Why the Future of Public Safety Will Rely on **Wireless Mesh Networks**

Despite the disparate nature of public safety threats, there are common needs shared by all stakeholders who work within the public safety sphere.

Brian Higgins, CPP, CSSP, President of Group 77 LLC

RAJANT

Table of Contents

Introduction

Why public safety leaders are turning to wireless mesh

Homeland Security, law enforcement, emergency management, first responders, physical security professionals, computer and IT security experts, firefighters; these and so many others play a critical role within the multi-faceted public safety sector. Despite the disparate nature of public safety threats, which range from the most serious of incidents like natural disasters and terrorist attacks to more mundane issues such as crowd control, there are common needs shared by all stake-holders who work within the public safety sphere. Across all scenarios, a successful response relies on accurate real-time situational awareness combined with accessible and reliable communications. These cannot happen without access to a robust, highly-secure network that is easily deployed and managed, offers fail-safe redundancy, delivers the speed and bandwidth to support all necessary systems and communication channels, and—of course—is affordable.

This white paper will address why, given these requirements, CSOs, CIOs, CTOs, public safety leaders, and decision-makers are increasingly turning to wireless mesh to support their mission-critical needs.

New Technologies, New Possibilities

Addressing evolving concerns

Just as public safety concerns evolve, so do the plans and programs devised to address them. Today, those plans include a new generation of technology that changes how public safety officials do their jobs, allowing them to be more proactive and responsive. We find an increasing use of drones and robotics within our clients' public safety plans, to facilitate surveillance and the execution of security and communications-related tasks.

Security cameras are no longer just static devices mounted at a fixed location. In addition to body cams, we are now seeing cameras mounted on drones and integrated within roving security robots. More importantly, they are not just recording locally. We can transmit full-frame, high-resolution video back to a security operations center where video from those moving assets can be viewed, managed, and searched just like any other camera. When you are dealing with large outdoor events, having access to this type of live video provides security and safety teams with an unprecedented level of situational awareness, informing every decision they make and action they take.

Drones and robots are also useful for other purposes. They can help handle tasks or enter areas that would be unsafe for humans. For example, a human-controlled robot could be part of a HAZMAT team (hazardous materials), used to disarm and dispose of hazardous packages or materials.

Another growing technology in public safety applications is high throughput scanning, whereby individuals no longer have to pause as they pass through a checkpoint. Examples include metal and explosive detection systems placed at building entrances, facial recognition software to automate access control and, now with COVID-19 concerns, thermal surveillance cameras that scan crowds to identify individuals with elevated temperatures.

There is also the proliferation of IoT applications. Parking meters to flood sensors, air quality monitors to medical devices, today, countless IoT devices are feeding a torrent of data into public safety systems.

These solutions are gaining traction so quickly because we now have networking options to support them. Mobility is a major driver. In some of these examples, you could go with a cellular connection, but when you're dealing with the amount of data these systems transmit, multiplied by a large number of devices, that gets expensive very quickly. From a networking perspective, it also creates a jumbled, disjointed solution. By contrast, wireless mesh creates a cohesive network with no recurring subscription or data use fees, is easily scalable, and can be quickly deployed to provide consistent, reliable coverage over areas of any size and topography. For the public safety sector, this makes wireless mesh a game-changer.

How It Works

Wireless mesh provides consistent, reliable access

The purpose of wireless mesh is to provide consistent, reliable access across an entire space. Instead of relying on a few network gateways or access points, which provide variable coverage, wireless mesh makes use of a network of nodes spread across an entire area, each located within communication distance of others. Mesh networks can be any size, from under ten nodes to several hundred.

To be clear, all mesh networks are not created equal. You need to look for one that allows data to travel across the mesh network, hopping from node to node, always seeking the best path and rerouting as necessary. The rerouting is based upon signal strength, bandwidth requirements, competing network traffic, and other factors. This “self-healing” process of superior mesh results in built-in redundancy. Many wireless mesh solutions support multi-frequency, multi-transceiver transmissions, mitigating the effects of RF interference.

Some wireless mesh networks provide additional capabilities. I learned this firsthand while consulting on a security robotics project a few years back. Namely, Rajant’s Kinetic Mesh® enables machine-to-machine (M2M) connectivity, by which mobile assets accessing the network are transformed into functional nodes themselves, fortifying an existing network with additional, fluid connection points or creating a new network where none existed. For example, a fleet of police cars, each equipped with a Rajant BreadCrumb® radio transceiver, can instantly create a network of nodes encircling an emergency site. Officers, firefighters or other first responders, outfitted with compatible radio transceivers on their bodies, can expand that network, facilitating transmission of video, audio, and data communications back to those police cars. Furthermore, the Rajant solution can communicate with satellite, LTE, 3G/4G, fixed wireless, and Wi-Fi networks that may also be available. This combination of flexibility, reliability, and ease-of-deployment makes wireless mesh ideal for applications that require mission-critical communications between multiple task forces.

Key Considerations: When we think about network requirements for public safety applications, there is "a continuum of needs." Long-term, permanent requirements, short-term, planned pop-up events, and completely unplanned situations, each pose unique challenges. However, in all instances, certain non-negotiable criteria dictate the choice of broadband networking options. These include security, ease-of-use, reliability/redundancy, scalability/flexibility, and cost. Compared to alternatives, wireless mesh performs consistently well.

Security: When dealing with the public safety sector, the first concern that comes to mind is security. Whenever we talk about cabled, hardwired systems, as opposed to wireless, people immediately assume the wireless is somehow less secure—that it's more hackable. That's a misconception we need to address.

The security of a network is a combination of the cryptographic solutions it employs as well as the degree to which system administrators adhere to best practices, such as password management. This pertains equally to hardwired and wireless mesh networks.

When advanced encryption and authentication algorithms are engineered within each node of a wireless mesh solution, network security is far more of a "given" than it is within hardwired networks, for which system administrators must be actively vigilant in addressing cyber-safety threats.

Cryptographic solutions will vary by wireless mesh manufacturer. Still, solutions are available that deliver the highest levels of security, including those used by the DoD for the most sensitive and secure communication systems. For example, Rajant Kinetic Mesh features AES 256-bit security and FIP's 140-142 compliant military-grade encryption. It is also HIPAA compliant, making it suitable for a wide range of healthcare applications.

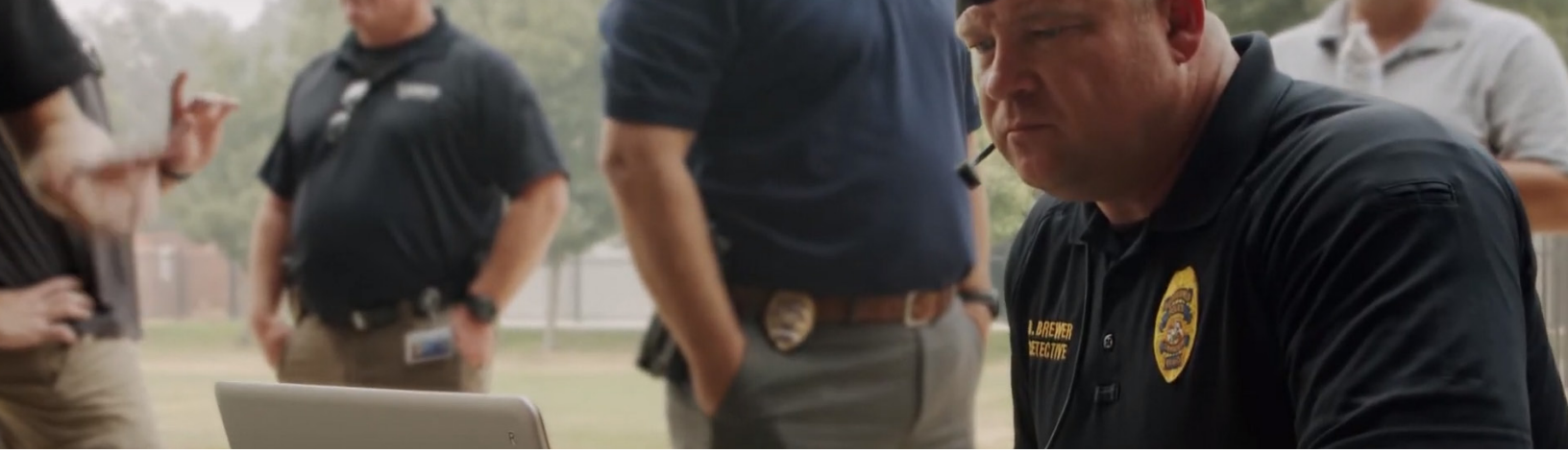
Ease-of-Use

Extremely important when every second counts

When evaluating technology for use in public safety, the second question that comes up almost immediately is, “How easy is it to use?” The IT people are very much involved in looking at networking issues, and there’s a perception that wireless mesh is difficult to put together, to operate, and that it’s just overall labor-intensive. That may have been true ten years ago, but it’s certainly not the case anymore.

As with any type of network, an IT professional must handle the initial system configuration of a wireless mesh. However, once that’s done, it is straightforward to break down and then re-setup. Nodes can be swapped in or out as needed, and the network automatically adjusts; everything autonomously connects with each other.

For systems like Rajant’s, which offer mobile, M2M connectivity, nodes can be assigned to changing assets, as needed. For example, this week, a radio transceiver might be attached to a camera as part of a temporary video surveillance network. Next week, it might be deployed as part of a public address system. As long as network configurations remain constant, no IT professional is needed to reuse the transceiver in a different setting or to reassign it to a different asset. This ease of set-up is beneficial at any temporary event but is extremely important in emergency scenarios where every second counts. With wireless mesh, public safety officials can arrive at a scene and, within minutes, have a secure, multi-channel, broadband network up and running, capable of sharing video, audio, and data between all invested parties.



Reliability, Redundancy, and Low-Latency

A network must be 100% trustworthy

Reliability, redundancy, and low latency—these matter a great deal in public safety. In mission-critical applications, you obviously can't have signals dropping, audio breaking up, and video acting glitchy. The network must be 100% reliable. Network configurations that ensure redundancy, sufficient bandwidth, and low latency transmission contribute to that reliability factor.

The decentralized topology of wireless mesh creates inherent redundancy, although not all systems are created equal. In traditional wireless networks, you might have a system with multiple controllers and up to 60 nodes connecting to each switch. If a node goes down here or there—no problem. Data is rerouted. You have redundancy. However, if a controller goes down, so does everything beneath it, wiping out a chunk of the network. By contrast, wireless mesh systems that offer a true peer-to-peer solution are free of all gateways. Each node is engineered with its own full routing capabilities in these systems, eliminating any possible single-point-of-failure. This level of redundancy is a huge advantage for public safety applications.

Reliability is further enhanced by support for a wide range of frequencies, including the 4.9 GHz public safety band and other licensed frequencies. Surveillance video, analytics data, voice communications, financial transactions—each can transmit over a different frequency, ensuring that every connected system has adequate bandwidth to maintain uninterrupted connectivity and optimal performance. Transmission is also fast. Because communication between systems and devices remains within the closed network, latency is far less than if communication is needed to access cellular towers or the cloud to get from Point A to Point B.

Scalability and Flexibility

Planning for the unexpected

The nature of public safety involves planning for the unexpected. A seemingly isolated incident, initially responded to by a single agency, can quickly escalate into a community-wide threat. A network that seamlessly scales up as needed, to support the communication and logistical needs of a widespread, multi-force response, is crucial for a successful, coordinated effort.

Compared to wired networks, it is far easier to expand accessibility to a wireless mesh system; you just add nodes. However, while traditional mesh networks degrade as nodes are added, the opposite is true of the newer generation of peer-to-peer networks. In these systems, each additional node actually reinforces the networks' overall connectivity, resulting in tremendous scalability. Networks can efficiently function with many hundreds of nodes.

In such systems, nodes can be added anywhere to both fixed and movable assets. Lightweight, compact transceivers within ruggedized enclosures can be deployed truly anywhere, regardless of environmental conditions. As assets move, their radios automatically detect and connect with nearby nodes, only disconnecting with one when another connection has been established. Practical applications for mobile connectivity include assigning transceivers to drones, robots, police and emergency vehicles, public transit, road maintenance and construction vehicles and assets, cargo containers, body cams, and much more.

Cost

Delivering real value

For budget-conscious municipalities and government agencies, a wireless mesh is particularly attractive when evaluated in terms of total-cost-of-ownership. Mesh networks involve a one-time purchase, with no perpetuating licensing or data-use fees. Full scalability allows customers to buy as many transceivers as needed for immediate use, with the option to add more over time. As nodes can be repeatedly repurposed, a single network can be useful for countless situations or events, with each node capable of supporting the transmission and connectivity needs of any type of asset.

Wireless mesh also reduces the overhead required for IT support. Cyber-security is hard-baked into the system, and, as mentioned earlier, configurations can be left in place across successive deployments as long as the LAN consistently connects back the same network.

Wireless mesh preserves the value of legacy solutions that may still make sense for specific connectivity requirements. It seamlessly integrates with Wi-Fi, LTE, and wireless point-to-multipoint systems, extending the network's reach beyond the mesh perimeter and eliminating the unnecessary expense of replacing functional systems.

When evaluating wireless mesh in light of all these considerations, it's a technology that delivers real value from a budgetary perspective.

Wireless Mesh in Action

Leveraging wireless mesh to its optimal capabilities

Based upon experience as a former Public Safety official and now, as a consultant to municipalities, public safety agencies, and other stakeholders, there is a range of scenarios in which wireless mesh could be leveraged to its optimal capabilities.

Emergency Management: Emergency management requires immediate, seamless inter-agency communications. Picture the devastation after a hurricane as an example. Emergency response must span a huge, multi-jurisdictional area. A fleet of drones, equipped with video cameras and remotely operated by law enforcement or homeland security, could assist with search and rescue operations, quickly identifying locations where civilians might be trapped. Rescue personnel, directed to those sites, could have access to the live video streams, as well as audio communications with medical personnel, firefighters, water-rescue, and other first responders. EMS vehicles could transmit patient data back to hospital emergency rooms, allowing staff to be better prepared for triage and treatment upon arrival. Thermal cameras could identify downed lines, gas leaks, and other hazardous conditions requiring attention. Responding HAZMAT teams and utility crews could explore those sites with remotely controlled robots that could be used to assist with dangerous operations. Dispatched FEMA trailers, tasked with coordinating response efforts, could have access to vital internet access, as well as clear, secure communications across narrow band and wideband public safety channels.

Large Scale Events: Imagine a large music festival staged in a rural setting, far from any municipal infrastructure. A wireless mesh network, easily set up prior to the event, could support everything from security operations, to preplanned gathering management technologies, to credit card transactions at point-of-sale kiosks. For example, a pop-up Security Operations Center could receive live video feed from cameras set up across the grounds, data from access turnstiles and visitor screening technologies, and – an unfortunate necessity in this day and age—alerts from gunfire detection sensors capable of identifying and geolocating gunshots. Temporary blue-light kiosks could be enabled, allowing concert goers to summon assistance for medical or other emergencies. Public address systems could be

supported. And, leveraging transceiver radios placed on each security staff team member, a dynamic map could display, in real-time, the location of each officer as they move around the property, making logistical coordination much easier.

Public Safety Services in Sprawling Suburban and Rural Areas: Today's cities often have permanent broadband infrastructure in place, combining wired and wireless, that can be tapped into by public safety agencies, but the farther you get beyond the city limit, the less likely that this infrastructure exists. Wireless mesh, and particularly wireless mesh that supports M2M connectivity, is ideal for these settings. A combination of permanently mounted nodes, spread throughout the community atop light poles or other structures, can form the foundation of such a network, with additional nodes placed within other permanent and movable assets. As moveable assets enter the geographic area supported by the wireless mesh, their communications would automatically switch over to leverage the network. In addition to the apparent communications benefits discussed in previous examples, M2M wireless mesh opens up other interesting possibilities. For example, public buses equipped with onboard security cameras would no longer have to wait until they returned to the depot to download the recorded video to the central monitoring platform. The high-speed, low-latency connection offered by wireless mesh, combined with free, unlimited data transmission, would allow those cameras to be remotely monitored and recorded in real-time. Road crews would also have access to the network, allowing them to manage temporary electronic signage or transmit data from their construction vehicles and laptops. Temporary COVID-19 test sites in parks and parking lots could communicate with far-away hospitals and coordinating state agencies, sharing patient data in real-time while complying with HIPAA data privacy requirements.

Summary

Not all wireless solutions are alike

The connected solutions fundamental to today's public safety initiatives require a broadband network that can be trusted to deliver in the most mission-critical situations. Today's latest generation of mobile, M2M wireless mesh offers many advantages over other networking options. From a functional perspective, these include cybersecurity protocols that ensure secure, military-level communications, a highly-redundant topology, multi-channel, high-throughput support, and complete flexibility and scalability. Operationally, wireless mesh is easy to manage and deploy quickly while delivering superior performance at a very competitive total-cost-of-ownership.

Remember that not all wireless solutions are alike. Specifications relating to bandwidth, redundancy, M2M support, physical size, weight, durability of node enclosures, and other factors will vary by manufacturer. When exploring options, look for systems that will not only serve your immediate needs but your vision for years to come. With the help of wireless mesh, the possibilities are limitless.

***Mr. Brian Higgins**, CPP, CSSP, is President of Group 77, an independent security consulting company offering clients a holistic approach to security plan development and training. Previously, he served as Chief of Police and Director of Public Safety for Bergen County, New Jersey. Higgins is an adjunct faculty member at John Jay College, where he teaches courses on emergency planning, emergency management, retail and commercial security, and homeland security.*