Using Wireless Communications in Security Applications

Designed right, wireless links are reliable and secure

When tasked with selecting equipment to protect a site, security professionals typically choose the technologies with which they have familiarity and confidence. This makes perfect sense – no one wants to risk using unproven technology when security is on the line. That being said, new technologies shouldn't be discounted, especially if they meet performance requirements and offer distinct benefits.

A good example of this is security devices that use wireless communication. Many traditionally hard-wired devices are now available in wireless versions, including network cameras, access control devices and intrusion detection sensors. Going wireless dramatically simplifies installation and lowers costs, as technicians no longer need to physically run copper or fiber cable to each device. Some devices may also be battery or solar-powered, leading to further savings.

However, questions remain about the reliability and vulnerability to hacking of these new devices, especially given people's experiences with consumer-focused technologies like WiFi or Bluetooth. For security professionals, the key is understanding that not all wireless technology is the same and that there are solutions designed specifically for security applications.

Radio frequencies and protocols matter

Devices can use different radio frequencies and communication protocols, and these design choices impact the security of the wireless link. Most security devices use radio spectrum in the Industrial, Scientific and Medical (ISM) bands, which includes the popular 2.4 and 5 GHz bands (used by WiFi, but also by other more specialized protocols). In North America, the 915 MHz band is also available (other jurisdictions use nearby frequencies).

When making sense of product capabilities, security professionals should keep the following guidelines in mind:

- Security devices should never use WiFi. While WiFi can employ strong encryption, whitelists and other protections, the risk to critical systems is simply too high. WiFi-based devices are vulnerable to network congestion, RF interference, hacking, Internet of Things (IoT) malware, and misconfiguration. With this in mind, WiFi's convenience and user benefits make it hard to avoid and it certainly deserves its place in non-security, non-critical applications.
- Devices using the 915 MHz band typically support longer transmission distances than ones using higher frequencies, mostly due to lower RF attenuation (higher frequency signals are more susceptible to absorption and scattering caused by rain, snow, and foliage). In addition, FCC regulations allow for more powerful transmitters in 915 MHz based devices. For applications on the perimeter or in remote building locations, the maximum communication range needs to be taken into account.
- Unlike WiFi, low-power RF technologies like IEEE 802.15.4 (popularized by the Zigbee IoT protocol) are designed to work in RF congested environments and are optimized for secure machine-to-machine (M2M) communication. For low-bandwidth applications like intrusion detection or access control, this set of technologies holds great future potential and its reliability is already field-proven.

The Senstar Wireless Gate Sensor eliminates the need to run sensor or power cables onto a moving gate panel. It uses 128-bit AES encrypted communications and includes supervision mechanisms that generate alarms if the device is physically moved or damaged, or if the RF communications link is in some way compromised. It also guards against replay and cloning attacks.

Reliability, resiliency and vulnerability

Like their wired counterparts, the connectivity of wireless devices must be monitored by the security system. Communication loss should immediately be reported as a supervision alarm. This also means that the communication links must be reliable enough that operators view a communications loss as a potential threat and do not disregard it immediately as a false alarm.

ARTICLE

Consider the following scenarios that could negatively affect communications:

- Device malfunction or loss – Wireless equipment must support frequent and periodic check-ins, within tens of seconds. If the link has been compromised to the point where alarm messages cannot be sent/received, or if bidirectional communications cannot be guaranteed, the system should indicate the device is offline.
- RF jamming – There is nothing to prevent a third-party from overwhelming the radio signal used by a device. However, the effectiveness of this type of attack is short-lived on a properly designed device, as an interference alarm will be raised almost immediately. If the jamming signal is strong enough to prevent all communication, the equipment should still be declared offline based on the check-in results.

One relatively new technology, mesh networks, shows great potential in security applications. In a mesh network, each device acts as a node within a dynamic self-organizing, self-healing topology. This architecture is particularly useful for systems that use large numbers of discrete sensors located in close proximity to each other. For example, low-power intelligent fence lighting can use a mesh network for communication between fixtures.

Mesh networks provide two key benefits: first, if a node malfunctions or is physically damaged, the system adapts and remains functional; second, the network mesh extends the coverage distance, as the furthest sensor can relay its messages to the central security network via the other nodes.

Resistance to advanced attacks

Physical damage and RF jamming are the two most basic attacks against wireless devices and are easily addressed. The next question is how well can a wireless security device fare against a sophisticated hacking attempt?

First, let's look at encryption. AES encryption is used today in financial transactions worldwide and is considered highly secure when correctly implemented. When used on a security device like a fence sensor, breaking the encryption would require far greater resources than virtually any other conceivable type of attack. In addition, with the exception of network cameras that use open standards, the protocols used in intrusion detection and access control devices are typically proprietary and their short over-the-air time makes demodulation via commercial radio sniffing devices extremely difficult.

As the encryption is virtually unbreakable, would-be attackers would likely try other disruptive approaches:

- Replay attack – This attack involves recording and replaying encrypted radio traffic that is not understood in an attempt to confuse or break the system. This attack can be thwarted by including sequence checking in the underlying protocol.
- Device swapping or cloning – Device swapping consists of someone attempting to use similar equipment running on the same radio channel to trick the system into reporting the status of the shadow device instead. Properly designed equipment will limit access to whitelisted equipment
via unique identifiers embedded into the physical hardware components during manufacturing. Another, albeit difficult variation on this attack,is cloning a device to use the same identifier. In this case, two simultaneous radio broadcasts using the same identifier would result in RF interference alarms being generated.

The Senstar LM100 Perimeter Intrusion Detection and Intelligent Lighting System uses an encrypted self-healing wireless mesh network for communication between luminaires. This eliminates the need to run communications wiring along the fence. The mesh network also maintains communications if several of the fixtures are physically damaged or have their power supply cut off.

Doing more with less

Security professionals, by trade, should be cautious when using new technology to secure sites. At the same time, new technology is a driving force behind better security and enables organizations to "do more with less". Wireless security devices, when designed and deployed correctly, can maintain the highest levels of security while reducing installation and operating costs. To help decide if a given wireless security device or system is suitable for a site, ask the vendors tough questions regarding its reliability, resiliency and potential vulnerabilities.