Without Wires…
Improving Network Security through Wireless

By Kevin Carey, Microwave Data Systems

Introduction
The use of radio to control and monitor mission-critical functions, such as traffic control, alarm system supervision and public safety dispatching has become a widely accepted practice over the past 10 years. This article explores the benefits of wireless communication as a more secure alternative (or complement to) hardwired solutions. We will discuss the major types of wireless technology in use today, and identify new and emerging trends in the wireless industry.

Wireless communication systems offer significant benefits over hardwired mediums such as telephone, fiber optics, and coaxial cable. With hardwired systems, security, installation cost, time-to-install, reliability, and availability are all potential concerns. These systems require dealing with issues such as rights-of-way, digging permits, the crossing of structures (bridges, railroad tracks or highways) all of which can present significant challenges to an installer. Once the system is installed, ensuring the security of the network can be nearly impossible. While no system can be 100% secure, we will discuss the areas where wireless solutions offer an inherently more secure communications infrastructure.

Wireless Applications Today
There are a host of potential applications for wireless networks in both the traffic and public safety arenas. These systems provide real-time information to traffic engineers and public safety personnel, enabling more effective management of traffic conditions and quicker response to emergency situations.

In traffic networks, wireless is being used successfully by many cities for remote communication with intersection controllers, variable message signs, weather monitoring stations, and to carry video images from cameras at key intersections or known trouble spots. The cities of Grand Rapids, MI, Colorado Springs, CO and the Kentucky State DOT are leaders in applying wireless technology to their networks. Most wireless systems for traffic control operate in a multiple address (MAS) arrangement whereby a network of remote field sites are polled for data by a central master station. MAS networks are discussed in greater depth later in this article.

Wireless is also being used increasingly in the public safety arena to link dispatch centers with outlying transmitter tower sites. In these systems, the dispatcher’s console is often located within city limits, and a point-to-point wireless link is used to transfer voice and data traffic to a remote tower site with more favorable terrain and less potential for interference. Even if some transmitting facilities exist at the dispatch center, many agencies depend heavily on remote tower sites to provide solid communications throughout all areas of their jurisdiction. More complex systems may also incorporate multiple “voting” receivers to determine which site provides the strongest signal from a mobile station.
The system used to connect the dispatch center to the remote tower site(s) is of vital importance. Leased telephone lines or other hardwire methods can be used, but often do not adequately address the concerns for reliability and high cost of operation—both in initial expense, and in ongoing access charges. (See sidebar Hardwire Communications—Understanding the Limits.) Mission-critical applications are often better served with a dedicated point-to-point radio link that provides continuous, instant communication with remote tower sites.

There are also cost benefits to this arrangement; once a point-to-point system is purchased and installed by a municipality, they own the medium, and all ongoing charges for communications are eliminated. The equipment costs for a point-to-point wireless link are often recovered within two or three years of operation, depending on the rates that were being paid for leased lines. A full description of point-to-point dispatching links exceeds the intended scope of this article, and will be presented for a future issue of the IMSA Journal.

The remainder of this discussion focuses on wireless systems in relation to traffic control and security applications, although many of the principles discussed apply to other types of radio networks, as well.

### Hardwire Communications—Understanding the Limits

Reliability and security are prime concerns in hardwired systems. By their nature, cables are vulnerable to breakage and other damage from storms, motor vehicle accidents, construction work, or even sabotage. An outage can be difficult to locate, and may take hours to repair depending on the priorities of maintenance crews. During a widespread event, such as a weather-related outage, repairs may have to wait for days or even weeks while overloaded crews respond to other pressing incidents. Traffic systems are not necessarily a leased line provider’s highest priority.

The availability of a wired network can be a concern; especially where the public telephone system is involved. During periods of heavy telephone use, such as may occur during a widespread emergency, it may not be possible to access the telephone network and get a message through. Unfortunately, this scenario will most likely occur at the very time a network is needed most by public service and municipal agencies. It is important to note that Cellular-based technologies, such as Cellular Digital Packet Data (CDPD), are also subject to these limitations. Consumer voice traffic is the first priority of cell providers, not telemetry data.

Aside from availability aspects, there are often stringent limitations on bandwidth and transmission speed depending on the length and type of cable being used. Video, for example, which is being incorporated in many traffic systems today, may require more bandwidth than can be accommodated in a typical wired network. And if leased circuits are used that can support video, the cost can exceed $300 per month. Noise, too, can be a limiting factor especially in older wired systems.

While no single communications medium is right for all situations, system planners need to be aware of all of their options when selecting a solution to meet their needs. Wireless alternatives may be appropriate when cost, reliability and performance are critical elements of a new or upgraded communication system.
Wireless IP over Ethernet—the Future is Here

One of the most exciting areas of growth in wireless communication today, involves the transmission of IP and industrial protocols over wireless Ethernet. This offers distinct advantages over serial communications, such as hardware and software platform interoperability, collision avoidance, high transmission efficiency, and the ability to add new devices to a network without disrupting traffic flow. The use of IP also opens up new possibilities for integrating a utility-wide Intranet, the World Wide Web and/or video into a network control scheme.

Until recently, most wireless Ethernet products were designed for office environments, and were not built to survive the harsh, external environments of industrial applications. Light duty transceivers of this type are often acceptable for carrying data short distances within a building, but should not be considered for long range, mission-critical applications.

Today, industrial-grade wireless devices such as the MDS iNET 900™ (Figure 7) can carry Ethernet and serial data considerable distances, effectively eliminating the risks involved with running long spans of cable. Additionally, the iNET is capable of handling multiple users and protocols in new and legacy networks. Products of this type have huge potential for application in traffic control, monitoring of intrusion alarms, and for transmission of video and other high bandwidth traffic.

Figure 7. The MDS iNET is a full-featured wireless Ethernet radio. This license-free unit is capable of range up to 30 miles. It supports Ethernet as well as serial data transmission, allowing it to coexist with established “legacy” networks.

A growing number of RTUs, intersection controllers and video surveillance cameras being manufactured today are equipped with direct Ethernet connections. This simplifies the connection of compliant wireless devices and makes the expansion of a network justifiable from a cost standpoint. Software development at the host computer is also simplified, since multiple protocols can now be addressed by a common interface. The responsibility to resolve the different locations, protocols, interfaces and baud rates is delegated to the network itself.

The operating frequency of an Ethernet radio deserves careful consideration. Many currently available designs (including office-grade wireless LANs) operate in the license-free 2.400-2.483 GHz band. By contrast, the 902-928 MHz license-free band offers
greatly improved range, and reduces the chance for interference with other Ethernet or consumer devices. (Many consumer devices already occupy the 2.4 GHz band, including microwave ovens and some home audio and video systems.) 900 MHz should be the preferred choice when range and reliability are paramount.

MAS System Design

A typical MAS system consists of a network (cells) of remote transceivers, with up to 30 or 40 units per cell, each linked to a central master station via a 200, 400 or 900 MHz radio frequency. The master station is often located at a Traffic Operations Center or other facility where personnel monitor and respond to traffic conditions. The radios may be of the licensed or spread spectrum, license-free design. (See sidebar Spread Spectrum—a Viable Alternative for more information on license-free radios.)

Figure 1 is a sample layout for a radio system serving a traffic application. The radio system serves the role of a traditional hardwired network, but does so without the required infrastructure of wire and cabling. It allows two-way communication throughout the network, and provides real time transfer of data to traffic control personnel. The system may be used to issue commands, download timing programs, collect status information or conduct diagnostics of remote equipment.

The purpose of the radio system is to transport data between the remote and master sites of a given network. As such, the radios do not change the data in any way—they simply transmit or receive the signals supplied to them by external equipment. This type of radio system is often referred to as being data transparent.

![Figure 1. Typical MAS wireless network](image)

Spread Spectrum Radio—a Viable Alternative

MAS systems can be licensed or license-free. Traditionally, radio users have operated on fixed frequencies licensed to them by the FCC, Industry Canada, or other applicable licensing authority. This arrangement is intended to limit radio interference to or from other users within a geographic area, and for the most part it works very well.

In recent years however, overcrowding of frequencies has made it difficult, if not impossible, to obtain a radio license in certain areas—especially in or near large cities where the density of transmitting stations is much higher than average. Overcrowding of frequencies has forced users to explore other options for wireless data transmission.
In the U.S.A., Canada, and many other countries license-free operation is permitted under certain restrictions, and may offer a practical alternative to traditional (licensed) radio operation. License-free radios are limited to a maximum output of 1-watt, and must use a spread spectrum technique that distributes their RF energy over a wide swath of frequencies. Despite their low power, spread spectrum radios often provide reliable coverage at ranges of 10 miles or more. Well-designed radios include a variety of interference-combating features and can rival the performance of licensed systems in many cases. More information on spread spectrum technology is available at the Microwave Data Systems website—**www.microwavedata.com**.

**Remote Transceivers**

Let’s take a closer look at a remote station. High performance remote transceivers used in traffic control systems are physically small units designed for extreme temperatures. This, combined with their low input power requirements, make them well suited for direct mounting inside equipment cabinets at many field locations. These transceivers typically produce a nominal RF power output from 1 to 5 watts and operate on frequencies established for telemetry communication in the 200, 400 or 900 MHz bands. (Other bands may be used, depending on the country of operation.) Transmission ranges of 25 miles or more can be achieved over favorable terrain, and repeater stations may be used to extend the range, if required. Figure 2 shows a typical remote radio used for data telemetry communication.

The newest frequency range to become available for traffic control and monitoring is the 200-222 MHz band. The Federal Highway Administration (FHWA) has been assigned five narrowband frequency pairs in this range to support Intelligent Transportation Systems (ITS) nationwide. These channels, plus 200 MHz frequencies held by other license holders are available for use in traffic communications systems in many areas. This spectrum provides favorable propagation for local and metropolitan networks, and may be available in areas where other frequencies are saturated with users. Microwave Data Systems currently offers 200 MHz data communications equipment.

![Remote Transceiver](image)

**Figure 2. The MDS 9710 is a typical remote transceiver designed for use at unattended field sites.**

Remote transceivers are commonly interfaced to a logic control device (e.g., intersection controller or other Remote Terminal Unit—RTU) that accepts inputs from various sensors at the remote site. These may include inputs from signaling equipment, subsurface loops, video imaging equipment, or alarm and diagnostic devices. The Remote
station transmits its data in response to a “poll” received from the master site, or it may be configured to send data only when specified events occur at the remote location. The latter form of operation is known as report by exception (RBE) mode.

Remote stations usually employ a directional antenna aimed at the master that maximizes signal strength (both receive and transmit) and reduces the possibility of interference from stations outside the network. Poll-mounted Yagi antennas, similar to the one shown in Figure 3 are the most common type of antenna used at remote sites.

![Directional Yagi antenna commonly used at remote field sites.](image)

Figure 3. Directional Yagi antenna commonly used at remote field sites.

A low voltage DC power supply is required to provide the operating power for a remote radio. Modern transceivers typically draw less than 2 amperes of current, so the power supply need not be a large and expensive component of the system. In some cases, a transceiver can be powered from an existing voltage source at the remote site, or may even be battery/solar powered. Figure 4 illustrates a typical remote station installation with all major elements connected—transceiver, RTU, antenna and power supply.

![Remote station setup with external equipment connected.](image)

Figure 4. Remote station setup with external equipment connected.
**Master Stations**

The master station radio is usually located at a central facility where the main traffic computer is installed. The radio is interfaced to the computer through its data port, enabling traffic to be rapidly exchanged between the computer and the field sites. The computer can be programmed to generate commands in response to incoming data, or personnel can “manually” initiate commands to request data or assert a change in remote operation.

Figure 5 shows a typical master station radio. As with remote radios, master units typically provide up to 5 watts of RF power and are frequency programmable within their band of operation. There are some important differences between masters and remotes however, and these factors generally make a master radio physically larger than its remote counterpart. Some of these differences are discussed below.

Since a master radio serves as the “hub” of a data communication system, it must be available for operation at all times for the network to operate. To ensure continued operation, master radios are often equipped with redundant equipment (RF board and power supply) that automatically come online in the unlikely event of a failure in a primary unit. If this occurs, the radio continues to provide communications, but an alarm is sent to maintenance personnel so that the problem can be located and corrected.

Master stations may also be equipped with a backup battery to provide continued operation during a power failure. In most cases, the battery is kept “trickle charged” by circuitry in the radio, and is automatically switched in-circuit upon loss of normal AC power. Backup batteries may be mounted internally or externally to the radio.

Finally, master radios of recent manufacture often include some form of front panel programming and display capability. An operator with the appropriate password can read or change parameters such as transmit and receive frequencies, power levels, modem speed, etc. using a front panel keypad and LCD display. Radio diagnostics, if present, allow the user to monitor the entire radio network from a central location and adjust key radio parameters over the air. This capability is important to minimize downtime and reduce field maintenance cost.

Master stations normally employ an omni-directional antenna (see Figure 6) to provide 360 degree transmit and receive coverage to its associated remote stations. As with all antennas, the master station antenna needs to be mounted in the clear and at a
sufficient height to provide adequate coverage throughout the network. If a tall building or other support is available, the antenna can often be mounted without the need for erecting a large, expensive communication tower.

We’ve given an overview in this article of how wireless systems can be used to improve the reliability, efficiency and security of network operations. This technology is now a practical reality, and is being chosen by municipal agencies to replace older, less flexible systems. Readers interested in more information about wireless applications for traffic control, telemetry or security monitoring can contact Microwave Data Systems, 175 Science Parkway, Rochester, NY 14620 (Tel. 585-242-9600). Additional information can also be found on the firm’s website at http://www.microwavedata.com/.