Securing Mobile Networks in an Operational Setting

William D. Ivancic, NASA/GRC,
David H. Stewart, Verizon/GRC,
Terry L. Bell, Lockheed Martin/GRC
Phillip E. Paulsen NASA/GRC
NASA Glenn Research Center
Cleveland, Ohio 44135

Dan Shell
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134-1706

Abstract—**This paper describes a network demonstration and three month field trial of mobile networking using mobile-IPv4. The network was implemented as part of the US Coast Guard operational network which is a ".mil" network and requires stringent levels of security. The initial demonstrations took place in November 2002 and a three month field trial took place from July through September of 2003. The mobile network utilized encryptors capable of NSA-approved Type 1 algorithms, mobile router from Cisco Systems and 802.11 and satellite wireless links. This paper also describes a conceptual architecture for wide-scale deployment of secure mobile networking in operational environments where both private and public infrastructure is used. Additional issues presented include link costs, placement of encryptors and running routing protocols over layer-3 encryption devices.**

Mobile-ip, networking, satellite communication, network security, encryption

I. Introduction

Cisco System and NASA Glenn Research Center, working together under a cooperative agreement (a NASA Space Act Agreement), have been performing joint networking research to apply Internet technologies and protocols to space-based communications. As a result of this joint research, Cisco Systems has developed a mobile-router for both the commercial and government markets. The mobile router (MR) implementation fully conforms to Mobile-IP [1], a routing protocol that allows hosts (and networks) to seamlessly "roam" among various IP subnetworks.

NASA is interested in applying mobile-IP technologies to its space and aeronautics programs [2, 3]. In particular, mobile-IP is expected to play a major role in advancing communications, navigation and surveillance (CNS) system research and development in support of modernization of the National Airspace System (NAS). Mobile networking will be applied to the Advanced Aeronautic Transportation Technology (AATT), Weather Information Communication (WINCOMM), Small Aircraft Transportation System (SATS), and NASA Exploratory Technologies for the National Airspace System (NExTNAS) initiatives.

The MR early field trial code was tested using 802.11b wireless links in a controlled laboratory setting at NASA's Glenn Research Center in order to validate the code and test the performance of handoffs and applications when transitioning networks [4]. To address "real world" deployment issues (e.g. issues associated with Firewalls, Network Address Translation [NAT], mixing of public and private address space, and security), we needed to deploy MR in an operational network. In the end, we chose to deploy the MR aboard a United States Coast Guard (USCG) cutter. NASA and Cisco approached the USCG to participate because:

- The USCG had immediate needs for mobile Internet connectivity, and a willingness to work the problem.
- The USCG had military network requirements.
- The USCG had a large enough network to uncover and address full scale deployment issues
- The USCG was small enough to work with.
- The USCG Cutter Neah Bay, home ported in Cleveland, Ohio, was determined to be available from Spring through Fall, and it already had a network onboard (used while in port).
- USCG had the same network issues regarding mobility, security, network management and scalability for deployed assets as NASA.

II. Getting Buy-In from the US Coast Guard

The USCG has adopted Internet technologies across the board as a way to improve productivity and reduce costs. This initiative, known as "E-Coast Guard", moves financial, personnel, procurement, inventory and other communications to Web-based deployment. This has proven to be problematic for crews stationed aboard smaller vessels when away from port as Internet connectivity is generally none-existent. In addition, in the current network deployments, ships can only obtain connectivity when connected to USCG owned infrastructure.

The organization responsible for all USCG networks is the Telecommunication and Information Systems Command (TISCOM). Anything that could in anyway affect the USCG network had to be approved by TISCOM (they are ultimately responsible for maintaining network operations and network security). Thus, for the purposes of this demonstration, TISCOM buy-in was absolutely necessary. In addition, we had to obtain approval to utilize UCSG assets from many others including: the 9th District Commander and the Captain of the Neah Bay.

A. Mobile Router Advantages

Mobile router technology provides many unique advantages over the current method of obtaining connectivity for ships when away from port. These advantages convinced the USCG to allow a field trial deployment in their operational network. MR advantages include:

- Mobile networking can utilize multi-homed interfaces thereby allowing use of the "best available link"[1] also known as preferred path.
- Depending on the security policies, mobile networking enables users to share wireless and network resources with other organizations, thereby dramatically reducing overall infrastructure costs.
- Mobile router is a "set and forget" technology. Once configured, no onsite expertise is required (keeping in mind that the network still has to be designed upfront).
- Mobile router is link independent and therefore capable of providing continuous connectivity over a wide variety of assets (wired, 802.11, and satellite-based services). This may or may not be important to particular deployments.
- Mobile router can provide additional robustness (and survivability) to the network via features such as multi-homing and the ability to deploy prioritized home agents.

B. Design Goals and Requirements

NASA and Cisco worked with TISCOM to develop the following design goals and requirements:

- Secure
- Scalable
- Manageable
- Fully interoperable with existing network systems
- Ability to share network infrastructure
- Robust
- Minimal Impact (No Impact) on existing operations

As this was only a field trial and not part of TISCOM's charter, they could only modestly support this effort. Thus the design and deployment had to require few of TISCOM's extremely limited resources.

In order to have minimal impact on operations, a design was implemented that allowed the USCG to toggle between their existing network and the new mobile network by simply throwing a switch.

In order to maintain network integrity at all times, all routers not in the complete and secure control of TISCOM were positioned to be outside the USCG operational network. In order to minimize the impact on TISCOM staff (needed to modify routers and firewall rules), all agreed that a failsafe layer-3 encryption device would be inserted between the Neah Bay LAN and the USCG. Initially a NSA-approved Type 1 encryptor (on loan from the NSA) was used, but, due to operational commitments related to 9/11, it had to be returned prior to deployment of our gear. In its place, a Type 2 encryptor capable of running Type 1 encryption algorithms was used [5]. This was advantageous as the physical security requirements for a Type 1 encryptor made it difficult to deploy in the environment provided. A few key issues regarding deployment of layer-3 encryption devices were uncovered during the course of our development process. These issues required Western DataCom, the encryptor device manufacturer, to make firmware modifications [6]. These modifications will be discussed later in the paper. The deployment had to be designed to be scalable and manageable. TISCOM wanted to be sure that if the technology demonstration was successful that it could be deployed on a large scale – potentially over the entire Coast Guard – and easily managed.

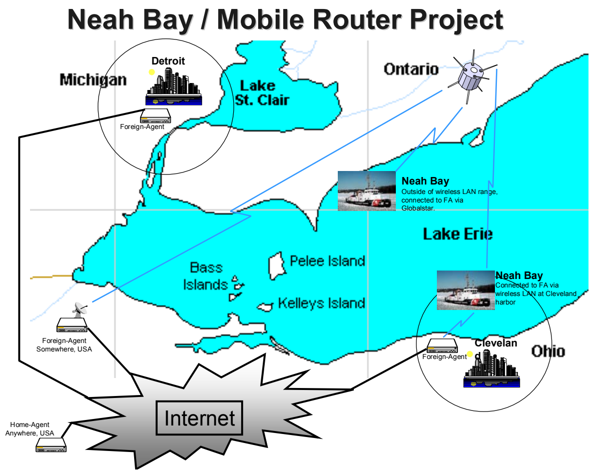

Neah Bay / Mobile Router Project
Detroit
Michigan
Lake St. Clair
Ontario
Foreign-Agent
Neah Bay
Outside of wireless LAN range, connected to FA via Globalstar.
Lake Erie
Bass Islands
Pelee Island
Kelleys Island
Neah Bay
Connected to FA via wireless LAN at Cleveland harbor
Foreign-Agent Somewhere, USA
Clevelan d
Foreign-Agent
Ohio
Internet
Home-Agent Anywhere, USA

Figure 1. Mobile Network Architecture

III. Network Architecture

Figure 1 shows the mobile network architecture that was used to demonstrate mobile networking in the USCG operational network. An MR was deployed onboard the Neah Bay with multi-homing capability. Three 802.11 networks and one satellite network were used to demonstrate handoffs between networks. The home agent (HA) was located in Cleveland, Ohio. Two 90 degree flat panel antennas were located 400 feet above Lake Erie on the Cleveland Federal Building. They provided coverage to approximately 20 statute miles [7]. Each of these antennas was intentionally connected to a different network (and foreign agent) to test handovers between networks. To provide geographic diversity, an additional 802.11 antenna was also fielded at the Coast Guard station in Detroit, Michigan. The MR was configured to preferentially choose between links based on throughput. When disconnected from a wired network connection the MR automatically sought an 802.11 link. When out of connectivity with any of the 802.11 links, the MR automatically switched to the satellite link.

[1] "Best Available Link" is determined via configuration in the mobile router and can be highest bandwidth, least cost, or some other criteria.

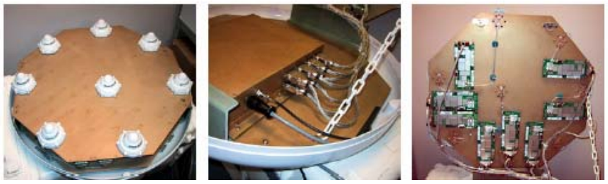


Figure 2. MCM-8 Field Demonstration Unit

The Globalstar satellite network and the Sea Tel MCM-8 modem were used for this demonstration [Fig. 2]. Globalstar is a Low Earth Orbiting (LEO) satellite designed to operate with hand-held phones utilizing omni directional antennas; thus, no tracking antennas are necessary. The latest MCM-8 commercial unit only requires a single antenna rather than the eight shown in Figure 2. The 8 channels are frequency multiplexed prior to being sent to the antenna. The MCM-8 modem can provide up to 56 kbps bidirectional connectivity when utilizing eight Qualcomm data packet modems, which are combined using a bonding router. The MCM-8 system requires that a corresponding bonding router be located somewhere on the open Internet – in our case, the USCG communications closet. The 8 packet circuits can be configured to operate with all channels up all the time or in bandwidth-on-demand mode (where only those channels that are needed will come up). During the experiments, the system was configured for bandwidth-on-demand.

One other issue had to be worked out in order to use the MCM-8. The system operates as a client/server. The initial connection has to originate from the MCM-8. Once up, bidirectional communication is possible. Because of this, deployment of a foreign agent service is not possible. Therefore, static collocated care-or-address (CCOA) capability needed to be developed and deployed for the demonstration.

IV. Mobile Network Topology

Figures 3 and 4 show the mobile network topology. The HA router, the binding router and another router offering foreign agent service were located in the USCG facilities in Cleveland, Ohio. They were attached to the open Internet via a commercial DSL circuit with 32 static addresses. The encryptor on the Neah Bay and in the communication closet provided the fail-safe protection.

Note that both the MR and the HA must have valid public addressing on at least one interface (the interface can be a loopback interface or a physical interface). Loopback interfaces are recommended. One caveat: if the MR tunnel endpoints terminate at the physical interfaces and one of those interfaces goes down, any mobile network virtually attached to that interface will go down

If one wishes to access devices attached to the MR from the open Internet, those devices must have public addresses (otherwise they will not be reachable). We attached some hosts to the unprotected mobile LAN during our demonstrations for debug and monitoring purposes.

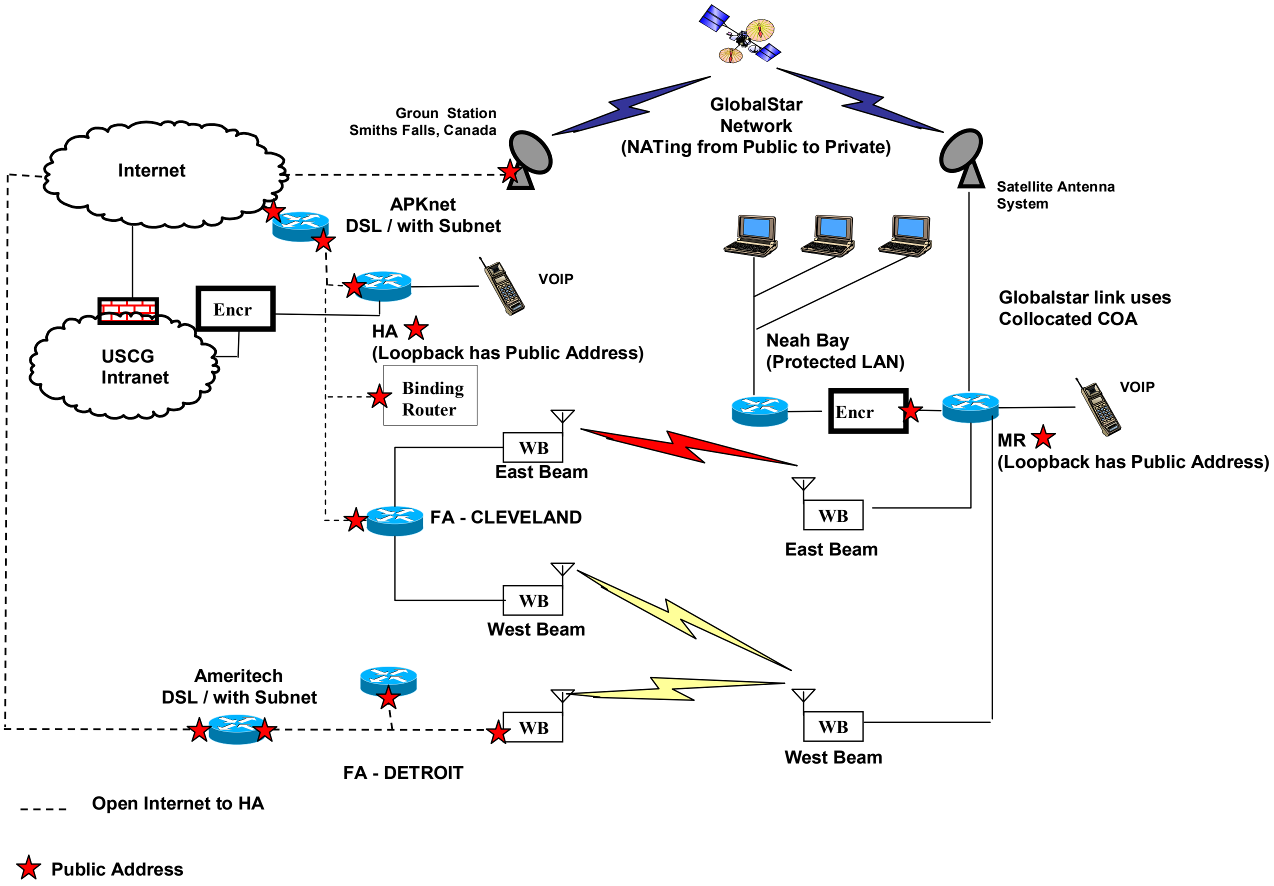


Figure 3. Mobile Network Topology

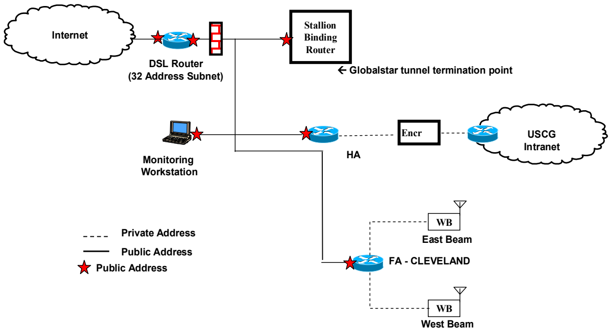


Figure 4. Open Internet

Therefore, the unprotected mobile LAN onboard the Neah Bay was in public address space.

Two 802.11 links were deployed in Cleveland. These links were on two separate networks in order to validate network handovers and preferred path selection. All wireless bridges were configured to use Wired Equivalent Privacy (WEP). This was done to keep unauthorized users from connecting to the wireless system and to protect the routers locally (the type-2 encryptors were already protecting the USCG operational network). Admittedly, WEP offers minimal additional security since current WEP implementations have known flaws and do not provide sufficient protection for USCG operational networks. We chose to use WEP since it was easy to implement, incurred a minimal impact on our mobile network, and was able to deny unsophisticated wireless access.

Reverse tunneling was used between the HA and MR in order to overcome ingress and/or egress filtering. A useful byproduct of reverse tunneling is that one can utilize private address space on the mobile LANs with corresponding private networks reachable via the HA. This is possible, because, with reverse tunneling, all source and destination headers are from the public addresses on the MR and HA. Unfortunately, reverse tunneling precludes triangular routing, the only standardized route optimization in mobile-IPv4.

For added security on the DSL circuit at the Federal Building [Fig. 4] an iptables firewall was added [8]. This firewall only allows traffic between the Detroit FA and HA, between the MCM-8 and Binding Router, or between specific subnetworks and the workstation. The workstation was used to control the routers as well as to monitor traffic using tcpdump [9].

A. *Encryptor Configuration*

The layer-3 encryptors are fail-safe and allow no data to pass unless specified. An encryptor discovery protocol was not running on the encrypted interface to the open Internet, nor was a routing protocol running on the protected LAN interface to the USCG network, so all routes had to be statically configured. In addition, all encryption rules had to be entered manually. With a single encryptor pair this was quite manageable.

Since all traffic onboard the Neah Bay's protected mobile LAN must to pass through the encryptor, it is not necessary for the Neah Bay router to *receive* route information as the route is already known. However, it is necessary to *send* route information from the Neah Bay to the mainland USCG network in order to maintain the existing network or utilize the mobile network (see section V). A static route was placed in the Neah Bay router (on the protected LAN), pointing all traffic to the encryptor box. The encryptor box passed all incoming traffic to the Neah Bay router, encrypted all outgoing traffic, and tunneled encrypted traffic to the HA encryptor via its next hop router, the MR [Fig. 5].

On the HA encryptor, attached to the USCG network in Cleveland, all encrypted traffic was deciphered and forwarded to next hop router on the USCG network. All traffic from the USCG network bound for the Neah Bay was encrypted and tunneled to the Neah Bay encryptor through its next hop router, the HA.

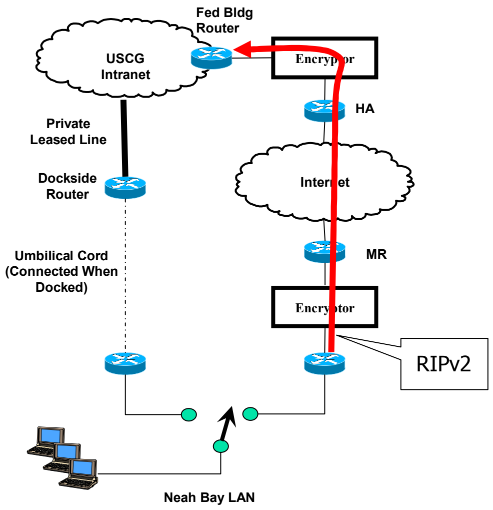


Figure 5. Dual Networks

V. MAINTAINING TWO NETWORKS AUTONOMOUSLY

When operating as a mobile network, all traffic bound to the Neah Bay had to be sent to the encryptor residing between the USCG mainland network and the HA. However, our design requirements were to maintain the existing network or utilize the mobile network without placing a large burden on TISCOM. TISCOM agreed to run RIPv2 in promiscuous mode on the Federal Building router so it could receive routing updates from the Neah Bay mobile LAN Router when using mobile networking. These RIPv2 routes would then be redistributed throughout the USCG network and all traffic destined to the Neah Bay would be forwarded through the encryptor. If one wished to utilize the current USCG network rather than mobile networking, one could simply throw an Ethernet toggle switch onboard the Neah Bay. Once the toggle switch was thrown, the LAN interface to the router on the protected mobile network would go down and that router would stop forwarding route updates. Following this action the USCG router attached to the HA encryptor would time out and cease to advertise the Neah Bay network. Instead, the Neah

Bay network would be advertised as available over the land line router [Fig.5]. This is an elegant solution except layer-3 encryption devices generally do not pass routing information.

Many routing protocols specify that the time-to-live (TTL) field in IPv4 or Hop Limit field in IPv6 be set to one. Since each router decrements the TTL field, this ensures that routing protocols will not be passed beyond the directly attached router. Further, IPSec states that a device acting as a secure gateway should always use tunnel mode for traffic that does not originate from the secure gateway. When tunneling, the inner TTL is decremented once before encapsulation, and is not affected by decapsulation. Thus, when a layer-3 encryption device strictly adheres to the IP Tunneling specification, all protocols that utilize a TTL or Hop Limit of 1 will not pass through the encryptor pair.

To alleviate this problem, Western DataCom modified their firmware to encrypt and pass broadcasts while not decrementing the inner TTL. This allowed RIPv2 to operate in one direction (sufficient for our demonstration). In order to pass broadcasts in both directions, further modification to the encryptor firmware will be required. Some type of source routing is required otherwise one cannot determine which interface the broadcast originated form and which interface to send the broadcast to.

For the particular case illustrated in figure 5, when the MR encryptor receives a broadcast, it encrypts it and forwards it to the HA encryptor. When the HA encryptor receives a broadcast, it simply passes it on to the Federal Building router. Thus, we can run RIPv2 in one direction using the RIPv2 broadcast option.

VI. Validation, Demonstration and Operations

Validations and demonstration of the mobile networking technology were performed in August and November of 2002 and are documented via presentations and video [10, 11]. During these validation exercises the following applications were demonstrated over secure and unsecured links:

- Voice over IP (VOIP)
- Whiteboarding
- FTP, SSH, Telnet
- Microsoft NetMeeting (with and without video)

Applications were run either between the secure LANs on the USCG network or between the unsecure LANs on the MR and HA. All applications running on the unsecure LANs could be viewed by all parties. Only the USCG could view the actual applications running on the secure LANs. Those on the unsecure LAN could only see encrypted packets from the secure network as they passed through the unsecure network.

The results and general feedback from the users indicated that all applications work very well over the 802.11b links. These links were limited to 1 Mbps in order to obtain connectivity up to 20 statute miles. The high bandwidth applications such as NetMeeting video suffered over limited bandwidth links such as the MCM-8 at 56 kbps. VOIP worked well over the MCM-8 as this application only requires approximately 11 kbps. Note that the round trip time delay through the MCM-8 system was 1.5 to 2 seconds, yet all applications performed acceptably with the exception of video (a high bandwidth application).

VII. Tunneling, Fragmentation and Maxmimum Transmission Unit (MTU) Discovery

During initial testing several applications did not operate correctly. Upon further investigation this appeared to be due to fragmentation from the encryption devices, or the MR tunnels, (or both), or someone, somewhere in the network adding a “deny icmp any any access rule” to their firewall. Most operating systems default to path maximum transmission unit (PMTU) discovery which requires icmp unreachables to get back to the server. This problem was alleviated during our tests by modifying the MTU being sent from the hosts. This is not a desirable solution since the MTU settings need to be configured in each host. A more scalable (possible yet untested) solution being investigated is to set the MTU on the Ethernet port of the protected LAN[2]. Thus when a host runs MTU path discovery, it will set its MTU accordingly. Similar MTU settings options should be made available on the encryption boxes.

VIII. Securing the WAN

There are situations were policy dictates that all wireless links be adequately secured. There are many reasons for this. Two in particular are: 1) to ensure that no eavesdropping occurs; and 2) to ensure that the routers do not get compromised. In this situation, the encryptors are placed between the wireless links of the routers [Fig. 6].

During the course of the initial investigations and early field trials mobile-IP was implemented in the secure WAN

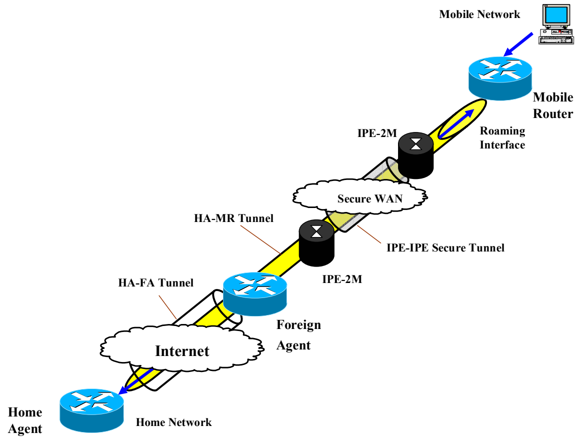


Figure 6. Secure WAN Configuration

[2] This can be accomplished in Cisco routers using the “ip tcp adjust-mss” command which alters all syn packets egressing the interface. This is usually used at the internet edge.

configuration. Mobile-IP would not initially operate properly. Upon detailed investigation it was noted that the TTL field in the mobile-IP agent discovery packets was being decremented from one to zero by the encryptor and then dropped. This is a technically correct operation according to the tunneling specifications. Western DataCom modified their firmware to accommodate mobile-IP by allowing broadcast messages to transition an encryption pair (currently only in one direction). Thus, in this current configuration, only foreign agent advertisements can be utilized and only in the limited broadcast configuration.

An Internet Draft was generated [6] to document that various routing protocols would not operate properly when passing though layer-3 encryption devices. The Internet draft should also aid the NSA which is currently defining its High Assurance Internet Protocol Encryption Specification (HAIPES). This draft describes some issues related to performing encryption at layer-3. In particular, the routing protocol problems that may result if the time-to-live (TTL) field in IPv4 or the Hop Limit field in IPv6 is decremented once before encapsulation. Also, special provisions may be necessary within the encryptor devices if broadcast messages are to transition the encryptor pairs.

IX. OPERATIONAL TEST

From July through September 2003, the Neah Bay was called into duty to escort ships containing strategic cargo, as well as naval ships and submarines in and out of harbors, mainly around New York and Boston [12]. This provided an excellent opportunity for a long term operational test. Of particular interest was the following:

- How much data was transitioning the links?
- What services applications were being used?
- Were their any problems and issues that did not surface during our short duration tests and demonstrations?

We did not want to bias any usage, so no policing of connection time was done initially. The MCM-8 was set to bandwidth-on-demand mode in the hopes of reducing costs. Thus, the crew was allowed to use the network as if connected to a shore-line. Also, no quality-of-service mechanisms were put into place at the Neah Bay or Federal Building routers to prioritize or restrict traffic.

As of the writing of this paper (September 15, 2003), all services are operating well. The main application has been email. Note that once the Neah Bay was 20 miles out of the Cleveland port, 802.11 connections no longer were available; thus, the Neah Bay immediately transitioned to the Globalstar satellite links. Seven of the eight MCM-8 channel modems were operational, providing approximately 50 kbps of bandwidth. Feedback from the Captain and crew is that *mobile networking has completely changed the way the ship operates when underway*.

After approximately 15 days of operation on the satellite, the cost was determined to be too great to continue. The MCM-8 was running approximately 1000 system minutes (7000 phone channel minutes) per day. In effect, the system was always on

To minimize satellite transmission costs, we requested that the Neah Bay use the mobile networking system only in the case of emergency. Additionally, we suggested that they revert to the land-line system when in dock in Boston and New York. Unfortunately, the Neah Bay could not get land-line connectivity in New York harbor, where they spent the majority of their tour. The Neah Bay was allowed to operate an additional 50 hours in September per the negotiated satellite service, 8 channels for 3000 minutes per month.

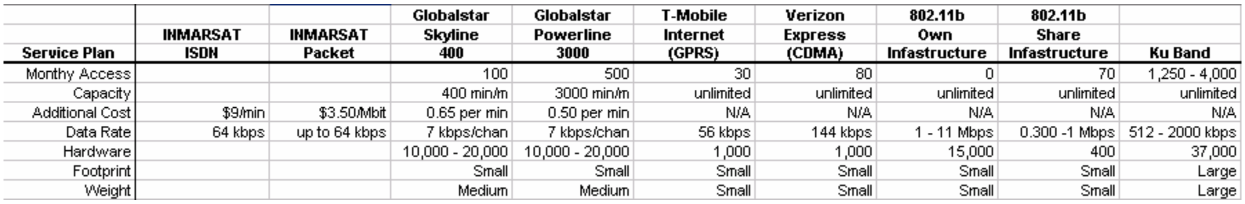
We are currently trying to determine if the system was always on due to actual business transactions such as to email and general E-Coast Guard operations or if the encryptors are sending key updates at a rate sufficient to keep all channels up. We suspect the later may be the case as when the Neah Bay operated for an hour or two a day, the USCG was able to get all of their electronic business completed and all of their emails transmitted – as most of their emails are text-based without large attachments.

X. COST OF CONNECTIVITY

During our initial testing of mobile networking cost of connectivity was not an issue (we owned the 802.11b links). Therefore, once the hardware was paid for, the links were free. The satellite connectivity was only for a period of hours per month when running experiments over the satellite. Note that the MCM-8 system costs approximately US $1.00 per minute to operate at the most favorable rates. Once the contacted minutes are exceeded, the cost becomes US $4.00 per minute. When compared with INMARSAT, these prices are extremely competitive. However, when running a mobile network with full-up, always-on connectivity, the costs quickly become unwieldy

Mobile networking technology is link independent. Thus, there are many possible alternatives and many trade-offs regarding connectivity. For instance, one may not find it acceptable to be connected all the time due to cost. However, one may find it acceptable to be connected most of the time for a fraction of the cost. One may also be willing

Table 1 Cost of Connectivity for Various Technologies and Services



			Globalstar	Globalstar	T-Mobile	Verizon	802.11b	802.11b	
	INMARSAT	INMARSAT	Skyline	Powerline	Internet	Express	Own	Share	
Service Plan	ISDN	Packet	400	3000	(GPRS)	(CDMA)	Infastructure	Infastructure	Ku Band
Monthy Access			100	500	30	80	0	70	1,250 - 4,000
Capacity			400 min/m	3000 min/m	unlimited	unlimited	unlimited	unlimited	unlimited
Additional Cost	$9/min	$3.50/Mbit	0.65 per min	0.50 per min	N/A	N/A	N/A	N/A	N/A
Data Rate	64 kbps	up to 64 kbps	7 kbps/chan	7 kbps/chan	56 kbps	144 kbps	1 - 11 Mbps	0.300 -1 Mbps	512 - 2000 kbps
Hardware			10,000 - 20,000	10,000 - 20,000	1,000	1,000	15,000	400	37,000
Footprint			Small	Small	Small	Small	Small	Small	Large
Weight			Medium	Medium	Small	Small	Small	Small	Large

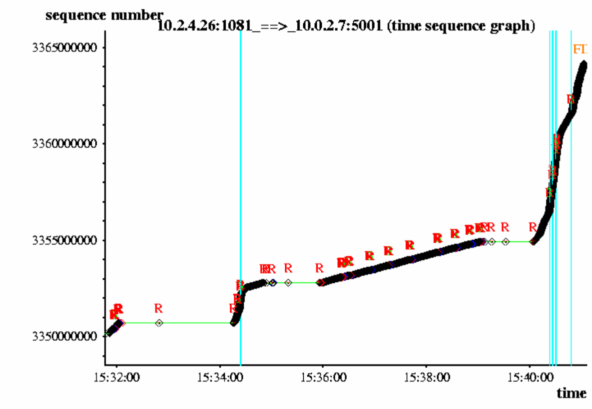


Figure 7. File Transfer in Mobile Network

to deploy new infrastructure or utilize techniques such as store and forward to obtain the necessary communication requirements at an affordable cost.

Phone usage and data usage are two distinctly different applications. One may be willing to self-policy phone usage to remain within contracted minutes. However, this may not be practical with data networks. Also the notion of paying per bit is rather unsettling and difficult to self-police. If one cannot self-police the usage, it will be very difficult to budget for system costs. Thus, the service providers that will be most sought after will be those offering flat-rate pricing – precisely what has happened in the terrestrial ISP market.

Table 1 shows various cost estimates for different wireless technologies. Note that G3 technologies and 802.11 technologies offer very good cost/benefit but may not provide connectivity everywhere. The cost of satellite connectivity, both in hardware and service, is very expensive. Thus the desire to have always-on connectivity must be weighed against those costs.

Figure 7 is a time-sequence plot illustrating a file transfer in a mobile network. This particular network was comprised of two distinct links. One link consisted of an 11 Mbps simplex link with a round trip time of between 20 and 40 milliseconds. This link is representative of a commercial WiFi connection. The second link emulated a "relatively good" mobile satellite link of 128 kbps and a RTT of 550 milliseconds. Notice that the vast majority of the data was transferred over the inexpensive WiFi link. In this example, which may be typical, over 90% of the communications cost would have been spent to transfer less than 10% of the data

"Are you willing to pay for always-on connectivity?"

XI. Share Network Infrastructure

One can deploy mobile routing technology over shared infrastructure thereby increasing robustness of the network while reducing system costs. Figure 8 shows one such example. Here, the USCG, the Canadian Coast Guard, the US Navy, private shipping companies and even pleasure craft could all share the same 802.11 links. Yet, each mobile network can effectively (virtually) reside on their own home network. The challenge for such an architecture is the deployment of scalable and manageable network access systems to authorize and authenticate users. This will be particularly challenging when users wish to utilize multiple Internet Service Providers, but only deploy one set of RF hardware for each link type such as WiFi and G3.

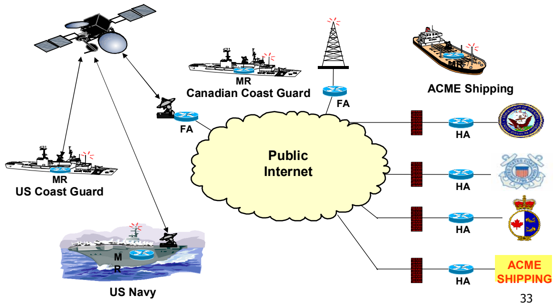


Figure 8. Shared Network Infrastructure

XII. Robust Networks

Mobile routing using mobile-IP provides at least three avenues to improve the robustness of the mobile network. The first is the ability to share network infrastructure. This ensures that hardware will be in constant repair as the hardware will be in continuous use [13]. The second is the ability to use other's networks and various RF links (multi-homing). This provides many opportunities to deploy redundancy across various link types and various service providers. The third is prioritized HA deployment [14]. The MR can be configured to utilize multiple HAs with different priorities. The MR registers with only the highest priority HA. However, an MR may roam to an area where registration with a closer HA is more desirable – geographically distributed home agent. This feature allows an MR to register with the closer HA using the combination of existing HA priority configurations on the MR and care-of address access lists configured on the HA.

If a MR cannot register with its primary HA for whatever reason, it tries the secondary HA. This feature can be used to place HAs in physically distant locations, thereby increasing the robustness of the network. Figure 9 shows an architecture whereby five geographically distant HAs are available for use by the MR – a rather extreme case. If for some reason, HA #1 were to become inaccessible, the MR

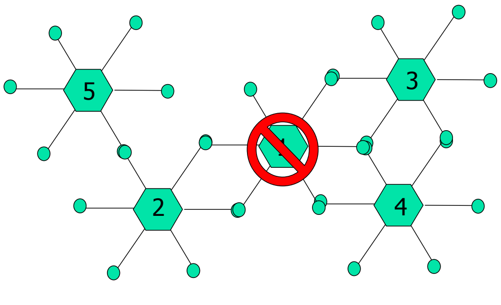


Figure 9. Redundant Physically Disperse Home Agents

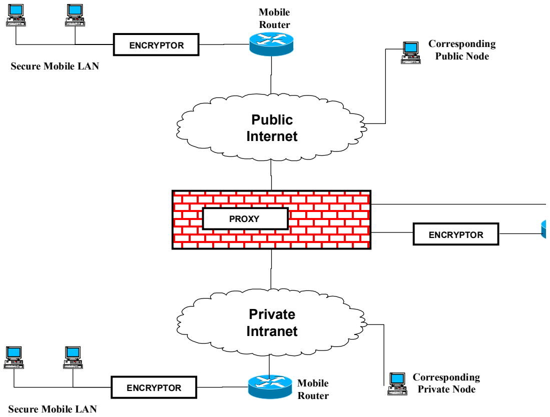


Figure 10. Mixing Private and Public Address Space

would use HA #2 (assuming that HA #2 was next in its priority list) and so on. This capability has many applications for military networks or homeland security [15].

XIII. Future Work

Many problems still need to be solved before wide scale deployment of MR technology will become a reality. NASA continues to work with industry to address these problems and develop scalable, manageable, and deployable solutions. Figure 10 shows an architecture that is being investigated for future operational deployment of mobile networking technology. The movement of a mobile network both inside and outside the firewall is being studied. The MR will be capable of using corporate infrastructure and the Intranet as well as shared open-Internet connectivity. All security policy will be managed at the firewall. Issues that have surfaced to-date and are being addressed include: firewall rules, crossing NATs, configuring of encryption devices, and the interaction of the firewall and proxy with mobile router features.

Mobile networking for IPv6 is still in its infancy. A new IETF working group, the network mobility (NEMO) working group, was formed to specifically address this problem [16]. NASA GRC is actively participating in this group to ensure that the needs of the aeronautics and space communities and the US Government are being considered. In particular NASA is interested in IPv6 deployments for aeronautical applications as Eurocontrol and the US Department of Defense are both moving toward adoption of IPv6 technology in their future systems.

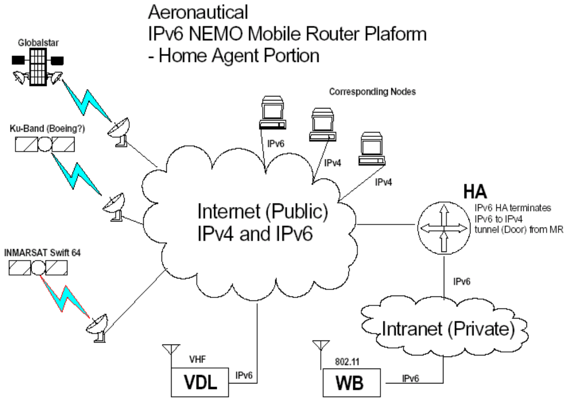


Figure 11. Home Agent Portion of IPv6 Architecture

Figure 11 shows the home agent portion of an architecture that is being investigated for deployment of IPv6 mobile networks across both IPv6 and IPv4 Internets. This architecture is one model for possible deployment of communication networks in the National Airspace System. This architecture also enables testing of migration strategies when moving from IPv4 to IPv6 deployments.

XIV. Summary

Mobile networking using IPv4 technology has been deployed for experimental use in an operational setting onboard the USCG Cutter Neah Bay. The deployment and demonstrations were successful and have provided practical information regarding securing mobile networks and possible full scale architectures. Problems related to mixing public and private address space, deployment of prioritized home agents, operating over public services such as G2, G3 and WiFi wireless, authentication and authorization, proxies and firewalls continue to be investigated. Future work includes deployment of IPv6 mobile networks over IPv4 and IPv6 Internets and application of mobile networking to the National Air Space communication system.

XV. Acknowledgments

The authors would like to thank the USCG for their support and in particular: the Captain and Crew of the Neah Bay, the many members of the 9th District Electronic Systems Division, and the Telecommunication Information Systems Command.

Figure 12. Neah Bay

XVI. REFERENCES

[1] C. Perkins, RFC 3344 August 2002

[2] W. Ivancic, “Architecture Study of Space-Based Satellite Networks for NASA Missions,” IEEE Aerospace Conference 2003, Big Sky, Montana, March 2003

[3] W. Ivancic, D. Stewart, T. Bell, D. Shell, K. Leung, B. Katchmar, “Application of Mobile-IP to Space and Aeronautical Networks,” IEEE Aerospace Conference 2001, Big Sky, Montana, March 2001

[4] W. Ivancic, D. Stewart, T. Bell, K. Leung, D. Shell, B. Kachmar, “Mobile Router Technology Development,” Fourth ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems, July 2001

[5] http://www.western-data.com/ipe2m.htm

[6] W. Ivancic, D. Stewart, “draft-ivancic-layer3-encryptors-00,” August 2003 work in progress

[7] W. Ivancic, D. Stewart, K. Edgein, V. Pansera, T. Bell, D. Shell, C. Miller, “Mobile Routing 802.11b Antenna Connectivity Tests – November 19, 2001,” NASA TM-2002-211511, June 2002

[8] http://www.netfilter.org/, August 2003

[9] http://www.tcpdump.org/, August 2003

[10] roland.grc.nasa.gov/~ivancic/secure_mobile_networks/smn.html, August 2003

[11] P. Paulsen, W. Ivancic, D. Stewart, T. Bell, “Mobile IP Networking – Secure Network Connectivity,” DVD, DFC-417, March 2003

[12] “Cutter en route to East Coast to protect ships,” Cleveland Plain Dealer, July 23, 2003

[13] W. Ivancic , “Mobile Networking White Paper,” March 2002 roland.grc.nasa.gov/~ivancic/papers_presentations/Mobile_Networking_White_Paper.pdf

[14] Cisco Mobile Networks—Priority HA Assignment, Cisco IOS Release 12.2(15)T, August 2003

[15] W. Ivancic, D. Stewart, T. Bell, D. Shell, “Use and Deployment of Mobile-IP Priority Home Agents for Aeronautics, Space Operations and Military Applications,” to be published IEEE Aerospace Conference 2004, March 2004

[16] http://www.ietf.org/html.charters/nemo-charter.html, August 2003