

SINEMO: An IP-diversity based Approach for Network Mobility in Space *

Pulak K Chowdhury,
Mohammed Atiquzzaman
School of Computer Science
University of Oklahoma
Norman, OK 73019-6151
{pulak, atiq}@ou.edu

William Ivancic
Satellite Networks & Architectures Branch
NASA Glenn Research Center
21000 Brookpark Rd. MS 54-8
Cleveland, OH 44135
wivancic@grc.nasa.gov

Abstract

IETF proposed Network Mobility (NEMO) Basic Support Protocol (BSP) to support network mobility. NEMO BSP is an extension of Mobile IP v6 (MIPv6), and inherits all the drawbacks of MIPv6 (like inefficient routing, high handover latency and packet loss rate). Satellites equipped with several IP-enabled devices is an example of network mobility in space networks. In this paper, we propose an IP-diversity based network mobility architecture called SINEMO, and show that SINEMO can exhibit better performance than NEMO BSP in satellite IP networks.

1. Introduction

Internet connectivity of mobile hosts has been studied extensively for the last few years. We are currently witnessing the emergence of mobile networks where a set of IP-enabled mobile hosts move collectively as a unit. A Low Earth Orbiting (LEO) satellite with on-board IP-enabled devices, such as telescopes, computers, etc., can be considered as a mobile network handing off between ground stations.

To reduce costs, future space communications will be based on commercial off-the-shelf Internet technology [2]. National Aeronautics and Space Administration (NASA) [14] [9] is, therefore, experimenting with Network Mobility (NEMO) Basic Support Protocol (BSP) [3], a network mobility protocol being developed by the Internet Engineering Task Force (IETF) to support network handovers. NEMO BSP [3] is an extension of Mobile IPv6 and allows all nodes in the mobile network to continue ongoing connection while the network moves.

In the NEMO BSP architecture, a Mobile Router (MR) takes care of handing over all the nodes in a mobile network

between home and visiting networks. The MR, a piece of software that resides in a network router, allows an entire network to roam; thus a device connected to the MR is unaware of mobility [3]. The operation of NEMO BSP is almost similar to that of Mobile IPv6 [11] for a single host with a few exceptions like double tunnel setup and different Home Agent(HA) update of MR.

NEMO BSP is based on Mobile IPv6 and thus inherits all the drawbacks of Mobile IPv6. In NEMO BSP, all the packets should be routed through the HA of the mobile router. Thus, when the mobile network moves further away from the HA of the mobile router, all the packets should follow a far, inefficient routing path [3]. Packet overhead also increases for encapsulating packet twice. During handover, the MR has to acquire its new care of address in the foreign network and register the new address with its HA which increases handover latency due to multiple level of indirection; incurring packet loss during handover period [3]. A number of proposal to improve performance of NEMO BSP have been introduced in the literature. Perera et al. [16] discuss different implementation designs and issues for network mobility, including NEMO BSP. Kim et al. [12] proposed route optimization to reduce latency and Ryu et al. [18] proposed improved handover technique for NEMO BSP. A secured, spoofing-proof extension of NEMO BSP is proposed by Kim and Chae [13]. But none of these proposals completely address the drawbacks regarding NEMO BSP [5].

To address these drawbacks of NEMO BSP, we propose an IP diversity-based network mobility management called Seamless IP diversity based Network Mobility (SINEMO). To handle the mobility of a single mobile host in IP networks, an IP-diversity based mobility management scheme, named as SIGMA (Seamless IP diversity based Mobility Management Architecture) [7] has been developed through collaborative efforts of NASA and University of Oklahoma. SIGMA exhibits low handover latency and packet loss rate during satellite handover [8].

*The research reported in this paper was funded by NASA Grant NAG3-2922.

SINEMO is an extension of SIGMA for mobile networks. The basic idea of SINEMO is to exploit IP diversity to keep the old path alive during the process of setting up the new path, thus achieving seamless handover of satellites between adjacent ground stations. IP diversity refers to having multiple IP addresses in a node. In addition to seamless handover, SINEMO has a number of advantages such as easier deployment in the Internet infrastructure, cooperation with Internet security protocols, and efficient utilization of network bandwidth. The *objective* of this paper is to propose a new architecture called SINEMO and compare it with NEMO BSP.

SINEMO's design incorporates a number of desirable features for mobile networks. The defining characteristic of network mobility is the notion of a set of nodes moving as a unit. The mobile network may contain both "mobility aware" and "mobility unaware" or fixed nodes. Mobility aware nodes can perform link layer handover inside the network; thus exhibiting nested mobility. SINEMO provides complete transparency of network mobility to the nodes in the mobile network. In SINEMO, the utilization of the wireless links is efficient, i.e., the majority of the bandwidth is dedicated to user data (i.e. minimum signalling).

NASA has already proposed to use mobile router and NEMO BSP in their aeronautics programs including AAAT, WINCOMM and SATS [14]. SINEMO can suffice the space communication goals of these programs using IP diversity. Our *contributions* in this paper are to develop IP-diversity based network mobility scheme, SINEMO, and show by comparison with NEMO BSP that SINEMO can improve the performance of network mobility IP based protocols in satellite networks.

The rest of the paper is organized as follows: Sec. 2 gives a brief overview of SIGMA handover. In Sec. 3, we illustrate the architecture of NEMO BSP. Sec. 4 describes the SINEMO architecture and signalling timeline. Sec. 5 compares the architectural features SINEMO with NEMO BSP. Finally, Sec. 6 includes the concluding remarks.

2. SIGMA Architecture

In this section, we give a brief description of SIGMA handover procedure in LEO satellite networks. Details can be found in [8].

A typical satellite handover in SIGMA (using SCTP as the transport protocol) is shown in Fig. 1, where the Mobile Host (MH) is a multi-homed satellite connected with the Internet through two ground stations. Correspondent node (CN) is a single-homed node sending traffic to MH, which corresponds to the services like file downloading or web browsing by mobile users. The handover process of SIGMA can be described by the following five steps [7].

STEP 1: Obtain new IP address

Refer to Figure 1 as an example, the handover preparation procedure begins when the satellite moves into the overlapping radio coverage area of two adjacent ground stations. Once the satellite receives the router advertisement from the new access router (AR2), it should begin to obtain a new IP address (IP2 in Fig. 1).

STEP 2: Add IP addresses into the association

After the satellite obtained the IP address IP2 by STEP 1, it notifies CN about the availability of the new IP address through SCTP Address Dynamic Reconfiguration option [19].

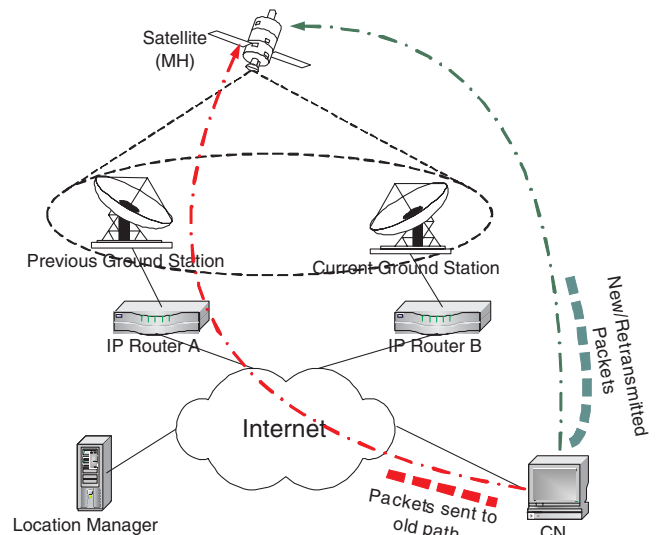


Figure 1. An SCTP association with a multi-homed satellite.

STEP 3: Redirect data packets to new IP address

When the satellite moves further into the coverage area of ground station 2, CN can redirect data traffic to new IP address IP2 to increase the possibility that data can be delivered successfully to the satellite.

STEP 4: Update location manager (LM)

SIGMA supports location management by employing a location manager which maintains a database recording the correspondence between MH's identity and MH's current primary IP address. MH can use any unique information as its identity such as home address like MIP, or domain name, or a public key defined in Public Key Infrastructure (PKI).

STEP 5: Delete or deactivate obsolete IP address

When the satellite moves out of the coverage of ground station 1, no new or retransmitted data should be directed to address IP1. In SIGMA, the satellite notifies CN that IP1 is out of service for data transmission, and CN then deletes the IP address. A less aggressive way to prevent CN from sending data to IP1 is MH advertising a zero receiver win-

dow (corresponding to IP1) to CN. This will give CN an impression that the interface (on which IP1 is bound) buffer is full and can not receive any more data. By deactivating, instead of deleting the IP address, SIGMA can adapt more gracefully to MHs zigzag (often referred to as ping pong) movement patterns.

3. NEMO BSP Architecture

The Mobile Router (MR) in NEMO BSP [3] takes care of all the nodes in the Mobile Network (MN) by ensuring continuous connectivity of all the nodes inside the MN even as the MR moves and changes its point of attachment to the Internet. A Mobile Router (MR) has its unique IP address and has one or more prefixes that it advertises to the nodes in the MN attached to it. MR provides complete transparency of network mobility to the nodes inside the MN, i.e., the nodes inside the mobile network are unaware of network mobility. NEMO BSP also supports nested mobility where a mobile network can contain multiple and nested subnets. Fig. 2 shows a NEMO BSP operational scenario.

When MR moves away from its home network and changes its point of attachment, it configures a new care-of-address from the visited network and sends a binding update to its HA. On receipt of the binding update by the HA, it creates a cache entry which binds the MR's home address with its care-of-address. When a CN sends data to a node in the MN, it is routed to the HA of MR. The HA of MR looks at its cache entry and forwards the packet to the MR using a bi-directional tunnel. The bidirectional tunnel between MR and its Home Agent (HA) is used to pass all traffic between the mobile network nodes and the CNs.

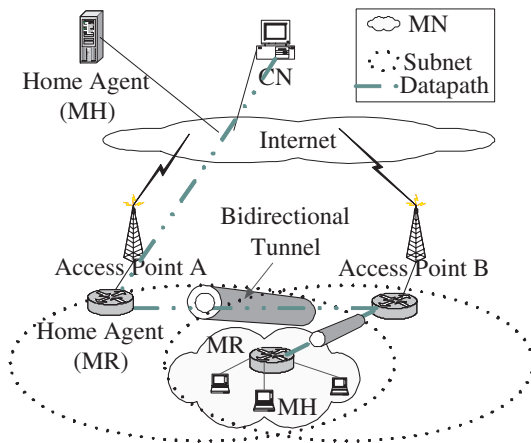


Figure 2. NEMO BSP architecture.

In NEMO BSP, two tunnels are established instead of one - one between the Home Agent (HA) and the point of

attachment (Access Point B in Fig. 2) of the MR in the foreign network and the other between the point of attachment and the MR [3]. The HA of MR encapsulates the packets twice which are destined for any nodes in the mobile network and forwards them to the FA. Access Point B performs one decapsulation and tunnels the packets to the MR. The MR performs the second decapsulation and forwards the packets to the node in the mobile network.

4. SINEMO Architecture

Fig. 3 depicts a typical SINEMO operational scenario of a mobile networks (like bus, train, satellite, etc.) equipped with several IP enabled devices where the onboard multi-homed mobile router is connected through two wireless access networks. Correspondent node (CN) is a single-homed node sending traffic (for services like file or image downloading etc) to one host inside the Mobile Network (MN).

SINEMO can be used with any transport layer protocol that supports IP diversity. For illustration purposes, we use SCTP (Stream Control Transmission Protocol) which supports IP-diversity, as our underlying transport layer protocol. Multihoming is a built-in feature of SCTP, which is convenient to introduce IP diversity in mobile computing environments.

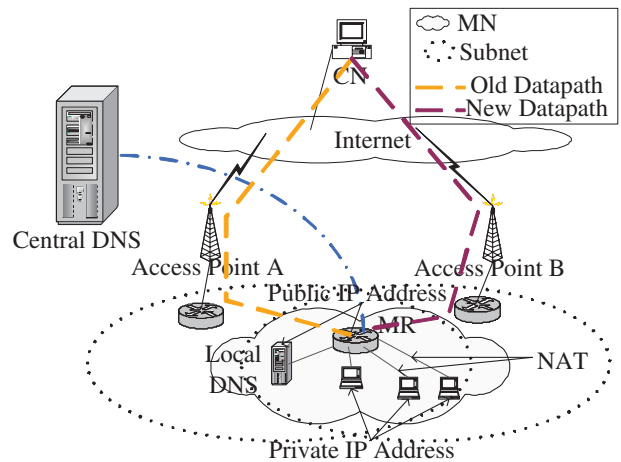


Figure 3. SINEMO architecture.

The MR in the mobile network acts as a gateway between all the hosts inside the MN and the Internet. The MR obtains an IP address from the current Access Point A when the MN moves into the coverage of that access point. It is also delegated one or more prefixes to allocate IP addresses to the hosts within the MN. These hosts consists of both Fixed Hosts (FH) and Mobile Host (MH). Each host inside the MN has both public and private IP addresses. The MR

provides each host with a private IP address from a predefined private IP address space. The MR contains a one-to-one mapping between the public and private IP address of each host. The hosts are not aware of their public IP addresses; MR manages this address space on behalf of the hosts. The MR thus hides the mobility from the hosts inside the network.

The MR uses Network Address Translator (NAT) to translate between the host's private address and a public (globally reachable) address delegated by the access point. A NAT mechanism is implemented in MR to swap the IP addresses in the network and transport headers of the packets [4]. This strategy provides efficient routing support and, most importantly, has the advantage of reducing signalling across air interface [5], as the hosts will not generate any dynamic DNS updates or binding updates while the MN moves.

When CN wants to send data to a host inside the MN, it gets the public IP address of the host and send data directly to the host. The MR intercepts the data packets, translates the IP addresses, and forwards the packets to the hosts.

4.1. Handover Management

When the MN moves into the overlapping radio coverage area of two adjacent access points (AP), the handover preparation begins. Once the MR receives the advertisement from the new Access Point B (Fig. 3), it obtains a new IP address and one or more new IP address prefixes for the hosts inside the MN.

As the MR has two interfaces, it can receive data using its old IP address while using the other interface for registering with the new AP and getting new address prefixes. After registration, it updates the public to private address mapping of the hosts with the new address prefixes. The MR also updates all the CNs which are communicating with the hosts in the MN. After the update, CNs can start sending data to the hosts inside the MN using the new IP addresses. When MR moves out of the coverage of Access Point A, it detaches its interface from that access point. Unlike NEMO, in our scheme, the MR can receive data packets using the old interface during the handover period; this reduces handover data losses.

A MN having more than one subnet inside the MN required multiple access points within the MN. MHs crossing subnets within a MN results in handover. The handover of MHs within the MN is similar to a MN handing over between the MR's access points.

4.2. Location Management

SINEMO requires a location manager which is not restricted to the same subnet as MR's home network (in fact,

SINEMO has no concept of home or foreign network). If we use domain name as host identity, we can merge the Location Manager (LM) functionality into a DNS server. The idea of using a DNS server to locate mobile users can be traced back to [1], and performance analysis of DNS as LM can found in the works of Reaz et al. [17]. This will make the deployment of SINEMO much more flexible than NEMO. Compared to NEMO's requirement that each subnet must have a location management entity (HA), SINEMO can significantly reduce system complexity and operating cost by not having such a requirement. SINEMO uses hierarchical location management for locating a host inside a mobile network.

When a host first enters a mobile network, it registers with the local DNS server associated with the mobile network and obtains a temporary name [17]. This local DNS server in the MN is co-located with the MR. It creates an entry for this host with a mapping between the temporary name and a public address. The MR delegates a private IP address to the host. To forward packets, the MR also creates a mapping between the public and private IP addresses of the host. After registration of the name, the host sends name updates to the central DNS server. When CN sends a query for the IP address of a host in the mobile network, the central DNS server forwards the query to the local DNS server inside the MN. The local DNS server responds with the public address of the host. After obtaining the IP address, the CN can start communication with the host in the MN. This approach makes use of new dynamic DNS low latency secure updates developed by IETF [20].

If an MH crosses subnet within MN (in case of nested mobility), it updates the local DNS with the new IP address while the central DNS entry remains unchanged. When the MN changes subnet, SINEMO only updates the IP address of the local DNS in the central DNS server so that central DNS server can forward the query to the local DNS server. This reduces signalling cost across the wireless interface.

4.3. Signalling Timeline

Fig. 4 summarizes the signalling sequences involved in SINEMO, the numbers before the events correspond to the step numbers in Sec. 4. The meaning of each signaling message has been explained in Sec. 4, so we will skip the detailed explanation of Fig. 4. Here, in the signalling diagram, the CN is acting as a server, and the MH inside the MN is a client. It should also be noted that until the old IP is deleted at CN (including the time for handover process of the MN), MH can always receive data packets (not shown in the figure) through MR from old IP in parallel with the exchange of signaling packets.

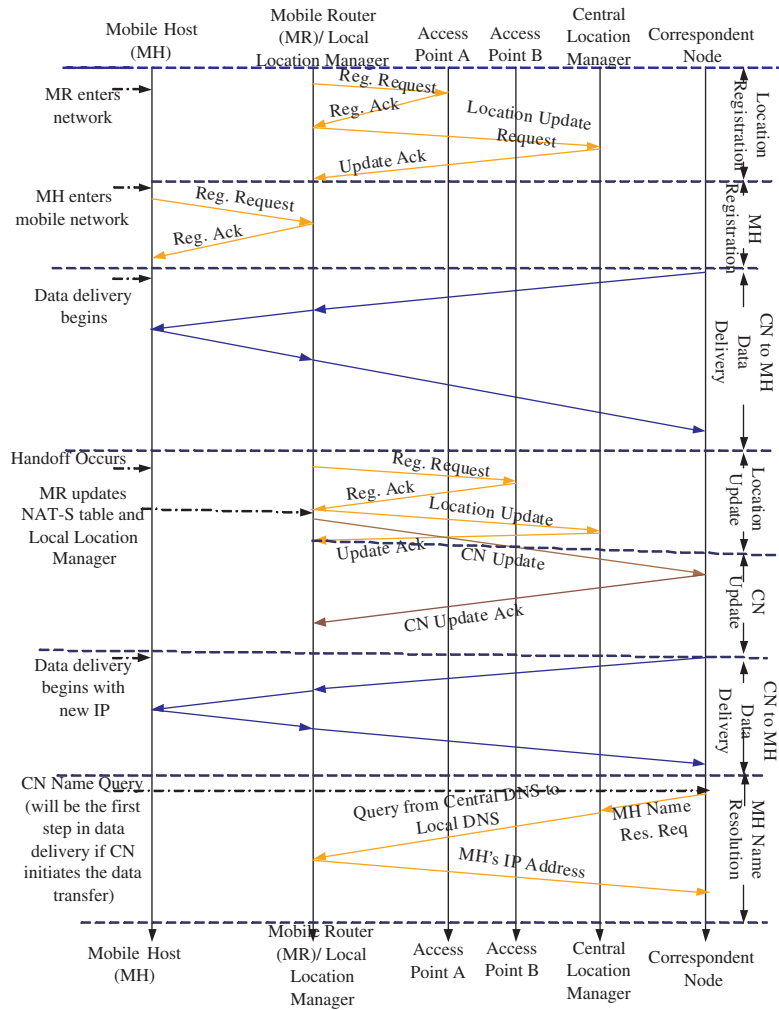


Figure 4. Signalling diagram of SINEMO.

4.4. Deployment of SINEMO in Space Networks

For convenience, we have described the SINEMO operational procedure using MN comprising of mobile computers. SINEMO can however be easily deployed in space networks. A Low Earth Orbit (LEO) Satellite with several onboard IP-enabled devices is a perfect example of a mobile network. NASA, along with Cisco and SSTL, has experimented mobile IP functionalities in space networks with UK-DMC disaster monitoring satellite, which has CLEO (developed by Cisco) router, and several onboard IP-enabled computers [10]. This kind of satellite can be considered as a mobile network, and SINEMO can be effectively used for smooth handover of a network on board a satellite between adjacent ground stations (similar to the access points in Fig. 3).

5. Comparison of NEMO BSP and SINEMO

In this section, we compare the features of NEMO BSP and SINEMO based on a common framework as summarized in Table 1.

- Signalling Cost:** Signalling cost of mobility management for a MN has two major components: signalling cost related to mobility of the MHs within the MN and their corresponding updates within the MN, and the signalling cost related to the movement of the network itself.

Signalling in NEMO BSP takes place when MH moves from the coverage of one subnet to another and has to update its location; when CN wants to send a packet to MH, it has to perform a name lookup at the HA.

SINEMO has similar signalling requirements as

Table 1. Comparison between NEMO BSP and SINEMO

Criteria	NEMO BSP	SINEMO
Signalling Cost	Low	Higher than NEMO BSP for CN updates
Routing	Inefficient	Efficient
Handover Packet Loss Rate	High	Low
Throughput	Low	High
Deployment	Change in existing Internet infrastructure needed	Not needed
Scalability	Home Agent of Mobile Router is the bottleneck	No such single point of failure
Suitability in Space Networks	Suitable	Suitable

NEMO BSP. Additionally, for SINEMO, CNs have to be updated when MH or MR cross subnets. However, hierarchical location management in SINEMO reduces location update cost (signalling cost across air interfaces) when the MN moves.

- Routing:** In NEMO BSP, all packets from the CN to a host inside the mobile network have to be routed through the HA of the MR. The HA of MR only knows the current location of the MN, thus HA intercepts all packets destined for the mobile network, encapsulates them twice, and forwards the packets to the care-of-address of the MR. As the mobile network moves further away from its home subnet, the routing path of the packets destined to the MN increases, as all the packets have to go through the HA of MR. This results in *inefficient* routing of data packets in NEMO BSP.

On the other hand, in SINEMO, the transport connection is end-to-end (from CN to MH). Packets from CN, therefore, do not have to be routed through a specific agent; standard IP routing routes the packets, which consequently renders the routing very *efficient*.

- Handover Packet Loss:** In NEMO BSP, packet loss is caused mainly due to the failure of the old path before the completion of the registration with the new network. As NEMO BSP is based on MIPv6, the communication resumes only after completion of registration. During registration, data packets are queued at HA; the packets are dropped if the queue is full or the packets time out.

In contrast, whenever there is a path available during the handover, SINEMO manages to send data packets through the available path. When the MN is changing subnet, SINEMO sends IP address update messages to all CNs in time. In the ideal case, the CN switches to the new IP address before the old IP address becomes unavailable. Therefore, packet loss is minimized by

using the IP-diversity features of the underlying transport protocol of SINEMO during the handover.

- Throughput:** Throughput refers to the total amount of data that are successfully received at the destination node. Compared to NEMO BSP, SINEMO should achieve much higher overall throughput for the following three reasons: (1) elimination of inefficient routing, (2) less association/session interruption during handover, and (3) reduced packet overhead.

As discussed before, SINEMO reduces the RTT of packets by using efficient routing path, while NEMO BSP routes packets through HA of mobile router, thereby increasing the RTT. During handover, SINEMO minimizes the possibility of session break by employing the multihoming feature of its underlying transport protocol. Specifically, SINEMO switches to the new path (associated with the new IP address) before failure of the old path. Moreover, NEMO BSP packets contain extra overhead arising from two encapsulations in the HA of MR. SINEMO has no such encapsulation which *increases* the end-to-end throughput.

- Deployment Complexity:** NEMO BSP requires data forwarding agents (Home Agent and point of attachment in the visiting network) in the network giving rise to deployment issues. Existing Internet infrastructure should also be changed to accommodate these agents. In contrast, SINEMO does not require any change in the existing Internet infrastructure as there is no concept of home and foreign network in SINEMO, which ultimately makes the deployment of SINEMO less complex than NEMO BSP. SINEMO uses hierarchical location manager, and existing hierarchical DNS system can be easily configured as location manager in SINEMO.
- Scalability Issues:** As mentioned before, in NEMO BSP, all the packets destined for the MN have to go

through the HA of MR. This makes the HA of MR as the single point bottleneck of the whole network. In case of HA failure, no packet will be forwarded to the MN, and the whole NEMO BSP mechanism will fail to work.

On the other hand, there is no such single point of failure in the SINEMO architecture making it more robust and fault tolerant.

- **Suitability in Space Networks:** NASA is using Mobile IP based schemes (MIP and MIPv6) to handle mobility in future space communication networks [15]. NASA has already experimented the functionalities of MIPv6 in space networks using the UK-DMC disaster monitoring satellite which has a CLEO router (developed by Cisco) and several onboard IP-enabled computers [10]. NEMO BSP has been found to be applicable for space networks. Fu et al. [6] showed that SIGMA can be used in space networks to provide smooth handover between spacecrafts. As SINEMO is based on SIGMA, it will also be applicable to space networks.

6. Conclusion

Mobile IPv6-based Basic Support Protocol (BSP) to support NEMO has several limitations that result in high packet loss and delay. SINEMO, our proposed scheme to support NEMO, on the other hand, avoids the inherent limitations of BSP by using IP diversity based handover and DNS as location manager. We conclude that SINEMO can suffice the goals of continuous network connectivity for mobile networks in NASA projects like Global Precipitation Measurement (GPM), Operating Missions as Nodes on the Internet (OMNI), Communication and Navigation Demonstration on Shuttle (CANDOS) mission, and GPM.

References

- [1] B. Awerbuch and D. Peleg. Concurrent online tracking of mobile users. In *ACM SIGCOMM Symposium on Communications, Architectures and Protocols*, pages 221–233, Zurich, Switzerland, 3–6 September 1991.
- [2] K. Bhasin and J. L. Hayden. Space Internet architectures and technologies for NASA enterprises. *International Journal of Satellite Communications*, 20(5):311–332, September/October 2002.
- [3] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Network mobility (NEMO basic support protocol). Internet Draft, RFC 3963, January 2005.
- [4] K. Egevang and P. Francis. The IP Network Address Translator (NAT). IETF RFC 1631, May 1994.
- [5] T. Ernst. Network mobility support goals and requirements. Internet Draft, draft-ietf-nemo-requirements-05, October 2005.
- [6] S. Fu and M. Atiquzzaman. SIGMA: A transport layer mobility management scheme for terrestrial and space networks. book chapter to be published by Kluwer Academic Publishers, 2005. www.cs.ou.edu/~netlab.
- [7] S. Fu, M. Atiquzzaman, L. Ma, and Y. Lee. Signaling cost and performance of SIGMA: A seamless handover scheme for data networks. *Journal of Wireless Communications and Mobile Computing*, 5(7):825–845, November 2005.
- [8] S. Fu, L. Ma, M. Atiquzzaman, and Y. Lee. Architecture and performance of SIGMA: A seamless handover scheme for data networks. In *IEEE ICC*, pages 3249–3253, Seoul, South Korea, 16–20 May 2005.
- [9] W. Ivancic. Secure, network-centric operations of a space-based asset: Cisco router in Low-Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC). Presentation, Net-Centric Operations 2005, Washington, DC, 10–11 May 2005.
- [10] W. Ivancic, P. Paulsen, D. Stewart, D. Shell, L. Wood, C. Jackson, D. Hodgson, J. Northam, N. Bean, E. Miller, M. Graves, and L. Kurisaki. Secure, network-centric operations of a space-based asset: Cisco router in Low-Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC). Technical Report NASA/TM-2005-213556, NASA, Hanover, MD, May 2005.
- [11] D. Johnson, C. Perkins, and J. Arkko. Mobility support in IPv6. IETF RFC 3775, June 2004.
- [12] H. Kim, G. Kim, and C. Kim. S-ro: Simple route optimization scheme with NEMO transparency. *Lecture Notes in Computer Science*, 3391(401–411).
- [13] M. Kim and K. Chae. A fast defense mechanism against IP spoofing traffic in a NEMO environment. *Lecture Notes in Computer Science*, 3391:843–852, January 2005.
- [14] K. Leung, D. Shell, W. Ivancic, D. Stewart, T. Bell, and B. Kachmar. Application of mobile-IP to space and aeronautical networks. In *IEEE Aerospace Conference*, pages 2/1027–33, Piscataway, NJ, USA, 10–17 March 2001.
- [15] K. Leung, D. Shell, W. Ivancic, D. H. Stewart, T. L. Bell, and B. A. Kachmar. Application of mobile-IP to space and aeronautical networks. In *IEEE Aerospace Conference*, pages 1027–33, Big Sky, MT, USA, 10–17 March 2001.
- [16] E. Perera, V. Sivaraman, and A. Seneviratne. Survey on network mobility support. *Mobile Computing and Communications Review*, 8(2):7–19, April 2004.
- [17] A. S. Reaz, M. Atiquzzaman, and S. Fu. Performance of DNS as location manager for wireless systems in IP networks. In *GLOBECOM '05*, pages 359–363, St. Louis, MI, 28 November - 2 December 2005.
- [18] H. Ryu, D. Kim, Y. Cho, K. Lee, and H. Park. Improved handoff scheme for supporting network mobility in nested mobile networks. *Lecture Notes in Computer Science*, 3380:378–387, January 2005.
- [19] R. Stewart, M. Ramalho, and Q. Xie. Stream control transmission protocol (SCTP) dynamic address reconfiguration. Internet Draft, draft-ietf-tsvwg-addip-sctp-08.txt, June 2004.
- [20] P. Vixie, S. Thompson, Y. Rekhter, and J. Bound. Dynamic updates in the domain name system (DNS update). RFC 2136, April 1997.