No strings attached – Why militaries no longer need to trade off security and scalability in wireless deployment

Wireless communications have completely changed the face of the modern battlefield. Military missions have become increasingly dependent upon wireless communications technology due to ease of use and greater flexibility. Chris 'CT' Thomas, Federal Solutions Architect, Ruckus Networks (an ARRIS company), outlines how wireless networking provides mission success, without making compromises on security and scalability.

Chris 'CT' Thomas, Federal Solutions Architect, Ruckus Networks

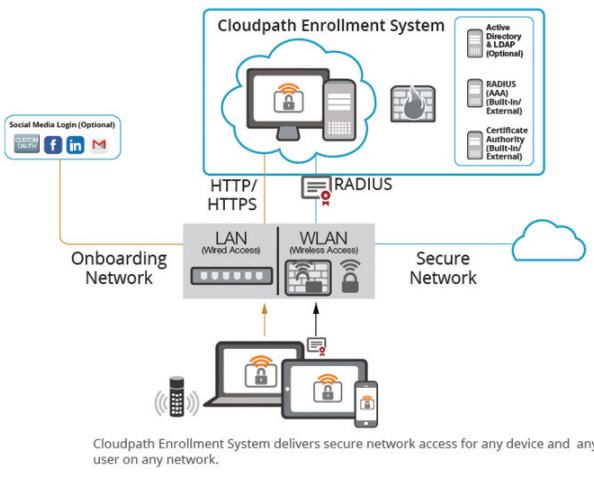
Federal agencies are in the midst of a technological paradigm shift. With the passage of the Modernizing Government Technology (MGT) Act and proliferation of remote access and BYOD across the public sector, now more than ever, agencies are on the cusp of decoupling from fixed workstations and embracing the age of mobile. Yet, military organizations have been slow to adopt wireless technologies for a myriad of reasons. Much of the challenge is rooted in the complex dimensions of modern militaries. In short, militaries have struggled to balance the need to both maintain high security consistency against the desire to be flexible, scalable and easy to manage.

Fortunately, military agencies have the opportunity to overcome such adversity, and marry both the practicality of wireless access and the challenges of security through new technology and processes, rather than viewing them as mutually exclusive – all with no strings attached.

Military wireless is the future

Challenges ranging from aged building infrastructure to extreme and remote terrain has resulted in slow adoption of widespread wireless networks for military agencies, whether domestically or in-theatre. That is changing, albeit slowly, as military agencies worldwide embark on expanding wireless technologies as part of broader modernization efforts. For example, to increase mission readiness, the US Marine Corps has announced a concerted investment in broader wireless use. The ultimate goal: To make wireless Internet as ubiquitous in defense as it is in civilian life.

It is easy to see why this change is taking place – wireless networking provides significant benefits over all-wired deployments: Easier installations, greater scalability of network resources, increased agility, and less reliance on physical presence of Ethernet ports.



Cloudpath Image from Collateral

Consider the case of a field medic treating a combat trauma victim. Advanced, secure wireless enables that medic to begin relaying key vital signs and other potentially lifesaving information back to medical facilities to begin preparations for surgery or other trauma care.

Another example of wireless use in military applications is in more efficient supply chain and logistics management. Since military agencies are among the largest logistics management enterprises on Earth, using mobile devices and connected Internet of Things (IoT) sensors can enable better and faster inventory assessments to streamline supply orders, increase efficiency and minimize backlogs.

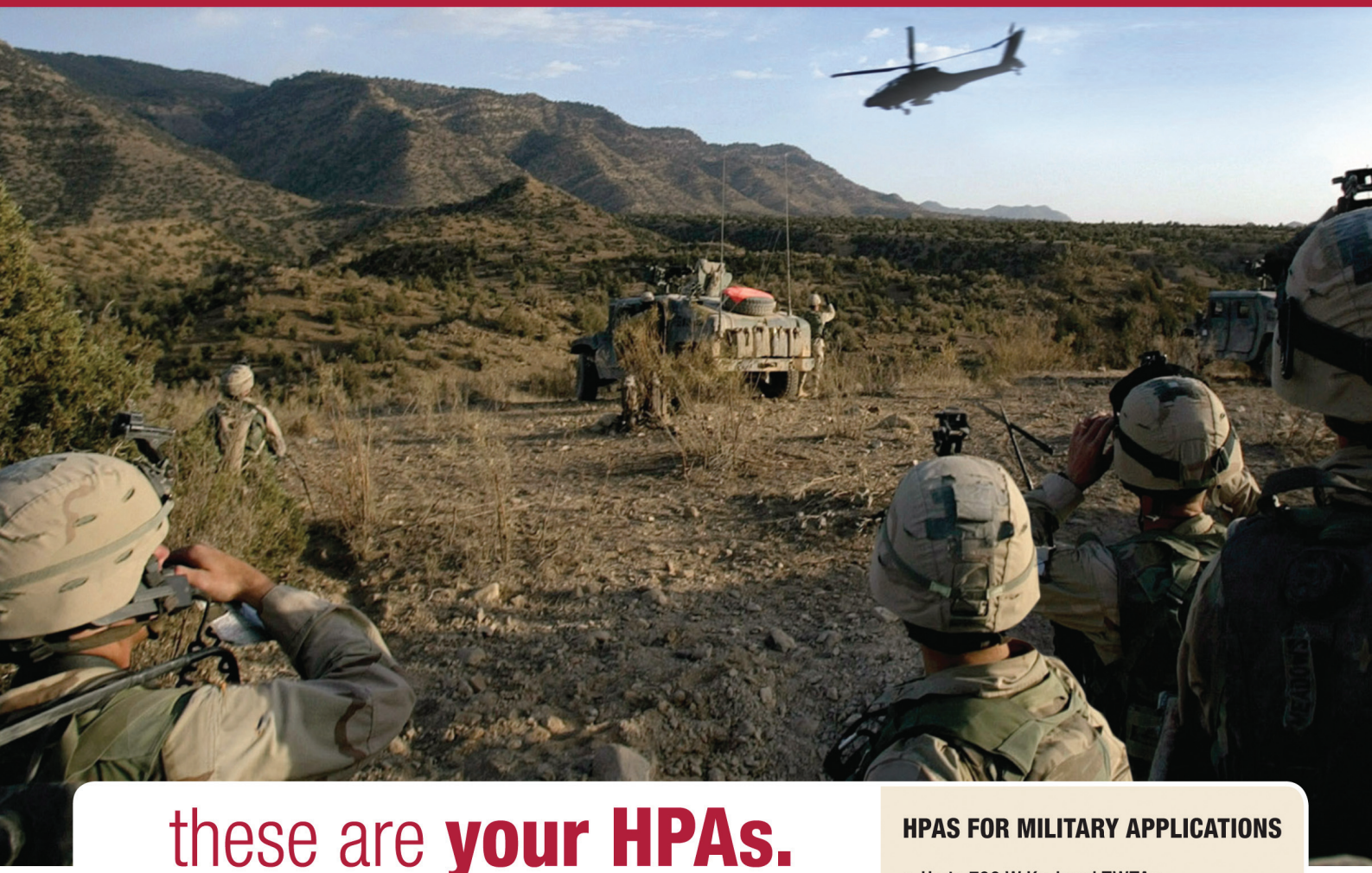
Indeed, consider the recent words of Paul Mehney, Director of Public Communications for the United States Army's Program Executive Office Command, Control, Communications-Tactical (PEO C3T): "By going wireless, command-post setup and teardown times may be reduced by hours, and less cable and protective flooring have to be transported from location to location," Mehney said. "Soldiers can be untethered from their workstations for improved collaboration. Most important, network downtime is significantly reduced. Following command-post setup, units can turn on their secure Wi-Fi hot spot and the network can come up first instead of last, in as little as minutes instead of hours. And soldiers can stay connected longer when jumping the command post."

However, adopting wireless is not a panacea for networking; the increased benefits of wireless also lead to new challenges that will need to be addressed.

Challenges of security and scale

Unlike wireless networks in the private sector, military networks require an added degree of security. Even devices reporting seemingly mundane energy information can reveal potentially

If this is **your office...**



these are **your HPAs.**

Superlinear® TWTAs
LEFT: 2.5 kW X-band
CENTER: 750 W Ku-band TWTA

Solid State BUCs
RIGHT: 160 W peak Ka-band GaN BUC

Warfighters shouldn't have to fight against their equipment.

That's why CPI amplifiers feature better efficiency and unmatched reliability even in the harshest of climates, keeping you connected anywhere at any time.

CPI offers:

- Better efficiency
- High reliability
- Rugged designs
- TWT, solid state and klystron technology
- Linearizer, BUC, and integral switch control options
- More than 20 service centers worldwide
- 24/7 technical support

For more information, please visit **www.cpii.com/satcom**, contact your local sales representative, or call us at **+1 (650) 846-3803.**

HPAS FOR MILITARY APPLICATIONS

- Up to 700 W Ka-band TWTAs
- SuperLinear® TWTAs in Ku- and Ka-band, delivering 25 to 540 watts of linear power
- C- and Ku-band HPAs for troposcatter applications
- 400 to 750 W C-, X-, and Ku-band indoor and outdoor TWTAs
- 2500 W SuperLinear® and CW X-band TWTAs
- X-, Ka- and Ku-band GaN BUCs

Download our new app!
Search: CPI Satcom

Download on the App Store

GET IT ON Google Play

CPI
Communications & Power Industries

satcom products

Photo courtesy of Ruckus Networks

important information about a facility's use to adversaries. They also require scale found in only the largest private telecom organization; militaries operate globally with an ever-evolving slew of network-connected devices.

Alone, the challenges of security or scale are relatively easy to manage. They have also traditionally been at odds with each other; deploying wireless infrastructure and devices on large scale has been hard to do while also maintaining high levels of security. Inevitably, users bring and connect unauthorized devices, fail to properly enable security credentials, or neglect routine security patches and updates.

Compounding these two challenges are the complex and varied environments in which militaries must operate; most businesses can reliably predict they will deploy wireless solutions in office buildings. Militaries must consider buildings, ships, aircraft, battlefields, temporary installations and more.

Merging practical scalability and security for better military wireless

What can military agencies do to mitigate the challenges that come with both ensuring security while also keeping wireless scalability practical? Militaries should adopt the newly-emerging industry paradigm of self-service, certificate-based on-boarding processes for network devices.

These certificate-based on-boarding processes, along with their management platforms, enable a host of advantages over traditional manual on-boarding procedures including the ability to pre-approve devices and automatically configure devices to comply with ordained security standards.

By putting network management into the cloud and creating certificate-based, self-onboarding, these platforms, like Ruckus' Cloudpath Enrollment System, bring network management away from the network edge and back to central IT services, providing numerous benefits.

With certificate-based security, network end-users no longer need to worry about passwords or lockouts; security credentialing is done once, after which a certificate lives at the device level. In the case of reported compromise – a lost device or detected security threat – the credential access can be revoked or altered via the cloud.

Such certificate-based security ensures that network and security administrators have complete control over which devices belonging to which users, are authorized to access to which resources. Simply put, certificate-based security allows granular user and device access control on your network.

Furthermore, it allows militaries to reduce network support footprints at installations translating to the need for fewer support staff and freeing up resources like food, lodging, and transportation for more mission-oriented personnel. And, with self-onboarding portals and automated security, Cloudpath ES also reduces IT tickets, freeing up resources for less menial tasks; some of our private-sector adopters have seen upwards of 20-person hours saved per week per 1,000 users.

Furthermore, being network and device agnostic, the interoperability of self-onboarding platforms results in fewer concerns over the wide array of devices requiring different configurations.

Don't let compromise get in the way of mission success

Defense agencies are in the middle of a major wave in IT modernization. Multiple new technology advances in data analytics, IoT, and cloud computing are transforming operations in ways that promise to cut costs and increase efficiency. And with the traditional barriers to widespread wireless deployment quickly being overcome, it is only natural that expanded and easier wireless makes its way into military applications.

Today's military missions increasingly rely on technology for communications, control and logistics capabilities. Those in turn, rely on easy to use, scalable and secure networks. Wireless networking offers even greater flexibility and efficiency, but too often came with tradeoffs between security and scalability; now it is possible to have both without tradeoffs. Time to start taking advantage of wireless; your mission success depends on it. **GMC**

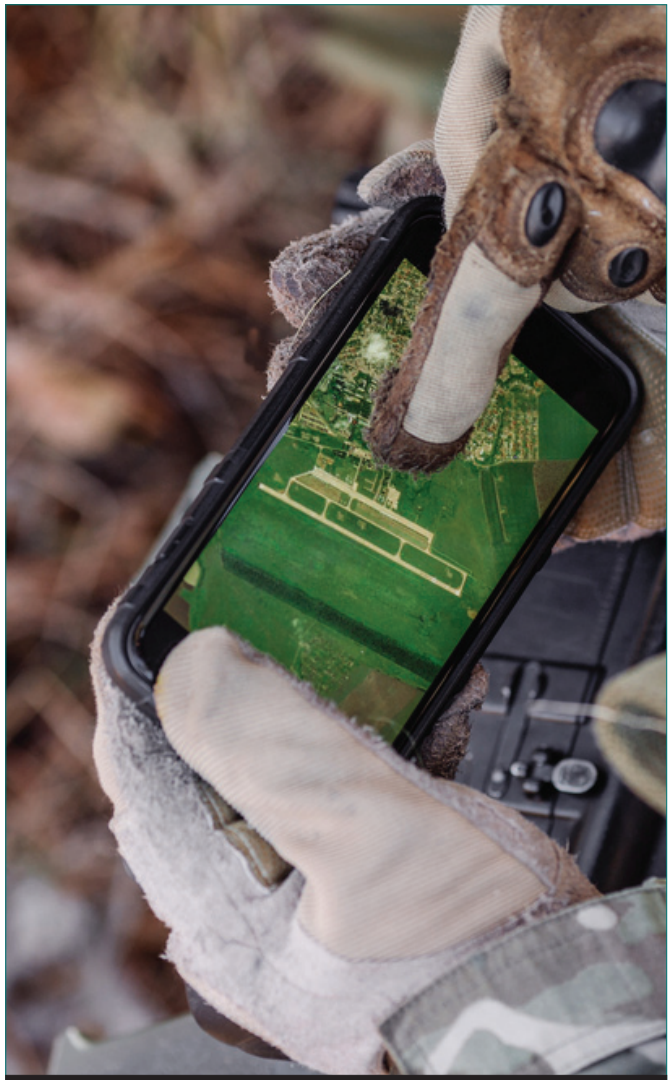


Photo courtesy of Ruckus Networks