Interoperable Networks for Secure Communications

Task 3 Mobile Networking Technology Assessment and Considerations

17 June 2005

INTRODUCTION

The Interoperable Networks for Secure Communications (INSC) project, currently in its second phase, is an international collaborative R&D activity between Canada, France, Germany, Italy, Norway, the Netherlands, the United Kingdom and the United States, with invited contributions from the NATO Consultation, Command and Control (C3) Agency. The objective of the project is to specify, implement, test, and demonstrate a common technical architecture for interoperable secure networks with mobility extensions, using commercial technologies, products and solutions wherever possible. The INSC Phase II project is broken down into subtask elements. The Mobility Task, Task 3 (T3), is responsible for experimenting with and investigating solutions to better support network mobility.

There are two main categories of mobile internetworking technology that T3 will be focusing on: dynamic, wireless routing technology (e.g. MANET) and edge system mobility technology (e.g. MIPv6, NEMO). The focus of this technical paper is to discuss rationale, technical tradeoffs and potential applications of each of these technologies, including a current assessment of implementation availability and maturity. In addition, there are a number of supplementary design issues which need to be considered that affect both dynamic wireless routing and mobile edge systems (e.g. autoconfiguration support and options). The purpose of this high level guidance and issues document is to provide rationale, tradeoffs, and guidance across several problem spaces for which such technology is being considered for future deployment. This document also discusses ways in which combinations of mobile technologies may work together to solve broader mobility problems.

PROBLEM AREA DEFINITION

There are two fundamental technology areas targeted for testing and demonstration within Task 3: *dynamic wireless routing* technology, and *edge mobility* technology.

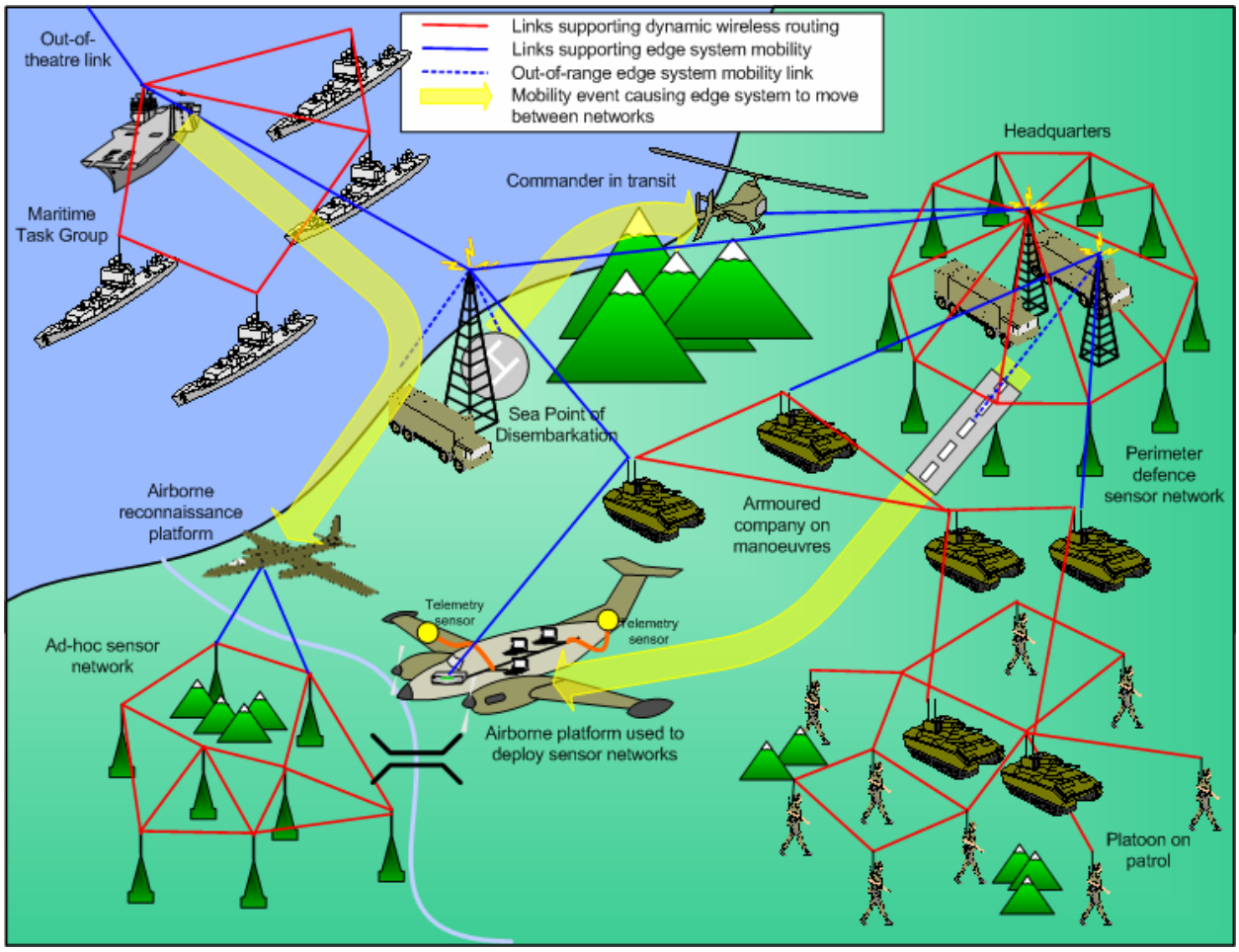

Figure 1: Architectural Mobility Variations

Figure 1 presents an imaginary military scenario in which both dynamic wireless routing and edge system mobility are playing important roles. In this example, a Maritime Task Group (TG) has formed a dynamic wireless routing area, establishing an internal communications mesh between all the ships in the group. The Capital ship is acting as a gateway out of theatre for the remainder of the Expeditionary Force (EF) through the node at the Sea Point of Disembarkation (SPOD). At the SPOD, a Commander has just left the area to visit the Headquarters (HQ) and, in doing so, has lost direct contact with the SPOD but has used an edge system mobility technology to re-establish communications through the gateway at HQ. Two other airborne platforms are in theatre, one of which has recently deployed an ad-hoc sensor network (that has now formed a dynamic wireless routing area of its own) via an air-drop. The other airborne platform is a reconnaissance craft that is flying over this ad-hoc sensor network, collecting data gathered by the sensor devices, which have low-power communications equipment that is unable to transmit to distant fixed assets without line-of-sight. Both of these airborne platforms have moved out of range of the links that they were using initially and have since re-established communications in other parts of the network via edge mobility. The platform that deployed the sensor network contains a LAN with multiple hosts and also has its own telemetry sensors relaying telemetry information on

the health of the platform's many components for fatigue analysis out of theatre. At the HQ, a second sensor network has been hand-deployed around the site perimeter to act as an intrusion detection system, with intrusion events being analyzed by staff within HQ. Finally, a platoon is on patrol and has formed a dynamic wireless routing area that has merged with a supporting armored company. Some of the infantrymen's radios are now using the armored platforms to forward information amongst themselves in order to preserve the more limited battery reserves of their man-packed radios. The armored platforms are also serving as a network gateway for the platoon to send data (reconnaissance pictures or video, situational awareness info, etc.) to HQ and receive orders from commanders.

Edge Mobility Overview

Edge mobility focuses on mobile users, systems, or even entire mobile networks that are capable of macro-mobility, moving across routing borders and within a larger wide area network (WAN). The main edge mobility technologies that will be discussed in this paper are Mobile IPv6 (MIPv6), designed to support individual roaming mobile hosts, and network mobility (NEMO) concepts, designed to support roaming aggregate networks. Both technologies require a supporting home agent (HA). The HA acts as an anchor point for roaming nodes or networks within a larger network, under the assumption that these nodes wish to retain their home-based associations and addresses. This is often useful if the roaming node or network has a server functionality that needs to maintain dynamic reachability via its old "home" address, or if there is a need to maintain existing connections while undergoing roaming conditions.

At a basic level, this broader type of mobility function is not always required since other methods including Dynamic Host Configuration Protocol (DHCP), peer-to-peer middleware, and dynamic Domain Name System (DNS) can allow for various degrees of edge system mobility support. A network node can move to a new area, obtain an address using DHCP or some other method (e.g., stateless autoconfiguration). A simple network client node (e.g., bursty web client) can typically use this type of service to receive adequate mobility support. More enhanced alternatives would include the additional use of dynamic DNS or possibly P2P middleware to update and register mobility information to allow clients to initiate communications with a mobile server. While these possible architectural alternatives should be considered in a broader context, INSC Phase II will focus its examination and demonstration efforts around MIPv6 and NEMO type technology and the relevance of this technology within a coalition battlespace application.

Dynamic, Wireless Routing Overview

Dynamic wireless routing is generally a more localized type of mobility. INSC Phase II is examining IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies. While IP routing protocols commonly in use on the Internet today (e.g. RIP, OSPF, BGP, etc.) are designed to handle network changes, they are not designed to cope with the high rates of change and unreliable channels inherent in mobile wireless networks. They are also generally designed with the assumption that data coming in an interface should never be forwarded back out

that interface, which is a valid assumption for the standard wired infrastructure routers in use on the Internet, but is not valid with typical packet radio interfaces. Although a broad range of academic work and dynamic wireless routing technologies are available, this paper will focus on the area of mobile ad-hoc networking (MANET) evolving within the Internet Engineering Task Force (IETF). Tactical technical considerations and enhancements envisioned will not be limited to present specifications. The fundamental MANET problem areas being addressed are that wireless link interfaces have some unique routing interface characteristics and that node topologies within a wireless routing region may experience increased dynamics, due to motion or other factors. Evolving IETF MANET specifications fundamentally provide improved operational IP routing performance for dynamic, wireless routing regions. This technology is applicable in stressed wireless tactical environments experiencing mobility or increased topological dynamics, but the tradeoffs between classes of approaches need to be carefully considered for both efficiency and robustness. The basic technology area is also potentially applicable for self-organizing sensor networks or groups of autonomous and semi-autonomous Unmanned Ground Vehicles (UGVs) and may be adapted in a hybrid operational context. Approaches are intended to be relatively lightweight in nature and suitable for heterogeneous adaptation across multiple hardware and wireless environments and for use in small, embedded systems as needed.

While MANET routing areas may operate in isolation from a larger connected Internet, a primary focus of the INSC II Task 3 work is to address its use as a routing technology extension at the edges of a coalition battlespace infrastructure. The technology directly supports a great dispersion of forces and resources and allows network connections to beyond line-of-sight (LOS) or beyond the capabilities of a single radio asset. The deployment of hybrid mesh infrastructures (e.g., a mixture of preferred fixed or resource advantaged nodes and highly mobile, disadvantaged routers) can also be supported by MANET specifications and management approaches and such a capability is considered important for tactical environments. In this way, without sacrificing flexibility-advantaged platforms or key network relays, nodes can be placed and preferred within the architecture when possible.

Mobility Support Technology and Protocols Overview

In the previous section, we have presented high level technical issues and an introduction to mobile networking work being executed within the INSC project. In addition, there are other more detailed issues and considerations that affect various mobile networking technologies and need to be considered before deploying or managing a particular mobility approach. One area of consideration is the interaction between the mobility protocols and the possible methods of address autoconfiguration and localized discovery services available in both IPv4 and IPv6. Each method has its strengths and weaknesses and related impacts on wireless applications and mobility. Wireless interface networking considerations are also unique in that cross-layer design aspects become more important than in wired networks. For example, in mobile systems, the wireless sensing of direct network neighbors and link status and quality is far more complex than in wired environments. While no standard practices exist across technologies, it is well accepted that improved cross-layer design approaches between

the wireless MAC layer and the network layer can improve mobile networking effectiveness. Such cross-layer design improvements will likely provide more consistent and accurate movement detection, neighbor discovery, and link quality assessment. Unfortunately, cross-layer interface design complexity may result in less flexible protocol stack designs. It is important to address the cost and flexibility impact of these approaches versus the relative performance gains expected. Detailed answers to such questions are often scenario and component specific. The ability of the mobility technology to support multicast is also an important aspect of the technology, especially in military scenarios and should be assessed for various application scenarios.

DYNAMIC, WIRELESS ROUTING TECHNOLOGIES

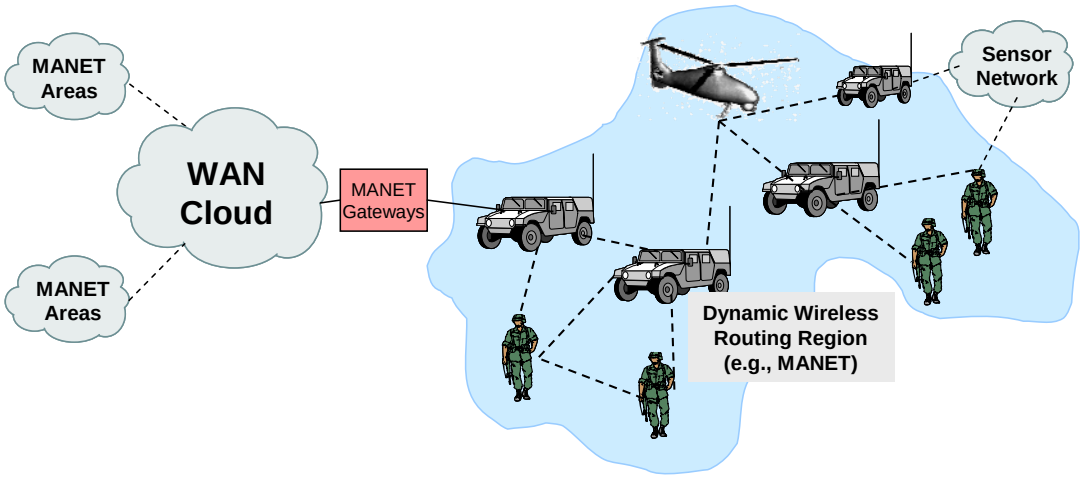

Figure 2: Mobile Ad-Hoc Network Example

Mobile Ad-Hoc Networking

A mobile ad-hoc network (MANET) is a group of mobile, wireless nodes that are able to act as routers and forward traffic (usually via the same interface on which it was received) for other nodes in the network. Each node must be able to forward traffic for other nodes, because the nodes may not always be able to talk to all other nodes in the network due to topology, distance, wireless effects, etc. The goal of the MANET routing protocol is to maintain topological reachability between the MANET nodes by quickly finding efficient routes through the network, and maintaining these routes under dynamic conditions, as shown in Figure 3.

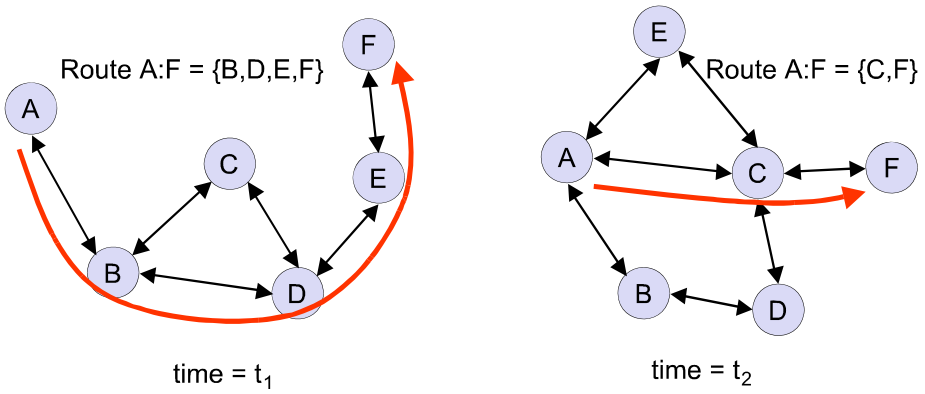

Figure 3: Dynamic Routing in Changing Topology

General MANET Technology Benefits

Obviously, the main goal of MANET, or any other related dynamic, wireless routing technology, is to effectively create reachability via routing amongst a set of operating nodes. This allows MANET to extend the edge of the network to include wireless regions multiple hops away from a more fixed network infrastructure. It also allows MANET technology to be used to create a mobile infrastructure, or to build a self-organizing, standalone network of MANET nodes to perform a common task or achieve a common goal in the absence of a fixed infrastructure.

While MANET solutions continue to evolve and are receiving ongoing, broad research attention, there are MANET solutions that are presently stable and are available to meet different performance criteria. Current MANET protocols can be largely divided into proactive and reactive protocols. In a proactive protocol (e.g. Optimized Link State Routing protocol, OLSR), each router node in the network constantly maintains a route to every other node in the MANET network. On the other extreme, reactive protocols (e.g. Ad-Hoc On-Demand Distance Vector routing protocol, AODV) search for and maintain routes to destination nodes upon demand from user traffic. Each of these methods has different performance characteristics, dependent upon the scenario of use. For example, proactive protocols may produce more network overhead under sparse user traffic loads than reactive protocols, due to the control messages required to maintain routes when the routes may not be needed. Of course, depending on the number of sender/receiver pairs and the frequency of communication, this overhead may not be significant when compared to a reactive protocol, particularly in a traffic scenario where many nodes are receiving data (as may often be the case in tactical networks). Reactive protocols, on the other hand, tend to produce more initial connection delay than proactive protocols, due to the time it takes to find a route when data needs to be sent. The overhead cost and needs are also less predictable and less uniform in nature than proactive protocols which may lead to difficulties in predictable performance under congested and stressed conditions. Thus, proactive protocols tend to have better peak performance, whereas reactive protocols have better average performance. There are also newer protocols (or enhancements to existing protocols) that have both proactive and reactive aspects to provide a more balanced design.

Additionally, protocol implementations tend to have different timers and performance parameters which can be adjusted to change relative performance characteristics.

At this point in time, the IETF MANET Working Group has several reasonably mature experimental specifications available for open use. There are many available reference implementations of these protocols, many of them open-source and reasonably mature, supporting both IPv4 and IPv6 on a variety of working platforms and simulation environments. Linux kernel modification is not generally necessary for these prototype implementations, though it may be required for more advanced features in the future. More concentration and specific work in IPv6-centric designs is also expected in the near future. The IETF MANET WG updated its charter in January 2005 to include several new work items. The target goals are to develop and specify one reactive and one proactive standards-track unicast MANET routing protocol. In addition, an item was added to work on a simplified multicast forwarding (SMF) concept for MANET environments. There is also a newer MANET-OSPF design team within the IETF that is developing standard extensions to OSPF to better support MANET environments. There is growing commercial and standards interest in developing enhancements to OSPF in this regard and the design team is in a stage of protocol design and development in which a number of experimental frameworks are still being tested and evaluated. Some early prototype Linux code is intended to be made available and may be adopted for some testing within the INSC Phase II schedule, along with present OLSR and other protocol testing.

As native IP routing, MANET technology can take direct advantage of other supported features within the IP protocol suite. For example, Quality of Service (QoS) can be added to routing control traffic to increase robustness, thereby improving throughput and overall network performance. It is also possible for MANET to support various autoconfiguration methods, including stateful IPv4/IPv6 configuration via DHCP/DHCP relay and IPv6 stateless autoconfiguration. A distributed form of IPv6 proxy prefix or router advertisement (RADV) extension is under consideration within INSC to advertise stateless network prefix information in a multi-hop wireless environment to ad hoc nodes.

MANET nodes are also capable of supporting attached network prefixes. This allows an entire IP subnet, or even multiple subnets, to retain efficient network connectivity to a larger MANET network (and possibly beyond) via a single MANET node they are attached to. This is useful, for instance, if you have a MANET node in a vehicle or command post with several attached network devices or local area networks (LANs). This capability, inherent in OLSR, can also be used to advertise and discover border gateways throughout the MANET network.

General MANET Technology Issues

MANET solutions are more applicable for supporting scoped mobile routing regions, and do not directly support macro-mobility (e.g. large scale roaming across a WAN or across routing boundaries). Such scenarios may be a better fit for the various edge mobility technologies and combinations of the technology are possible.

Varying application areas require specific examination of multiple solutions and MANET protocol options available. There are proactive and reactive protocols to choose from, as well as hybrid protocols having both proactive and reactive aspects. There are many implementations to choose from, and each implementation has a parameter set (e.g., hello intervals, timeout values, etc.) that may need to be changed from default values to meet given scenario-specific performance criteria.

While MANET technology may generally improve routing convergence and packet delivery under mobile conditions, the network end-to-end packet delivery will still experience increasing variance in delay and loss. This can be due to possible congestion, routing protocol overhead, and the time it takes to detect link failure and find a new route. Other technologies and existing protocol extensions, including applications layers and transport layers, need to be examined along with the routing protocol and can lead to drastically varying results versus looking at only raw packet delivery ratios.

MANET and dynamic network technology is still an ongoing topic of considerable research investment and interest and will likely continue to be over the coming years. It is not presently clear how well MANET will support backbone transit/infrastructure portions of network architecture design or how to best tradeoff security requirements with dynamic, mobility requirements. These are emerging technology areas needing more investigation and continued evolvement. Another area needing investigation is the tradeoff between network scaling performance and design complexity along with interactions with various MAC layers and evolving wireless technologies.

Dynamic, Wireless Routing Examples

Dynamic, wireless routing is of most value when the intention is to form topologically unplanned networks. This can be as a result of the method of network deployment or, more usually, as a result of (ongoing) mobility within the network. Within a military context, such networks are commonplace in the tactical domain as a result of both operational (e.g. pursuing the tempo of battle) and doctrinal (e.g. movement to protect assets) requirements.

At the Front Line of Own Troops (FLOT), sections of dismounted soldiers may be tasked with an objective requiring them to move around one another as they tackle their objective. It is crucial that the soldiers are free to manoeuvre as the operational situation (rather than the communications constraints) dictates. Dynamic, wireless routing treats each member of the section as a relay in order to pass information (voice or data) between members that are not within direct wireless range of each other. This property provides a transparent range extension in order to support extended manoeuvre. In addition, the soldiers may deploy expendable wireless micro-routers at strategic locations in challenging wireless environments, e.g. inside a building that is being neutralized, to increase the density of their MANET and therefore bolster their existing communications links or to maintain contact to and between UGVs used for reconnaissance inside buildings or in contaminated areas.

Behind FLOT, tactical backbone networks are required to link together Headquarters in order to update one another with operational developments and commands from higher authorities. These tactical HQs are moving periodically to avoid detection, but the location of their destination may only recently have been decided, thus forcing the formation of unplanned network topologies. Dynamic, wireless routing copes gracefully with these situations by automatically forming opportunistic links with neighbours whenever they are within range of one another. Dynamic, wireless routing can also be used to rapidly establish wireless LAN communications around a deploying HQ without the need for an RF survey of the area; additional relay nodes are deployed until the desired level of connectivity is established.

One significant enhancement of MANET allows for a sort of hybrid or hierarchical MANET. As shown in Figure 4 below, it is possible for MANET nodes to set a degree of preference for whether or not they wish to be a forwarding node (e.g. a router willingness factor). This has numerous management and deployment possibilities relating to policy, energy conservation, etc. It allows one to easily and quickly set up a fixed (in this example) grid or mesh of nodes with more powerful antennas than the other nodes, or with an alternate, higher-bandwidth wireless technology interconnecting them. This willingness factor could also allow mobile nodes with limited battery life to remain functional for longer periods of time, since nodes will prefer to go through the AC-powered nodes that have a higher willingness factor, thus resulting in less traffic being forwarded by the power-constrained nodes. This capability also has significant implications in sensor networks, scenarios using intermittently-connecting PDAs, etc.

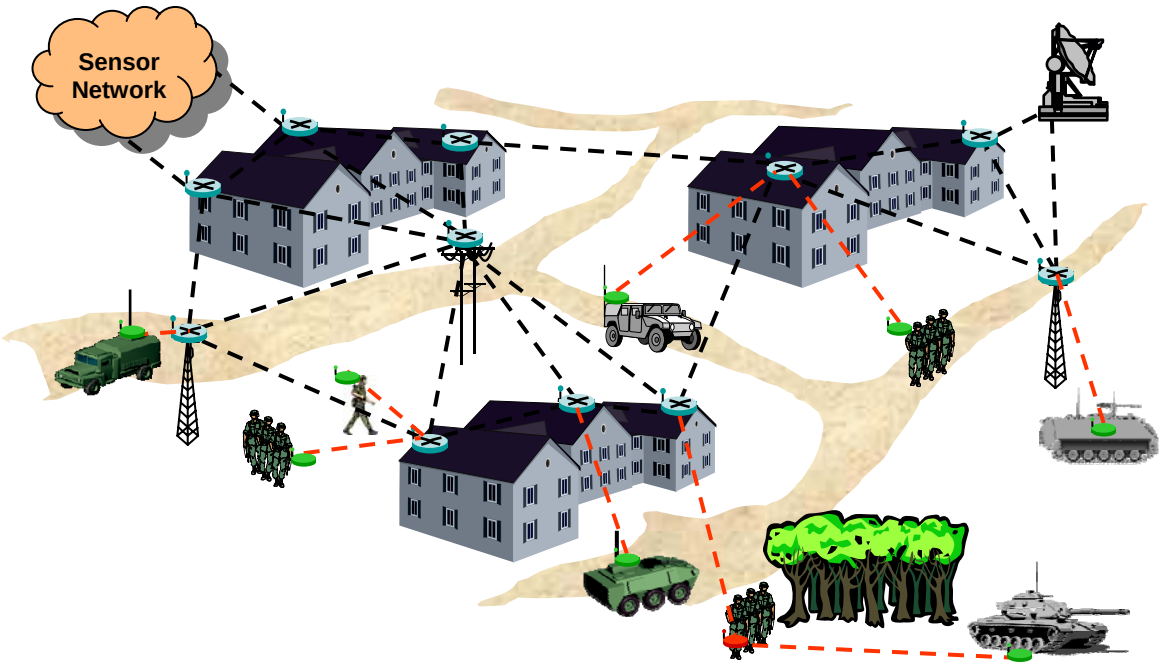

Figure 4: Hybrid MANET Access Grid Application

A sensor network is a collection of sensing devices communicating with one another throughout an area of interest. Events of interest are detected within the sensing range of one or more devices and sensor data on these events is passed around the network towards a designated device that forwards the information on to a more capable device for analysis and action (though some platforms are capable of limited computation). This device may either be attached locally or situated in a remote facility at the end of a long haul communications link. In a military context, sensor networks can be used as a remote, unmanned surveillance and target tracking system. They can be deployed using a variety of methods, such as hand-emplacement, air drop, and artillery firing into an area of interest. Examples applications for sensor networks include monitoring uncontrolled territory for advance detection of enemy troop and armor movements, and detecting intrusions into the perimeter around friendly bases of operation in the battle space.

Dynamic, wireless routing technology allows the sensing devices to be used as relays for one another so that topologically-challenging terrain can be circumvented using the meshed organization of the network. In addition, dynamic, wireless routing also allows the automatic formation of a network, negating the need for manual management of the network and allowing greater flexibility of deployment. Finally, although typically no actual device mobility takes place after a sensor network has been deployed, dynamic, wireless routing technology is necessary to overcome topological changes created by the environment (transmit distance may change due to rain, for instance) or the loss of devices due to power failure or destruction.

EDGE MOBILITY TECHNOLOGIES

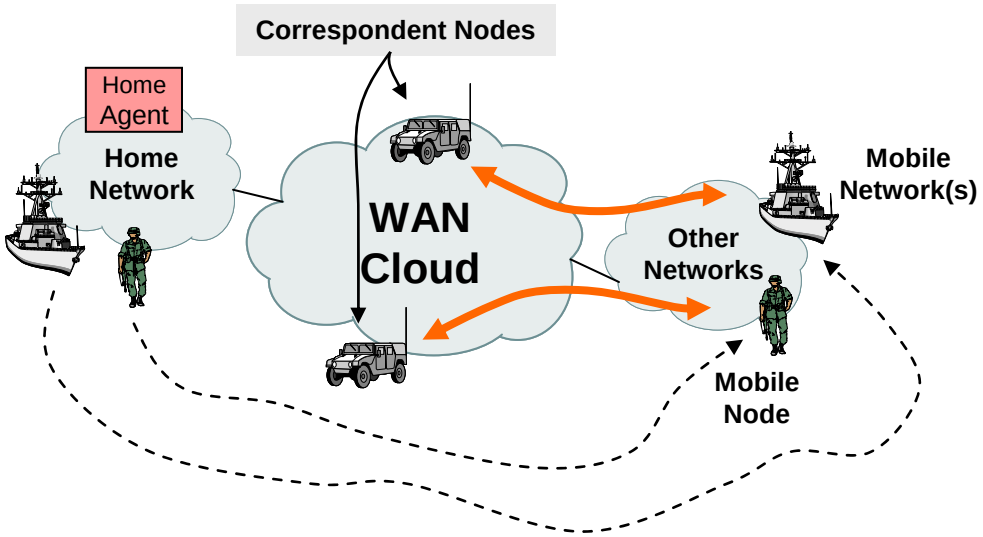

Figure 5: Edge Mobility Technologies

Mobile IPv6

Mobile IPv6 has three main components: the mobile node (MN), the home agent (HA), and the correspondent node (CN). The way Mobile IPv6 works is as follows. The mobile node registers with a specific home agent. When the MN moves to a new network (presumably by connecting to some sort of access point), it must detect that it has moved to a new network, and obtain a new IP address. While a new address can be obtained via DHCPv6 after being triggered by some sort of movement detection process, the more common method uses router advertisements (RADV) to detect movement and automatically assign a new address using stateless autoconfiguration. See the "other mobile systems issues and considerations" section below for more information on the stateless autoconfiguration process. Once this new address is obtained, the mobile node sends a binding update (BU) to the HA and any correspondent nodes it is currently communicating with, notifying them of its new care-of address (CoA).

There are two possible modes of communication between the mobile node and a correspondent node. The first mode, bidirectional tunneling, does not require MIPv6 support at the correspondent node. In this mode, the home agent intercepts all packets destined for the MN using proxy neighbor discovery, and tunnels them to the MN. Packets that the MN sends to the CN are also tunneled back through the home agent. The second mode of communication, route optimization, requires the correspondent node to have Mobile IPv6 functionality. This process starts out the same as the bidirectional tunneling mode, with the HA intercepting packets destined for the MN, and tunneling them to the MN's Care-of Address (CoA). With route optimization, the MN then informs the CN about its CoA, and the CN and MN can then communicate directly, without the aid of the HA. As long as a session is active, the MN needs to send a binding update (BU) to the CN when it moves to a new network, so that they may continue direct communications.

General MIPv6 Benefits

The main goal of Mobile IPv6 is to create and maintain dynamic reachability as a node moves to various points in a network. MIPv6 accomplishes this by setting up and maintaining tunnels. The two main advantages MIPv6 has over other edge mobility technologies is the ability to maintain reachability via a constant "home address" when it is on a different network, and to retain active sessions under motion.

MIPv6 has mature IETF standards-track specifications for its core functionality, as well as for the added ability to use IP Security (IPSec) to encrypt signaling between the MN and the HA. There are a few reasonably mature MIPv6 implementations available covering the Linux, BSD, CISCO IOS, and Windows operating systems, as well as simulation environments.

There is still significant evolving research being done in the area of MIPv6. Emerging enhancements and modifications, such as Hierarchical MIPv6 (HMIPv6) may help improve the performance and scalability of the protocol.

General MIPv6 Issues

MIPv6 is only necessary for mobile end systems which require a stable IP address for identification or for retainment of in-progress sessions while roaming between networks. If these conditions need not be met, and it is acceptable to obtain a new address and restart current sessions, then the combination of DHCP and dynamic DNS, as one possible example, may be sufficient to meet mobility criteria, and MIPv6 maybe unnecessary.

The main MIPv6 specification includes a mechanism for Dynamic Home Agent Address Discovery (DHAAD), which can be used for avoiding a manual configuration of the Mobile Node with the Home Agent's address. However, there is currently no mechanism that allows a Mobile Node to detect the prefix of its home network when attached to a visited network. This must currently be done manually, though there is work underway to address this aspect in an automatic way using the Authentication, Authorization, and Accounting (AAA) infrastructure. Additionally, while multiple home agents are supported, they must be on the same home network. In a military environment, MIPv6 deployment scenarios and robustness requirements may need to be carefully considered due to the single point of failure inherent at the home network.

As one might expect from the name, Mobile IPv6 is designed specifically for use with IPv6. There is also a Mobile IPv4 specification available, but it does not have the enhanced efficiency and scalability features due to lack of route optimization and other mobility-oriented aspects inherent in the IPv6 protocol. Unfortunately, there are not a wide variety of MIPv6 implementations available at present to choose from on any given platform. Only the Linux, BSD, and Windows operating systems have implementations. The most recent Linux implementation still requires a minor kernel modification of the mobile node, which many users may wish to avoid. In addition, nodes wishing to communicate with a mobile node must also be running a modified kernel in order to take advantage of route optimization. These requirements should disappear in a future release, when everything can be done in user space.

MIPv6 has some additional performance issues that need to be carefully considered. The tunneling required by MIPv6 introduces extra overhead into each packet and decreases available Maximum Transmission Unit (MTU). These tunnels may be passing through additional IPSec tunnels so the degree of nesting can become an overhead and architectural design concern, particularly if there are a large number of mobile hosts. Additionally, fast handoff of a mobile node has significant limitations due to the required local interface protocol standards. For example, even with increased RADV timers for mobility detection improvement, it takes a minimum of 1 second on many kernels to complete duplicate address detection (DAD) after movement to a new network is detected and a new IPv6 address is statelessly autoconfigured. This delay could cause major issues (possibly timeouts) at the transport/application layers, and should be investigated in scenarios where session handoff is important. One alternative could be to avoid using DAD in a wireless environment; however, a more elegant "make-before-break" mechanism is currently being researched in the IETF. With this method, a mobile node tries to predict upcoming movements, and performs the time-

consuming tasks of IPv6 Neighbor Discovery (ND) and DAD on the new point of attachment before disconnecting from the previous point of attachment.

Network Mobility

Network Mobility (NEMO) is essentially an extension to Mobile IPv6. NEMO is designed to apply to entire networks in motion, rather than just individual nodes in motion. The Basic Support protocol is run between a new MIPv6 entity called the mobile router (MR) and the home agent (HA). The MR provides routing services and reachability to the nodes attached to it within the mobile network. The mobility of the MR and the network as a whole is transparent for the nodes within the mobile network. In the case of MIPv6, an alternative solution for ordinary client machines is to simply obtain a new address and restart any existing sessions. However, such an alternative is not recommended for mobile networks, because it requires every node within the mobile network to obtain a new address in a local prefix or the Mobile Router to inject specific host and/or network routes for the mobile network into the WAN at its point of attachment. Neither of these options is particularly scalable for large numbers of mobile networks.

To indicate to the HA that a node is function as a Mobile Router instead of a standard Mobile Node, a new flag is set in the binding update to the home agent. The MR informs the HA via the binding update of the network prefixes that should be forwarded to the MR's Care-of Address. The HA then sets up forwarding to the Mobile Router's CoA for these prefixes. The MR also functions as a standard MN for sessions addressing the MR at its home address.

When the MR is not at its home network, all packets destined for, or originating from, nodes in the mobile network are sent over a bidirectional tunnel between the MR and HA, similar to the MIPv6 bidirectional tunneling mode. The mobile network can contain numerous Local Fixed Nodes (LFN) and Local Fixed Routers (LFR) as shown in Figure 6, which are permanently attached to the mobile network. The mobile network can be the home network for MIPv6 Mobile Nodes, and can also support visiting Mobile Nodes and/or Mobile Routers attaching to it.

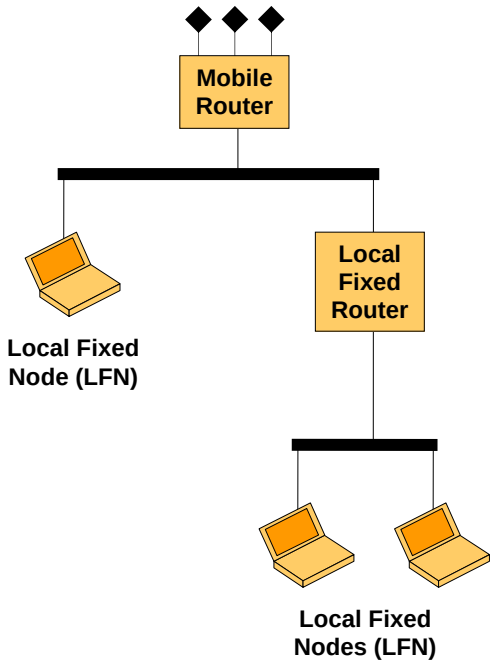

Figure 6: A NEMO Mobile Network

General NEMO Benefits

NEMO extends the benefits of MIPv6 to apply to entire networks in motion, rather than individual nodes. This extension results in a decrease in required protocol signaling traffic. There is an IETF standard-track specification detailing the exact functionality of the NEMO basic support mode. An implementation is available for CISCO IOS, and an open-source implementation for Linux and BSD has also been released.

General NEMO Issues

While the NEMO basic support mode has been specified, work on the extended support mode addressing route optimization is still ongoing within the IETF. Therefore, the idea of nested NEMOs (one Mobile Router connecting to another Mobile Router's mobile network) currently results in additional encapsulated tunnels between the Mobile Router and the Home Agent. There are several possible methods for improving this, but it is not very well defined in the specification currently. Thus, any solution based on it at this time will possibly need to be changed at a later date to conform to more mature specifications.

The basic benefit of NEMO is still with regards to supporting macro-mobility, and it is not an appropriate protocol for managing significant amounts of localized mobility. The reliance on a home agent is a similar issue as with MIPv6 and needs to be carefully examined for deployment relevance.

Edge Mobility Technology Examples

An example of how NEMO technology can be conveniently exploited in an operational environment is presented in Figure 7. The example shows a military vehicle equipped

with an on-board LAN, which may include several PCs and one or more Wireless Access Points (APs) for local Wireless LAN (WLAN) coverage. The WAN connectivity for this moving network is provided by a mobile router with multiple WAN interfaces (HF/VHF, satellite, WLAN, Ethernet, etc.). The NEMO protocol, which is implemented on the mobile router and on the Mobile IPv6 Home Agent located in the headquarters, gives the on-board LAN uninterrupted WAN connectivity independent of the radio access being used by the mobile router to plug into the tactical IPv6 backbone. The mobile router is free to select at any time the most convenient access technology, based on coverage conditions and vehicle velocity.

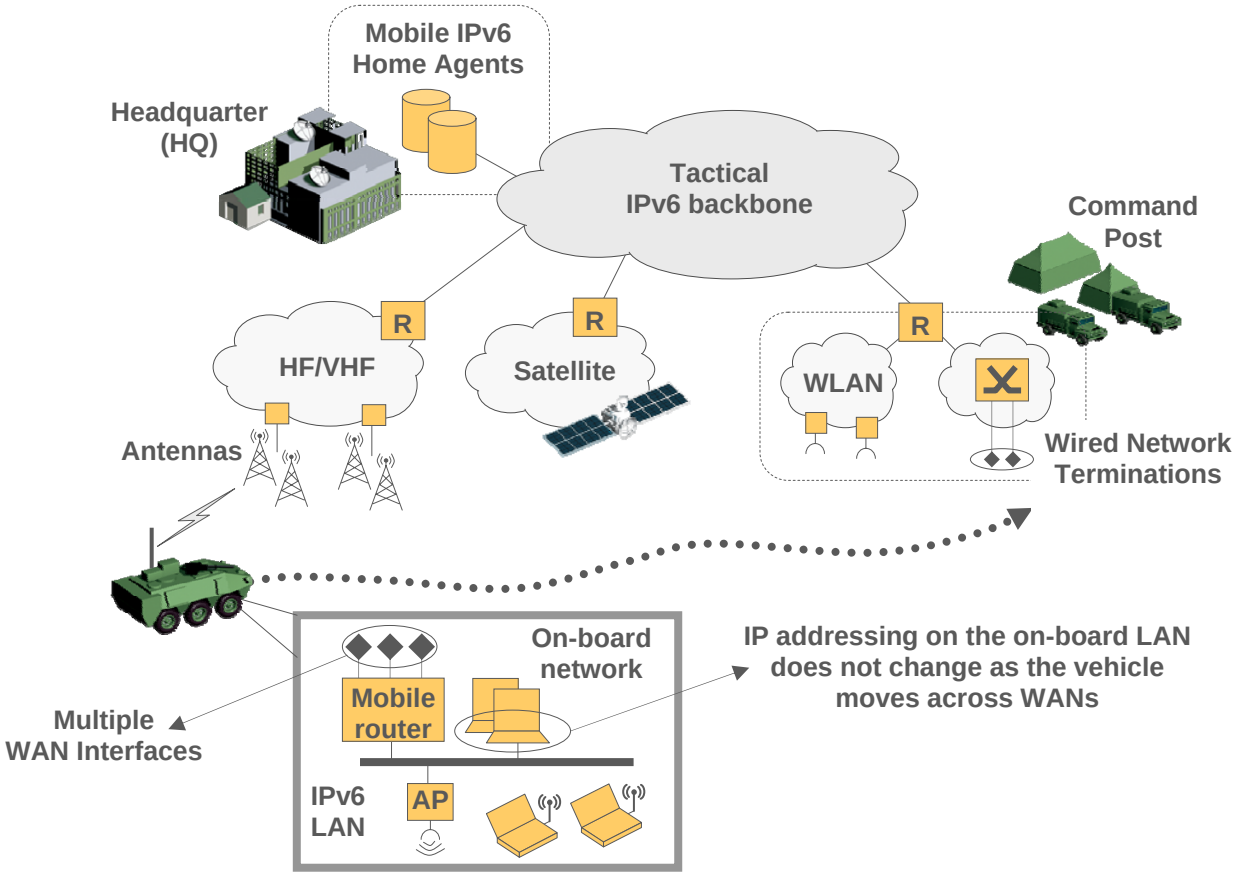

Figure 7: Basic NEMO scenario

In a typical operational scenario, the military vehicle can exploit HF/VHF or satellite while in the battlefield, and can relay on high speed links, like WLAN or Ethernet, when parked in a command post. NEMO technology allows all of these movements across access WANs to take place transparently. All active communications survive to movements and there is no need to re-configure the PCs or other appliances located on the on-board LAN, which can be made constantly reachable at their long-lived IPv6 addresses.

Moreover, even though the scenario in Figure 7 refers to vehicles moving on the ground, the same concepts can be applied to ships or other naval units. For example,

using NEMO, it would be possible for a ship docked at a port to switch from satellite to cable connections without the need of any manual intervention on the on-board equipment.

Figure 8 shows an example of nested NEMO scenario. It is assumed that the military vehicle hosts one or more soldiers, each equipped with a PDA (or another personal appliance) providing connectivity to a set of wearable tools (weapons, healthcare sensors, etc.). The PDA and the other tools form a Personal Area Network (PAN), which can be managed as a "personal moving network", with the PDA running the NEMO protocol (i.e. the PDA is the mobile router). In this way, each PAN is permanently reachable independently of the actual location of the soldier.

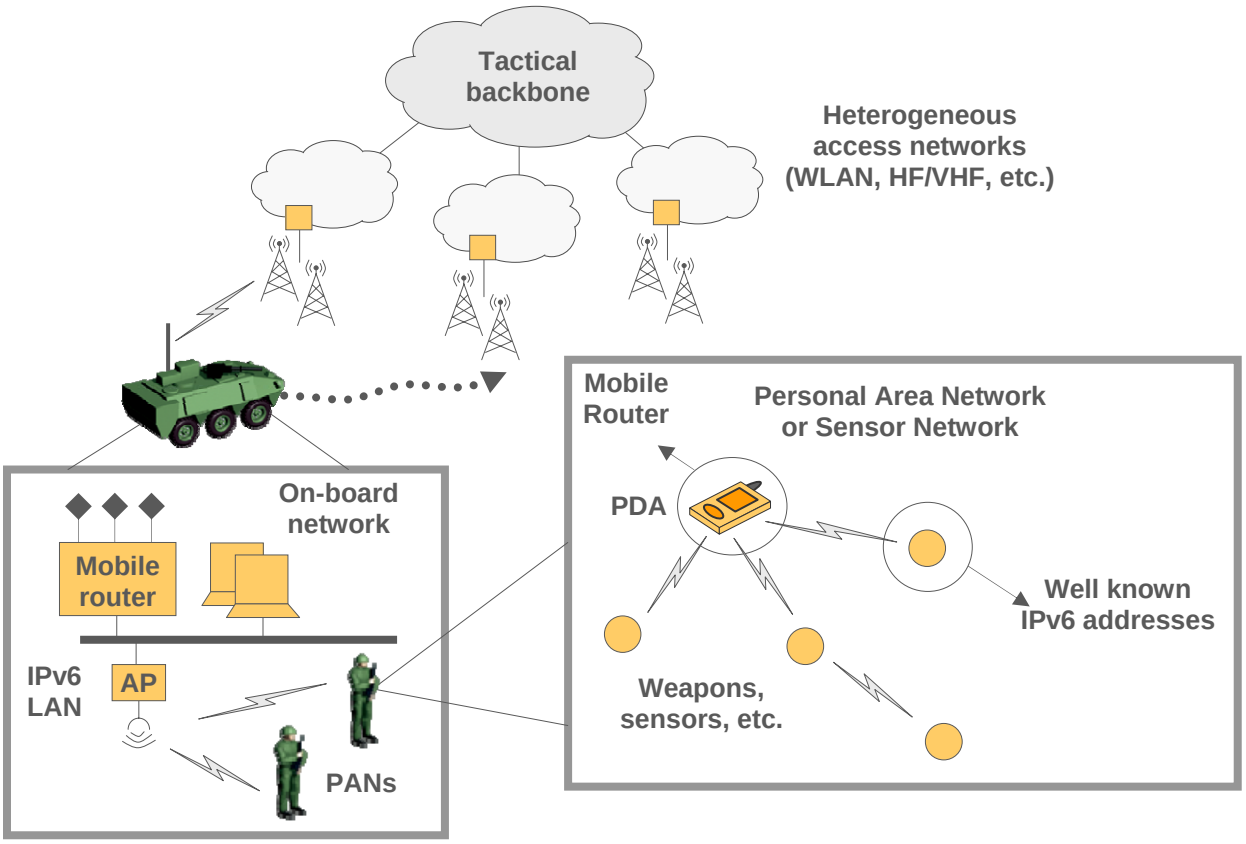

Figure 8: Nested NEMO scenario

Figure 9 shows a couple of examples of how NEMO and MANET can be used together. The simplest option is to have a moving network providing WAN connectivity to a MANET (see Figure 9-A). In this case, the WAN interface of the MANET gateway is connected to the on-board LAN and the MANET gateway can be either implemented as a stand alone machine or co-located with the mobile router. As a result, the MANET can benefit from mobile connectivity to the tactical IPv6 backbone.

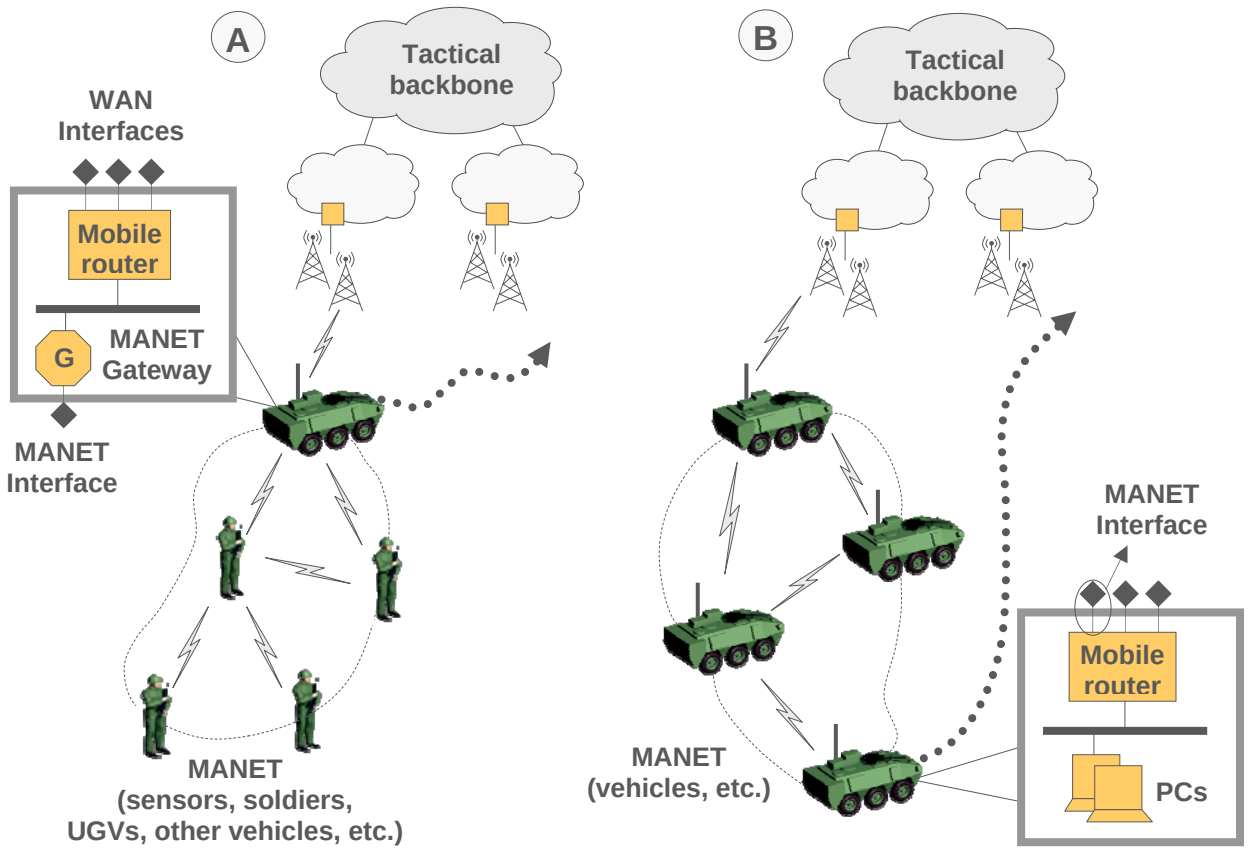

Figure 9: Combined usage of NEMO and MANET

Another interesting option is to use a MANET, made up of soldiers or other vehicles, as the access medium for a moving network (see Figure 9-B). In this case, the mobile router is equipped with a WAN interface running a MANET routing protocol such as OLSR. Another possibility is for the mobile router to connect as an attached network to a MANET node. NEMO support allows the vehicle to transparently move from the MANET to an infrastructure-based access (e.g. HF/VHF, satellite), or vice versa.

OTHER MOBILE SYSTEM ISSUES AND CONSIDERATIONS

Autoconfiguration

While there are numerous possible methods for node autoconfiguration, there are two well-established, fundamental methods used in IPv6. The first fundamental method is stateful autoconfiguration (e.g., DHCP), where a node sends out an address request, and a server responds with an assigned address, and potentially other information (DNS addresses, gateways, etc). The second fundamental method is stateless autoconfiguration, where the node listens for (and optionally solicits) a router advertisement from a router running the RADV daemon. It then uses the prefix received in the router advertisement, along with its EUI-64 identifier to assign itself an address which should be unique (since the EUI-64 identifier should be unique). In extreme mobile computing environments, manual node configuration is often not an option;

some degree of autoconfiguration functionality is needed. Unfortunately, existing autoconfiguration methods were designed with single hop LAN environments in mind, so they translate poorly to dynamic, multi-hop, wireless environments. Fortunately, some of these limitations can be overcome with extensions to the protocols, and INSC Phase II will address some of these issues for military-relevant MANET and MIPv6 environments.

DHCP is sufficient for getting an address for an Edge Mobility technology. Unlike router advertisements, however, DHCP cannot be used for MIPv6 or NEMO movement detection; consequently, when using DHCP for automatic address configuration of a Mobile Node or Router, a different mechanism is required for movement detection (e.g. a layer 2 trigger). The DHCP specification was designed to work in a low loss, 1-hop LAN environment, which is obviously problematic for MANETs. Fortunately, the DHCP specification is extensible by design and also allows for the concept of DHCP relay agents, which can relay DHCP requests between a server/client pair, thus allowing the protocol to be extended to support multi-hop environments, including MANETs. However, this may add some additional complexity to system design and may not be the most scalable approach, since every node must have the ability to act as a DHCP relay for the network to properly support autoconfiguration. The performance of such a mechanism in these environments needs further examination.

Stateless autoconfiguration in IPv6 also does not directly translate well to mobile networking environments. For example, Duplicate Address Detection (DAD) must be run after a node assigns itself an IP address, in order to ensure that the address is unique. The one second timeout assigned to the DAD process in its specification severely limits fast handoff in MIPv6, though new methods such as “make-before-break” may eliminate this problem. It may be possible to fix this problem by altering the timeout value within the DAD implementation, or even by disabling DAD, since EUI-64 identifiers (and therefore IPv6 addresses) may be better managed and controlled in a military environment. Stateless autoconfiguration is also a problem in the MANET environment, again due to its multi-hop nature. There currently exists no multi-hop IPv6 Neighbor Discovery and Duplicate Address Detection method, so if a MANET node assigns itself an address which is already taken, it will not be able to detect that condition unless the other node happens to be its immediate neighbor. As with MIPv6 though, DAD may be unnecessary since EUI-64 identifiers may be better-controlled in military environments. Stateless autoconfiguration depends on the use of router advertisement (RADV), which is also designed for more classical one-hop networks. However, we can get around this problem by having each MANET node run an RADV daemon (or something similar), at the cost of added system complexity due to requiring each node to support this. The performance of this mechanism also needs further examination.

Cross-Layer Design

A current limiting factor in MANET is the injection of added signaling traffic to detect neighbors, and the inaccuracies of judging link quality based on this injected traffic using timeouts. Links and neighbors can be lost because of motion, wireless effects, or

even network congestion. Most of this signaling traffic would not be necessary if it were possible to get feedback from the link layer at the routing layer. A promising future improvement of MANET would be the ability to obtain a list of neighbors, link quality metrics, etc. from the link layer, and use this information to make better and more elaborate routing decisions more quickly, without the extra signaling overhead. Unfortunately, it is very difficult at this time to get such information from the network interface drivers, and in such cases where it can be obtained, the solution is very specific to the radio hardware used, due to lack of a standardized interface. Link layer feedback could also be very useful in MIPv6/NEMO, where there is added signaling overhead used for the purpose of detecting node motion if fast switching is desired. With link layer feedback, it would be possible to improve detection of when a node is moving from one network to the other.

Specific radio technologies can also have a great effect on wireless mobility technology. Bandwidth limitations, propagation delay times, and requirements for low probability of interception and detection (LPI/D) are example of characteristics that affect the feasibility and effectiveness of different mobility solutions. Wireless characteristics and environmental effects must be taken into account when deciding on a specific mobility solution or when adapting protocol performance parameters for a given scenario. Next generation software-defined radios should be designed with mobility and protocol flexibility in mind, and emerging radio technologies and associated MAC layer designs such as orthogonal frequency division multiplexing (OFDM), spread spectrum, an ultra wide band should be investigated for use in a variety of mobile networking technologies.

Other Issues

In a military environment, multicast can be very useful to efficiently send data (e.g. situational awareness) to multiple recipients while using the least amount of bandwidth required. Multicast support in mobility technologies is unfortunately not highly mature. In MANET, specifications and prototype implementations are currently being developed to allow intelligent and efficient flooding of multicast packets through the network (some of this work is being done within INSC). True multicast capabilities, where nodes dynamically join and leave groups, rather than simply flooding the packets throughout the entire network, are an ongoing development. In Edge Mobility technologies, there is the issue of whether a given multicast group should be joined locally at the current point of attachment, or whether the multicast packets should be tunneled between the current Care-of Address and the home network, so that the mobile node or mobile network can join and retain a connection to multicast groups on its home network. At present, INSC Task 3 members are further investigating issues relating to edge system mobility and multicast support features and related protocols. Proper answers to these questions are likely scenario dependent.

Within future envisioned architectures, the broad range of mobile network application scenarios and topological dynamics results in specialized security and management approaches that must be considered. The appropriate approaches to consider are dependent upon the scenario and component specifics, so there is likely no one approach. Additional considerations should be given to the better defining the

appropriateness and level of management and security required in various mobile network scenarios.

Network partitioning is also a concern in the various mobile networking technologies. In NEMO and Mobile IPv6, network partitioning can cause total loss of all connections and reachability. If the new point of attachment for a Mobile Node or Network loses its connection or its route to its Home Agent, then the tunnel to the HA will be lost, as will all connections traveling through that tunnel. The same problem may occur if the Home Network loses its connection or route to the Care-of Address of the Mobile Node or Router. In MANET, nodes (or groups of nodes) are able to separate from the main MANET network and continue to maintain network connections to and from reachable nodes. Nodes may also rejoin the network when they come back in range. Fragmentation and reforming of network routing segments create more complex problems in autoconfiguration. If the nodes split off and connect to a new node which does not have an address, the autoconfiguration (particularly stateful approaches) may fail. This may be a secondary concern, if the only main purpose of the network scenario in question is for nodes to maintain a connection and use a gateway to the WAN. On the other hand, if the primary purpose of the MANET is for nodes to talk to each other, there may be a need to establish some sort of temporary address until the networks rejoin. Network partitioning is a topic in all mobile networking technologies that still needs further investigation and scenario specific consideration.

SUMMARY

As mentioned in the introductions, the two main categories of mobile networking technology focus in INSC II Task 3 are dynamic, wireless routing technology and edge system mobility technology. While there are numerous solutions falling under the general categories of dynamic, wireless routing technology and edge system mobility technology, the Task is concentrating on non-proprietary technologies currently evolving within the IETF: MANET for dynamic, wireless routing technology, and MIPv6 and NEMO as edge system mobility technologies. Each of these technologies has its own technical tradeoffs and potential applications. Edge system mobility technology is useful for macro-mobility across routing boundaries within a larger WAN, while dynamic, wireless routing technology is suited for more localized mobility. When deciding which mobile networking technology best matches a particular scenario and environment, there are many factors that must be taken into account, from technical tradeoffs of the various technologies to issues which effect both dynamic, wireless routing and edge system mobility, such as autoconfiguration and radio technology effects. This paper has discussed some of these issues and tradeoffs and has tried to provide relevant scenario description and potential use cases.

At this point in time, there are a number of MANET protocols with relatively mature experimental specifications, and there are multiple reference implementations of each of these for a variety of platforms and simulation environments. These implementations generally have multiple parameters which can be tuned to further alter the performance of a protocol to meet a given problem space. There are also newly evolving MANET

protocols, such as the MANET extensions to OSPFv3 that can play an important role in future deployments and interoperability scenarios.

With the recent push for IPv6 in the military, it is also important to note that MANET protocol specifications and implementations exist for both IPv4 and IPv6, although further work on IPv6 specifics continues to evolve. Other MANET features we have discussed include support for various autoconfiguration methods, the ability to take advantage of other IP-layer features and technologies (e.g. QoS), support for attached IP network devices and prefixes, and the ability to use router willingness to create a hierarchical MANET and hybrid MANET meshes. Some MANET features can also be adapted to improve energy and bandwidth efficiency within the mobile network.

The main benefit of MIPv6 is that mobile nodes are reachable by their home address on any network they are attached to, and that they are able to retain sessions under motion. MIPv6 has mature IETF standard-track specifications, and is supported under several operating systems and simulation environments, but there are not many implementations available to choose from on any given platform. Future improvements such as HMIPv6 may help the protocol's scalability issues but these advancements are uncertain. One major issue of MIPv6 is the question of its usefulness in military scenarios, as there are other ways to maintain reachability (e.g. dynamic DNS, middleware) and session retention is not always necessary. Other current issues include the effects of tunneling on the MTU, required manual configuration of the home network prefix, and the inefficiency of the IPv4 version due to lack of route optimization.

The benefits of NEMO are similar to those of MIPv6, except that NEMO is designed to apply to entire networks in motion, rather than individual nodes. The NEMO basic support protocol is specified in a standard-track IETF specification. Implementations exist for CISCO IOS, Linux, and BSD.

There are other general issues relating to both mobile edge system and dynamic, wireless routing technologies. One of the biggest issues is autoconfiguration. In INSC Phase I, it was learned that the duplicate address detection (DAD) process used by stateless autoconfiguration for MIPv6 results in excessive delays during fast mobile node handoff. Early recommendations from INSC Phase I are that DAD should not be used in many wireless mobility scenarios. Autoconfiguration is also an issue in MANET, because DHCP, RADV, and DAD were all designed to work in reliable, robust, one-hop environments. Cross-layer design, especially feedback from the link layer to the network layer, has great potential for improving performance of any mobile networking technology. Specific lower layer wireless effects and designs must also be taken into account when deciding on a mobility solution. Multicast support and the effects of network partitioning must also be taken into account when choosing a mobility technology to fit a given scenario.