US soldiers talk on their radios during military operations

Picture credit: Getty

COMMS ON THE BATTLEFIELD

Michael Van Rassen *explains the challenges faced in maintaining a network when it really matters*

The evolution of warfare technology, designed to aid and abet communications across the battlefield, has and continues to rapidly change the way that armed forces function. From an 'eye in the sky' drone to a swarm of robotic land machines, troops and federal governments are embracing machine intelligence capabilities that assist soldiers and military personnel like never before.

Using connected technology, armed forces can detect threats earlier, make decisions faster and provide situational awareness of the battlefield based on more timely and secure information. While this idea is not new to conflict, new developments in autonomy mean operators in hostile environments can reap the benefits that a connected battlefield can bring.

Despite the enthusiasm to install these new technologies, a coalition of unique challenges plague military environments. While civilians in London, Paris or Dubai take reliable networks for granted, troops – based in rugged, harsh conditions with limited cell towers – suffer from negative consequences of fixed networks and both RF and man-made interference. For a soldier trying to make contact through their radio for life-support, critical communication that encounters down-time could be downright catastrophic. Along with challenging terrain and changing operations in time-consuming, complicated deployments in the midst of battlefield pressures, it is becoming clearer that traditional networks are no longer reliable.

SECURE COMMUNICATIONS

Maintaining secure communications in military environments is also critical for the safety of important information; when a British man hacked into the US Department of Defense satellite systems in 2014, he was able to steal the confidential data of over 800 employees from 30,000 satellite phones. Higher transmission speeds require higher levels of encryption, decryption and authentication, while warfare communications demand powerful, military-grade protection. With a host of potential threats such as extraction, traffic spoofing and blocking, special protection for data in transmit and at rest is needed in the battlefield.

KINETIC MESH NETWORKS PROVIDE FULLY MOBILE WIRELESS BROADBAND THAT IS FAIL-PROOF

When you consider time-sensitive missions, complex deployments and other battlefield pressures in hostile situations, having complete, accurate and up-to-the-minute data is crucial. Yet military and defence personnel continue to battle with the complexities of establishing and maintaining broadband connectivity in remote, mobile and harsh environments.

The challenge now facing our military technology leaders comes with finding a reliable, mobile and secure network, ensuring mission-critical intelligence reaches military personnel in real-time.

A network in this environment must provide continuous communications to in-motion and stationary personnel, vehicles and equipment, therefore ensuring troops have always-connected, secure access to applications and information at their fingertips.

Across all markets, military networks have the highest level of responsibility for ensuring critical communications, non-negotiable in the fact that they must be secure to prevent potential hacking, interference or loss of data. While the need for wireless, mobile connectivity in the constantly changing regulatory environment on the battlefield has never been greater, a unique form of wireless is needed to prevent an ongoing trauma headache.

Many look to wireless mesh networks, often used for widespread areas of coverage, as the answer. The mesh communications network is made up of radio nodes structured in a net topology, self-configuring to exchange information continuously and dynamically adjusting radio channels to create the least possible interference. When military personnel need to exchange information within milliseconds, mesh networks are the most reliable for transmission.

Although satellite communications are optimal for many GPS-centric and navigational activities, high latency limits its ability to fully support strategic and tactical missions. By expanding terrestrial broadband and existing infrastructure with low latency wireless mesh networks and integrated communications, sub-second per hop latency is possible.

Yet it must be noted that not all mesh is equal. Traditional mesh has many limitations such as the number of nodes, inefficient use of radio frequencies and the fact that mobile nodes cannot talk to each other directly. Traditional mesh also makes inefficient use of radio frequencies and suffers limitations of having to communicate to a single infrastructure node – a potential point of failure.

Kinetic mesh networks, unlike any other offering on the market today, provide fully mobile wireless broadband connectivity that is simple, instantaneous and fail-proof in any application – ideal for mission-critical environments like the battlefield.

Whether land, sea or air, the military is increasing its levels of autonomy to drive new trends and technologies that aim to improve the unique issues that plague mission-critical communications, by turning to kinetic mesh networks, which are proven to enable faster, cost-efficient, flexible and 'always on' networks.

First built for military and defence applications over 15 years ago, kinetic mesh networks are specifically designed for the rugged terrains and harsh physical environments seen by troops in the field and have been battle-tested to support the mission-critical communications they need to overcome environmental adversity.

THE PERFECT COMBO

The kinetic mesh network combines wireless network nodes and networking software, employing multiple radio frequencies and any-node-to-any-node capabilities to instantaneously route data via the best available traffic path and frequency, with up to 300Mbps transfer rates.

Being able to connect personnel benefits the military in more ways than one, from better effectiveness and awareness to most importantly – paramount safety. Timing in military operations is everything, as data is engagement-critical or even safety-critical, just a few milliseconds delay could create an issue – meaning data needs to be as close to real-time as possible.

By using network technology with kinetic mesh, the network remains operational even when nodes are lost or radio frequencies are jammed. The network is then able to dynamically utilise all available frequencies for any and all functions. If there is interference on any one frequency, the node will make use of one of the other available frequencies to complete its transmission. This capability provides robust fault tolerance, high throughput and low latency even in situations where the enemy is attempting to block communications.

Kinetic mesh trumps traditional mesh on the battlefield where mobility is grave. Traditional mesh networks have various limitations, but kinetic mesh can morph as requirements evolve, providing the most mobile, fail-proof, high-performance, private wireless network.

FILLING IN THE GAPS

If a certain path becomes unavailable for any reason, such as an antenna failure, the nodes on the network use an alternate route to deliver the data, eliminating any gaps in communication and allowing on-the-fly transmission of voice, video and data, despite conditions that would cripple other networks. The nodes self-configure, making it simple to expand the network. Each node serves as a singular infrastructure, which enables everything within the network to be mobile: wireless nodes can move, clients can move, network traffic can move – all in real time and without manual intervention. Kinetic mesh can also deliver networking capabilities for handheld radios, ground and airborne vehicle communications as well as security and tactical wireless sensors quickly, efficiently and securely.

With kinetic mesh, there is no central control node and no single points of failure. These self-healing, peer-to-peer networks support Wi-Fi, integrate easily with Ethernet-connected devices and scale to hundreds of high-bandwidth nodes – in fact, the more nodes, the more pathways are established and the network becomes securer and stronger. This helps create a force multiplier in combat situations as well as during other mission-critical environments. It eliminates the challenges of time-consuming, complicated deployments in the midst of battlefield pressures, challenging terrain and changing operations.

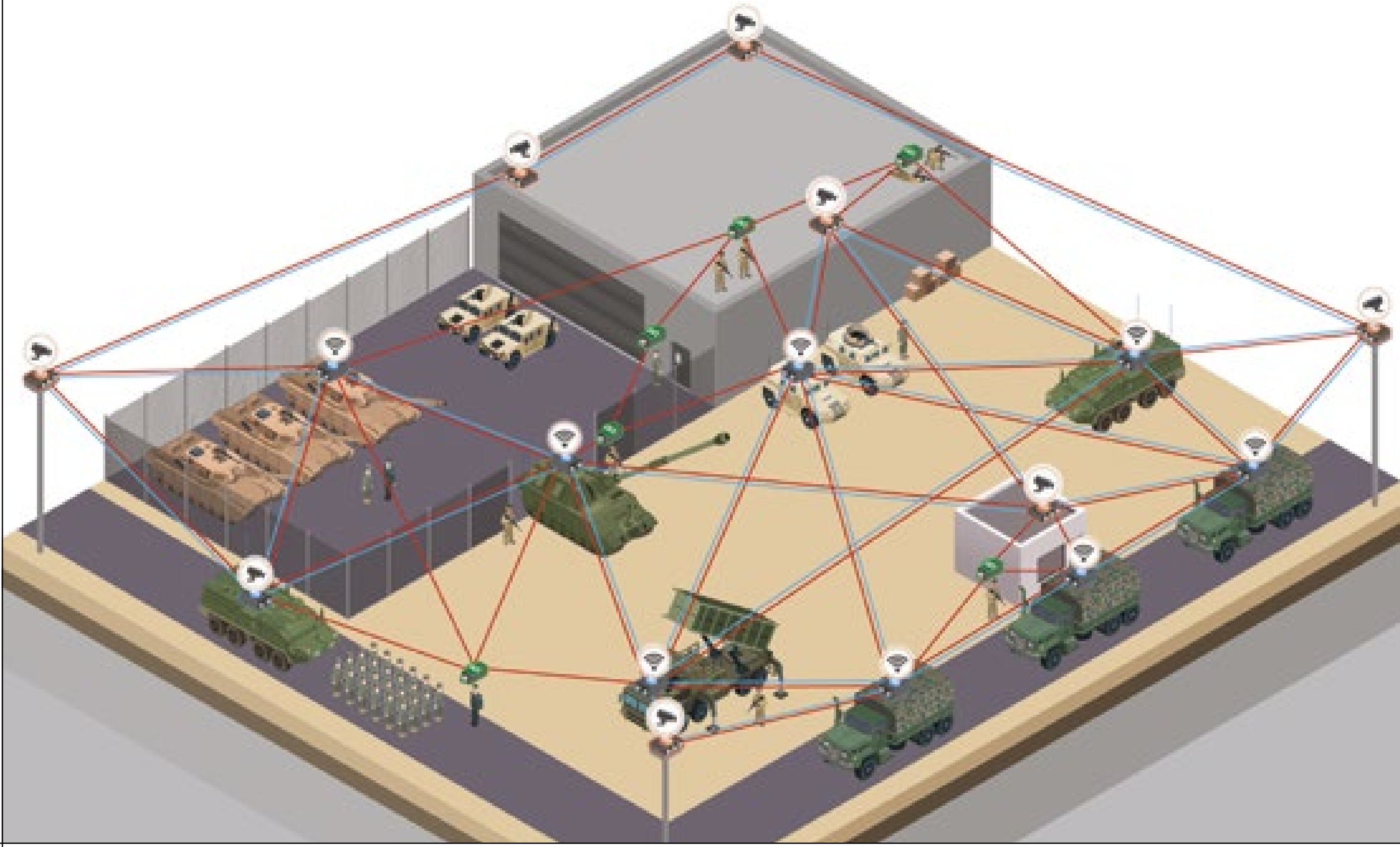
The emergence of kinetic mesh came in the immediate aftermath of the terrorist attack on 11 September, 2001 in New York. The attack resulted in communication networks, mainly in the city itself, being weakened; it took months and even years for the networks to be fully restored. After this, there became a growing need for a truly mobile technology like kinetic mesh, which delivers a broadband network with infrastructure devices constantly in motion, with wireless nodes strewn around an incident site that could link up and provide a more secure and stable connection. Now almost 17 years on, the technology is the only mission-critical network available today, a key player in securing fast communication connections between troops on battlefields across the world.

THE CHALLENGE FACING MILITARY LEADERS IS FINDING A MOBILE AND SECURE NETWORK

Kinetic mesh provides field forces with the military grade security they need to focus on the task at hand, without the prospect of failing connectivity and weakened mobility. The track record of kinetic mesh speaks for itself as it has been used in several high-profile military programs – and even during rescuing efforts. By reimagining the battlefield with machine-to-machine networks utilised with kinetic mesh networks that are capable of more than we ever thought, militaries can no longer assume the best-case scenario, but prepare to effectively communicate when under attack ●

Michael Van Rassen is executive vice president of business development for Rajant. Prior to Rajant, Van Rassen founded the C-RAM program – a set of systems used to detect and/or destroy incoming artillery, rockets and mortar rounds in the air before they hit their ground targets – in the summer of 2004, and led that effort until his retirement from Federal Service in 2016. During that tenure, he led acquisition efforts in Command and Control, Missiles, Guns, Radars, and Communications.

Kinetic mesh networks are designed for rugged terrains and harsh physical environments



Picture credit: Rajant