SAND97-1249C

SAND--97-1249C

Concepts and Applications of Wireless Security Systems for Tactical, Portable, and Fixed Sites *

CONF-9706109--2

John J. Harrington
Sandia National Laboratories
Albuquerque, NM 87185-0781
505-844-2911 jjharri@sandia.gov

Abstract

Intrusion detection systems sometimes use radio signals to convey sensor status in areas that wire conduits do not service or as a redundant path to wired systems. Some applications benefit from radio technology by minimizing setup time and reducing installation and operation costs. In recent years with the explosion in wireless communications, these radio-based security systems have become more capable while lowering costs, size, and power consumption. However, the very nature of radio communication raises issues regarding setup, operation, and security of these systems.

Sandia National Laboratories, in cooperation with government and industry, has addressed many of these issues through the analysis and development of security systems, communications protocols, and operational procedures. Message encryption and frequent channel supervision are used to enhance security. Installation and maintenance of these systems are simplified by incorporating built-in radio link analysis, menu-driven configuration equipment, and other techniques. Commercial communications satellites and spread-spectrum radios are also being integrated to provide unique capabilities to the security community.

The status of this work is presented herein along with details of its development. These techniques and lessons learned can be applied, in many cases, to other radio-based security systems. Realizing certain limitations, wireless communications can be utilized in a wide variety of security applications.

Introduction

Security systems have long used radio equipment to provide connectivity to remote areas that were not serviced by wire or other conduits because of installation, maintenance, and right-of-way costs. As these costs rise and the capabilities of wireless grow, radio technology can compete favorably even with areas that have an existing infrastructure of

* This work was supported by the US Department of Energy under Contract DE-AC04-94AL85000 and the Electronic Systems Center of the US Air Force. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

wire conduits while reporting alarm status reliably. New wire installations can cost $1 per linear foot depending on the area; and with good practice and luck, maintenance can be low. At the rate of $70 per month (including maintenance) for a leased telephone line, the incremental cost of a radio-based system can be amortized in 6 months per site.

When compared to user-owned, dedicated wires, maintenance of wireless systems can be quite low considering the quality of modern radios and a backhoe's affinity for buried cables. This physical vulnerability of wire can also be exploited by adversaries who can compromise a security system unless effective line supervision is used. In contrast, wireless systems are immune to these types of physical attacks, and an entirely different set of skills must be employed to compromise such a system. An adversary must trade in his or her wire cutter, voltmeter, and resistor substitution box for a spectrum analyzer, modulation detector, oscilloscope, computer, and transmitter to attack an alarm reporting path.

Besides the resistance to physical attacks, some applications require the use of radios to meet specific objectives. The temporary nature of some sites can benefit greatly from the ease by which wireless systems can be deployed and then later moved to another site. Overseas, US military bases are prime examples of the need for portable systems. Most intrusion detection systems for covert and tactical situations, such as US border crossing and military special forces applications, could not even be considered without the use of wireless devices.

Notwithstanding these advantages, radio-based alarm reporting systems possess their own unique set of liabilities. While physical lines can be measured and analyzed, so can radio signals—and without the need to gain physical access. In addition to eavesdropping on radio waves, an adversary can interject signals into the communication channel, even at considerable distance. As wired-systems are sometimes disrupted by breaks or electrical noise, so can radio receivers suffer from unintentional interference arising from adjacent channel and intermodulation signals, especially in metropolitan areas. Malicious interference can also be experienced in the form of radio jamming that, even if detected, can result in a system-wide tamper condition. Just as an adversary must acquire new skills to attack a wireless alarm system, so must installers become adept at basic radio operation if a reliable system is to be achieved. Antenna placement, link margin, and network configuration are on the skills list.

Licenses must be obtained to operate in frequency coordinated bands, or congestion in FCC Part 15 bands must be endured. These factors tend to reduce the available channels that route all system messages which makes it difficult for a radio system to service as many alarm points and to achieve the same response of a wired system. Consequently, if an effective wireless alarm system is to be developed for the protection of valued assets, all of these issues should be considered in the design, installation, and operation of the alarm reporting system.

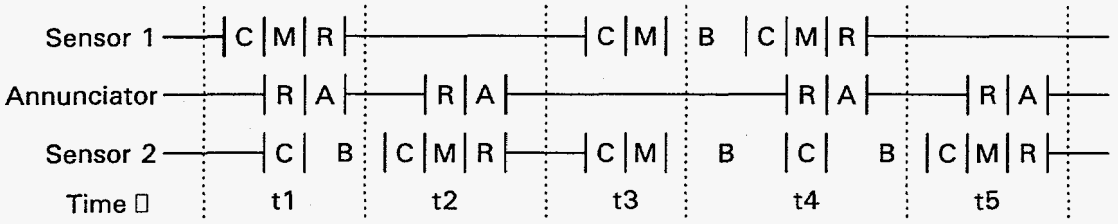
System Design

Fundamental to any wireless system is the type of radio, modulation technique, and frequency of operation. To a large extent, these three parameters determine functional capability. An alarm system that is based solely on transmitters at remote sensor locations and a central station receiver is fairly limited compared to a transceiver (combined radio transmitter and receiver) at every location. By using only a transmitter at the remote end, a sensor cannot determine if its message is blocked due to a marginal signal or collision with another message. However, by employing a transceiver, the remote end can listen before transmitting in hopes of avoiding a collision. A remote unit can also be programmed to repeat a message if an acknowledgment from a recipient is missing. Transceivers permit command messages to be received at a remote unit for the purpose of switching relays, polling for status, or initiating diagnostic functions. The additional cost of a transceiver over a receiver or transmitter is small, and the radio can be turned off during periods of non-use to conserve energy in battery-powered installations. These benefits make a strong case for using transceivers at every node.

The ability to communicate many messages with little delay requires high data rates. Advanced modulation techniques typically achieve these rates by trading-off communication range which can sometimes be regained by increasing transmitter power or using a better antenna to boost signal levels. Without strong signals, bit errors can force so many message retransmissions that it will nullify any benefit of higher data rates. Direct Sequence Spread Spectrum (DSSS) is one modulation technique that achieves high data rates (> 100K bits/s). However, due to frequency (>900MHz) and power (<1W) restrictions, range is limited unless the link is ideal. DSSS radios are also unlicensed, which tends to attract other users which could result in mutual interference. Contrary to some advertisements, DSSS signals can be detected, intercepted, and jammed—but not as easily as conventional modulation methods. Frequencies in the VHF and lower UHF bands penetrate objects better than DSSS frequencies, but line-of-sight paths are still advantageous. Buildings with tight-fitting metal doors and small windows may give DSSS radios an advantage over radios operating at lower frequencies with equal power. The decision of modulation, frequency, and message throughput should be based on system level requirements and operational environment.

Beyond the actual radios, the capabilities and performance of a wireless network are largely defined by a communications protocol. Protocol embodies the rules that govern the actual steps of message handling and routing. As an example, many protocols allow sensors to share a common radio channel by taking turns sending messages. This process is referred to as Time Division Multiple Access (TDMA). Another technique allowing multiple access is Frequency Division Multiple Access (FDMA). TDMA is usually chosen over FDMA considering the limitation of available channels and the hardship imposed on the central station to simultaneously monitor every frequency. Code Division Multiple Access (CDMA) is another technique that DSSS can exploit.

TDMA systems work best when message transmission time is brief and some form of collision avoidance is used. This was previously mentioned and is called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Typically, a unit desiring to transmit a message first monitors the channel. If no other signal is detected, the unit is free to begin transmitting. Assuming another signal is present, the unit backs-off a short random amount of time before again sensing the channel. This form of CSMA is called non-persistent which continues until the message is sent. The benefits from CSMA are enhanced when network radios switch quickly from transmit to receive (and vice versa) which is called T/R attack time or turnaround time.



A = acknowledgment; B = backoff; C = CSMA; M = message transmit; R = Receive

- t1 Sensor 1 performs CSMA, transmits a message to the annunciator, and then receives an acknowledgment while sensor 2 detects this traffic and backs-off.
- t2 After back off, sensor 2 performs CSMA again and conveys a message to the annunciator which promptly acknowledges the message.
- t3 Sensor 1 and sensor 2 sense the channel simultaneously and not detecting any signal, both decide to transmit which results in a collision and message loss.
- t4 Sensor 1 completes backoff before sensor 2 and after detecting a clear channel, retransmits the message while sensor 2 performs CSMA and backs-off again.
- t5 Sensor 2 is now free to retransmit its message and receive an acknowledgment.

Figure 1. Two sensors communicating with an annunciator using non-persistent CSMA.

Message routing is another important attribute that defines a system's capability, reliability, and ease of setup. Alarm reporting paths tend to resemble a spoked wheel where messages must flow from rim (sensor) to the hub (central station). This path fulfills a system's primary objective—to convey sensor status to an annunciator. In a polled network, messages first originate at the hub in the form of interrogation requests and travel to the rim which invites a sensor-to-annunciator message. If a sensor cannot communicate directly with the central station because of distance or obstruction, an alternate link must be used, typically through a repeater. Another remote sensor node can also serve as a surrogate repeater if it has a viable link to the hub. Even when a viable path is achieved, conditions can change to the point where a particular link fails, especially if the link is marginal from initial setup or a repeater fails. In these cases, a system that re-routes messages through another path is more reliable. Alternate channels are also useful if the original path is blocked by radio interference. Unfortunately, the more interconnected a network becomes, the more difficult it can be to set up. Some systems offer automatic configuration capabilities with built-in alternate paths based on path directness and signal quality. While auto-configuring systems certainly simplify setup and add redundancy, a certain level of trust must be placed in their algorithms; and

message delay time can vary depending on the chosen path. Figure 2 illustrates a simple and interconnected network.

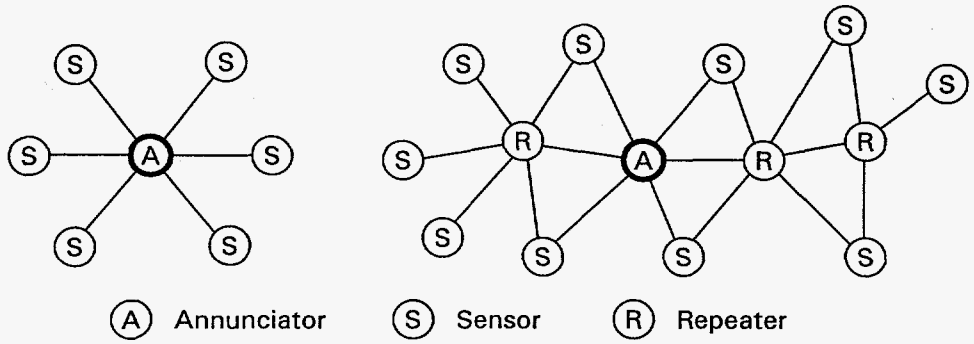


Figure 2. A simple and moderately interconnected network

Systems that are based on interrogation or that are highly interconnected are not typically well suited for battery operation. This is because nodes (remote sensors and repeaters) must power their radio receivers continually to respond to spontaneous messages directed at them. One alternative is to create time slots during which a node is actively receiving and at other times is powered down. This is an effective method of reducing power consumption but at the expense of creating considerable delay because a sensor must wait until its allotted slot before sending alarm status. In a system that contains a hundred or more sensors, the delay can be prohibitive.

Network Setup

As mentioned earlier, manual setup of interconnected and path-redundant networks can be a complicated task—one that may be unsuitable for untrained personnel or for anyone in adverse conditions, e.g., war or weather related. Factor in the vagaries of RF signals, and the establishment of a reliable link can be a daunting task for anyone without the proper equipment. One of the most valuable tools and simplest to use for setting up an RF link is a signal strength indicator. Normally, an RF path between two radios is reciprocal—meaning the signal travels equally well in both directions. However, there are instances when this is not the case; so if possible, the signal strength should be measured at both ends and reported to the side that is manned. Signal strength can easily be provided in a system that offers 2-way communication. Using the combined signal strength and conservative limits, an installer now has the information to select antenna type and position, set transmitter power, and decide whether a repeater or alternate path is advisable. Link quality can also be sent to the central station through periodic state-of-health (SOH) messages for archival. In this way, maintenance personnel can identify trends in high security installations before actual problems arise. Signal strength measurements are equally important in portable and tactical installations because these

systems are set up quickly and cannot always achieve optimum antenna placement in their particular environment (non-line-of-sight, antenna at ground level, dense foliage, etc.).

Sensor setup of portable and tactical applications is also simplified if built-in local annunciation is provided for walk-testing. Likewise, built-in battery readout is useful and reduces the amount of support equipment that must be carried to set up an alarm reporting system. In the same way that signal strength can be sent to the central station, battery levels can be sent and monitored as advanced warning of impending maintenance.

Usually, a system that is very capable also has many options. These options must be set correctly during a process of configuration if the system is to perform as intended. A challenge exists to clearly present the options to an installer. Menu-driven configuration programs simplify this process; and, if properly structured, many options can be set automatically or altogether skipped based on previous answers. Explanations of options can accompany the questions and serve as an on-line manual. Another approach is to default all but the most basic parameters for certain users while retaining the flexibility for more highly trained operators. Some options can be set aside in advanced setup menus. These techniques can make a complicated system appear simple while preserving all of its capability.

System Operation

In operation, the challenge of any alarm reporting system is to convey messages reliably with a minimum of delay. This challenge is magnified in wireless systems because many sensors are often sharing a common communication path, viz., a single bandwidth-limited channel. A high rate of SOH messages reduces the time available to communicate alarm messages, and a single sensor can generate a plethora of messages that results in self-jamming for the entire network. Accessing a sensor at the central station quiets the annunciator but leaves havoc reigning on the network. A wireless network should control these factors and preserve the network for vital communication.

Excessive alarm messages can be constrained at the remote sensor end in varying stages. The first stage should take a sensor signal that toggles at a high rate (enters alarm then secure then alarm again every second) and filter this to no more than one message in five seconds for example. The next stage can monitor the number of resulting messages and constrain this amount after the third message to only one per minute. After a period of time, the constraints can be backed off to their initial values. These measures tend to preserve the network and still convey relevant and timely alarm status to system operators. These techniques are so effective that some sensors can be left in secure mode even during operational hours when personnel are generating continual alarms. However, this type of nuisance alarm can also be controlled by configuring the sensor communication nodes to enter periods of access and secure automatically as a function of time, or local alarm panels can be used to access an area manually. In either case, it is advisable to communicate this changing status to the central station.

The alarm reporting hardware should also supervise the channel and equipment to ensure a viable system. This task consists of monitoring sensor lines for evidence of tampering, the communication channel for jamming, and batteries and other hardware for signs of failure. These SOH messages should be communicated to the annunciator on a time schedule so that any absent or tardy message can alert operating personnel. Unlike wired-systems, radio-based communications cannot provide continuous supervision of many sensor nodes when only one channel is available. If 100 sensor nodes constitute a network and only one SOH message can be sent per second while still reserving time for alarm and other messages, then every node can only be supervised once in 100 seconds. In this example, an adversary can wait till a particular node has sent its SOH message then disable the node, knowing that the tamper will go undetected for 100 seconds. Consequently, the response force will be delayed 100 seconds. If the intruder task time is less than 100 seconds plus the guard force response time, a vulnerability exists.

SOH messages can be sent unsolicited or polled. Polling for SOH is attractive because the network hub is in control of individual rate. The rate can be randomized or can adapt to changing circumstances. A high polling rate can be reduced momentarily to accommodate a large number of alarm messages. Rate can also be adjusted to reflect security posture—raising the rate during periods of tension. Battery-powered sensor nodes can conserve large amounts of power by sending unsolicited SOH messages because their receivers do not operate continually in order to receive a poll message. Another network/battery saving technique is to only send SOH at a rate that is commensurate with asset value, target attractiveness, and task time.

Regardless of how SOH messages are initiated, they should be spread evenly over time to provide a uniform sampling of the RF channel and to avoid clumping. Unlike other forms of jam detection, SOH messages constitute the heartbeat of a system assuring security personnel that equipment is operational and that the RF channel is capable of passing messages. Even though every node might be sending SOH at a definite rate, it is possible for many nodes to transmit SOH at the same time and exceed the networks capacity for communicating messages. If possible, SOH messages should be synchronized to prevent this occurrence.

An alarm reporting system normally tries to relay status messages with a minimum of delay, but some clandestine situations should intentionally delay transmission. This is because covert sensor locations, such as border crossing detection systems, are only effective as long as their locations are unknown. Once a sensor location is discovered, intruders need only avoid that particular area to escape detection. Wireless systems tend to reveal their position if they transmit alarm messages immediately. A savvy intruder only has to carry a receiver tuned to the correct frequency to isolate a buried sensor. However, this strategy can be thwarted by delaying transmission of alarm messages by a random amount of time.

Security Enhancement

Up to this point, the design, setup, and operation of an effective alarm reporting system has been presented which should provide adequate security in many instances. However, to raise the ante for determined adversaries, jam detection and cryptography should be considered. Because radio signals extend beyond secure areas, a vulnerability may exist from message interception, substitution, and jamming. A steady flow of SOH or other system message normally implies an unjammed channel. However, if message traffic is sparse, or for covert reasons supervisory messages are unacceptable, an active form of jam detection should be employed. The criteria for detecting simple jamming can be based on sensing an RF signal above some threshold for a minimum time, but sophisticated jamming can easily escape this form of detection. Beyond this level, it is difficult to absolutely detect jamming apart from SOH signals. Even then, if the SOH messages are not encrypted, an adversary can eavesdrop on the network and can allow the supervisory signals to pass while jamming only selected alarm messages.

The level of encryption should be based on the threat and asset value. Some commercial systems use internally developed algorithms; but since they are proprietary, it is difficult to judge their strength. Encryption may prevent an adversary from reading a SOH message; but if these messages are repeatedly sent without any change, an adversary can still record a valid message and retransmit it on cue. For this reason, SOH messages should be encrypted in such a way so as to force a change from one message to the next. This can be accomplished by incrementing a sequence number within the message or by using the current time as a message part. Alarm messages should also be encoded in a similar way. If a message is received with either an old sequence number or time, the message authenticity is suspect. Otherwise, an adversary can retransmit a large number of previously recorded alarm messages to swamp an annunciator and draw attention away from a valid alarm message. If encryption is used, the security keys must be managed in such a way that permits new keys to be entered into the system without disrupting alarm reporting. New keys should not be transmitted over the RF channel; but if each node already has several keys, a message can be sent to switch to one of those new keys.

Current Development

Through the sponsorship of the Electronic System Center, Sandia developed most of these techniques for the Air Force's Tactical Automated Security System (TASS). New capabilities that address security related issues regarding wireless alarm reporting are being developed for DOE applications using Sandia's Universal Network Interface Radio (UNIRad). Some capabilities extend beyond security and show merit for other applications such as unattended ground sensors, tracking, and cooperative monitoring. UNIRad incorporates a narrowband FM radio in either the VHF or UHF band. Extended links of 80 miles have been in operation for over a year. Power conservation techniques allow UNIRad to operate for nearly one year on internal AA batteries. SOH messages can be programmed from once every two seconds to once every six days. Over 2000

sensor nodes can operate in a network. Triple-DES encryption is offered with the ability to hold three sets of keys at once. Throughput rates have been demonstrated up to five acknowledged messages per second using a p-persistent CSMA protocol.

A menu-driven, PC-based loader is operating that guides installers through configuration. Link test and walk test functions facilitate link and sensor setup. Each unit can be configured to function as a sensor interface, repeater, or annunciator interface. As a sensor interface, up to six sensors can be connected using conventional end-of-line resistor supervision. UNIRad is capable of simple sensor fusion processing. SOH monitoring and jam detection are built-in. A text-based annunciator is available that operates on a PC platform. The UNIRad module is commercially available, but the software is currently only supported by Sandia.

Future development will offer a spread spectrum radio for close-range covert situations and a hand-held annunciator for force protection and other portable applications. Integration with orbiting satellites will extend network communication world-wide. Different network structures are being developed to create a LAN/WAN structure that will allow RF channel reusage.

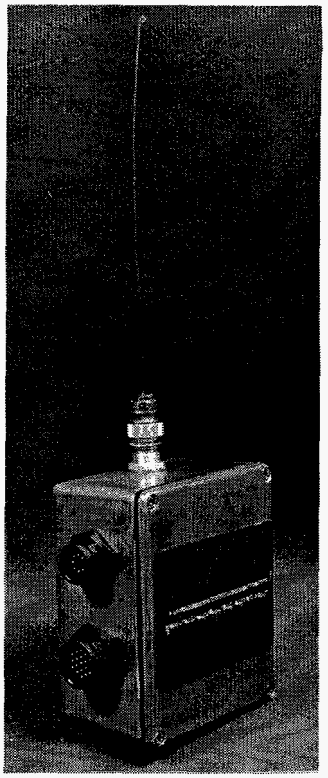


Figure 3
UNIRad

Summary

This paper has addressed the issues of design, setup, operation, and security of wireless alarm reporting systems. There are obvious cost and setup advantages when compared to wired systems. Utilizing 2-way radios enhances performance and provides unique capabilities. Operational environment and performance requirements should dictate the type of radio and what frequency to use. Message acknowledgments and alternate paths increase the reliability of communication. Setup of a robust RF-linked network is not trivial, and the proper tools with good human-interfaces should be offered. Nodes must communicate alarm status in a timely manner and preserve the radio channel from superfluous traffic that can result from constant sensor alarms. Frequent channel supervision is desirable to minimize delay when a SOH message is missed; but this desire must be balanced with the RF channel's capacity and the need to send alarm messages. Encryption is absolutely necessary in high-security systems to thwart determined adversaries. Short of being completely jammed, which creates a system-wide tamper, wireless alarm reporting can achieve an acceptable level of security for many situations.