ROBOTICS

Making the deployment of robotics possible

Todd Rigby, Director of Sales, Rajant explains how seamless mesh networking connectivity is keeping security robotics on guard

Security is paramount for every industry, especially those managing a sprawling environment. From industrial work areas to college campuses, security and surveillance are integral to ensuring the safety of people, safeguarding equipment, fortifying infrastructure and protecting valued information stored in a physical setting. Threats can occur around the clock and security must follow suit with 24/7 proactive monitoring.

While still a relative novelty, on the-move robotic and autonomous solutions have made recent inroads within security and public safety applications. The pandemic exposed new operational challenges that could be more effectively addressed by augmenting human resources with robotic options. Organisations will undoubtedly explore this once they have time to take stock of their "new normal" and evaluate the technologies they have at hand.

Many companies worldwide have gradually adopted these autonomous solutions and studies predict that the security robotics market will reach $71.8 billion by 2027, a CAGR of 17.8% from 2022. However, widespread adoption remains to be seen. Common misconceptions are prevalent, including the false perceptions that the solutions are expensive and fear over how employees and the public may react.

In addition, people may have concerns regarding the reliability of Wi-Fi or LTE services to trust their physical security. Rest assured, 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 expensive, inaccessible and sometimes unreliable.

> "SECURITY IS PARAMOUNT FOR EVERY INDUSTRY, ESPECIALLY THOSE MANAGING A SPRAWLING ENVIRONMENT."

Securing the scene with autonomous machines

Autonomous security robots can perform sophisticated tasks ranging from advanced inspection of potentially dangerous territory, detection and prediction of threats, such as explosives or toxic substances, to assessment tasks and support for disaster rescue teams. AI and machine learning is arming robots with the tools they need to be self-directed, insightful and better at anticipating and responding to developing situations. With robotics technology augmenting human resources, dangerous and mundane tasks can be reliably and consistently addressed with a variety of viable robotic options.

Robotic applications range from monitoring and intrusion detection to asset, property and personal protection. They bring benefits such as cost reduction and greater specialisation of personnel in security management. Therefore, many companies have already begun introducing autonomous robots to improve their surveillance and security operations. For many security professionals, most of their work is spent monitoring and patrolling.

This is a significant time investment, especially when staffing vast areas. Security robots can help enhance the capabilities of security professionals, rather than replacing them, taking over more mundane and time-consuming tasks so workers can focus on those with higher value. They can provide 24/7, continuous data from onboard audio, video and sensors and protect guards from dangerous, at-risk tasks.

Autonomous robotic solutions are expanding technology's role in enhancing security and public safety while creating operational efficiencies and cost savings. They offer tremendous benefits for stakeholders who deploy them wisely. What may surprise you is that the most challenging component of deploying security robotics is not the robots – it is the mission-critical wireless communications which are vital to receiving accurate and timely data reporting from the robots.

Applying the right network infrastructure is crucial

As the use of robots to supplement security workforces increases, secure data sharing and device cross-communication becomes even more critical. These assets are highly mobile and demand continuous high capacity links to transmit audio, video and sensor data. If there are drops in connectivity, even momentarily, the

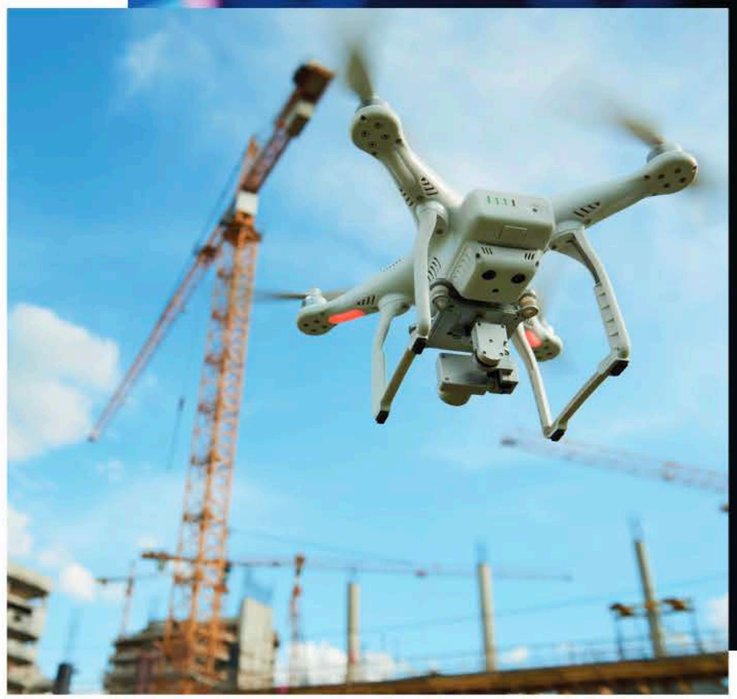
systems cannot talk to each other. Important information can be missed and security or safety breaches can occur.

When used in security and public safety applications, these devices are loaded up with cameras, two way audio and other sensors. The payload can be anything from accurate gunshot detection or the presence of hazardous materials, from toxic chemicals to radiation. All of these systems demand high bandwidth, low latency connectivity.

The greatest challenge in supporting robotic and autonomous solutions is keeping them connected. Systems engineers have traditionally turned to either cellular or Wi-Fi solutions. Both have drawbacks. Cellular is a poor option – there are plenty of locations that lack adequate coverage. Even where coverage is strong, cellular networks are designed to service smart phones. As a result, carriers focus the majority of network capacity on the download stream, for example, cell tower to device. This is why it is so easy to stream video to your LTE-enabled handheld.

“WITH ROBOTICS TECHNOLOGY AUGMENTING HUMAN RESOURCES, DANGEROUS AND MUNDANE TASKS CAN BE RELIABLY AND CONSISTENTLY ADDRESSED WITH A VARIETY OF VIABLE OPTIONS.”

Taking this one logical step further, the remaining narrow allocation of bandwidth left for upload is often insufficient for these robotic solutions to work well at scale. This



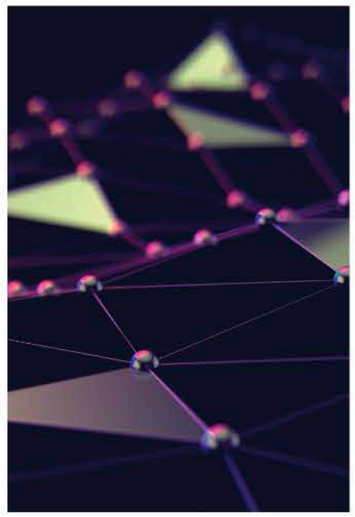
is why when you record video on your LTE-enabled handheld device, it is a slow painful process to upload or send to another location/device. And lastly, anytime there is a large gathering of people, LTE networks become swamped. Can you really afford to have your physical security solution compromised due to an unexpected traffic jam?

Wi-Fi has always been challenged by mobility. If you do not believe me, put your phone in airplane mode, connect to your home Wi-Fi and go for a walk. You will probably be surprised how little you have to walk to leave the small coverage area from your home Wi-Fi router. Many may say: “We will install many Wi-Fi Routers around our site” – the challenge then becomes Wi-Fi roaming.

Wi-Fi uses break-before-make. You have to drop a connection before you make a new connection. Best case, this is two-to-five second dropouts. Worst case, the robot stops and you must send a person to manually get the robot connected to the next hotspot. It is at this point you may be thinking, ‘I thought we were considering robots to keep people from having to do mundane or unsafe work.’

Empowering robotics with ‘never-break’ connectivity

A mesh network comprised of several communication nodes can automatically identify and transmit data between them. These nodes can adjust to find the fastest and most stable connections. Mesh networks can easily scale up and down quickly by adding or removing nodes. Data can be seamlessly rerouted depending on the bandwidth needs, signal strength or competing traffic. Having a network



with machine-to-machine (M2M) connectivity is a huge boost. With mobile assets equipped with mesh node, the mobile robots remain connected to the network with no drop-outs.

Wireless mesh is dynamic. It provides reliable, redundant connectivity, crucial in the most challenging environments from a crowded stadium to a sprawling campus or plant environment. It autonomously overcomes challenges such as sprawling property size, topography, obstacles, weather conditions, local RF interference, congestion and even infrastructure outages.

It is less expensive than wired infrastructure, such as fibre and other 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 low total cost of ownership. The ability to provide coverage across a broad area through mobile robotic technology, in place of many more cameras, sensors and live human security guards, can reduce the initial required technology investment and eliminate the recurring costs commonplace for security operations.

A drone, or swarm of drones, can facilitate omnidirectional coverage over an extended area while simultaneously providing video surveillance and other situational data. Ground vehicles enjoy freedom of movement, expanding the network as they roam. The mesh structure has no single point of failure as data pathways form wherever connectivity is needed, empowering and strengthening an around-the-clock security program. This allows terrestrial robots or unmanned ground vehicles to patrol a location, including off-road.

As a bonus, people can easily access Wi-Fi from the mesh network while navigating the environment.

Not only can the team securely communicate with each other, but the officers in the security operations centre gain a more detailed and nuanced understanding of the overall state of security through transmitted audio and video. Support for a wide range of frequencies ensures adequate bandwidth is always available. Because the wireless mesh is a private network, transmission is faster than over public solutions and you never pay for data.

“A THOROUGH ASSESSMENT OF ROBOTIC SOLUTIONS SHOULD INCLUDE EVALUATING THE PROS AND CONS OF VARIOUS NETWORKING METHODS.”

The future of public safety and security

Many organisations have identified the need to look beyond traditional security solutions to protect against new threats. Including security robots as part of your security plan is flexible and cost-effective. However, do not make the mistake of assuming any network will give you the expected ROI. You need to ensure you have laid the ground work for a successful robotic deployment first to reap all of the benefits drones and robots can potentially give.

Too often, technology investments are evaluated based on what they “can” do without sufficient focus on how they will function 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 certain 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 on the move or repositioned in different geographic areas, a wireless mesh network is unique in its ability to maintain fluid and reliable connectivity while reducing the total cost of operations. ▪