

# **ProSoft Technology**

**Product Development Group**

Technical White Paper

## **Wireless Security on the Plant Floor**

November 02, 2007



## Your Feedback Please

We always want you to feel that you made the right decision to use our products. If you have suggestions, comments, compliments or complaints about the product, documentation or support, please write or call us.

### **ProSoft Technology**

1675 Chester Avenue, Fourth Floor

Bakersfield, CA 93301

+1 (661) 716-5100

+1 (661) 716-5101 (Fax)

<http://www.prosoft-technology.com>

Copyright © ProSoft Technology, Inc. 2000 - 2007. All Rights Reserved.

ProSoft Technology Wireless Security on the Plant Floor

November 02, 2007

ProSoft Technology®, ProLinX®, inRAX®, ProTalk® and RadioLinX® are Registered Trademarks of ProSoft Technology, Inc.

# Contents

Your Feedback Please .....	2
<b>1 WIRELESS SECURITY ON THE PLANT FLOOR.....</b>	<b>5</b>
1.1 Authentication: Open and Shared .....	6
1.2 Authorization: MAC Layer .....	6
1.3 What are the top seven wireless security problems confronting corporate LANs and industrial automation applications? .....	7
1.3.1 Area A .....	7
1.3.2 Area B .....	12
1.4 Additional wireless security guidelines to follow.....	13
1.5 Define your wireless network .....	14
1.5.1 Is the network Point-to-Point, Broadcast, Point-to-Multipoint, ad hoc (Figure G) or infrastructure (Figure F)?.....	14
1.6 Will I use open or proprietary standards? .....	15
1.6.1 "The RadioLinx RLX-FH radio has been designed to provide customers with confidence of a secure network.".....	16
1.7 What type of data will be transmitted and what type of protocols will I use?.....	17
1.8 Will I need corporate LAN access to sensitive data or simple device to device communication? .....	17
1.9 Will I use Ad hoc (peer-to-peer) or Infrastructure (access point) type network? .....	18
1.10 Do I need open industry wireless standards? .....	18
1.11 What application layer protocols will be used in transmission? .....	19
1.12 Comments from AirSnort web site .....	19
<b>2 FHSS AND DSSS PRIMER .....</b>	<b>21</b>
2.1 FHSS .....	21
2.2 DSSS .....	22
<b>3 REFERENCES.....</b>	<b>23</b>
3.1 Focus of this paper .....	23
3.2 Seven Security Problems of 802.11.....	23
3.3 Network Analyzers.....	24
3.4 AirSnort home page.....	24
3.5 ARE WIRELESS LANS READY FOR PRIME TIME? .....	24
3.6 NetStumbler.....	24
3.7 FTP, HTTP, POP3, Telnet .....	24
3.8 Types of Spread Spectrum .....	25
3.9 VPN and WEP .....	25
3.10 Hotspots.....	25
<b>INDEX.....</b>	<b>27</b>



# 1 Wireless Security on the Plant Floor

## *In This Chapter*

- Authentication: Open and Shared ..... 6
- Authorization: MAC Layer ..... 6
- What are the top seven wireless security problems confronting corporate LANs and industrial automation applications? ..... 7
- Additional wireless security guidelines to follow ..... 13
- Define your wireless network. .... 14
- Will I use open or proprietary standards?..... 15
- What type of data will be transmitted and what type of protocols will I use? ..... 17
- Will I need corporate LAN access to sensitive data or simple device to device communication? ..... 17
- Will I use Ad hoc (peer-to-peer) or Infrastructure (access point) type network? ..... 18
- Do I need open industry wireless standards? ..... 18
- What application layer protocols will be used in transmission?19
- Comments from AirSnort web site..... 19

Wireless networks can consist of many radio types based on the radio frequency and the modulation methods. Radios may be required to obtain a license to operate in an area or be part of the FCC approved unlicensed ISM band. Radio technologies in the ISM band are most commonly available supporting either "open" or proprietary standards. It is within the "open" standards such as 802.11 where most security issues are prevalent and primarily what this document will discuss.

Typical (page 25) 802.11a/b/g (DSSS) wireless LAN architectures consist of wireless clients, wireless access points, wired computers and industrial PLC processors. Wireless Clients typically are laptop computers but can also be industrial protocol/network gateways or PLC rack based modules. These wireless clients can communicate to other "wired" devices over LANs typically through a wireless access point (AP) in "Infrastructure" mode or communicate directly with each other peer-to-peer in "Ad hoc" mode. An access point provides coverage to a particular area known as a cell or "Hot-Spot" and is usually connected to the wired network. Some access points like the ProSoft Technology RLX-IH act as a

repeater and allow for a "wireless" backbone connecting several wireless hotspots (page 25).

The goal of wireless network implementations is to provide benefits identical to common wired networks and protect the network and resources from security related issues. Protecting the wired or wireless network may require a sequence of events to occur depending on whether the resources are part of the corporate LAN and/or industrial networks:

- **Authentication** is the verification process by which a user attempts to confirm identification with network resources to establish trust with the available resources.
- **Authorization** protects computer resources by only allowing those resources to be used by resource consumers that have been granted authority to use them. Provides
- **Encryption** is the process of obscuring information to make it unreadable without special knowledge.
- **Integrity** refers to the validity of data from malicious and accidental altering.

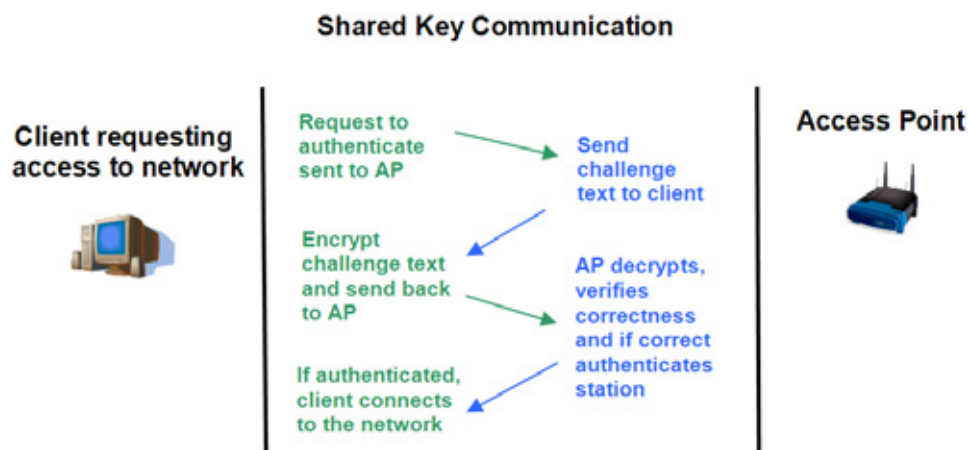
### 1.1 Authentication: Open and Shared

- Open system authentication: This is the default setting where any client can associate with the access point.
- Shared key authentication: Uses a shared secret key to authenticate the client to the AP. Uses a challenge-response protocol (Figure A)

### 1.2 Authorization: MAC Layer

- Can configure the AP to talk to specific MAC addresses
- Controls access to wired network not wireless

Figure A



A network missing any of these elements may expose known vulnerabilities to hackers and allow them to breach the confidentiality and integrity of the network resources.

The need for wireless security is obvious but what are the top most security areas of concern and are these security concerns really related to all wireless network applications – Corporate and Industrial (page 23)?

### 1.3 What are the top seven wireless security problems confronting corporate LANs and industrial automation applications?

Seven Security Problems of 802.11 (page 23)

- 1 Easy Access
- 2 Rogue Access points
- 3 Unauthorized use of service
- 4 Service and performance constraints
- 5 MAC spoofing and Session Hijacking
- 6 Traffic Analysis and Eavesdropping
- 7 Higher Level Attacks

Each of these concerns can be grouped into two specific areas.

- **Area A** – Security concerns relating to issues when accessing corporate LANS through authentication and authorization and
- **Area B** – Security concerns relating to issues about over-the-air wireless data packets.

Many industrial wireless applications are not subject to all of these security issues because not all wireless devices require connection to the corporate/industrial LAN and need only to be concerned with Area B security concerns. Grouping of these security concerns helps wireless site planners focus their attention to specific areas of security.

Each of the above seven concerns are grouped and defined below with suggestions to help guide the planner to avoid getting into trouble when setting up a wireless network.

#### 1.3.1 Area A

Security concerns relating to issues when accessing corporate LANs through authentication and authorization.

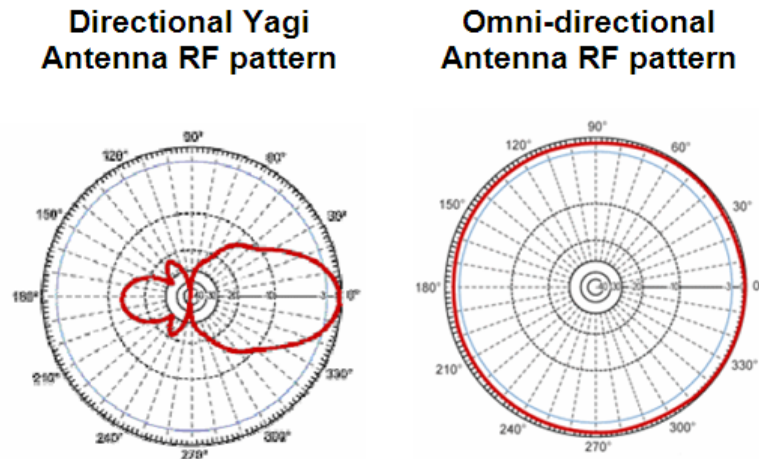
- 1 Easy Access
- 2 Rogue Access points
- 3 Unauthorized use of service
- 4 Service and performance constraints
- 5 MAC spoofing and Session Hijacking
- 6 Higher Level Attacks

Easy Access.

Finding wireless LANs is not difficult and with open wireless specification and protocols attackers can with the correct tools gain access to your network becoming authorized and authenticated to an internal LAN and then access corporate domain servers if left unprotected.

- Turn ON WEP or WPA securities features and use 128 bit encryption.
- Turn OFF beacon frames when using 802.11 type access point radios. If you want your radio network to be hidden from other 802.11 users, hide the network SSID by selecting not to broadcast the beacon frames. With the SSID hidden, your network does not show up when clients scan for an access point. You can still connect clients to the "hidden" network by typing the network SSID for client radios.
- Use low-gain directional and polarized antennas. Focus radio waves and energy to a confined area (Hotspot). See Figure B

Figure B



The objects above display radiation patterns for directional and omni-directional antennas. Access points using omni-directional antennas allowing anyone to connect throughout the building area. Directional antennas focus the radiation to only a small section of the building.

Rogue Access Points.

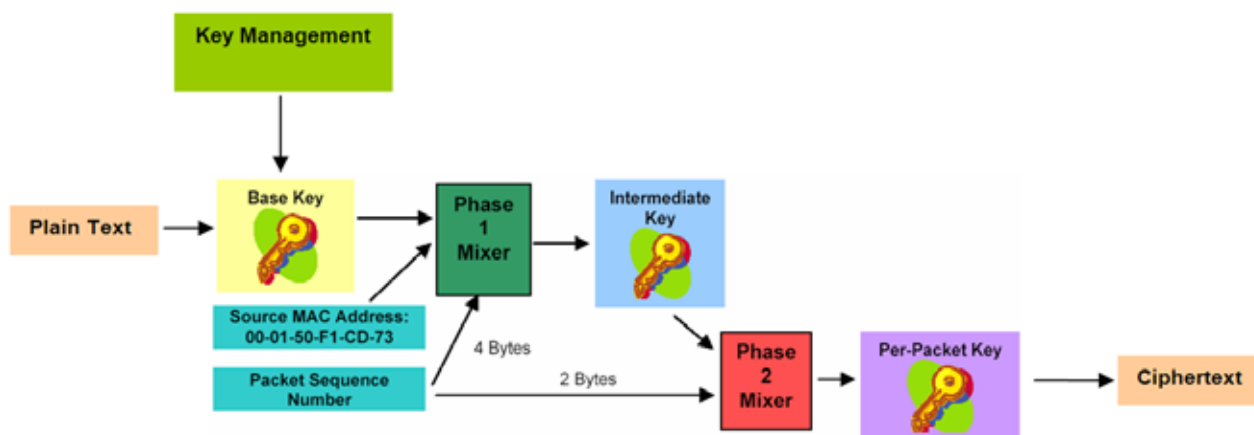
Developing administrative security policies and monitoring for "rogue" access points are fundamental to reduce the risk of certain LAN access violations.

- Place wireless access points outside of security perimeter such as firewalls and use VPN - IPsec protocol technology built-in to firewalls. (page 25)
- Learn and identify where unauthorized networks have been deployed and remove before attackers exploit them. ProSoft Technology's RLX-PC-IB laptop radio card and NetStumbler (page 24) can be used to locate wireless networks.

According to [AirSnort](#) (page 24) WEB site, AirSnort program requires approximately 5 to 10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second. WLAN vendors implemented a key management fix to make up for WEP's weaknesses. WEP key management prevents and confuses these programs from obtaining the key mathematically to "crack" the encryption key.

Figure C

## WPA (TKIP) Encryption Key Protection



TKIP provides three security improvements over standard WEP: fast-packet keying (key-hashing per packet), real message integrity checking (to prevent forgery) and dynamic key management (re-keying).

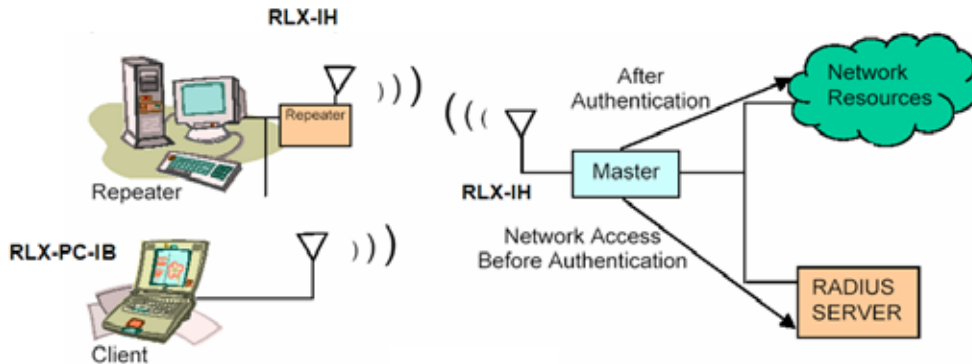
Unauthorized use of service.

The biggest defense against unauthorized use is to prevent unauthorized users from accessing the network. Use of strong, cryptographically protected authentication (ProSoft Technology's RLX-IH with TKIP encryption) where sensitive corporate LAN data is located and is a precondition for authorization - **Figure C**. VPN solutions deployed to protect traffic in transit across the radio link provide strong authentication (page 25).

- Use strong authentication schemes to prevent unauthorized network access. Install a RADIUS server for access point authentication. The 802.11i standard allows the use of a RADIUS (remote access dial-in server - **Figure D**) to manage encryption keys and control which radios are allowed to access the network. The radio first associates with the access point, and then is granted access only to the radius server. If the radio and server successfully authenticate each other, the radius server sends a master key to the access point, which negotiates a session key with the radio. After authentication, the radio is connected to the network.
- Also session hijacking can be prevented by using a strong cryptographic protocol such as IPSec. Analyzer's can determine what security level is in

use informing network administrators if the desired security protocols are in use.

Figure D



### Service and Performance Constraints.

With the proliferation of wireless products today wireless LANs can become crowded and overwhelmed with traffic. Wireless networks have limited transmission capacity. For example, 802.11b/g have bit rates of 11 and 54 Mbps respectively and the actual effective throughput amounts to about half of the nominal bit rate. With that in mind it can be imagined how local applications might flood a network with limited capacity or how an attacker could launch a denial of service attack.

- Perform regular audits of wireless network access equipment to ensure that strong authentication mechanisms are in use and that network devices are properly configured. If an unauthorized station is found connected to the network, a handheld receiver can be used to track down its physical location. Analyzers like the [AirMagnet](#) (page 24) can also be used to verify configuration of many access point parameters and raise alarms when access points expose security vulnerabilities

### MAC spoofing and Session Hijacking.

Attackers can use spoofed frames to redirect traffic and corrupt ARP tables. At a much simpler level, attackers can observe the MAC addresses of stations in use on the network and adopt those addresses for malicious transmissions. By requiring authenticating potential users, unauthorized users can be kept from accessing the network. Attackers can use spoofed frames in active attacks as well. Attackers can pretend to be an access point.

- Use MAC address filtering. Each radio has a MAC address that can be placed on a list. The access point will only communicate with radios on the list.
- Adopt Strong Protocols and use them. Until the ratification of 802.11i, MAC spoofing will be a threat. Using IPsec and TLS protocols for LAN access points are important to proving identity.

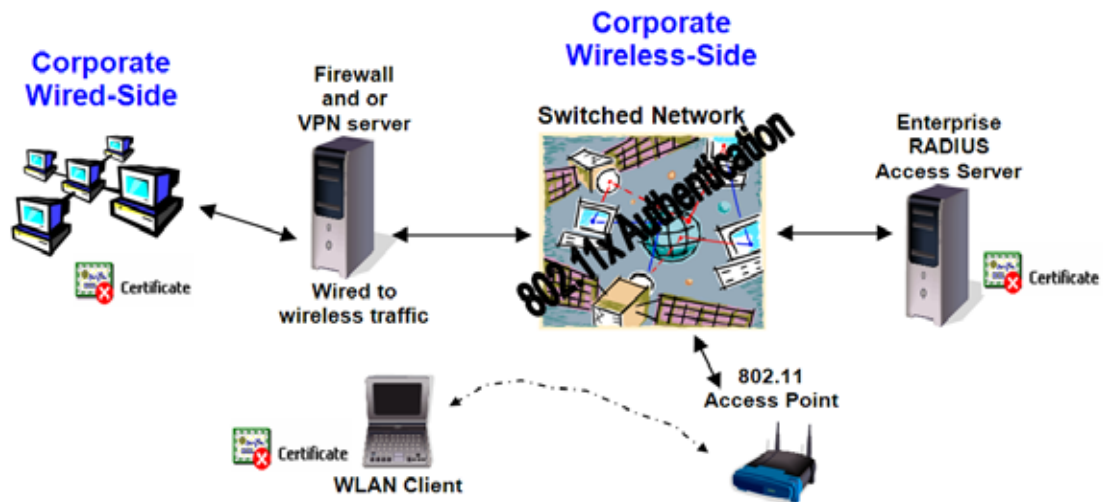
Higher Level Attacks.

Once an attacker gains access to a wireless network, it can serve as a launch point for attacks on other systems. Many networks have a hard outer shell composed of perimeter security devices that are carefully configured and meticulously monitored (Figure E). Inside the shell, though, is a soft, vulnerable center. Wireless LANs can be deployed quickly if they are directly connected to the vulnerable backbone, but that exposes the network to attack.

- Using non-open standard radio types such as 900 MHz and 2.4 GHz FHSS (Frequency Hopping Spread spectrum) radio transceivers offer a much higher degree of protection against would be intruders. These radio types typically use proprietary type binary protocols and the hopping sequence is unknown. ProSoft Technology offers several FHSS (page 25) type radios, such as RLX-FHS, RLX-FHE and RLX-FHES with serial and Ethernet based communications.

Figure E

Corporate LAN Diagram using 802.1x Authentication



The 802.1x standard is an authentication framework designed to provide controlled port access (and to deny access to the port when authentication fails) between wireless client devices, access points, and servers that use the Extensible Authentication Protocol (EAP) and a RADIUS server. 802.1x further enhances security by enabling mutual authentication: the access point can validate the client, and the client can determine whether the access point is legitimate.

Preinstalled Digital Certificates authenticate that their holders are who or what they claim to be. WPA (Wi-Fi for Protected Access) includes both 802.1x and TKIP.

### 1.3.2 Area B

Security concerns relating to issues about over-the-air wireless data packets.

#### Traffic Analysis and Eavesdropping.

Use encryption and proprietary binary protocols to prevent an eavesdropper or man-in-the-middle attack from understanding any intercepted transmission. 802.11 wireless packet frames can be visible to someone with a wireless network analyzer. Management and control frames are not encrypted or authenticated by WEP, leaving an attacker easy access to disrupt transmissions with spoofed frames. Earlier WEP implementations are vulnerable to cracking by tools such as AirSnort (page 24) and WEPcrack, but the latest firmware releases from most vendors eliminate all known attacks.

Products like the ProSoft Technology's ProLinx 6000 series gateways, go one step further and use key management to change the WEP key often so even the busiest wireless LAN could not generate enough data for attackers to recover the key in the interval of time allocated.

- Use non-open standard radio types such as 900 MHz and 2.4 GHz FHSS Frequency Hopping Spread Spectrum (page 25).
- Use key management protocols for dynamic "key-rollover". Changing the key prevents an eavesdropper from understanding what each packet of data consists of.
- Use low-gain directional antennas. Focus radio waves and energy to a confined area.
- Use of industrial (non-plain text based) binary based application protocols embedded in ProSoft Technology products help drastically in prevention of hijacking and spoofing attacks. One of many industrial Ethernet protocols are binary encapsulated within the 802.11 frame. These binary protocols are often secret and therefore present a high degree of complexity to would be trespassers. *ProSoft Wireless Protocol (PWP) is not published and is therefore proprietary in nature.* Security tools and management software like AirMagnet (page 24) can detect AP spoofing and can be configured by default to raise an alarm to alert administrators to investigate any such violations.

"Though much has been written about potential security problems with wireless networks, the majority of these concerns are overblown. While it is true that one could roam the streets, find an unprotected access point and attach to a wireless network, it is far different from actually gaining access to a company's network resources. **To date, we are not aware of a single reported `break-in' and theft of confidential files over a wireless access point.**

The problem is that most access points are set up to broadcast by default the Service Set Identifier (SSID- the password used to identify who can access the LAN). In these situations, virtually anyone with a compatible wireless card can attach to the network. Through a simple configuration change - setting the broadcast feature to 'no' - this security hole can be closed.

Even if this is not done, most networks still protect file sharing and resources by requiring a valid user ID and password.

While it is true that the WEP code has been broken, this was done in a lab with a bank of servers and more than 10GB of encrypted data. It would take a dedicated team of hackers to pull those resources together in a van outside an office to break the code and then read what is being transmitted."

Source: The Online Industrial Ethernet Book – Technical Article: *ARE WIRELESS LANS READY FOR PRIME TIME?* By David Hrivnak

#### 1.4 Additional wireless security guidelines to follow

- Implement a robust networking and security architecture using standards such as PEAP and 802.11i authentication and authorization methods.
- Use 802.11x EAP-TLS digital certificates and dynamic per-user/session WEP keys or IPsec VPNs (page 25).
- Deploy security tools and management software. Visit the websites of wireless security experts such as AirDefense – <http://www.airdefense.net/> and AirMagnet – <http://72.3.236.219/index.htm> (<http://72.3.236.219/index.htm>) to learn more.
- Use commercial or industrial type firewalls to separate wireless from wired LANs. A PLC with two unbridged network cards acts as a firewall but is not physically connected to each other acting as a data concentrator. The PLC data concentrator performs the communication with each network programmatically, controls the frequency of polled and/or change of state data and ultimately controls the channel bandwidth and overall network performance.
- Turn on WEP encryption and never deploy "open system". Use 128-bit WEP keys. Change WEP keys often. Use products with dynamic key management features.
- Use MAC access control by using access points with MAC address filtering.
- Do not use default passwords and network names (SSID) and use difficult to crack passwords not subject to dictionary attacks. Use key and password generating programs to help.

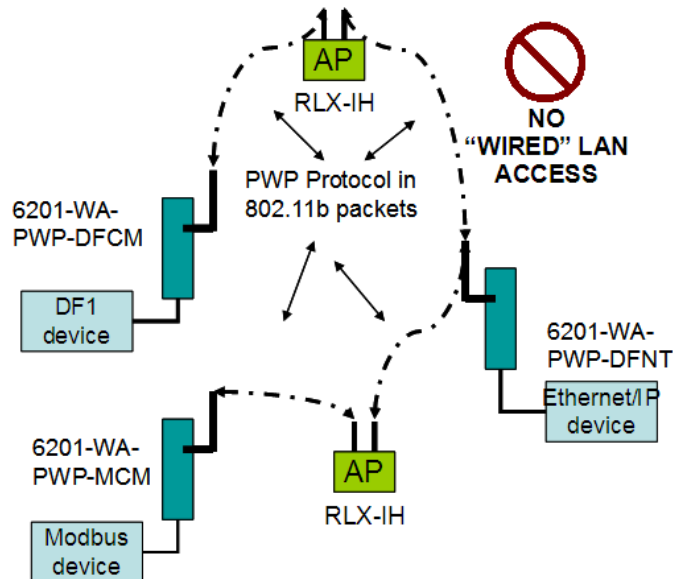
Up to now we have discussed many of the security problems, Corporate and Industrial Automation network planners face today and have classified these concerns to minimize the confusion in preparation of setting up wireless networks. Establishing network security starts with planning and designing the wireless network. The following topic provides some basic questions and helps with defining wireless networks and gives emphasis to industrial automation solutions available from ProSoft Technology

## 1.5 Define your wireless network.

### 1.5.1 Is the network Point-to-Point, Broadcast, Point-to-Multipoint, ad hoc (Figure G) or infrastructure (Figure F)?

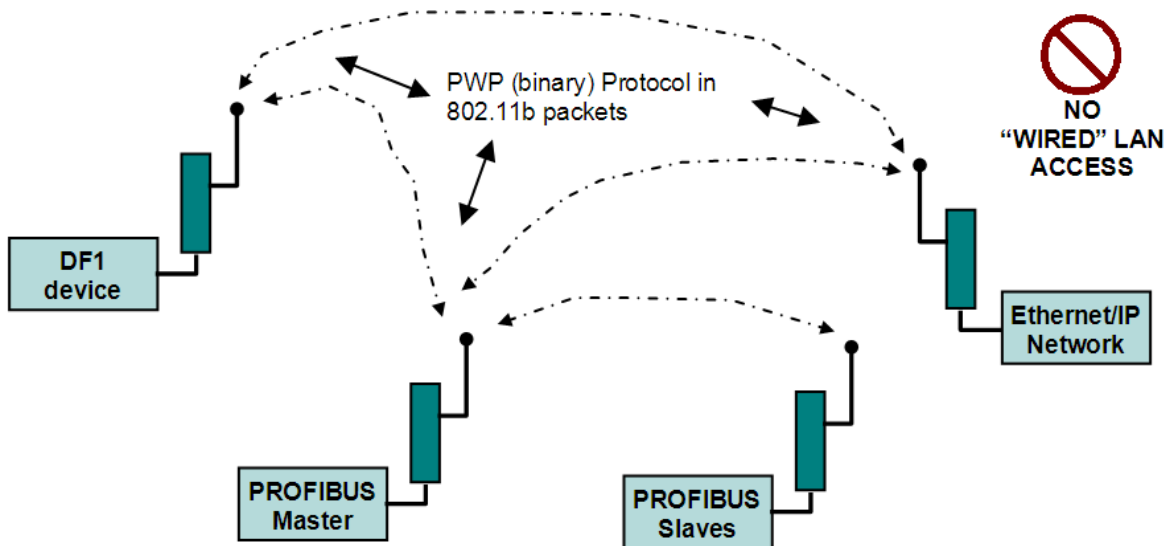
Interconnecting industrial networks and device applications may only require simple peer-to-peer communications. Some applications will connect devices and networks within the building and others interconnect adjacent buildings. Developing and controlling internal radiated hotspots and/or long-haul wireless connections are an important part of the planning process. Different radio products from ProSoft Technology help minimize the areas of security concerns when connecting two building for sensitive data exchange or simple plant floor device to device communication.

Figure F



**Infrastructure Mode:** ProSoft Technology wireless 6000 gateways using RLX-IH repeater AP's

Figure G



Ad hoc mode: ProSoft Technology wireless 6000 Gateways in peer-to-peer

## 1.6 Will I use open or proprietary standards?

It is virtually impossible for a would-be intruder to access raw or encrypted data from FHSS devices. These industrial wireless modems provide the highest level of security for virtually any user's needs.

- The RLX-FH radios provide three levels of security for the RadioLinx data networks.
- Inherent security in Frequency Hopping Spread Spectrum Technology
- Encryption at the hardware level
- Proprietary architecture

**1.6.1 "The RadioLinx RLX-FH radio has been designed to provide customers with confidence of a secure network."**

Unlike 802.11b radios, the RLX-FH radios do not conform to open encryption standards (Figure H). Therefore, third party radios or "sniffer software programs" like AirSnort cannot be used to circumvent the security of a customer's network. Radios that adhere to open standards, such as 802.11b, are vulnerable to security breaches, in that they allow penetration of a portion of the radios overall security, allowing other radios and sniffer software to gain access to encrypted data that passes over the air. Without access to the encrypted data it is not possible to decipher the data.

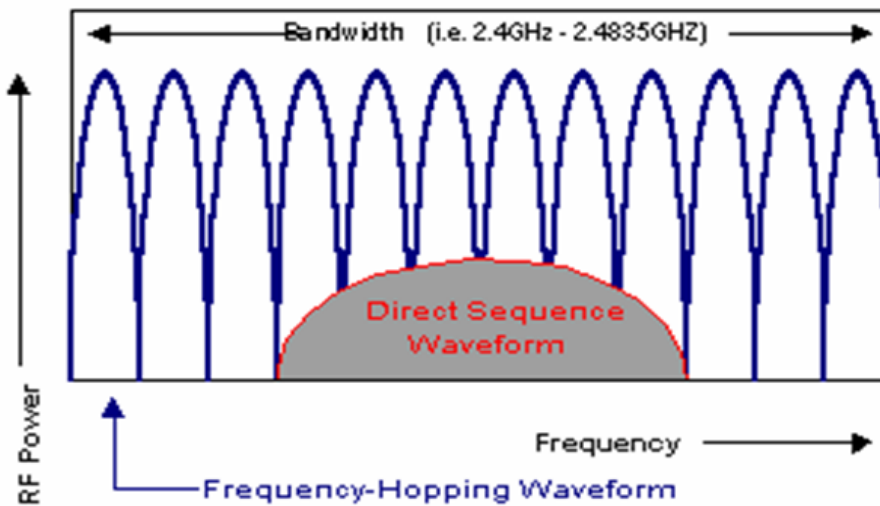


Figure H

Frequency and Direct Sequence Spread Spectrum

The RadioLinx RLX-FH first layer of security contain Frequency Hopping Spread Spectrum (FHSS) technology, which guarantees that RadioLinx radios can detect and communicate only with other RadioLinx units.

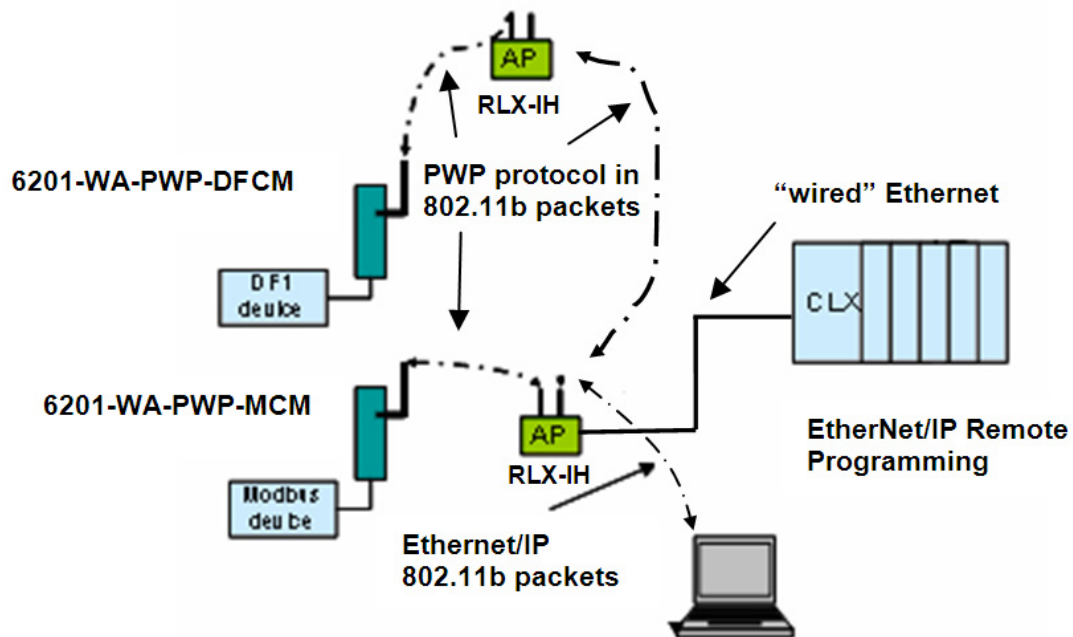
### 1.7 What type of data will be transmitted and what type of protocols will I use?

Simple device to device communication as with ProSoft Technology PROFIBUS wireless master to slave devices inherently provides over-the-air security all the way up to the application layer using the PWP producer/consumer wireless protocol. These devices also provide encryption "key roll-over" management features and have built-in firewall (internal database) protection.

### 1.8 Will I need corporate LAN access to sensitive data or simple device to device communication?

Many industrial wireless applications provide simple communication between a PLC and a remote instrument or second PLC processor which is not connected to a physical LAN. Security concerns for this type of wireless network are outlined in Area B, # 6 - Traffic Analysis and Eavesdropping. Some wireless applications require short connection times, for example when programming a PLC over-the-air through a ProSoft Technology wireless in-rack module. (Figure I)

Figure I



Industrial Wireless network allowing multiple producer/consumer peer devices to communicate with a PLC using in rack wireless module, 6000 series gateways, and RLX-IH (AP) repeater/access points from ProSoft Technology. Laptop wireless client and RLX-IH provide convenient over-the-air PLC Programming capabilities for processors.

### 1.9 Will I use Ad hoc (peer-to-peer) or Infrastructure (access point) type network?

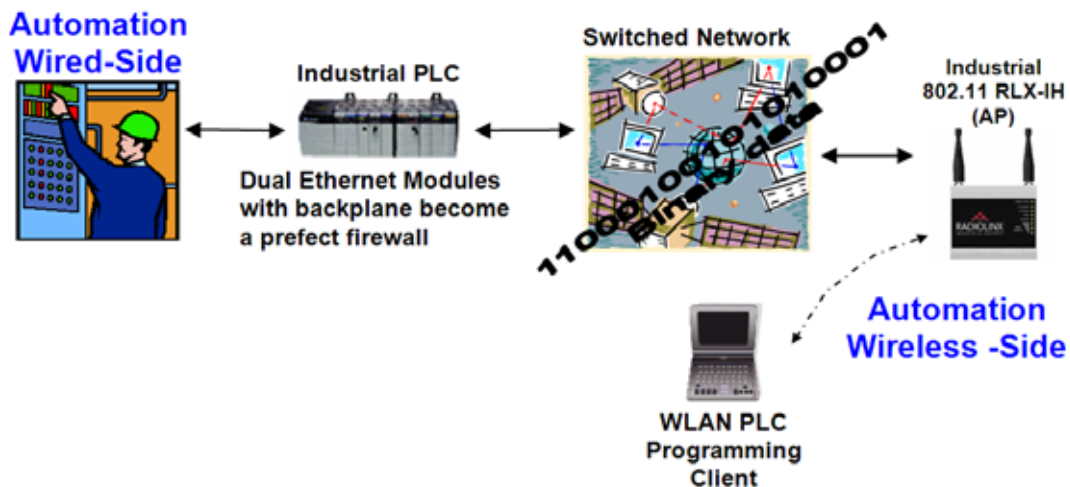
Ad hoc device to device communication or PLC to PLC backplane communications are isolated from corporate LAN sensitive data because when using this type of device-to-device communication topology a LAN access point may not be required (Ad hoc). The PLC backplane becomes an additional firewall to industrial sensitive data especially when in-rack based wireless modules are implemented.

### 1.10 Do I need open industry wireless standards?

ProSoft Technology offer many ISM radio product solutions. Wireless products vary in types of RF modulation (FHSS and DSSS), physical interface types (serial, Ethernet, Ethernet to serial) and whether the products meet open industry standard specifications such as 802.11 or incorporate more secure specifications based on non-standard Frequency Hopping patterns and proprietary data protocol. Depending on network requirements and the type of security required, one or any combination of ProSoft Technology wireless products will help meet the most demanding security requirements.

Figure J

**Example Industrial Automation Wireless/Wired Network:** PLC program controls communication polling to remote devices and overall bandwidth

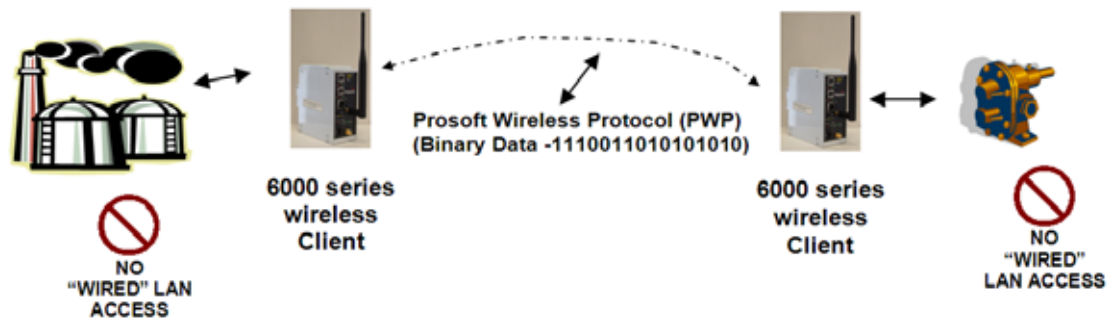


### 1.11 What application layer protocols will be used in transmission?

Are the transmission packets (page 24) using ASCII text (plain-text) based or binary coded data frames? Many 802.3 protocols are ASCII based and expose easily the data being transmitted. Binary protocols like ProSoft Technology's PWP plus encryption technology to scramble the data prior to transmission offer a high degree of protection (Figure J). The binary data (ones and zeros) are meshed with a WEP key like the ASCII protocols but do not expose the data in a plain text format that can be at all understood. The ProSoft Technology wireless ProLinx 6000 series gateway technology add an additional layer of protection because of the internal database. Separate protocol drivers communicate with each device network then perform read and write functions to the database (Figure K). This gateway technology acts as firewall for the connected networks. Another type of gateway technology used with ProSoft Technology is PLC in-rack modules. Like the stand alone gateway it consists of an internal database but the other unexposed side of the database communicates directly with a processor backplane. This technology combined with RF site management creates a difficult challenge for someone to penetrate the remote network or compromise the integrity of the data.

Figure K

Peer-to-peer (Ad hoc) network one-to-one or one-to-many communication



### 1.12 Comments from AirSnort web site

We suggest that you assume that every packet will be readable by the world. Protocols like SSL and SSH are trusted for a good reason; they've both withstood numerous attacks over the years, and emerged (mostly) unscathed. The latest versions of each allow users to protect data, even on totally public channels. This is what's referred to as end-to-end encryption. End-to-end protection measures are fundamentally more resistant to attacks like AirSnort's. Also make use of RADIUS (or some such) authentication to keep users off your network should they crack your key.

To crack a WEP password, AirSnort needs a certain number of packets with weak keys. Out of the sixteen million keys which can be generated by WEP cards, about nine thousand are weak (for 128 bit encryption.) Call these packets with weak keys "interesting". Most passwords can be guessed after about two thousand interesting packets.

To get an idea, assume that your business (it's not very big yet) has four employees, all using the same password. These employees surf the net pretty continuously throughout the day (they're not very good employees.) These employees will generate about a million packets a day. These employees will generate approximately a hundred and twenty interesting packets every day, so after sixteen days, the network will almost certainly be cracked.

However, this network is nowhere near being saturated. As networks approach saturation, the capture time approaches a single day. In some situations, different physical networks may use the same passwords. If this could be determined, this would usually linearly diminish the cracking time also.

We realize that some of our early numbers were much lower than this. The reason for this is simply that we were lucky in our initial tests, and we did not actually calculate the average amount of time it would take. This can happen in the real world too, the best case and worst case are significantly different from the average case. All of the informal calculations performed here assume the average case. You should too.

AirSnort (page 24) is a wireless LAN (WLAN) tool which recovers encryption keys.

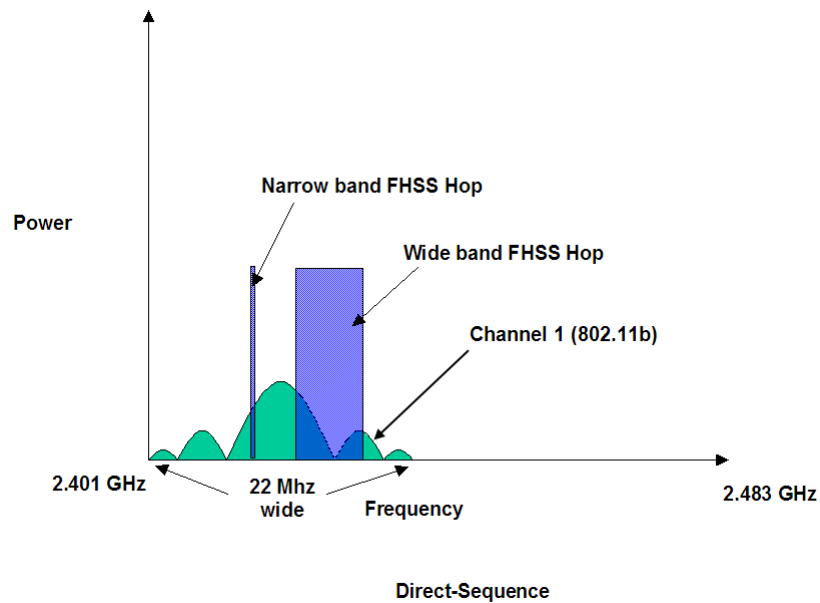
## 2 FHSS and DSSS Primer

### *In This Chapter*

- FHSS ..... 21
- DSSS ..... 22

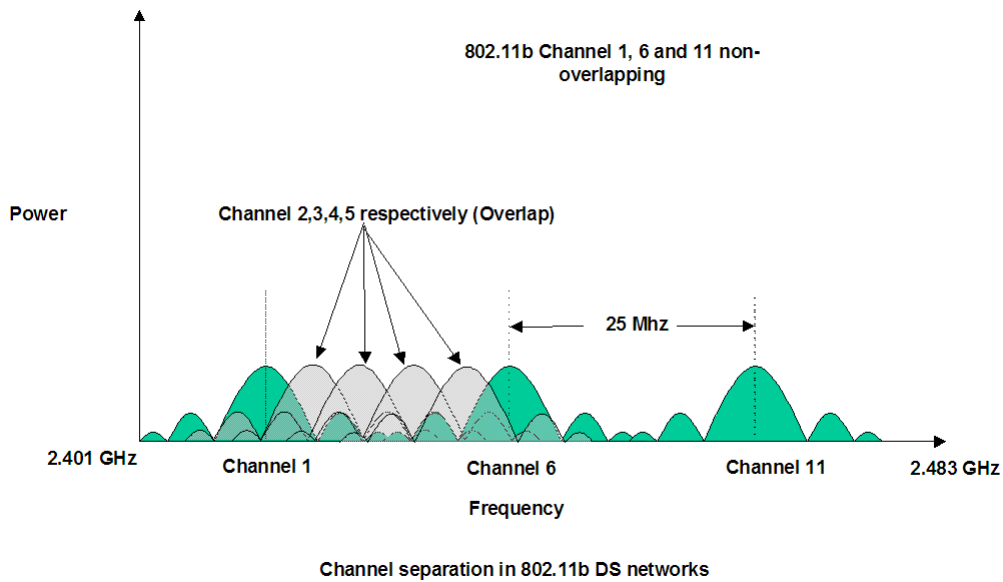
### 2.1 FHSS

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.



## 2.2 DSSS

Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered (and, of course, more bandwidth is required). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low-power wideband noise and is rejected by most narrowband receivers.



RadioLinx products from ProSoft Technology provide solutions using Frequency Hopping Spread Spectrum and Direct-Sequence Spread Spectrum technologies. RLX-FH products use frequency hopping (80 hops per second, at 500Khz bandwidth) to hop over the entire 2.4 GHz band. RLX-IH (802.11b), on the other hand, uses direct sequence. A single (1 of 11, 13 Europe) DSSS channel occupies approximately one third of the 2.4 GHz band.

## 3 References

### *In This Chapter*

- Focus of this paper..... 23
- Seven Security Problems of 802.11 ..... 23
- Network Analyzers ..... 24
- AirSnort home page ..... 24
- ARE WIRELESS LANS READY FOR PRIME TIME? ..... 24
- NetStumbler ..... 24
- FTP, HTTP, POP3, Telnet ..... 24
- Types of Spread Spectrum ..... 25
- VPN and WEP..... 25
- Hotspots..... 25

### 3.1 Focus of this paper

Most papers written on wireless security concerns address corporate LAN access. This paper discusses both Corporate and Industrial wireless concerns but places an emphasis on the Industrial Automation wireless security aspects.

### 3.2 Seven Security Problems of 802.11

Seven Security Problems of 802.11 – O'Reilly Network – Matthew Gast and AirMagnet. A copy of the article is available from [www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html](http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html)

### 3.3 Network Analyzers

Network Analyzers can be obtained from AirMagnet. AirMagnet, AirWISE, PocketNOC, the AirMagnet logo are trademarks of AirMagnet Inc. Per AirMagnet, wireless network analyzers can be a valuable tool for any network administrator. Network analyzers offer reports on the signal quality and network health at the current location. They can break the received traffic down by either transmission speed or frame type. An analyzer should be able to display instantaneous speeds on all channels and give a strong visual indication of the available capacity a channel, which display how crowded a channel has become. Excessive traffic on an access point can be addressed by segmenting the access point's coverage area into smaller coverage areas, or by applying a traffic shaping solution at the confluence of the wireless network with the corporate backbone. Analyzers have built-in alarms for detecting malicious unauthenticated control and management frames and high levels of noise. Its expert analysis engine can also identify malicious clients attempting to launch denial of service attacks against access points.

### 3.4 AirSnort home page

Source: AirSnort home page, <http://airsnort.shmoo.com/> .

### 3.5 ARE WIRELESS LANS READY FOR PRIME TIME?

Source: The Online Industrial Ethernet Book – Technical Article: ARE WIRELESS LANS READY FOR PRIME TIME? David Hrivnak is a member of Eastman Chemical Company's Emerging Digital Technology group

### 3.6 NetStumbler

NetStumbler (<http://www.netstumbler.com/>) is a tool for Windows that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It has many uses:

- Verify that your network is set up the way you intended.
- Find locations with poor coverage in your WLAN.
- Detect other networks that may be causing interference on your network.
- Detect unauthorized "rogue" access points in your workplace.
- Help aim directional antennas for long-haul WLAN links.
- Use it recreationally for WarDriving.

### 3.7 FTP, HTTP, POP3, Telnet

The Internet application suite of protocols such as FTP, HTTP, POP3 and Telnet etc. are ASCII based (some like FTP can use both ASCII and Binary transmission mode) and are easily subject to eavesdropping, while most industrial application layer protocols such as PWP, EtherNet/IP and Modbus TCP/IP are binary coded and are inherently secure.

### 3.8 Types of Spread Spectrum

There are basically two types of Spread Spectrum modulation techniques: Frequency Hopping (FHSS) and Direct Sequence (DSSS) spread spectrum. FHSS and DSSS both occupy a section of the 2.4 GHz ISM band that is 83 MHz-wide. See Addendum A – FHSS and DSSS Primer.

### 3.9 VPN and WEP

A Virtual Private Network (VPN) enables users on a public network, such as the public Internet or a WEP-based 802.11 wireless LAN, to establish a secure connection to a private network. The VPN protects the wireless LAN by creating a tunnel that shields data from unauthorized access. VPNs are widely used to permit secure remote access to corporate intranets. VPNs enable a high level of trust through proven industry-standard security mechanisms, including IPSec (Internet Protocol Security). IPSec employs strong algorithms such as Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES) to encrypt data, with other algorithms for authenticating data packets. IPSec also employs digital certificates to validate public keys. When used over a wireless LAN, the VPN gateway handles authentication, encapsulation and encryption. The combination of an IPSec-based VPN and 802.11 with WEP provided a stopgap solution, albeit an expensive one, for protecting mission-critical data transmitted over a wireless LAN. Combining a firewall with a VPN effectively isolates the wireless LAN to protect data and access to enterprise networks. With the availability of WPA, VPNs are beginning to play a more limited role in WLAN deployments, providing secure access for home users rather than a primary security tool for all employees. Source: Wi-Fi Protected Access and Intel Centrino™ Mobile Technology Deliver a Robust Foundation for Wireless Security document - Intel Corporation 2003.

### 3.10 Hotspots

Hotspots are localized and controlled zones established for wireless communication.

The zones are three-dimensional bubbles controlled by several elements.

- 1 RF radio output power
- 2 Antenna Gain
- 3 Antenna type (directional or omni-directional and polarization) and
- 4 RF radio output frequency or channel.



# Index

## A

Additional wireless security guidelines to follow • 13  
 AirSnort home page • 9, 12, 20, 24  
 ARE WIRELESS LANS READY FOR PRIME TIME? • 24  
 Area A • 7  
 Area B • 12  
 Authentication  
   Open and Shared • 6  
 Authorization  
   MAC Layer • 6

## C

Comments from AirSnort web site • 19

## D

Define your wireless network. • 14  
 Do I need open industry wireless standards? • 18  
 DSSS • 22

## E

Easy Access. • 8

## F

FHSS • 21  
 FHSS and DSSS Primer • 21  
 Focus of this paper • 7, 23  
 FTP, HTTP, POP3, Telnet • 19, 24

## H

Higher Level Attacks. • 11  
 Hotspots • 25

## I

Is the network Point-to-Point, Broadcast, Point-to-Multipoint, ad hoc (Figure G) or infrastructure (Figure F)? • 14

## M

MAC spoofing and Session Hijacking. • 10

## N

NetStumbler • 8, 24  
 Network Analyzers • 10, 12, 24

## R

References • 23  
 Rogue Access Points. • 8

## S

Service and Performance Constraints. • 10  
 Seven Security Problems of 802.11 • 7, 23

## T

The RadioLinx RLX-FH radio has been designed to provide customers with confidence of a secure network. • 16  
 Traffic Analysis and Eavesdropping. • 12  
 Types of Spread Spectrum • 5, 11, 12, 25

## U

Unauthorized use of service. • 9

## V

VPN and WEP • 6, 8, 9, 13, 25

## W

What application layer protocols will be used in transmission? • 19  
 What are the top seven wireless security problems confronting corporate LANs and industrial automation applications? • 7  
 What type of data will be transmitted and what type of protocols will I use? • 17  
 Will I need corporate LAN access to sensitive data or simple device to device communication? • 17  
 Will I use Ad hoc (peer-to-peer) or Infrastructure (access point) type network? • 18  
 Will I use open or proprietary standards? • 15  
 Wireless Security on the Plant Floor • 5

## Y

Your Feedback Please • 2