WiFi: What's Next?

Paul S. Henry and Hui Luo, AT&T Labs — Research

ABSTRACT

WiFi, also known as 802.11b, has become the preferred technology for wireless local area networking in both business and home environments. Even though it was designed primarily for private applications, WiFi is also being deployed in public places to create so-called hotspots, where WiFi-capable users can obtain broadband Internet access. This new domain of application could be the major future market opportunity for WiFi, but in order to take advantage of it, several key challenges, both technical and business-related, must be overcome. In this article we outline these challenges and discuss approaches to solutions.

INTRODUCTION

WiFi, the popular name for wireless local area networks based on the IEEE 802.11b standard, is one of the brightest areas of the communications business [1]. Annual industry revenue already exceeds $1 billion and is expected to pass $4 billion by 2007 [2]. No longer just an add-on capability implemented through a PCMCIA interface card, WiFi is now available as a built-in feature in a wide range of user devices. Equally impressive is the way WiFi has captured broadbased interest in the popular press [3]. Increasingly, it is viewed as not just a newfangled networking gadget, but rather as the vehicle that will usher in a new era of untethered broadband Internet access for the general population.

This article paints a picture of a national (or even global) landscape dotted with inexpensive WiFi hotspots offering easy, and often free, broadband Internet access to anyone equipped with a WiFi-capable laptop or PDA. The picture is, of course, unrealistically rosy, but at its core captures the idea that WiFi, although originally intended primarily as a wireless extension of office Ethernets, could be much more: it could be the platform for ubiquitous broadband access. Extension of WiFi from the office environment to wide-area coverage opens new vistas for WiFi technology and will likely be a key driver of its future growth. But this will not happen simply by marketing WiFi to a broader audience. Substantial challenges on both technical and business fronts must be addressed. In this article we take a more careful look at the vision of ubiquitous WiFi and identify the challenges that must be met to make it a reality.

To put the discussion in context and allow us to focus on specific details and problems, we choose a service scenario likely to be important to WiFi growth; namely, delivering broadband IP connectivity to the traveling professional, the laptop-toting road warrior. The challenge is to give him or her a computing environment similar to the one available with a desktop computer supported by Ethernet in a conventional office setting. Stated succinctly, our goal is to *reproduce the desktop experience* for the traveling professional, as illustrated in the following scenario [4].

Jill, a major account saleswoman, is at her corporate home office, as shown in Fig. 1, working on her WiFi-connected laptop, when she must leave to catch a flight to visit a customer. Although she has several applications open, some running on network drives, she does not close them. She simply stops work and suspends her laptop. Once at the airport, she finds that the gate area is a WiFi hotspot. When she opens her laptop and authenticates herself, the computer immediately builds a secure tunnel through the Internet back to her corporate intranet and presents her with the open applications she was using at the office earlier in the day. The experience to Jill was almost the same as if she had remained at the office, but had locked her computer while she stepped away from her desk to attend a meeting. As far as she could tell, her laptop was "always on"; there was no need for annoying shutdown and reboot when moving from office to airport. When she walks over to the airport restaurant, she has the same "close and go, open and resume" experience. In the air, using the plane's internal WiFi network connected via satellite back to the ground, she continues her work. Finally, upon arrival at her client's premises, she discovers that WiFi network access is unavailable. Undaunted, she slips a cellular network interface card into her computer and continues, albeit at reduced bandwidth, where she left off.

To make WiFi networking an everyday tool for road warriors, as commonplace as their cell phones, major enhancements to existing WiFi technology are required. At the risk, perhaps, of oversimplification, the challenges ahead for WiFi engineers can be grouped into four broad categories: ease of use, security, mobility, and network management. While there is considerable overlap

0163-6804/02/$17.00 © 2002 IEEE

across these areas, the grouping is nonetheless useful for structuring further discussion.

Ease of use: From the beginning, simplicity of operation has been a paramount concern for wireless LANs (WLANs). They were designed to add functionality to existing wired LANs without imposing added inconvenience on the user. Maintaining that philosophy — hassle-free operation — as WiFi capabilities are extended to support the road warrior is a major challenge.

Security: Both on corporate premises and off, WLANs represent potentially serious security vulnerabilities. It is still not clear whether adequate security is compatible with the ideal of simple low-complexity implementation that has contributed so much to the popularity of WiFi up to now.

Mobility: Enabling WiFi mobility within a single building is relatively simple. Extending it to public hotspots with secure always-on connectivity is far more difficult. (Integration with cellular WANs, which will be discussed only briefly in this article, only adds to the problem.)

Network management: WiFi networks, especially those containing hotspots, present daunting management challenges. Service must be provided despite selfish behavior by users, hacker attacks, and interference from other systems.

We take up these challenges in the next four sections.

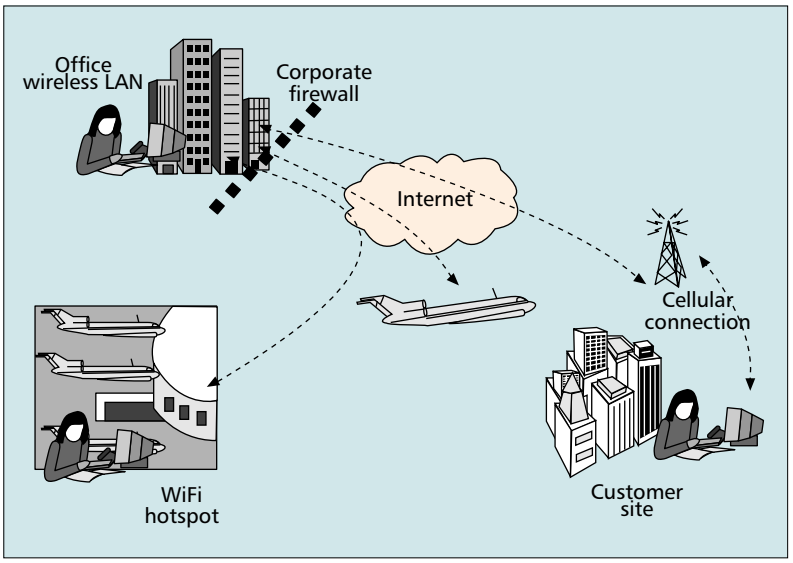

Figure 1. *Always-on connectivity is maintained as the road warrior moves from office to airport to customer site.*

Ease of Use

In a recent column R. W. Lucky lamented the complexity of wireless data networking [5]. He describes a scene at an engineering conference where a group of networking experts tries to get their laptops linked to a WiFi network. After recounting the frustrations of the adventure, he concludes with the plea, "What I want is a push-to-talk button." What Lucky encountered was the all too common problem of configuring WiFi for public networks. That is, one has to set up the service set identifier (SSID), choose "open authentication" as the link layer authentication method, disable the use of Wired Equivalent Privacy (WEP), and then restart DHCP. This process, which is annoying at best, could well become a serious impediment to broad-based adoption of WiFi networking.

Lucky has it right: ease of use is at the top of the list of challenges facing WiFi. Although impressive advances have been made in this direction, we are still far from a satisfactory solution. Universal Plug and Play, for example, has made it vastly easier to interconnect computing devices, especially in the home environment [6]. And in an attempt to deal specifically with the complexity of WiFi networking, Windows XP offers "automatic wireless network configuration," whose purpose is to automatically establish connection with nearby WiFi access points (APs). Initial setup to enable this feature, however, is far from simple. In a typical academic environment, 18 steps are required for initial configuration, an open invitation to error and user frustration [7].

WiFi configuration is even more burdensome in the corporate environment, where data security is a primary concern. WEP, the native security capability offered by WiFi, was designed for simplicity of operation, but it is sufficiently difficult to use that in many WiFi installations, including businesses where security is important, it is not even turned on at all. The reasons behind such behavior are unclear, but the net result is that a key feature of WiFi, communications privacy, is often left unused, even in critical situations.

Still another layer of complexity arises when our road warrior wants to use a commercial WiFi hotspot (e.g., at an airport). The hotspot operator's access control mechanism must serve the dual purpose of authorizing existing subscribers while also enabling first-time users to sign up and one-time users to pay on site. Browser-based authentication, a popular technique that serves both these ends, is convenient and user-friendly, but vulnerable to relatively simple theft-of-service attacks. A more comprehensive approach, as specified in the 802.1x standard [8], protects against this and several other attacks, but only at the cost of added complexity; namely, the WiFi user at the hotspot must have a prearranged service account. This is a serious, perhaps unacceptable, disadvantage in the still embryonic hotspot business, where subscriber acquisition is a top priority.

No matter what other features WiFi networking may offer, until it provides user-friendly setup and secure hotspot sign-on, it will be unable to live up to its full potential.

Security

Most of the breathless predictions of WiFi growth focus on the appeal of free public access, a mildly utopian vision where issues of network security are of secondary importance. There is another, darker side to the WiFi story, however, which concerns its vulnerabilities to eavesdroppers and other hackers. A commonly reported scenario involves a hacker, and not a very skillful one at that, sitting in a parking lot listening to the WiFi communications of a nearby retail establishment. This takes no great skill, because WEP, as mentioned earlier, is often not enabled, so valuable data like credit card numbers are

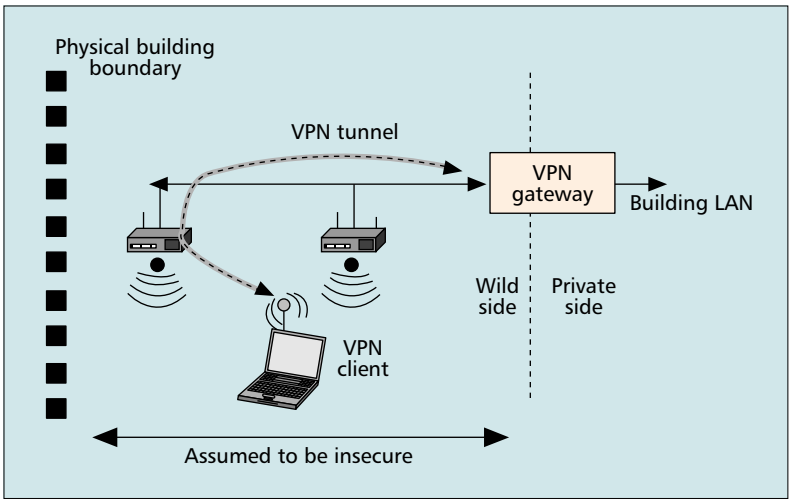

Figure 2. *A VPN tunnel protects data in an insecure environment.*

easy to capture. Revelations such as these have raised serious concern about the viability of WiFi in the commercial world, an issue that has only been exacerbated by the discovery that even when WEP is operating, the encryption key can be recovered by a hacker with only a modest amount of effort. [9] Thus, whether WEP is on or off, WiFi networks are essentially insecure.

In defense of WEP, it should be borne in mind that it was never intended to be a bullet-proof security solution. Rather, WEP was designed to be a simple, easy-to-use technique to provide wired equivalent privacy. That is, the effort required to break the cipher was expected to be roughly comparable to the effort needed by an intruder to tap into a wired Ethernet. The ease and efficiency of the key recovery attack, however, showed that WEP could not provide even this modest level of security. Recognizing that such a shortcoming could be a fatal blow if not corrected quickly, the WiFi community has developed two approaches to dealing with the problem: retain the native security approach of WEP but fix its flaws, or abandon it and provide a separate security overlay, a virtual private network (VPN) on top of the insecure WiFi network. Both of these have the potential to restore faith in WEP security, but whether either can offer the balance of security and ease of use needed for broad-based market acceptance remains to be seen.

Native Security (Enhanced WEP)

The effort to improve WiFi security within the IEEE 802.11 organization aims at the same goal that motivated design of the original WEP: protection of the air link between the AP and the WiFi user. It is assumed that the wired network supporting the AP is adequately secure and needs no further protection. The proposed improvements to WEP focus on two areas: access control, addressed in the 802.1x standard, and encryption, being developed under 802.11 Task Group i. [10] To protect against man-in-the-middle attacks, which are easily carried out in the WLAN environment, 802.1x provides a framework for mutual authentication; that is, a process that enables the network to authenticate itself to the user, and vice versa. It relies on a database of authorized users and permits WLAN access only to those who properly authenticate themselves. Network access can be controlled and configured by a central authority, which eliminates the cumbersome key distribution process required by conventional WEP. A second important feature of 802.1x is support for frequent key exchange between the endpoints of a WiFi air link. This mechanism enables the use of Temporal Key Integrity Protocol (TKIP) [8], an improved encryption procedure able to thwart the key recovery attack that was so damaging to the original WEP. Although still not endorsed by 802.11 Task Group i, which is evaluating several encryption techniques, TKIP is considered to be so promising as a cure for WiFi's security problems that it is being rushed to market in prestandard form.

There are two challenges facing the 802.1x/802.11i approach. The first relates to time to market. Enthusiasm for WiFi, which has been strong for the past few years, has weakened recently because of security concerns. The longer it takes to develop a standardized security system to replace WEP, the harder it will be to rebuild WiFi momentum. The second challenge is to convince skeptical system administrators that they can safely entrust their company's private communications to a solution that has had only limited public scrutiny.

Virtual Private Network

The VPN approach to WiFi security assumes that the wireless LAN (including the wireless link and the wired network supporting the access points) is insecure, regardless of whether WEP is turned on or off. Protection is provided by a separate security mechanism, typically an IPsec tunnel, running on top of the wireless link and extending from the user's computer to a VPN gateway installed behind the APs, as shown in Fig. 2. [11] This provides end-to-end protection, independent of the vulnerabilities of the underlying network. A straightforward extension of this architecture, of course, can also protect the communications of an employee using an off-site WLAN, such as a WiFi hotspot.

VPN technology has been commercially available for several years and is generally considered to provide strong security, but the cost, especially for corporate WLANs, is significant. Since the APs and associated wiring are assumed to be insecure, they must be kept physically separate from the existing premises wired LAN. That is, a distinct, independent wired network must be installed and maintained. And since all WiFi communications, even traffic confined within the corporate premises, must be processed by a VPN gateway, scaling to large numbers of users is difficult.

If a practical security solution to replace WEP is not found quickly, there is a real danger that WiFi could lose the marketplace momentum it has built over the last few years.

One solution, enhanced WEP, has the advantage of fitting naturally and simply into the WiFi infrastructure, but market acceptance may be disappointing due to standardization delays and user community concern that the debacle of original WEP security could be repeated. VPN, on the other hand, is an established, trustworthy security

solution, but implementation complexities, especially on corporate premises, may prove unacceptable.

One final issue of WiFi security concerns attachment of an unauthorized access point, a "rogue AP," to the corporate intranet. Whether through negligence or malice, such an action can have disastrous consequences. Further discussion is postponed until "Network Management" below.

MOBILITY

Mobility, of course, is a core feature of WiFi networking. Even the most rudimentary WiFi deployment allows, at the very least, roaming within the vicinity of a given AP. By analogy with telephony, this might be called "cordless roaming." What is needed to support the road warrior, however, is something more akin to the global roaming capability of cellular systems.

TECHNOLOGY

The first step on the path to WiFi mobility is device-level multivendor interoperability, which ensures that the wireless LAN network adaptor (typically a plug-in card) employed by a WiFi user can establish communication with APs built by different manufacturers. Reliable interoperation, which is not guaranteed simply by conformance to the 802.11b standard, was achieved through the WiFi initiative under the Wireless Ethernet Compatibility Alliance (WECA) [1]. Indeed, WiFi certification has become the de facto standard for 802.11b-based products. Further progress toward large-scale service-level roaming is being driven by another WECA initiative known as Wireless Internet Service Provider roaming (WISPr). Although details of WISPr are not public, it appears that the goal of the effort is to build consensus on best common practices for wireless roaming. Such capability would enable a subscriber of one WISP to roam to another's territory, authenticate himself, and gain access to that network. The WISPr proposal would provide a uniform mechanism for handling the authentication, authorization, and accounting (AAA) functions needed to do this. A more ad hoc approach to roaming across multiple WISPs is to aggregate them under an umbrella organization and resell their services via a single subscription. Boingo, which will be discussed later, is an example of this approach.

While the WISPr or aggregator capabilities described above can form the basis of ubiquitous WiFi access, they are not enough to enable the kind of mobility that was enjoyed by our road warrior described earlier. The missing component is always-on mobility, which requires an infrastructure that can provide a secure wireless connection promptly on demand, and that permits close-and-go, open-and-resume operation. That is, the system must maintain suspended computing sessions, and provide a secure connection "instantly," whenever needed. This feature is more than just an added frill. Customer response to cable- and DSL-based broadband Internet access suggests that the convenience of being always on is as important to the subscriber as broadband data capability per se [12].

Always-on mobility can be implemented via Mobile IP (MIP) or a number of other approaches [13]. Typically what is needed is a central mobility manager (the home agent in MIP) to keep track of the mobile user and orchestrate conventional IP routing, and a mobility client (the foreign agent in MIP, which can be either deployed as a standalone component in a foreign network or built into the OS of the mobile computer) to handle connection details in the vicinity of the user, as shown in Fig. 3. Together, the manager and client create and move the MIP routes as needed by the user, and ensure that sessions do not get broken when the user suspends operation or is handed off from one subnet to another. Note that for typical data applications there is no need for the real-time seamless handoff used in cellular telephony. A gap of a few seconds while a connection is being rerouted will cause no great harm. If, however, mobile WiFi customers begin to use time-sensitive applications, such as voice or streaming media, the luxury of slow handoff will no longer be tolerable.

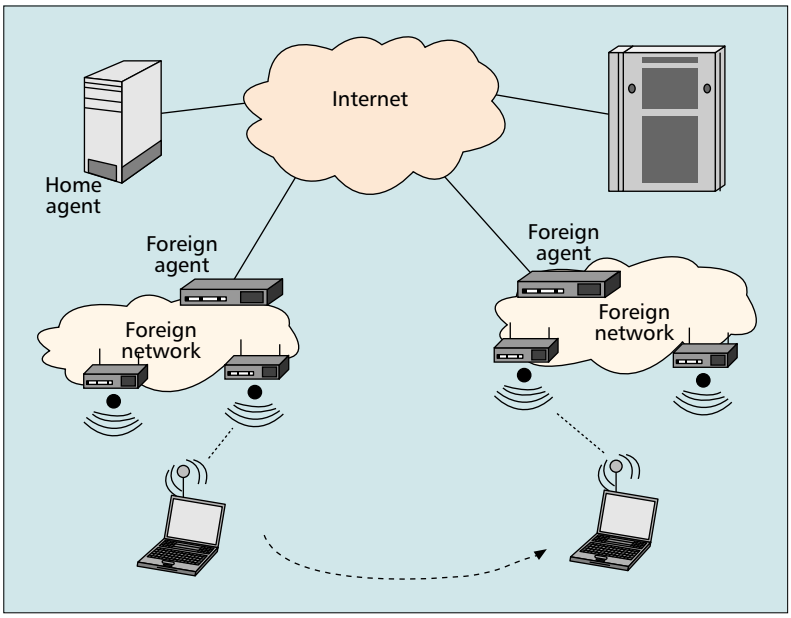

Figure 3. *Mobile IP manages routing as the mobile host moves.*

Mobile IP, together with an end-to-end security solution such as a VPN, provides a conceptually satisfying approach to the always-on connectivity needed by our road warrior. Unfortunately, this capability is not currently available as a standard feature of popular operating systems (OSs) such as Windows or Mac, and implementing it on such closed platforms presents a major challenge. The problem stems from the fact that both MIP and VPN are layer 3 approaches, best implemented in the OS's IP stack. For closed OSs, however, this avenue is blocked; the only recourse is to wait for an OS release that offers the feature, or resort to workarounds. Both hardware and software workarounds have been proposed (e.g., by Ecutel and IPUnplugged), and trials are now underway.

Whether through OS release or workaround, a user-friendly solution for secure, always-on mobility is a key requirement for extending WiFi support to the corporate road warrior.

Since it is unclear which strategy, if any, can succeed in this embryonic business, many WiFi service entrepreneurs are focusing simply on staking out real estate, attempting to lock up prime sites for hotspots to maximize their future revenue potential and/or attractiveness to potential suitors.

Service Providers

There seems to be little question that the technology for secure, always-on WiFi mobility is within reach. The economic viability of such a service, however, is far more problematic. The experiences of recent wireless broadband service providers are not encouraging. One of the pioneers, Metricom, went bankrupt in July 2001. MobileStar, an ambitious hotspot operator, followed in December. Other companies are struggling. Nevertheless, the potential business opportunity is so great that there is no shortage of entrants into the fray. [14] The central issue is how to achieve scale. It is widely conceded that large networks are much more likely to be profitable than small ones, but especially in the current economic climate there is no realistic possibility of securing enough capital to create, say, a national network in one stroke. Instead, entrepreneurs must start small and arrange to grow quickly to profitability, or at least survive until a national player, perhaps a cellular operator, sees the value in owning a large-scale WiFi network and buys them out. Since it is unclear which strategy, if any, can succeed in this embryonic business, many WiFi service entrepreneurs are focusing simply on staking out real estate, attempting to lock up prime sites for hotspots (airports, hotels, etc.) to maximize their future revenue potential and/or attractiveness to potential suitors. The three major approaches to establishing a presence on the WiFi service provider landscape are the franchisor, the carrier, and the aggregator.

The Franchisor

This model is probably the simplest approach to building a public WiFi access network. A franchisor (i.e., franchising company), such as Joltage, strikes an agreement with an individual location, perhaps a restaurant, that already has WiFi installed for its own internal business purposes. The franchisor provides software and back office operations to allow the franchisee to offer paid public access to the network. The revenue from the resulting hotspot operation is split between franchisee and franchisor.

The WiFi Carrier

The WiFi carrier typically owns and operates a number of APs in public spaces. Subscribers may use the service whenever they find themselves in one of the carrier's hotspots. Some carriers, like SurfAndSip, are "pure play" WiFi operators whose sole product is WiFi service. They tend to be small, with only a few dozen access points. Larger carriers, like Wayport, tend to offer a variety of services, like wired broadband access, in addition to WiFi. The larger company, of course, has a survival advantage over the smaller pure-play operator. Other WiFi carriers, such as T-Mobile HotSpot, are wholly owned by a parent communications company. The WiFi carrier gets vital support through infancy, and if it prospers, the parent (T-Mobile USA in the case of T-Mobile HotSpot) can integrate it smoothly into its larger portfolio of communications services. Such a scenario would be especially attractive to cellular carriers, a point we will return to later.

The Aggregator

The aggregator strikes wholesale partnerships with WiFi operators and resells their services, thus giving its subscribers access to a number of networks. This approach is well suited to rapid scale-up in size because the aggregator owns little or no infrastructure. It grows by making deals with infrastructure owners. Boingo, probably the most well-known aggregator operating today, offers its subscribers access to several hundred hotspot locations operated by a variety of carriers, including Wayport, SurfAndSip, and AirPath.

If WiFi public access shows signs of economic viability, cellular carriers will likely be interested in participating, through either partnership or direct acquisition. Even if WiFi hotspot service is marginally unprofitable, synergies with a cellular system, such as one-stop shopping and joint billing, might allow it to rise to profitability. Although it is clear that cellular operators can bring strength to WiFi, it is not so obvious that WiFi brings strength to cellular. One could make an argument that WiFi only cannibalizes revenue that would otherwise have gone to third-generation (3G) cellular, and that the best course for the cellular operators is to encourage WiFi's demise. A more prudent view, however, suggests that a WiFi service offer could buy time for the cellular operators and ease the pressure for a rapid (and expensive) rollout of 3G, which has already suffered from a number of well publicized delays [15]. In time, as 3G makes its appearance, it could be offered as the wide-area complement to existing WiFi service. Certainly from the user's point of view, integrated WiFi and wide-area cellular would be an attractive offer. This message has apparently not been lost on the cellular industry. Ericsson, for example, has started shipping infrastructure equipment to enable a cellular operator to provide integrated WiFi/cellular service. Lucent has also announced similar products, and Nokia offers a PCMCIA network interface card with both WiFi and General Packet Radio Service (GPRS) capability. On the operator side, Sprint PCS is an investor in Boingo, VoiceStream (now T-Mobile) has purchased MobileStar's assets, and Rogers AT&T Wireless has conducted trials of combined cellular and WiFi service.

The key to broad-area WiFi mobility is an infrastructure of public access hotspots, but at this early stage in the evolution of such businesses, it is not clear if building an independent infrastructure for WiFi is economically viable. A possible solution, which could enable cellular operators to establish an early foothold in the WiFi business, is to reuse the cellular data infrastructure via vertical handoff techniques on mobile devices equipped with both WiFi and cellular interfaces. That is, a MIP client could use the cellular network to provide default always-on connectivity while scanning for WiFi APs. As soon as an AP is found, the client switches to the WiFi connection. Regardless of how the public WiFi industry develops, survival tends to favor larger networks, so over the next few years the smaller operators are likely to disappear in the face of consolidation among WiFi carriers, growth of aggregators, and possibly acquisition by cellular operators.

NETWORK MANAGEMENT

Innovative wireless technology and a well thought out business plan will come to nothing if the WiFi network is poorly managed. In addition to the usual tasks associated with management of wired LANs, such as monitoring equipment health and traffic load, WLANs present additional challenges because network performance is heavily dependent on variable and unpredictable characteristics at the physical layer (i.e., the air link). Managing the network to ensure even minimal physical-layer performance — delivery of adequate signal strength with an acceptable level of unwanted interference — is a major problem. Cellular systems face a similar issue, but have the advantage that, for the most part, they are designed as complete systems, with adequate management tools integrated from the outset. WLANs, on the other hand, are more frequently overlays onto the existing wired infrastructure, with only rudimentary tools for managing signal strength and interference. Indeed, the very ease with which an AP can be added to a wired LAN is itself the source of a serious network management problem, the so-called rogue AP, which is discussed later.

SIGNAL STRENGTH

In a wired LAN, signal strength problems almost always stem from gross component failure, such as a broken wire or faulty interface card; physical-layer performance is essentially binary: either it works or it does not. The situation is altogether different in the wireless world, where routine changes in the location of a user can cause signal strength variations of 30 dB and more. The network manager must be able to distinguish between variations caused by normal operation and those that indicate impending failure, caused, perhaps, by reconfiguration of office partitions. For a small network, consisting of, say, a dozen or so APs, signal strength issues can be managed by a hands-on administrator, a local expert, who through personal experience has developed a close familiarity with the network and its inevitable idiosyncrasies. A large network, however, consisting of hundreds or even thousands of APs cannot be run in such a personalized fashion. This problem is particularly acute for operators of public hotspots, where management is typically done by a centralized staff at a remote site. Personal familiarity with the physical network environment is a practical impossibility, so powerful physical-layer management tools are needed. The IEEE 802.11 community, recognizing this need, has chartered a Radio Resource Measurement Study Group to address the problem [10]. This effort is a first step in developing the physical-layer tools that will make WiFi networks truly manageable entities.

INTERFERENCE MANAGEMENT

Here again, the management task is similar to that faced by cellular operators, but with a crucial difference: cellular systems operate in licensed frequency bands, whereas WiFi networks use unlicensed spectrum. The cellular operator, in principle at least, can manage the radio spectrum across the service area to optimize system performance. The WiFi operator, by contrast, must cope with multiple sources of interference, many of which are not under his control. In such an environment, the entire notion of network management might seem to be an oxymoron. But the situation, while challenging, is by no means hopeless. Through a carefully crafted combination of MAC-layer techniques and frequency channelization, WiFi networks are able to perform at least rudimentary management of mutual interference among users. Going forward, moreover, IEEE 802.11 Task Group e will likely recommend additional tools to enable different grades of service (presumably at different price points) to be offered to specific groups of users. Such tools will be important weapons in dealing with the bandwidth hogs likely to appear at public WiFi sites [10]. Despite these advances, however, WiFi networks will remain vulnerable to other sources of interference, such as a microwave oven operating in the same frequency band or a nearby WiFi network under the management of a different business organization. This latter problem is not serious today because the density of WiFi installations is still relatively low, but it will become increasingly severe as WiFi proliferates. It is imperative that management tools be developed to enable system administrators to monitor interference, identify its source, and take corrective action.

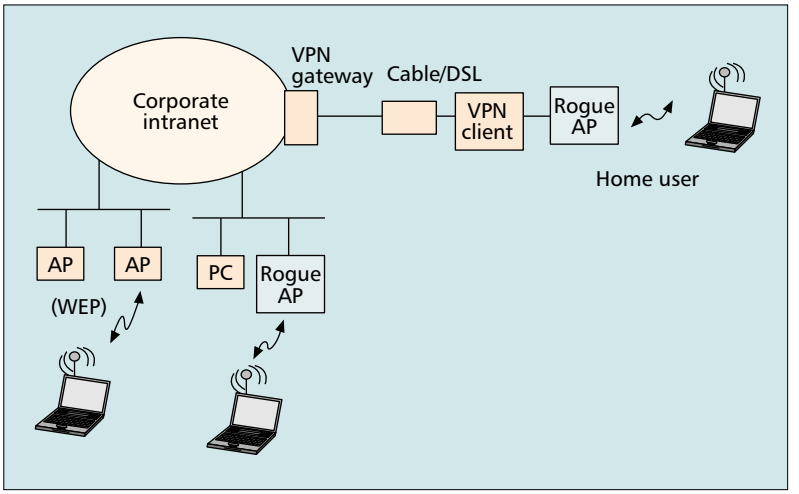

Figure 4. *A rogue AP represents a major security vulnerability.*

THE ROGUE AP

A particularly nettlesome issue for the WiFi network manager is the problem of the rogue AP: an unauthorized AP attached to the corporate intranet, perhaps on company premises, or possibly in the home of a teleworker, as shown in Fig. 4. In addition to being a source of interference, the rogue AP is a major security vulnerability. Independent of whether the corporation uses WEP or VPN, a rogue AP with WEP disabled can expose internal corporate communications to the outside world. Even if WEP is enabled on the rogue, corporations using VPN to secure their WLANs become vulnerable to attacks that would otherwise be harmless. Detecting rogues on corporate premises, perhaps through sniffing and pinging techniques, will be an added, but probably manageable, burden for network man-

WiFi networks will remain vulnerable to other sources of interference, such as a microwave oven operating in the same frequency band or a nearby WiFi network under the management of a different business organization.

agers. Much more difficult will be the problem of detecting rogues in employee residences. If WiFi is to continue to expand into the business environment, tools and techniques must be developed that will give administrators confidence that security is not being compromised by rogues, whether on premises or off.

SUMMARY

WiFi is a wonderful example of how a solution to a narrow problem — wireless extension of Ethernet — can become the foundation of a grand vision: ubiquitous broadband mobility. In this article we explore what will be required to make this vision a reality. We focus on WiFi service to support the traveling professional, and through this scenario identified four areas — ease of use, security, mobility and network management — that presented key challenges to WiFi evolution. The technical problems, although by no means trivial, seem tractable, and the proposed approaches to solution are promising enough to give one hope for the future. Much less certain, and much more troubling, are the business issues. The economic viability of the public hotspot market, which is a cornerstone of ubiquitous WiFi access, is still unclear. Nonetheless, current WiFi momentum, combined with the business potential of integrated WiFi and cellular services, are enough to justify at least cautious optimism.

ACKNOWLEDGMENT

For countless discussions and helpful suggestions, we thank our many colleagues, especially Zhimei Jiang, B.-Y. J. Kim, Kin Leung, and N. K. Shankaranarayanan.

REFERENCES

[1] WiFi (Wireless Fidelity): http://www.wi-fi.org
[2] C. S. Loredo and S.W. deGrimaldo, "Wireless LANs: Global Trends in the Workplace and Public Domain," The Strategis Group, 2002
[3] "Special Report — Wireless Internet," *Business Week*, April 29, 2002.
[4] H. Luo *et al.*, "Internet Roaming — A Wireless LAN/3G Integration System for Enterprises," *Proc. SPIE APOC 2002 — Wireless and Mobile Commun. II*, Shanghai, China, Oct. 2002.
[5] R. W. Lucky, "Cannot Connect," *IEEE Spectrum*, vol. 39, no. 1, Jan. 2002, p. 112.
[6] B. A. Miller *et al.*, "Home Networking with Universal Plug and Play," *IEEE Commun. Mag.*, vol. 39, no. 12, Dec. 2001, pp. 104–9.
[7] Univ. of So. CA, http://www.usc.edu/isd/doc/wireless/winxp/wirelesswinxp.html
[8] Cisco Aironet Wireless LAN Security Overview, http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm
[9] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," *8th Annual Wksp. Sel. Areas in Cryptography*, Aug. 2001.
[10] 802.11 Working Group: http://grouper.ieee.org/groups/802/11/
[11] S. Convery and D. Miller, " SAFE: Wireless LAN Security in Depth" http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm
[12] L. Gill, "Broadband Adoption on the Rise," *Ecommerce Times*, June 24, 2002, http://www.newsfactor.com/perl/story/18355.html
[13] A. T. Campbell *et al.*, "Comparison of IP Micro-Mobility Protocols," *IEEE Wireless Commun.*, vol. 9, no. 1, Feb. 2002.
[14] P. Wuh *et al.*, "Why Wireless Carriers Should Care About Wi-Fi," *Goldman Sachs Res.*, May 3, 2002.
[15] J. Blau, "More Delays, Uncertainty Rock Wireless Europe," IDG News Serv., Aug. 12, 2002, http://www.idg.com.sg/idgwww.nsf/unidlookup/2F994CF8CE57C85348256C1300065051?OpenDocument

BIOGRAPHIES

PAUL HENRY [F] (psh@research.att.com) has been with AT&T (Bell) Laboratories since 1970, engaged in research on communications networks and circuits as well as radio astronomy instrumentation. He is currently head of the Broadband Wireless Systems Research Division in Middletown, New Jersey, where his research interests focus on bringing high-speed Internet connectivity to mobile and portable computers. He served as a Technical Editor of *IEEE Communications Magazine*, a Guest Editor for the *Journal of Lightwave Technology*, and has published papers or patented inventions in several fields, including wireless systems, data security, millimeter-wave radio techniques, and cosmology. He was a Traveling Lecturer for the IEEE Lasers and Electro-Optics Society as well as Keynote Speaker at Infocom 2002. He received his A.B. and Ph.D. degrees in physics from Harvard and Princeton University, respectively.

HUI LUO received his Ph.D., M.S.E.E., and B.S.E.E. degrees in 1994, 1991, and 1990, respectively, all from the Department of Automation, Tsinghua University, Beijing, China. From 1995 to 1997 he was a postdoctoral research associate with the Department of Electrical Engineering, University of Notre Dame, Indiana, where his research area was blind signal processing. From 1998 to 1999 he worked as an R&D engineer with Digital Video Express LP, Herndon, Virginia, where his research area was digital watermarking. Since mid-1999 he has been working at AT&T Labs-Research, Middletown, New Jersey, where his research areas include wireless/mobile networking, network security, and signal processing for wireless communications. He is now a principal technical staff member with AT&T Labs.