GENERAL DYNAMICS
Canada

Advanced Tactical Communications Mobility

Enabling Internet-like communications in mobile, ad hoc networks

Abstract

The most fundamental characteristic that differentiates a Tactical Internet (TI) from a standard internet is its core mobility: it cannot rely on any other elements of the TI to be present or at the same location for a significant period of time. While it can use fixed infrastructure and can even be connected to the commercial Internet, the protocols that underpin it cannot assume the presence of such infrastructure. Therefore, it must be able to adapt to situations where the paths between networks are constantly changing. To properly leverage Internet-based applications, military organizations need a solution that is tailored to operate within the context of a TI. The ideal solution should provide reliable data delivery by connecting the low bandwidth tactical edge network to the higher bandwidth core network. Most importantly, it must consolidate must-have networking features into an easy to manage network appliance designed and qualified for use in space constrained tactical vehicles.

Table of Contents

INTERNET-BASED APPLICATIONS AND THE TACTICAL INTERNET

As every commander knows, communication is the key to successful in-field operations. Without an effective communications system, intelligence information may not reach personnel when required, surveillance data may not be relayed properly, and reconnaissance observations may not arrive in time to be factored into command decisions. For this reason, military organizations around the world continue to search for the most efficient and effective communications solutions to enhance Command, Control, Communication, Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) efforts.

In this ongoing quest for advanced solutions many organizations are looking for ways to enable the always-on, instant communications capabilities of today's commercial Internet in a military environment. Ideally, this effort will allow familiar, Internet-based consumer applications, such as e-mail, instant messaging, and video chatting, to be adapted for use in military networks. This will enhance the bi-directional flow of communications between in-field mobile users, and between those users and the center of operations.

But while commercial communications networks continue to deliver advanced, multimedia communications applications to end users, military networks have been unable to do the same. The fact is that, to date, in-field military networks have been unable to leverage the Internet's network protocols and standards to provide the same applications military personnel have become accustomed to using at home. Quite simply, the very nature of in-field communications networks makes it almost impossible to recreate the Internet's network environment. By necessity, these networks must be mobile and ad hoc. Typically, they are established using low bandwidth high frequency (HF), very high frequency (VHF) or ultra-high frequency (UHF) radio links, and there is no fixed infrastructure to leverage. Most advanced, data-centric applications require high bandwidth links and, unlike military mobile networks, the commercial mobile networks that support them are all tethered to high bandwidth backbones, which provide the throughput quality necessary for data-centric applications.

In addition, the dynamic, self-forming, self-healing nature of mobile ad hoc networks does not offer the reliable end-to-end connectivity required to support advanced data applications. This makes it impossible for users to reliably exchange data information. More importantly, it does not allow for data prioritization, which is required to ensure that a commander's intent is properly relayed to in-field personnel.

Although some products have emerged that attempt to address these problems, most are not mature and don't completely address the quality, assurance and reliability transmission requirements. In addition, most of these options are not optimized to address the Size, Weight and Power and Cost (SWaP-C) concerns of current military platforms.

To properly leverage Internet-based applications, military organizations need a solution that is tailored to operate within the context of a Tactical Internet (TI) — a collection of heterogeneous, mobile, sub-networks inter-networked in a manner similar to the Internet. The ideal solution will provide reliable data delivery where Internet standards fail: at the low bandwidth and disrupted tactical edge network. It will connect the low bandwidth tactical edge network to the higher bandwidth core network. Most importantly, it will consolidate must-have networking features into an easy to manage network appliance designed and qualified for use in space constrained tactical vehicles.

THE REALITIES OF THE TACTICAL INTERNET

A Tactical Internet is a seamless network of heterogeneous sub-networks that have varying characteristics, but which must maintain communications links without a fixed infrastructure. Typically, this type of network is used by military organizations to provide communications services that connect strategic decision makers with commanders at deployed headquarters, and to extend that connection all the way to individual soldiers and vehicles on patrol. It is also used for deployable crisis management, border security, and search and rescue systems.

The most fundamental characteristic that differentiates a TI from a standard internet is its core mobility: it cannot rely on any other elements of the TI to be present or at the same location for a significant period of time. While it can use fixed infrastructure and can even be connected to the commercial Internet, the protocols that underpin it cannot assume the presence of such infrastructure. Therefore, it must be able to adapt to situations where the paths between networks are constantly changing. This creates communications networking challenges that cannot be completely addressed through the use of the commercial Internet’s Transmission Control Protocol/Internet Protocol (TCP/IP) suite.

In addition, a TI is usually comprised of a number of wired and wireless bearers. Constraints introduced by the geographic dispersion of nodes mean that it often needs to use bearers that operate in the VHF and HF ranges of the frequency spectrum. As such, there is usually a major variation in bandwidth (sometimes less than 1 Kb/s), latency and packet loss from one end of the network to the other.

Upper and lower components

For networking purposes, a TI can be divided into upper and lower components.

The **Upper TI** usually serves decision makers with communications applications that most closely resemble those of a typical corporation. For example, users of the Upper TI often require teleconferencing and video conferencing facilities, as well as the efficient storage and exchange of large quantities of data. As a result, high network capacity, low latency and low packet loss is of paramount importance for the Upper TI, but mobility is not. Therefore, standard Internet protocols are usually capable of supporting its communications needs.

By contrast, the **Lower TI** serves users who have ‘boots on the ground’, are geographically separated by significant distances, and are often on the move. For these users, high capacity, directional wireless communications technologies are often inappropriate. As a result, the Lower TI must use technologies that generally have much lower capacity, higher latency and greater packet loss than the Upper TI. Therefore, standard Internet protocols do not perform as well in this portion of the network.

Communications capability trade-off

Beyond its basic structure, a TI differs from the commercial Internet in the core technologies it uses.

The commercial Internet is built on internetworked technologies of like capability. It integrates sub-networks of high capacity and long range into the network core that forms its backbone. Unfortunately, to be effective for all users and address two levels of communications requirements, the TI must create a seamless, end-to-end communication infrastructure with a collection of sub-networks that have very different capabilities. In addition, the integration must be achieved in a manner that enables the network to adapt to the sudden inclusion or disappearance of any of the sub-networks.

All traditional communications technologies available to the TI are limited in some way by the range, capacity, and mobility trade-off (Figure 1).[1] In the Lower TI, range and mobility are most important, so the wireless sub-networks use the HF, VHF, UHF portions of the radio spectrum to address these requirements at the expense of capacity.[2]But the upper TI must provide high capacity and range. Therefore, the wireless technologies deployed in the upper TI typically include fixed, point-to-point radio sub-networks that employ Super High Frequency (SHF) trunk radios, and large, static satellite ground terminals for geo-synchronous X- and Ku-band satellite communications. These technologies provide capacity and range, as well as lower latency and packet loss, but offer little mobility.

New technologies are emerging that solve the range, capacity, mobility trade-off. However, these technologies tend to create infrastructure dependency. For example, the Upper TI can also have core mobility while maintaining high capacity. This can be achieved through the use of satellite communications on-the-move (SOTM) technology. However, this approach presents a significant cost to the network, which is beyond the means of most private organizations and many governments. Furthermore, SOTM relies on the presence and availability of a satellite network.

Likewise, some networked elements in the Lower TI can have high capacity, but at short ranges only.

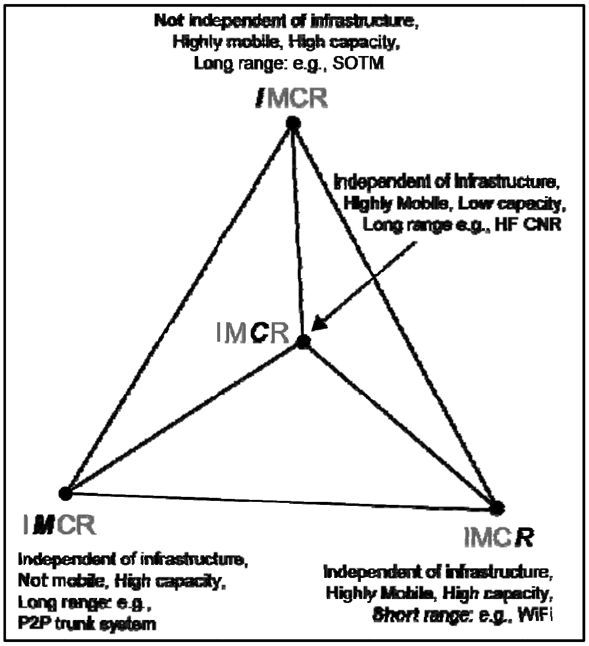
Not independent of infrastructure,
Highly mobile, High capacity,
Long range: e.g., SOTM
IMCR
Independent of infrastructure,
Highly Mobile, Low capacity,
Long range e.g., HF CNR
IMCR
IMCR
Independent of infrastructure,
Not mobile, High capacity,
Long range: e.g.,
P2P trunk system
IMCR
Independent of infrastructure,
Highly Mobile, High capacity,
Short range: e.g., WiFi

Figure 1. The range, capacity, mobility infrastructure independence trade-off

[1] "*Tactical Communications for the Digitized Battlefield*", M. J. Ryan and M. R. Frater, Artech House, Norwood MA, 2003

[2] "*Communications in the Digital Age. Volume One: HF Technology*", Harris Corporation, May 1996

Mobility challenge

The need for mobility also causes additional networking challenges in a TI.

Unlike the sub-networks in the Internet core, which are fixed, the sub-networks in a TI core — especially in the Lower TI —are mobile. This mobility continuously creates routing changes for networked traffic. Routing changes consume bandwidth, which is required to propagate routing updates in a timely fashion and may, depending on the time it takes for a new route to be determined and advertised, disrupt data traffic that is in transit.

In some cases, mobility may also cause network address changes, which can also affect traffic. If a network node changes its address then name-address bindings may need to be updated in addition to routing updates. As a result, packets addressed to the old address may be dropped, which means communications in progress at that time may fail. This has an impact on the way communications services are provisioned because advanced, Internet-based consumer applications, such as e-mail, instant messaging, and video chatting, require some level of name-address resolution to work properly. But the mobile nature of the TI core means that there is no guarantee any of the name servers in a list of preferred servers will be available at any given time.

Capacity and delay issues

The nature of the bearer technologies used to enable mobility and move traffic in a TI also present highly variable capacity and delay challenges. In this environment, name resolvers designed for the Internet will fail when high latencies are encountered. As a result, a name service designed to work in the high capacity, low delay fixed commercial Internet core may find that data transfer is a challenge in low capacity sub-networks. Essentially, a variation in delay may result in a routing protocol receiving information about a destination through high latency sub-networks long after deletion notifications arrive along low latency paths.

To resolve this problem, user applications must ensure that enough information is passed through the lowest capacity sub-networks and be able to recognize and deal with the wide range of latencies involved. In addition, routing protocols used in a heterogeneous network must be immune to delay and function when not all valid links or paths are known. This will allow the protocol to recognize old information, ignore it, and avoid a routing loop.

Disruption

The sub-networks of the TI are also prone to significant disruption. This may be caused by operational changes, such as an imposed radio silence, or the effects of electronic counter measures. Or it can be the result of technical challenges, such as terrain obstruction. Whatever the reason, these disruptions can result in end-to-end information being unnecessarily retransmitted when a single sub-network becomes unavailable.

The delay and disruption-tolerant networking (DTN) approach defined in current communications standards may provide a way of dealing with this in the TI. However, significant architectural work is required to create a DTN overlay network that works with the Layer 3 and Layer 4 routing and transport protocols of the TI.

Multiple security levels

The security of communications is also a challenge in the TI. To date, the majority of tactical radio networks have only supported one security level. Therefore, the internets that have been made up of multiple radio networks have also only supported one security domain. Typically, these networks rely on a single encryption device, which is often embedded in the radios. This is due, in large part, to the fact that single-level security mechanisms are easier to design, implement and accredit than their multi-level counterparts.

But, single-level security solutions are not viable in a network that must support a higher level of interworking of applications between users in the Lower TI and those in the Upper TI. The very nature of the communications and information these applications will carry requires a method of supporting multiple levels of security.

Multimedia support

Addressing all these challenges is extremely important for the accurate and efficient delivery of all applications, but it is critical for advanced, multimedia applications. Although data is more tolerant of delays, interactive, multimedia streaming applications, such as video conferencing, require short delays, high capacity, and no disruptions to be useful in a command and control environment.

In general, multimedia traffic is not useful over low capacity, high latency links. Unfortunately, source applications are not usually informed when only such paths are available. Therefore, there must be a way for applications to be informed about path characteristics and the links must be protected from potentially large amounts of data that may inadvertently be sent over them. For those links that may provide some useful bandwidth transcoding may be required to lower bandwidth streams. If the streams are encoded appropriately this may be possible at the source and the packets may be marked in a manner that allows only the appropriate subset to go over more constrained links.

Network configuration responsiveness

Finally, any attempt to introduce advanced Internet-based applications in a TI must take into consideration the dynamic nature of the Lower TI. By its very nature, the Lower TI is a constantly evolving and changing collection of heterogeneous sub-networks. Connections are made and dropped as required, when required. Therefore, the TI must be responsive to dynamic configuration changes, including adjustments to mitigate the effects of battle damage.

To be effective, configuration changes must be made in a manner that does not require extensive operator skill, excessive time, or a complex procedure to implement. Ultimately, changes must be applied in a manner that allows personnel to quickly get accurate information about the status of the TI, communications destinations available, bandwidth, and how much of that bandwidth is currently being used.

ENABLING ADVANCED APPLICATIONS IN A TACTICAL INTERNET

Given the inherent challenges associated with the TI, supporting advanced Internet-based applications that can enhance C4ISR efforts can only be achieved with a solution that can collect information about the quality of the path linking one user with another:

- The capacity of the slowest link in a path;
- Packet latency, excluding queuing delays and hop count;
- Packet loss rate;
- Congestion, measured as the expected queue length of the most congested link in the path;
- Stability, locally calculated as a function of expected time remaining for a path to a destination.

Once collected, the ideal solution will use this network information to enable applications or users to adapt to network changes and deliver application data to its destination, regardless of mobility, latency, and capacity issues.

Using network information

If the network information is integrated with application data, all applications must be provided with a standard networking Application Programming Interface (API), which will make the applications network-aware. Unfortunately, this requires a substantial investment in the reprogramming of applications, which is an unrealistic expectation for most applications that may need to run over a TI.

The most realistic approach is to allow unmodified applications to run over the TI, and enable network information to be used by a layer of services operating between user applications and the network. These services intercept network transmissions from applications and re-package the transmissions using protocols suitable for the TI, in effect acting as a transparent proxy. With this approach, applications are not provided with path feedback directly. Instead, path feedback is provided to users who can then adjust their communications behavior based on the indicated path quality to an end point.

Managing ephemeral data

In addition to using a transparent proxy, the ideal solution should also be able to manage the transmission of all data more efficiently. This includes short-lifespan, low-volume ephemeral data, such as position reporting data and, in some cases, tactical naming updates, as well as data used to achieve tactical time synchronization. Transmission efficiency of this data can be achieved by optimizing the use of bandwidth.

A feature of tactical radio networks is that transmissions usually occur in a frame. Frame sizes are quantized due to the use of interleaving and forward error control blocks. As a result of this quantization, there are usually unused data bytes in a radio transmission. These unused spaces are too small to carry another large IP application packet, but are often big enough to carry a routing update packet, position report, or time distribution update. Therefore, significant improvements in performance can be obtained if the frame packing protocol can use this free transmission bandwidth to manage overhead and adapt to route changes.

Leveraging transport protocols

Enabling Internet-based applications on a TI will also require a more effective use of transport protocols.

The TCP is the primary transport protocol used in the Internet. Unfortunately, this protocol does not work well in the Lower TI because it cannot:

- Distinguish between loss due to congestion and loss due to corrupted packets caused by other factors, such as RF interference;
- Support multicast delivery efficiently because packet streams are not sufficiently protected against the impact of RF interference, fading and link outages;
- Provide a coherent strategy for handling long outages.

A number of protocols have been designed, developed and fielded for the Lower TI in the past five years, which address the problems associated with the use of TCP. These protocols use a combination of packet level forward error correction (FEC), congestion control based upon inter-packet arrival time analysis, and algorithms for fast start and fly-wheeling through link and network outages. They can be configured to provide users with a real time picture of the progress of message delivery to each of the intended recipients. And they are able to take advantage of the broadcast and semi-broadcast mechanisms of tactical radio networks.

The Negative Acknowledgment (NACK)-Oriented Reliable Multicast (NORM) transport protocol is an example of a new protocol engineered to work in the TI and deliver these benefits.

Optimizing routing protocols

In addition to transport protocols, the ideal TI communication solution must be able to optimize the use of routing protocols.

Many TI bearers come with their own interior gateway protocol that provides a functioning routing solution for individual sub-networks. However, to enable Internet-based applications on the TI these sub-networks must be stitched together into a single TI. Since classic route redistribution schemes are not robust enough to operate under the degree of heterogeneity within a general TI, an intermediate level routing protocol is required to provide an automated, self-healing TI.

The Inter-Autonomous Routing Domain (Inter-ARD) protocol can be used, but it must be as lean as possible. It must compress the information as much as possible when working with low capacity sub-networks. And it must be immune to delay and function when not all valid links or paths are known.

In addition, since paths will change over time it may be appropriate to ensure that data meant for paths through higher capacity sub-networks does not get re-directed through low capacity sub-networks when changes occur. This can be achieved by using DiffServ Code Points (DSCP) to mark packets so they aren’t allowed to congest low capacity sub-networks. Similarly, DSCP settings for precedence can be used to ensure that high priority packets gain preferential access to low capacity sub-networks.

Using multicast protocols

Because unicast routing is a difficult problem in a TI, the ideal solution should also make efficient use of multicast protocols in low capacity sub-networks. This will reduce the number of packets that need to be transmitted and, potentially, the number of routes that need to be propagated through the TI.

Interfacing to radios

Finally, the ideal solution for the delivery of advanced Internet-based applications that can enhance C4ISR efforts in a TI should support multiple radio-based systems. This is a complicated requirement because no two radios from different manufacturers behave the same way, have the same characteristics or provide the same interface. Typically, there are differences in the data rates from a few hundred bits per second on radios connected to HF networks to megabits per second on UHF networks. These data rates are supported by a variety of media connections from raw serial to serial with Point-to-Point Protocol (PPP) and Ethernet.

Legacy radios often do not provide Layer 2 Media Access Control (MAC) to the Air Interface, so they require an appropriate Network Access Control (NAC) algorithm, which needs precise feedback to function properly. This and higher layer functions must be controlled by the TI system.

New, software-defined radios contain functions for MAC and contain Layer 3 routing capabilities. But this additional functionality creates two additional requirements for the interface to the radio. First, the radio must be able to exchange routing information with the system to maintain a converged view of the network. The exchange of this management information can be by standard protocols, such as Simple Network Management Protocol (SNMP), or by vendor-bespoke protocols. In either case, these management interfaces may be provided in-band with a data connection or via a separate management interface. Second, the radio and higher level TI services must be able to modify costs and add or remove routes to ensure the most efficient path is taken to a particular destination, depending on net load and availability.

Regardless of whether the network is supporting new or legacy radios, maximizing the performance of the radio is the key to efficient communications in a resource-limited TI. This can be achieved with prioritization and FEC.

Selecting the proper router

Obviously, the network router is the key to an effective solution that supports multiple radios and provides the most effective movement of secure Internet-based traffic in a TI. Ideally, the router should be engineered specifically to address the problems associated with enabling Internet-based applications in low-bandwidth environments (Table 1). Therefore, it should be designed from the ground up for self-forming, self-healing mobile ad hoc networks. It should leverage HF, VHF, and UHF to provide the benefits of Internet-style applications on current mobile, ad hoc networks and provide a path to the full capabilities of the Tactical Internet. It should support voice, data and multimedia traffic, including video, and offer a simplified system management process. Most importantly, it should be designed to address the SWaP-C considerations of current and future military platforms.

Table 1. Addressing the problems associated with enabling Internet-based applications in low-bandwidth environments

Problem:	Solution:
Users cannot reliably exchange data under dynamically changing link conditions and node topologies.	Provide a data delivery mechanism using store and forward techniques that eliminate the need for continuous end-to-end connectivity. Enable auto-selection of User Datagram Protocol (UDP), TCP, Comprehensive FEC-based Protocol (CFP), and DTN transport protocols based on path quality. Manage a wide range of peak user data rates.
Low bandwidth mobile radio links (HF, VHF) affect the proper use of current tactical applications.	Provide performance enhancement proxies for applications designed to use commercial protocols, such as Hyper Text Transfer Protocol (HTTP), and Extensible Markup Language (XML), as well as applications, such as, e-mail, Short Message Service (SMS), and chat. Assure scalability to a large number of nodes in an ad hoc mobile radio network, comprised of multiple sub-networks and addressable devices.
Current networking links and feedback will not allow for data prioritization of a commander’s intent.	Provide policy based prioritization, automatic data rates and decision services using open standards quality of service (QoS). Characterize links using QoS to provide network feedback and allow for prioritization based on commander’s intent.
System management is complex and time consuming.	Ensure network management provides identification for each platform and configuration for each net. Include self-discovery, self-healing, and self-configuring capabilities.
Current products are bulky, power hungry, hard to use and not suited for harsh environments.	Consolidate “must have” features into a small form factor. Ensure qualification and certification for reliable, rugged operation in harsh environments.

THE GENERAL DYNAMICS CANADA TACTICAL INTERNET ENABLER

General Dynamics Canada addresses the requirements of the Tactical Internet with integrated communications and networking solutions specifically engineered to enable the delivery of Internet-based applications. These solutions take advantage of existing commercial technologies in the Upper TI and effectively integrate them into the rugged, mobile ad-hoc communications equipment required in the Lower TI. The General Dynamics Canada approach provides maximum flexibility with solutions that are:

- Easy to use, manage and maintain, with minimal planning;
- Modular and built on industry standards to allow the use of the best equipment and software to suit specific needs;
- Engineered with multiple independent levels of security integrated into the hardware and software components to ensure confidentiality, integrity, and availability of information.

For example, the MESHnet®[3] line of products provides a suite of independent components that can be operated as standalone equipment or integrated to create a voice and data network infrastructure in tactical platforms. These rugged products are designed and tested for operation in tactical environments worldwide. Networked together, they provide:

- An open, IP-based, integrated voice and data tactical communication network;
- A distributed, network-centric, self-healing, fault/failure tolerant architecture;
- Scalability from individual vehicles to joint task force system-of-systems;
- Open interfaces to sensors and tactical, joint, strategic and commercial networks;
- Interoperability with allied and coalition partners.

MESHnet products combine internet protocol data and toll-quality digital voice together in a single high bandwidth, autonomous local area system. This complete system is integrated with HF and VHF combat net radios, data radios and wide area systems to form a homogenous voice and data network with interfaces to external tactical and commercial networks. In addition, self-discovery capabilities enable the network to be connected together with minimal operator set-up and configuration.

The open, IP-based architecture on which MESHnet products operate is designed to facilitate technology insertion for future enhancements. This ensures that MESHnet can be adapted to meet the inevitable changes that occur in tactical communications.

MESHnet equipment includes:

MESHnet Tactical Mobile Router (TMR), which enables the use of e-mail, instant messaging or web-based applications in self-forming, self-healing mobile ad hoc networks where end-to-

[3] MESHnet is a registered trademark of General Dynamics Canada.

end communications may not be stable and bandwidth is limited.

MESHnet Communications Selector Box (CSB), which provides a single access point for voice and data services, including intercom, radio and telephony.

MESHnet Tactical Network-layer Gateway (TNG), which provides a backbone for interfaces to external networks.

MESHnet Power Distribution Unit (PDU), which distributes up to 50A of vehicle-supplied 28V DC power to vehicle-mounted electronic equipment, and provides the first line of defence against transients and noise pickup on power leads.

MESHnet Tactical Mobile Router (TMR)

As the key component of the MESHnet solution, the MESHnet TMR addresses the problems associated with managing Internet-based application traffic in a TI (Table 1). It is engineered to support self-forming, self-healing mobile ad hoc networks with devices capable of self-configuration based on topology changes. This ability to adapt to network path and link changes assures reliable data exchanges for any commercial level communications application in disrupted Combat Net Radios (CNR), satellite communications (SATCOM) and wireless Local Area Network (WLAN) environments where conventional Internet protocols break down.

The TMR uses a CFP and a Low Bandwidth Routing Protocol (LBRP) along with DTN store and forward techniques to deliver messages over the most appropriate bearer links available in the network at the time of communication. This eliminates the need for continuous, end-to-end connections and ensures that any mobile end point can continue to send and receive over the network at any time.

In addition, the modular design of the TMR enables easy configuration for a variety of military radios and other wireless systems using a variety of small form factor enclosures. This simplifies system integration in military platforms where SWaP-C considerations are paramount.

With the TMR, standard networking protocols are enhanced for tactical mobile performance to ensure in-field personnel have a familiar (Internet-like) user experience when interacting with the Tactical Internet.

CONCLUSION

The Tactical Internet presents a number of communications networking challenges to military organizations looking for an efficient way of enhancing C4ISR efforts with Internet-based applications. The very nature of in-field communications networks makes it almost impossible to recreate the Internet's network environment and ensure the reliable delivery of high-bandwidth, high-capacity data where Internet standards fail: at the low bandwidth and disrupted tactical edge network.

The ideal Tactical Internet communications solution will connect the low bandwidth tactical edge network to the higher bandwidth core network. Most importantly, it will consolidate must-have networking features into an easy to manage network appliance designed and qualified for use in space constrained tactical vehicles.

General Dynamics Canada addresses the requirements of the Tactical Internet with MESHnet integrated communications and networking solutions specifically engineered to enable the delivery of Internet-based applications. These solutions take advantage of existing commercial technologies in the Upper TI and effectively integrate them into the rugged, mobile ad-hoc communications equipment required in the Lower TI.

As the key component of the MESHnet solution, the MESHnet TMR is engineered to support self-forming, self-healing mobile ad hoc networks with devices capable of self-configuration based on topology changes. This ability to adapt to network path and link changes assures reliable data exchanges for any commercial level communications application in disrupted environments where conventional Internet protocols break down. With the MESHnet TMR, the always-on, instant communications capabilities of today's commercial Internet can be efficiently extended to the Tactical Internet.

ACRONYMS

Term	Definition
API	Application Programming Interface
C4ISR	Command, Control, Communication, Computing, Intelligence, Surveillance and Reconnaissance
CFP	Comprehensive FEC-based Protocol
CNR	Combat Net Radio
DTN	DISRUPTION-TOLERANT INTEROPERABLE NETWORKING
DSCP	DiffServ Code Points
XML	Extensible Markup Language
FEC	Forward Error Correction
HF	High Frequency
HTTP	Hyper Text Transfer Protocol
Inter-ARD	Inter-Autonomous Routing Domain
LBRP	Low Bandwidth Routing Protocol
MAC	Media Access Control
NAC	Network Access Control
NACK	Negative ACKnowledgment
NORM	Negative Acknowledgment (NACK)-Oriented Reliable Multicast
PPP	Point-to-Point Protocol
QoS	Quality of Service
SATCOM	Satellite Communications
SHF	Super High Frequency
SMS	Short Message Service
SOTM	Satellite Communications On-The-Move
SNMP	Simple Network Management Protocol
SWaP-C	Size, Weight and Power and Cost

TI	Tactical Internet
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
UHF	Ultra-High Frequency
VHF	Very High Frequency
WLAN	Wireless Local Area Network

REFERENCE

The Tactical Internet: Understanding the challenges of inter-networking highly variable sub-networks using open standard protocols, Mark R. A. Adcock, Paul Bristow, Marc Jones, Marc Levesque, E. Neil Viberg, Stuart Wood, General Dynamics Corporation; Brian H. Davies, QinetiQ

Contacts

www.gdcanada.com info@gdcanada.com