A HOLISTIC NETWORKING PERSPECTIVE ON MOBILE TACTICAL NETWORKS FOR THE DEPARTMENT OF THE DEFENSE

Mehul Gandhi (Booz Allen Hamilton, Arlington, VA, USA, gandhi_mehul@bah.com)

ABSTRACT

The Department of Defense's (DoD) IP-based Global Information Grid (GIG) will encompass tactical mobile ad hoc networks (MANETs). Tactical MANETs will exist in the airborne, maritime and ground domains. These networks will utilize a black core infrastructure by using IPSec-based Virtual Private Networks (VPNs) to separate Communities of Interest (COIs) and classification levels.

These networks will require routing and mobility support, multicast, information assurance, Quality of Service (QoS), network services and network management services to be operational. Tactical MANETs place challenges on each of the functions. This paper provides an overall perspective on the current work, DoD challenges, open issues and possible solutions paths for these challenges.

1. INTRODUCTION

The GIG, the DoD's IP-based globally reachable network, will extend to the tactical battlefront to provide greatly enhanced transport services for the warfighter. Today's DoD tactical transport systems are point to point, difficult to set up, and do not keep up with the pace of battle. MANETs, with software defined radio components, are under development today to fulfill these enhanced capabilities. Program such as the Joint Tactical Radio System (JTRS) and the Warfighter Information Network – Tactical (WIN-T) are developing such transport enhancements.

These dynamic, self-forming, and self-healing networks utilize a specialized class of routing protocols. Most of the technical literature and research to date focuses on the routing challenges in MANETs. To initialize, secure, and maintain these networks a variety of networking functions beyond routing are needed. These functions include mobility support, multicast, information assurance, quality of service, network services and network management. Performing each of these functions in a distributed MANET imposes unique challenges on these technologies, compared to how they are traditionally deployed in an enterprise class network.

2. MOBILE TACTICAL NETWORK DOMAINS

Tactical MANETs for the DoD will exist in several mobile network domains. These domains are airborne, maritime, and ground. Once the vision of the GIG is achieved, these domains will be interconnected by a IP-based inter-network.

2.1. Airborne Domain

The airborne domain will consist of military aircraft including widebody aircraft, tactical fighters, rotary wing aircraft and Unmanned Aerial Vehicles (UAVs). The airborne domain can be further broken down into these regions.

- *Airborne Backbone*

Widebody aircraft will be used to provide backbone services to the rest of the airborne domain. These widebodies will operate in stable mobility patterns. They will be far enough away from a battle to be out of immediate danger, but close enough to be within communications range of aircraft performing missions.

- *Airborne Tactical Edge*

Aircraft directly involved in performing missions will be in the Airborne Tactical Edge. While in-flight to a mission, tactical edge nodes will have stable mobility patterns relative to one another. Relative to ground and maritime nodes they will be considered fast movers. Tactical edge nodes will likely utilize the airborne backbone for reach back services into the core of the GIG.

- *Airborne Communications Relay and Intelligence Surveillance Reconnaissance (ISR)*

UAVs will be used to provide both communications relay services to ground nodes and also to relay ISR data from on-board sensors. A UAV loitering over ground nodes can provide relay services to partitioned networks and augment capacity. Many UAVs will carry sensor payloads, such as infrared cameras, radar, and video cameras for imagery. Once the sensor captures this data, it will be streamed across the network to receiving nodes.

- *Near Ground Air*

This region consists of rotary wing aircraft and weapons. Rotary wing aircraft will be used to transport supplies/troops and support of ground missions. Mobility patterns for rotary wing aircraft will vary, since they are capable of hovering over nodes and moving quickly. While hovering over ground or maritime nodes, they will be communications relays. Additionally, these aircraft can be fast movers relative to ground or maritime nodes. Networked weapons will need communications services for in-flight control, relay of ISR data and continuous location data as the munitions are in-flight.

These four regions of the airborne domain, will provide networked transport services across the airborne domain and interconnections with ground and maritime nodes. Because the airborne domain will contain the fastest moving nodes quick network join times, fast network convergence and fast movers will represent domain unique challenges.

2.2. Maritime Domain

The maritime domain will consist of maritime vessels, tactical edge aircraft that leave from maritime vessels and amphibious vehicles. This domain has three regions: ship to ship, ship to airborne tactical edge, and ship to ground.

- *Ship to Ship*

In this region, when ships are in communications range they will be able to utilize a MANET to interconnect a group of vessels. MANET links will be used to augment capacity from satellite links. During normal operations ships will have stable mobility patterns relative to one another. During battles these patterns will be less predictable.

- *Ship to Airborne Tactical Edge*

Tactical airborne aircraft that leave from maritime vessels will eventually become part of the Airborne Tactical Edge.

- *Ship to Ground*

Amphibious vehicles will be launched from ships toward the shore for various missions. These vehicles will need to maintain communications between each other and back to the ship while in the littoral battlespace. Once ashore, depending on the mission, these vehicles may join other ground forces.

2.3. Ground Domain

The ground domain consists of portable but stationary operations centers, ground vehicles (i.e. tanks, HUMVEEs, etc), and soldiers on foot.

- *Ground Backbone*

The ground domain will utilize a backbone that is composed of portable communications equipment and vehicles with deployable antennas. The portable communications equipment will typically be setup in a Tactical Operations Center (TOC). Vehicles with deployable antennas can be moved to different locations to setup optimal coverage and data rates. The ground backbone will provide transit, global reachback, and traffic aggregation for lower regions of the network.

- *Ground Vehicular*

In this region, ground vehicular nodes are directly involved in missions. These nodes will be very mobile, with unpredictable mobility patterns. Ground nodes will form one or many MANETs and will provide transit and reach back services to lower tier networks.

- *Mobile Solider*

Once a solider, with a handheld or manpack communications device dismounts from a vehicle, he or she will represent a MANET node. These nodes will move slowly (compared to other platforms), but will have unpredictable mobility patterns.

The ground domain will be the largest in terms of number of nodes. The scalability challenges will be greatest in this domain.

4. TACTICAL NETWORK ARCHITECTURE DESCRIPTION

To ensure end to end network reachability and a robust security architecture, the GIG will utilize a black core. This black core will provide a unified transport infrastructure for different COIs and classification levels.

4.1. IPSec Based VPNs

COIs will be separated using high assurance IPSec as described in [1]. The IPSec suite of technologies will be used to setup cryptographically separated overlays for each COI over a black core infrastructure. Figure shows the basic concepts of the black core. Red enclaves contain hosts and unencrypted traffic are contained within vehicles. When packets are forwarded to the VPN Gateway, they are encrypted and forwarded to a black router. When packets reach a destination VPN Gateway, they are decrypted and sent to the host.

IPSec tunnels between VPN Gateways are manually configured based on prior knowledge of address information for the VPN Gateway and red enclaves. The GIG will contain thousands of these high assurance VPN gateways. To scale to such a large number, automated ways of configuring these devices are needed.

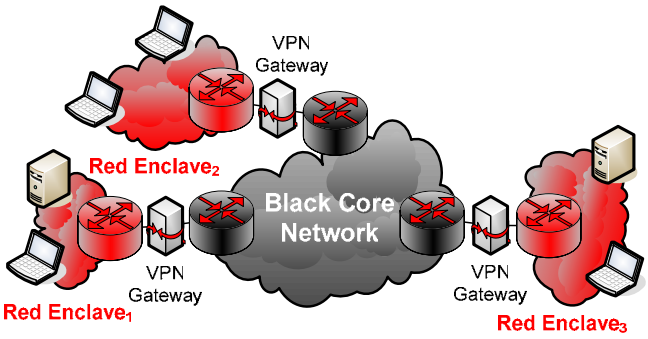


Figure 1 Red Enclaves Interconnected by a Black Core

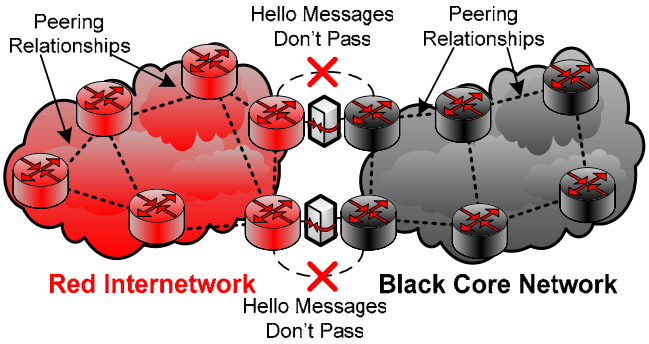


Figure 2 Topology Masking Between Red And Black Inter-Networks

depicts a black core network that interfaces with a red inter-network. When security policies do not allow an exchange of control plane information (such as router "hello" messages) across the VPN gateway boundary, the topology of the red network is masked to the black network and vice versa. This challenge occurs on large deck ships in the maritime domain. Large decks will utilize a on-board inter-network and send off board traffic across black core infrastructures. Topology masking also occurs when black core networks interface to existing red inter-networks such as the DoD's service provider class network called Defense Information Systems Network (DISN).

4.3. Advantaged Nodes and Fast Movers

Advantaged nodes, such as radios on a hill top or on a loitering aircraft, will provide communications relay services to nodes with lower elevations. Advantaged nodes are placed in locations where they have significant communications visibility to other nodes.

Fast movers are nodes that move very quickly relative to slower moving nodes in the network. For instance, during a close air support mission a tactical aircraft will provide munitions support to ground forces in need of help. Networking ground forces with tactical aircraft will significantly increase the effectiveness of this mission. As the tactical aircraft flies over ground forces, it can continuously receive up-to-date location and red force information from a forward observer. Without special mechanisms built into the network, this node will look like an advantaged node and will try to form peering relationships with a ground nodes visible to it. Since it is moving quickly, it will be out of range in a short period of time. Ground networks routing topologies will need to re-converge, causing a flood of routing information. Figure illustrates this phenomenon without prevention mechanisms.

5. ROUTING AND MOBILITY SUPPORT

Maintaining a routing topology and forwarding packets to their destinations is perhaps the most transformational capability that tactical MANETs will support.

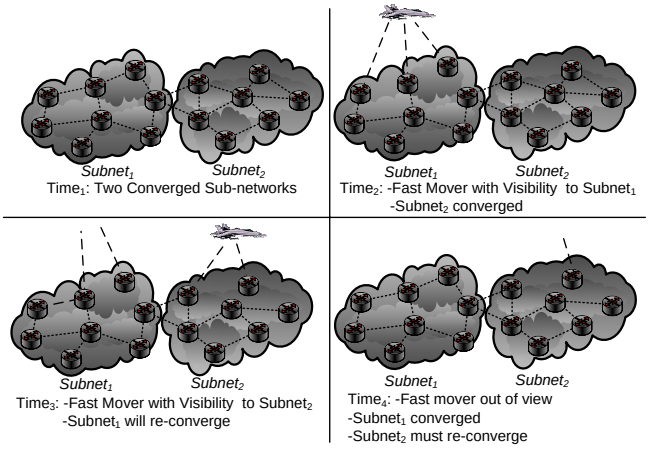


Figure 3 Fast Mover Looks Like An Advantaged Node

5.1. Current Work

Internet Engineering Task Force's (IETF) MANET Working Group performed much of the recent research in mobile ad hoc routing protocols. They are developing standards recommendations for reactive and proactive routing protocols for wireless environments. [2] defines MANETs as stub networks to a larger fixed network infrastructure, where hosts and routers are typically the same device.

5.2. DoD Challenges

DoD tactical MANETs present several unique challenges. First these networks will need to provide transit routing services to other networks. Next they will need to seamlessly inter-network to external networks using widely implemented routing standards such as OSPF and BGP. Finally, some tactical MANETs will need to support routing for ranges of IP addresses rather than a single host. These services differ significantly from the definition of a MANET in [2].

5.3. Open Issues and Possible Solutions

Route summarization is a technique that is commonly used to allow larger inter-networks to scale the number of routers. IP address ranges are allocated hierarchically across a network. This hierarchy allows address ranges to be summarized, as route updates move up the hierarchy. Therefore routing processes can send less control plane data, consume less processor cycles and memory to support packet forwarding. Larger tactical MANETs, as those encountered in the Ground domain, will contain thousands of routers. Even if a tactical MANET's IP address range is allocated hierarchically, these IP subnets will be mobile across the network. This ensures the optimal IP address range hierarchy will not be maintained, leading to more routes propagating across the network. A more dynamic, robust mechanism for maintaining address hierarchy is necessary.

Tactical MANETs acting as transit networks will inter-network with networks running different routing protocols. As a transit network, a MANET must present its topology and/or route information to a neighboring network. This enables a neighboring network to make optimal routing decisions. There are several existing techniques for this function:

- *Route Redistribution*

With route redistribution, two routing process, running on a separate router interfaces exchange routing information about the routing domains they are connected to. A MANET routing protocol and a traditional IGP will likely use different cost metrics for calculating routes. Careful consideration must be given to the mapping of cost metrics

between both protocols. Additionally, route redistribution will only communicate routes between networks rather than topology information.

- *Enhance An Existing IGP With MANET Routing Features*

[3] and [4] are enhancements to the existing OSPFv3 protocol to better support MANETs. The philosophy of this approach is to borrow optimizations for MANET protocols and incorporate them into an existing, well-known Interior Gateway Protocol (IGP). The benefit of this approach is that the IGP is already capable of internetworking. The IGP is extended over a MANET domain. One of the features borrowed from MANET protocols is the concept of Multi Point Relays (MPR) described in [5]. MPRs are dynamically elected nodes that are responsible for distributing up-to-date routing information to small sections of the network.

- *Run A MANET Routing Protocol Below The IP And Overlay An IGP*

[6] describes a technique where a MANET routing protocol routes based on hardware address or a unique node ID, below the IP layer. An IGP is overlaid over top of the MANET domain. Cross layer optimizations, such as relaying topology information from the MANET routing process to the IGP are possible. This increases the accuracy of the topology and can reduce control plane overhead from two simultaneous routing protocols operating on the same network. Without cross layer optimizations, the IP layer IGP and the lower layer MANET protocols are considered "ships in the night."

Regardless of the solution, several key challenges exist for internetworking MANETs to fixed networks or other MANETs. A clear one-to-one mapping of cost metrics will be difficult. MANET protocols often optimize in one dimension, such as energy savings in battery powered devices or link bandwidth. Developing a mapping between cost metrics will require the mapping of these dimensions to one another. Another issue is that, in tactical MANETs, route flapping is common. If the MANET presents an exact connectivity graph of the physical topology to a neighboring network, this network will consistently see routes flapping at the peering points. If a MANET presents an abstraction of its physical topology, the neighboring network may not make optimal routing decisions. A sweet spot in the middle of these two points is needed.

Two well known problems in ad hoc networks are scalability and fast convergence. As the number of nodes in the network grows, so does the control plane overhead required to maintain the network topology. The problem is exacerbated in high-mobility environments. The Ground domain will likely contain the most nodes and will require solutions to reduce control plane overhead. Fast convergence is required for the airborne tactical edge region. Since aircraft will have significant mobility, relative to one another, fast convergence will be required to ensure optimal delivery of packets.

7. MULTICAST

Secure multicast routing will be required to support a variety of applications such as group voice, situational awareness, and collaboration in tactical MANETs.

7.1. Current Work

Two basic multicast techniques exist for MANET environments. Tree based multicast, forms a tree from the source to the receivers in a multicast group. Mesh based multicast forms a redundant mesh between a source and receivers. Since mesh MANET multicast protocols employ redundant paths, they tend to provide more reliable delivery in environments without stable links. [7] provides a survey of multicast techniques for MANET environments.

7.2. DoD Challenges

Tactical MANETs will need to inter-network multicast MANET routing protocols with external networks. The same issues with internetworking unicast MANET routing protocols are applicable. Secure multicast services will require source authentication, group key management and data confidentially for multicast traffic.

7.3. Open Issues and Potential Solutions

Pre-planned group keys can be used to secure multicast groups. Unfortunately, this technique does not allow a subset of nodes to be pulled from the multicast group. Eventually when group key management techniques mature, compromised nodes can be pruned from the multicast group. [8] provides a survey of security issues and techniques for multicast.

8. INFORMATION ASSURANCE

8.1. Current Work

Tactical MANETs will utilize computer network defense functions such as firewall and intrusion detection systems (IDS). Firewalls and IDS sensors can be configured on nodes with adequate computing resources.

The tactical MANET's black core infrastructure is dependent on routing protocols to maintain the network topology. Authentication, integrity, and data confidentiality of routing control plane traffic are needed to protect against insider threats.

8.2. DoD Challenges

Ideally, firewalls and IDS sensors are deployed at each node rather than deployments at network boundaries. Since nodes are mobile, network boundaries may be difficult to determine. Since nodes, with less processing power, may not be able to run a firewall or an IDS sensor, careful placement of these functions will be necessary.

8.3. Open Issues and Potential Solutions

IDS sensors typically roll-up state information to a central server. This server will have a global view of each IDS sensor, can determine when an attack is occurring and the appropriate response. In a tactical MANET, these functions must be distributed across the network.

9. QUALITY OF SERVICE

Tactical MANETs will support a variety of traffic types and will require various quality of service mechanisms.

9.1. Current Work

The DiffServ framework, described in [10], provides service differentiation on a per hop basis. Packets are marked with priority levels based on a network wide QoS policy. This policy ensures consistent treatment of traffic across the network. Ensuring a consistent QoS policy in commercial service provider networks is difficult. Services providers must develop Service Level Agreements (SLA) at peering points to each other's networks. Since the DoD is one organizational entity, it can define and execute a consistent QoS policy across the network.

The IntServ framework, defined in [11], describes how to implement guaranteed services over IP networks. This framework utilizes the Resource ReSerVation Protocol (RSVP) provides a mechanisms to reserve bandwidth end to end between a source and destination. RSVP is described in more detail in [12].

9.2. DoD Challenges

Many nodes in DoD environments will be size, weight, and power constrained devices with small amounts of memory. This will effect the granularity of the QoS policy that can be implemented on these devices. With less memory, they will not be able to implement the same number of queues with the same queue depth as service provider class routers in the core of the GIG.

RSVP presents well-known scalability challenges. RSVP requires each node to maintain state information about each traffic flow. As the number of traffic flows grows, so does the memory required to maintain this state information. In tactical MANETs, guaranteed services require bandwidth reservation support from media access control (MAC) layers. Since MANET nodes have continually changing link conditions guaranteeing resources will be difficult. Additionally, MANET MAC layers don't have a centralize resource control (such as a base station allocating time slots or CDMA codes in a cellular network).

9.3. Open Issues and Potential Solutions

To support guaranteed services, a MAC with distributed resource control is needed. Without this, each node will not be able to support reservation of bandwidth. Bandwidth brokers (BB) may alleviate the scalability challenge encountered with bandwidth reservation. If a tactical MANET partitions into two or more fragments, this centralized BB may not be available to all fragments. A more distributed approach to BB could help ensure no fragment is without a BB.

10. NETWORK SERVICES

As with any network, tactical MANETs will need routers and hosts configured with IP address pools and name-to-address translation services.

10.1. Current Work

The Dynamic Host Control Protocol (DHCP) is widely used to configure requesting hosts with IP address, gateway and Domain Name Services (DNS) servers. IP address pools are centrally allocated to DHCP servers by an administrator. The DNS hierarchy scales across the entire internet. A host simply need to know the location of a closest server within the DNS tree. The DNS server must be known by an administrator and configured on the DHCP servers. Dynamic DNS, described in [13], allows servers to change their IP addresses and still maintain their name to address mapping.

10.2. DoD Challenges

Tactical MANETs will not have an fixed infrastructure. Centralized support mechanisms may not operate if a network fragment can no longer reach the server.

10.3. Open Issues and Potential Solutions

Multicast DNS, described in [14], allows hosts to request DNS information through multicast. This alleviates the need for a known locations of services, but is focused on small scale networks. [15] describes a set of auto configuration services for large scale dynamic networks. Example services from [15] include :

- IP Addresses of an interface
- Network parameters (e.g., default maximum transmission unit, MTU, size)
- Server addresses (e.g., for DNS or certificate authority server)
- Routing information (e.g., default route or routing protocols)
- IP address pools (e.g., for DHCP or MADCAP server)
- Security keys

Autoconfiguration of network parameters would also significantly reduce the administrative burden on operators.

11. NETWORK MANAGEMENT

Tactical MANETs will require: careful planning, well designed and flexible network architectures, radio configuration and initialization, and monitoring and management services.

11.1. Current Work

Tactical Network Management Systems (NMSs) will be hierarchal. Lower tier NMSs will receive planning information from higher tier NMSs. Lower tier NMSs will be optimized to manage specific tactical regions.

Interfaces from NMSs to network devices are available in the form of SNMP and newer XML based protocols such as NetConf which is specified in [16].

11.2. DoD Challenges

Tactical MANETs require a variety of unique network management services. In the planning phase, spectrum must be allocated to different regions of the network. A tactical NMS will request spectrum from a higher level spectrum management system, based on the designed network architecture.

Tactical NMSs will require display of geographic maps and display node locations for situational awareness. An agent on each node will send location information to the NMS periodically for visualization.

Joint missions will require planning to be performed across different domains. To support a close air support mission, a tactical aircraft will be provided the same software waveform and physical to network layer configuration parameters as a ground vehicular and mobile solider networks. This will enable the tactical aircraft to dynamically join the ground network.

Typically NMS rely heavily on centralized operations and servers. As tactical MANETs partition into different fragments they will lose connectivity to an NMS.

11.3. Open Issues and Potential Solutions

Tactical MANETs will utilize very flexible media access control techniques that allow for spatial reuse of allocated frequencies. Additionally, software radio waveform components will be capable of operating on a variety of frequencies within the limitations of the radio hardware. This spectral flexibility will allow a planner to trade off network performance and mission effectiveness with available spectrum. The process of allocating frequencies should be more dynamic and allow spectrum managers and network planners to make tradeoffs.

FCAPS management functions require centralization. Fault detection, root cause analysis, and security management techniques require traps to be sent from network elements to a central management server. A hierarchical and distributed NMS is needed for tactical MANETs to ensure these functions can be performed when networks partition.

Pushing configuration changes to MANET nodes along links with high packet loss rates may require different transport layer mechanisms. Episodic link connectivity may prevent this data from being sent or received by the management station. Reliable multicast and messaging buses such as the Java Messaging Services (JMS) offer two possible solutions.

Operators of the tactical NMSs, will be less sophisticated than those encountered in commercial networks. Tactical NMSs will need to incorporate automation features and self optimizing features to reduce operator burden.

13. CONCLUSIONS

The IP suite of protocols were originally designed for a wireline environment. Tactical MANETs, which operate in a wireless, infrastructureless environment, will drive changes to the existing protocols and ways of managing networks. While solutions to some challenges are under development, there is significant room for innovative approaches to solving the challenges of tactical MANETs.

REFERENCES

[1] D. Lofquist, “JTRS Networking Services and the Wideband Networking Waveform”, *Government Microcircuit Applications and Critical Technology Conference*, Feb. 2004

[2] S. Corson, J. Macker, “MANET: Routing Protocol Performance Issues and Evaluation Considerations”, RFC 2501, Jan. 1999

[3] M. Chandra, et al. “Extensions to OSPF Supporting Ad Hoc Networking”, draft-chandra-ospf-manet-ext-03.txt, Apr. 2005

[4] R. Ogier, P. Spagnolo. “MANET Extension of OSPF using CDS Flooding”, draft-ogier-manet-ospf-extension-04.txt, Jul. 2005

[5] T. Clausen, P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”, RFC 3626, Oct. 2003

[6] T. Henderson, et al. “Interlayer Routing Issues for Wireless Networks”, *NATO Workshop on Cross Layer Issues in the Design of Tactical Mobile Ad Hoc Wireless Networks* (http://www.valcartier.drdc-rddc.gc.ca/tgonimdg/documents/tactical/Henderson-nato.pdf), Jun. 2004

[7] C. Cordeiro, et al., “Multicast over Wireless Mobile Ad Hoc Networks: Present and Future Directions”, *IEEE Network*, Jan/Feb. 2003

[8] P. Judge, M. Ammar, “Security Issues and Solutions in Multicast Content Distribution: A Survey”, *IEEE Network*, Jan/Feb. 2003

[9] E. Ertekin, C. Christou, "Internet Protocol Header Compression, Robust Header Compression, and Their Applicability in the Global Information Grid", *IEEE Communications Magazine*, vol. 42, no. 11, Nov, 2004

[10] Carlson, M., et al., “An Architecture for Differentiate Services.” RFC 2475, Dec. 1998

[11] Braden, R., et al., “Integrated Services in the Internet Architecture: An Overview.” RFC 1633, Jun. 1994

[12] Braden, R., et al., “Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification.” RFC 2205, Sept. 1997

[13] P. Vixie, et al., “Dynamic Updates in the Domain Name System”, RFC 2136, Apr. 1997

[14] S. Cheshire, M. Krochmal, “Multicast DNS”, draft-cheshire-dnsext-multicastdns-05.txt, Jun. 2005

[15] K. Manousakis, “Network and Domain Autoconfiguration: A Unified Approach for Large Dynamic Networks”, *IEEE Communications Magazine*, vol. 43, no. 8, Aug. 2005

[16] R. Enns, “NETCONF Configuration Protocol”, draft-ietf-netconf-prot-08, Sept. 2005

A HOLISTIC NETWORKING PERSPECTIVE ON MOBILE TACTICAL NETWORKS FOR THE DEPARTMENT OF THE DEFENSE

Software Defined Radio Forum
November 2005

Mehul Gandhi
gandhi_mehul@bah.com
703.696.8966

Booz | Allen | Hamilton

Table Of Contents

Booz | Allen | Hamilton

The Global Information Grid, the DoD's IP-based globally reachable network, will extend to the tactical battlefront to provide greatly enhanced transport services for the warfighter

- **Today's DoD tactical transport systems are**
  - Point to point
  - Difficult to set up
  - Do not keep up with the pace of battle
- **MANETs, with software defined radio components, are under development today to fulfill these enhanced capabilities**
  - Program such as the Joint Tactical Radio System (JTRS) and the Warfighter Information Network – Tactical (WIN-T) are developing such transport enhancements
- **These dynamic, self-forming and self-healing networks utilize a specialized class of routing protocols**
  - Most of the technical literature and research to date focuses on the routing challenges in MANETs
  - To initialize, secure, and maintain these networks a variety of networking functions beyond routing are needed
- **These functions include mobility support, multicast, information assurance, quality of service, network services and network management**
- **Performing each of these functions in a distributed MANET imposes unique challenges on these technologies, compared to how they are traditionally deployed in an enterprise class network**

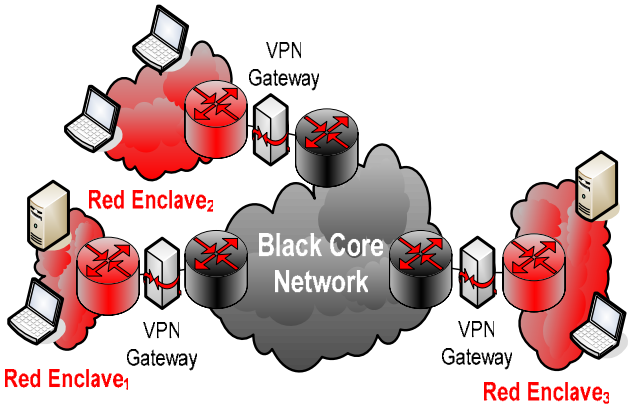
Tactical MANETs for the DoD will exist in Airborne, Maritime, and Ground mobile network domains

- **Airborne Domain – will consist of military aircraft including widebody aircraft, tactical fighters, rotary wing aircraft and Unmanned Aerial Vehicles (UAVs)**
  - *Airborne Backbone* – Widebody aircraft will be used to provide backbone services to the rest of the airborne domain
  - *Airborne Tactical Edge* - Aircraft directly involved in performing missions
  - *Airborne Communications Relay and Intelligence Surveillance Reconnaissance (ISR)* - UAVs will be used to provide both communications relay services to ground nodes and also to relay ISR data from on-board sensors
  - *Near Ground Air* –This region consists of rotary wing aircraft and weapons systems
- **Maritime Domain – will consist of maritime vessels, tactical edge aircraft that leave from maritime vessels and amphibious vehicles**
  - *Ship to Ship* - when ships are in communications range they will be able to utilize a MANET to interconnect a group of vessels
  - *Ship to Airborne Tactical Edge* - Tactical airborne aircraft that leave from maritime vessels will eventually become part of the Airborne Tactical Edge
  - *Ship to Ground* - Amphibious vehicles will launch from ships toward the shore for missions
- **Ground Domain – will consist of portable but stationary operations centers, ground vehicles (i.e. tanks, HUMVEEs, etc), and soldiers on foot**
  - *Ground Backbone* – will utilize a backbone that is composed of portable communications equipment and vehicles with deployable antennas
  - *Ground Vehicular* – ground vehicular nodes are directly involved in missions
  - *Mobile Solider* - Once a solider, with a handheld or manpack communications device dismounts from a vehicle, he or she will represent a MANET node

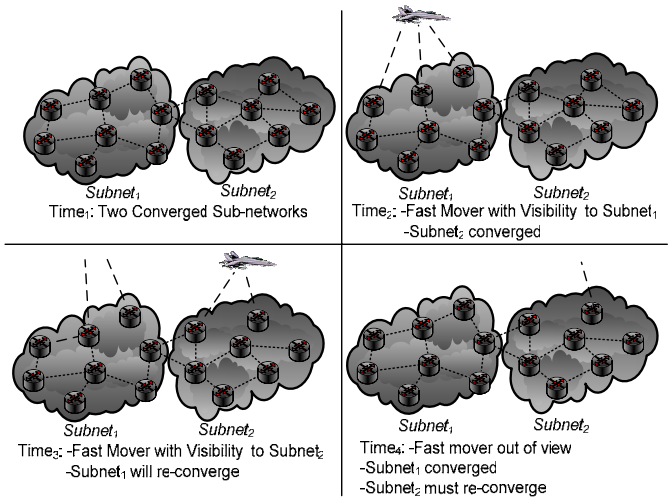
To ensure end to end network reachability and a robust security architecture, the GIG will utilize a black core that will provide a unified transport infrastructure for different COIs and classification levels

- **IPSec Based VPNs**
  - A high assurance version of the IPSec suite of technologies will be used to setup cryptographically separated overlays for each COI over a black core infrastructure
  - Red enclaves, usually located within vehicles, will contain hosts and unencrypted traffic
  - When IPSec gateways security policies block routing topology information, red internetworks will not know the topology of a black core

- **Advantaged Nodes and Fast Movers**
  - Advantaged nodes, such as radios on a hill top or on a loitering aircraft, will provide communications relay services to nodes with lower elevations
  - Fast movers are nodes that move very quickly relative to slower moving nodes in the network
  - Without special mechanisms built into the network, this node will look like an advantaged node and will try to form peering relationships with any ground nodes visible to it



Red Enclaves Interconnected by a Black Core



Fast Mover Looks Like An Advantaged Node

Booz | Allen | Hamilton

Maintaining a routing topology and forwarding packets to their destinations is perhaps the most transformational capability that tactical MANETs will support

- **Current Work**
  - Internet Engineering Task Force's (IETF) MANET Working Group performed much of the recent research in mobile ad hoc routing protocols
  - The IETF defines MANETs as stub networks to a larger fixed network infrastructure, where hosts and routers are typically the same device
- **DoD Challenges**
  - These networks will need to provide transit routing services to other networks
  - Next they will need to seamlessly inter-network to external networks using widely implemented routing standards such as OSPF and BGP
  - Some tactical MANETs will need to support routing for ranges of IP addresses rather than a single host
- **Open Issues and Possible Solutions**
  - Route summarization, which is used to larger inter-networks to scale the number of routers. IP address ranges are allocated hierarchically across a network
  - Larger tactical MANETs with mobile IP subnets, will contain thousands of routers
  - This ensures the optimal IP address range hierarchy will not be maintained, leading to more routes propagating across the network
  - A more dynamic, robust mechanism for maintaining address hierarchy is necessary

Maintaining a routing topology and forwarding packets to their destinations is perhaps the most transformational capability that tactical MANETs will support

- **Open Issues and Possible Solutions (Continued)**
  - Tactical MANETs will act as transit networks and must present its topology and/or route information to a neighboring network running different routing protocols. Several solutions are available:
  - *Route Redistribution*
    - A MANET routing protocol and a traditional IGP will likely use different cost metrics for calculating routes
    - Route redistribution will only communicate routes between networks rather than topology information
  - *Enhance An Existing IGP With MANET Routing Features*
    - This approach borrows optimizations form MANET protocols and incorporate them into an existing, well-known Interior Gateway Protocol (IGP)
    - The benefit of this approach is that the IGP is already capable of internetworking
  - *Run A MANET Routing Protocol Below The IP Layer And Overlay An IGP*
    - An IGP is overlaid over top of the MANET routing protocol that routes based on hardware addresses
    - Cross layer optimizations, such as relaying topology information from the MANET routing process to the IGP are possible
  - Regardless of the MANET internetworking solution, several challenges exist
    - MANET protocols often optimize in one dimension such as energy savings or link bandwidth, so a clear one-to-one mapping of cost metrics is difficult
    - Route flapping, which is common in tactical MANETs, will cause routes on the non-MANET part of the network

Secure multicast routing will be required to support a variety of applications such as group voice, situational awareness, and collaboration in tactical MANETs

- **Current Work**
  - Two basic multicast techniques exist for MANET environments
    - Tree based multicast - which forms a tree from the source to the receivers in a multicast group
    - Mesh based multicast – which forms a redundant mesh between a source and receivers
    - Mesh based techniques tend to perform better in tactical MANETs with frequenct link failures because of redundant paths
- **DoD Challenges**
  - The same issues with internetworking unicast MANET routing protocols are applicable
  - Secure multicast services will require source authentication, group key management and data confidentially for multicast traffic
- **Open Issues and Possible Solutions**
  - Pre-planned group keys can be used to secure multicast groups. Unfortunately, this technique does not allow a subset of nodes to be pulled from the multicast group
  - Eventually when group key management techniques mature, compromised nodes can be pruned from the multicast group

Tactical MANETs will utilize computer network defense functions such as firewalls and intrusion detection systems (IDS)

- **Current Work**
  - Firewalls and IDS sensors can be configured on nodes with adequate computing resources
  - The tactical MANET's black core infrastructure is dependent on routing protocols to maintain the network topology. Authentication, integrity, and data confidentiality of routing control plane traffic is needed to protect against insider threats
- **DoD Challenges**
  - Since nodes are mobile, network boundaries may be difficult to determine. Ideally, firewalls and IDS sensors are deployed at each node rather than deployments at network boundaries
  - Since nodes, with less processing power, may not be able to run a firewall or an IDS sensor, careful placement of these functions will be necessary based on the network architecture and potential threats
- **Open Issues and Possible Solutions**
  - IDS sensors typically roll-up state information to a central server. This server will have a global view of each IDS sensor, can determine when an attack is occurring and the appropriate response
  - In a tactical MANET, these functions must be distributed across the network

Tactical MANETs will support a variety of traffic types and will require various quality of service mechanisms

- **Current Work**
  - The DiffServ framework, in which packets are marked with priority levels based on a network wide QoS policy, provides service differentiation on a per hop basis
  - The IntServ framework describes how to implement guaranteed services over IP networks. This framework utilizes the Resource ReSerVation Protocol (RSVP) provides a mechanisms to reserve bandwidth end to end between a source and destination
- **DoD Challenges**
  - Battery and memory constrained devices will effect the granularity of the QoS policy that can be implemented across the network
  - RSVP requires each node to maintain state information about each traffic flow, increasing a devices memory requirements as the number of traffic flows grow
  - In tactical MANETs, guaranteed services require bandwidth reservation support from media access control (MAC) layers. Since the link conditions are continually changing, guaranteeing resources will be difficult
- **Open Issues and Possible Solutions**
  - Distributed bandwidth brokers (BB) may alleviate the scalability challenge encountered with network layer bandwidth reservation
  - To support guaranteed services, a MAC with distributed resource control is needed

As with any network, tactical MANETs will need routers and hosts configured with IP address pools and name-to-address translation services

- **Current Work**
  - The Dynamic Host Control Protocol (DHCP) is widely used to configure requesting hosts with IP address, gateway and Domain Name Services (DNS) servers. IP address pools are centrally allocated to DHCP servers by an administrator
  - The DNS hierarchy scales across the entire internet. A host simply need to know the location of a closest server within the DNS tree
  - Dynamic DNS allows servers to change their IP addresses and still maintain their name to address mapping
- **DoD Challenges**
  - Tactical MANETs may not have an fixed infrastructure
  - Centralized support mechanisms may not operate if a network fragment can no longer reach the server
- **Open Issues and Possible Solutions**
  - A set of autoconfiguration services, to reduce operator burden and increase how dynamically the network adapts, is needed for the large scale tactical MANETs. Example services include :
    - IP Addresses of an interface
    - Network parameters (e.g., default maximum transmission unit, MTU, size)
    - Server addresses (e.g., for DNS or certificate authority server)
    - Routing information (e.g., default route or routing protocols)
    - IP address pools (e.g., for DHCP or MADCAP server)
    - Security keys

Tactical MANETs will require: careful planning, well designed and flexible network architectures, radio configuration and initialization, and monitoring and management services

- **Current Work**
  - Tactical Network Management Systems (NMSs) will be hierarchal. Lower tier NMSs, which are optimized to manage specific tactical regions, will receive planning information from higher tier NMSs
  - Interfaces from NMSs to network devices are available in the form of SNMP and newer XML based protocols such as NetConf
- **DoD Challenges**
  - Spectrum Management - A tactical NMS will request spectrum from a higher level spectrum management system, based on the designed network architecture
  - Situational Awareness - Tactical NMSs will display geographic maps with node locations
  - Joint Mission Planning – will require collaboration between different domain planners
  - Centralized Network Management - Typically NMS rely heavily on centralized operations and servers. As tactical MANETs partition nodes will lose connectivity to an NMS
- **Open Issues and Possible Solutions**
  - Tactical MANETs will utilize very flexible media access control techniques that allow for spatial reuse of allocated frequencies. The process of allocating frequencies should be more dynamic and allow spectrum managers and network planners to make tradeoffs
  - FCAPS management functions require centralization. A hierarchical and distributed NMS is needed for tactical MANETs to ensure these functions can be performed when networks partition
  - Pushing configuration changes to MANET nodes along links with high packet loss rates may require different transport layer mechanisms
  - Operators of the tactical NMSs, will be less sophisticated than those encountered in commercial networks

Extending the DoD's Vision of the GIG to Tactical MANETs, will place new challenges on network layer functions

- Tactical MANETs will operate in the Airborne, Maritime and Ground domains
- The DoD's tactical network architecture will consist of red enclaves that utilized high assurance IPSec Gateways and a black core transport infrastructure
- Routing and mobility support will be provided by scalable MANET routing protocols with transit networking capabilities
- Multicast services will require MANET specific routing protocols, source authentication, group key management and data confidentiality
- Network layer information assurance will be provided by computer network defense functions such as intrusion detection systems, packet filtering and routing protocol security techniques
- Quality of service will be provided by service differentiation techniques. Guaranteed services will require media access control techniques with distributed resource control
- Tactical MANETs will require specialized network services that will reduce operator burden and operate in environments where networks fragment
- Tactical MANETs will utilize scalable network management systems that support DoD unique requirements for spectrum management, situational awareness and Joint mission planning
- Tactical MANETs, which operate in a wireless, infrastructureless environment, will drive changes to the existing protocols and ways of managing networks