

# White Paper – Wireless Network Security

By Scott Akrie

## **Introduction**

One of the most frequently asked questions put to a wireless broadband service provider by their subscribers is, "what about security?" It is indeed wise for subscribers to be concerned about security, on any type of network. Disgruntled former employees, hackers, viruses, Internet-based attacks, and industrial espionage are an unfortunate fact of life in any form of networking today. This white paper addresses the similarities and differences between security on wire-line and wireless networks, threats to the security of any network, and those elements unique to wireless technology used by SkyRiver available to combat these potential threats.

## **Similarities and Differences Between Wire-Line and Wireless Networks**

Common questions from those considering broadband wireless service often revolve around security. While these concerns are sensible, valid and justified, it is ironic that users rarely ask these question with the same level of concern about their wire-line network services. The security of information on the wire is, perhaps incorrectly, assumed as a given. Many have images of data on a wireless network floating freely in the air waiting for someone with a scanner to capture it, and as data packets begin traveling through the air, a high degree of anxiety sets in. After all, it is reasoned, the wire-line network is secure and the data stays on the wire, only available to authorized users with physical connections to that wire.

A wireless network has all of the properties of a wire-line network (except, of course, the wire), and thus security measures taken to ensure the integrity and security of data in the wire-line network environment are applicable to wireless networks as well. The primary difference between a wire-line network and a wireless network is at the physical layer (wire versus airspace) and all other network strengths and weaknesses remain.

With the advent of wireless broadband service, wireless service providers and equipment manufacturers have included an additional set of unique security elements that are not available in the wire-line world. Based on these elements, the argument can easily be made that wireless networks are at least as secure as wire-line networks.

## **Threats to Network Security**

Any network, wireless or wire-line, is subject to substantial security risks and issues. These include:

- Threats to the physical security of a network
- Unauthorized access
- Privacy

**Physical Security.** Given the obvious reliance of wire-line networks on the wire, anyone gaining access to that wire can damage the network or compromise the integrity and security of information on it. Without the proper security measures in place, even registered users of the network may be able to access information that would otherwise be restricted. Disgruntled current and ex-employees have been known to read, distribute, and even alter valuable company data files. Network traffic can be intercepted and decoded with commonly available software tools once one has physical access to the network cabling. In a wire-line network including cable systems, countless cases have been documented of wiretapping, hacking by authorized users and even people down the street hacking into their neighbor's computers.

Subscribers, regardless of whether or not they have wireless segments on their networks, need to have the appropriate security products for their environments, the proper security levels set for their users, and an on-going process to audit the effectiveness of security policies and procedures. Physical access to network wires needs to be protected. Unfortunately, the vast amount of wire inherent in most networks provides many points for unauthorized access.

**Unauthorized Access.** Another area of concern for security-conscious subscribers is the growing use of the Internet. Often, if users from inside can get out to the Internet, then users from outside can get into a network if proper precautions haven't been taken. And this applies not only to the Internet, but also to any remote network access capabilities that might be installed. Remote access products that allow traveling sales and marketing people to dial in for their email, remote offices connected via dial-up lines, intranets, and "extranets" that connect vendors and customers to a network can all leave the network vulnerable to hackers, viruses, and other intruders. Firewall products offering packet filtering, proxy servers, and user-to-session filtering add additional protection.

Many products are available to help subscribers secure their networks from the above threats. User authentication and authorization is provided by most network operating systems, and can be enhanced by adding third-party products.

**Privacy.** Perhaps the most difficult threat to detect is someone just looking at (and likely copying) raw data on the network. Wire-line networks are particularly vulnerable to eavesdropping. Most Ethernet adapters on the market today offer a "promiscuous mode" that, with off-the-shelf software, enables them to capture every packet on the network. Most network administrators have some kind of "packet sniffer" and/or network traffic analyzer for trouble-shooting the network. Inexpensive and readily available hardware and software let anyone with physical access to the network to read, capture, and display any type of packet data on the net.

While data encryption is the only line of defense against this kind of threat unfortunately, no wireline network service provider incorporates this technology as even an option that subscribers could use with their product.

## Security on SkyRiver's Wireless Network

We can see clearly that data security considerations impact the entire network architecture. And while these data security considerations apply equally to wireless networks, the technology used in the physical layer (airspace) of wireless networks actually increases overall network security, as follows:

**Spread Spectrum Technology.** SkyRiver's wireless networks use a form of spread-spectrum radio transmission technique. Spread spectrum technology was first introduced about 50 years ago by the military with the objective of improving both message integrity and security. Spread-spectrum systems are designed to be resistant to noise, interference, jamming, and unauthorized detection.

Spread spectrum communications is a means of transmitting a signal over a much wider frequency bandwidth than the minimum bandwidth normally required to transmit the information. The minimum is for the spread spectrum to have a bandwidth of at least 10 times the information bandwidth.

A typical radio signal contains both the data itself (which is the useful content) and a carrier frequency, which is modulated or blended with the data signal in order to "carry" the transmission across the operating range of the transmitter.

In SkyRiver's Direct Sequence Spread Spectrum (DSSS) transmissions, another element is introduced called a pseudo-noise (PN) code sequence. This is a binary – and hence digital – code sequence which, when modulated with the carrier frequency and original content, causes the resultant signal to spread across a much wider frequency spectrum, whereas the original radio signal would have occupied only a specific radio frequency. This has the resultant effect of dissipating the signal intensity over a broad range of frequencies, thus shrouding the transmitted signal, and making it indistinguishable from random white noise.

At the receiver end, in a process known as "correlation", a similar pseudo-noise code sequence matching exactly the one used by the transmitter is generated in order to "decode" the transmission by reconstituting the spread spectrum signal into intelligible information again. Naturally, without this code sequence, the spread spectrum signal is useless.

Therein lies the security-enhancing feature of DSSS transmissions, which explains why there is military interest in the technology. Because DSSS transmissions are harder to detect, there is a lower probability of interception. Because it does not occupy specific radio frequencies, it is harder to jam. And because it employs binary code sequences to "encrypt" the transmitted data, it makes it hard for unauthorized parties to "listen in", or to spoof or imitate network members.

Finally, SkyRiver's DSSS equipment incorporates the use of optional encryption. The IEEE 802.11 standard, under which SkyRiver operates, includes a security technique

known as "wire-line equivalent privacy" (WEP), which is based on the use of 64-bit keys and the popular RC4 encryption algorithm. Users without knowledge of the current key (password) will find themselves excluded from network traffic. Encryption, as noted above, is always advisable on any network, and is certainly easier to implement in wireless networks than in their wire-line counterparts. In addition to WEP, SkyRiver has the ability to support DES, IDEA and Blowfish as well as a proprietary version of encryption.

**Station Authentication.** SkyRiver's wireless network like most wireless networks, has the ability, through an authentication management function, to specifically authorize or exclude individual wireless stations. Thus an individual wireless user can be included in a network, or, at any time, locked out. Stations also need to know a wide variety of information, including radio domains, channels (specific frequencies) as well as IP addresses and subnets in order to access the network. Thus unauthorized network access becomes very difficult even for hackers who possess the equipment to attack the SkyRiver network.

**Physical & Network Security.** SkyRiver's network elements are in secure locations with environmental controls (including but not limited to remotely monitored intrusion alarms). These equipment rooms require specific authorization for access. Moreover, since the access points used in wireless network function as routers, individual wireless subscribers are isolated from the majority of network traffic. Network subscribers are unable to gain IP access to any network elements again limiting the possibility of network penetration or access to raw network packets.

**VPN.** It is a commonly accepted fact that Internet technologies have changed the way that companies disseminate information to their customers, partners, employees, and suppliers. Initially, companies were conservative with the information they published on the Internet – product information, product availability and other less business critical items. More recently, using the Internet as a means of providing more cost effective access to business critical information such as order status, inventory levels, or even financial information has gained wider acceptance through Virtual Private Networks or VPNs. A Virtual Private Network is a business solution that provides secure, private connections to network applications using a public or "unsecured" medium such as the Internet. With a VPN deployed across the Internet, virtual private connections can be established from almost anywhere in the world.

While subscribers currently have the capability to implement VPNs on their network through external CPE, SkyRiver will soon have the ability to offer an integral VPN option in its network.

**Adaptive Polling.** SkyRiver overcomes many of the problems inherent in wireless networks by centralizing control of the wireless network at the SkyRiver Base Station. The SkyRiver Base Station uses a highly optimized polling technique to tell remote wireless stations when they can transmit.

First of all, SkyRiver polling is adaptive. Each station's polling interval is determined by a number of independent factors, including the remote station's recent usage history. The total number of currently connected systems (among other variables) is used to determine maximum and minimum polling intervals.

Second, SkyRiver polling is dynamic. As remote stations transmit less frequently (i.e. they do not have a packet to transmit when polled), they are polled less often. For example: a station, which has been dormant for several minutes, may not be polled for an extended period of time. Stations that have data ready to transmit when polled are polled more often. This enables SkyRiver to make optimum use of the wireless bandwidth, while still maintaining a high level of "fairness" between wireless clients.

To avoid problems associated with pure polling schemes, SkyRiver also employs a "free for all" period to enable stations that have data available but are low in the polling queue to transmit without much delay. The "free for all" period allows a station that may not have transmitted for a long period of time to begin transmitting once again and move to a higher priority in the polling scheme.

The determination of polling intervals based on a complex combination of factors is finely tuned and the result of years of research into wireless performance in production environments. SkyRiver polling and the associated "free for all" period, combined with super-packet aggregation, allow wireless networks running SkyRiver to perform at the highest rate possible.

## **Conclusion**

The diligent management of security is essential to the operation of networks, whether they have wireless first mile or not. It's important to point out here that absolute security is an abstract, theoretical concept - it does not exist anywhere. Any network, wireless or wireline, is vulnerable if precautions are not taken or if someone is motivated enough and has enough money. No one wants to risk having the network data exposed to the casual observer or open to malicious mischief. Regardless of whether the network is wire-line or wireless, steps can and should always be taken to preserve network security and integrity.

It should be clear from the discussion above that wireless networks can take advantage of all of the security measures available on wire-line networks, and then add additional security features not available in the wire-line world. As a result, wireless networks can be as secure, and in fact more secure, than their wire-line counterparts.