TACNET: MOBILE *AD HOC* SECURE COMMUNICATIONS NETWORK

Loren E. Riblett, P.E.
Sandia National Laboratories
PO Box 5800, MS-0775
Albuquerque, NM 87185-0775
USA

James M. Wiseman
Sandia National Laboratories
PO Box 5800, MS-0775
Albuquerque, NM 87185-0775
USA

Abstract – On the road and during tactical maneuvers, the Blue Force must maintain situational awareness to effectively react and respond. The Tactical Network, or TacNet, is a mobile *ad hoc* communications network developed by Sandia National Laboratories to provide Blue Force personnel with secure access to critical data, such as real-time maps of resource positions. During development of the system, the Sandia team addressed a variety of issues, including the need for (a) mobile communications without fixed infrastructure and (b) security features, e.g., an access control list. The team considered commercial-off-the-shelf products, but determined that a semi-customized system would better suit its requirements. The final product, TacNet, a field-tested and proven mobile network, incorporates two major systems: (1) an In-Vehicle System, including a graphical user interface, and (2) a Dismounted Solution, also known as Tracker. TacNet employs a line-of-sight mesh radio network, which is self-forming, self-healing, and multi-hopping. Both the In-Vehicle and Tracker systems can be applied in combination or separately to a variety of purposes, including real-time training analysis, targeting capability, and friend or foe identification. This paper describes the development process for TacNet and its future potential, such as extending line-of-sight through unmanned aerial vehicles.

Index Terms – *ad hoc* communications network, secure mobile communications, Blue Force

INTRODUCTION

The Tactical Network, or TacNet, is a mobile *ad hoc* communications network that provides a roving Blue Force with secure access to critical data, such as real-time maps of resource positions. Developed by Sandia National Laboratories, TacNet incorporates two major systems: (1) an In-Vehicle System, including a graphical user interface (GUI), and (2) a Dismounted Solution, also known as Tracker. TacNet employs a mesh radio network, which can be tailored to particular missions and provides the Blue Force with the following capabilities:

- Blue Force personnel can send data (e.g., messages, maps, photos) over a line-of-sight mesh radio network, which is self-forming, self-healing, and multi-hopping.
- Only vehicles/personnel on an access control list can exchange information, ensuring flexibility and protection.
- Enhanced security features provide additional assurance, including Triple Data Encryption Standard (DES).

TacNet interfaces between wired and wireless networks using either the Sandia-developed TacNet Vehicle Module (TVM) or a commercial off-the-shelf (COTS) solution. TacNet's advantage over other wireless networks is its ability to operate on the road among moving vehicles without fixed infrastructure. Both the In-Vehicle System and Tracker can be applied in combination or separately to a variety of purposes, including real-time training analysis, targeting capability, and friend or foe identification.

During development of TacNet, the Sandia Communication Systems department addressed a variety of issues, including the need for (a) mobile communications without fixed infrastructure and (b) security features. The team considered using only COTS products, but determined that a semi-customized system would better suit its application's requirements. This paper provides (a) background leading up to the current TacNet system, (b) development decisions and existing features, and (c) expected future enhancements.

BACKGROUND

For the past two decades, Sandia National Laboratories has investigated solutions to improve security for mobile communications. Historically, mobile communications have primarily used point-to-point radio links, e.g., Radio A communicating with Radio B. In the early 1990s, Sandia researchers pursued advances in communicating location data through the Intraconvoy Vehicle Data Network (IVDN) project. During this project, Sandia developed a communications protocol that passed location information; however, no attempt was made at that time to incorporate Internet Protocol (IP). Although IVDN was considered adequate for a group of three to four vehicles, its control features were narrowly focused and not adaptable to large-scale efforts.

In early 2000, Sandia researchers began to evaluate various *ad hoc* networks, including offsite research with Mesh Networks Inc. Mesh had manufactured the *mēa* (mesh enabled architecture) product, a mesh network that had evolved from studies sponsored jointly by the Defense Advanced Research Projects Agency (DARPA) and U.S. Department of Energy (DOE). The *mēa* Mesh product attracted commercial customers such as municipalities—e.g., police, firefighters, and maintenance crews—who needed a means to communicate among themselves in real time. The *mēa* Mesh network system is composed of a subscriber device (card), a vehicle-mounted modem (VMM), and a mobile integrated switch controller (MISC). Current commercial systems, such as the 1000-plus node system operating in Garland, Texas, depend on fixed infrastructure, such as wireless routers on telephone poles, to complete the network.

Mēa was the first attempt by Sandia's Communication Systems department to use purely *ad hoc* communications for the Blue Force. In early 2000, wireless components were so new to the field that the Sandia team had to conduct their initial testing offsite (i.e., away from the military base on which Sandia is located) because of early security concerns over wireless. However, extensive offsite testing indicated that the *ad hoc* network worked well, could be scaled up, and could operate at highway speeds. This latter point was particularly important for Sandia's application, which depends upon mobile communications without infrastructure. Based on research and testing of the mesh network, the Communication Systems team at Sandia believed this network held promise for its application.

Sandia's network design, TacNet, added layers of utility to the original *mēa* Mesh network product. In particular, Sandia developed a system that (a) provided connectivity to a complete in-vehicle network, (b) operated in a mobile environment without fixed infrastructure, and (c) incorporated additional security features.

DEVELOPMENT OF CURRENT SYSTEM

Sandia developed TacNet to provide authorized Blue Force personnel, in a mobile environment, access to messaging and other critical data, such as maps with real-time positions of vehicles and assets. TacNet is being released in two phases: In-Vehicle System (2007) and Tracker (2008).

The In-Vehicle System serves mobile security forces by providing communications among vehicles, including messaging and map displays. Using a touch-screen In-Vehicle GUI, the Blue Force can exchange data, images, and voice over the mesh radio network. Asset positions are displayed on street-level and topographical maps inside each vehicle. Only authorized vehicles can exchange information, ensuring flexibility and security. TacNet can also be connected to a wired network, providing data refresh, increased speed, and communication with central command.

Tracker, also known as the Dismounted Solution, extends the In-Vehicle System by adding portable communications for individuals in the Blue Force. Sandia developed Tracker to enable individuals to communicate securely via portable handheld units. Tracker provides numerous capabilities—including the potential for Bluetooth communications, Universal Serial Bus (USB) ports, and image displays—within a ruggedized, pocket-sized unit. Sandia's Tracker is designed to accommodate several network options, such as Motorola's Mesh radio network or 802.11 wireless. When combined with a radio network, individuals can communicate securely across unpredictable terrain.

Development of TacNet In-Vehicle System

The TacNet In-Vehicle System extends the existing Sandia-developed Vehicle Network System (VNS).

Vehicle Network System (VNS): Sandia's existing mobile communications Ethernet-based network, VNS, is designed so that users can communicate to a command center using high-frequency (HF) radio or digital messages via Qualcomm. VNS is composed of several wired components that are identical in each vehicle within a fleet. The user interacts with the VNS communication devices via a touch-screen GUI. VNS was designed so that all fleet vehicles would deploy identical sets of network and communications devices, thus facilitating maintenance and updates. The network addresses are consistent throughout the fleet.

On its own, VNS allows communications from vehicles to a command center in a spoke-like configuration, i.e., each vehicle can communicate with the command center and, via the VNS GUI, can display maps with an icon representing its own location. The addition of TacNet expands this network by providing a means to network among authorized vehicles along the highway. For example, with TacNet, the map displays icons representing real-time locations of all authorized vehicles.

Mobile ad hoc network: TacNet incorporates a mobile *ad hoc* network consisting of node types such as vehicles, trackers, and repeater nodes. The TacNet network is referred to as *ad hoc* because the network dynamically forms based on nodes available, i.e., when a transmitter discovers a node within a range, it forms a network with the node. If a unit becomes separated (e.g., line-of-sight is lost), the remaining components "self-heal" the network by forming another path.

TacNet interface with Vehicle Network System (VNS): Because of the VNS design, in which communications devices in each fleet vehicle are assigned identical IP addresses, the challenge for TacNet was to interconnect identically wired networks in a wireless network, while addressing each vehicle uniquely and securely. To span from a wired network with common addresses (VNS) to a wireless network with unique addresses (TacNet), Sandia used a bridging technique. This bridge is composed of a D-Link router and Motorola's VMM6300. Fig. 1 shows how TacNet is connected to the original VNS design.

The D-Link router and VMM6300 are housed in a Sandia-developed unit, the TVM (Fig. 2). The D-Link Ethernet router is the key to translating network addresses from a wired network address to a wireless network address, i.e., from a Local Area Network (LAN) address to a Wide Area Network (WAN) address.

TacNet associates each VMM6300 with a unique IP address. For this discussion, assume we have a VNS-TacNet vehicle containing a VMM6300 with a unique address of 10.150.235.9 (Fig. 1). Sandia designed the system so that the address on the WAN side of the D-Link router is one greater than the VMM6300 address, or 10.150.235.10. This WAN gateway address (10.150.235.10) is the unique value for addressing the vehicle configured with the TVM.

The LAN side of the D-Link router serves as the gateway between the VNS devices and TacNet. To communicate with TacNet, a VNS device must send data to and receive data from the LAN gateway's IP address, i.e., 192.168.1.254 (Fig. 1). The Mobile Interface Controller (MIC) for VNS uses the VxWorks operating system, which permits parameters specified in the gateway portion of the VxWorks boot parameters to send data to and receive data from the correct gateway address.

Operation without fixed infrastructure: TacNet is a pure *ad hoc* communications network that can operate without fixed infrastructure. Fig. 3 shows an example of vehicles in TacNet's mobile *ad hoc* network. In this example, the unique IP addresses for the three vehicles are: 10.150.235.10, 10.148.55.10, and 10.200.88.10

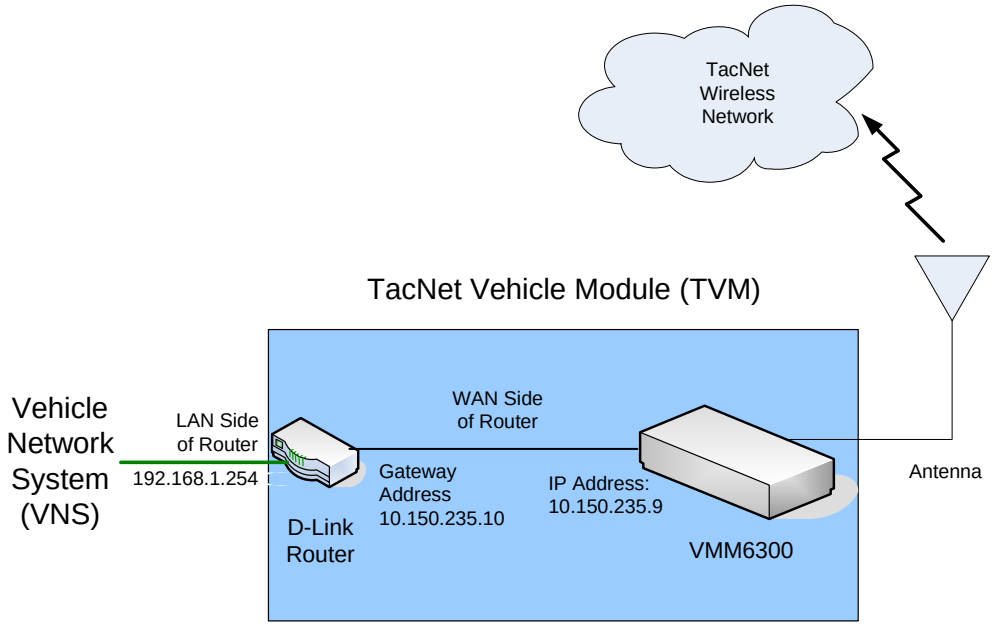

Fig. 1. TacNet interface to VNS Vehicle

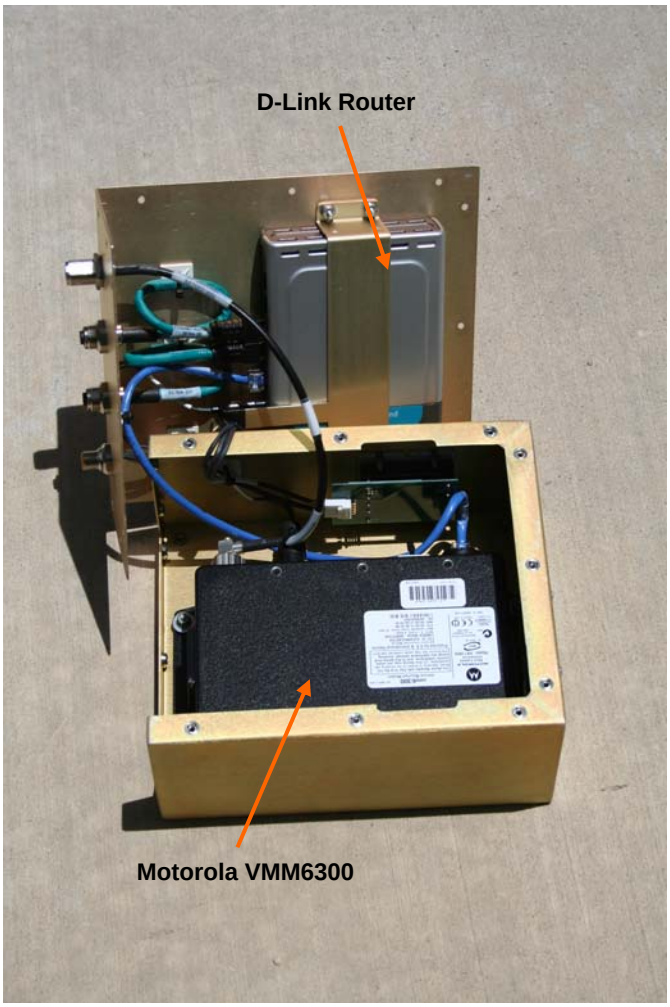

Fig. 2. TacNet Vehicle Module (TVM).

Although a limitation of the mesh radio network is line-of-sight, its ability to dynamically self-heal allows it to overcome some line-of-sight constraints. For example, assume Vehicle 1 sends a message to Vehicle 2, but Vehicle 2 is on the other side of a hill (Fig. 4). Vehicle 3, however, is in line of sight of Vehicles 1 and 2. In this case, Vehicle 3 receives the message and automatically resends the message, which is then received by Vehicle 2. To ensure security of messaging in this system, Sandia layered additional features onto the original mesh network system.

TacNet security features: With TacNet, when a transmission encounters a node that meets requirements to propagate, the node repeats the transmission, thus expanding the *ad hoc* network. Before TacNet transmits information, however, there must be assurance that only acceptable data recipients will receive the TacNet transmissions.

This assurance is achieved using an access list. Each vehicle has a uniquely defined access list, which is a list of IP addresses that are allowed to receive TacNet transmissions from a particular vehicle. For example, in our examples in Figs. 3 and 4, all three vehicles have the same access list and so are able to repeat and receive transmissions to and from each other.

The VMM creates the access list by (a) forming a neighbor list, i.e., any other mesh device in the area, (b) comparing the neighbor list to the master access list, which is a list of all hardware units in the network, and (c) creating a vehicle access list or “push” list, consisting of neighbor units that are also on the master access list.

Sandia selected User Datagram Protocol (UDP) data unicast transmission for the wireless network rather than TCP/IP. UDP unicasting is a connectionless protocol that runs on IP networks primarily to broadcast messages, and it does not break communications or have error responses or fault recovery. UDP unicasting simply transmits the message on virtual port 1000, which is used for port forwarding.

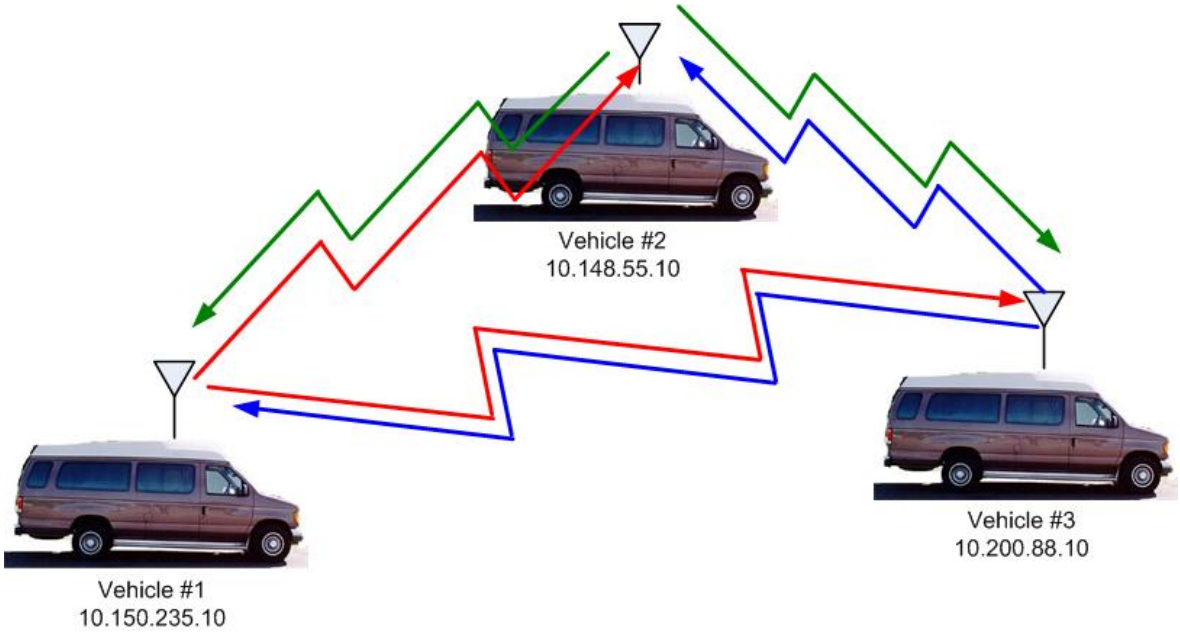

Fig 3. Three TacNet vehicles communicating over *ad hoc* network.

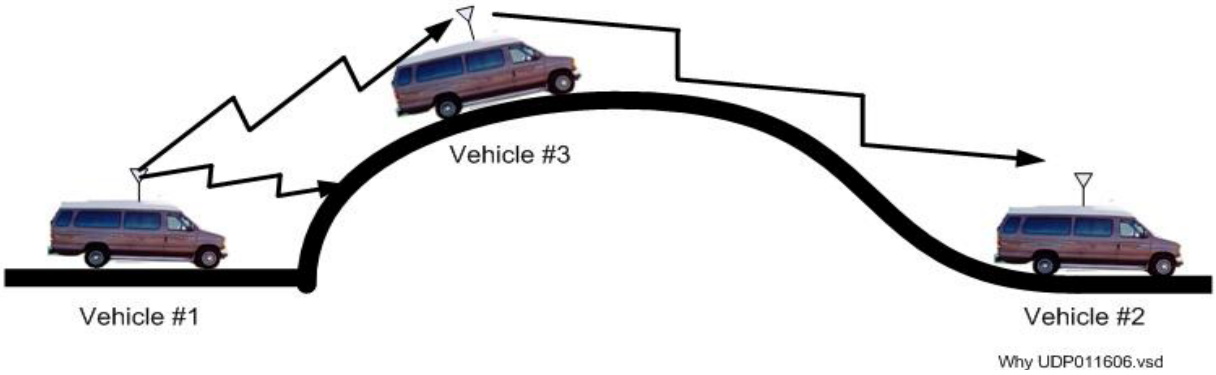

Fig. 4. Vehicle 2 receives message from Vehicle 1 via Vehicle 3.

Finally, TacNet incorporates Triple Data Encryption Standard (DES) to provide additional assurance that all messages can be read only by authorized vehicles.

In summary, VNS can be extended over a wireless *ad hoc* network using the TacNet system. Each vehicle can be identified uniquely, and triple DES encrypted data is permitted to flow securely from vehicle to vehicle based upon access lists.

Graphical User Interface (GUI). Although the touch-screen GUI was initially developed and installed with VNS, Sandia designed it with the increased capabilities of TacNet in mind. For example, with VNS only, the GUI displays the host vehicle's location; with TacNet, it displays icons that represent locations of all nodes on the vehicle's access list.

The GUI is a geospatial map-centric system that aids in situational awareness by displaying resource locations and messages. The GUI is the main interface device for the user and includes a messaging interface, via HF radio or digital messages; alerts, e.g., system or cargo state of health monitoring and alarm features; and custom maps. Alarms are presented via voice synthesis and color/shapes on map displays. Sandia selected a touch screen as its GUI so that it could be used easily on the road.

Currently, icons representing nodes are shown on the GUI via street-level and topographical maps. However, Sandia designed the GUI to accommodate potential enhancements. For example, in future versions a Blue Force responder with a portable Tracker may be able to call the

commander with the position of an adversary or obstacle; in turn, the commander could add the position to the GUI's map and the position could then be broadcast to all nodes on the access list (Fig. 5).

Fig. 5. In-Vehicle GUI touch screen.

Sandia developed the GUI with COTS hardware components, an MS Windows operating system, and software development kit. Hardware components include a Data 911 Inc. Central Processing Unit (CPU) and touch display with high brightness (1200 cd/m^2), a rugged external hard drive (for security requirements and operation in a mobile environment), and network connections. The map data engine (ESRI, Inc.) features layers down to street-level as well as topographic maps. Sandia developed GUI software in a Visual Basic environment, including extensions, e.g., file transfer protocol (FTP).

Development of TacNet Tracker (Dismounted Solution)

By early 2000, Sandia's customer had identified a need to extend the In-Vehicle System with portable units for a two-hour mission. Sandia's Communication Systems team began research on a "dismounted solution" in 2001. Initially, the team believed that a system could be developed using COTS products. Specifically, the team investigated using a rug-gedized personal digital assistant (PDA) with display, keyboard, and Bluetooth capabilities. The team used the IPAQ 5550 during demonstrations of the concept and anticipated being able to add mobile communications components (e.g., *mēa* Mesh transceiver, Global Positioning System [GPS] receiver) and then develop an application to control the communications.

However, early research showed that adding capabilities to a COTS product could not be easily achieved for the following reasons: (1) PDA architecture throughout the industry is closely held by the manufacturers, so that layering new applications is difficult and requires significant reverse engineering, (2) the PDA life cycle is only 18 months, yet Sandia's customer required a minimum 5-year obsolescence in hardware, and (3) the costs were high (about $5K to $8K per unit). In response, Sandia's Communications System team chose to develop a semi-customized design by (1) beginning with a reference design from Arcom, Inc., (2) developing the application and selecting hardware for the Sandia-developed design, and (3) contracting with a design manufacturing company to package the final design (Tracker). Sandia teamed with Arcom, Inc. because of its previous experience with projects that required large volume production and the use of reference designs.

The reference design selected by Sandia was Arcom's "Viper" board, which closely resembled the IPAQ 5550. Sandia's team proved the concept for its design with a prototype based on the Viper board, including a Sandia-developed application to control Tracker's components, such as GPS, and a Wind River Systems-developed VxWorks driver (developed from an existing Linux driver) for the *mēa* Mesh subscriber device.

Tracker is designed to use TacNet's mesh radio network, including all security features such as access lists and Triple DES data encryption. Sandia is currently testing five Tracker prototypes (Fig. 6). A total of 45 first production units (FPUs), with a final production run of 750, are expected by late 2007.

Fig. 6. Tracker prototype.

Tracker is low cost (<$1000 without radio) with hardware availability of 5 to 10 years. This pocket-sized, lightweight unit (Figs. 7 and 8) offers the following built-in features:

- 12-channel GPS receiver
- Composite video output
- Bluetooth enabled
- 50-way Input/Output (I/O) connector
- Compact Flash (CF) memory card socket and Personal computer (PC) Card socket for Mesh radio or 802.11 card
- Embedded antennas for GPS and 2.4 GHz radio
- Built-in rechargeable Li-Poly battery pack
- Joint Test Action Group (JTAG) interface (IEEE 1149.1 standard) to enable addition of custom operating systems
- Ethernet connection
- Serial and digital I/O lines; General Purpose I/O (GPIO) expander
- 64 MB Synchronous Dynamic (SD) Random Access Memory, 32 MB Flash
- Membrane keypad
- USB interface

Fig. 7. Pocket-sized Tracker.

Fig. 8. Tracker has a variety of built-in features.

TacNet Applications

TacNet In-Vehicle and Tracker systems can be deployed separately or in combination to enhance security options for a variety of purposes, such as (a) protective force situational awareness, (b) friend or foe identification (i.e., identifying which personnel have known authorized units), (c) enhanced Central Alarm Station (CAS) oversight of security systems, (d) vehicle dispatch, (e) real-time training analysis, and (f) day-to-day tracking and tactical operations.

FUTURE WORK

Sandia is currently conducting research and development into enhancements for TacNet's In-Vehicle and Tracker systems. As funding becomes available, Sandia intends to add the following features to further assist in Blue Force situational awareness.

Advanced Encryption Standard (AES)

To provide additional security for mobile communications, the Sandia team expects to replace the current Triple DES encryption with the more robust 128- or 256-bit AES.

Streaming Protocols

Currently, the In-Vehicle GUI displays text messages as well as street-level and topographical maps. Future enhancements may include streaming protocols over the *ad hoc* network for slow-frame rate video and voice-over IP.

Display Capabilities on Tracker

Tracker is already configured with an extension that would allow for additional display capabilities such as maps, photos, slow-frame rate video, and voice-over IP.

Beyond Line-of-Sight (BLOS) Capability

A current limitation of TacNet is its 2.4-GHz (microwave) system, which is line-of-sight only. Although its self-healing and multi-hopping functions significantly compensate for this constraint, Sandia is beginning research and development into capabilities that would improve BLOS capability. For example, Sandia is investigating the use of multiple radios (e.g., satellite) or unmanned aerial vehicles (UAVs) to extend line-of-sight. Another possibility under consideration is a short-range rocket that could be fired for temporary BLOS capability.

Communication by Proxy

TacNet expects to incorporate communication by proxy, which has the potential to reduce costs and provide redundant communication paths. For example, a convoy of vehicles might be assigned one vehicle with a relatively expensive broadband connection. When necessary, any other vehicle on its access list could also utilize that connection (Fig. 9). In the same vein, if a standard HF radio in one vehicle fails during a mission, Tacnet could seamlessly allow the user to continue HF transmissions by means of another vehicle's HF radio.

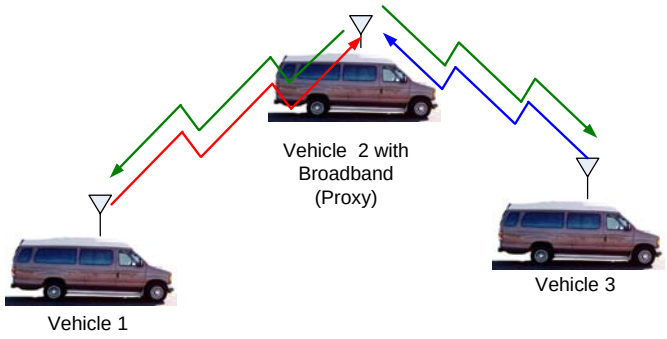

Fig. 9. Communication by Proxy

Targeting Capability

TacNet's Tracker, in conjunction with its In-Vehicle System, has the potential for identifying a target via GPS and securely communicating that information to the command center or other force multipliers.

CONCLUSIONS

TacNet's In-Vehicle and Tracker systems are field-tested and proven devices that provide pure ***ad hoc*** mobile communications that significantly contribute to increased situational awareness for the Blue Force. Although many applications leverage the research and data gathered for fixed site security and awareness, TacNet is unique in its demonstration that a purely ***ad hoc*** mobile communications network can operate at highway speeds and reliably move data. Its use of the self-forming, self-healing, and multi-hopping mesh radio network significantly overcomes the constraints of line-of-sight radio. Additional security layers, such as access lists and data encryption, ensure that TacNet can be used securely. Furthermore, its potential future enhancements promise that supplementary critical data can be moved freely and securely within a mobile environment and across unpredictable terrain.

ACKNOWLEDGMENTS

The authors wish to thank the following for their contributions to this paper: Greg Corbett (Sandia 6452), VNS GUI design engineer; Erik Dawson, photographer; and Janet Chapman and Patricia Oliver, technical writers.

REFERENCES

[1] *Mesh Networks mēa 3.1 Network Security Guide* (Document Revision 3.1.6)

VITA

Loren E. Riblett, P.E., is currently a Principal Member of the Technical Staff (PMTS) at Sandia National Laboratories in the Communication Systems organization (6452). Riblett has contributed to other technical areas at Sandia, including mobile communications, automatic target recognition, and seismic and acoustic sensors. Previously, Riblett worked for Allied Signal in the area of radar test equipment. Earlier papers include *Using Embedded Microcontrollers in Radar Test Equipment* by Richard S. Binney and Loren E. Riblett (Automatic Radio Frequency Techniques Group [ARFTG] Conference, Volume 17, May 1990) and *Acoustic/ seismic identifications, imaging, and communications in Steel Rattler* by Kevin T. Malone, Loren E. Riblett, and Thomas Essenmacher (Proc. SPIE Vol. 3081, p. 158-165, Peace and Wartime Applications and Technical Issues for Unattended Ground Sensors, Gerold Yonas, editor, 1997).

James M. Wiseman is currently a Member of the Technical Staff (MTS) at Sandia National Laboratories in the Communication Systems organization (6452). While at Sandia, Wiseman has worked in the area of mobile communications, building several hardware units with embedded controllers for fleet delivery. Previously, Wiseman was employed as a broadcast engineer for commercial radio stations and also worked for Allied Signal in the area of radar test equipment.