

BASICS OF WIRELESS SECURITY

INTRODUCTION

RAE Systems offers a number of wireless connectivity solutions for easy installation and rapid (re)deployment of RAE sensors. Numerous questions arise when wireless systems are introduced into a realistic chemical, biological, radiological and/or physical parameter measurement area. Paramount are concerns such as: Will this wireless channel get jammed? Can someone eavesdrop on my information? Can the transmitted data be spoofed somehow? Is it possible for someone to gain access to my overall network via this wireless channel? This Technical Note clarifies and provides answers to such questions.

A FEW WIRELESS FUNDAMENTALS

While there is a great deal of information available pertaining to aspects of wireless communications, it is worthwhile to see what happens in the “wired security” realm. To begin with, it is appropriate to examine the frequency spectrum assignments for the U.S. Notice that the assignment table shown in Figure 1

is a logarithmic chart graphically showing the user/operational assignments for frequencies ranging from 3kHz to 300 GHz. The chart isn’t totally legible (at this scale), so for a legible version, visit the National Telecommunications And Information Administration’s web site and view a PDF (<http://ntia.doc.gov/osmhome/allochrt.html>) that lets you scale the table to readable proportions; you can also order a wall chart of the table. Notice, for instance, that the color yellow refers to frequencies that are used in astronomy (e.g., listening at the 21cm H₂ line for extraterrestrials). The big patches of blue are used in AM & FM radio, TV and cordless and cellular telephony. Similarly, the green patches illustrate the Industrial, Scientific and Medical (ISM) bands – spectral regions where most license-free radios operate, including RAE Systems wireless systems. On Figure 1, line 5, the first green band is approximately 433MHz (followed by various TV and cellular phone bands). The small green slice in the middle of line 5 indicates the 902-928MHz ISM band. It is followed by frequencies allocated for various uses (Defense Dept., police, GPS, radio astronomy). On the far right side

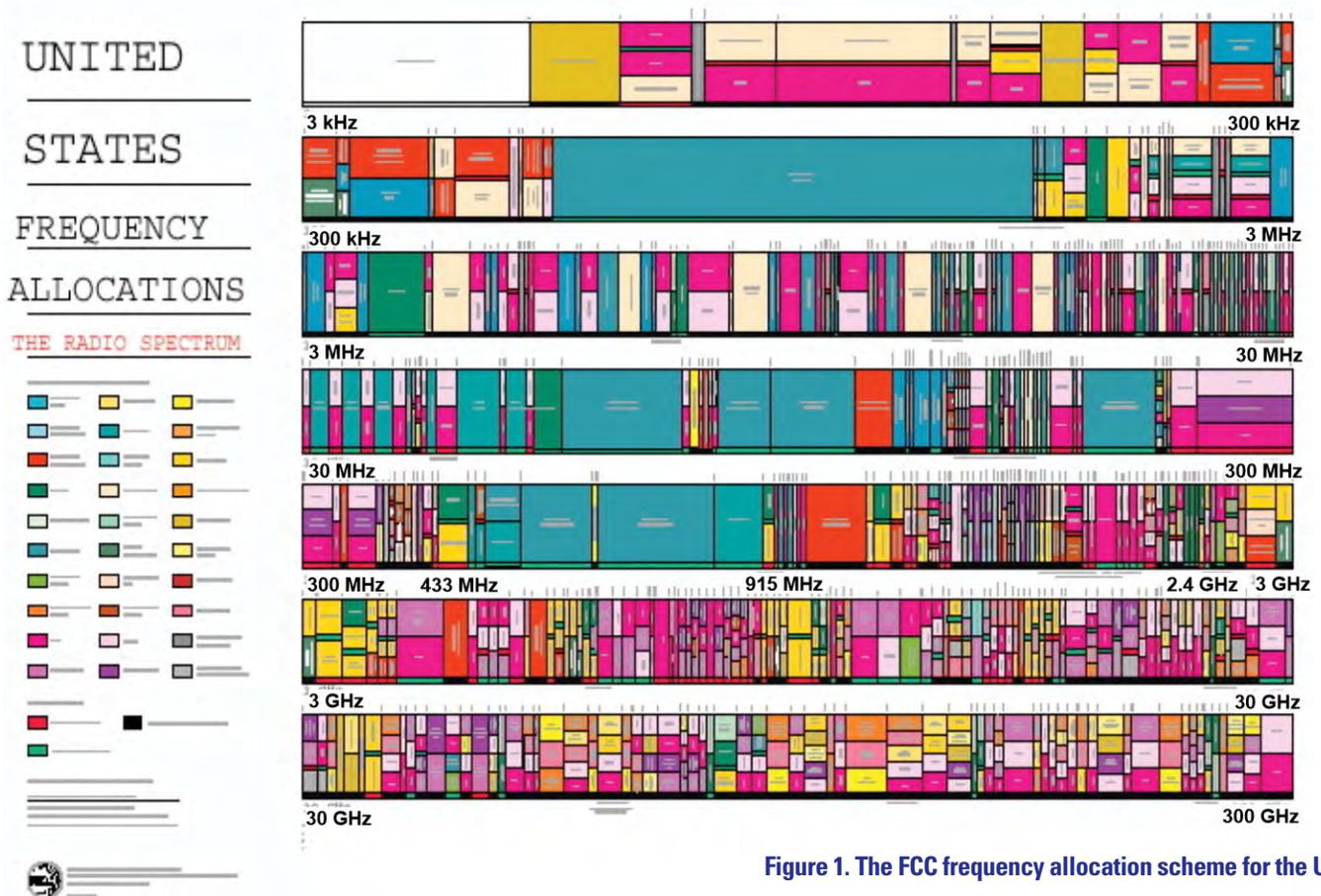


Figure 1. The FCC frequency allocation scheme for the US.

of line 5 is a small green patch, the 2.4GHz ISM band – which is heavily used in various worldwide unlicensed work. In summary, in unlicensed ISM band operation, the RF transmissions typically reside in either the 433MHz, the 915MHz, or the 2.4GHz band.

Fixed-Frequency (Narrowband) Transmission

Traditional AM and FM radio stations are assigned specific transmission center frequencies (think “980 on your AM dial”). The beauty of such a fixed frequency is that the receiver knows where it must be tuned in order to receive the broadcast signal. This situation is shown in Figure 2, which illustrates what a traditional narrow-band signal might look like on an ordinary spectrum analyzer. The carrier frequency is modulated with the information to produce variations in the carrier frequency that are then picked up and demodulated in the receiver. Anyone in the area with a spectrum analyzer can see that there’s a signal being transmitted. Similarly, anyone with a receiver simply has to tune to the broadcast frequency to receive the signal. Demodulating the signal and extracting the information becomes an exercise in cryptography.

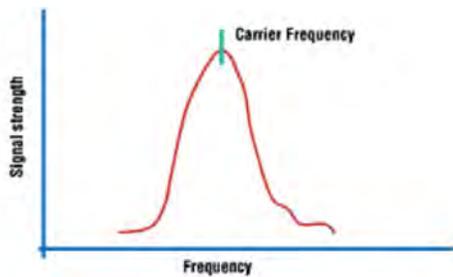


Figure 2. A narrowband, fixed-frequency transmission.

Numerous radio systems using narrowband transmission have been deployed. The analogy to AM or FM radio is particularly useful: co-channel interference occurs when two radios are broadcasting on the same frequency at the same time within the same radiated location. This level of co-channel interference results in neither transmission being correctly received. In other words, a narrowband transmission is susceptible to a number of limitations.

Frequency-Hopping Spread Spectrum (FHSS)

In a frequency-hopping system, the center frequency of the transmission is varied with time, as shown in Figure 3. At any particular moment, the system operates as a narrowband transmission and essentially all the energy is concentrated in this main lobe. The “spreading” occurs in that the lobe’s center frequency moves around. For example, a Bluetooth wireless transmission relies on FHSS, hopping 1,600 times per second over an 80 MHz bandwidth. With FHSS, the receiver must know the hopping pattern in order to follow the transmission. Additional

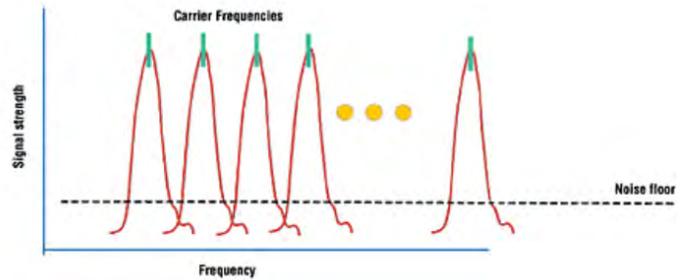


Figure 3. A frequency-hopping spread-spectrum transmission.

security can be added by changing the jumping pattern (which typically follows a Fibonacci number sequence) with time, typically in a pseudo-random manner.

Direct Sequence Spread-Spectrum (DSSS)

A fundamentally different type of spreading a narrowband transmission spreads the signal energy to several frequencies and transmits them simultaneously. As shown in Figure 4, this is achieved by interleaving the information (data) bits with additional 0 or 1 bits.

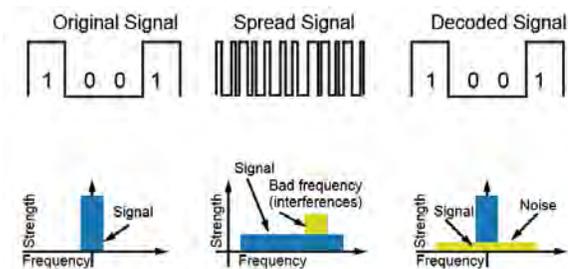


Figure 4. By injecting a spreading code into the data, the resultant narrowband signal is broadened.

These additional bits are not random, but rather are configured in an exact sequence that allows multiple transmissions to reside in the same spectral band simultaneously. The ordering also provides a method of correcting for various errors that may crop up during the wireless transmission.

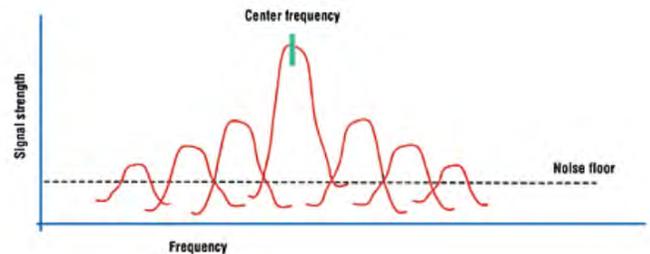


Figure 5. A Direct-sequence spread-spectrum transmission.

In a DSSS signal, more energy is moved to the side lobes, and less is in the carrier frequency, which makes the carrier harder to detect. Figure 5 shows a representative spectrum for an 11-bit spreading code. Note that most of the energy is still in the center frequency.

The more bits in the spreading code, the more energy is transferred into the side lobes. In the "final" case, the energy in the transmitted signal rivals that of the noise floor. This makes the signal even more difficult to locate and tap into, while the authorized user can still detect it easily.

Wired Security: Encryption

In a wired communications environment, security of the data transmission relies on the physical media (cable, coax, or fiber), not being tampered with, and a level of encryption. This situation is shown in Figure 6.

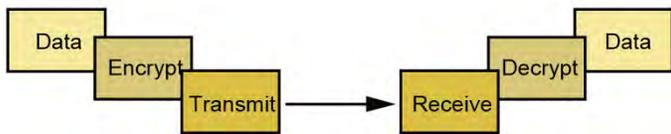


Figure 6. Wired security.

Wired networks normally use encryption as the only weapon against clandestine attacks. This has been effective for many years, but recent attacks are showing that encryption may not be enough.

Wireless Security: Encryption

The use of spread spectrum techniques and interleaving, when combined with encryption, as shown in Figure 7, yields a system that is more secure than its wired counterpart.

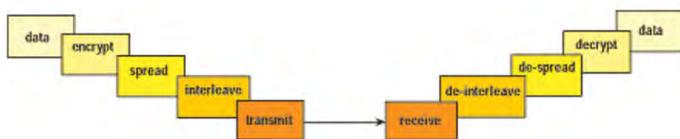


Figure 7. Wireless security.

Wireless networks use a variety of techniques to enhance security, such as spreading and interleaving. These techniques can make the signal virtually undetectable without prior knowledge about the network. This improves the security of the network by orders of magnitude.

IMPLICATIONS FOR RAE SYSTEMS WIRELESS DEPLOYMENTS

The previous descriptions have provided a general overview of various fundamental aspects of wireless communications and networked security. In many deployments of RAE Systems' networks, the network architecture also becomes important. Consider the case associated with multiple AreaRAEs integrated with a ProRAE Remote controller. In this star network configuration (see Figure 8), the AreaRAEs transmit their readings to the base station.

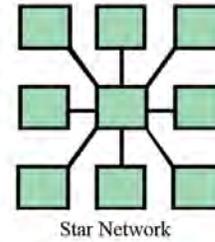


Figure 8. Star Network topology.

In an actual RAE Systems implementation, the communication between the sensor nodes and the base station is an encrypted Frequency Hopping spread spectrum transmission.

RAE Systems' Wireless Security

Devices such as RAELink or the wireless portion of an AreaRAE rely on a combination of encryption, a spectrally efficient Gaussian filtered frequency shift keying (GFSK) modulation, and frequency-hopping spread-spectrum (FHSS) within the 902 to 928MHz ISM band. The actual hopping pattern employed (hopping rate, pseudo-random number encryption code key) are not described in this document (for obvious security reasons).

Specifications:

Radio link:	
Frequency Range	902-928 MHz
Method	Frequency hopping spread spectrum
Hopping Patterns	15 per band, 105 total, user selectable
Hopping Channels	50 to 112, user selectable
Hopping bands	7, user selectable
Range, Line-of-sight	60 miles
Occupied Bandwidth	230 KHz
Modulation	GFSK, 144 ~ 188 Kbps

Figure 9. RAELink RF security operational parameters.

Through the implementation of a 32-bit cyclic redundancy check (CRC) error-correction scheme, needs for retransmission (a potential security concern) are minimized. Actual data encryption is via a dynamic key assignment, substitution encryption scheme.

Data Transmission:

Error Detection	32 bit CRC, retransmit on error
Data Encryption	Substitution, dynamic key
Link Throughput**	115.2 Kbps standard speed, 38.4 Kbps low speed

Figure 10. Encryption and error correction are used.

A WORD ABOUT 802.11 SECURITY

While the wireless communications between RAE Systems' sensor modules and a RAE Systems Host Controller or AreaConnect utilize FHSS and the security inherent within such a transmission, many users also have 802.11 (WiFi) wireless communication networks. WiFi networks receive a significant portion of the information bandwidth for all types of wireless security, and therefore deserve some discussion in this technical note.

802.11 Background

In 1999 the Institute of Electrical and Electronic Engineers (IEEE) completed and approved the standard known as 802.11b, and wireless local area computer networks (WLANs) were born. Finally, computer networks could achieve connectivity with a useable amount of bandwidth without being networked via a wall socket. From its inception, the 802.11b standard was not meant to contain a comprehensive set of enterprise-level security tools. Still, there are some basic security measures included in the standard which can be employed to help make a network more secure. With each security feature, the potential for making the network either more secure or more open to attack exists. The 802.11 standards have been modified over time, resulting in the mix of systems available today (such as 802.11a, 802.11b, and 802.11g).

WiFi Security

Key WiFi/802.11 security features include:

1. The use of the Service Set Identifier (SSID), which allows the 802.11 card to differentiate networks from one another.
2. Network associating, a feature to allow networks to require authentication immediately after a device associates, before it attempts communications across the access point – supposedly providing an extra layer of keyed security. This feature can be set to either shared key authentication or open authentication.
3. Wireless Encryption Protocol (WEP). WEP was intended to give wireless users security equivalent to being on a wired network. With WEP turned on each packet transmitted from one radio to another is first encrypted by taking the packet's data payload and a secret 40-bit number and passing them through a shredding machine called RC4. The resulting encrypted packet is then transmitted across the air waves. When the receiving station picks up the packet, it then uses the same 40-bit number to pass the encrypted data through RC4 backwards, resulting in the host receiving good, usable data.

A SYNOPSIS OF WIFI SECURITY

As you can see from the previous few paragraphs, there are various technical details implemented to make WiFi (802.11) a secure wireless transmission channel. However, as has been reported in the popular press, there are legitimate concerns involved with respect to the use of a WiFi (802.11) system. WEP provides an initial measure of security – a level that every user should employ, whether at their home or an office setting. The 802.11 standards boards are busy ratifying more secure schemes, most notably WPA and 802.11i. However, neither of these schemes is fully backward compatible with deployed WiFi routers, access points, and end nodes.

Figure 11, a table of results generated after compiling WiFi security “sweeps” in the June 2004 World War Drive shows that most WiFi systems do not have even the very modest security features delivered by WEP activated. If nothing else, the responsible wireless Internet user will begin using WEP.

WWWD4 stats of located, wep-known points:		
Category	Total	Percent
Total APs Found	228,537	100%
WEP Enabled	87,647	38.3%
No WEP Enabled	140,890	61.6%
Default SSID	71,805	31.4%
Default SSID and No Wep	62,859	27.5%

Figure 11. WiFi (World War Drive IV) statistics.

Overall Security Situation – A RAE Systems Perspective

Security concerns during wireless data transmission are realistic, but can be minimized, if not eliminated, through the use of technical nuances associated with such a channel. First and foremost, the node to base station communications must use some form of spread-spectrum technology. RAE Systems employs the energy-efficient, latency-minimizing technique of frequency-hopping spread-spectrum. Not only does this make the actual transmission much more secure, but it also allows for a substantial increase in network reuse by allowing numerous users to simultaneously transmit within the same overall frequency (ISM) band. Coupled with encryption of the actual information transmission, these two steps make it nearly impossible for the accidental and/or malicious corruption of the actual transmitted information. The net result for RAE Systems is a suite of wireless products that allow for numerous “clouds” of sensor nodes to be co-resident with other similar transmissions.



Figure 12. RAE Systems Wireless Products.