LEVERAGING ROBOTICS TO ENHANCE INDUSTRIAL SECURITY & PUBLIC SAFETY WITH the Help of Wireless Mesh

Autonomous robotic solutions are expanding the role that technology plays in enhancing security and public safety while creating operational efficiencies and cost savings.

Paul Benne, PSP, CPOI, Founder & President of Sentinel Consulting

RAJANT

Table of Contents

Interest in Robots is Growing

New networking options are a significant factor

While still a relative novelty, robotic and autonomous solutions have made recent inroads within security and public safety applications. By now, we've all seen them in action, if not firsthand, then in the media: robots patrolling parking lots and shopping malls; drones flying over sporting events and crime scenes. Still, widespread adoption has been challenging. Robotic solutions are perceived as expensive. They can be unresponsive or unreliable due to connectivity issues. And security management often remains hesitant to deploy robots in a thorough security posture due to trepidation over how employees and the public may respond to them.

Nevertheless, the tide is turning. Artificial intelligence and machine learning are making robots smarter, more autonomous, and more fluid in their ability to anticipate and respond to situations at hand. The pandemic has exposed new operational challenges that could be more effectively addressed by augmenting human resources with robots – options that will certainly be explored once organizations have time to take stock of their "new normal" and evaluate technologies. Most importantly, innovative, cost-effective, and highly reliable wireless mesh networks are making the deployment of mobile robotics possible in a vast range of settings where other options are prohibitively expensive at best, inaccessible or unreliable at worst.

Mobile Technology Offers Many Benefits

Keeping it connected is crucial

At the most basic level, today's robots are computers placed on mobile platforms. Sometimes they are used in a sentinel mode, stationed at doorways or tethered in the air, but they deliver the most value when organizations have the flexibility to move them around as needed. When it comes to planning for security deployments, technological mobility is a paradigm-changer. Hundreds of detection points, cameras, and sensors can be replaced with far fewer mobile, autonomous solutions covering the same territory. Robots themselves may be costly, but their expense is fractional compared to the overwhelming amount of infrastructure necessary to support permanent security devices.

When CSOs evaluate technology options, their foremost consideration is "How will this solve my problem?" CTOs' concerns over "How will this work?" deserve equal weight. The method by which robots connect and communicate across the network is fundamental to their viability and overall cost. Technological challenges and performance limitations can render them untenable, regardless of the robots' capabilities and features. Wireless mesh, which enables highly secure, fluid communications between hundreds of devices, including those in motion, alleviates a broad swath of stakeholders' concerns.

The greatest challenge in supporting robotic and autonomous solutions is keeping them connected. Wireless mesh networks are unique in their ability to provide consistent, reliable coverage across virtually any space, regardless of the property's size, topography, physical obstacles, RF traffic, and weather conditions. There's no digging of trenches to lay power or a wired infrastructure; no strategic positioning of gateway access points for devices to connect through.

Instead, the network comprises any number of radios, or nodes, that automatically identify and transmit to others within range, continually adjusting to find the fastest and most stable connections. Data is rerouted based on changing conditions, including signal strength, competing traffic, bandwidth needs, and other factors.

For robotic and autonomous solutions, where mobility is of critical importance, Rajant Kinetic Mesh goes a step further, offering machine-to-machine (M2M) connectivity and dual radios for alternative pathways to send and receive. In such networks, mobile assets are each equipped with a transceiver. As a result, their connection to the network supports their own communication and strengthens the network by creating new data pathways. Plus – particularly relevant for drones and robots—as these assets move, so does the network supporting them.

Wireless Mesh Delivers on All Fronts

From optimized performance to reduce overall cost

How does wireless mesh measure up compared to other networking options? It is superior in almost every way to support unmanned ground vehicles, drones, and other robotic devices.

Security: The risk associated with a hacked robotic security device is two-fold; bad actors could compromise its sensing and reporting capabilities, but they could also interfere with its physical operation, causing harm to those in its proximity. Wireless mesh is a very secure technology, a top consideration for decision-makers tasked with protecting their businesses' networks.

Rajant Kinetic Mesh features AES 256-bit security and FIP's 140-142 compliant military-grade encryption. It is also HIPAA compliant. All transmission occurs at Layer 2, with no IP addresses assigned to individual devices. Opportunities for successful cyberattacks are practically non-existent.

Reliability and Redundancy: For the challenges of supporting drones and robots, system engineers have traditionally turned to either cellular or wireless point-to-point solutions. Both have drawbacks.

Cellular is not an option everywhere. There are still plenty of locations that suffer from "one-bar service," places where an autonomous solution's data demands cannot rely on cellular. Even where coverage is strong, service may be inconsistent during times of heavy traffic. Mission-critical security systems require better than this.

Point-to-point wireless also poses limitations. Unlike the completely decentralized, peer-to-peer topology of wireless mesh, point-to-point wireless relies on communication towers that serve as communication gateways. An unobstructed line-of-site between towers and supported devices must be maintained. For mobile solutions, point-to-point is much more temperamental in establishing and maintaining its connection; device connectivity doesn't seamlessly hop from one tower to the next. And, if any tower goes down, the signal connection is lost. Redundancy is very costly, as it requires maintaining a second continuous communication pathway.

By contrast, wireless mesh's fluid nature provides inherently reliable, redundant connectivity, especially when M2M capabilities exist. A drone, or swarm of drones, can facilitate omnidirectional coverage over an extended area while simultaneously providing video surveillance and other situational data. Ground and water vehicles enjoy the freedom of movement, expanding the network as they roam. The mesh structure has no single-point-of-failure; data pathways form wherever connectivity is needed. Support for a wide range of frequencies further ensures that adequate bandwidth is always available.

High Bandwidth, Low-Latency Transmission: Robots transmit a lot of data. It's not just the communications necessary to maintain their mechanical movement and navigational functions. When used in security and public safety applications, these devices are loaded up with cameras, two-way audio, and other sensors. All of those systems also demand high-bandwidth, low-latency connectivity.

Because the wireless mesh is a closed network, transmission is faster than if systems were accessing cellular towers or transmitting through the cloud to communicate between connected devices. Networks can contain any number of nodes – from under ten to many hundred; each additional node functionally strengthens the network. Networks can be scaled up and down quickly and easily through the addition or removal of devices and their associated nodes. The mesh adjusts automatically, making new connections based upon what's available.

Cost: When selecting a network capable of supporting robotic solutions, wireless mesh is not only superior in performance; it's also less expensive than alternatives. The savings result from the network's cost and the ability to leverage mobile robotic solutions to replace a more expensive static security infrastructure.

Mesh networks offer long-term value and comparatively low total-cost-of-ownership. The only upfront expense is the purchase of nodes and the minimal labor necessary to get up and running. There are no recurring licensing or data-use fees. Furthermore, the ability to provide coverage of a broad area through mobile robotic technology, in place of many more cameras, sensors, and live human security guards, can reduce the required initial technology investment and the recurring costs for security operations

.

Wireless Mesh in Action

Applications abound for robotic security technologies

Robotics can improve the security posture of a wide range of environments, particularly those that involve expansive properties or require customer service as part of their security operations. Following are some examples of what these scenarios might involve:

Heightened Security Environments: Certain sites require more than just standard perimeter and building security systems. These are properties that, for any number of reasons, are on the radar of criminals or terrorists and face an elevated risk of attack. They range from the private estates of high-profile, high-net-worth corporate executives and celebrities to critical infrastructure facilities like data centers and utilities.

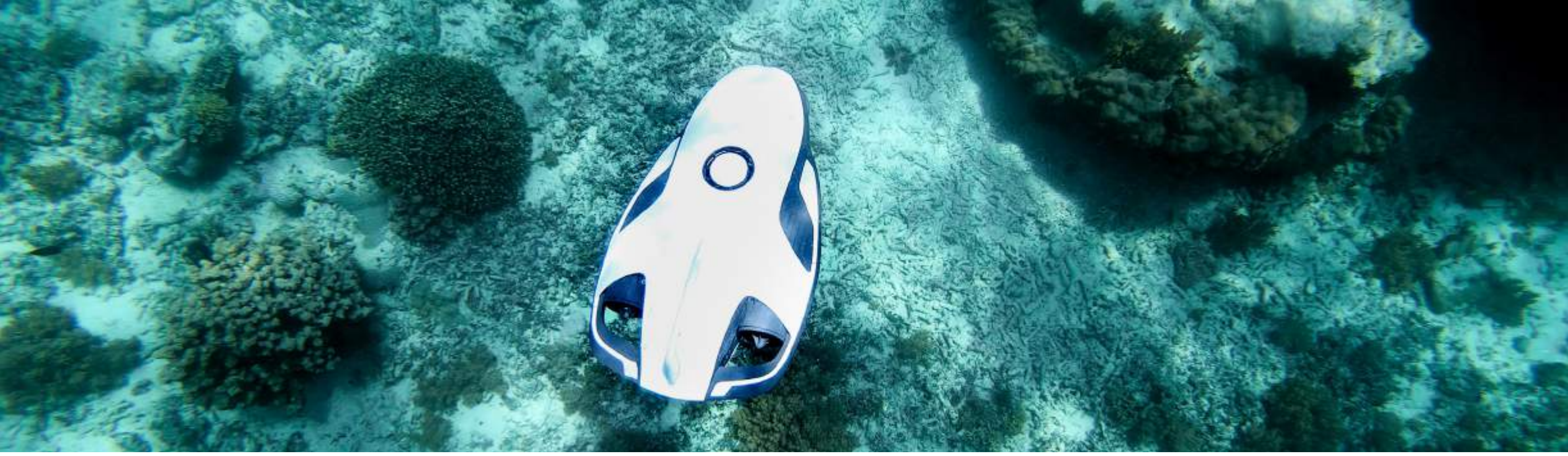
Security teams need to have comprehensive situational awareness of what happens across these properties from the moment their perimeter is penetrated. Blanketing these sites with security technology can be difficult. The grounds may cover hundreds of acres or more, with wooded areas, hilly terrain, and only one roadway in and out. Trenching power out to strategic locations is extremely expensive. Plus, even the most extensive permanent infrastructure would fail to provide connectivity across the entire site.

Bringing in a wireless mesh solution allows security teams to lay out a comprehensive network that supports the deployment of security and communications technology wherever needed. The network's nodes can utilize fixed power sources, solar power, or in the case of M2M connections, be powered by the mobile devices to which they're assigned.

By levering such a network, drones can simultaneously provide wide-area surveillance and omnidirectional connectivity for mounted cameras and sensors below. Terrestrial robots or unmanned ground vehicles can patrol the grounds, including off-road. On foot or in vehicles, human patrol officers can access Wi-Fi through the wireless mesh network as they move about the property. They can securely communicate with each other, view live video, call up events and receive alerts on their mobile devices. Officers in the security operations center gain a much more detailed and nuanced understanding of the state of security at all times.

Shopping and Entertainment: Security robots are already in use in large retail complexes, performing patrols of interior spaces, surrounding grounds, and parking areas. They offer a combination of surveillance capabilities as well as customer service.

As a robot moves about a shopping and entertainment complex, there are places along its patrol where it loses its connection to the network. When that happens, it continues along its route, programmed to do its job. However, during these connectivity gaps, the robot does not provide real-time security information; it's collecting information until it reconnects.



From a customer service standpoint, going offline is a problem. If a customer approaches the robot and requests assistance, the robot must open a live communication channel with a security officer stationed back at central command. The need may be urgent, such as a medical crisis or a crime in action.

If a network connection isn't available, a robot may rely on cell phone service instead. Unfortunately, cell phone service may be unreliable. For example, during the busy holiday season, local cell towers can be overwhelmed by traffic from shoppers using their phones. The same is true during emergencies. There's a good chance that the robot will not have connectivity in these situations, meaning that when security operations teams most need the robot as a resource, it is inaccessible to them.

A wireless mesh network is an ideal alternative. M2M connectivity provides flexible connectivity that accommodates the technology's movement with unbroken signal transmission and is independent of external networks. It can provide consistent, highly reliable connectivity and communication between the Command Center and all of the network's edge devices, including mobile, throughout the time of an emergency or high system use.

Emergency Response and Disaster Recovery: Floods, tornados, plane crashes, earthquakes, fires… when emergencies like these occur, everything is turned upside down. During such events and their aftermath, first responders don't have essential resources available. Utilities are down. There's no communication. No infrastructure. Roadways may be impassible. And yet, first responders need to do their jobs.

Disaster recovery efforts benefit from technologies that enhance the ability to determine where the most significant damage exists, where victims may be, and how to best allocate resources. Aerial technologies like drones, thermal vision, ground-based robots with video surveillance technology, and a host of different sensors all assist with these efforts. They are all dependent on connectivity. Responders could leverage point-to-point wireless networks, but these systems are not quick to deploy and are limited in their ability to support mobile technology.

Today's wireless mesh networks are well suited for emergency work and recovery scenes, which by nature are very fluid. They allow responders to immediately set up a wide-reaching network, with any number of nodes, so that they and their devices can move about seamlessly throughout the entire area. Mobile command centers, set up in vehicles brought to the site, can manage the operation locally and relay information back to a remote center where additional experts share recommendations, insights, and decision-making responsibilities.

Summary

Successful security outcomes require the right network infrastructure

Autonomous robotic solutions are expanding the role that technology plays in enhancing security and public safety while creating operational efficiencies and cost savings. They offer tremendous benefits for stakeholders who deploy them wisely, but doing so requires a networking design that will deliver the expected functional outcome.

Too often, technology investments are evaluated based upon what they "can" do, without sufficient focus on how they will work once installed within their intended environment. A thorough assessment of robotic solutions should include evaluating the pros and cons of various networking methods. There are certainly scenarios where hardwiring a particular device makes sense, especially if the site involves a low device count and does not require mobility. However, for larger deployments, where machines will continuously be moving or repositioned in different geographic areas, wireless mesh is unique in its ability to maintain fluid connectivity while reducing the total cost of operations. For robots, drones, and other autonomous mobile solutions, there is no better option.

Mr. Paul Benne, PSP, CPOI, *is the Founder and President of Sentinel Consulting, a full-service security consultancy that provides clients with technical and operational security expertise. Mr. Benne's professional career has included work in emergency management, law enforcement, firefighting, security management, crowd management, operations, training, and technical fluency in the design, implementation, and management of physical and electronic security systems, all of which form the basis for his uniquely broad and deep security perspective. His company offers risk assessment, security master planning, technical and architectural security design, operations, and training.*