https://doi.org/10.48009/2_iis_2005_331-337

RECENT WIRELESS LAN MANAGEMENT TECHNOLOGIES: TRENDS AND OUTSTANDING ISSUES

Young B. Choi, James Madison University, choiyb@jmu.edu
Jae-Yoon Park, James Madison University, park4jx @jmu.edu
Daniel Fernandez, James Madison University, fernandr@jmu.edu
Kook-Bong Kim, James Madison University, kimkj @jmu.edu

ABSTRACT

This paper describes how outstanding issues and trends in Wireless LAN (WLAN) management technologies affect the IT world. The research results show that the usage of Wireless LAN technology is growing exponentially and the industry is striving to continuously to cope with the outstanding issues and trends.

Key Words: Wireless Local Area Network (WLAN), Smart Access Points, WLAN Switches, IEEE 802.11, HomeRF, Hot Spot, WEP, Shared Static Key, UTP, Optical Fiber, Radio Frequency ID (RFID), G4, Ultrawideband (UWB), Propagation

INTRODUCTION

Wireless Local Area Networks (WLANs) are being deployed all over the world. Over the years, companies all over the world have been implementing WLAN infrastructures into their offices to provide more convenience and better communication of data across their LAN. New issues and trends have emerged due to the popularity of WLAN technology [6]. The dominant WLAN technology used today are the 802.11 standards, primarily 802.11b. This standard is used to provide solutions for enterprise, home, and "hot spot" WLAN needs. Companies have been marketing WLAN management solutions that may improve WLAN technology. Currently, recent WLAN management technologies include radio frequency IDs, ultrawideband, and fourth generation stations.

Trends: Different Wireless LAN Technologies and Standards

There are many WLAN solutions available today [2]. Each solution varies in levels of standardization and interoperability. The two major solutions that leads the industry today are Wi-Fi (IEEE 802.11b) and HomeRF [5]. Between the two of them, the 802.11 standards have wider support and support the WLAN needs for enterprise, home, and public "hot spots." "Hot spots" are the access points places where users typically gather, such as conference rooms and cafeterias.

Table 1 compares the 802.11b and HomeRF solutions:

IEEE 802.11 Standards

The 802.11b solution for WLAN management technology is just one of the standards provided by IEEE 802.11 family. The 802.11 is the working group for WLANs [9]. There are many products that are sold by Venders that conform to different WLAN technologies, such as 802.11a, 802.11b, 802.11g, and Bluetooth. In order to select a technology that is suitable for a company's network, an understanding of the pros and cons of each is necessary.

Table 1: Comparison between IEEE 802.11b and HomeRF [8]

	IEEE 802.11b	**HomeRF**
Major Industry Support	Cisco, Lucent, 3Com WECA	Apple, Compaq, HomeRF Working Group
Status	Shipping	Shipping (Low speed)
Range	50-300 feet	150 feet
Speed	11 Mbps	1, 2, 10 Mbps
Use	Home, Small Office, Campus, Enterprise	Home
Cost	$75-$150/card	$85-$129
Security	WEP/802.1x	NWID/encryption
Vendors	Over 75	Under 30
Public Access Points	Over 350	None
Market Share of Wireless NICs	72%	21%

The 802.11b standard was built as an expansion of the original IEEE 802.11 standard. 802.11b supports bandwidth up to 11Mbps and uses the same radio signaling frequency (2.4 GHz) as 802.11. Although it is the most popular standard currently out, there are a few problems that are brought up with it. Interference can incur from appliances such as microwaves and cordless phones that have the same 2.4 GHz range. One way to solve this problem is by installing the 802.11 gear distant from these appliances.

The pros that 802.11b standard has are 1) lower cost and 2) the signal range is best. The cons are 1) slower maximum speed, 2) fewer simultaneous users are supported, 3) and appliances can interfere with the frequency band.

The 802.11a standard is the second extension to the original 802.11 standard. What many people do not know is that 802.11a was created at the same time as 802.11b. This is due to the fact that 802.11b gained popularity much faster. While 802.11b fits better with the home market, 802.11a fits for the most part in the business market because of its higher cost.

The pros associated with 802.11a are 1) fastest maximum speed, 2) more simultaneous users are supported, and 3) regulated frequencies stops interference from other devices. The cons are 1) higher cost and 2) range signal is shorter and can easily be blocked.

The newest standard is 802.11g and it has rated speeds of 54Mbps which it is similar to 802.11a. However, for compatibility and distance, 802.11g is more attractive because it operates in the lower 2.4GHz unlicensed radio band, while 802.11a operates in the higher 5GHz unlicensed radio band. This means 802.11g throughput falls off more slowly with distance than 802.11a throughput. On the other hand, sometimes 802.11a standard is in favor, because the 5GHz band provides many more nonoverlapping channels than 802.11g.

With 802.11g access point, 802.11b and 802.11g NICs can operate together. Therefore, it makes 802.11g a smooth upgrade path in existing 802.11b networks because old NICs can still be used under the circumstances of having new access points. The 802.11g NICs also will drop down to

802.11b operation when it associates with an 802.11b access point. However, 802.11g throughput falls off dramatically when even one 802.11b station deals with an 802.11g access point.

HomeRF (Home Radio Frequency)
HomeRF, in contrast to the 802.11 standards, is the WLAN solution that is designed specifically for wireless networks at homes. The HomeRF networks are projected to be more affordable to home network users than other wireless technologies. This technology is based on frequency hopping and uses radio frequency waves for the transmission of voice and data.
A list of HomeRF traits is included in Table 1.

Radio Frequency IDs (RFIDs)
RFID chips are read by radio over short distances. A way to understand how RFID chips work is to think about the products in grocery stores. The products have Universal Product Code (UPC) bar codes. A cashier runs the products by a reader which records their sales. This is slow and labor-intensive. RFID chips solve this problem [4]. With RFID chips, less labor is required for the checkout. The items only need to pass near the RFID scanner. The warehouses "smart shelves" that are allowed by the RFIDs offer continuous inventory information to a central computer. Generally, RFIDs provide real-time data for many information systems [4].

Ultrawideband (UWB)
Ultrawideband transmission system uses channels that are more than 100 times wider than traditional spread spectrum transmission [8]. The UWB uses low-powered, short-pulse radio signals to transfer data over a wide range of frequencies. It is attractive because it can provide huge transmission speed over distances of about 10 meters. A few services that UWB is capable of delivering are wireless television transmission within a home, high-speed switch-to-switch transmission within a telecommunications closet, and server-to-switch transmission in a server room. A concern, however, with UWB is the interference between UWB systems and other wireless technologies. Due to this problem, UWB products are limited with short range propagation.

Fourth-Generation (4G) Stations
There are several major radio-based technologies for WLANs. With many computers, two or more of these technologies may be required to work with in different locations. The 4G station helps make this possible. The station works with multiple radio standards in multiple bands [4]. Instead of the traditional horizontal communication model, the 4G systems use a vertical communication model, which integrates different existing and evolving wireless access systems on an IP-based platform, to complement each other for different service requirements and radio environments [8]. Also, in order to enable interworking between these different wireless access systems through vertical (inter-system) and horizontal (intra-system) handovers, multimode terminals are required that support different existing and newly emerging air interfaces. New air interfaces for 4G broadband cellular networks are currently being developed with the support from the World Wireless Research Forum and the IEEE 802.20 study group for Mobile Broadband Wireless Access [8].

Bluetooth

Bluetooth is another wireless technology that has a different purpose comparable to WLAN. It is designed to serve for personal area networks (PANs) which it only serves a few devices carried by a person or around a desk. It basically offers cable connections or replacement between devices. For example, a cell phone can print to the same wireless printer and place a call through the firm's telephone system instead of paying to make a cellular call [4].

The pros associated with bluetooth are 1) lower cost, 2) lower battery drain, and 3) it provides application profiles. Application profiles are application-layer standards designed to allow devices to work together automatically, with little or no user intervention [4].

Some of the cons associated with bluetooth are concerned with rated speed, distance, number of devices, and scalability. Bluetooth provides 722 kbps with back channel of 56 kbps and it may increase. However, it is much slower than 802.11 standards. Also, it can only go 10 meters for maximum distance and it needs 10 piconets where each with up to 8 devices. The scalability is poor comparing with 802.11 where 802.11 has a good scalability because it allows multiple access points.

The problem that bluetooth has is that it can interfere with 802.11b networks because they both operate in the 2.4GHz unlicensed radio band. People are currently working to reduce transmission interference between these two networks but it still has some problems.

RECENT WIRELESS LAN TECHNOLOGY DEVELOPMENTS

The New Developments in Industry

Over the years, new developments have been emerging by companies in a mission to advance the growth of WLAN technology. In September of 2004, two WLAN equipment vendors, Proxim and Netgear, revealed software products to help enterprises manage their wireless networks. The ORiNOCO Smart Wireless Suite, the new software provided by Proxim, is a package of software supplied by Wavelink and Ehaku that simplify site surveys conducted before deploying WLANs. The management and optimization of WLANs is also provided by the suite. The suite simplifies the set up of 802.11i security. In addition to the Smart Wireless Suite, Proxim [10] also launched ORiNOCO AP-700. This software supports the draft 802.11e standard for Quality of Service (QoS). QoS is considered necessary for applications such as voice-over-WLAN [8].

Netgear announced that it has included support for Propagate Network’s AutoCell radio frequency management technology into its WLAN access points and network interface cards. This technology is aimed at small and medium-sized businesses. The AutoCell technology makes it possible for network managers to improve WLANS with tools such as automatic channel selection and load balancing across access points. Additional security capabilities are provided as well [8].

In May 2004, Computer Associates released the Unicenter Wireless Site Management (WSM). CA declared that this product will allow network managers secure and manage WLANs and end-user access to them [7].

WSM automatically discovers and maps out WLANs and wireless devices. WSM will map, monitor, and secure wireless nets by using agents on wireless devices and centralized management software installed on a server. The agents will give users access to 802.11 nets [7]. WSM provides many benefits to its users. Users of the WSM have acknowledged that the software reduces the number of man hours needed to maintain the WLAN. The George Washington University Hospital gives a good example of how accommodating the WSM software can be. The product imposes location-based access controls and manages performance for the doctors, nurses, and support staff at the hospital. One source says "Healthcare providers have no choice but to go wireless. But we also need to secure the patient data [7]."

An important feature included in the WSM is automatic encryption key management. CA stated that WSM will generate, distribute, rotate, and synchronize Wired Equivalent Privacy (WEP) keys. The WEP keys are used to secure wireless communications based on policies identified by security administrators.

Pros

There are several advantages with the recent WLAN management technology. The pros for RFIDs are 1) it allows much less labor resulting reduced cost in checkout 2) keeps constant inventory updating, and 3) it supplies real-time data for business people. The pros for UWB are 1) it uses channels more than 100 times larger 2) provides enormous transmission speed (480Mbps) with a distance of about 10 meters 3) allows wireless TV transmission in homes and wireless communication within a telecommunication closet or server room. The pros for Fourth Generation stations are, 1) it creates to work with multiple radio standards in multiple bands and 2) reduce multiple hardware implementations for different wireless standards.

Cons

Along with the advantages, WLAN management has brought along a few concerns to its users. With the growth of the size and popularity of WLAN technology, the problems it brings have become perceptible. There are inherent weaknesses with wireless networks. Slower Ethernet speeds range from 10Mbps. Corporations usually require high bandwidths. Also, the radio frequency signals used by WLANs can pass easily through barriers such as cubicles, partitions, glass, and standard walls. However, the signals will experience problems passing through solid barriers. These interferences cause disruptions in connection.

Another concern that can be an issue is the WLAN technology market. Systems from different vendors may not be interoperable [3]. The installation for these systems is expensive as well, causing a great cost for the enterprise. WLAN equipment also requires a significant amount of attention in order to preserve tight security and the best performance possible [1]. Currently, traditional network management solutions do not address problems like these, which forces companies to ignore them, manage them by hand (resulting in more time and expense), or consider third-party solutions.

The outstanding trends in WLAN management technology have a few issues. Problems that prevent the use of RFIDs are excessive cost and the inability to meet demand for replacing bar codes. As mentioned earlier, UWB systems have limited short range propagation due to the interference between UWB products and other wireless technologies.

OUTSTANDING ISSUES

Wireless Propagation Problems

Wireless transmission problems and serious propagation problems are very common. For example, people often lose connections with their cellular telephone. If a signal is found by injecting a UTP cord or optical fiber cord, the transmission losses along the way can be fairly predictable. However, wireless transmission, we have much less control over the transmission path between the sender and the receiver. Several wireless propagation problems include rapid attenuation, shadow zones (dead spots), multi-path interference, electromagnetic interference (EMI), and frequency-dependent propagation.

The wireless signal strength attenuates according to an inverse square law meaning a signal's strength gets weak during propagation. It attenuates much faster than in wire or optical fiber transmission. Sometimes these wireless signals can go through or around objects. However, it cannot go through if there is a thick wall or a large object blocking the path between the sender and receiver. The area is called the shadow zones or dead spots not allowing the transmission. In general, there is usually more than one signal that the receiver would receive consists of a direct signal and one or more reflected signals. These signals travel different distances and so may be out of phase when they reach the receiver [4]. This multi-path interference generates the signal to range from nonexistent to strong signal.

Lastly, EMI is a major propagation problem such it is created by electrical motors and devices. For example, fluorescent lamps, cordless telephones, microwaves, and other devices would produce electromagnetic interference. Additionally, there is a frequency-dependent propagation problem. Higher frequency signals attenuate much faster than lower frequency signals because they are absorbed more rapidly by moisture in the air, leafy vegetation and other water-bearing obstacles [4]. For example, WLAN signals approximately around 5 GHz attenuate much faster than signals around 2.4 GHz.

Security

Companies first began to implement 802.11 WLANs and they discovered that people can just read traffic from outside or can also send malicious traffic into the network. The worst problem with wireless security is simply that security traditionally has been turned off by default. In older products the installation default was to have no security at all.

WEP

When 802.11 was introduced in 1997, it was introduced with a security system called Wired Equivalent Privacy (WEP). All stations share the same encryption key with the access point. Its key is rarely changed. Having all stations use the same shared static key allows possible for cryptanalysts to crack the key in hours or days because key sharing allows WEP keys to be broken by collecting only 100 megabytes to one gigabyte of data.

802.11i Security

It is a full security mechanism introduced in 2003 and considered as a very good security. It uses the Temporal Key Integrity Protocol (TKIP), which gives each station its own unshared key after authentication and which changes this key frequently [4]. It also adds the Extensible

Authentication Protocol (EAP). When a station requests service, the access point requires the station to provide authentication data. In return, the station transmits such authentication data as a password or proof that it has a digital certificate. Then access point passes through authentication data on the authentication server and checks the authentication data and sends back an affirmation or a rejection message. Therefore, the station can be accepted or rejected.

CONCLUSION

We have found that WLAN management has been implementing new and improved technology to further the advancement of wireless networks. The recent emergence of high-rate WLAN communications is enabling a wide range of new capabilities for enterprises and institutions across numerous industries. With these capabilities, many organizations can obtain a key competitive advantage. IT managers and others involved in network communications will want to be familiar with the increasingly popular WLAN technology.

As a large fraction of company's critical information is made available to WLAN users, security will become more of a concern. Currently, WLAN standards offer very substandard level of security that one could not place their full trust on. It is expected that wireless LAN user will expect a wired equivalent security in wireless environment as well. The use of stronger encryption and WEP has lightened the issue with security but still not enough to meet good standards. New products are being brought in by manufacturers with additional RF and security features, guaranteeing that all terminals are equipped with the proper software release. However, most solutions are still vendor proprietary. With the constant improvement on WLAN management technology, users will have more mobility and security along with more efficient transmission of data.

REFRENCES

1. Bailey, D. (Aug 2004). Wireless Access Report: Security issues dog hotspots. *Network Week*, 26.
2. Chowdhurry, D. D. (2000). *High speed LAN technology handbook*. New York: Springer.
3. Dubie, D. & Cox, J. (May 2002). Vendors to address wireless LAN foibles; Management, security to be featured in new products. *Network World*, 6.
4. Panko, R. R. (2004). *Business Data Networks and Telecommunications* (5th Ed). New Jersey; Upper Saddle River: Prentice Hall,
5. Tan, T. (2003). *The world wide Wi-Fi : technological trends and business strategies***.** Hoboken, NJ: Wiley-Interscience.
6. (2002). WLAN System Centralizes Management. *eWeek*, NA.
7. Dubie, D. (2004). *CA unveils WLAN management*. Retrieved October 2004 from http://www.nwfusion.com/news/2004/0525cawlan.html
8. Horlin, F. (2004). *The Generic Transmission scheme for Fourth Generation Wireless Systems*. Retrieved November 19, 2004, from http://www.imec.be/wireless/sdr/publications/WWRF_2004_generic.pdf
9. Mitchell, B. (No Date). *Wireless Networking: 802.11 Standards. Retrieved* October 2004 from http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm
10. Mobile Pipeline News. (2004). *Proxim, NetgearUnveil WLAN Management Capabilities*. Retrieved November 18, 2004 from http://www.networkingpipeline.com/wireless/47903008