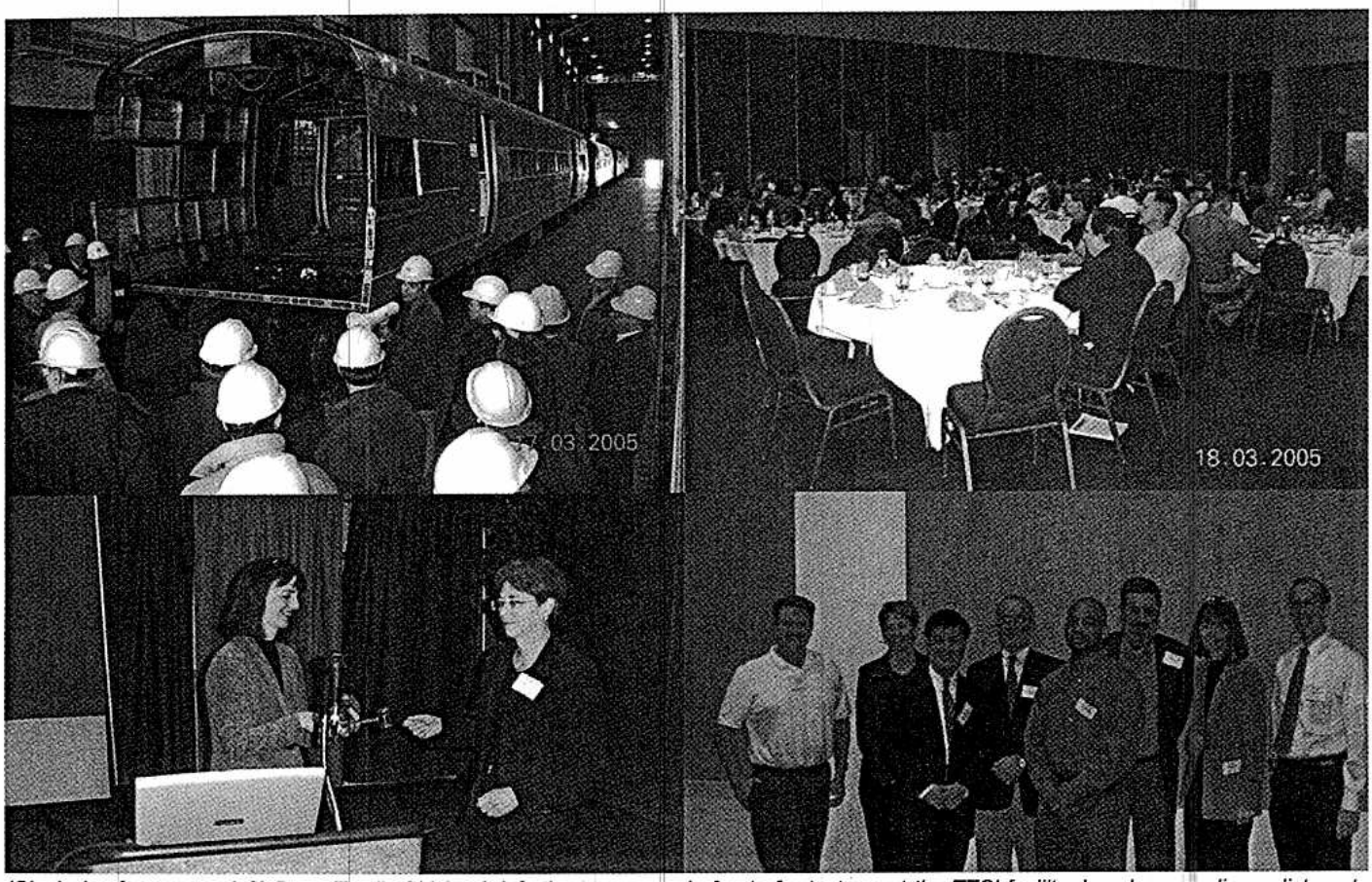
Rail Dynamics Lab and Center Services Building to see the Crash Test Car(see the figure below), plus a riding tour to Test Track Substations, Component Test Lab, and Emergency Response Training Center. After the tour the group joined the AAR Research Review participants for a picnic style lunch at TTCi for Accelerated Service Testing Facility. After lunch the Conference starts technical sessions along with table-top exhibitions.

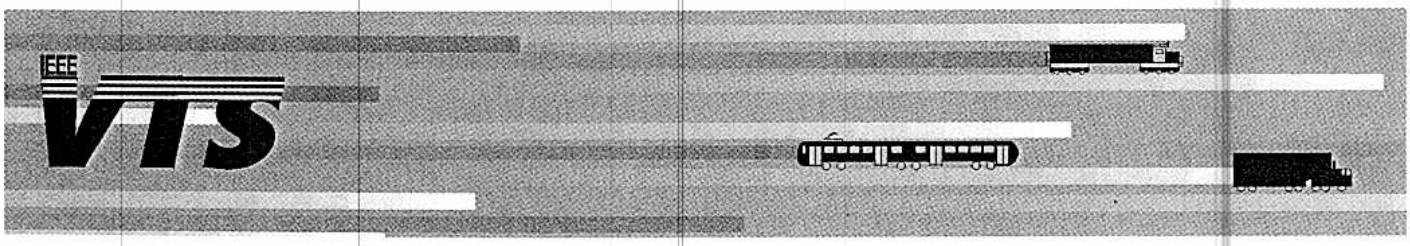
Over 120 people participated in the Conference from all over the world including Australia, Denmark, Italy, Taiwan, as well as from Canada and the USA. Fifteen Electrical Engineering-related papers and twenty-one Mechanical Engineering-related papers were presented on a variety of technical topics from "Communications Based Train Control (CBTC)" to "Progress in Locomotives, Freight Cars and Improved Performance Issues". All papers generated a great deal of audience interest and questions.

At the Conference Luncheon the IEEE VTS LTD Chair, Margaret Burnett, LTK Engineering Services, passed the gavel to the incoming Chair, Denise Burleson, Lea+Elliot, Inc. The other officers elected for 2005-2006 were: Vice Chair, Bih-Yuan Ku, National Taipei University of Technology in Taiwan; Secretary, Lamont Ward, Long Island Rail Road; Papers Chair, Michel Thomet, Bechtel Civil Company; and Publicity Chair, Paul Flaherty, Goatlick Engineering, Ltd.

Papers of the 2005 Joint Rail Conference and previous year Joint Rail Conference can be purchased at ASME website http://www.asmeconferences.org/JRC05/index.cfm.




*(Clockwise from upper left) Dave Tyrell of Volpe briefs the tour group in front of a test car at the TTCi facility; Luncheon audience listens to speaker George Binns, Chief of Inspections and Evaluation, Amtrak; Outgoing Chair Margaret Burnett transfers gavel to incoming Chair Denise Burleson; LTD 2005-2006 Executive Committee members gather during a session break*




# Trends in IEEE 802.11 WLANs

*Ali Ghazizahedi, Cisco Systems, Inc, Xinrong Li, UNT, Kaveh Pahlavan, WPI*

*This paper provides an overview of the emerging WLAN applications in home networking, hotspot and corporate environments. The paper starts with an overview of the evolving markets. Then it provides a survey of related important standardisation activities, followed by how these technologies are incorporated into applications, and finally*

*it discusses the current technical challenges for WLAN security.*

## Introduction

The concept of wireless LAN (WLAN) was first introduced in late 1970's; the first serious commercial endeavor initiated in mid 1980's shortly after announcement of ISM bands in 1985 [1-3]; the first IEEE standard emerged after around one decade of committee work in 1997 [4]. Numerous innovative technologies and application scenarios were examined over the time [1-8], and in spite of all optimistic market predictions the first sizable market started to appear only in the recent years. This market has evolved in three branches, enterprise networks, home networks, and hot-spot access.

After proving themselves in vertical markets such as health care, education, and retail, WLAN is beginning to make inroads in general business-computing environments. According to a recent META Group study, 29% of 435 enterprises surveyed in the US had deployed WLAN as an adjunct to the campus network. Furthermore, an additional 44% indicated they would deploy WLAN within the next 24 months. To date, more than 25 million WLAN devices have been shipped worldwide and 741 models have been approved by Wi-Fi Alliance.

The WLAN is typically an extension of a wired Ethernet LAN. Ideally, this wireless extension should support the same functionality as the wired network, providing tight controls through rich feature sets, such as security, management, and quality of service (QoS). Enterprise WLAN must also scale from hundreds to thousands of devices. Viewing the WLAN as an extension of the wired LAN helps to simplify operations, management, and security

In addition to the traditional wireless data and voice applications, more recently indoor positioning is emerging as a new technology to be integrated into the existing local ad-hoc networks [9]. This technology is expected to help hospital personnel track in-demand equipment, help parents locate children, help family members and care-givers track special-need and elderly relatives away from supervision, and help public-safety and military units locate fire fighters and war fighters inside buildings during their missions.

## Market Trends

The year 2003 was characterized by renewed enterprise adoption of the WLAN technology. The bulk of this growth continues to be driven by key vertical markets such as healthcare, retail, manufacturing, and education, all of which require networks that can provide the utmost flexibility in terms of connectivity and mobility. Furthermore, the growing trend toward embedding WLAN capability into mobile computing devices (laptop, PDA, cellular phone, etc.) will generate an enormous amount of demand from the client perspectives, which should help to speed continued infrastructure build-outs.

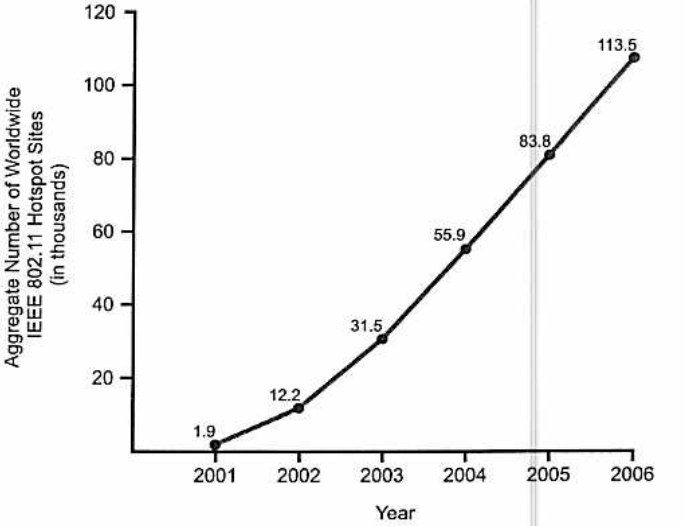
In 2003, total sales for WLAN equipment increased 41.1% year-over-year and it is estimated that the total WLAN market reaches to $3.7 billion by 2004 and $5.2 billion by 2008 [10]. Sales for SOHO (small office, home office)/home WLAN equipment in 2003 increased 66% comparing to 2002. Growth in this segment continues to be driven by aggressive pricing, strong sales of 802.11g devices, and, to a lesser extent, the introduction of multimedia devices for the home. It is estimated that this market will grow 62% in 2004 and reach nearly $2.7 billion and surpass the $3.8 billion mark by 2005 [10]. Similar patterns can be seen in EMEA (Europe, Middle East and Africa) but in Asia-Pacific area there was an increase in WLAN sales (25%) but decrease in the number of unit sold (6%) according to [11].

The year 2003 also marked the introduction of two new enterprise segments, WLAN switches/controllers and "light" access points. The demand for mobile voice technologies in the workplace is growing rapidly. Voice, as an application, is and will continue to drive the adoption of WLAN in the enterprise. In 2003 the market for Voice over WLAN phones grew 115% to $33 million. Moreover, it is estimated that this market will grow at a compound annual growth rate (CAGR) of nearly 30% over the next five years, as vertical markets such as healthcare, retail, manufacturing, and corporate enterprises continue to drive and speed the adoption of these devices [10].

The market for enterprise WLAN infrastructure grew nearly 20% in 2003 to $618 million and should surpass the $1 billion mark by 2007. Much of this growth will be driven by the growing number of large-scale WLAN deployments in the aforementioned vertical markets as well as increased adoption by the enterprise. Additionally, this market will also be fueled by sales of new classes of products including WLAN switches/controllers and "light" access points [9-11]. According to Infonetics Research, in the third quarter of 2003, enterprises made up 47% of worldwide WLAN hardware revenue, consumers made up 42%, and service providers (for hot-spot services) made up 11% [12]. And the enterprise proportion will show the most significant continued increase as enterprise-class switching and security systems drive adoption into this market.

Finally sales of SOHO/home client and infrastructure devices increased 43% and 91% respectively in 2003. It is predicted that going forward, growth of these devices should be slowed by initiatives such as Intel's Centrino and Intel's recent announcement that it intends to integrate access point functionality into PCs themselves [9].

Hotspots are locations that provide Internet access via WLAN. These are among the reasons that In-Stat/MDR expects WLAN hotspots to grow in number worldwide from 31,455 in 2003 to 113,555 in 2006 (see Fig.1), when worldwide user revenues will reach more than US$1.2 billion [13]. Another research firm, Gartner, predicts that there will be 70 million users of public hotspots by 2007 [14].




*Source: In-Stat/VIDR, Scottsdale, Arizona, 2003*

***Figure 1.*** *Worldwide trends for Wi-Fi hot-spot growth*

## Trends in Standards

The current and emerging important standardization activities related to WLAN are under either IEEE or Wi-Fi alliance. Table 1 and 2 summarizes these activities.

***Table 1.*** *Important WLAN Related IEEE Standards*

| | |
|---|---|
| 802.11a | *It defines 54Mbps in the 5GHz band; low usage makes it least subject to interference.* |
| 802.11b | *It defines 11Mbps bandwidth in the 2.4GHz band; it is the most widely deployed standard and, thus, is the most subject to interference.* |
| 802.11g | *It defines 54Mbps bandwidth in the 2.4GHz band; it has wider range than 802.11a, but is also subject to 2.4GHz channel interference.* |
| 802.11n | *It will support speeds of up to 108Mbps.* |
| 802.11e | *It would add extensions to support QoS for voice applications, while retaining backwards compatibility with existing variants.* |
| 802.15 | *It is a low power solution with multi-month to multi-year battery life and very low complexity for applications such as sensors, interactive toys, smart badges, remote controls, and home automation. The 802.15.1 Bluetooth that operates in 2.4GHz band interferes with 802.11 2.4GHz devices.* |
| 802.1X | *It defines port-based authentication in LAN environments; authentication credentials are never transmitted over wireless connections without encryption; EAP authentication types such as LEAP are components of 802.1X.* |
| 802.11i | *It is draft security standard that defines AES encryption and EAP device authentication for 802.11 wireless networks.* |

***Table 2.*** *Wi-Fi Alliance*

| | |
|---|---|
| **Wi-Fi Protected Access** | Interim technology to strengthen user and device authorization/authentication schemes prior to release of 802.11i standard. It includes support for 802.1X, EAP authentication, and TKIP encryption. |
| **Wireless Multimedia Enhancements (WME)** | Interim technology to synchronize client device and access points in terms of how to handle queuing, channel access and collision avoidance, so as not to configure devices specially to recognize VoIP phones and their traffic. WME uses four priority levels rather than eight as in 802.11e. |

The WLAN standardization first started under IEEE 802.4L in late 1980's because 802.4 Token Ring was focused on manufacturing and the first dominant market perceived for WLAN was in the manufacturing floors. Soon after that IEEE 802.11 was formed to focus on WLAN. It took over a decade to finalize this standard for 1-2Mbps direct sequence, frequency hopping and infrared technologies in 1997 when the standard was already late [15]. The 802.11a was started soon after completion of the first standard. However, the 11Mbps B operating in 2.4GHz ISM bands emerged first and captured the developing markets soon. The 54Mbps A products operating in 5GHz bands appeared later and as of now it has been struggling in capturing a sizable portion of the emerging markets. Some experts believe that with the continued growth of 2.4GHz market and reduction of the cost and complexity of installation of WLAN access points, at certain point the interference in the 2.4GHz will develop a market for 5GHz products that enjoy larger number of non-overlapping channels. Meanwhile the 54Mbps G that is backward compatible with the B is replacing the B products.

Because of the progress in standardization, businesses are now evaluating running A and G WLAN, which each run at the speeds of 54Mbps, alongside 11Mbps B networks. The availability of all these WLAN types opens up new opportunities, as well as architectural and management considerations. For example, G is backward compatible with B, which is extremely desirable from a migration perspective, since G and B clients and access points can be mixed and matched. Still, if you deploy only B and G access points in a given coverage area (and no A), you remain limited to three non-overlapping channels. This could lead to interference. Also, G technology works such that once a B client associates with a G access point, G network throughput is impacted, even if the B client is not transmitting any packets. This is because special headers, which create network overhead, must be appended to G packets to enable B packets to detect and avoid G traffic.

Fortunately, tri-mode chipsets supporting B, A, and G recently began shipping, which means that decisions about which types of access points and clients to deploy will soon no longer be interdependent [16]. In other words, organizations could run any mix of B, A, and G access points that among them have as many as 27 non-overlapping channels (depending on imminent decisions about global cooperation on the use of the 5GHz spectrum) for easily configuring networks to avoid interference. Tri-mode clients supporting B, A, and G could simply associate with the best network connection available to them in a given location.

Interoperability of B products from different vendors is ensured by an independent organization called the Wireless Ethernet Compatibility Alliance (WECA), which identifies compliant products under its Wi-Fi Brand. With Wi-Fi membership boasting more than 140 companies, spanning component manufacturers, equipment vendors, and service providers, the future of the 802.11 standard is secured.

The 802.11n is another initiative in 802.11 to boost the performance to above 100Mbps. In 802.11n, nothing can be removed from 802.11 but only mechanisms that affect throughput hikes and from that perspective, backwards compatibility with both 2.4GHz G and 5GHz A must be maintained, with N itself likely to run in both bands. A final requirement, added by the task group itself rather than mandated in the charter, is that the N protocol will enable 100Mbps throughput modes within the existing 20MHz channels. This does not preclude even higher-throughput modes via the use of wider channels.

The other initiative is 802.11e. The original medium access control (MAC) protocol for WLAN does not support differentiation of traffic types or sources, making it unsuitable for applications where certain traffic needs to be prioritized, such as voice or video over IP. In 802.11's current state, there are two modes of communications, both of which will be enhanced in 802.11e. With DCF (distributed coordination function), based on 'listen before talk' technology, a wireless station waits for a quiet period on the network before transmitting data and detecting any collisions. An optional second mode PCF (point coordination function) goes a step further as it supports time sensitive traffic. It splits the time into contention-free and contention periods and transmits data during the former. However, while these two modes offer coordination and time sensitivity, neither distinguishes between different types of traffic.

The proposed 802.11e standard would add extensions to both modes to support QoS for voice applications, while

retaining backwards compatibility with the existing WLAN variants. The DCF would be enhanced with support for eight different traffic categories, with lower priority categories of traffic waiting for the others to go first, before accessing the medium. However, there are no guarantees of service, which could still limit the viability of heavy-duty voice over IP implementations.

### The Related 802.15 WPAN Standard

The 802.15 WPAN is an initiative by the IEEE focused on developing a common set of standards for Wireless Personal Area Networks (WPAN) or short distance wireless networks. Established in January 1999, the WPAN working group, which is part of the Local and Metropolitan Area Network Standards Committee of IEEE, has since formed four task groups, each focused on necessary standards. The Bluetooth SIG (special interest group) specification serves as the foundation for developing the IEEE 802.15 WPAN standard, which would standardize the MAC and physical layers of Bluetooth. The Bluetooth SIG, established in 1998, made their specifications publicly available in the middle of 1999.

The idea behind 802.15 WPAN is to publish standards that allow devices such as PC, PDA, mobile phone, pager, and other handheld devices to communicate and interoperate with one another. The goal of publishing the 802.15 standards will be to accommodate wider adoption and applicability, and to deal with issues like coexistence and interoperability with IEEE 802.11 networks. The IEEE 802.15 working group defines three classes of WPAN characterized by data rate, power usage, and quality of service [4]:

IEEE 802.15.1 and Bluetooth—The 802.15.1 WPAN standard is based on Bluetooth version 1.1 specifications. While Bluetooth devices that are currently available are most likely to be v1.1, the Bluetooth standards body has pushed ahead of the 802.15.1 standard and developed a specification that should see devices being developed that offer data rates of about 10Mbps. Whilst the maximum range of Bluetooth v2.0 devices (currently 10-100m) is still being discussed the greater data rates means that Bluetooth is likely to be used both as a WPAN technology and as a WLAN technology that competes with 802.11b.

*Table 3. General Differences between WLANs, WPANs, and LR-WPANs*

| | WLAN (802.11) | Bluetooth-based WPAN (802.15.1) | Low-rate WPAN (802.15.4) |
|---|---|---|---|
| Range | *~100 m* | *~10 - 100 m* | *~10 m up to 75m* |
| Data throughput | *~2 - 11 Mb* | *~1 Mbs* | *~0.25 Mbs* |
| Power consumption | *medium* | *low* | *ultra-low* |
| Size | *larger* | *smaller* | *smallest* |
| Cost/complexity | *>6* | *1* | *0.2* |

IEEE 802.15.2—This is a standard focused on recommended practices for coexistence between WPAN and WLAN. This standard is yet to be ratified.

IEEE 802.15.3—The 802.15.3 working group has been tasked with developing a high data rate (up to 55Mbps) WPAN technology capable of handling multimedia content. This technology has been designed to offer QoS meaning that data such as video should be delivered between devices with no break down in quality of picture. This draft standard is yet to be ratified and as such no devices with 802.15.3 connectivity are currently available.

IEEE 802.15.3a and Ultra Wide Band (UWB)—UWB is being considered by the IEEE as the 802.15.3a standard. This technology is a short-range technology (up to 10m) with high data rates (planned data rates of about 400Mbps) for applications which involve imaging and multimedia. Currently two industrial alliances, led by Motorola and Intel, respectively, are working on two different technologies for UWB, that is, DS-UWB and Multiband OFDM technologies.

IEEE 802.15.4 and Zigbee—The Zigbee standard has now been endorsed by the IEEE as the official 802.15.4 standard. This is a WPAN technology developed by an alliance of companies with the aim of producing a low power consumption and low cost WPAN technology that could be included in a range of low data rate devices such as mouse, keyboard, joystick and educational games platforms. The data transfer rates of Zigbee depends on the frequency used (250Kbps at 2.4GHz, 40Kbps at 915MHz and 20Kbps at 868MHz) and the range of Zigbee can go up to 75m depending on a number of factors including the power used.

Table 3 compares range, data throughput, power consumption, size and complexity of 802.11, 802.15.1 and 802.15.4.

## Technology Trends for Emerging Applications

In response to the fast increasing demands for WLAN, manufacturers in this industry are clearly tailoring their products to different application sectors, that is, home networks, enterprise networks, and hot-spot access. The technologies applied to these applications have evolved through different paths with different mentalities. In the following three sections we provide specifics of the technologies used for these three application sectors.

### Home Networking Alternatives

Several technologies have been examined for wireless home networking applications. One of the early solutions was the HomeRF technology, the next competitor was the Bluetooth technology, and IEEE 802.11b WLAN finally captured the current market. The newer 802.11g is replacing 802.11b devices. HomeRF and Bluetooth technologies were under WPAN activities that are currently under 802.15. Table 4 compares the feature of these four technologies.

It should be noted that the maximum number of devices supported by each standard depends on data rate per device, and 40- to 128-bit RC4 refers to very robust data security algorithms.

*Table 4. A Brief Comparison of HomeRF, Bluetooth, and 802.11 WLAN Standards*

| | HomeRF | Bluetooth | 802.11b | 802.11g |
|---|---|---|---|---|
| **Date Rates** | 1 or 2 Mbps | 1Mbps | 11Mbps | 54Mbps |
| **Max # Devices** | Up to 127 | Up to 26 | Up to 26 | Up to 26 |
| **Security** | Blowfish | 0-, 40-, and 64-bit | 40- to 128-bit RC4 | WEP |
| **Range** | 150 ft | 30 to 300 ft | 150 ft indoors, 300 ft outdoors | 150 ft indoors, 300 ft outdoors |

### Technologies for Hot-spot

WLAN hotspots are essentially 802.11-based IP networks and based on this fact, use of core protocols developed in the IEEE (such as 802.1X) and the Internet Engineering Task Force (IETF) are prevalent [17]. Usually the visited hotspot accommodates a variety of credential types (e.g., user-

name/password, Subscriber Identity Module (SIM), and X.509 certificates). In a subscription-based access model, it must be possible to provide end-to-end security for authentication and authorization. It is desirable for different users to avail of different levels of service depending on whether they are in the home provider's network or in a visited network.

Another issue is secure key distribution. Current standards for WLAN key distribution do not fully meet this requirement in roaming scenarios but it is desirable that key distribution between home providers and visited networks for wireless link layer encryption should be secured and cryptographically bound to authentication and session information.

Other concerns about hot-spots are re-authentication and protocol translation. When moving between access points managed by the same network, operator must not cause significant delay and must not require user interaction. If protocol translations are required to be integrated with legacy or proprietary authentication back-ends, such translations should occur within the premises of the legacy network.

In the situations where the integration of services requires inter-working with another network (such as a cellular operator's core data network), it is recommended to have "loose coupling" between the WLAN hotspot and core networks. In other words, WLAN networks should be seen as standalone networks based on IEEE and IETF core protocols as opposed to radio access networks, and should not require the use of domain-specific mobility management protocols over the client's WLAN interface (for example, GPRS Mobility Management or GMM) [18].

### Enterprise WLAN Technologies

The WLAN access points designed for consumer market for home networking are not deployable in enterprise environment due to its lack of security, scalability, manageability among many other features critical to enterprise applications.

Currently there are two competing technologies in designing enterprise-class WLAN access points. One is the so-called fat-AP solution. With such technology, the AP for enterprise application is an enhanced version of the one for home application. All the features critical to enterprise applications are integrated into the AP, which makes it fatter as compared to the AP designed for home applications. The fat-AP solution has some serious shortcomings. For example, as the WLAN in cooperate campus grows, maintaining and managing larger number of AP's over large area become a challenging issue. Such a solution also lacks scalability and flexibility in system upgrade and capacity expansion. The fat-AP architecture concentrates all of the WLAN intelligence in the AP. This is the most common AP architecture used today, where AP handles the RF communication, as well as authenticating users, encrypting communications, secure roaming, WLAN management, and in some cases, network routing. Towards solving the problems faced by fat-AP technology, most recently a thin-AP solution has entered into the market [19,20]. Strongly backed by several companies, a lightweight-AP protocol (LWAPP) has been submitted to IETF for standardization for the thin-AP solution. With thin-AP solution, WLAN AP functionalities are carefully divided and a portion is moved from AP to a WLAN access controller which conveniently provides a centralized management and maintenance point for the whole enterprise WLAN network. The thin-AP architecture actually uses two components—an AP that's essentially a stripped down radio and a centralized management controller that handles the other WLAN system functions. Wired network switches are also required. By centralizing the configuration and management of the AP's, this architecture greatly simplifies the management of hundreds of AP's.

A variation of the thin-AP is one that's often described as a "fit-AP." In this architecture, the AP is slightly beefier than just an RF radio, the network switches are optimized for both wireless and wired environments and the central control point is also present. The AP handles the RF and encryption, while the network switches, because they are aware of the wireless users' identities and locations, handle secure roaming, quality of service, and certain aspects of user authentication. The central management controller also handles AP configuration and management.

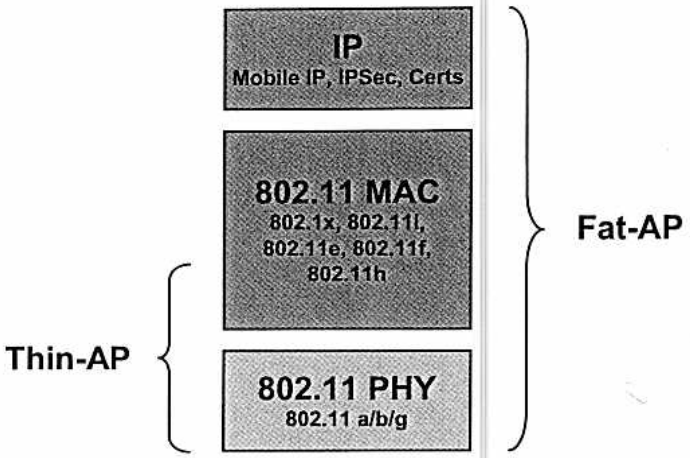



*Figure 2. Fat and thin Access Point components*

With such a new architecture, many novel applications can be conveniently implemented for the enterprise WLAN networks—including centralised traffic monitoring and location tracking of mobile users for security and performance optimization purposes; centralised RF management, such as dynamic channel assignment and power control, to optimise the coverage and throughput of the wireless network.

The major benefit of using thin-AP vs. fat-AP is scalability and cost. Thin-AP minimizes the intelligence in the AP. With this approach, relatively simple AP's can share the features that enhance wireless communications in a cost-effective and efficient manner. For a small WLAN, with fewer than 10 AP's which is usually deployed for a small business or a workgroup in a larger corporation, the fat-AP architecture—or the traditional approach—may be more cost-effective. However, as the WLAN grows, the thin- or fit-AP architectures, which offer greater manageability and centralized control, will be the approach that most enterprises will adopt [21,22].

## Trends in WLAN Security

Security is one of the leading concerns of the WLAN industry. While home networking and hot-spot users are also interested in better security, the enterprise application users are leading serious investigation to improve the existing security measures. Recent security advances such as Wi-Fi Protected Access (WPA) product compliance and interoperability certification mean that dynamic encryption keys, 802.1X authentication, and other important security capabilities have been added to Wi-Fi products for standards-

based security. WPA is a subset of the forthcoming IEEE 802.11i standard for stronger security than was offered in 802.11's initial Wired Equivalent Privacy (WEP) algorithm, which relies on static encryption keys. While vendors took it upon themselves to plug the security holes with robust solutions of their own, the additional availability of standards-based technology allows interoperability among different vendors' clients and access points.

In addition, many vendors are adding automated capabilities to detect security policy violations, to log and track user connections, and to authenticate users based on their personal identity, rather than only on a MAC or IP address. This action is important, given that small devices can easily be lost or stolen, opening up potential access opportunities to outsiders.

The authentication of both users and networks is a critical component of wireless LAN security. However, unlike data encryption (the other major component of wireless network security) authentication was not specified in the original 802.11 wireless LAN standards. As a result, the wireless industry has rallied around a protocol called 802.1X as a standard authentication framework for 802.11 LANs.

The IEEE 802.11 Task Group I, for example, is drafting amendments to the 802.11 specifications to include 802.1X. Some vendors have implemented 802.1X and compatible authentication algorithms in their products. These algorithms are based on the Extensible Authentication Protocol (EAP), which is specified in IETF RFC 2284.

In the next two sections, we will elaborate on importance of EAP and 802.1X for security and also challenges facing enterprise customers for providing connectivity between WLAN and wired network.

### EAP

EAP was originally created for use with PPP (point-to-point protocol)-based WAN (wide-area networks) such as dial-up networks. There are now many derivatives of EAP for use in 802.11 and other LANs. The 802.1X standard leaves the choice of the algorithm up to the network implementer.

Why are there so many EAP? Two variations are EAP Wireless and EAP-TLS (transport layer security). In addition, products will eventually support an emerging algorithm called Protected EAP (PEAP), currently an Internet draft protocol. Similarly, Microsoft, in the newer versions of its operating systems, supports 802.1X and EAP-TLS and has announced plans to support PEAP.

EAP-TLS uses digital certificates instead of usernames and passwords to fulfill the mutual challenge. When a client requests access, the response from the authentication server is a server certificate. The client has a certificate, signed by an in-house or third party certificate authority that has been preconfigured by the network administrator. The client will reply to the authentication server's challenge with its own certificate, rather than with a password. Using its digital certificate, the client also validates the server certificate. Based on the certificate values, the EAP-TLS algorithm can derive dynamic WEP keys, and the authentication server will send the client the WEP key for use during that session.

Certificate-based algorithms like EAP-TLS are highly secure, as it is nearly impossible to forge a certificate digitally signed by a certificate authority. On the other hand, the management of certificates can be more complex and expensive than username/password-based authentication.

In PEAP, the conversation between the EAP peer and the backend server is encrypted, and integrity is protected within a TLS channel. Mutual authentication is required between the EAP peer and the backend server. The client uses EAP-TLS to validate the server and create a TLS-encrypted channel between client and server. The client uses some other EAP mechanisms, such as Microsoft Challenge Authentication Protocol (MSCHAP) version 2, over this encrypted channel to enable server validation. Because the challenge/response packets are sent over a TLS encrypted channel, the password and the key are not exposed to offline dictionary attacks.

## What is 802.1X?

802.1X is a port-level access control protocol that sits between one of any number of optional authentication algorithms and an underlying LAN. It is not an authentication algorithm itself. Rather, it translates messages from an authentication algorithm into the appropriate frame formats of the LAN access types. The LAN type pertinent to this discussion is 802.11, but 802.1X can also be used as the authentication method for other 802-based LANs, including 802.3 Ethernet or 802.5 Token Ring networks.

802.1X leaves both the choice of authentication algorithm and key management method up to each EAP authentication type. Specifically, a piece of the 802.1X protocol called PAE (port authentication entity) runs on the three components of a secure wireless network system: the client device, the access point (AP), and the back-end authentication server such as a RADIUS (remote authentication dial-in user service) server.

In 802.1X terminology, when the PAE is functioning on the client device being authenticated, it is called the supplicant. The PAE function on the AP is called the authenticator, and the software on the back-end server is called the authentication server. The authentication server must support the same EAP authentication algorithm in use by the client.

## References


[1] K. Pahlavan, T. Probert, and M. Chase, "Trends in local wireless networks", IEEE Communications Mag., March 1995.

[2] K. Pahlavan, "Wireless office information networks", IEEE Communications Mag., June 1985.

[3] M. Marcus, "Regulatory policy considerations for radio local area networks", IEEE Communications Mag., July 1987.

[4] V. Hayes, "Standardization efforts for wireless LANs", IEEE Network Mag., November 1991.

[5] K. Pahlavan, A. Zahedi, and P. Krishnamurthy, "Wideband local access: WLAN and WATM", IEEE Communications Mag., November 1997.

[6] A. Ghazizahedi., K. Pahlavan, P. Krishnamurthy, "Wireless networks", chapter in Encyclopaedia of Electrical and Electronics Engineering, John Wiley & Sons, Inc., 2000.

[7] A. Ghazizahedi, K. Pahlavan, "Telecommunications terminals", chapter in Encyclopaedia of Electrical and Electronics Engineering, John Wiley & Sons, Inc., 2000.

[8] A. Ghazizahedi and K. Pahlavan, "Capacity of a wireless LAN with voice and data services", IEEE Trans. on Communications, July 2000.

[9] K. Pahlavan, X. Li, and J. Makela, "Indoor geolocation science and technology", IEEE Communications Mag., February 2002.

[10] A. Vance, R. Mota, J. Duke, "Quarterly update and

worldwide forecast report", Synergy Research Group, Inc., October 2003.
[11] Dell'Oro Group, "World-wide WLAN sales – Q2-CY04", 2004.
[12] Infonetics Research, "The evolution of the enterprise-class wireless LAN access point", January 2004 (available at www.airespace.com).
[13] In-Stat and MicroDesign Resourse (MDR), http://www.instat.com
[14] L. Godell, "WLAN and Bluetooth update: Beyond the hype", Forrester Report, June 2003 (available at www.forrester.com).
[15] IEEE 802.11 standards, http://ieeexplore.ieee.org
[16] R. Merritt, "Chip makers question need to redraw 802.11 map", EE Times, May 2002.
[17] A. Balachandran, G. Voelker, P. Bahl, "Wireless hotspots: Current challengers and future directions", WMASH'03, September 2003.
[18] P. Iyer et al, "Public WLAN hotspot deployment and Internetworking", Intel Technology Journal, August 2003.
[19] Airespace, http://www.airespace.com
[20] Legra Systems, Inc., http://www.legra.com
[21] E. Callaway, P. Gorday, L. Hester, J.A. Gutierrez, M. Naeve, B. Heile, V. Bahl, "Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks", IEEE Communications Mag., August 2002.
[22] J.A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, B. Heile, "IEEE 802.15.4: a developing standard for low-power low-cost wireless personal area networks", IEEE Network, September/October 2001.

*Ali Ghazizahedi (azahedi@cisco.com) received his Ph.D. in Wireless Communications from Worcester Polytechnic Institute, Worcester, MA, and his MS and BS in Electrical Engineering from University of Tehran. Currently he is an Architect in Cisco Systems Inc., San Jose, CA. His primary research interests include voice over IP and Wireless traffic engineering.*

*Xinrong Li (xinrong@unt.edu) received his Ph.D. from Worcester Polytechnic Institute, Worcester, MA, a ME from the National University of Singapore, Singapore, and a BS from the University of Science and Technology of China, Hefei, China. Currently he is an Assistant Professor of EE at the University of North Texas, Denton, TX. His recent research has been focused on signal processing and channel measurement and modeling for wireless communications.*

*Kaveh Pahlavan (kaveh@wpi.edu) is a Professor of ECE and CS and the Director of the CWINS at WPI, Worcester, MA. He is also a Visiting Professor at the University of Oulu, Finland. He is the principal author of the Wireless Information Networks, John Wiley and Sons, 1995 and Principles of Wireless Networks – A Unified Approach, Prentice Hall, 2002. He has published numerous papers, served as a consultant to a number of companies, and sits in the board of a few companies. He is the Editor-in-Chief of the IJWIN; the founder of the IEEE Workshop on WLAN, and a co-founder of the IEEE PIMRC conference. For his contributions to evolution of the wireless networks he has been elected as a Fellow of the IEEE, become a Fellow of Nokia, and received the first Fulbright-Nokia scholarship award.*

# IEEE VTS NEWS

## Gaspar Messina

Readers will be sorry to hear of the death, on 4th June 2005, of VTS News Senior Editor Gaspar Messina. Gaspar was a very long-standing contributor to the society, both as Chapters Co-ordinator, a position he held until the month before his death when it was reorganised into a newly reorganized Membership Development Committee that includes chapter relations and distinguished lecturer coordination, and as Senior Editor responsible for Chapter News and Meetings. He took up his position on the VTS News in November 1982, taking over from then Vice-President Sam McConoughey. At that time VTS had 25 chapters, and in his first column he 'hoped to see a flurry of Meeting Reports and Election Results sent to the Chapters Activities Chairman'. Unfortunately that never appeared to the degree that he would have liked, and Gaspar was frequently chasing people for reports for his column. He will be missed.

## VTC2005-Spring in Stockholm

A highly successful VTC2005-Spring attracted almost 800 attendees to Stockholm at the end of May. 659 papers were presented, along with panels and plenary presentations, and delegates were hosted by the Mayor of Stockholm for a reception at the City Hall on the first night. A full report on the conference will appear in the next VTS News.