WHITE PAPER

VIDEO SURVEILLANCE WIRELESS NETWORKING BEST PRACTICES

POWERFUL. VERSATILE. RELIABLE.

redline®
communications

TABLE OF CONTENTS

INTRODUCTION

The rapidly decreasing cost of video cameras is allowing government agencies, the private sector and military organizations to deploy video surveillance without significantly increasing their public safety and security budgets. As a result, the number of video surveillance systems is expected to grow exponentially worldwide. The vast majority of these systems will employ outdoor wireless technology. This white paper presents the benefits of using wireless and examines key issues and best practices related to deploying wireless technology for video surveillance.

BENEFITS OF WIRELESS FOR OUTDOOR VIDEO SURVEILLANCE SYSTEMS

Fast Deployment

Wireless networking eliminates the time-consuming installation of data cables. The small, lightweight radios and cameras simplify mounting requirements, making installation quick and easy.

Modern wireless equipment employs non-line-of-sight (NLOS) technology, eliminating most building-related issues and simplifying outdoor deployment.

Cost Efficient

Video surveillance saves money and uses resources effectively. For example, a prominent police department estimates that 30 cameras are equivalent to 30 surveillance officers on the street, while the central monitoring station requires only two officers.

The cost and time of acquiring rights-of-way, digging trenches, and installing and testing a wired network are prohibitively high compared to the cost of installing a wireless network. A wireless network can be operational and delivering benefits for a fraction of the time and cost.

Wide Coverage

Public safety video surveillance systems must cover hundreds of miles of road and many square miles of a city and link remote video surveillance systems to a central monitoring station. The long range and the high throughput provided by wireless (more than 80 km at 100s of Mbps) allow quick, easy and cost-effective surveillance.

Flexibility

Wireless is the leader in flexibility. You can easily move or add cameras, and you can quickly reconfigure a network to allocate bandwidth to locations requiring higher resolution images. Wireless lets you react in real time without waiting for a wired network to catch up to your needs.

CONSIDERATIONS FOR NETWORKING CAMERAS

The amount of bandwidth used by video surveillance cameras is determined by the number of cameras, the image resolution, the compression ratio, the movement or activity being monitored, and the frame rate. Clearly the more cameras you have, the more bandwidth you will use on the network. A single frame can contain from 30 kilobytes to more than 160 kilobytes for high-resolution images. At multiple frames per second (fps), each camera could easily require 10 megabits per second (Mbps), excluding any network protocol overhead. Fortunately, there are ways to reduce this.

Image Resolution

The higher the resolution, the greater amount of detail you can capture in a video image. A standard-definition TV image has a resolution of 352x240, and your PC typically 704x480. High-resolution cameras deliver up to 2592 x1944 and enable digital pan, tilt and zoom (PTZ) around an image even after the video has been stored.

As the amount of bandwidth required rises with image quality, it is best to find a level that meets your needs.

Compression

Video compression is an important tool for easing strain on a network. It allows high-quality video transmission without hoarding bandwidth. Video surveillance systems typically use MJPEG, MPEG-4 or H.264 compression technology. Your choice depends on your application and your needs. MPEG-4, which provides better compression but lower resolution, is usually used when you need to conserve bandwidth and storage. MJPEG compression is usually used by the higher resolution cameras and offers the advantage of very clear screen shots when a photograph is preferred over a video clip. H.264, the latest compression technique, offers an excellent trade-off between quality and bandwidth. H.264 provides about twice the compression of MPEG-4 for the same video quality.

Movement and Activity

Modern compression algorithms work by comparing the differences between frames, which means the bandwidth requirement is directly related to motion in the monitored area. For example, monitoring a static scene requires less bandwidth than monitoring traffic or a public area where there is a lot of motion. The latter requires higher network bandwidth because the compression rates are low.

Frame Rate

The number of fps relates to how smooth motion appears in the video. Standard TV runs at 30 fps, providing excellent motion but at a high bandwidth cost. Fortunately, in most video surveillance applications, there is little motion. For example, a frame rate of four fps would be sufficient for a person walking through a room. Many cameras minimize bandwidth by increasing the frame rate only when motion is detected.

The Bottom Line

Due to the many factors that contribute to video bit rate, there is no exact method to calculate total bandwidth requirements. Each camera manufacturer and each encoder model has different requirements, and every installation introduces unique variables.

Most wireless video surveillance systems are installed outdoors. Weather conditions, topography, line-of-sight conditions, and interference spectrum impact the amount of bandwidth on a given link. Careful planners provide an additional 20 per cent bandwidth to mitigate the impact of these variations.

The following charts provide a starting point for planning a camera network:

Resolution	Image Rate	Activity Level	Bit Rate (Kbps)
CIF	30	Medium	500
2CIF (352x288)	3	Medium	320
2CIF	7	Medium	370
2CIF	15	Medium	400
2CIF	30	Medium	1,000
4CIF (704x576)	3	Medium	640
4CIF	7	Medium	740
4CIF	15	Medium	800
4CIF	30	Medium	2,000

Table 1: Typical CIF to 4CIF Bandwidth Requirements

Compression	Megapixel	Resolution	Image Rate	Bit Rate (Mbps)
H.264	1	1,280 x 1,024	5	0.7
H.264	2	1,600 x 1,200	5	1.03
H.264	3	2,048 x 1,536	5	1.6
MJPEG	1	1,280 x 1,024	5	4.7
MJPEG	2	1,600 x 1,200	5	6.2
MJPEG	3	2,048 x 1,536	5	9.6
H.264	1	1,280 x 1,024	15	2.0
H.264	2	1,600 x 1,200	15	3.8
H.264	3	2,048 x 1,536	15	4.8

Table 2: Typical Megapixel Camera Bandwidth Requirements

WIRELESS IS DIFFERENT

Security in an “Open” Medium

Wireless is an open medium, which means others could easily listen in if precautions are not taken. For example, many Wi-Fi networks are unsecured allowing easy connection of your laptop. It is critical that any wireless network used for video surveillance have sufficient encryption and authentication controls to prevent unauthorized persons from seeing images of your operations, your people or your customers.

Camera Operation Impacts Wireless Performance

Most of the time, video surveillance cameras watch a static scene. During periods where little or no motion is detected, the cameras send very little information over the network. However, when a large amount of motion or a major change in a scene occurs, the amount of data sent can skyrocket, resulting in what is called a data shower. Wireless networking gear that does not include data shower caching will drop frames, potentially losing the most important moments of an incident.

Latency

Latency in wireless can be quite high compared to a wired network. For real-time applications such as video, latency can result in lost detail or a jumpy or pixelated picture. High latency will also make PTZ camera operation difficult or frustratingly slow. If your wireless video surveillance network carries other applications such as voice or control system data like SCADA, then high latency can result in expensive and time-consuming reconfiguration and testing, in some cases making the application unusable.

Throughput

When designing the wireless network for video, the question will arise of how much throughput (sometimes called bandwidth) is needed and more throughput always translates into more radios. Getting a solid estimate of throughput requirements up front will ensure excellent performance within budget.

All radio manufacturers specify throughput; however, it is critical to understand how it is measured. Most manufacturers specify throughput using only large packet sizes, which inflates the throughput available. For example, a radio processing 1,500-byte packets might have a throughput of 48 Mbps. However, the same radio processing 60-byte packets might provide less than 2 Mbps. Since the compression process results in varying packet sizes, selecting radios that provide consistently high throughput under varying packet sizes is critical.

Management

Network management tools used in wireless networks are similar to those used in wired networks, except that wireless network management tools must be capable of providing over-the-air (OTA) management, not only for configuration and monitoring but also for software updates. Being able to update or load new software OTA is critical for maximizing uptime while minimizing support costs.

Comprehension Challenges

From an engineering perspective, wireless is harder to understand. Instead of a simple wire that provides a huge amount of throughput regardless of most other conditions, wireless is teaming with jargon and changing operating conditions affects performance. You need to understand the geography of the installation in relation to the characteristics of radio frequency signals. You need to understand that leaves, rain, fog, snow, buildings and nearby wireless users all provide interference that can degrade video quality. All of this means that wireless systems must perform additional functions to ensure fair and efficient use of the wireless link. It is all about balancing performance and reliability in varying link conditions (fading, distance, movement).

AVAILABLE TECHNOLOGIES

Wi-Fi

Most people are familiar with Wi-Fi. It is the wireless network of choice for indoor Internet access for laptops and PCs, as its cost is low and it provides high bandwidth; however, Wi-Fi networks have a limited range of 70 meters (230 feet). 802.11 uses Carrier Sense Multiple Access (CSMA) to determine when a node can send data. Each node listens to the link to make sure it is clear before sending. If the channel is not clear, the node waits for a random period of time before retrying. The upshot is that latency — the delay in sending video images across the network — is long and variable. To reduce latency to a suitable level, traffic loading must be controlled by reducing the number of cameras on each node, so that the cameras consume less than 30 to 40 per cent of the total available bandwidth. As the network grows, latency will increase and become more variable. As mentioned earlier, latency can be harmful to real-time applications such as video surveillance. The ability to allocate bandwidth ensures images will not be lost or delayed. However, the CSMA protocol makes this difficult. While there are schemes to address this, the typical Wi-Fi approach is to design the network with significantly more bandwidth than the cameras actually need.

In short, Wi-Fi networks do not scale well and are better suited to small systems with few cameras.

Mesh

Mesh networks are based on the 802.11 Wi-Fi standards. Although Wi-Fi is designed for indoor use, creative vendors have adapted the ready-made Wi-Fi chip sets to work outside.

Each node in a mesh network connects to each of its neighboring nodes as shown in Figure 1. Each node communicates regularly with its neighbors to create routing tables that tell the node how to route video through the mesh. This makes mesh networks very flexible and resilient as they automatically reconfigure routing as new nodes are added or if a node fails. However, designers and operators of large networks often do not want their networks to be dynamically changed. They prefer to build reliable links, with consistent performance, and have those links remain fixed, stable and, in particular, measurable.

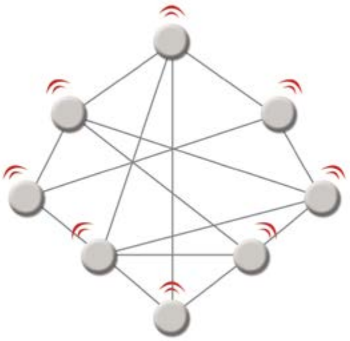

Figure 1: Mesh Network

Additionally, because it is 802.11-based, mesh suffers from the same issues as Wi-Fi, that is, high variable latency and an inability to allocate bandwidth. Mesh radios are available in two configurations: single radio and dual radio. Single radio mesh nodes do not scale well as they use the same radio for uplink and downlink. On the other hand, dual radio mesh nodes use a different radio for uplink and downlink, so they scale well up to mid-size networks supporting several tens of cameras. However, dual radio mesh nodes cost significantly more and can be harder to install.

WiMAX

WiMAX is a wireless digital communications system intended for broadband wireless access up to 50 kilometers or 30 miles for fixed stations, and 5 to 15 kilometers (3 to 10 miles) for mobile stations. Designed primarily for wireless telecommunication service providers, WiMAX operates on both licensed and non-licensed frequencies, providing a regulated environment and a viable economic model for wireless carriers.

While WiMAX provides Wi-Fi-like data rates, it provides significantly better coverage and quality of service (QoS) controls.

Although suitable for low- to mid-performance video surveillance, WiMAX is designed to deliver high downlink rates and low uplink rates, the opposite of the requirements of what high performance video surveillance networks require. Further, WiMAX has quite large latency, in the order of 20 – 40 msec, which can impact video quality.

Specialized

Specialized networks are specifically designed to provide high-capacity, high-performance, wide-coverage networks that support hundreds of cameras, including high-resolution cameras. These wireless networks are typically based on a high performance wireless standard such as 802.16, the basic air interface technology used in WiMAX and LTE, but with additional hardware and software specifically designed for video surveillance.

The use of 802.16-based networks provides important characteristics for video surveillance networks:

1. Fixed amounts of bandwidth can be allocated to each camera to guarantee video images will be transmitted regardless of network traffic loading.
2. Latency is low and not variable. High latency can be disastrous for video surveillance, making camera control functions such as PTZ frustratingly slow, and making advanced video surveillance functions such as license plate recognition completely unusable. With constantly low latency, network designers are assured of consistent performance despite significant variations in traffic loading.
3. The routes are fixed. Images from cameras always take the same route, which ensures consistent performance over all operating conditions and as the network grows.
4. Specialized networks scale well. The radios are used in point-to-point (PTP) and point-to-multipoint (PMP) configurations to build networks that scale very well for large area coverage with many cameras, much like a cell phone network. They have deterministic performance and a hierarchical structure. Thus, adding more cameras does not impact the performance of existing cameras.
5. Memory allocation and processing power can be increased to accommodate the "bursty" nature of data compression. Data showers during high-activity periods can often overflow the memory buffers of standards-based radios.

SELECTING THE APPROPRIATE TECHNOLOGY

Choice is driven by price Versus performance. Consider the following questions:

1. Is your network outdoors?
2. Are you monitoring high-activity areas such as an airport, a shopping mall, or traffic?
3. Do you need high-resolution cameras?
4. Will you be using video analytics and PTZ cameras?
5. Will you be expanding from a few cameras to a large number?
6. Do you need to cover a large area?
7. Is the topography difficult?
8. Will your network carry other applications?

No two video surveillance networks are alike, making it difficult to choose the best technology.
The following scenarios may help you determine the correct network for your needs.

If your application is completely indoors and uses a few tens of mainly low-resolution cameras, then Wi-Fi is a very good choice. Wi-Fi is low cost, easy to install and to maintain and provides reasonable coverage.

Wi-Fi or mesh is a good choice for simple video monitoring of a store's perimeter, a parking lot, and so on. These applications typically use a few 10s of cameras at lower resolutions. They can easily be accommodated by Wi-Fi or mesh, which are low cost, provide reasonable area coverage and are easy to install and manage. Additionally, mesh allows you to extend coverage around buildings and other obstacles due to its self-learning capability.

For mid-size systems with several tens of cameras in an all-outdoor application, you need to consider networks that can cover a wider range and that support higher bandwidth. WiMAX and dual radio mesh may be a good solution. The extra performance provided by these networks will cost more; however, they are reliable and easy to manage. The downside of WiMAX and mesh is their high latency, which limits performance (jumpy video, pixilation) and may prevent the addition of other real-time applications such as voice or data acquisition (SCADA).

For large all-outdoor systems that have hundreds of cameras over a wide area, the specialized wireless network is a very good choice. The radios in these networks were designed from the start as an outdoor solution and guarantee performance over a wide range of operating conditions, in harsh environments and in difficult weather conditions. The low latency and high bandwidth ensure PTZ cameras and video analytics perform as expected. Specialized wireless networking devices carry more cameras per subscriber station, thus keeping the overall network cost low. Some wireless network suppliers test their products with cameras from the major camera suppliers for added assurance that your system will work right out of the box. To improve picture quality, some manufacturers include specialized software that improves error correction performance and data shower caching for better video quality.

For all-outdoor systems with high resolution or megapixel cameras, the specialized wireless network is the best choice as it supports several high-resolution cameras per subscriber station and covers large ranges easily.

A word about high-quality video: in some jurisdictions, law enforcement requires a printed photograph to obtain a conviction. Since clear screen shots require MJPEG compression, specialized wireless networks are the only choice for these applications. Protection of vital assets, site security, industrial safety and military applications are other areas where specialized networks may be required to provide high-quality video.

Consider other applications today and tomorrow. If your wireless network needs to carry other real-time applications, or you expect the network to grow significantly in terms of numbers of cameras and quality of resolution, then specialized wireless networks offer the ultimate in future-proof protection.

Should you mix technologies? In some case, this makes sense. For example, 2.4 Ghz Wi-Fi is well-suited for indoor use and it can propagate very well through walls. Combining Wi-Fi with a specialized network to cover all your facilities inside and outside may be the best overall solution. Similarly, combining mesh and specialized networks may produce a good trade-off in local flexibility for coverage and performance. On the other hand, staying with a single supplier makes a lot of sense.

RECOMMENDED BEST PRACTICES

Project Management

This is likely familiar to you, but it bears repeating:

- Finalize requirements as early as possible. This may compromise flexibility, but it eases comparison of vendors and solutions. Or consider finalizing key requirements, leaving others open for suggestions from vendors.
- Talk to multiple vendors to get different viewpoints, learn the latest trends and validate your thinking.
- Work with professionals such as VARS and system integrators who have successfully completed wireless video surveillance systems in your business arena.
- Seek references. It is not always easy to determine a quality vendor from brochures and sales people. While vendors give you the names of their best customers, it is worth introducing yourself, talking to references directly and seeing their solutions first-hand.
- On larger projects, try to visit an existing wireless video network that has many of the same requirements and challenges as your project at hand.

Think about the Future

Cameras will continue to have higher resolution. You will need more cameras in more locations. You will think of more uses for video. Vendors will come up with more video applications. Do not build a network infrastructure that will require changing later. Even at a few thousand dollars per wireless node, additional wireless capacity is far less costly to install early on than replanning your wireless network at a later date.

Conduct a Spectrum Analysis

Failure to conduct a spectrum analysis to identify available bandwidth and potential interference over the area to be covered can lead to poor performance and expensive corrections later on, particularly for unlicensed radios, which are the majority of radios used in video surveillance.

Test and Configure before Deployment

Ensure the cameras you select are tested over the wireless gear you want to use. Preprogramming radios before installation in the field avoids employing bucket trucks to make adjustments in the field.

Ensure Security

Make sure the radios support encryption and authentication – at least AES-256 and private-key authentication. The security features should be certified by a third party; for example, selecting a FIPS 140-2 certified radio ensures it has been independently tested. Remember, wireless is an open medium – others can easily see your unprotected images. Not only could you lose proprietary information, you may also inadvertently violate a person's privacy. Ensure the product's network management interface can be protected by user name and password authentication.

Match Specifications to the Application

For all-outdoor applications, make sure the radios are IP67 certified or better. In marine environments, ensure the equipment and in particular the connectors will not deteriorate under salt spray.

GLOSSARY OF TERMS

NLOS Non-line-of sight refers to a radio transmission across a path that is partially obstructed.

MPEG-4 / H.264 MPEG (Moving Pictures Expert Group) and H.264 is a collection of methods defining compression of audio and visual (AV) digital data.

MJPEG MJPEG (Motion Joint Photographic Experts Group) is the name for a class of video formats where each video frame or interlaced field of a digital video sequence is separately compressed as a JPEG image.

fps Fps (frames per second) is the frequency (rate) at which an imaging device produces unique consecutive images called frames.

CIF CIF (Common Intermediate Format), also known as FCIF (Full Common Intermediate Format), is a format used to standardize the horizontal and vertical resolutions in pixels of analog YCbCr sequences in video signals

SCADA SCADA stands for supervisory control and data acquisition. It refers to industrial control systems that monitor and control industrial, infrastructure, or facility-based processes.

CSMA CSMA (Carrier Sense Multiple Access) is a probabilistic Media Access Control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium such as a band of the electromagnetic spectrum.

QoS QoS (Quality of Service) is a traffic engineering term that refers to resource reservation control mechanisms used to provide different priority to different applications, users, or data flows, to guarantee a level of performance to the data flow.

Wi-Fi Wi-Fi is a trademark of the Wi-Fi Alliance. A Wi-Fi enabled device such as a personal computer can connect to the Internet when within range of a wireless network connected to the Internet.

WiMAX WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunications protocol that provides fixed and mobile Internet access.

LTE LTE (Long Term Evolution) is the latest standard in the mobile network technology tree.

802.16 IEEE 802.16 is a series of Wireless Broadband standards authored by the IEEE.

802.11 IEEE 802.11 is a set of standards for implementing a wireless local area network (WLAN).

AES AES (Advanced Encryption Standard) is a symmetric-key encryption standard adopted by the U.S. government.

FIPS FIPS (Federal Information Processing Standard) is a U.S. government computer security standard used to accredit cryptographic modules.

IP67 IP (International Protection) code consists of the letters IP followed by two digits and an optional letter classifies the degrees of protection provided against the intrusion of solid objects (including body parts like hands and fingers), dust, accidental contact, and water in electrical enclosures.

ABOUT REDLINE COMMUNICATIONS

Redline Communications (www.rdlcom.com) is the creator of powerful wide-area wireless networks for the world's most challenging applications and locations. Used by oil and gas companies, militaries, municipalities and telecom service providers, Redline's powerful and versatile networks securely and reliably deliver M2M, voice, data and video communications.