SECURE MESH WIRELESS NETWORKS DRIVE COMMAND POST MOBILITY

Author: Dominic Perez, Curtiss-Wright Defense Solutions

For years, the goal of our armed forces has been mobility at the command post, with Army leaders setting the standard to be able to move hourly, with the command post's network ready, powered up and receiving in five minutes.

That goal is understandable and achievable, but is difficult to achieve with today's approach to edge networking. Imagine a typical scenario: while tents are being set up at the new command post location, soldiers must also run 100 ***CAT5/6 Ethernet cables*** to connect everything, all within minutes.

It's simply not possible to meet the setup time goal using traditional copper or fiber optic Ethernet cables. Beyond set up, there are logistical issues: the use of traditional Ethernet in the battlefield brings with it the requirement to manage spools of CAT5/6, as well as the challenge of re-terminating the cables in the field.

There is a solution, though, that can optimize mobility in the field. A secure wireless command post system can be setup and servicing tens to hundreds of users in just a matter of minutes.

While many military users still have trepidation about the security of wireless networks in the military, those concerns have been met and mitigated through the proven use of ***NSA*** approved Commercial Solutions for Classified (CSfC) encryption, using two layers of approved software and/or hardware encryption approaches. In fact, a mobile, rapidly deployable and extendable network is possible today and qualified to TRL9.

It is true that when compared to traditional direct Ethernet cabling, there's a trade-off when using wireless networking where you gain connectivity speed at the cost of connection throughput. However, that trade-off becomes compelling when one considers that the nature of threats keeps changing and the demands of warfighters keep expanding.

There is a growing awareness of the challenge of command post survivability. Two years ago, in 2020, Maj. ***Jeremy Horton*** and Col. ***Ted Thomas*** issued a thought piece on this topic, and the events of 2022 only further highlight the threat and challenge.

"Recent events in Eastern Europe demonstrate that command posts (CPs) are not only susceptible to detection but that they can be destroyed within minutes if they do not adapt. To address this, the Army must understand how a peer adversary will exploit CP vulnerabilities; and then develop improved survivability approaches to mitigate detection and attack, while maintaining effective command and control (C2) that ensure the success of the operations they are designed to orchestrate."

Our adversaries are increasingly sophisticated and Command Posts can be detected and destroyed within minutes. The warfighter needs to understand these vulnerabilities and mitigate the effects of an attack and next generation of Command Posts will contain the necessary communication infrastructure on vehicle platforms

While few would argue that a wireless network can compete with cable for connection speed, while everyone knows that the advertised max speeds on Wi-Fi can only be met under laboratory conditions, with Wi-Fi 6 multi-hundreds of megabits of throughput can realistically be deployed in the field.

Dominic Perez

Another advantage of wireless networking is its support for mesh topologies, which can be used to eliminate the threat of a single point of failure in the network. That means that the loss of a single node or vehicle does not bring down the entire network, delivering true network resiliency.

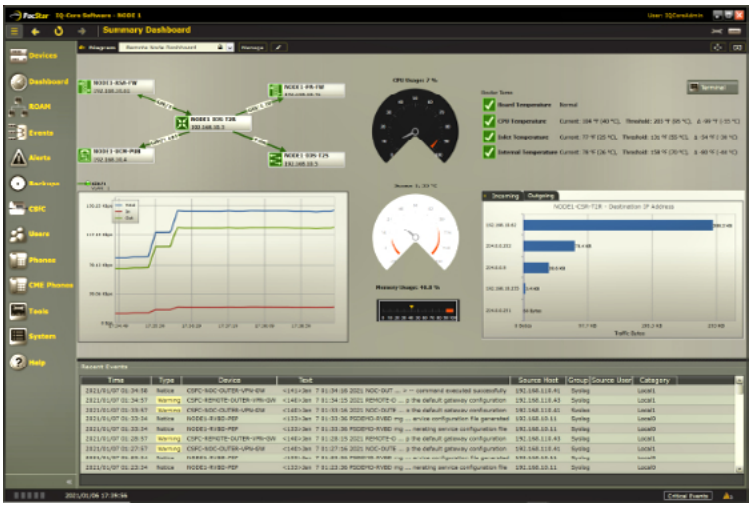
A mesh network can exist in many different topologies, and a key attribute of meshing is the ability to route across the network with direct hop, single hop, or multiple hop, data distribution to connect any two nodes on the network. Meshing can come in a variety of formats, with the most common example in the field provided by **MANET** (***Mobile Adhoc Network***) radios. Usually, each user would have to have their own MANET compatible radio, which while fine for handheld communications, is less than ideal for data based comms, which if needed would require the user, for example, to plug-in into a laptop or tablet.

Curtiss-Wright SWCP Wi-Fi

Commercially sourced Wi-Fi solutions typically have built in support for mesh network topologies. Unfortunately, that class of network solution is not always compatible with NSA requirements for CSfC. Commercial Wi-Fi can be a short cut to setting up a CUI network, but it's not going to get you to a secret or higher network.

The use of ***secure wireless mesh networks*** (**SecMesh**) delivers a leap forward, if not revolutionary at least evolutionary, in the distribution of data connections to our warfighters. With SecMesh the warfighter can setup a wireless network that provides connectivity between vehicles as well as creating a bubble that's broadcasting to end-users. The SecMesh approach enables vehicle-to-vehicle mesh communications, along with the ability to do tunnel-in-tunnel CSfC encryption.

For several years, ***Curtiss-Wright*** has been deploying **Secure Wireless Command Posts** with the Army and with other groups. In a typical deployment, best practice has been to install a secure wireless command post system on each vehicle, where each vehicle would then have an actual network connection outbound, and not connect to other vehicles that are in the same area.



Core Network Comms Manager dashboard

While this style of deployment means that each vehicle can operate independently, it results in duplication of equipment and sub-optimal SWaP-C (Size, Weight, Power and Cost). Further, with each system operating independently users and devices cannot roam between systems without being pre-registered with each system they may encounter.

The next generation evolutionary step in SecMesh technology will be to mesh vehicles together such that multiple true-north bound network connections can be available in that case that one of the vehicles is lost. That approach will enable the users that are registered with one wireless system to roam between all of the wireless systems on the secure network.

Beyond that, where system designers are headed is for true vehicle secure network connectivity vehicle-to-vehicle while on the move. This capability has been shown today in the field and development continues, ensuring that this capability will only get more robust going forward.

The vehicle-to-vehicle links, don't need to be commercial Wi-Fi; they can be any IP based communications transport such as Wi-Fi, 4G, 5G, mmWave, MANET, LOS, or wired connections. Yes, even wired. When vehicles are going to be parked some place for a long time and higher speed comms is required between the vehicles, they can be hard-wired and connected to each other using traditional Ethernet or fiber optic cabling.

One example of how you can up a SecMesh network in the battlefield today is to use a Curtiss-Wright ***PacStar Secure Wireless Command Post (SWCP***) as a network hub. A secure wireless ***PacStar Command Post-X,*** serving as a first gen, non-meshing network, is then combined with a ***PacStar Secure Meshing Command Post*** (**SMCP**) system, which provides the full hardware and software suite needed to setup any number of vehicles into a mesh topology.

Typically, setting up a mesh network topology can be complicated because many legacy applications have built-in assumptions about the network on which they will operate. For example, the application will expect that network to be set up as a Layer 2 LAN instead of Layer 3 routed network.

That puts the burden on the network designer and network maintainer to hide the true nature of the underlying network to ensure it just works, both for the users and for the applications they are running on the network.

It's at this stage that ***PacStar IQ-Core Software*** can greatly simplify the setup, monitor and manage process, reducing the task to mere minutes by eliminating the need for the system manager to manually set each individual node on the network. Manual setup might take hours, which again, undermines the Army's goal to optimize mobility and reduce network setup to five minutes in the field.

Even better, the SecMesh approach can be deployed in extremely harsh environments.

Users can select the hardware form factor that is appropriate for the node, whether this is a communications vehicle with an enclosure for things such as the PacStar 400-Series, or a more combat focused vehicle, whether land or amphibious, that requires fully sealed electronics made possible by a SOSA-aligned design based on VPX hardware. As threats continue to evolve, we must, as industry partners to government, continue to expand our capabilities and rise to these challenges.

www.curtisswrightds.com

CURTISS-WRIGHT