

Wireless Wonder: WLANs, Public Wireless, and an Emerging Ubiquitous Internet

Sanjay Ginde¹

Roddy Knight²

Chris Zeiders³

December 10, 2002

¹sjg@duke.edu

²rhk@duke.edu

³cmz@duke.edu

Abstract

Wireless networks are creating a mobile, ubiquitous Internet. Rapid proliferation of this emerging technology is creating viable solutions for mobile users. Wireless networks are presenting new opportunities for mobile users, but are also causing tension between broadband Internet Service Providers and their customers. Wireless networks present unique networking problems due to the air-medium for the transfer of data. In addition to transmission concerns, engineers are addressing security issues to ensure that wireless networks have a comparable level of security to traditional "wired" networks. This paper will address the social aspects, technical details, and security considerations of wireless networks.

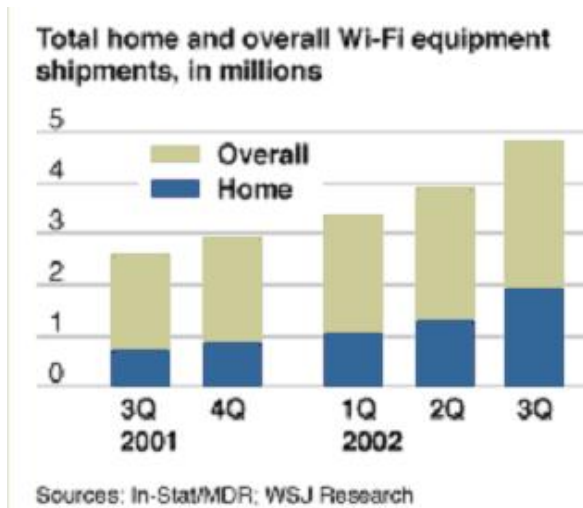


Figure 1: Wireless Growth

1 Public Wireless Internet

The wireless network phenomenon has the potential to revolutionize Internet access. Dell Computer sells all new laptops with integrated wireless cards and Intel is incorporating wireless technology directly into its new microprocessor dubbed Banias. Intel expects wireless capability to be a standard feature in new computers. Wi-Fi equipment sales have doubled from last year and will reach 16 million units this year [1]. Public wireless net-

works in particular empower laptop owners with wireless cards to surf the web in public areas such as parks and cafes after a relatively minimal investment in wireless equipment. In some cases public networks are funded by local governments seeking to attract tech-savvy citizens and in others by the magnanimity of a loose network of individuals. These individual providers generally offer connectivity through an access point attached to the broadband connection in their home or small business. Although public wireless networks are established for varying purposes, they share the common goal of offering ubiquitous Internet access to mobile users. The free public networks, however, face a legal challenge that the commercial ones do not. Several ISPs have explicitly forbidden customers to attach public access nodes to their residential broadband connection. Indeed, customers have received a plethora of threatening legal notices ordering them to terminate public wireless access at their location. Accordingly, commercial public access networks



Figure 2: New York Hot Spot Map [2]

will become the standard as they are better publicized and more deliberately maintained.

1.1 Wireless User Groups

User groups are partly responsible for the proliferation of free public access networks. By maintaining web sites with lists of hotspots, user groups keep their members informed about where to look for publicly accessible networks. The membership base is comprised of broadband customers with

freely accessible nodes attached to their connection. Because wireless networks are imperceptible to the human eye, a database of access points is invaluable to the mobile Internet user. The sites, such as NYC wireless, display the status of access points to alert users to congestion problems [2]. The common designation of "full" forewarns a member that he should wait for a more opportune time to attach to the access point. NYC wireless reports that around 60 to 70 users per day access each hotspot [3]. In addition to status information, many user groups, such as the Bay Area Wireless Users Group, provide an online forum for promoting issues related to public access and sponsor monthly meetings of members [4]. In this way, user groups sponsor a sense of community among wireless users. The charter of the Seattle Wireless user group states [5]:

The wireless technology used by the members of the Seattle Wireless network creates the first telecommunications infrastructure that is not only inexpensive, but widely available and easily used so that it is now

truly possible for a network to grow from the grass roots of our community, based almost entirely on a wonderful combination of self interest and community spirit.

Wireless user groups are clearly popular because of the communal ideals they espouse. An acronym commonly referred to by the wireless user groups is "NYASPTWYOMB: not yet another service provider to whom you owe monthly bills." Most consumers, hounded by monthly service bills ranging from cell phones to cable television, find the concept of free access very appealing. As evidence of the diversity of the wireless user groups, BAWUG describes its membership base as a disparate alliance of "networking professionals, IEEE authors, and computer geeks". Like the successful free software movement, wireless user groups have an assortment of volunteers who invest their valuable time and equipment into making the network function properly.

1.2 Municipal Wireless Networks

The initiative of municipalities to fund local wireless projects in an attempt to attract high-tech entrepreneurs has also played an integral role in the growth of public access networks. For example, the city of Pittsburgh recently partnered with a nonprofit and a local business to offer wireless access in downtown parks. The city's partners, 3 Rivers Connect and Grok Technology, plan for the network to eventually cover a four-square-mile area of downtown Pittsburgh [6]. Although the network is free for now, expansion plans detail a customer charge of \$20/month once the network is complete. The Pittsburgh Public Wireless Internet project provides 10-megabit Internet access from two antennae on a metropolitan building. In a similar effort, public officials in Jacksonville, Florida and Ashland, Oregon have created wireless networks in shopping areas and neighborhoods to provide free Internet access. The city of

Jacksonville, in particular, hopes the network will lead to an increase in pedestrian traffic in an area of shops it wishes to revitalize. Municipal initiatives treat wireless networks as an infrastructure investment similar to roads and subways. Like proper transportation, wireless networks attract people to a particular location.

1.3 University Wireless Networks

Universities have discovered that wireless networks are a cost efficient and effective means of connecting the student body. With network nodes retailing for as little as \$100, the infrastructure investment necessary to enable wireless access is a fraction of the cost of wiring a building with copper cable for Ethernet. For example, Duke University provides wireless access in over forty-five locations around campus [7]. Duke plans to expand network coverage in the months ahead and simplify the authentication process. Cur-

rently, new users must e-mail the Office of Information Technology the Ethernet address of their wireless adaptor before Duke's network will assign their laptop an IP address. Similarly at UNC, forty wireless locations connect the mandatory laptops of all students. Wireless signals even reach nearby restaurants and cafes due to several carefully placed antennae. Course work there is tightly integrated with the Internet to exploit the universal connectivity. Students in English class employ the wireless Internet to share drafts and conduct research [8]. Learning is no longer limited to the classroom when resources are available through wireless across campus. UNC aims to produce tech-savvy graduates by placing essential technology at the fingertips of the student body. Dartmouth, however, has completed the most aggressive Wi-Fi rollout. More than 500 antennas broadcast signals to over 200 acres of campus. E-mail has replaced the phone as the dominant form of communication due to the ubiquity of the network. "Nobody here

knows anyone's phone number," remarks exchange student Ben Kadson [9]. Moreover, the network has inspired students to invent tools that take advantage of the network's broad reach. Mr. Kadson has patented a security device the size of a cigarette lighter that uses the Wi-Fi base stations to pinpoint its location. When the owner presses it during an emergency, it transmits its position to the proper authorities. Wi-Fi networks encourage ingenuity and promote collaboration in academia.

1.4 ISP Resistance

Internet Service Providers have not looked favorably upon the proliferation of public access networks connected to residential broadband lines. Rick Tate, a member of the NYC wireless project, received an ominous letter last June from Time Warner Cable warning him to cease offering public wireless access through a node attached to his cable modem. Time Warner Cable warned that Rick would

be held liable for any illegal activity perpetrated by a user attached to his wireless network because the activity would be traced back to him. The letter states [10]:

Individuals utilizing the Road Runner system to carry out criminal activity would be able to do so in an anonymous manner. In such circumstances, when law enforcement attempted to trace such activity, the trail would end with your account.

Although Time Warner Cable appears to have Rick's interest in mind, a more plausible motivation for the letter than protecting Rick from liability is that public access networks present a significant resource drain to Time Warner Cable. Indeed, cable modems are particularly susceptible to problems resulting from public wireless networks. The president of Road Runner, the high-speed Internet unit of Time Warner, refers to wireless user groups' practice of advertising node availability as "cable theft," [11].

1.5 Cable Service Issues

Cable modem users, unlike DSL users, share a common upstream pipe with others in their neighborhood to the carrier's backbone. DSL users each have an individual link to the carrier's backbone through a central office switch. Indeed, Verizon Communications and SBC Communications, the two largest national DSL providers, sell Wi-Fi equipment directly to their customers. Unlike their cable counterparts, DSL carriers realize that "to fight something that's available to someone is kind of fruitless," according to SBC product manager Alyssa Williams [3]. Cable modem service, on the other hand, is based on the assumption that only a small portion of the total cable modems in a neighborhood will be utilized at any given time. A public wireless network attached to a cable modem adversely affects the performance of the other cable modems in the neighborhood because it results in the maximum utilization of the cable modem's bandwidth around the

clock. To alleviate this problem, the carrier must add more capacity to the network, an expensive proposition. Hence, carriers have a monetary interest in preventing residential users from offering public wireless access through their cable modems. The wireless access nuisance is remarkably similar to a problem the cable industry has been battling for years-cable signal piracy. A survey by the National Cable Television Association in 2000 determined that cable operators lose approximately \$6.6 billion per year, 10% of total revenue, to cable pirates [3]. The rush to crack down on broadband customers with public access points is undoubtedly an attempt to prevent an analogous revenue shortfall. Network carriers forbid residential users from hosting a web server on their broadband connections for comparable economic reasons. Web serving continually taxes upstream bandwidth and forces the carrier to increase capacity in order to improve performance.

1.6 Electronic Frontier Foundation Initiative

In response to the determined efforts by Internet Service Providers to discourage customers from connecting public wireless networks to their residential broadband lines, the Electronic Frontier Foundation has created a list of ISPs that respect public wireless networks. On its web site, the EFF outlines the importance of public access networks [10]:

Community wireless networks are more than community-building exercises or a way to enable geeks to connect from coffee-shops. As Time Warner's legal department has noted, these networks are also a critical means of providing anonymous Internet access. Democracy demands that people be free to speak their minds, and sometimes the only way that can happen is if the speaker is shrouded in anonymity.

The very anonymity that Time Warner attacks in its letter to Rick is the primary benefit of public wireless networks according to the EFF. Anonymity not only encourages

whistle blowers to reveal the corrupt practices of corporations, but it also protects the speech of dissidents in America seeking asylum from repressive regimes such as China. More importantly, the anonymous wireless access provided by NYC wireless saved countless lives during the September 11th disaster last year. Survivors of the attack utilized wireless nodes provided by NYC wireless to spread the word about action on the ground and coordinate relief efforts over the Internet on their laptops. As the EFF remarks [10]:

The NYC Wireless group was on the front lines of disaster relief in Manhattan from the moment the attacks began.

Wireless user groups are undeniably valuable to the community and therefore deserve public support.

1.7 Joltage Commercial Service Model

Most of the fifteen ISPs on the EFF list have an Acceptable Use Policy that expressly per-

mits bandwidth sharing, but Atlas Broadband goes even further by offering customers free hardware to establish a wireless access point. Atlas Broadband has a deal with Joltage, a company that distributes free wireless nodes to broadband customers in exchange for user agreement to join the Joltage network. The Joltage network is an alliance of broadband customers with wireless networks that charge the small fee of \$2/hour for access. Joltage handles billing and distributes 50% of the revenue to the administrator of the access point. Commercial business models for public wireless networks like Joltage can certainly coexist with free access models. The user benefits from both because wireless network coverage is more expansive than it would otherwise be with only one access model.

1.8 Threat To Cellular Networks

In addition to cable providers, cellular operators perceive Wi-Fi networks as a serious threat. Cellular carriers have spent over \$6 billion dollars the last several years upgrading their networks for high-speed Internet access. The expensive bet on the future of connectivity is predicated on the assumption that consumers will browse the web and send e-mail wirelessly from their laptops and hand-held devices. Because Wi-Fi networks require a fraction of the infrastructure cost and offer bandwidth many times greater, cellular carriers are understandably concerned about their investment. Indeed, the price of Wi-Fi receivers for laptops has dropped from roughly \$500 three years ago to under \$100 today. Similarly, transmitters have fallen from over \$1000 to around \$200. "What [Wi-Fi] hotspots do is they really kill about 80% of the good near-term applications that the cellular providers were expecting to make

money off of,” according to Danny Briere, president of a telecommunications consulting firm [3]. In response, cellular operators are scrambling to grab a piece of the commercial Wi-Fi market. Spring PCS, the fourth largest cellular provider, has partnered with Wi-Fi firm Boingo Wireless. Boingo currently manages 950 hotspots and plans to deploy nodes in all Wyndham International hotels [1]. AT&T Wireless has positioned access points at Denver International Airport and intends to sell a PC card by Nokia that would utilize a Wi-Fi network when available and AT&T Wireless’s cellular network when out of range of a hotspot. Thus, cellular operators such as John Stanton, Chairman of VoiceStream Wireless, consider Wi-Fi “both a threat and an opportunity,” [3].

1.9 Expansion of Commercial Networks

Due to the legal concerns facing individuals administering public access points from

home, businesses will become the primary provider of public wireless Internet access. Businesses agree to a different Acceptable Use Policy than residential users when they sign up for broadband access; the service contracts for businesses typically do not preclude them from offering wireless access to multiple users. For instance, Starbucks has launched a concerted effort to offer wireless access through a business partner in all its stores. Indeed, it now offers wireless access in 1000 of its locations nationwide through connectivity provided by the German telecommunications firm T-Mobile [12]. T-Mobile charges a \$30 per month fee, similar to a broadband service provider, or \$2.99 for 15 minutes of access. Although a commercial service is certainly less appealing to consumers than the free access advocated by the wireless user groups such as NYC wireless, commercial service is typically more reliable. The nagging problem of congestion facing the free services is averted with commercial services like T-mobile because the necessary infrastructure

investment is recoverable through a monthly fee. T-Mobile plans to expand its commercial wireless network into 100 airline lounges and 400 Borders Bookstores through a \$100 million investment in Wi-Fi infrastructure [3].

1.10 Cometa Networks

The most ambitious company to date, Cometa Networks, has announced the aggressive goal of installing enough hotspots to provide coverage for the top 50 metropolitan cities. The venture, backed by AT&T, Intel, and IBM, will position the nodes in coffee shops, hotels, and public venues. Rather than marketing its services directly to consumers, the company will resell its product through Internet Service Providers who will be responsible for billing and customer support. Cometa has an advantage over the free service provided by wireless user groups because of "consistent, uniform service at a variety of locations," says AT&T Vice President Rose Klimovich [1]. The roughly 20,000 ac-

cess points the company requires to complete its network will come at a cost of \$10 million. After the network is finished, the company expects its partners to charge customers \$50 per month for service. The eagerness of the blue-chip companies to profit from the spread of Wi-Fi networks "obviously gives credibility to this whole arena," says Roberta Wiggins, director for wireless mobile services at Yankee Group [1]. The question remains whether the network will attract enough users to become a financial success.

2 Technical Overview

There currently exist many competing standards for wireless networks. The IEEE alone has three working groups for wireless network standards-the IEEE 802.11 working group for local area networks (WLANs), the IEEE 802.15 working group for wireless personal area networks (WPANs), and the IEEE 802.16 working group for metropolitan area networks (WMANs). Another stan-

dard, HomeRF is specially designed for wireless networks in a person's home or small office. The widely used Bluetooth wireless networking specification developed by Ericsson has recently been repatriated under the IEEE 802.15 WPAN specification [13]. The 802.11 WLAN standard began in 1989 and was originally intended to provide a wireless equivalent to Ethernet. As such, it has developed a succession of robust enterprise grade solutions that in some cases meet or exceed the demands of the enterprise network [13]. The 802.15 (WPAN) and 802.16 (WMAN) standards build upon the architecture of the 802.11 standard to suit more specialized needs. In this section of the paper, we will show how the 802.11 WLAN standard meets the needs of a wireless network and leave the other protocols for future research.

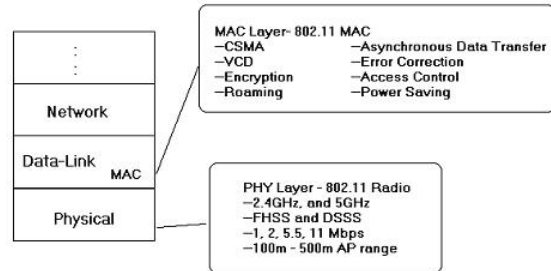


Figure 3: The IEEE 802.11 Protocol Stack

2.1 802.11 Protocol

The 802.11 standard fits into the physical and data link layer of the traditional OSI network. In the Physical layer the 802.11 standard supports such things as radio frequency Spread Spectrum technologies, support for the 2.4GHz and 5GHz ISM bands and supports access speeds up to 11Mbps with additional speeds available in the future. In the Data-Link layer, the 802.11 protocol also defines a standardized Media Access Control layer (MAC) which supports TCP/IP, UDP/IP, etc., a Virtual Collision Detection scheme, error checking, WEP encryption, roaming, power-saving schemes, and interfaces to OS drivers [13].

The IEEE 802.11 initiative is very active and there are currently nine task groups that address specific issues related with Physical and MAC layer optimizations/enhancements, security, and vendor interoperability. The 802.11b standard (known as "Wi-Fi") was the first WLAN specification and adopted by commercial vendors [14].

2.2 WLANs: Transmitting Data

Public wireless networks will drastically change how we use the Internet. It is important to understand the necessary requirements for wireless solutions. The most prominent difference between wireless networks and wired networks is the medium for the transmission of data. There no longer exists a physical connection between a client computer and the server-data is sent "through the air", and the most common medium of data transmission is via radio waves. (Data can also be transmitted through infrared signals,

but since infrared typically requires a direct sight-line between the two users, wireless networks generally demand the omnidirectional radio waves.)

2.3 Spread Spectrum: FHSS and DSSS

Although radio technology provides significant benefits-no longer any need for wiring a locality for connectivity thereby improving network cost, aesthetics, and "where" networks can exist-it also has its limitations. Radio waves can travel in any direction, up or down and side to side, travel through walls, and can bounce off solid object and cause interference. These unforeseeable interference patterns can render the receiving of signals very difficult [13]. To help resolve these problems, wireless networks use Spread Spectrum communication schemes. Spread Spectrum provides a means of using noise-like carrier waves and expanding the information contained within a signal so that

it is spread over a larger bandwidth than the original signal [13]. There are two types of Spread Spectrum schemes-Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS)-and wireless technologies usually use one or a combination of these implementations.

In Frequency Hopping Spread Spectrum, the signal continually switches the frequency of transmission in a predetermined "random" pattern. The sender and the receiver agree upon this pseudorandom pattern and ensure they are in synch with one another as the information transmits. The FHSS technique helps reduce interference, since a specific frequency is used for a very short period of time, and also reduces eavesdropping from alien computers because the alien computer is not in synch with the frequency-hopping pattern.

In Direct Sequence Spread Spectrum, the digital data signal is inserted in a higher data rate chipping code according to a

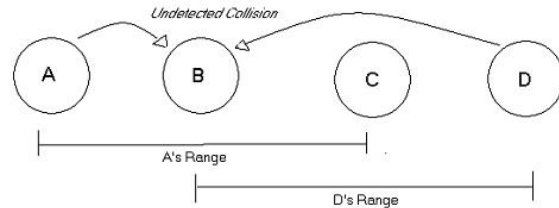


Figure 4: The Hidden Nodes Problem

predetermined spreading ratio [13]. The original bit sequence is incorporated into this predetermined chipping sequence, so that if interference occurs and the signal is compromised, the receiver has a chance of recovering the lost data based on the amount of chipping code it does receive. Thus, the longer the chipping the code, the higher chance of recovering bad data; but longer chipping codes requires a large use of bandwidth.

2.4 Unique WLAN Problems

Once there are solutions to how to physically transmit data, there are still many other important issues that need to be solved in order to make a wireless network successful. First

of all, there needs to be some mechanism to ensure that the data sent by the sender is appropriately received by the receiver. This problem is not unique to wireless networking, but wireless networks do introduce two new complications since all nodes are not always within the reach of each other—the hidden nodes and exposed node problems. We will first illustrate these two problems and then show how the 802.11 standard successfully solves them.

The hidden nodes problem is shown in Figure 4. In this example, the range of each node spans two nodes to its left and right. In the hidden nodes problem, both node A and node D may want to communicate with node B, but node A and D do not know about each other, since their respective signals cannot carry far enough. Thus, when both node A and D attempt to establish a connection with node B, they will collide, but neither A or D is aware of this collision. Their signals will unknowingly interfere around



Figure 5: The Exposed Nodes Problem

node B and very likely produce bad data for B to receive. Nodes A and D are said to be “hidden nodes” with respect to each other [15]. To solve this problem, Node B needs to possess some collision detection scheme so that only one node will be transmitting to it at a particular moment.

The exposed nodes problem is shown in Figure 5. Nodes A, C, and D are all in the range of B, and suppose B is sending to A. Node D is aware of this communication because it hears B’s transmission, and it does not want to start its own transmission because D’s signals may interfere with B’s signals. It would be a mistake, however, for D to conclude that it cannot transmit to any node in its range simply because it can

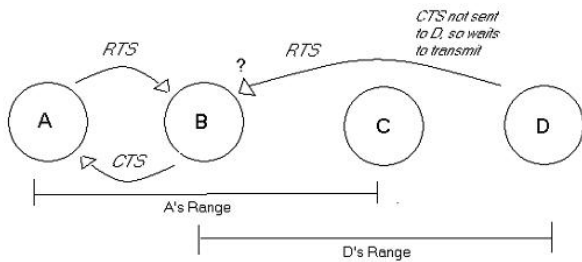


Figure 6: The Hidden Nodes Solution

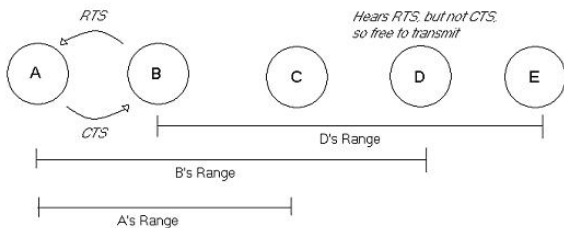


Figure 7: The Exposed Nodes Solution

hear B's transmission. In this example, D is free to transmit to any node without fear of interfering with B's signals because A is out of the range of D [15]. In other words, Node B should only block its transmission if it is in the range of both the sender and receiver of another transmission.

The 802.11 protocol addresses this problem with its Media Access Control (MAC) layer

combined with a Virtual Collision Detection (VCD) algorithm that keeps interference to a minimum. The fundamental idea behind the VCD algorithm is that the sender and receiver exchange control frames before the transmission of any data. In particular, the sender sends a Request to Send (RTS) specifying the length of transmission and the receiver thereby replies with a Clear to Send (CTS) acknowledgment (echoing the length field back to the sender). This exchange of control frames enables the sender and receiver to establish a "vacuumed" connection where all nearby nodes are cognoscente of this transmission. The Request to Send and Clear to Send algorithm solves the hidden node problem whereby any node that is close enough to the receiver to see the Clear to Send acknowledgment, knows that it cannot transmit to that node for the specified length of time. Similarly, VCD solves the exposed node problem whereby any node close enough to the sender to see the Request to Send but not the Clear to Send, knows

that it is not close enough to the receiver to interfere with the transmission, thus is free to transmit. When all the data is transmitted, the receiver sends an acknowledgment (ACK) back to the sender which releases all the nodes waiting to transmit. Finally, the VCD algorithm does not directly handle collisions when two nodes send a RTS to the same node, but when the two nodes do not receive a CTS after a specified amount of time, each node will wait a random time and send another RTS to the receiver [15]. The solution to the hidden node problem is shown in Figure 6. Figure 7 shows the solution for the exposed node problem.

2.5 Access Points

In a widespread public wireless network requires the use of "base stations" or Access Points that are connected to a distributed system, since equipment and other users are typically out of the range of a particular user. In addition to facilitating communication

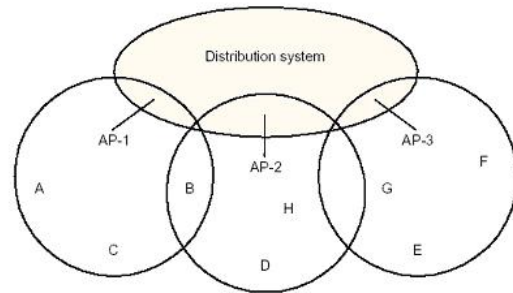


Figure 8: Example of Distributed System with Three Access Points [15]

between nodes that are not within range of each other, the distributed system is also responsible for maintaining a seamless wireless connection as the user roams throughout the range of the network. (This distributed system can be connected via an Ethernet connection or could be wireless itself.) If two nodes want to communicate with each other and they cannot actively "see" each other, then they can send the RTS to their specific Access Point, who in turn locates the end user via the distributed system, sends back a CTS, and allows the data to transmit over through this transmission "vacuum." The 802.11 protocol does not dictate how the

distributed system determines which AP to relay the data to, but it does specify how a node selects its AP ("scanning") and how it re-selects its AP (to maintain seamless connectivity) as it roams throughout the network.

The 802.11 technique for selecting an AP involves the following four steps [15]:

1. The node sends a Probe frame.
2. All APs within reach reply with a Probe Response frame.
3. The node selects one of the access points, and sends that AP an Association Request frame.
4. The AP replies with an Association Response frame.

The node sends the Probe frame when it connects to the wireless network, and also when it becomes dissatisfied with its current AP's strength (thereby, hoping to connect to a closer, more powerful AP.) Access Points themselves periodically send a Beacon frame

that contains its capabilities and nodes receiving this Beacon can switch their AP by sending back an Association Request.

2.6 Mobile IP

This connecting and re-connecting to access points and wireless networks introduces an important technical problem concerning how to effectively route packets to a wireless user's IP address. In a typical static network, one machine has a "fixed" IP address that is tied to the network-based on the IP address, the TCP/IP protocol finds this sub-network and ultimately the specific machine holding the specific IP address. When a mobile user is connecting and reconnecting into various networks, there is no stable network that the user's IP address is associated with, thus making packet routing impossible. Mobile IP, developed by a working group in the IETF, is a proposed solution to this problem. Mobile IP assigns a wireless user a fixed home address and a care-of address that

changes at each new point of attachment [16].

A wireless user has a static home address that is used to identify TCP connections. Located at this home address is a "home agent" node that is capable of rerouting the information to the wireless user. When a user connects to a "foreign" wireless network (a network not the user's home network), it sends a "care-of" IP address to its home agent. The home agent essentially adds this care-of-address address to its routing table. The home agent rearranges the IP information (setting the care-of-address address as the destination IP address) so that the information can be sent to the mobile node's current point of attachment. When the packet arrives at the care-of address, the reverse transformation is applied so that the packet once again appears to have the mobile node's home address as the destination IP address. When the packet arrives at the mobile node, addressed to the home address, it will be processed properly

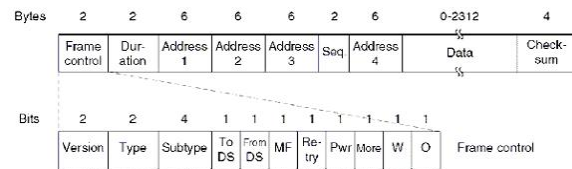


Figure 9: The 802.11 Frame [15]

by TCP or whatever higher level protocol logically receives it from the mobile node's IP processing layer [16].

2.7 802.11 Frame Format

The frame format for the 802.11 protocol contains all the information one would expect—a source and destination address, a duration slot to handle transmission, and a control field for handling collision detection along with other features. The peculiar thing about the 802.11 frame format is that it contains four, rather than, two addresses. How these addresses are interpreted depends on the settings of the ToDS and FromDS bits in the frame's Control field. These bits account for the possibility that the frame had to be for-

warded across the distribution system, which would mean that the original sender is not necessarily the same as the most recent transmitting node [15].

2.8 Other Issues

In addition to transmitting the information via radio waves, the range of a radio signal, which frequency to use, the size of data throughput, and speed of transmission are important factors in a wireless network. Typical Access Points can cover a range from 10 to 300 meters [13], but radio signals significantly fade the farther they travel, and even more so when they must propagate through walls and other boundaries. It is very crucial to a public wireless network designer to be aware of a locality's special conditions and to smartly plan the position, range power, and the number of access points. Secondly, most wireless radio frequencies operate on the unlicensed Industrial Scientific and Medical 2.4GHz to 2.483GHz band along with other

products such as cordless telephones, baby monitors [13]. As the number of wireless devices increases, this frequency range will become more and more crowded, and the chance of interference of competing devices on this frequency range will also increase. In regards to the speed of data transmission and the amount of bandwidth available, wireless networks can support speeds ranging from 1.6 Mbps to 11 Mbps. As wireless technology advances, this speed will increase-currently there are plans to support access speeds up to 50 Mbps and beyond [13].

3 Wireless Security

With packets of information flowing openly through the air for anybody to look at and difficulty with authentication for service providers, public wireless Internet creates many problems dealing with security. The two most important goals for public wireless security are privacy and authentication.

3.1 Privacy

The importance of privacy with the Internet general should be obvious. With increasing e-business, credit card transactions, and other sensitive communications being exchanged, the necessity of confidentiality can be seen. Wireless technology makes the issue of privacy becomes even more complicated than it already is because no longer is a user's connection completely encapsulated in a physical wire. Instead a user's traffic flows freely through the air between an access point and a mobile user. If the connection is not protected properly, it is open for anybody with the right knowledge and skill to snoop.

Public wireless Internet poses some unique privacy issues that would not occur under normal cable-tethered Internet service because of the openness of the connection. To counteract that, wireless traffic access point between a user and access point is

encrypted, under the 802.11b standard, by a protocol known as Wired Equivalent Privacy (WEP). However the WEP protocol is flawed and thus does not provide the security it promises. Also, the WEP protocol was designed to only protect from outside attacks, so all users who connect to a particular access point can decrypt and view any other user's traffic that goes through that point because they are "within" the system.

3.1.1 How Wired Equivalent Privacy Works

Before looking at the how the Wired Equivalent Privacy standard is flawed, it must first be explained. WEP uses the RC4 cryptographic stream cipher. How it works simply is that the data bits are exclusive-ORed (XORed) with a stream of bits, known as the keystream, generated by the RC4 encryption algorithm. Figure 10 demonstrates a stream cipher operation. To generate the keystream, a symmetric key is used, meaning that both the source and

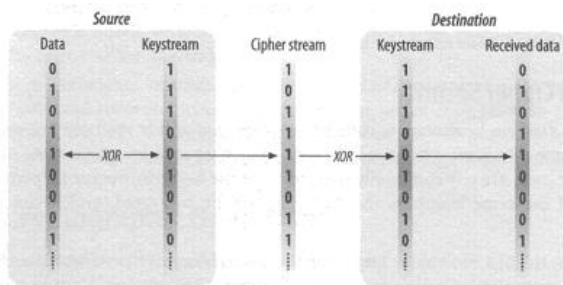


Figure 10: Stream Cipher Operation [17]

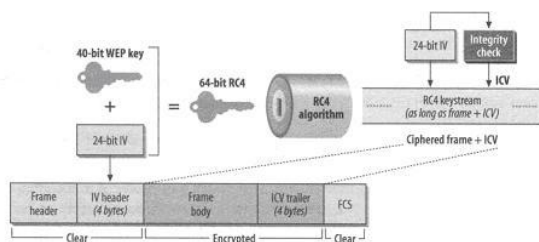


Figure 11: WEP Processing [17]

the destination need to know the key to generate the proper keystream.[17] The use of a symmetric key is one of the reasons that contributes to the WEP standard being flawed and will be discussed later.

Figure 11 shows the WEP cryptographic processing in detail. For integrity, the frame body is run through an algorithm that generates a hash called an integrity check



Figure 12: WEP Frame [17]

value (ICV). The ICV is used to protect the contents against being altered by making certain that the frame body has not changed while being sent through the network. The frame and ICV are then both encrypted so that it is not open for attackers to view or tamper with. The WEP standard is based on the use of a 40-bit secret, symmetric key. That secret key is then combined with a 24-bit initialization vector (IV) to create a 64-bit key for use with the RC4 encryption. The 64-bit key is then used to generate the keystream (which is equal to length of the frame body with the addition of the ICV).[17]

By looking at the WEP frame in Figure ??, it can be seen that four keys can be used between an access point and stations using it, as the key ID is two bits. The

use of the key ID allows for the receiver to know which key to use for decrypting the packet. The initialization vector (IV) is used to vary the keystreams to prevent cipher analysis, however there are faults within the IV architecture that pose security risks. [17]

3.1.2 Problems with WEP and Public Wireless Internet Access

Some of the security flaws touched on earlier are described in more detail in this section. The major problem, with respect to a public wireless Internet, is the issue of key management. Also problems arise with the sharing of WEP keys for a given access point and through keystream reuse.

Key Management: Noted cryptographer Bruce Schneier called key management the hardest part of cryptography [23]. This applies to WEP as one of its biggest problems, with respect to public access wireless, is with key management. There is no automated key management protocol within the standard,

meaning that the keys must be entered manually into each computer. This adversely affects hope for a secure public wireless Internet. Distributing the keys manually to each station would make the ubiquitous nature of it impossible. For secure access the mobile users and providers would have to communicate directly to swap the keys. That would create a large burden on the wireless provider, especially if she or he was simply publicly sharing their Internet with people through a user group such as NYC Wireless. The burden would most likely turn off many providers from providing secure access.

Mobile users that seek wireless roaming between access points, such as with mobile IPs, and have secure access would also be hindered with WEP. Having to manually obtain the keys and enter them makes smooth mobility between access points non-existent. Clearly, automated key distribution is needed for the ability to switch seamlessly between

access point networks. The most efficient way to distribute the keys under the WEP standard with public wireless Internet would be to publish them on the Web. But then anybody could find them and use them, there by taking away the security.

Key Sharing: However, even if WEP provided automated key distribution, public wireless networks would still have another security problem to tackle. This has to do with the fact that the same four WEP keys are shared with all users of an access point. It results in that everybody that is using the access point has the power to sniff the packets of everybody else using the same access point because they have the keys already. While on small networks where everybody is known (such as a family's or small company's) this may not be a big problem, but with public wireless Internet there is a major security risk. Due to the anonymity of the users at any given access point there can be no trust on the wireless network. On public networks

anybody could get secure access, obtain the secret keys, and then proceed to sniff all the traffic on it.

Keystream Reuse: Another problem with WEP that hurts the the potential for a secure public wireless network is keystream reuse caused by a flawed IV architecture and infrequent rekeying. With key stream reuse the stream cipher becomes vulnerable to analysis, thereby helping a snooper obtain information about messages (recall the use of XOR).

$$If C_1 = P_1 \oplus RC4(v, k) \quad (1)$$

$$and C_2 = P_2 \oplus RC4(v, k) \quad (2)$$

then

$$C_1 \oplus C_2 = (P_1 \oplus RC4(v, k)) \oplus (P_2 \oplus RC4(v, k)) \quad (3)$$

The above equations [18] simply mean that the keystream (RC4(v,k)) cancels out when the two ciphertexts (C1 and C2) are XORed, resulting in the XOR of the two plaintexts (P1 I P2). [18]

Of course for the above to work, it has to be known that a keystream is being reused. The WEP standard attempts to counteract the reuse of keystreams with the IV, as the keystream $RC4(v,k)$ are generated with both the secret key k and the public initialization vector v . The IV changes for every packet, thereby changing the keystream for each packet sent. The IV is public, as can be seen in Figures 11 and ?? , so that the receiver can use it. While the IV is public and available to snoopers, there is still the 40-bit secret key to maintain the security. [18]

Within the IV however lie the faults with WEP's keystream. Since the IV is public, keystream reuse can be detected, if the secret keys are changed rarely. Given that the IV is only 24 bits long, collisions can actually occur quite often, as there is only so much space allowed for differing the IV value. It is theoretically estimated that if an access point operates at 5 Mbps (less

than half the potential 11 Mbps transmission rate), the available IV space would be exhausted in less than half a day. On top of this, WEP has been poorly implemented by some manufacturers that make it even easier to detect keystream reuse through the IV. [18]

The best way to counteract the above attack is to frequently rekey and change the secret keys. However this would be extremely difficult for a public wireless access point to accomplish, given the manual key distribution. When to change the keys would be difficult to deal with. For companies they could simply change them when an employee leaves, however with public wireless, there are random users using the service, and it would be impossible to keep track of when a user leaves and rekey, making sure to distribute it to all the current users.

3.2 Authentication

Along with privacy, authentication is an important aspect of public wireless security. Since many public access points, such as those of NYC Wireless, allow random anonymous users they potentially put themselves in liability for illegal activity done by the users. The precedence holding public access points accountable for copyright infringement by its users is set by the case *ALS Scan Inc v. RemarQ Communities Inc.*

The ISP RemarQ Communities was warned by ALS Scan Inc that they provided access to two newsgroups that contained postings that infringed on ALS Scan's copyrights. RemarQ claimed to have safe harbor under the Digital Millennium Copyright Act (DMCA). However, RemarQ was given notice of copyright infringement and lost its safe harbor and as a result they were liable [22].

The fate of RemarQ could easily apply to public wireless providers. The DMCA defines a "service provider" as [22]:

an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, or material the user's choosing, without modification of the content of the material as sent or received.

With that definition public access points most certainly fall under the same provisions as RemarQ set by the act. Also, anonymity provides a motivation for mobile users to engage in illegal activity over a public wireless network. Then given that many public access points are merely regular Internet users sharing their broadband connections they could be at risk and would stop making their access point public at the mere threat of legal action. There is no reason that a body such as the Recording Industry Association of America would not send cease and desist orders to wireless providers of such user groups as NYC Wireless who would not have

the resources to fight a legal battle. It is important to point out though that there have been no cases of this occurring, according to NYC Wireless Networking Developer Terry Schmidt. Nevertheless, it is in the opinion of the authors that authentication is necessary so that the specific users can be held liable for illegal activity, and not the providers.

Recently, some have also been referring to Wi-Fi as a terrorist tool. The idea has been perpetrated because of the insecurity of most public wireless networks [20]. While the idea is being discussed within the Homeland Security cabinet, it is important to point out the necessity here for authentication. With authentication, public wireless providers could regulate and authorize who is allowed on the network and what they are allowed to do.

3.2.1 Authenticating with Public Wireless Internet

With the 802.11b standard, authentication is merely done by MAC addresses, which is unique for each network card. An access point can change the settings of her or his access point and only allow certain MAC addresses to use it through manual entry.[17]

By using MAC address the standard is inflexible, as authorized users would not be able to use different computers (with different network cards) without making sure that every access point is updated to allow access for the new MAC addresses. Also, for free public access wireless, the standard would not work simply because an access point would have to allow all MAC addresses to allow all users access.

To deal with the issue of authentication the IETF has been developing the Extensible Authentication Protocol (EAP), which is known as the 802.1x specification. EAP

applies to networking in general and is therefore applicable to wireless. The main idea behind the protocol is that it is flexible so that different authentication methods can be applied, such as Kerberos, RADIUS, and digital certificates.[17] Most important is that an authentication server would be required. For companies providing pay-for public access this might not be a problem, as it is in their interest to have authentication servers to control access for paying customers.

Authentication server problems arise with the free wireless providers who potentially do not have the resources to have authentication servers and software. Also, the simple process of merely searching for an access point and connecting would be gone, as users would have to register with the access point network so the authentication servers could grant access.

Registering with a single free network

would not be inconvenient if a user only connected to that single network. Problems arise with wireless roaming on free networks. The ubiquity of seamless roaming would be hindered greatly. With EAP there are different authentication mechanisms and no central authentication server. Different free wireless providers will have their own servers with their protocols. Roaming between different networks would be difficult, as a mobile user would have to make sure he or she could be authenticated with each service and then re-authenticate. It seems that the best way to allow an authenticated ubiquitous wireless Internet would be through a centralized public-key infrastructure or possibly even through some kind of a decentralized authentication system, but both of these possibilities are very difficult to organize and implement and thus are not viable in the near future.

3.3 VPN: A Possible Solution

It is clear that the current standards for wireless security are not as secure or simple as they seem, potentially hurting the development of public access wireless Internet. Key management issues and poor implementation makes WEP insecure. Also, authentication for a ubiquitous free wireless Internet looks to be very difficult. Currently the best form of security for wireless networking is Virtual Private Networking (VPN).

Virtual private networking has been used in the past to secure remote access networking and can be easily applied to wireless networking. There are many different VPNs, but the most common is Internet Protocol Security (IPSec). VPN provides more secure encryption than WEP to protect privacy and can supports different authentication methods. [21]

However, VPN is not a perfect solution

for public access wireless. It takes a certain level of computer savvy to configure virtual private networking and thus could prevent many non-tech mobile users from using it. The wireless provider BOINGO does attempt to ease this by providing software to make VPN easier to configure and use [19], but they can afford to create the software, as they are a pay service. Free public access providers might not have the money. They could rely on open source software, but that type of software has not been known for being the very user friendly. Also, with VPN, additional servers are still required for authenticating, which, as discussed earlier, is potential obstruction for the development of free providers.

4 Conclusion

Wireless networks are rapidly producing a ubiquitous Internet. Although they have entered the main stream, there are still numerous technical and legal concerns left unre-

solved. Given their salutary benefits to society, it is important that wireless networks are free to develop uninhibited. Compatibility between competing wireless protocols is paramount to ensure that the multitude of wireless devices can effectively communicate. Furthermore, extensive security measures must be developed so that wireless networks attain the same level of security as their wired counterparts.

References

- [1] <http://online.wsj.com/article/0,,SB1039109828499400393,00.html?mod=home%5Fwhats%5Fnews%5Fus>
- [2] <http://www.nycwireless.net/>
- [3] http://online.wsj.com/article/0,,SB1038529896943393228,00.html?mod=todays_us_pageone_hs
- [4] <http://www.bawug.org/>
- [5] <http://www.seattlewireless.net/>
- [6] <http://news.com.com/2100-1033-918439.html>
- [7] <http://www.oit.duke.edu/access/wireless/>
- [8] <http://www.newswise.com/articles/2001/1/WIRELESS.UNC.html>
- [9] http://www.wired.com/wired/archive/10.10/dartmouth_pr.html
- [10] http://www.eff.org/Infra/Wireless_cellular_radio/wireless_friendly_isp_list.html
- [11] <http://online.wsj.com/article/0,,SB1038529896943393228,00.html?mod=home%5Fpage%5Fone%5Fus>
- [12] <http://www.starbucks.com/retail/wireless.asp>
- [13] Barnes, C., et al. *Hack Proofing Your Wireless Network*. Syngress Publishing, Inc., 2002.
- [14] textsIEEE 802.11 Standard Tutorial. Online. November 2001. <http://www.wave-report.com/tutorials/ieee80211.htm>.
- [15] Davie, Bruce S., et al. *Computer Networks: A Systems Approach*. Morgan Kaufmann Publishers, 1999.
- [16] Perkins, Charles E. *Mobile Networking Through Mobile*. Online. 9 Dec. 2002. <http://www.computer.org/internet/v2n1/perkins.htm>.
- [17] Gast, Matthew S. *802.11 Wireless Networks: The Definitive Guide*. O'Reilly and Associates, Inc.: Sebastopol, CA. 2002.

- [18] Borisov, Nikita, Ian Goldberg, and David Wagner. *Intercepting Mobile Communications: The Insecurity of 802.11*. University of California – Berkeley. Online. [⟨http://www.drizzle.com/~bobba/IEEE/wep-draft.zip⟩](http://www.drizzle.com/~bobba/IEEE/wep-draft.zip).
- [19] Koerner, Brendan I. "Sky Dayton's Long Road to Internet Nirvana." *Wired*. Online. October 2002. [⟨http://www.wired.com/wired/archive/10.10/boingo-pr.html⟩](http://www.wired.com/wired/archive/10.10/boingo-pr.html).
- [20] Boutin, Paul. "Feds Label Wi-Fi a Terrorist Tool." *Wired News*. Online. 10 December 2002. [⟨http://www.wired.com/news/wireless/0,1382,56742,00.html⟩](http://www.wired.com/news/wireless/0,1382,56742,00.html).
- [21] "Wireless Security and VPN." *Intel Coporation*. Online. 2001. [⟨http://www.intel.com/ebusiness/pdf/prod/related_mobile/wp0230011.pdf⟩](http://www.intel.com/ebusiness/pdf/prod/related_mobile/wp0230011.pdf).
- [22] Wernick, Alan S. "In Focus: Intellectual Property." *The National Law Journal*. New York Law Publishing Company: New York. 14 May 2001. LexisNexis.
- [23] Schneier, Bruce. *Applied Cryptography*. John Wiley & Sons. 1995.