

SRM Series Wireless Security

Data-Linc Group SRM Series Wireless Security

Industrial wireless transmission has arrived providing clear and significant advantages. Nevertheless, security is always an important issue and a question often asked is, "Will information be secure when broadcast via Data-Linc Group wireless modems?" The answer can be found in understanding the technologies employed in these products and, to that end, this paper will provide the understanding needed.

This paper applies to the SRM6000, SRM6100, SRM6200E, SRM6300E, SRM6210E and SRM6310E radio modems.

Synopsis

The Data-Linc Group SRM series of modems are sophisticated devices that utilize complex technologies including adaptive frequency hopping, proprietary RF (Radio Frequency) packets, data compression and encryption, as well as a wide variety of configuration options. Unlike the 802.11 wireless radios designed for easy and universal access to which security can be applied, the SRM Series is designed for inherently secure and reliable communications.

The design is based on frequency hopping spread spectrum technology as funded and developed by the Defense Advanced Research Products Agency (DARPA) for the United States Military to ensure secure and reliable communications under the most severe wartime battlefield conditions. Although other RF technologies could possibly provide higher communication throughput, they do not approach the security level provided by the SRM Series technology.

Data security is further enhanced through proprietary information packets, data compression, and fast changing dynamic key encryption of all information transferred.

There are many configurations available for the SRM Series modems and their exact settings must be known for any modem to operate within a wireless network. The design of a method to monitor or interject new and/or modified data on this wireless network poses a significant technological and cost prohibitive challenge. A possible form of entry could be via another SRM Series modem, which incorporates the correct technology. However, without network configuration knowledge, any outside modem would be unable to establish communications.

Any security system is theoretically vulnerable. Nevertheless, Data-Linc Group modems are particularly secure and can be enhanced by:

- Limiting physical access to the radio equipment
- Using Point-to-Point operating mode
- Properly securing network configuration information
- Periodically changing network configuration
- Further data encryption before presenting it to the wireless network.

Using technologies designed for the particularly rigorous security demands of the US Military, the SRM Series modems provide several levels of inherent security that, if

SRM Series Wireless Security

deemed necessary, can be further strengthened by network configuration management and additional external security measures.

Frequency Hopping

The FCC certified SRM modems are Frequency Hopping Spread Spectrum (FHSS) transceivers that operate in the license free Industrial, Scientific and Medical (ISM) bands of either 902 to 928 MHz or 2.4 to 2.4835 GHz.

Frequency hopping is achieved in the 902 to 928 MHz band by dividing the RF band into 112 operating channels and hopping through the channels one at a time, in a pseudo-random pattern. (The RF band is divided into 50 channels for the 2.4 GHz band.) There are over 90 programmable hopping patterns. Based on radio operational characteristics, the hopping pattern is further modified (adaptive hopping).

Other wireless devices also operate on these frequencies but are not compatible with the SRM Series hopping, packet, compression and encryption methods. Other radios may receive an SRM Series RF packet but cannot decode them. Furthermore, due to frequency hopping, it would be rare they would receive more than one sequential packet.

Compatibility with 802.11X Standards

The SRM Series modems incorporate proprietary technologies that were uniquely designed and can only communicate with compatible products using the same core technology. This proprietary technology is not compatible with 802.11 products nor any other technologies. Strategies designed to penetrate 802.11 wireless security cannot compromise the SRM Series layered security.

RF Packets

At each frequency hop, using this unique technology, an RF packet is constructed and emitted. The packet is synchronous, bi-directional, encrypted and CRC checked. The clock rate and packet size are programmable and must be matched exactly for all radios.

Data Encryption and Error Detection

SRM Series information (modem specific and user data) exchanged between the modems is compressed, encrypted using a Substitution Dynamic Key and checked with one or more 32-bit CRC (Cyclical Redundancy Check) words. The dynamic key is changed more than 100 times a second and is generated based on network dynamics. The CRC error detection and correction, along with data encryption, ensures the data gets through securely and without corruption or is rejected.

SRM Series Wireless Security

Wireless Network Configuration

There are two modes of operation for a SRM Series network of radios, point-to-point and point-to-multipoint. Each will be approached separately.

Point-to-Point Operation.

In this mode, connection configuration is achieved by call number addressing. Each modem has a unique call number imbedded within its processor that cannot be changed or duplicated. A wireless network is composed of one master, one slave and optionally, one or two repeaters. Each modem in the system is configured to communicate with specifically addressed modem(s) and thus forms a “closed system” in that no other modems can participate in the conversation. This is extremely secure especially when considering data injection.

Point-to-Multipoint Operation.

A multi-point wireless network will include one master, one or more slave radios and optionally, any number of repeaters or repeater/slaves. Like the Point-to-Point mode, call number addressing can be used or alternatively, Network ID. Network ID provides the highest level of security in this mode so only it will be discussed.

The Network ID parameter, with 4095 possible settings, is one of nine configuration parameters that must be matched exactly by any modem within the network to achieve communication.

When using repeaters, a Subnet ID can also be utilized. Subnet ID is a communications routing scheme that allows the user to dictate the path a slave and/or repeater uses to move data between master and slaves. Although designed as a method of ensuring reliable communications, it also provides another level of security by adding additional configuration parameters that must match to establish communications. Combined with the other multi-point configuration parameters that must match, and that most of these parameters have at least 15 possible settings (Network ID having 4095 selections), there are at least 165 million, and as many as 40 billion possible configuration combinations. Given that modem parameters can only be changed approximately 100,000 times (a limitation of the configuration EEPROM) before failure and assuming each configuration change could be accomplished in ten seconds, it would take 1600 modems and 52 years (working 24 hours a day) to cycle through all possible configurations.

Intrusion Methods

How could information be hacked from a SRM wireless network? There are theoretically three approaches; reverse engineer the information that can be received, reverse engineer the SRM hardware, or discover and utilize network configuration. Please note that it is probably far easier to design a new wireless radio system than to reverse engineer an existing undocumented wireless system. Reverse engineering the SRM hardware, assuming it was successfully accomplished, would still require knowledge of the existing network’s configuration so that will not be explored further.

SRM Series Wireless Security

Hacking in without using a SRM Product

Here, at a high level, is what might be needed and the steps involved in hacking into the SRM Series wireless network.

A single individual or team would need in-depth engineering level skills for the design of RF frequency hopping circuitry, RF and data pattern analysis, modulating/demodulating techniques, data communications and cryptography. Necessary equipment might include advanced RF test equipment, computer programming languages and a complex library of elaborate software tools.

With that, the steps taken to monitor the data could include:

Discover exactly the RF hopping pattern and its adaptive criteria in order to gain access to sequential RF packets. Build an RF receiver to which the learned RF hopping lessons could be applied.

Analyze the modulation type employed and build the appropriate demodulator and logic translator so received RF packets could be collected on a computer.

Using the collected data, ascertain its structure, encryption method, and compression algorithm. Build tools to strip out the data, decrypt it and uncompress it.

To transmit data into the wireless network would basically be the reverse of the above and additionally, a wireless transmitter developed. Just to transmit however is not enough. Complete understanding of radio identifiers, network protocol and transmit management must be learned and implemented.

Hacking in with a SRM Series Product

As discussed in an earlier section of this document, there are many configuration settings that must match exactly. With proper configuration management and protection the configuration is not known forcing the hacker to use trial and error cycles to gain entry. The modem would be programmed with a configuration followed by attempted reception. Proper reception would be determined by observing correct responses on the SRM indicators followed by examination of the data at the SRM data port which could be RS232 or Ethernet information in user protocol. If not successful, try again.

Monitoring data in a SRM wireless network is an extraordinarily difficult matter - layered technology that crosses several engineering disciplines and of considerably greater complexity than required to hack into 128 bit encryption (see reference 3). Injecting data is even more daunting. Add a management process that causes periodic configuration change and the hacking work must be done again. This is why the technology employed by the SRM family is used on the battlefield for the US military.

Conclusion

The open architecture of 802.11 offers relatively easy access to interject data into the wireless network. To compensate for the inherent security weaknesses of 802.11 technology, heightened universal encryption methods, such as 128-bit encryption, is commonly used. In the end, these methods have yielded little protection. Universal encryption methods are constantly under attack and at least 10 percent can be easily

SRM Series Wireless Security

decrypted in less than 24 hours by a third party utilizing a mobile PC with decryption software. Historically, as each is cracked or becomes threatened, 802.11 security methods must be constantly improved through new algorithms and/or strengthened WEP keys.

The proprietary industrial SRM Series modems are designed for utmost reliability and security in contrast to the 802.11 standards wireless technologies. By design, Data-Linc Group SRM Series technology offers optimal data security in contrast to alternative, universally available WEP technologies. Data-Linc SRM Series technology provides proprietary, non-disclosed design and programmable network configurations.

If any customer requires additional levels of security such as 128 bit encryption it can be added to the system as is the case with 802.11 technology.

References

1. B. Aboba, *IEEE 802.11-00/253 Presentation*, Microsoft, May 2001.
2. Cisco Systems, Inc., *Product Bulletin: Cisco Aironet Security Solution Provides Dynamic WEP to Address Researcher's Concerns*, November 2001.
3. Intel Corporation, *Wireless 802.11 Security in a Corporate Environment, 2001*.
4. J. Walker, *IEEE P802.11 Wireless LANS, Unsafe at any key size; An analysis of the WEP encapsulation*, October 2000.