2018 AFCEA ARMY SIGNAL CONFERENCE

MARCH 6–9, 2018 • WATERFORD AT SPRINGFIELD, SPRINGFIELD, VA

SOLUTIONS SHOWCASE

AFCEA Army Signal Conference Solutions Showcase

AFCEA International is pleased to host this important forum for members of the military to openly discuss current and future requirements and the private sector to describe available and upcoming advances in technology solutions.

The U.S. Army is strengthening its relationship with technology providers to incorporate a new class of capabilities. Army leaders agree that the future state of the service must feature a network that is survivable, resilient, protected, intuitive, standards-based, interoperable, sustainable and highly mobile. The service plans to assume a position where it is articulating its intent, a process that's being described as "adapt and buy."

As part of the conference, the Army identified these areas as opportunities for industry to offer potential solutions to problems the service and joint force must address both today and in the near future:

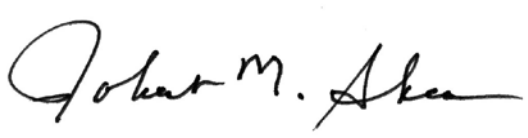
- **Unlicensed Long Term Evolution (LTE)**
  The Army is challenged to fully deploy LTE capabilities to date and would like to include operating on host nation cellular networks—when available and prudent—into its network strategy.
- **Spectrum Agility**
  For the Army to realize its future networking objectives, it must maximize its use of available of spectrum.
- **Mobile Ad Hoc Vulnerabilities**
  The Army would like to better understand the cyberspace security and operations implications of a fully employed mobile ad hoc networking environment at the tactical edge.
- **Reducing EMS Signatures**
  The Army envisions future command posts that emit minimal electromagnetic signatures, making them more difficult to detect.

AFCEA International received potential solutions for these problem areas from a range of industry partners and conference participants. The AFCEA Technology Committee reviewed 23 submissions and selected eight solutions to present at the conference. The solutions were evaluated on three criteria: innovation, potential effectiveness and maturity of solution.

I personally invite you to read these abstracts with an eye toward how these solutions address your command's needs or how your organization can support or enhance them. The ultimate goal is to support warfighters with the best possible tools to complete missions safely and successfully.

It has been a pleasure working with the Army, its planning team and industry to bring this conference together. The discussions that occur here not only will improve future Army operations but also collaboration between the military and industry to combat continuously evolving threats to national security.

Respectfully,



Lt.Gen. Robert M. Shea, USMC (Ret.)
President and Chief Executive Officer,
AFCEA International

Problem Statements

Unlicensed Long Term Evolution (LTE)

Problem Statement: The Army is challenged to fully deploy LTE capabilities to date and would like to include operating on host nation cellular networks—when available and prudent—into its network strategy.

Why this is a problem: The Army requires more bandwidth to realize its assured mobile networking strategy. Carriers around the world own most of the available spectrum in commonly used frequency bands. Conducting operations on these bands often requires the use of foreign-controlled networks, introducing the risk that those networks could be denied. Deploying LTE is one way of maximizing utilization of U.S. assets and reducing the need for foreign-owned networks.

Spectrum Agility

Problem Statement: For the Army to realize its future networking objectives, it must maximize its use of available of spectrum.

Why this is a problem: In a combat environment, limited spectrum is further degraded by hostile emitters. The Army needs the ability to employ radios that can scan for emitters, identify free spectrum and transmit at a new (uncontested) frequency utilizing advanced cognitive techniques for spectrum assignment and sharing to provide assured communications.

Mobile Ad Hoc Vulnerabilities

Problem Statement: The Army would like to better understand cyberspace security and cyberspace operations implications of a fully employed mobile ad hoc networking environment at the tactical edge.

Why this is a problem: Assured communications are essential to gaining and maintaining situational understanding for accurate and timely decision-making. If the Army employs mobile ad hoc networking solutions for combat operations, it must fully understand how adversaries might compromise these networks so that it can preempt the threat and harden them.

Reducing EMS Signature

Problem Statement: The Army envisions future command posts that emit minimal electromagnetic signatures, making them harder to detect.

Why this is a problem: The Army has studied the changing character of war and recognizes that command post survivability is threatened in an age of advanced direction-finding and artillery systems threats.

Table of Contents

Highlighted abstracts selected as presenters at conference as of February 28.

Deploying Unlicensed Long Term Evolution (LTE) Capabilities

Spectrum Agility: Maximize Use of Available Spectrum

Understanding Mobile Ad Hoc Vulnerabilities

Reducing EMS Signature

Army Aims for Network Modernization

Improving Spectrum Access for Military LTE Systems

Mike Jacobs, Chief Engineer, Booz Allen Hamilton • jacobs_michael@bah.com

ABSTRACT

The Long Term Evolution (LTE) technology behind 4G networks has won the battle to become the go-to solution for wireless wide area network (WWAN) applications over competitors such as WiMax. The technical advantages of LTE along with the sizable ongoing R&D effort behind it at little or no cost to the military makes it very attractive for wireless high-speed data networking for military applications.

The challenge in employing military LTE networks is that civilian spectrum demands and the primary application of LTE as a civil technology make it difficult to deploy LTE in areas where the available LTE frequency bands are already saturated with commercial networks. Recent developments in technology and spectrum policy have opened up new avenues for military LTE networks to deploy alongside civil networks in domestic and host nation applications.

LTE networks operating through software-defined radio (SDR) platforms can be configured to operate on nontraditional LTE frequency bands, including military spectrum such as the 225-400 MHz UHF band or other unoccupied spectrum. The 3.5 GHz band is becoming available in some areas for shared use through a dynamic spectrum access policy that allows users to request frequency assignments and make bids in competitive situations.

LTE-U is a concept to deploy LTE technology in 5 GHz unlicensed bands to augment licensed spectrum but presages the availability of LTE devices for new bands not traditionally used for LTE. Demonstration of LTE in the military UHF and other nontraditional spectrum using existing SDR technology will prove the feasibility of this application in allowing the deployment of military LTE networks and reducing the dependence on foreign-owned systems.

Making LTE Work for Tactical Expeditionary Communication Capabilities

Bill Ross, Vice President, General Dynamics Mission Systems • bill.ross@gd-ms.com

ABSTRACT

Long Term Evolution (LTE) is the high-performance mass market cellular technology that has achieved global success reaching more than 2 billion subscribers in 2017. Many governments and militaries around the world are actively working to capitalize on these technical advancements and economies of scale in network infrastructure and end-user devices by incorporating LTE into their future military communications plans. However, one substantial challenge that must be addressed to tap the value of LTE for tactical communication capability is assured access to spectrum, which is dependent on the nature of a deployment, especially whether it is a domestic or expeditionary scenario. This must be managed in conjunction with the availability of user devices such as cell phones that operate in the chosen bands.

The ultimate goal would be to have a choice of several frequency bands of operation that are applicable in domestic or expeditionary scenarios as well as LTE infrastructure and devices that support these bands. The subsystems in this infrastructure, when not working in host nation and carrier-controlled spectrum, would automatically identify and select interference-free unlicensed bands for operation.

The General Dynamics Mission Systems Fortress LTE solution has been designed to provide the spectrum flexibility needed to unlock the potential of LTE to improve war-fighter access to data and shared situational awareness in a tactical environment. Other warfighter needs uniquely addressed by the Fortress LTE solution include simplified management, reduced size/weight/power footprint, ease of deployment, self-organizing network capabilities, electronic warfare resilience and end-to-end security.

The solution briefing will provide a short summary of how Fortress LTE solves many of the unique challenges for far-forward tactical expeditionary communications, while giving the warfighter the ability to tap into the rich ecosystem of capabilities, devices and applications fueled by commercial LTE investments.

BIO: Bill Ross is the vice president of business development and strategy for the C4ISR Technologies line of business within General Dynamics Mission Systems. Ross' responsibilities include developing and executing strategies that give the warfighter a compelling operational advantage in the electromagnetic spectrum domain.

Spectrum Aggregation Using Opportunistic Modem™

David Beering, Co-Founder, Continuous Satellite Data LLC •
drbeering@intelligentdesignsllc.com

ABSTRACT

Opportunistic Modem™ (OM™) is a groundbreaking technology for spectrum optimization and management. OM is a patented method that makes it possible to aggregate up to eight disparate channels of satellite spectrum in each direction—16 channels total per modem—into a bi-directional IP data stream. OM is implemented in custom logic cards on the Datum Systems M7/M7L IP Modem.

The OM algorithm features a very high level of resiliency. When any operational channel is impaired by either jamming or interference, it can be logically removed from the OM aggregate, dropping the data rate of the aggregated IP stream by that channel's contribution to the overall data rate while preserving traffic occupying the other unaffected channels. Conversely, once the channel impairment is no longer present, the channel can be re-integrated seamlessly into the aggregate IP stream. Leveraging this feature of the technology would allow end users and satellite/teleport operators to reduce the spectral exposure of mission-critical traffic by distributing it across multiple carriers, potentially spanning multiple transponders.

BIO: David Beering is the owner of Intelligent Designs LLC, a small business based in Wheaton, Illinois. The primary focus of Intelligent Designs is engineering, systems integration, project management, and research and development in the field of satellite-enabled high-performance communications systems. He is passionate about employing space to further U.S. economic and national security interests.

Beering also is the co-founder of Continuous Satellite Data LLC, a firm that focuses on delivering innovative, algorithm-based solutions to the satellite industry.

During his more than 25-year career, Beering has held leading roles in over 85 projects developing and deploying satellite communications systems for organizations including the U.S. Naval Research Laboratory, U.S. Army, Missile Defense Agency, Airbus Defense & Space and many others.

Cognitive Radio Applications of Machine Learning-Based RF Signal Processing

Mike Calabro, Senior Lead Engineer, Booz Allen Hamilton • calabro_michael@bah.com

ABSTRACT

Cognitive radio applications could use efficient and low-latency methods to characterize the limited radio frequency (RF) spectrum to dynamically take advantage of open spectrum and avoid occupied or contested spectrum for military applications. Current signal processing architectures complicate the ability of any single radio–especially one in a tactical form factor–to host all the processing required to fully realize a cognitive radio network.

Booz Allen Hamilton proposes a new way of searching and evaluating spectrum based on a trained neural network capable of recognizing signals it has been trained against and then selectively processing against them in real time. The company will describe performance advantages of the approach that sets it apart from classical spectrum characterization and present a specific network training methodology optimized for radio frequency processing applications with both modeled and empirical results. Finally, the company will show how well the complexity scales to a dynamic RF environment to suggest it as a potential scalable solution for the Army's networking objectives for tactical radios and other needs.

Spectrum Agility via Software-Defined Wide Area Networks (SD-WAN)

Paul Cassell, Consulting Systems Architect, SD-WAN Solutions, Cisco Systems •
gmendiol@cisco.com

ABSTRACT

In the Army tactical environment, battlefield maneuver is enabled by the rapid deployment of nodes interconnected by radio frequency (RF) links. Spectrum agility is achieved through spectral diversification and full utilization of any available links and sometimes all links at the same time. Typical routed networks are only able to leverage the one best path at a time, and multilink utilization is cumbersome and difficult to configure.

Cisco supports diversified link aggregation, load balancing, policy and intent-based routing via its software-defined wide area networks (SD-WAN) platform that is available as a stand-alone device or fully integrated in the Cisco ISR 4K platform, ubiquitous in the tactical architecture. The solution offers an easy-to-configure and manage solution via a GUI-based interface that enables the dynamic and intent-based configuration of WAN interconnectivity on the battlefield achieved via spectral diversity.

BIO: Paul Cassel is a consulting systems architect focused on software-defined wide area networks and has been at Cisco for more than 10 years. Cassel is on his second tour at Cisco and came to the company via the acquisition of Viptela, the market leader in SD-WAN solutions. While at Cisco, he has focused on solutions for the U.S. Army tactical and enterprise systems.

Spectrum Agility via Dynamic Link Exchange Protocol (DLEP)

Shawn Jury, Cisco Systems Engineer, Federal Sales, U.S. Army Operations, Cisco Systems • gmendiol@cisco.com

ABSTRACT

The key to spectrum agility is through diversification and adaptability in the data transmission systems interconnecting the underlying Internet protocol (IP) networks. To achieve full spectral efficiency, that is to fully utilize the capability of any and all radio frequency (RF) links, the network nodes must dynamically adjust the available throughput of the various links and not solely rely on their up or down state to make routing decisions.

Dynamic Link Exchange Protocol (DLEP), governed by RFC 8175 ratified in June 2017, is a new protocol that builds on the lessons learned from radio aware routing and performance-based routing to dynamically adjust quality of service and traffic shaping based on the detailed status of the RF links. Cisco is currently enabling DLEP across its small form factor and enterprise-class devices and is building support in the RF transmission systems industry to enable the capability as well.

BIO: Shawn Jury has been a systems engineer at Cisco Systems serving the Army Special Operations community for more than 14 years. Jury is a graduate of the U.S. Military Academy at West Point and served as a Signal Corps officer for six years before coming to Cisco.

Redefining the Lower TI Architecture to Enable Technology Insertion at the Edge

Steven Modica, Chief Technologist, Booz Allen Hamilton • modica_steven@bah.com

ABSTRACT

In my time supporting the Army, the focus has been on purchasing equipment that can be sustained for 10 or more years. Software-defined radios were viewed as one method of enabling a longer life span.

Newer technologies have evolved in the commercial and SOCOM space, and those technologies have not been leveraged because of the larger scale of a Brigade Architecture.

Booz Allen Hamilton proposes a new way of thinking about the Army's Upper and Lower Tactical Internet that will create a modular architecture whereby elements of the network can be replaced without redefining the architecture. This can be done by adopting modern commercial networking concepts like core/edge building deployments and Content Delivery Network architectures.

BIO: Steven Modica has been supporting PM Tactical Radios for the past three years with Booz Allen Hamilton. Prior to this, Modica was owner and CTO of Small Tree Communications, a storage and networking company writing device drivers for Intel and Apple Ethernet products. He also spent time working for SGI/Cray as the network device drivers manager, overseeing the engineering work involved in writing and supporting SGI's suite of supported network products.

Adapting to Communication Interference

Joseph Schneible, Technical Lead, IR&D, Technica Corporation •
jschneible@technicacorp.com

ABSTRACT

Radio frequency (RF) communication is vital in times of crisis and on the battlefield; however, jammers and even everyday devices can interfere with RF signals. Technica has designed the Communications Interference Monitor (CIM), a low-cost portable sensor device to detect RF interference and visually alert the user. The CIM device will use sequential element-space processing (SESP) to replicate the capabilities of a distributed receive element—or aperture—in a small form factor. SESP employs only one aperture in place of a phased array. That aperture is moved in a linear motion and, if the interfering source does not move or moves slowly, the sequential measurements are equivalent to the simultaneous measurements at the multiple elements of the phased array. However, SESP has only been developed for linear motion where the returns form a hyperbola. Users often operate in environments where perfect linear motion is not possible. Technica's design accomplishes SESP for both direction of arrival and nulling, correcting for non-linear variable speed.

CIM will utilize deep learning in the form of convolutional neural networks (CNNs) to analyze images of the hyperbola-like paths of the interferers and correct for non-linear, variable speed motion of the device. CNNs have become the standard for deep-learning image analysis. Inspired by the visual cortex, CNNs learn receptive fields, or filters, to identify features in the image. The hyperbola-like measurement profiles only occur for point scatterers. In complex scattering environments, the profiles will be much more complex and will overlap more. The CNN approach will extend well to these more difficult scenarios.

The CIM device will collect data regarding the frequency extent and modulation of potential interference. It will fuse measurement results from spatial, frequency and modulation domains to provide a more accurate characterization of the interference. The CIM also can be used to actively cancel the interference. As RF bands become more congested, this ability to cancel interference will become vital in federal and commercial sectors.

BIO: Joseph Schneible is a technical lead in the IR&D department at Technica Corporation. He has experience in developing and optimizing parallel simulations. As a prior research scientist at The George Washington University, he developed low overhead heuristics for load balancing peta-scale simulations and efficient work distributions for multi-accelerator-based simulations. Currently, he designs data analytics applications for resource constrained devices on the SmartFog. As part of this project, he developed a federated anomaly detection application that trains a model on data from multiple sensors, simultaneously.

PlusN's Smart Carrier Aggregator

John Terry, Chief Technology Officer, PlusN • mike.brody@plusn.com

ABSTRACT

PlusN's Smart Carrier Aggregator (SCA) improves the tradeoff between peak-to-average power ratio (PAPR) and error vector magnitude (EVM) in downlink, intra-band carrier aggregation (CA), enabling a cellular site to increase capacity based on increasing the range of all constellations and thereby doubling the speed for upgraded subscribers.

PAPR-EVM Tradeoff Curve Example

The PAPR measures the efficiency of a cellular site. A high PAPR speaks to a host of challenges at peak demand hour: range and heat dissipation. The EVM measured at the receiver is the error when attempting to interpret data in a constellation. There is a tolerable amount of EVM for each constellation, decreasing with higher constellations. PlusN considers an example that assumes that the company want to minimize EVM for a 7-dB PAPR, which enables upgrading the constellation if the EVM decreases sufficiently.

Without the SCA, the network begins with a signal that has a 13.0 dB PAPR before introducing any EVM. To reduce the PAPR to a common 7.0 dB tolerance, the cellular site employs a crest factor reduction (CFR) technique that introduces additional error with an EVM of more than 6 percent.

The SCA optimally combines the input waveforms, which reduces the PAPR from the original 13.0 dB to 9.5 dB before introducing additional error. Instead of CFR, PlusN uses tone injection to trade off fidelity (EVM) for further PAPR decrease. The effect is similar to that of CFR, though tone injection reduces the PAPR from only 9.5 dB to 7.0 dB, but it also introduces some EVM. However, this use of tone injection for the smaller reduction in the PAPR only introduces 2.5 percent EVM instead of more than 6 percent from the CFR version (from the original 13.0 dB PAPR).

Quadrature Amplitude Modulations

64-QAM cannot accommodate the 6 percent EVM in the version without the SCA because the data for each point bleeds too much—the receiver cannot discern where a bit is supposed to be. In practice, the network would use 32-QAM instead of 64-QAM if the EVM were more than 6 percent, but 64-QAM can accommodate 2.5 percent EVM. In version with SCA, the network is

able to upgrade the constellation employed for a specific subscriber from 32-QAM to 64-QAM. All subscribers would have similar upgrades of one constellation, implying a 2x lift in capacity by adding the SCA to an existing CA application of three CCs each of 20 MHz.

BIO: John Terry, Ph.D., is a recognized industry expert in wireless communication system design and implementation, with specialization in OFDM and MIMO. Terry is a much sought-after expert analyst for law firms and is a member of the Army PEO-I Independent Review Team to assess Technology Readiness Level (TRL) and Software Readiness Level (SRL) for ASAALT. He previously served as principal scientist and director of baseband system at Nokia Research Center and WiQuest, respectively. In both roles he was responsible for guiding R&D teams in the development of OFDM-related products.

Terry has extensive experience supporting wireless standard activities, including serving as vice chair of the IEEE 802.11g standard and as a contributing member to the WiMedia 1.0 PHY specification. He also has participated in 3GPP-LTE and ITU-R standardization bodies. A senior member of the IEEE, Terry has generated more than 25 pending/issued domestic and foreign patents related to wireless technology, including three essential patents for the Digital Chaos™ Technology. He also is the co-author of *OFDM Wireless LANs: A Theoretical and Practical Guide*.

Terry earned his doctorate from Georgia Institute of Technology and has received numerous technical achievement awards.

The New Cyber Army

Michael Chung, Head of Solutions, Government, Bugcrowd Inc. •
michael.chung@bugcrowd.com

ABSTRACT

Today's Army requires advanced technologies such as mobile ad hoc networks to carry out mission-critical objectives. Assured and constant communications are essential to gaining and maintaining situational advantages and timely decision making to carry out warfighting missions. Using these advanced digital and network technologies can often leave forward-deployed units susceptible to exploits from multiple attack vectors. It's imperative to understand how adversaries can penetrate systems and, more importantly, how to harden them.

Attack vectors include:

- Application layer: Open to data corruption through SQL Injection and XSS
- Transport layer: Exploiting encryption methods and authentication by attacking TCP/UDP SYN
- Network layer: Interruption of the ad hoc routing and forwarding protocols
- Data link: Breaking down MAC protocol and degrading link layer security support
- Physical: Denial of Service (DoS) attacks and jamming by physically attacking the active interface by eavesdropping and jamming

To address the complex attack scenarios by enemy threats, the Army can leverage the resources of a digital army, comprising primarily the world's best white hat hackers and researchers, to provide live support for forward-deployed units. This approach can be broken down by splitting the crowd into Intrusion Detection Support Units (IDSU) and Vulnerability Assessment Units (VAU).

Intrusion Detection Support Units (IDSU)

These units will monitor traffic flow and packet types using statistical measures— standard deviation of the number of packet sizes—to determine different types of attacks. These units will comprise a set of highly skilled and diverse group of researchers/hackers to provide cover

for forward-deployed units in real time. This digital army can provide mission-critical protection during live missions and minimize the damage created by bad actors of enemy nation states.

Vulnerability Assessment Units (VAU)

These units will assess vulnerabilities prior to and during deployments to best reveal any weaknesses within the Army's network and hardware. They can help ramp up units before deployments by conducting real-life scenarios to help prepare the warfighters for the different types of attacks they may encounter and to outline secondary and tertiary protocols in the event of a malicious cyber event.

This next generation solution of leveraging a crowd of highly versed researchers and hackers to provide cover for forward-deployed units will be imperative to fight against cyber threats. There is no better solution than to have the world's best hackers provide real-time support for the warfighter and to mitigate the attack vectors that pose a threat to the military.

BIO: Michael Chung ran the Hack the Pentagon Program for the U.S. Defense Department. He has collaborated with Cybercom, the NSA, the Air Force and the Army in strategic hacking events. He is a former naval officer who served in operations Enduring Freedom and Iraqi Freedom (2000-2007). He has worked for a number of startups and technology companies including Apple.

Cybersecurity Training

Sean Hulbert, Founder and CEO, Security Centric Inc. •
shulbert@securitycentric.net

ABSTRACT

Security Centric will demonstrate live fire cybersecurity and hacking labs utilizing three skill levels. Once trainees have completed one of the three skill levels, they will be able to advance to the capstone project called Field Readiness, the ultimate training program under real-world conditions. In class or in the field, trainees will be able access Security Centric's secure cloud called Fortress and put their training to use.

Security Centric is able to rebuild any network topology within its cloud environment even infrastructure control systems such as those found in water plants, nuclear plants, oil pipeline control systems and stoplight subsystems. Security Centric is the first company in the industry to offer access to live IoT devices. It will demonstrate live hacking of IoT devices within its lab environment, which is critical to understanding how WiFi works and how hackers exploit flaws in IoT.

BIO: Sean Hulbert has more 30 years experience in cybersecurity, hacking and computer forensics. Author, co-author and developer of Jones and Bartlett ISSA training program, Hulbert also is the author and developer of Capella University's cybersecurity training program and a developing designer in the university's Capture The Flag environment.

Key Orchestration and Attestation for True System-level Security with IoT Devices

Robert McClellan, Enterprise Solutions Architect, Micron Semiconductors •
rjmcclellan@micron.com

ABSTRACT

Hardware and storage buyers have rightful concerns on the provenance of the technology being acquired, also known as securing the supply chain. Micron has noted this concern and has built technology branded Authenta in their embedded solutions that allows for demonstrating that hardware and firmware provided is in its intended state and has not been altered.

With key management technology providers such as Fornetix's Key Orchestration, it is possible to have a solution in place that can support Internet of Things-scaled attestation services. The availability of technology coupled with Micron's Authenta embedded technologies for memory, storage and firmware make this possible.

For example, during manufacturing, Micron can generate unique characteristics to a given Micron product. This information is provided to an Army customer to uniquely identify a given product and attest to the integrity of the product. This information can be registered into the Fornetix Key Orchestration Appliance and be used as a baseline to receive attestation requests.

As technology that uses Authenta is fielded, KMIP MAC-Verify Operations or Signature Verify operations are utilized against the Key Orchestration Appliance with information provided from the Micron Authenta embedded technology. If the Verify or MAC Verify is successful, then the Micron technology is in the same state that it was when it left.

The result is an ability to prove that memory, storage and other embedded components have not been tampered with from the point of manufacture to the point in which the attestation happens. If desired, deeper attestation can be demonstrated by using nonce and calculations that takes Authenta-Side processing to provide nonce and make a calculation off of it.

BIO: Robert McClellan is a seasoned technical solutions architect with more than 25 years of global systems engineering and technical consultative experience up and down the compute stack with an emphasis on compute, memory, storage and storage security. He contributes to research, design, test, evaluation, integration and implementation efforts to optimize systems and architectures from the core to the tactical edge for U.S. DoD/IC customers.

Building a Stronger Layer of Trust for IoT

Robert McClellan, Enterprise Solutions Architect, Micron Semiconductors •
rjmcclellan@micron.com

ABSTRACT

Building true system-level security for Internet of Things (IoT) devices involves creating layers of protection, using hardware roots of trust and ensuring that all subcomponents within a system are trusted. This foundation for trust at the component level includes strong identity and device authentication for both the IoT device itself and the content that resides in the non-volatile memory.

Micron's Authenta™ technology is a new solution that provides protection for the lowest layers of IoT device software, starting with the boot process. By combining a unique device-specific identity that only a hardware root of trust can offer along with the measurement capabilities necessary for in-memory secure boot, Authenta technology provides the strong cryptographic footprint necessary to authenticate IoT devices directly with a local or cloud-based host. This kind of device integrity will enable additional functionality, such as hardware-based device attestation and provisioning, as well as administrative remediation of the device. By infusing cryptography into the memory fabric, the Army can extend the highest levels of security and information assurance out to the tactical edge with cloud, cloudlets and IoT devices. This technology also has deep application potential in securing a supply chain.

BIO: Robert McClellan is a seasoned technical solutions architect with more than 25 years of global systems engineering and technical consultative experience up and down the compute stack with an emphasis on compute, memory, storage and storage security. He contributes to research, design, test, evaluation, integration and implementation efforts to optimize systems and architectures from the core to the tactical edge for U.S. DoD/IC customers.

Making Every Device a Vulnerability Analyst

Mark McLarnon, Chief Technology Officer, CyberPoint International •
mmclarnon@cyberpointllc.com

ABSTRACT

Convergence. Army experts are talking about it, the news is reporting on it and our enemy will exploit it. Attacks on ECB networks like the Tactical Internet (TI) and especially the Lower TI could be launched from halfway across the world today. As converging technology such as mobile ad hoc networking is brought online, the attack surface only increases. How are we supposed to keep pace?

Leveraging experience in Cyber Quest 2017, CyberPoint is working to bring its CATO platform to today's soldier. CATO is an extensible DCO platform for network and host enumeration, active and passive scanning, and even DCO-RA when credentials are available. CATO can be tasked from the BCT TOC by the 255S 25D as well as the members of a CPT.

CATO executes campaigns of operations to produce findings with severity ratings from None all the way to Critical. A CATO operation includes a series of one or more individual tasks utilizing popular open-source tools, such as vulnerability and port scanners and disruptive technology developed by CyberPoint, to fill gaps left by the best-of-breed open-source toolset(s). CATO tasks include support for manual tasks, parsing outputs from commercial and open-source tools that haven't yet been fully automated.

Thanks to its containerized architecture, CATO can be installed on a physical or virtual server for scanning endpoints in the TOC, on a ruggedized laptop for scanning and operating against endpoints on the battlefield, and on an embedded appliance (requiring only 5V of power) for installation on an aerostat or UAV or as a leave-behind device to scan a communications tower, router or similar device.

In addition to TCP/IP support, the CATO appliance brings multiple levels of USB-based RF support from 802.11 b/g/n/ac to Bluetooth 1-4.1 (class 1), software-defined radio and LoRA; new RF technologies are being added each month. Current operations include not only RF survey but also device profiling and vulnerability analysis for those devices that contain TCP/IP capabilities. At the push of a button, CATO can be programmed to constantly survey for vulnerabilities in Army mobile ad hoc networks.

CATO pre-canned operations can be scheduled for automatic execution without operator intervention and requested for execution with planner approval. It also offers the ability to construct new operation templates on the fly. From a single browser on WIN-T, a CATO mission planner could schedule operations for asset identification, vulnerability analysis, spectrum survey and waveform decoding (for supported mediums) covering devices on the Lower TI and Upper TI then share results with the BCT commander, mission planners at the division and operators all the way back to DODIN.

CATO is not "another pane of glass" in the TOC. CATO will integrate with existing Army systems at the push of a button, and the company is working with partners to ensure automatic integration into their cyber situational awareness systems.

BIO: Mark McLarnon has worked in defensive cyber operations for nearly 20 years from the Department of Commerce to the White House, across the Intelligence Community and overseas. Currently, he runs CyberPoint International's DCO and OCO product development, commercial DCO operations and DCO research and development. He holds patents in automated malware analysis and has been featured in numerous publications as a recognized authority in malware analysis, reverse engineering, vulnerability analysis and network exploitation.

Vulnerability Mitigation Through Enterprise Class Security Features and Active Flow-Based Monitoring

Gustavo Mendiola, Systems Engineering Manager, Cisco • gmendiol@cisco.com

ABSTRACT

Emerging mobile ad hoc networking (MANET) solutions are providing a level of mobility and flexibility that is unprecedented. However, development has been focused on survivability, range and throughput. While the inherent nature of a MANET provides a level of physical security, the MANET must have the same security feature set that an enterprise-class switch or router because the MANET is an extension of the enterprise network. Furthermore, user devices on the MANET must exchange mission information with systems on the enterprise network and should be afforded the same level of protection.

Cisco is proposing that MANET solutions include security capabilities such as 802.1x, network access control and other user and machine authentication features as enterprise-class devices. Furthermore, Cisco is partnering with leading MANET solution developers to enable flow-based security analytics using the Cisco Stealthwatch platform. Cisco Stealthwatch leverages industry-leading machine learning and behavioral modeling using telemetry from the MANET to detect advanced threats and respond to them quickly either in real time during missions or as post-mission analysis.

BIO: Gustavo R. Mendiola is the engineering manager for the Army Enterprise Region, leading Cisco solutions for the Army customer set. Mendiola retired from the U.S. Army as a network engineer after 17 years of service.

Darrin Pearce is a consulting systems engineer focused on security and has been at Cisco for more than 12 years. He has spent the majority of his time at Cisco focused on the security needs of the U.S. Army.

Securing Mobile Ad hoc Networks Through the Comply to Connect Framework

Erick Messing, Manager, Systems Engineering (DoD), ForeScout Technologies Inc.

• erick.messing@forescout.com

ABSTRACT

Comply to Connect (C2C) is a U.S. Defense Department security framework that provides a much higher level of assurance for authentication, authorization, compliance assessment and automated remediation of devices connecting to the enterprise network. Within the C2C framework, all devices are authenticated and assessed for compliance against Defense Department security policy prior to being authorized and granted access to enterprise network resources. Compliant devices gain full access to the network. Non-compliant devices receive limited access to network services and are automatically remediated. Unauthorized devices are restricted and unable to access the network.

Securing a mobile ad hoc network (MANET) is another use case that illustrates the value of adopting the C2C framework as the foundation of cybersecurity for Defense Department networks. Knowing what mobile devices are connecting and ensuring each is compliant with organizational security policies create an environment that enables the MANET to move data from the source to the destination securely.

MANET Security Through Comply to Connect

The value of implementing MANETs within the C2C framework is that only properly managed and configured mobile devices will be allowed in the MANET. This is accomplished in three ways: control of the mobile device within the source network; control of the mobile device within the destination network; and assured compliance of devices that are within the MANET.

Control of Mobile Device at the Source

Controlling the access point where the MANET connects to the source infrastructure network allows security steps to be taken.

Step 1: Authentication and Authorization Policy (control network access)

Step 2: Pre-Connect Compliance Policy (compliance on connection)

- Mobile device is being managed
- Mobile device is properly configured
- Mobile device is properly patched

If the mobile device is not compliant, ForeScout will automatically block it from connecting, which would take it out of the shortest path solution of the MANET and protect the enterprise network.

Control of Mobile Device at the Destination

Controlling the access point where the MANET connects to the destination infrastructure network follows the same process described above for the source infrastructure network.

Assured Compliance within the MANET

Within the C2C framework, ForeScout prepares mobile devices to operate securely in a MANET by following the above process when the mobile device connects to the enterprise at the home station. However, in this case, when pre-connect compliance policy checks determine that a device is non-compliant, the ForeScout platform directs the device to a limited-access network segment where it is remediated. Once remediated and reassessed as compliant, the ForeScout platform provides full access to a network and continuously monitors the device while connected.

The result is that mobile devices are maintained fully compliant while accessing home station enterprise networks. As a result, when they are taken into the field and become part of a MANET, users can be confident that each device in the MANET is compliant with the latest standards and, if a device is compromised, the added controls keep any effects localized.

BIO: Erick Messing began his professional career 21 years ago as an officer in the U.S. Navy, where he served as a communications officer and an nuclear engineering officer aboard two surface ships. After leaving military service, Messing joined Booz Allen Hamilton and supported the Navy/Marine Corps Intranet program office. In this role, he developed information assurance strategy and was responsible for the management and deployment of numerous security solutions to the enterprise network. Specific areas of responsibility included endpoint security, full disk encryption, public key infrastructure, and identity and access management. He transitioned into a sales engineering role with ForeScout in 2012, selling ForeScout CounterACT to both Department of Defense and U.S. public sector accounts and delivering agentless visibility and control of all devices connecting to those customers' networks.

NetScout nGenius Cyber Operations at the Tactical Edge

Jerry Miller, Senior Army Account Manager, NetScout working with Granite Gov Solutions • jerry.miller@netscout.com

ABSTRACT

NetScout Systems is an undisputed market leader in proactive cybersecurity, network performance monitoring and network health monitoring capabilities. The NetScout products currently in use across the U.S. Defense Department, services and agencies have the ability to provide high-speed, on-the-wire, real-time always-on monitoring and analysis to enable holistic visibility into all data, voice and video traffic flowing across converged, global networks.

NetScout products are scalable at the strategic, operational and tactical layers of the network to meet the operational and functional needs of the world's largest and most demanding enterprise and service provider networks. When properly deployed and utilized, NetScout products proactively collect, organize and analyze traffic data in real time to enable organizations to go on the offense against performance degradations and avoid service outages. Additionally, NetScout Systems' products are capable of feeding API data to other modeling and simulation (M&S) tools that currently support the DoDIN and support their M&S requirements.

Currently, NetScout products are utilized by myriad customers across the DoDIN. A few of NetScout's customers Armywide include NETCOM, MEDCOM, USASOC, MEPCOM, ARCENT, PEO EIS, HRC and AAFES. This white paper is targeted at current and future customers to provide deeper insight about the power and capabilities NetScout can bring to the table in today's ever-elusive battle for superiority in cyberspace.

NetScout's further commitment to the Defense Department has led the company to develop the Collection and Development Platform (CAP). CAP is a self-contained deployable kit for defensive cyber operations and network and application performance assessments comprising NetScout's scalable enterprise-class products that ensure application services and cybersecurity.

CAP passively captures relevant packets from up to 48 1G/10G data sources using copper and fiber and can be employed either offline—not connected to a network being assessed for covert operations or when adding traffic to a network might contribute to the existing performance issue—or online. NetScout's product provides an effective platform to meet the problem of

understanding cyberspace security and cyberspace operations implications of a fully employed mobile ad hoc networking environment at the tactical edge.

NetScout will demonstrate how its products can provide for assured communications that are essential to gaining and maintaining situational understanding for accurate and timely decision making. If the Army employs mobile ad hoc networking solutions for combat operations, NetScout can help it understand how adversaries might compromise these networks so that it can preempt the threat and harden them.

BIO: Col. Jerry Miller, USA (Ret.), is the senior NetScout global account manager for the Army, U.S. STRATCOM, U.S. SOCOM, U.S. CENTCOM, INSCOM and AAFES. In his 30 years in the Army, Miller served and commanded at the tactical, operational and strategic layers of joint and Army networks. He has spent the majority of his career in operational units on both the conventional and unconventional side of the business. His last military assignment was as deputy commanding officer for NETCOM. Prior to that position, Miller was the chief of operations and plans, G357, for NETCOM. He is a former brigade commander of the 2nd Signal Brigade in Germany.

Device-Level Security in MANET

Emily Miller, Director of National Security & Critical Infrastructure Programs, Mocana Corp. • emiller@mocana.com

ABSTRACT

Perimeter-based defenses and threat detection technologies are not enough to defend against modern cyber attacks in mobile ad hoc networks (MANETs). The reality of modern warfighting necessitates lightweight mobile technology that integrates devices controlling ever more technologies, very likely including cell phones and other mobile wireless devices as nodes in MANETs. In this new environment, enemies seeking to cause harm will not only look to extract and/or corrupt sensitive data and information being transferred through MANETs but also leverage command and control capabilities against the devices themselves. Securing MANETs will require transparent, lightweight solutions that enable multiple protected mobile gateways—not only a handful of nodes—to affiliate quickly and maintain network resilience.

Rather than chase network vulnerabilities or simply seek to detect real-time threats against MANETs, there are two basic ways to address the long-term resilience of MANETs: 1) harden the code within the devices themselves to make them more resistant to manipulation and virtual tampering; and 2) protect the integrity of the data being transmitted between these devices to ensure authenticity and reliability of the information.

In its solutions brief, Mocana will discuss creating trustworthy environments for MANETs that lead to resilient and tamper-resistant solutions. Used by more than 200 OEMs to protect more than 100 million devices, Mocana's IoT Security Platform is a FIPS 140-2-validated embedded cybersecurity software solution that ensures device trustworthiness and secure communications across devices by:

- Hardening devices with multifactor authentication using X.509 certificates and trust chaining
- Securing the boot process to validate the firmware, OS and applications
- Enabling secure, cryptographically signed over-the-air (OTA) and over-the-wire (OTW) firmware updates
- Integrating hardware or software-based roots of trust such as TPM, SGX, TrustZone, HSMs, SIMs, and MIMs
- Replacing open source crypto software such as OpenSSL

Reducing MANET Vulnerabilities by Eliminating Network Control

Ram Ramanathan, Chief Scientist, goTenna • ram@gotenna.com

ABSTRACT

One of the key vulnerabilities in current mobile ad hoc networks (MANETs), especially in a tactical communications environment, is the reliance on network control information (packets) for computing routes and/or broadcast backbones. Routing algorithms for MANETs can be broadly classified as proactive, for example link-state routing such as optimized link state routing (OLSR) or reactive such as ad hoc on-demand distance vector (AODV). Both these sets of protocols rely heavily on control packets—beacons and link-state updates—or route-discovery packets, respectively. If these control packets are compromised, application packets cannot be routed even though a physical route may exist. Similarly, backbone construction for efficient broadcast in many schemes, such as the multipoint relay mechanism in OLSR, relies on obtaining 2-hop topology information, typically using beacons.

An adversary can compromise such a system in several ways. For instance, the link-state update or route-response packets may be spoofed, advertising routes that direct all packets to the adversary; or a jammer may selectively jam the control packets using little energy to cause extensive damage; or eavesdropping on the packets might provide the adversary with valuable information on the network topology. While there exist mechanisms such as authentication and control packet encryption, these add overhead and complexity that are prohibitive in a low bandwidth wireless network.

goTenna contends that the very existence of control packets is not secure and proposes a novel approach where all control packets are eliminated. Routing or backbone state is created based on information in data packet headers, and data packets are routed or broadcast based on that state. The company has implemented and currently is testing a proprietary zero-overhead broadcast backbone creation approach for its goTenna devices that reduces the total payloads by a factor of two to three times more than pure broadcasting in random mobile networks. goTenna currently is investigating similar zero-overhead approaches for routing. By removing control packets from the system, the goTenna network is intrinsically much less vulnerable.

Furthermore, goTenna proposes that tactical radios may not need to have their encryption keys within but instead can move toward a public/private key architecture for all internal com-

munications as opposed to running on standard IP-based connectivity that relies on global encryption keys that can be entirely compromised with the loss of a single radio.

BIO: Ram Ramanathan is chief scientist at goTenna Inc. where he architects and helps build a decentralized off-grid wireless network. Ramanathan's research areas broadly include mobile multi-hop wireless networks, network analysis and control algorithms, graph theory and network science. He has published widely in international journals and conferences, including award-winning papers at IEEE MILCOM, IEEE INFOCOM and ACM SIGCOMM. He has served on the program committees of several conferences including MILCOM, MobiCom, MobiHoc and INFOCOM and was the TPC co-chair of MobiCom 2007. Ramanathan has served on the editorial boards of several journals and as the associate editor in chief for IEEE Transactions on Mobile Computing. He received his doctorate in computer and information sciences from the University of Delaware. He is a Fellow of the IEEE.

Electromagnetic Signature Reduction Properties of Synchronized Pseudo-Random Waveforms

Mike Calabro, Senior Lead Engineer, Booz Allen Hamilton •
calabro_michael@bah.com

ABSTRACT

Reducing EMS is a multi-dimensional trade space. Operators can reduce transmission volume or transmit in waveforms optimized to minimize EMS. Waveforms designed to minimize EMS may be complex to process and low powered. They are therefore susceptible to denial or require complex antenna assemblies.

Booz Allen proposes a time-synchronized pseudo-random waveform to enable secure communications. These can be resistant to classical profiling techniques without significantly increasing waveform processing requirements. Typical signal profile techniques exploit signal properties and periodicities in the time or frequency domain such as symbol rate, statistical features of different modulation schemes or known power spectral densities. Booz Allen's proposed encoding technique would remove these features at the physical transmission layer.

This solution depends on establishing and maintaining tight time synchronization between transmitter and receiver pairs. In addition to detailing this proposed encoding technique, Booz Allen will discuss global, regional and local methods to establish and maintain this synchronization securely and resiliently.

JERICHO Bringing PON to the Tactical Environment

Kevin Helmick, President, Technical Control Consultants LLC •
kevin.helmick@tc2.us

ABSTRACT

JERICHO was developed as an answer to several long-standing issues in the tactical area of operations. One of these issues is extending transmitters back outside the wire to mitigate RF seeking munition threats. The company utilizes cutting-edge technologies and tactical fiber to accomplish the task. It couples this with another RWI interface to operate single-channel assets and cross band all these assets together over an IP soft client. The next step is to reduce EMI by eliminating most of the copper IP fabric required in the camp by utilizing commercial capabilities to connect all the LAN users over tactical fiber. This approach has been tested and found to be extremely effective. The company also uses this technology to reach out to LP/OPs that are located at much greater distances outside the wire. This allows full access to communication resources back at the main location, including the radio assets, telephony, email and chat, all accomplished via fiber. Coupled with some security appliances available today, the technology also can monitor the dead space in between for troop/vehicle movement, for example, giving new capabilities to resources already deployed. Technical Control Consultants also has reduced the number of hardware vulnerabilities, eliminating thousands of IP vulnerable points. The miniaturization of the computing apparatus required to implement this new network reduces size, weight and power as well. By switching from copper to fiber, environmental exposure, such as weather, also is mitigated by eliminating lightning strike probabilities.

BIO: Master Gunnery Sgt. Kevin Helmick, USMC (Ret.), was a technical control chief and systems planning engineer. He has owned a Service-Disabled Veteran-Owned Small Business for more than 10 years. He has more than 30 years of tactical communications experience and is a veteran of operations Desert Storm, Enduring Freedom and Iraqi Freedom.

Voice Transmissions for the Soldier Radio Waveform in an EMCON Configuration

Carla Russo, Senior Lead Engineer, Booz Allen Hamilton •
carla.s.russo.ctr@mail.mil

ABSTRACT

The software-defined nature of modern tactical radios allows for the rapid development and deployment of new features to address emerging user needs without replacing fielded hardware. Recent global events have exposed a need for the U.S. Army to develop mitigations to threats arising from electromagnetic emissions. In response, a new electronic protection mode of the Soldier Radio Waveform (SRW), commonly referred to as EMCON PTT, was developed and delivered to the U.S. Defense Department Information Repository for industry to integrate. A prototype version was tested in a representative electronic support environment. The relatively simple techniques employed also are expected to provide a robust voice-only capability to address the electronic attack threat, and further testing is planned.

EMCON PTT provides a voice-only capability that maintains radio silence when the user is not actively placing a voice call, while minimizing the over-the-air profile during active transmissions. Unlike legacy systems, some overhead is necessary to complete a voice call in the absence of GPS. Careful consideration of tradeoffs between electronic protection and performance were made throughout the design process.

Modifications maintained over-the-air interoperability, a requirement that has historically prevented the implementation of groundbreaking enhancements to the main operating modes of the Army-owned waveforms. The recommendations of the IDA Air-Land Mobile Tactical Communications Network Assessment will enable true innovation in the area of electronic protection to take place.

The new mode was delivered by the CERDEC S&TCD SRW Reference Implementation Lab (RIL) and integrated by the SwISS vendor into the SRW formal baseline for release to the vendor community as a fully qualified SRW 1.2.2.1 within one year of concept development.

BIO: Carla Russo has been a systems engineer with Booz Allen Hamilton since 2012 supporting PM Tactical Radios and previously CERDEC S&TCD. Currently, she is the lead systems

engineer for the Army's enterprise Over The Air Management, a waveform agnostic protocol to facilitate remote key and radio management activities for Unit Task Reorganization. Russo also has been heavily involved in the PM Tactical Radios threat response.

Russo came to Booz Allen Hamilton from ITT Industries where she worked as a modeling and simulation engineer on the Soldier Radio Waveform (SRW) and Soldier Level Integrated Communications Environment programs and a systems engineer for the Ground Mobile Radio and SRW Network Management programs. While in CERDEC, she developed and validated a free automated test suite for tactical radio verification testing. She received her Bachelor of Engineering and Master of Engineering degrees in electrical engineering with a concentration in wireless communications from Stevens Institute of Technology in 2004 and is a certified Project Management Professional and Cisco Certified Network Professional.

Network Transport in a Contested Environment - Solution Concept

Patrick Ward, Senior Associate/Chief Technologist, Booz Allen Hamilton •
ward_patrick@bah.com

ABSTRACT

The Army today has an immediate requirement to ensure flat, fast, mobile and protected network transport in contested environments. Contested environments exist within operational theaters today. Contested means the risk to stationary U.S. assets increases significantly over short periods of time.

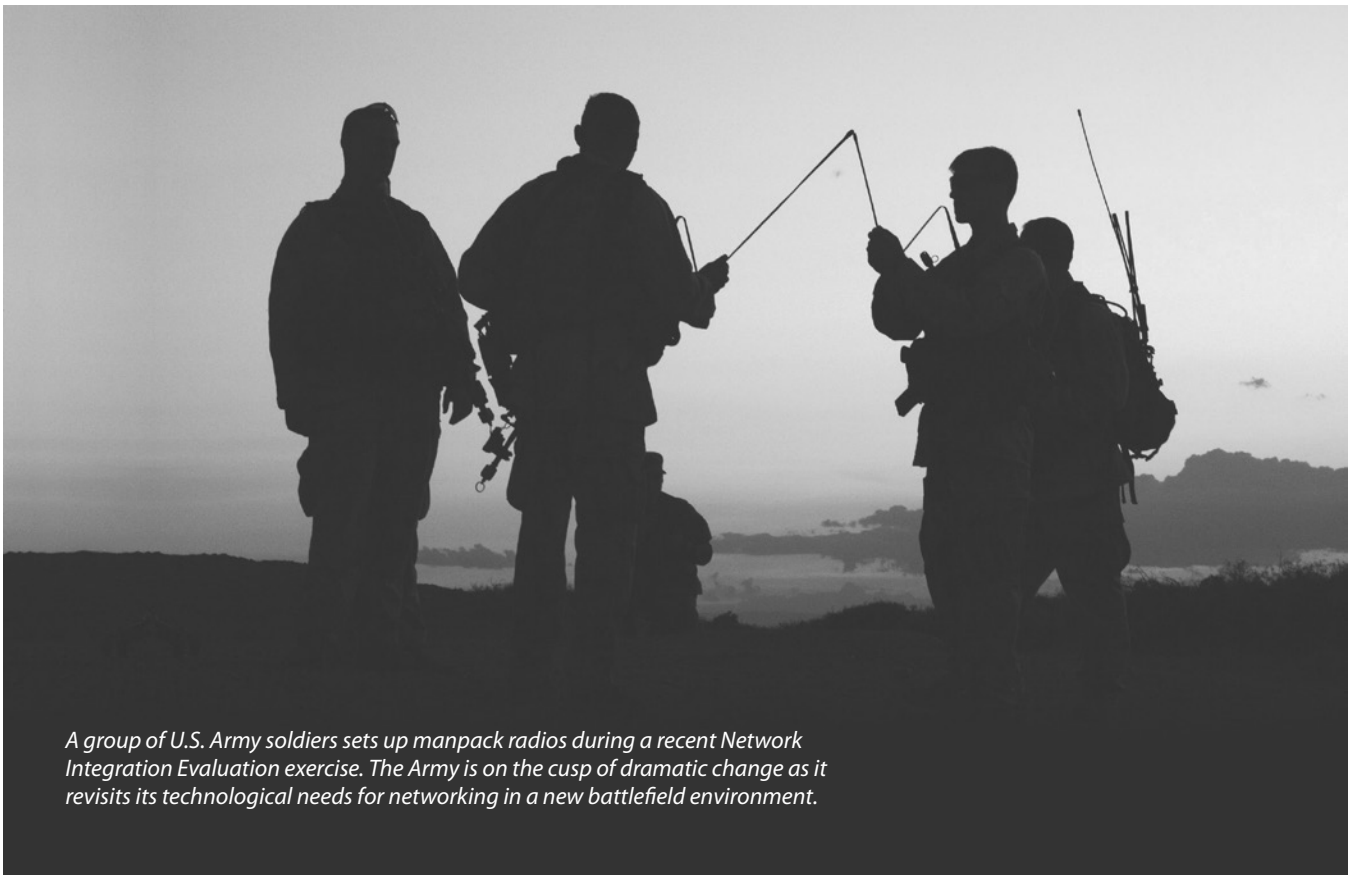
Today, commercial off-the-shelf (COTS) technologies can be combined to deliver highly available, high-capacity transport in a contested environment. These technologies must be simple to install, operate and maintain as well as resilient in a denied/degraded electromagnetic and space environment.

One possible solution concept combines: 1) low-EMI physical transport media in the local and wide area network like terrestrial optical transport, free-space optical communication, wideband satellite communication and light fidelity (Li-Fi) visual light communications; 2) software-defined wide area network (SD-WAN) devices and orchestration; 3) EM-shielded/protected chassis and containers; and 4) novel physical-layer network device maneuver systems, such as low-cost drones, to distribute terrestrial optical fiber rapidly across and throughout an area of responsibility. This solution concept would provide high-capacity, resilient, low-EMI common network transport over a geographical area. Individually, each of these COTS systems is somewhat complex and has certain operational vulnerabilities. When combined, they offer multiple options for commanders and Signal staff to provide flat, fast, mobile and protected network transport in a contested environment.

BIO: Patrick Ward is a chief technologist and engineer in Booz Allen's Defense & Intelligence Group. Ward provides enterprise information environment capability development and engineering support to clients in the U.S. Defense Department and Headquarters Department of the Army. He is managing Booz Allen's investments in network modernization and resilience. Ward has a Master of Science degree in computer science and a graduate certificate in computer security and information assurance from The George Washington University and a Bachelor of Science degree in computer systems engineering from Boston University. He also is a certified ITIL v3 Expert and a CISSP. Ward is a member of AFCEA and the IEEE Computer Society.

Army Aims for Network Modernization

The service's CIO and G-6 charts a digital change in direction.



A group of U.S. Army soldiers sets up manpack radios during a recent Network Integration Evaluation exercise. The Army is on the cusp of dramatic change as it revisits its technological needs for networking in a new battlefield environment.

BY ROBERT K. ACKERMAN

The U.S. Army is creating a new definition of communications on the move as it prepares to shift from past information systems. Without weakening operations, the land service looks to incorporate a state-of-the-art class of capabilities by overhauling its relationship with technology providers.

These new requirements owe their origins to innovative technologies as well as to international near-peer pressure. Emerging network capabilities offer more flexible and effective ways of operating just as potential rivals improve their own information warfare measures in ways that constitute broad-based threats to the Army.

The very nature of force command and control is changing both doctrinally and physically. Threat capabilities already demonstrated by potential adversaries in theater pose a significant challenge to Army operations, and many strike at the heart of network-enabled warfare.

Lt. Gen. Bruce T. Crawford, USA, Army chief information officer (CIO) and G-6, reports that the changes looming in Army tactical networking have been building over several months of review. Among the near-term conclusions is that the service's network does not meet the requirements of operational commanders. "The network that we currently have is not the network we believe we need to fight and win against a peer adversary," he declares, adding that the term "network" represents the Army's full information enterprise. This includes the transport—the Warfighter Information Network-Tactical (WIN-T)—along with tactical radio strategies and mission command systems.

This enterprise is neither optimized nor mobile, and it is too complex, fragile and vulnerable, easy to detect and

jam, and difficult to secure, the general explains. He says these conclusions lead to a defining question: "If the network that we have is not the network that we need, then what are the characteristics and attributes of the future state that we should build toward?"

First and foremost, that future state must feature a network that is survivable and protected, the general says. The network also must be intuitive, interoperable and sustainable as well as standards-based. And it must be highly mobile.

"If you're not moving every hour on the battlefield, then it's unlikely that you'll be able to survive," he warrants. "We're moving into a new age where gone are the days when technology that allows you to orient, decide and act faster is tied to a fixed command post or office. Things are born mobile these days. The development from day one is armed with an assumption that this capability has to be mobile—which is a game changer in terms of our thinking going forward."

The Army has a three-part strategy for addressing its network challenges. The first part is halting programs that do not meet new objectives. The second part is fixing the Army's ability "to fight tonight," he says, which identifies four priorities. Those include improving command post survivability and mobility; creating a universal transport layer for devices to select the right medium to send messages; developing a universal suite of mission command systems and applications; and adding air-to-ground integration to joint and coalition interoperability.

The third part ensures that the Army does not find itself in the same fix five years from now. This will require a pivot to a different method of acquiring equipment. "It's not just what we buy. It's a strategy that changes how we buy," Gen. Crawford emphasizes. The Army must move away from activities such as overprescribing requirements to its industry partners and instead assume a position where it is articulating its intent. He describes this new process as "adapt and buy."

The process enhances experimentation and demonstration on the front end, streamlining acquisition time, among other improvements. It would entail incorporating feedback from soldiers and commanders into what the Army buys. This would bring operators and industry developers closer so that the commercial sector would have better insight into how each user interfaces with products.

And the Army would shift away from a lowest price technically acceptable (LPTA) approach to more of a best-value method. "I do not believe LPTA should be a one-size-fits-all for every source-selection methodology when we get ready to buy something," Gen. Crawford offers. "Given what we are looking for in terms of the quality of the product, I think we have to go best value in some of our source-selection methodologies. And to get to a best-value approach, the Army must really think through what we are really looking to pay more for in a best-value proposition.

Lt. Gen. Bruce T. Crawford, USA, is the Army chief information officer (CIO) and G-6.

"You can expect the Army to start behaving more like a customer instead of just a consumer—the way we have been approaching the delivery of capability in the past," he warrants.

From this move, industry would gain the predictability it seeks to fulfill the Army's needs, and the service would obtain the flexibility it wants. "Ultimately, what we are looking for is what's the best return on investment for the Army," he says. "The process that we currently have is not a road to lead us to getting that best return on investment."

Having been in his position only a few months, Gen. Crawford emphasizes that he did not assume his billet with any agenda. He spent the first four months visiting many Defense Department and Army organizations and speaking with a range of personnel worldwide before his plans began to take shape. He tapped expert opinions from the monthslong review as well as the experience of technologists and operators.

His vision is an Army network that comprises four characteristics: flat architecture, speed, mobility and protection. He explains that the flat aspect meshes well with ongoing network convergence efforts in which more than 60 disparate Army networks are being consolidated. Network speed addresses Army battlefield requirements for fast action. Mobility acknowledges a change from static environments to combined arms maneuver and wide-area security against an evolving hybrid threat. And protection is the linkage to cybersecurity as well as the G-6 support to Army cyberspace operations.

The general says the Army is not near this vision yet. "There's a lot of work that has to be done to achieve that objective state," he says. "There will be more to follow as we unfurl this."

Central to achieving this vision are several priorities. His top one is readiness: "the idea of fixing what we have to enable the current fight," Gen. Crawford states. He offers that for the past 16 years of continuous combat, the force purchased a lot of information technology, and these acquisitions did not include actions that would generate an effective life-cycle sustainment process. For example, the Army lacked a structured, integrated technical architecture because of many contingency acquisitions.

The general's second priority is to modernize the information technology acquisition process. He wants the Army to "influence, shape and leverage" the marketplace instead of reacting to it. Over the past 16 years, the Army neither was postured to understand what technology was available nor quickly

Army satellite transportable terminals establish links with orbiters to provide communications support to ground forces. The Army faces a pressing need for better antijam satellite communications amid an increasingly hostile electromagnetic environment.

integrated that technology into warfighting formations. This was nobody's fault, he emphasizes, but the service must change. Developing an overarching plan for how to integrate new technology will require institutional change, the general states.

Shaping the force is Gen. Crawford's third priority. Both uniformed and civilian information technology personnel must be properly aligned in size, scope and responsibility across the service, he imparts.

The general's fourth priority involves cybersecurity policy. As Army CIO, he is responsible for cybersecurity, which is a critical enabler for the operational commander in cyberspace. This cyber policy must move from a compliance focus to a readiness focus, Gen. Crawford states. The Army must articulate cybersecurity's importance to cyberspace operations, and doctrine, tactics, techniques and procedures must reflect this.

Fixing Army tactical networking is only part of the battle. Enterprise initiatives face similar challenges, such as network flattening, and these are the general's fifth priority. Establishing baselines for enterprise initiatives would help the Army leverage the initiatives to increase force lethality, Gen. Crawford says.

The final priority he names to realize a more modern network is to optimize information technology resourcing to reduce risk and increase operational effectiveness.

That is a tall order, but the biggest challenge confronting Army information technology is keeping pace with the ever-evolving threat. The new networking plan is "threat-informed," the general declares. "We've had an opportunity to closely monitor and study the actual threat to our network," he explains. "It's not just the cyberthreat; there are electronic warfare threats."

Tactics, techniques and procedures have played out from the Russian New Generation Warfare Study, a recent paper that examined how soldiers will meet threats between 2020 and 2040, he continues. "What Russia was able to do on the cheap was to tie sensor to shooter using very cheap drones and cellphone technologies for direct and indirect fires and virtually decimate immobile command posts," Gen. Crawford says.

He points out that the Army also must extend the range of its line-of-sight capabilities without operating at full power all the time on the battlefield—a perfect scenario for detection by a hostile power.

A related problem is that the electromagnetic signatures emitted by command posts reduce their survivability in the electronic warfare (EW)-kinetic environment. Traditional doctrine has called for cutting the emissions put out by each box in the command center, but the new approach is to allow command posts to hide in plain sight among ambient noise, Gen. Crawford states. This does not entail raising the noise level to hide signals, he emphasizes, but simply camouflaging command post emissions among everyday noise. "We've advanced technology to the point where we ought to be able to leverage that capability," he asserts. "It reduces the risk of emitting electromagnetic signatures on the battlefield in our command posts, and ultimately, it is a game-changing technology."

He notes that the Army is asking industry to invest in this approach.

The general adds that the Army is putting Wi-Fi in its command posts, and it is looking at Li-Fi, a wireless optical networking technology that

uses light-emitting diodes (LEDs) for data transmission. The technology switches LEDs on and off quickly for signal linkage, which would prove more difficult to detect by an adversary that is not inside a command center. Gen. Crawford says the two wireless technologies can coexist.

Another concern is the lack of an antijam satellite communications capability. The past 16 years have seen the Army become overly reliant on satellite communications, but the service's operational systems are not antijam. The only antijam capability the Army has is in the 278 legacy Secure Mobile Antijam Reliable Tactical Terminal (SMART-T) units in the inventory the service is striving to modernize. Gen. Crawford stresses the need for industry to come up with the next generation of antijam satellite waveforms.

Among the other challenges the Army must overcome to improve its networking are internal cultural issues. The service needs to remove its risk-averse mindset and replace it with a test-faster, more experimental and demonstration-oriented mindset, Gen. Crawford posits. This mindset must say, "We're going to take risks in the development and integration of commercial technologies," he emphasizes. Commercial investments in networking made over the past few years are bearing fruit, but this is happening much faster than the Army's current processes will allow it to harvest them.

At the same time, challenges bring opportunities, and Gen. Crawford sees several inherent in the new networking approach. First, the Army can have a closer partnership with the commercial sector. "We cannot achieve the objective state without commercial industry really understanding what we are trying to accomplish," he says. In meetings with industry leaders, the general asks them, "What policy changes are required to achieve the objective state?" He emphasizes that the Army's networking goals cannot be realized without fundamental policy changes, and he seeks industry's input on those changes. Debate over LPTA versus best value surfaces frequently, he notes.

Gen. Crawford also asks industry leaders how the commercial sector can be brought closer to users to gain a better understanding of how operators interact with products. The difference between simply fulfilling a requirement and learning what the user actually needs manifests itself in complexity that confronts the user in the field, he offers.

Above all, the Army wants the best potential technologies from industry. "What we really need is industry showing us not just what technologies are available today, but helping us paint the picture of what's in the art of the possible," Gen. Crawford states.

In addition to antijam waveforms and reduced electromagnetic signatures on the battlefield, several other technologies can help Army networking, the general says. At the top of the list are artificial intelligence and machine learning, which allow personnel to automate activities and make decisions faster—both in delivering capability and operating on the battlefield, he notes. Advances in these areas "will allow us to better see ourselves and take stock of the various pieces of software that are out there," he says.

The Army also needs technologies to automate information sharing and analysis, Gen. Crawford continues. "Data has almost become a new currency: the ability to protect it, the sharing of data, the interest in analyzing it," he declares.

Advances in robotics continue to drive innovative thinking about their use, especially in the evolution of autonomous vehicles on the battlefield. "As I look at autonomous vehicles, I think about the network being flat, being fast, being mobile and being protected," Gen. Crawford offers. "What network do I need to put in place to be able to allow autonomous vehicles to operate on the battlefield? You're literally moving from autonomous vehicles to weaponized autonomous vehicles that can be remotely controlled."

WHAT IS AFCEA?

AFCEA is a member-based, non-profit association for professionals that provides highly sought after thought leadership, engagement and networking opportunities. We focus on cyber, command, control, communications, computers and intelligence to address national and international security challenges.

The association has 31,070 individual members, 139 chapters and 1,625 corporate members. For more information, visit www.afcea.org

For a PDF version of this Solution Showcase, go to

https://url.afcea.org/signalconferenceabstracts18