Bringing Mobile Ad Hoc Networks to the battlefield using COTS open standards

The U.S. Army is creating their Enterprise Network utilizing standards-based commercial technology. However, utilizing commercial products to network combat vehicles, aircraft, and soldiers on the battlefield where there's no fixed infrastructure may not pass muster. A better COTS network is needed.

By Dave Barker, Extreme Engineering Solutions

The U.S. Army has a mandate to get better real-time information to soldiers on the battlefield – in the Army's vernacular, "providing the network to the tactical edge". This tactical edge is a soldier, and the mandate is to provide voice, data, and video to soldiers wherever they are – mounted in combat vehicles or dismounted. The tactical edge is part of the Army's "tactical network" – a network of fixed and mobile assets on the battlefield that is a component of the Army's Warfighter Information Network-Tactical (WIN-T). WIN-T is a critical enabler for the Army's LandWarNet, or the "Network", which is the Army's contribution to the DoD's Global Information Grid (GIG).

To create the Network, the Army has established the Common Operating Environment (COE), which defines a commercially based set of computing technologies and standards to which the Network itself and all applications and systems residing the Network must adhere. Alignment with the COE is now mandatory for new systems and capabilities. Much of the Network, including Enterprise and Tactical Servers, Client (desktop and laptop systems), and the networking equipment required to connect these portions of the Network, can use commercial hardware and software. The Army is even planning to support commercial PDAs and smartphones for mobile connection into the Network. However, commercial hardware will not always work for combat vehicles, aircraft, and soldiers on the battlefield where there is no fixed networking infrastructure (Ethernet cables, hot spots, ISPs, etc.) in place (Figure 1).

Networking on the Battlefield

There are some major differences between creating a traditional fixed infrastructure network and providing a battlefield network to the tactical edge. The obvious differences are that the networking equipment must be rugged to withstand the harsh battlefield environment and must be Size, Weight, and Power (SWaP) optimized because it will be carried by soldiers or deployed in combat vehicles.

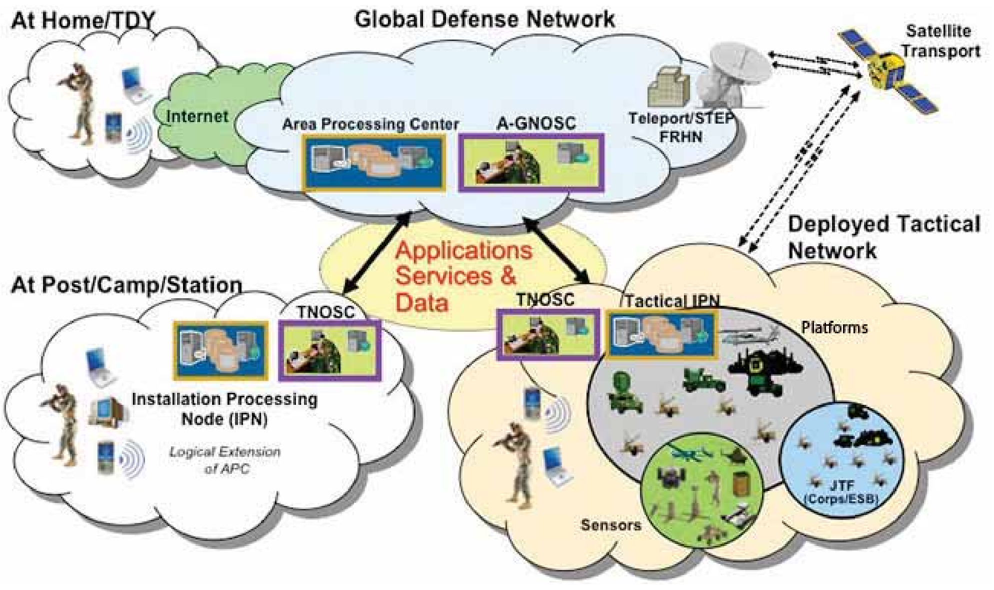

Figure 1: The Global Defense Network is the Army's contribution to the DoD's Global Information Grid initiative. The Global Defense Network includes the Tactical Network which integrates Platforms (combat vehicles and aircraft), Sensors, and soldiers on the battlefield. (Courtesy: the Army's Office of the Chief Information Officer.)

However, there are other differences because of the inherent nature of a battlefield (Table 1). On a battlefield, there is no fixed networking infrastructure. Soldiers and assets are mobile. Even if they do not have a connection back to the Network at the command post, they still have a need for voice, data, and video communications with each other. Since assets are mobile, traditional IP routing using static routing tables

Fixed Networks	Battlefield Networks
Commercial grade hardware	Ruggedized hardware
Large, heavy, power hungry	Size, Weight, and Power optimized
Centralized control	No central point of control
Routing seldom changes	Routing often changes

Table 1: Differences between fixed infrastructure networks and mobile battlefield networks

is not suitable for creating networks. Neither will dynamic routing protocols used in fixed networks work well in the dynamic environment of the battlefield because the network convergence time is too slow to support the real-time communication requirements.

As stated in the COE Architecture document:

> "The COE will leverage commercial-off-the-shelf (COTS) solutions and other commercial capabilities first, including open source solutions. The objective is to leverage market-leading COTS technologies to the fullest extent possible and to utilize DoD solutions for military-specific needs. Customization of packaged applications will be minimized. Reuse of existing packages will be exploited where possible."

Where commercial COTS products cannot satisfy the requirements for platforms on the battlefield, military COTS products will need to be used to satisfy the LandWarNet and COE requirements.

In the civilian world, what we call the Internet is made up of fixed networking infrastructure – routers, gateways, switches, ISPs, wireless access points, etc. – and the only components that are mobile are wireless clients. If a wireless client is not within range of a wireless access point, it has no access to the Internet. The Internet can be thought of as a central point of control that is always available for clients to connect into. This may not be the case on the battlefield because there's no fixed networking infrastructure, and all of the infrastructure equipment has to be mobile and carried with the troops. Even if there is no access to the Tactical Network, soldiers and combat vehicles still need to communicate. Since their communication is IP-based, the clients need to have the ability to create their own ad hoc network with no central point of control.

Mobile Ad Hoc Networks

Without any fixed networking infrastructure, a battlefield network has to be created "on the fly". This is known as a Mobile Ad hoc NETwork or MANET (Table 2). A MANET is a self-configuring, infrastructure-less network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction and therefore will change its links to other devices frequently. Each must participate in routing traffic unrelated to its own use.

Self-forming	Nodes that come within radio range of each other can establish a network association without any pre-configuration or manual intervention.
Self-healing	Nodes can join or leave rapidly without affecting operation of the remaining nodes.
No Infrastructure	In an ad hoc network, mobile nodes form their own network and essentially become their own infrastructure.
Peer-to-peer	Traditional networks typically support end systems operating in client-server mode. In an ad hoc network, mobile nodes can communicate and exchange information without prior arrangement and without reliance on centralized resources.
Predominantly Wireless	Historically, networks have been mostly wired and enhanced or extended through wireless access. The ad hoc environment is essentially wireless, but can be extended to support wired resources.
Highly dynamic	Mobile nodes are in continuous motion, and ad hoc networking topologies are constantly changing.

Table 2: Characteristics of mobile ad hoc networks

The fact that these networks are self-forming and self-healing facilitates deployment and minimizes the need for manual configuration and intervention. They support multi-hop networking to extend coverage and provide redundant paths for increased resilience. Ad hoc networks also can operate with or without connectivity to a centralized network.

The Army has chosen to deploy equipment for the Tactical Network in combat vehicles, which makes perfect sense because it's easier for vehicles than soldiers to carry the equipment (Figure 2). Dismounted soldiers can still connect into the MANET as clients with IP-enabled military radios or smart phones. Each vehicle carries the networking equipment necessary to join and participate in a MANET (Figure 3).

There are two key pieces of networking equipment used to create MANETs – IP-enabled radios and IP routers. In order to make the network usable, both the radios and routers need to support Radio Aware Routing (RAR) protocols.

Several radios that currently support RAR can be used as the wireless transport layer in MANETs. The Highband

Figure 2: Networking equipment for battlefield networking shown at Network Integration Evaluation (NIE) 12.1 in 2011. (Courtesy: U.S. Army.)

Figure 3: Mobile Company Command Posts (CCoP) displayed at NIE 12.1 in 2011. (Courtesy: U.S. Army.)

Networking Waveform (HNW) radios, the Linkabit Network Centric Waveform (NCW) SATCOM radio, Joint Tactical Radio System (JTRS) Wideband Network Waveform (WNW), Tactical Common Data Link (TCDL), Tactical Targeting Network Technology (TTNT), SATCOM, Enhanced Position Location Reporting System (EPLRS), and PRC-117/152 radios all are IP-enabled and support RAR.

Routers Supporting Radio Aware Routing

When a link or router fails in a fixed infrastructure network, the network must reconfigure itself to reflect the new topology by updating routing tables, possibly across the entire network. Until the network reconverges, it is in an unstable state. The time it takes for the network to reconverge is known as the convergence time. It can take several minutes for a network to reconverge using the Routing Information Protocol (RIP) or Interior Gateway Routing Protocol (IGRP). A network of a few routers using the Open Shortest Path First (OSPF) can converge in a matter of seconds.

On the battlefield, vehicles are moving in and out of visual and radio range. Terrain, weather conditions, antenna type, and mobility make radio communication dynamic, causing constant changes in routing. When communicating real-time voice, data, and video, soldiers cannot wait minutes or even seconds while the network reconverges. There is a need to have routing protocols that can gracefully and quickly handle these dynamic changes. That is what Radio Aware Routing is designed to do.

RAR enables a radio to provide a router with information about the quality of links between radios and can report on the presence or loss of potential routing neighbors. Key to the concept of RAR protocols is that a router may connect to a radio using standard Ethernet, but the radio can convey information about the true characteristics of the over-the-air radio links to the router, including the actual available bandwidth, delay, or link quality. This functionality is critical with today's dynamic radio waveforms, which can vary frequencies and power based on current conditions in real time. The resulting changes in bandwidth or other characteristics must be communicated to a router using the radio channels, in order to apply QoS or to communicate metric information within routing protocols.

> ***This may not be the case on the battlefield because there's no fixed networking infrastructure... all equipment has to be mobile and carried with the troops.***

The actual available bandwidth to any given radio neighbor may, in fact, be different from any other neighbor and certainly may be different from the bandwidth of the physical connection between a radio and a router. The bandwidth to any specific neighbor also can change, and such changes need to be taken into account for both IP routing and Quality of Service. Neighbor up/down signaling enables routers to provide faster network convergence by reacting to link status signals generated by the radio, rather than waiting for protocol timers to expire. Routers can factor link quality metrics reported by radios into their OSPF- or IGRP-based route cost calculations. Utilizing bandwidth metrics, routers can provide flow control for data to minimize the need to queue and buffer data in radios, allow voice to be prioritized over video when radio links are degraded, and provide consistent QoS for networks with multiple radios.

In addition to radio aware routing, the routers used in military MANETs must provide other critical functionality. Some of the more important features they must support are IPV6, Type 1 and next-generation Suite-B encryption, threat control and intrusion prevention through the integration of firewalls, QoS, and traffic management.

Small and Rugged Too?

The Network Integration Evaluation (NIE) is a series of semi-annual events intended to further integrate, mature, and rapidly progress the Army's tactical network. As seen in Figures 2 and 3, there were some rather large and non-ruggedized pieces of networking equipment at the NIE 12.1 event in 2011. The WIN-T program will be implemented in four increments. Increment 2 provides initial networking on-the-move, giving commanders in the field the same level of communications they would have from the Tactical Operations Center (TOC). WIN-T Increment 2 successfully participated in NIE 12.1 in fall of 2011. Figure 3 shows a vehicle at NEI 12.1 equipped with a Mobile Company Command Post.

These photos show that capabilities can be demonstrated, but these technologies are far from being ready for deployment on a battlefield, for instance, inside a Bradley Fighting Vehicle or Stryker. The networking equipment is just too big and heavy. The networking functionality to create MANETs has to be provided within the combat vehicles' SWaP budget and must be able to pass the appropriate MIL-STD-810 environmental and MIL-STD-461 EMI specifications.

When communicating real-time voice, data, and video, soldiers cannot wait minutes or even seconds while the network reconverges. That is what Radio Aware Routing is designed to do.

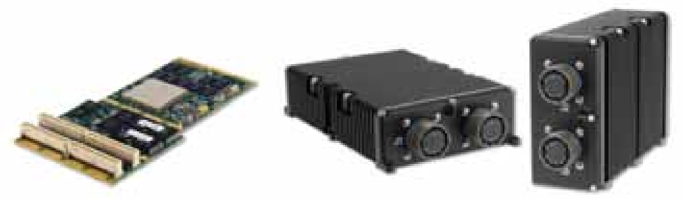

Figure 4: The Extreme Engineering (X-ES) XPedite5205 PMC/XMC Embedded Services Router (ESR) and SFFR packaged router. Both provide 4 Gigabit Ethernet ports and run Cisco IOS Software.

Routers that meet the SWaP and ruggedization challenges, as well as support the latest RAR protocols and necessary security features, are the Extreme Engineering Solutions (X-ES) 4-port XPedite5205 PMC/XMC-based Embedded Services Router (ESR) with Cisco IOS, and the SFFR packaged 4-port router with Cisco IOS (Figure 4). The XPedite5205 ESR is the smallest available rugged router of this class on the market – it can be integrated into equipment to be deployed in a vehicle. The SFFR packaged router weighs less than 3.5 lbs. and displaces less than 72 cubic inches. It can be deployed immediately in almost any ground vehicle or aircraft.

What the Future Holds

WIN-T Increment 3 is to provide full networking on-the-move – MANETs utilizing line-of-sight radios, UAVs, and satellite communication. NIE 12.2, occurring in May/June of 2012, is still focused on WIN-T Increment 2. This means that WIN-T Increment 3 will happen sometime in the future.

There is still work to do in the area of radio aware routing to support MANETs. The RAR protocols need to be supported in the radios and the routers. The latest RAR protocol, Dynamic Link Exchange Protocol (DLEP), is not yet an RFC; it is still in the draft phase, which means it cannot be specified yet in RFQs.

There is another initiative that could affect how WIN-T is implemented. The Army's VICTORY initiative defines an IP-based network in combat vehicles to drive [literally and figuratively, Ed.] interoperability in order to reduce system redundancy and SWaP. The VICTORY architecture includes several routers, encrypter/decrypters, and firewalls in each combat vehicle. Since routers can have encryption and firewall capabilities built in, it is technically possible that the same router in a vehicle used to create MANETs could also provide the router, encryption, and firewall capabilities that are required by VICTORY. This would further reduce SWaP in the vehicle. However, at this time, it is unknown how VICTORY and WIN-T will play together.

The Army WIN-T, the Air Force Joint Airborne Layer Network (JALN), and the Navy Automated Digital Network System (ADNS) initiatives all support the goal of the DoD's Global Information Grid to get the right information to the right place, the warfighter, at the right time, anywhere on earth. They all have similar requirements and challenges. There is still a long way to go, but industry is developing the technologies to support this massive upgrade to the U.S. fighting forces.

Dave Barker is the Director of Marketing at Extreme Engineering Solutions (X-ES). He headed marketing and business development at VMETRO and was the VME product manager at the Motorola Computer Group. Previously, Dave held a number of software development, technical marketing, and marketing roles. Dave has a BS in Computer Science from the University of Pittsburgh and an MBA from the University of Phoenix. http://www.xes-inc.com