RF signal which is dynamic and difficult to predict [13]. Small changes in position or direction of a receiver (relative to a transmitter) may result in wide variations in signal strength. Within office structures, RF propagation is dependent on office dimensions, obstructions, materials, and signal frequency. Consequently, WLAN range data performance is highly dependent upon the surrounding physical environment.

Another impact to range performance in dense office environments can be the choice of the antenna [11]. With a properly selected antenna the effects of multipath can be reduced and the range improved.

Outdoor wireless environments affect the network performance in similar ways. WLANs can be corrupted by interference due to propagation and attenuation. High signal-to-noise ratios and interference due to shadow fading (i.e., signal attenuation due to buildings and other objects) are other common variables that affect a wireless physical medium.

Fine Tune the Network

To ensure optimal performance, be aware of the network's configuration parameters and fine tune them based on the network's behavior. As an optional feature, the 802.11 standard includes the ability for radio-based network interface cards (NICs) and access points to segment packets for improving performance in the presence of interference and marginal coverage areas. In addition, through the proper use of Request to Send/Clear to Send (RTS/CTS), one can fine-tune the operation of the WLAN depending on the operating environment. Keep in mind, however, that an increase in performance using RTS/CTS is the net result of introducing overhead (i.e., RTS/CTS frames) and reducing overhead (i.e., fewer retransmissions).

INTELLIGENT WIRELESS MANAGEMENT

The majority of applications in today's Internet use Transmission Control Protocol (TCP) and 802.11 compatible WLAN products are designed to operate with TCP/IP. However, current WLANs do not jointly optimize wireless link and network protocols during operation [11]. Instead, trade-offs between data rate and signal strength are fixed at "design time." In addition, the condition of the wireless channel tends to be highly dynamic. Such networks may suffer from excessive data loss caused by RF interference and frequent and prolonged connection drop-outs.

While new WLAN standards reduce the frequency of drop-outs, it also presents applications with the challenge of effectively using a network with varying capacity. Intelligent Wireless Management (IWM) improves network performance based on the state of the highly dynamic wireless channel. Network performance is not limited to the worst case scenario with the integration of IWM's network layer and physical channel management. This section briefly introduces IWM and provides a subset of simulation results.

IWM is a meta-layer that maintains characteristics of the wireless link and executes modifications to the link layer protocol based on the information that is received. IWM maintains these error characteristics to efficiently retransmit lost or dropped packets by identifying non-congestion related errors, modifying the link layer protocol, and adding adaptively aggressive timeout and retransmission policies.

Implementation is designed to for networks that experience lossy links, out-of-order packet delivery, dynamic changes in delay, and limited bandwidth. The first technique modifies the link layer protocol to provide reliable transmission of data over the wireless link. Using aggressively adaptive error-recovery mechanisms, segmentation and reassembly, fault-tolerant techniques based on information redundancy, and estimates of wireless conditions (i.e. good fade and bad fade time) along with round-trip delay. The second technique is an Intelligent Wireless Management (IWM) knowledge base that maintains the characteristics of the wireless link. IWM controls the retransmission of lost or dropped packets by identifying non-congestion related errors, modifying the link layer protocol, and adding adaptively aggressive timeout and retransmission policies.

The goal of our protocol is to provide a link layer that is reliable and transparent to higher layers, is aggressively adaptive and incorporates an Intelligent Wireless Management (IWM) knowledge base meta-layer which makes modifications to the link layer based on wireless conditions.

Performance Evaluation

Performance evaluation is based on the results of experiments conducted using the network simulator (ns) [9]. The simulated network consists of a simple wireless network interconnecting wireless nodes to access points. Experiments show that the overall wireless performance of TCP is significantly improved by using the link layer / IWM knowledge base meta-layer combination.

Table 2 displays a small subset of simulation results comparing the throughput under adverse bursty wireless conditions with IWM (right) and without IWM (left). For higher error rates the throughput of the network without IWM significantly decreases, while the opportunistic network with IWM increases throughput by at least 46%.

	without IWM	with IWM	
Simulations	**Throughput (KB)**	**Throughput (KB)**	**Throughput Improvement**
Goodfade – High Packet Loss Badfade	1879.687	3413.671	≈ 80%
Goodfade with Small Delays - High Packet Loss Badfade	1523.437	2234.765	≈ 46%

Table 2: Simulation Run Output

Multiple simulation runs concentrated on a high rate of packet loss during each bursty bad fade period. The primary objective is to specifically focus on the effectiveness of the IWM meta-layer in handling losses under adverse bursty wireless conditions. Each run performed without using IWM induced TCP congestion control mechanisms, thus ultimately degrading the performance of the network.

For each simulation run, packet traces are obtained as graphical output from the simulator. The following graphical output provides a small summary of experimental results. The **Throughput** graph displays the throughput performance of the network. The horizontal-axis shows the time in seconds, while the vertical-axis denotes packet number mod 90.

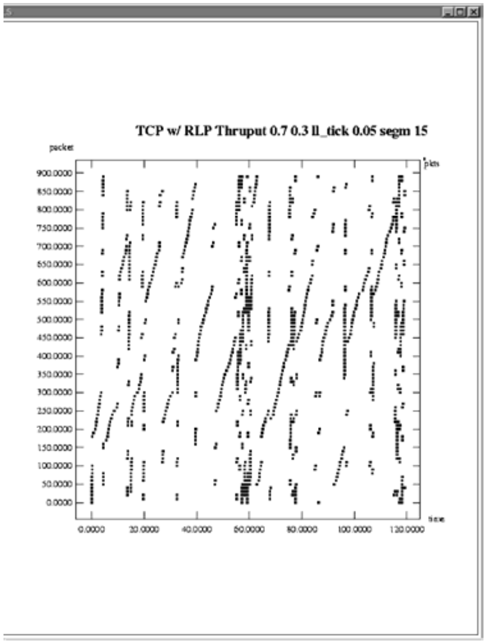

Figure 3: Throughput output without IWM

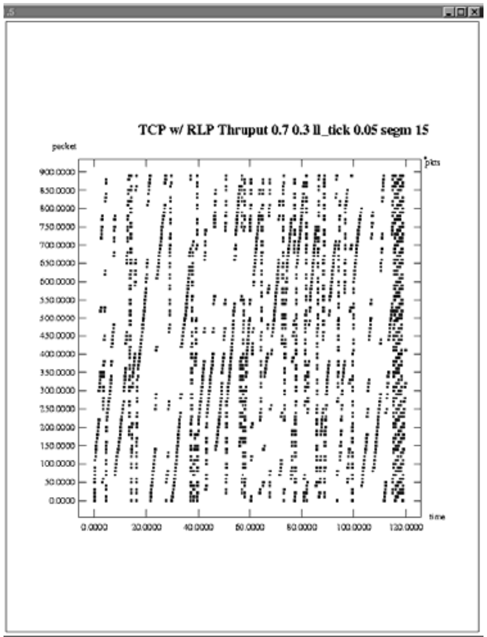

Figure 4: Throughput output with IWM

Figure 3 graph shows the network throughput performance is 3172.265 Kbytes. Figure 4 displays network throughput performance is 5076.562 Kbytes. A comparison of these two graphs clearly shows a 60% throughput increase with IWM to without IWM, verifying the throughput improvement due to IWM.

Results confirm that IWM effectively uses the characteristics of the physical medium. IWM makes intelligent decisions based on these characteristics to modify the link layer protocol. Furthermore, these results confirm that IWM can effectively improve performance in the heavier instances (worst-case scenarios). Overall, simulation runs with IWM were able to improve the performance by more than 46% over simulation runs without IWM.

CONCLUSION

As increasing numbers of businesses and institutions adopt WLAN technology, critical interference and security issues cannot be ignored. This paper attempts to educate users about the open nature of WLANs by briefly addressing the security flaws in the 802.11 data link protocols and describing interim solutions created to deal with its vulnerabilities. A discussion of performance issues is given and a new protocol, Intelligent Wireless Management (IWM) is briefly introduced. IWM is a meta-layer that improves WLAN performance. IWM maintains characteristics of the wireless link and executes modifications to the link layer protocol based on the information that is received.

REFERENCES

1. Balakrishnan, H., Padmanabhan, V. H., Seshan, S. and Katz, R. H. (1997). A Comparison of Mechanisms for Improving TCP Performance over Wireless Links, IEEE/ACM Transactions on Networking, 5(6), 756-769.
2. Borisov, N., Goldberg, I. and Wagner, D. (2001). Intercepting Mobile Communication: The Insecurity of 802.11, MOBICOMM 2001, 180-188.
3. Elaarag, H. (2002). Improving TCP Performance over Mobile Networks, ACM Computing Surveys, 34(3), 357-374.
4. Ferguson, N. M. An Improved MIC for 802.11 WEP. IEEE 802.111 doc 02-020r0, Jan. 17, 2002; grouper.ieee.org/groups/802/11.
5. Fluhrer, S., Mantin, I., and Shamir, A. (2001). Weaknesses in the key schedule algorithm of RC4. Fourth Annual Workshop on Selected Areas of Cryptography.
6. IEEE P802.11 Wireless LANs Alternate Text for TGi 8.3.4 (2002). Available at http://eecs.oregonstate.edu/~zier/ece679/Alternate_Text_for_TGi_834.pdf
7. ISO/IEC 8802-11 ANSI/III std 802.11-1999. Information technology – Telecommunications and information systems, Local and metropolitan area networks, specific requirements - Part 11: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) specifications.
8. National Institute of Standards and Technology. Advanced Encryption Standard (AES). FIPS Pub 197.
9. Network Simulator. (2000). Available at http://www.isi.edu/nsnam/ns/index.html.
10. Rappaport, T. S. (1996). Wireless Communications Principles and Practice, IEEE Press/Prentice Hall PTR New Jersey.
11. The Working Group for Wireless LANs, IEEE P802.11(2003). Available at http://www.ieee802.org/11/
12. Wu, H., Peng, Y., Long, K., Cheng, S., and Ma, J. (2002). Performance of Reliable Transport Protocol over IEEE 802.11 WLAN: Analysis and Enhancement. IEEE INFOCOM.