



802.11 Wireless Networks

By Jason G. Andress

Introduction

The 802.11 IEEE standard defines wireless networking over radio on the 2.4 and 5GHz frequency bands. Wireless networking is currently in widespread use, and the wireless industry enjoys a very high rate of growth. Wireless technology can be found in a staggering number of locations, both industrial and residential, with more appearing all the time. Even McDonalds offers 'McDWireless' with your McNuggets¹.

Several properties motivate the popularity of wireless devices:

- ▲ Trivial deployment; no wires necessary for users
- ▲ Low cost of wireless devices
- ▲ Growing demand for wireless connectivity
- ▲ Adequate and available communication bandwidth

Wireless networking's popularity can be seen in the sales figures for wireless devices. Sales in 2004 for 802.11 wireless networking equipment grew 26 percent, with a total revenue of 2.3 billion dollars for the top six market leaders². Since older devices are not becoming obsolete as quickly as newer equipment is shipping, wireless connectivity is expanding dramatically. The advent of practical Voice-over-IP (VoIP) devices might fuel an even greater appetite for wireless devices.

The 802.11 Standard

The 802.11 standard encompasses a wide range of protocols, frequency bands, and capabilities. These different implementations are denoted by a lower case letter suffix to 802.11. In common use are:

- ▲ 802.11a - operates at up to 54Mbps on 5GHz and was the first widely used revision
- ▲ 802.11b - operates at up to 11Mbps on 2.4GHz and is currently the most widely used revision
- ▲ 802.11g - operates at up to 54Mbps on 2.4GHz and is the most recent revision

The listed 'transmission rates' are not bit rates measuring end-to-end, but rather the peak bit rate of these transmissions. Measured throughput often falls to 50-60% of these rates.

The more recent list of proposed 802.11 versions now stretches to 802.11w, with a,b,g, and i being the only revisions to have been ratified by the IEEE at this time. Only 802.11b and g are in widespread use currently; some newer, more expensive hardware supports 802.11i, and 802.11a has

fallen into disuse to a large extent. The next revision in line is 802.11n, which is in the ratification process at the time of this writing.

802.11 Security

In the world of computer networking, maintaining a secure network environment is critical. Companies and individuals devote significant time and resources to ensure that their borders are solid, and many people base their careers on supporting these endeavors.

One technology that has gained wide attention in the world of computer security is wireless networking. Securing wireless networks is critical because they transcend the normal physical boundaries of the wired network and thus present a new security paradigm. Many of the measures in place for securing physical access for wired networks simply do not apply to wireless networks. A single rogue access point can completely bypass complicated and expensive firewall equipment and intrusion detection systems, and both allow and enable the attacker direct access to the network.

Encryption techniques are the primary protection mechanism for wireless networks. Several types of encryption can be found in consumer-grade wireless devices, most commonly: WEP, WPA, and WPA2.

The older and much less secure Wired Equivalency Protocol (WEP) ultimately proved to have fundamental weaknesses in its RC4-based encryption scheme that enabled it to be easily cracked. Most 802.11a, b, and g devices are capable of using WEP, but it is commonly considered to be inferior security.

A newer protocol, Wi-Fi Protected Access (WPA), replaced WEP. While generally considered to be fairly secure, WPA was a stopgap measure created by the Wi-Fi Alliance in order to solve the immediate security issues until 802.11i could be ratified. WPA still used RC4, but had been modified to remove the flaws that WEP contained.

Encryption under the 802.11i revision, referred to as WPA2, switched from the RC4 stream cipher to the Advanced Encryption Standard (AES) block cipher, a considerably more secure method of encryption.

802.11i also makes use of 802.1X, which allows the use of the Extensible Authentication Protocol (EAP) and authentication servers such as Remote Authentication Dial In User Service (RADIUS). In simple terms, this allows something like the following:

1. The wireless client (called the supplicant) sends a request to be authenticated
2. The wireless access point (called the authenticator) receives the request and passes it to the authentication server, typically a RADIUS server

3. The authentication server sends a challenge back to the authenticator, which reformats it and passes it to the supplicant
4. The supplicant responds back to the authenticator with the answer to the challenge, which the authenticator passes to the authentication server
5. If the supplicant answered the challenge correctly, the authentication server sends a success message to the authenticator, which passes the message on to the supplicant
6. The authenticator now allows the supplicant access to the network, based on the instructions that the authentication server gives it

In addition to using encryption for signal security, most wireless devices are capable of additional measures, such as disabling broadcast of the Service Set Identifier (SSID) or using MAC address filtering. Disabling the SSID broadcast prevents the device from sending beacons over the network that announce its presence. MAC address filtering allows the device to permit or deny access based on a list of specific MAC addresses. These additional measures do not constitute strong security by themselves, but can be used to strengthen a layered security approach.

802.11 Weaknesses

802.11 wireless networks are subject to not only the set of attacks to which wired devices are subjected, but also to attacks specifically directed at wireless communications. Most of these wireless-specific problems revolve around the fact that physical access to the wireless network cannot be limited. The signal can be encrypted and steps taken to limit the usefulness of captured data, but it is still accessible to anyone within range. Some of the more common attacks include attacks on encryption, spoofing, denial of service attacks, software exploits, and radio frequency jamming.

Encryption

Attacks on the encryption used by 802.11 wireless networks are difficult to defend against. With a weaker encryption method, such as WEP, an attacker can capture data for a period of time, then attempt to crack the encryption at their leisure. This is possible because WEP uses a fixed secret key and sometimes uses weak initialization vectors to encrypt packets. When enough packets are present for analysis, the information from the packets that were encrypted with weak initialization vectors can be used to recover the secret key³. Several tools exist that will automate this process, such as AirSnort⁴ and WEPCrack⁵.

WPA and WPA2 are much more secure against the type of attack that is used to compromise WEP. WPA uses the Temporal Key Integrity protocol (TKIP) to change the encryption key every 10,000 packets in order to mitigate this vulnerability. WPA2 uses stronger encryption, as well as a four-way handshake using temporal keys in order to make this sort of attack very difficult.

Spoofing

Some institutions restrict which physical MAC addresses can connect to their wireless networks. The 'MAC spoofing' attack requires knowledge of a legal MAC address (gained by sniffing the wireless network) and subsequent spoofing of that address by the attacker (Tech Faq, 2004). MAC address filtering should never be considered a security measure in its own right, only another layer to add.

A somewhat more complex and thus less common attack is Wireless Access Point spoofing. This attack involves setting up a rogue wireless

access point which is configured with the same SSID as the legitimate access point. The attacker then sends management frames to the wireless clients that force them to disconnect from the legitimate access point and reconnect to the spoofed access point⁶. This attack method can be used to collect information such as the secret key or pass phrase that is in use⁷.

A management frame spoofing attack can take a variety of forms. Tools such as wlan_jack⁸ and omerta⁹ can be used to send a flood of deauthentication and disassociation frames or altered authentication request frames out to be picked up by the wireless device. Sending mangled management frames will generally completely disrupt the traffic on a wireless network. Frames can also be deliberately formatted to cause the wireless device to generate a larger amount of traffic than normal. This can be used as a denial of service attack or can be used as a precursor to other attacks that require a lot of data to work with.

DOS/DDOS

Denial of Service and Distributed Denial of Service attacks, which are an unfortunately common attack on wired networks, are found on wireless networks as well, and are generally harder to combat in the wireless environment. These attacks include RF jamming, spoofing of management frames, overflowing the buffers on the wireless device, and deliberately setting off the collision avoidance mechanism of the wireless networking device.

Jamming

Jamming is very difficult to prevent from happening or to stop once it has begun. The only real solution is to shut down the source of the interference. Jamming can be a malicious attack or might stem from another electronic device on a similar frequency and is generally very difficult and expensive to locate the source of. This type attack can be accomplished with a wireless NIC and software such as FakeAP¹⁰, Void11, or File2Air¹¹, or with something as simple as a cordless phone.

One particularly novel form of attack was discovered by graduate students at an Australian university who were researching methods for preventing or mitigating wireless attacks¹². A wireless device can be programmed to interfere with the Carrier Sense Multiple Access with Collision Avoidance, or CSMA/CA, mechanism that is used to prevent collision on wireless networks. This attack prevents wireless devices from properly using the Clear Channel Assessment function, which has the effect of keeping the device from sending any data over the wireless network. This attack reportedly will disrupt any 802.11-based wireless networks within receiving range of the attacking device. Although this is a rather sophisticated attack, it still ultimately amounts to jamming.

Software Exploits

Wireless access points can be also attacked by overflowing the internal buffers used for access point authentication and association. Many access points do not implement any protection against buffer overflow attacks and will crash after a large amount of data is sent to them¹³. Attack tools such as Void11 and macfld.pl¹⁴ are available and capable of carrying out this sort of attack.

802.11n

802.11n is the next revision of the 802.11 standard in line to be ratified by the IEEE. Many companies in the wireless industry are taking a great interest in this technology. 802.11n will be a revision that is reflected in a hardware change, as opposed to 802.11i which was a software change,

meaning that a whole new set of equipment will be on the market. The 802.11n revision is intended to solve several problems:

- ▲ Interference from other wireless devices
- ▲ Short range
- ▲ Poor coverage
- ▲ Low speed

Revision	Over the Air (OTA) Estimates	Media Access Control (MAC), Service Access Point (MAC SAP) Estimates
802.11a	54Mbps	25Mbps
802.11b	11Mbps	5Mbps
802.11g	54Mbps	25Mbps (without 802.11b present)
802.11n	200+ Mbps	100Mbps

Figure 1¹⁴: 802.11 Transfer Rates

802.11n is intended to be interoperable with the four previously ratified revisions of 802.11, meaning that the security features of 802.11i will be included in this version of the standard. 802.11n will operate on both the 2.4 and 5GHz bands, allowing it to be backwards compatible with 802.11a, b, and g, a task which currently requires separate devices or devices with multiple radios. Both proposals also operate on the 20 and 40MHz bandwidths. Current technology uses solely the 20MHz bandwidth.

A feature of 802.11n that many will be happy to see is a different approach to the measurement of transfer rates. The transfer rate will now be measured at the MAC layer instead of at the physical layer, resulting in a considerably more accurate measurement. Measurement at the MAC layer gives a much clearer picture of the actual throughput of the devices, as can be seen in Figure 1.

As an excellent accompaniment to the new method of transfer-rate measurement is Multiple-input Multiple-output (MIMO)¹⁵. MIMO allows an increase in the physical transfer rate of wireless devices by using multiple antennas for both the transmitting and receiving ends. Multiple antennas provide the ability to process spatially different signals simultaneously, using spatially separated receive antennas. Multi-path signals are the reflected signals arriving at the receiver some time after the original or line of sight (LOS) signal has been received. Multi-path signals are typically perceived as interference that degrades the receiver's ability to process the signal correctly. MIMO allows the receiver to resolve multi-path signals, thus allowing the signal to be correctly processed.

MIMO also allows Spatial Division Multiplexing (SDM). SDM can spatially multiplex several independent data streams that are transferred within one spectral channel of bandwidth. SDM significantly increases throughput as the number of data streams is increased. In order for SDM to function, each data stream requires a separate pair of transmit and receive antennas at each end of the transmission.

The Proposals

Two main proposals are on the table for the technology that will run 802.11n, Task Group n Synchronization (TGn Sync)¹⁶ and World Wide Spectrum Efficiency (WWiSE)¹⁷. The TGn Sync proposal (backed by Intel, Agere, Atheros, Sony, and Philips, among others) claims to have a bandwidth cap around 630Mpps. The WWiSE proposal, (backed by Motorola, Nokia, Texas Instruments, Conexant, and Airgo, among others) claims to have a bandwidth cap around 540Mbps. The major differences between TGn Sync and WWiSE are in the implementation of the MAC and physical layers. TGn Sync has a more complex MAC that it says will allow for future expansion in a better fashion.

In March of 2005, the IEEE voted between these two proposals for the 802.11n draft standard. As a result of the vote, WWiSE was eliminated. After this vote, another vote was held to confirm TGn Sync, which did not receive enough votes (75%) to pass. A second confirmation vote was held

in May of 2005, with similar results. Currently both the WWiSE and TGnSync proposals are up for reconsideration.

The TGn Sync and WWiSE groups are reportedly discussing an arrangement that will merge the two disparate proposals into one and resubmit the unified proposal, hopefully gaining the needed votes to move forward. When contacted, one of the authors of the original two proposals declined to comment on the specifics of a combined proposal, and the other author could not be reached¹⁸.

The Market

Current bickering notwithstanding, the 802.11n proposal is expected to be ratified in late 2005 or early 2006. It is likely, considering previous releases of such technology, that equipment will start appearing shortly before the standard is actually ratified. With the release of 802.11g, several manufacturers were selling early versions of hardware and later shipping firmware releases to bring the devices up to standard. An interesting aspect of this particular update to wireless technology is that several manufacturers have adapted their current 802.11g product lines to use MIMO technology¹⁹. This enables an intermediate step of devices that are not actually 802.11n, but do enjoy some of its range and speed benefits.

The advances in technology may cause the market for 802.11n to expand somewhat over previous 802.11 revisions, as the new features will make it more useful and more secure than previous revisions. Although it's not yet on the market, the price range for this new technology will likely be in the same general range as new releases of previous revisions.

Conclusion

The next few years of wireless technology should be interesting to watch. Wireless networking continues to increase in popularity, as well as continuing to develop into a more mature technology. Some of the planned revisions of 802.11 may prove to be very interesting, such as 802.11s, a proposal which would implement wireless mesh networking. Wireless mesh networking allows each node of the network to essentially function as a repeater, therefore greatly expanding the potential range of wireless devices. Another potentially interesting wireless technology is 802.20, which proposes high-speed, long-range wireless networking, which will allow a more universal wireless network. 

Jason Andress works as a system administrator for Agilent Technologies. He has recently completed a master's degree in CS and will soon be starting work on a doctorate. He is also a recent Debian convert.

¹ McDonald's Corporation and Affiliates. (2005). McDonald's Wireless Connectivity. Retrieved May 10, 2005, from <http://www.mcdonalds.com/wireless.html>.

- ² Dell'Oro. (2005, March). Worldwide Wireless LAN Market Exceeds 26 Percent Revenue Growth in 2004 Retrieved April 25, 2005, from <http://www.delloro.com/news/2005/WL030105.shtml>.
- ³ Fluhrer, S., Mantin, I., Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. Retrieved April 20, 2005, from IEEE database.
- ⁴ AirSnort. (2004, Winter). AirSnort Homepage. Retrieved May 3, 2005, from <http://airsnort.shmoo.com/>.
- ⁵ Rager, A. (2004, Summer). An 802.11 key breaker. Retrieved April 18, 2005, from <http://wepcrack.sourceforge.net/>.
- ⁶ Yu-Xi, L., Schmoys, T., Levine, J., Owen, H. (2003). Wireless Intrusion Detection and Response. *Proceedings of the 2004 IEEE Workshop on Information Assurance*. Retrieved April 20, 2005, from IEEE database.
- ⁷ Hurley, C., Thornton, F., Puchol, M.(2004). *Wardriving Drive, Detect, Defend A Guide to Wireless Security*. Rockland, MA: Syngress Publishing Inc.
- ⁸ Beetle. (2004). Wi-Fi Dog of War Mini How-To. Retrieved April 20, 2005, from http://www.geekspeed.net/~beetle/download/wifi_dog.html.
- ⁹ Schiffman, M. (2003, June). 802.11 Deassociation Packet. Retrieved May 2, 2005, from <http://www.securityfocus.com/archive/89/326248>.
- ¹⁰ Black Alchemy Enterprises. (2001). fakeAP. Retrieved April 20, 2005, from <http://www.blackalchemy.to/project/fakeap/>.
- ¹¹ Wright, J. (2004). <http://home.jwu.edu/jwright>. Retrieved April 19, 2005, from <http://home.jwu.edu/jwright/>.
- ¹² AusCERT. (2004, May). Denial of Service Vulnerability in IEEE 802.11 Wireless Devices. Retrieved May 5, 2005, from <http://www.auscert.org.au/render.html?it=4091>.
- ¹³ Vladimirov, A., Gavrilenko, K., Mikhailovsky, A. (2004). *Wi-Foo The Secrets of Wireless Hacking*. Boston, MA: Pearson Education Inc.
- ¹⁴ Wilson, J. (2004). The Next Generation of Wireless LAN Emerges With 802.11n. *Technology@Intel Magazine*. Retrieved April 15, 2005, from <http://www.intel.com/technology/magazine/communications/wi08041.pdf>.
- ¹⁵ Ahlen, A., Lindskog, E., Sternad, M., Tidestav, C., Wennstrom, M. (2002). Research On Multi-Antenna Receivers and MIMO Systems in Digital Mobile Radio. Retrieved April 17, 2005, from <http://www.signal.uu.se/Research/rdiversity.html>.
- ¹⁶ Tgn Sync. (2005). Tgn Sync Proposal for 11n. Retrieved May 2, 2005, from <http://www.tgnsync.org/home>.
- ¹⁷ WwiSe. (2005). Welcome to WwiSe.org. Retrieved May 2, 2005, from <http://www.wwise.org/>.
- ¹⁸ Coffey, S., Mujtaba, S. (2005). Personal communication. May 3, 2005.
- ¹⁹ Netgear. (2005). RangeMax Wireless Router. Retrieved April 21, 2005, from <http://www.netgear.com/products/details/WPN824.php>.

