HYBRID NETWORKS WITH A SPACE SEGMENT - TOPOLOGY DESIGN AND SECURITY ISSUES

by Ayan Roy-Chowdhury, John S. Baras,
Michael Hadjitheodosiou, Nicolas Rentz

CSHCN TR 2005-6
(ISR TR 2005-87)

HYBRID NETWORKS WITH A SPACE SEGMENT - TOPOLOGY DESIGN AND SECURITY ISSUES

Ayan Roy-Chowdhury, Michael Hadjitheodosiou, John S. Baras
Electrical and Computer Engineering
and Institute for Systems Research
University of Maryland
College Park, Maryland 20742
Email: {ayan, michalis, baras}@isr.umd.edu

Nicolas Rentz
INP Grenoble Telecom
38402 St Martin d' Heres Cedex France
Email: nrentz@umd.edu

Abstract— **In this paper we investigate a hybrid network topology that is suitable for supporting interplanetary communications. We define an architecture comprised of a network of sensor nodes on a remote planetary surface, connected to a hybrid terrestrial network of wired and wireless LANs through a series of satellite relays. All the nodes in the network are IP-addressable and support public and symmetric key cryptography. The resulting network forms a hierarchical hybrid mesh that connects users on Earth to networks on or around a remote planetary surface. We describe the design of the network and present preliminary simulation results illustrating the network performance for various parameters. We also discuss how algorithms for user authentication, message integrity and data confidentiality can be incorporated in the network infrastructure for secure end-to-end communication.**

I. Introduction

The new phase of space exploration involves a growing number of human and robotic missions with varying communication and service requirements. These will include continuous, maximum coverage of areas of concentrated activities, such as in the vicinity of in-space planetary outposts, orbiting missions (single spacecraft or constellations) around the Earth, Moon or Mars. These IP-addressable nodes would be connected back to Earth through a broadband backbone and relay infrastructure. This Space Information Highway would serve the dual role of providing virtual presence to space, mission telemetry and control and coordination between missions but also broadband capability to download collected data back to Earth.

Several network topologies that involve a space component have been proposed. Most of the proposed topologies are for scientific interplanetary communication, with satellites acting as relays to connect remote networks on distant planets to networks on Earth. The resulting networks form hierarchical hybrid meshes and present interesting challenges to overcome the constraint of long propagation delay, ensure robustness against fluctuations in satellite channel conditions due to atmospheric changes, and to ensure secure communication between users.

In this paper we consider a lunar exploration scenario, and design the topology to connect networks on the Moon to networks on Earth. The proposed network shares many similarities with terrestrial wireless and sensor network architectures. However, the issues related to performance, robustness and security are different due to the long delay over the inter-satellite links, the limited power of the space nodes, the special hardware required to support functionality in space, and very different conditions on the lunar surface. Therefore solutions that are geared towards terrestrial wireless networks might not be suitable for the interplanetary network we consider. We discuss the important performance and security issues for this network, and the solutions to some important problems.

The rest of this paper is organized as follows. In section II, we describe in detail the network topology we assume. We highlight the important problems for efficient performance in the proposed network in section III. A discussion of the issues for secure communication is in section IV. Section V describes a simulation setup for the proposed network and gives preliminary performance results on the network latency, connectivity (for a specific time window), end-to-end delay, throughput and satellite link utilization for different traffic patterns. We conclude the paper in section VI with a discussion of our current and future research.

II. A Communication Architecture for Supporting Space Exploration

We make certain assumptions about the mission characteristics since the mission requirements are not yet available. We follow a “bottom-up” approach, specifying the network starting with the topology on the lunar surface, and then extending it to Earth. The network on the Earth is more easily defined - either existing scientific networks with extensions to the open Internet, or an overall open architecture.

A. Planetary Surface Network

One of the fundamental components of a lunar network will be a sensor network to collect data about various conditions on the lunar surface. We assume that sensors will be placed in clusters based on their geographical location and radio range proximity to one another. Each group of sensor nodes might have a base station (BS) that aggregates the data collected by the sensor nodes in its range. There might be multiple base stations that can communicate wirelessly with

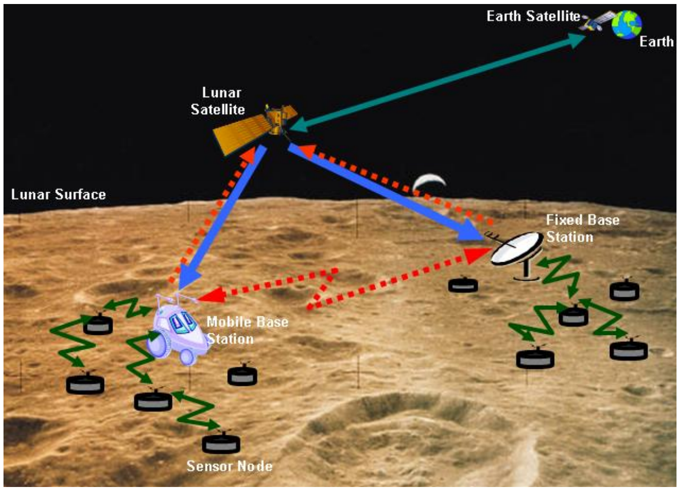


Fig. 1. Proposed sensor network on remote planetary surface

one another. The base stations can also communicate with a mission satellite orbiting the moon. The satellite relays the data collected from the base stations to satellites circling the Earth. We assume that all network components on the remote planetary surface are robotic, i.e., the nodes and base stations are capable of functioning without direct human involvement. The basic functionalities of the nodes are pre-programmed in software and/or hardware embedded in the nodes before they are launched from Earth. However, provisions are made to modify the functionality if necessary at a later time. For such purpose, the network is managed from a dedicated control center on Earth that can send remote commands via satellite uplink. The remote commands may include instructions to the mobile base stations to move to specific locations, or send new functionality requirements to be downloaded to the base stations and/or the sensor nodes. A schematic of the lunar network is given in fig. 1.

1) Sensor Node: The sensor nodes “sense” various physical phenomena on the lunar surface and collect data on the observed phenomena periodically. The collected data is transmitted to the base station at periodic intervals through wireless channels. We assume that the sensor nodes are small in dimension, lightweight, and limited in quantity - ranging in number between a few tens to a few hundreds. We assume that the sensor nodes are stationary, though the network can be extended to include mobile sensors too. Each sensor node has limited processing power and storage, to perform basic sensing applications and store several megabytes of data. The energy of each sensor node is renewable, based on solar sources. An IP address is associated with each node, and each also supports ad hoc routing protocols. A sensor node in a cluster can communicate with other sensor nodes in the subnetwork either directly or through ad hoc communication paths. We assume that the sensor nodes can support security functions. However, due to the limitations on computation power and storage, public-key cryptography is not suitable since it makes heavy demands on computation, energy and space to store keys, for resource constrained devices. Therefore we assume that the sensor nodes support public-key cryptography on a limited scale, primarily for bootstrapping security functions. Otherwise, for all security applications, the sensor nodes support symmetric cryptographic algorithms for encryption, authentication and data integrity, which are much less computation and energy-intensive. The security algorithms are encoded in software and hardware in the sensor nodes, and such functionality is re-configurable by downloading new software from the base stations The important parameters in the function of a sensor node are: lifetime (i.e., energy), maximizing data collection, and maximizing the data transfer.

2) Base Station: The base stations have two primary functions - (a) to collect data observed by the sensor nodes, aggregate the data collected and transmit the data to the orbiting satellite and (b) act as a sensor and collect data itself, which it sends to the orbiting satellite. We assume that the base stations have higher processing power, more storage and higher energy compared to ordinary sensor nodes. Each base station is IP-addressable and supports ad hoc routing protocols. A base station can communicate wirelessly with other base stations either directly or through paths established by ad hoc routing protocols. The wireless channel for $station \leftrightarrow station$ is different from the channel for $basestation \leftrightarrow sensor$ communication and is of a higher bandwidth.

The base stations can be either fixed or mobile. The fixed base stations are mostly similar to fixed satellite gateways. The mobile base stations are robotic vehicles with movement patterns determined by mission control on Earth. A base station may service multiple clusters. Some of the sensor clusters have dedicated base stations. Other clusters are serviced periodically by mobile base stations. Each base station is capable of content caching, and can store data locally, to be transmitted at a later time to the sensor nodes or to the satellite, either based on timers or on remote commands from the control center on Earth. The base stations support both public key cryptographic operations and symmetric cryptographic operations.

3) Lunar Satellite: There could be one or more satellites in elliptic orbit around the moon. For our current design, we assume there is one satellite that collects data from the base stations, and relays the collected data to the satellites around Earth. The coverage of the lunar satellite is concentrated on a particular area of the lunar surface, where the surface network is located. The satellite also relays command and control data from Earth to the base stations, and subsequently downloaded to the sensor nodes as needed.

The lunar satellite supports multiple spot-beams, and has a switch for onboard processing of the data. The satellite can be IP addressable. It is capable of supporting security functionalities for both public key and symmetric cryptography. It is also capable of content caching, and can store data locally.

B. Lunar Satellite to Earth Satellite Connectivity

The lunar satellite is connected to one or more geostationary (GEO) relay satellites orbiting around the Earth. The connection uses directional antennas on the satellites and is characterized by high bandwidth and high delay. A schematic is given in fig. 2. The GEO satellites operate in Ka-band (27-40GHz). Each GEO satellite covers a large geographical area on Earth. Each has an onboard switch and is capable of onboard processing. Each supports multiple spot-beams and can switch data between the different spot-beams (for example,

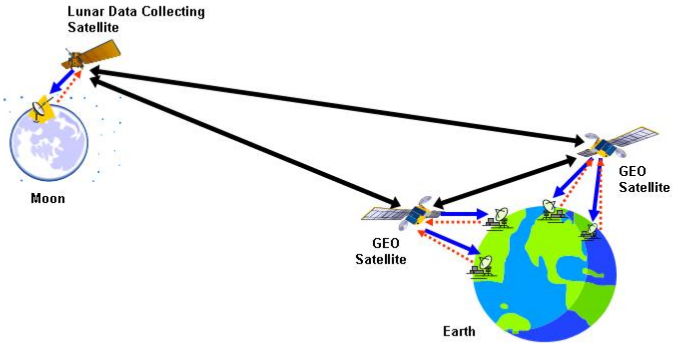


Fig. 2. Interplanetary connectivity with GEO satellite

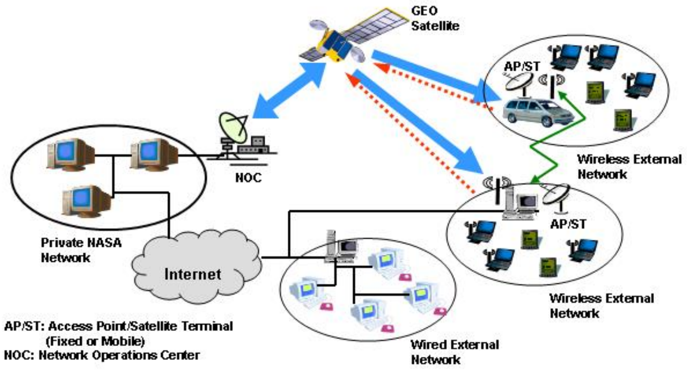

GEO Satellite
AP/ST
Wireless External Network
NOC
Private NASA Network
Internet
AP/ST
Wireless External Network
Wired External Network
AP/ST: Access Point/Satellite Terminal (Fixed or Mobile)
NOC: Network Operations Center

Fig. 3. Interplanetary mission terrestrial network with GEO satellite

[1]). Each GEO satellite also has an associated IP address and can support both public and private key cryptography. We assume that the relay would be the next generation Tracking and Data Relay Satellite (TDRS) system [2].

C. Terrestrial Network

A schematic of the terrestrial network is given in fig. 3. The satellite gateway on Earth is connected to the network operations center (NOC) and the associated private network of the mission operators. The private network is connected to the open Internet through high-speed terrestrial links, with suitable protection by network firewalls. External wired or wireless LANs can receive authorized mission data by connecting via the Internet. We assume that the wireless LANs have one or more access points connected to the Internet. Some wireless LANs (for example, in remote locations) might not have Internet connectivity. The access points in these wireless LANs have satellite connectivity and can therefore connect directly to the satellite. The user nodes in the wireless LANs are typically mobile devices. All the access points and mobile nodes have IP addresses and support ad hoc routing protocols. The user nodes connect to the local access point either directly or via ad hoc routing paths through other mobile nodes in the LAN.

The access points are capable of public key and symmetric key security operations and have no constraints on computation, storage or energy. The user nodes might have limited computation power, storage capacity and energy (for example, PDAs). We assume these nodes are also capable of both public key and symmetric key operations, though to preserve energy and for efficient computation, symmetric cryptographic operations are preferred.

III. Network Constraints on Performance in the Hybrid Space Network

The space communication network proposed in section II suffers from several important limitations due to its unique characteristics. The primary problem is the large propagation delay due to the long physical distances in the network. One-way propagation delay from the terrestrial gateway to a GEO satellite is approximately 125 milliseconds. This delay is large compared to the delay in ground networks, but an even higher delay is the propagation delay between the terrestrial satellites and the lunar satellite. From our simulation studies, the delay is calculated to be approximately 1.5 seconds in one direction. This large delay severely limits the performance efficiency of standard communication protocols. For example, TCP is very delay-sensitive, and it performs very poorly in this environment. Several modifications have been proposed to allow efficient TCP performance in space networks, which are described in [3]. One standard solution employed by the industry today for terrestrial GEO networks is to perform *TCP splitting*, i.e., break the end-to-end TCP connection into multiple connections on each leg of the communication path, with proxy servers at the gateways and user nodes doing the TCP translation [4]. A consequence of the delay is that applications that require immediate reception and action are not possible in this network. Any command message from the Earth should always factor in the finite delay, and the supported applications can be *near-real-time* at best.

Another issue is that the GEO satellite channel in Earth's atmosphere is susceptible to burst errors due to atmospheric conditions, in addition to random bit errors. GEO satellites operating in Ka-band are severely affected by fading due to rain [5]. Efficient feedback and retransmission mechanisms are required to allow data and command messages recover from such errors.

The sensor nodes on the lunar surface have finite energy, even if the energy is renewable. The ad hoc routing path between a sensor node and its base station might not be available if an intermediate sensor node's energy is depleted. Also, the path might go through a sensor node with a critical function (for example, it being the only sensor in a location observing a particular phenomenon). The lifetime of a critical node should be maximized, hence it should be avoided as a routing node if possible. Therefore ad hoc routing protocols in the sensor network should have multiple routes, and the routing parameters should include the "importance" of a sensor node in the network and the amount of energy available to each sensor node [6].

The mobile base station might not reach certain clusters due to various circumstances, and therefore data from the nodes in these clusters cannot be collected in time. Therefore the sensor nodes should have sufficient storage to cache previously collected data for certain time periods beyond the normal collection time, if necessary. Also, contingency measures to collect data from the sensor nodes should be there, if the mobile base station fails.

Due to the movement of the lunar satellite in orbit, it would be out of contact with the surface network for brief periods of time. Likewise, the connectivity between the lunar satellite and the GEO satellites can be interrupted. The network is therefore intermittently connected. The lunar satellite and the base stations should have the ability to do *data caching*.

The primary objective for the space mission is to ensure that communication between the command center on Earth and the planetary surface network is always *available*, and the planetary surface network performs its functions correctly. Therefore, the network should be designed with the following requirements in mind:

- the network should be robust,
- additions/modifications to the functionalities of the network components on the remote planetary surface should be possible after deployment and
- the command and data traffic is secure.

IV. Secure Communication in the Space Network

Only the mission control center on Earth should be able to send messages to the lunar network, and the collected data from the lunar network should be accessible only to mission control (and possibly to other involved scientists in external networks), and no other entity. Therefore suitable security mechanisms should be in place to ensure that (a) the satellites and/or the lunar network do not accept spurious command and control messages from unauthorized entities on Earth, and (b) the data sent by the planetary network is accessible only to authorized entities on Earth. This requires that the nodes in the network be able to authenticate the source of command messages, and verify the integrity of the messages to ensure they are not modified in transit. The traffic should be encrypted end-to-end so that unauthorized entities cannot read anything meaningful from the satellite broadcast. Security is equally important in the terrestrial section of the networks, where it is much easier for unauthorized entities to eavesdrop on the communication, or attempt to send spurious messages or modify the messages in transit.

The authentication, message integrity and encryption algorithms implemented in the network should fine-tuned for the peculiar characteristics of the network. Standard security protocols employed for end-to-end communication in terrestrial networks would fare poorly in the space setting. For example, IPSEC [7], is widely used for encryption, authentication and message integrity for unicast communication in ground networks. But IPSEC encrypts the traffic at the IP layer end-to-end, and this would disable the functionality of the TCP performance enhancing proxy (PEP) servers [8]. It is based on public-key cryptography, therefore the energy required for generating signatures for authentication and message integrity, and the associated computation delay, is quite high for resource-constrained devices like the satellites and sensor nodes. The end-to-end encryption means that intermediate nodes cannot check for spurious messages and discard them. Also, IPSEC or its CCSDS [9] variant SCPS-SP [10], does not allow the base station to transmit simultaneously to multiple sensor nodes in a group setting.

Therefore, the following considerations are important in the implementation of security algorithms for the proposed space network.

- Entity authentication and message integrity for the sensor nodes, the satellites and similar devices with resource constraints should be secure but lightweight. The algorithms should minimize the energy expenditure and the computation latency of the nodes.
- In parallel, public key cryptography can be used for nodes with higher resources. Therefore the end-to-end authentication and message integrity protocols should allow different algorithms to co-exist and inter-operate in different segments of the network.
- Encryption for unicast communication should not disable TCP (or any other higher layer protocol) optimizations. Therefore the end-to-end encryption might need to be broken up into multiple segments in the network so that the proxy servers can read the header data as needed. This requires trusted proxy servers and trusted security gateways to do encryption/decryption operations on the traffic in transit.
- The encryption protocols might be based on public-key cryptography and/or symmetric cryptography in different segments of the network. The different algorithms should co-exist and inter-operate as needed to provide the strongest security possible without penalizing performance.
- Algorithms for secure group communication should be implemented. These algorithms should allow data encryption and also user authentication and message integrity in a group setting. Similar to secure unicast communication, end-to-end security for group communication should allow different protocol optimizations to work correctly, and public-key and symmetric cryptographic algorithms to inter-operate in different segments of the network.

We have proposed an algorithm for authentication and message integrity in resource-constrained devices that is ideally suited for the sensor network in our proposed topology [11]. Named *extended TESLA certificates*, the algorithm is based on authentication using TESLA key hash chains [12] and its extension to a certificate infrastructure [13]. Our algorithm makes use of public-key cryptography on a limited scale to perform initial bootstrapping of the nodes. Authentication and message integrity at the nodes is done using symmetric cryptography-based certificates which are computation and energy-friendly. The algorithm requires a certificate authority with higher capabilities reachable by all the users in the network. In the sensor network, the base stations are ideally suited for this function. The extended TESLA certificate algorithm also allows for authentication and message integrity in group communication, with very low overhead.

To allow TCP and other higher level protocol proxies to function effectively with IPSEC encryption, a layered IPSEC protocol has been proposed [14], [15]. These proposed protocols split the IPSEC encryption into two levels. The header is encrypted at one level, with the keys shared with the proxy servers so that they can decrypt the header information for performance optimization. The data payload is encrypted with a separate key that is known only to the end users. We suggest extending this layered approach for other higher layer protocols, for example, SSL [16], described in [8].

Enabling secure group communication requires that the keys for encryption/decryption be available to all the group members at the same time. The keys are also updated when members join or leave, or refreshed periodically. Several key management protocols for space networks have been proposed [17], [18]. These protocols are mainly suited for dynamic environments where the user set is not constant. In the space network proposed here, group communication for the sensor network does not have this characteristic - the sensor nodes remain constant for the lifetime of the network; the only reason they might leave is if their battery is depleted. However, on the terrestrial portion of the network, the GEO satellites might broadcast the lunar data to multiple gateways on Earth, to be sent to different users. A hierarchical approach to key management is well-suited to this network. We have proposed a hierarchical key management framework for a terrestrial satellite network in [19]. We divide the network into two levels - the lower level comprised of the terrestrial LANs where the users are located, and a higher level consisting of the satellite, the Network Operations Center (NOC), and the satellite gateways (which we term *RPs*) in each LAN, which together form an *overlay* interconnecting the terrestrial LANs. The RPs act as the "bridge" between the two levels.

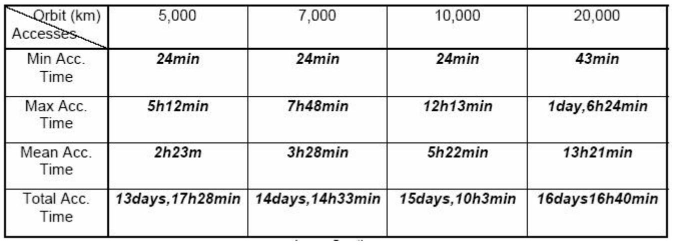
Key management is done separately in the two levels. In each LAN we introduce a local group controller (called the "subnetwork key controller" or SKC) to manage the keys for all groups active in the LAN. The SKC uses the Logical Key Hierarchy (LKH) [20], [21] algorithm to manage keys in its LAN, creating a logical key tree that we term the *SN Tree*. Each group active in a LAN has its own SN Tree.

The overlay has its own key management, also based on the LKH algorithm. At the overlay level, the key management for a particular group is controlled by the satellite gateway/RP (called the *root RP* for that group) of the LAN that has group sources active for the longest continuous period in the group. The logical key tree for any group thus formed at the overlay is termed the *RP Tree*. Each group has its own RP Tree.

Our algorithm therefore builds a hierarchy of logical key trees that closely follow the hierarchy in the network topology. We term the framework, *Tiered Tree-based Key Management*. This framework is extensible to the space network in this paper. The hierarchical approach allows key management with various parameters and cryptographic algorithms in different network segments, with the base stations, satellites and gateways acting as encryption translators in the periphery of the different segments.

V. Network Simulation Description and Preliminary Results

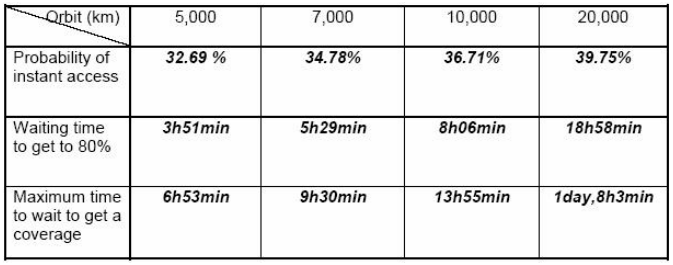
We have modeled the network proposed in section II in the Satellite Tool Kit (STK) 4.3.0 [22] and collected statistics for network access time, coverage and delay by considering four different elliptical orbits for the lunar satellite. Each orbit has a perigee of 300km, while the apogee varies as 5000km, 7000km, 10,000km or 20,000km to highlight the extreme cases. We selected the Sea of Tranquility, close to the lunar equator, for locating the lunar network. The location is on the visible side of the Moon and gives better coverage with the single lunar satellite. On the Earth segment, we consider the three most recent TDRS satellites (TDRS H, TDRS I, TDRS J) and three NASA STDN ground facilities: Guam, Wallops and White Sands. Table I gives the end-to-end access duration for a 43-day time period. The access time is mostly defined by the inter-satellite links. Due to the localization of the moon network, there is no major gap in the lunar satellite⟨−⟩lunar network communication. The effect of the terrestrial ground⟨−⟩GEO satellite links is also negligible.



Orbit (km) Accesses	5,000	7,000	10,000	20,000
Min Acc. Time	***24min***	***24min***	***24min***	***43min***
Max Acc. Time	***5h12min***	***7h48min***	***12h13min***	***1day,6h24min***
Mean Acc. Time	***2h23m***	***3h28min***	***5h22min***	***13h21min***
Total Acc. Time	***13days,17h28min***	***14days,14h33min***	***15days,10h3min***	***16days16h40min***

TABLE I

End-to-end access time for inter-planetary network



Orbit (km)	5,000	7,000	10,000	20,000
Probability of instant access	***32.69 %***	***34.78%***	***36.71%***	***39.75%***
Waiting time to get to 80%	***3h51min***	***5h29min***	***8h06min***	***18h58min***
Maximum time to wait to get a coverage	***6h53min***	***9h30min***	***13h55min***	***1day,8h3min***

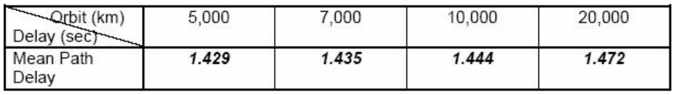
TABLE II

End-to-end coverage time for inter-planetary network

The coverage time of the lunar network is illustrated in table II. Due to the location of the lunar network on the visible side of the Moon, the lunar satellite has simultaneous access to the lunar network and the TDRS satellites.

The mean path delay for the end-to-end communication is illustrated in table III. The delay between the lunar satellite and the TDRS constellation is up to 80 times higher than the delay due to the Moon network⟨−⟩Moon satellite link, and the delay between TDRS and NASA STDN facilities is on the order of 0.13 second. This delay does not include the processing time of the data. We can say that the end-to-end delay is thus dominated by the propagation delay of the Moon to TDRS link.

We validate the results further by the network simulation in Opnet Modeler 11.0 [23].The end-to-end delay, including processing time, for voice applications is shown to be slightly



Orbit (km) Delay (sec)	5,000	7,000	10,000	20,000
Mean Path Delay	***1.429***	***1.435***	***1.444***	***1.472***

TABLE III

End-to-end path delay for inter-planetary network

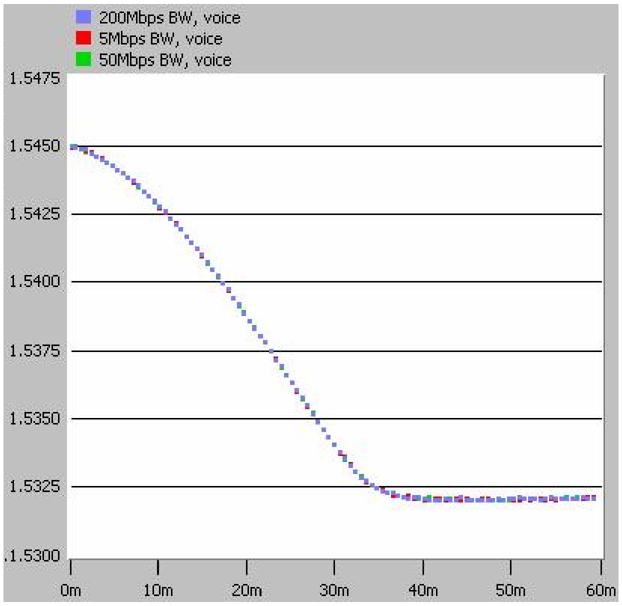


Fig. 4. End-to-end voice application delay (seconds)

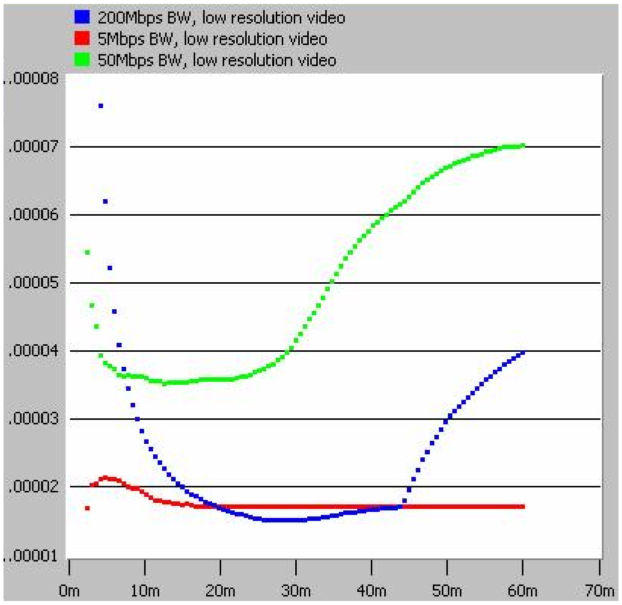


Fig. 5. Video application packet delay variation

over 1.5 second (fig. 4[1]). The delay does not include overhead due to addition of security protocols. Applications implemented for the lunar network should take into account the large delay involved, and this precludes the use of applications that require real-time transfer. Also, security protocols that are designed for the space network ideally should not add to the delay. Therefore, public-key technologies should be avoided if possible, since they incur significant processing delays for resource-constrained nodes, like the sensor nodes we consider for our lunar network. The variation in the packet delay is due to the variation in connectivity as the lunar satellite revolves round the Moon, and the Moon moves around the Earth.

The effect of orbital motion on the delay is more acute on high data-rate applications, as shown by fig. 5, which illustrates the packet delay variation for low resolution (10 frames/second) video application.

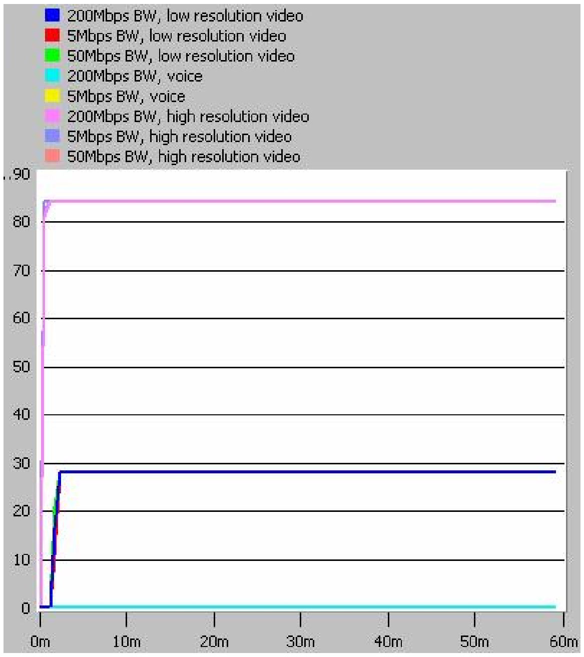


Fig. 6. Satellite link utilization (percentage)

In our Opnet model, we have considered the lunar satellite orbit set to a perigee of 300km, and an apogee of 5000km, and varied the bandwidth in the inter-satellite links between 5Mbps, 50Mbps and 200Mbps. The lunar network comprises a fixed gateway and a mobile gateway, each tending to a cluster of wireless sensor nodes over IEEE802.11 channels. The terrestrial network is a collection of wired and wireless LANs, with the terrestrial gateways located in White Sands and Wallops in the US, and in Guam. The link utilization of a inter-satellite link for the different satellite link bandwidths for data transmission from the lunar network to the Earth, is illustrated in fig. 6. The utilization is related directly to the data rate of the application. For high data-rate video (15 frames/second), the utilization is around 70%, for medium data-rate video (10 frames/second), it falls to around 30%, while the utilization is very low for voice application. We use standard TCP and other protocols in our simulation, without optimizations for the space environment. The results suggest the need to optimize the protocols for space links so that the satellite link utilization is high for various data-rate applications.

The satellite link throughput for different applications is shown in fig. 7. The link throughputs vary with the application data-rate, but is not affected by the link bandwidth. This also suggests the need to design efficient schemes to support different application throughputs over the same link bandwidth, rather than modifying the bandwidth for different data rates.

VI. Conclusion

In this paper we have designed a network architecture for supporting a space exploration to the Moon. We have described

[1] In all the subsequent results figures, the horizontal coordinate is the simulation time in minutes

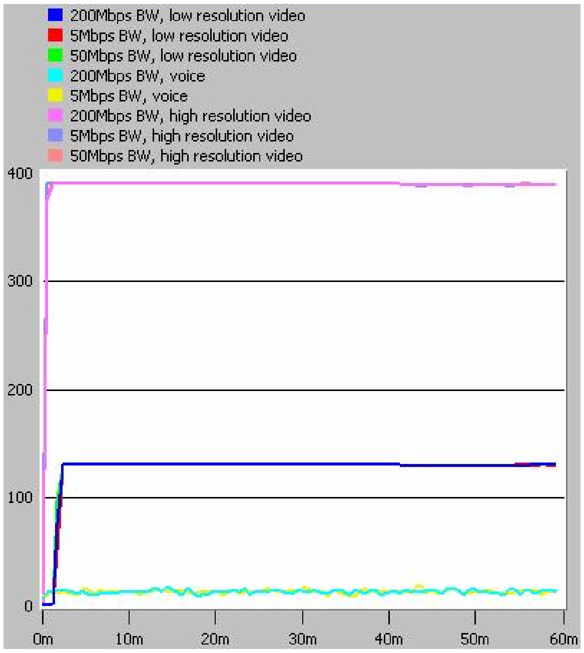


Fig. 7. Satellite link throughput (packets/second)

each segment of the network in detail, and highlighted the important constraints on performance due to the unique characteristics of the network. We have also laid out a case for secure communication in this architecture, and suggested approaches for security without sacrificing performance. Finally, we have validated our architecture through simulations and provided results on various network parameters.

The design of the optimal network for supporting a lunar mission is an open question. We plan to design and analyze various network topologies, and investigate their performance under different traffic conditions. We intend to test modifications to network and transport layer protocols for optimal performance in the space setting. We are also designing security protocols for authentication, message integrity and encryption that are well-suited for the space environment and we intend to validate these protocols through simulations and analysis. Even though much needs to be done, we believe this paper will serve as a useful reference for future research on this topic.

ACKNOWLEDGMENT

The research work reported here is supported by the National Aeronautics and Space Administration (NASA) Marshall Space Flight Center, under award number NCC8-235. The views expressed in this paper are solely the responsibility of the authors and does not reflect the views or position of NASA or any of its components.

REFERENCES

[1] E. J. Fitzpatrick, “”Spaceway System Summary”,” *Space Communications*, no. 13, pp. 7–23, 1995.

[2] “Nasa’s tracking and data relay satellite,” http://www-pao.ksc.nasa.gov/kscpao/nasafact/tdrsmain.htm, December 1992.

[3] P. Chitre, M. Karir, and M. Hadjitheodosiou, “”TCP in the IPSEC environment”,” in *22nd AIAA International Communications Satellite Systems Conference and Exhibit (ICSSC) 2004*. Monterey, California: AIAA, May 2004.

[4] N. Ehsan, M. Liu, and R. Ragland, “”Evaluation of performance enhancing proxies in Internet over satellite”,” *Wiley Int. J. Communication Syst.*, vol. 16, pp. 513–534, August 2003.

[5] F. Gargione, T. Iida, F. Valdoni, and F. Vatalaro, “”Services, Technologies, and Systems at Ka Band and Beyond - A Survey”,” *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 2, February 1999.

[6] Y. Chen and M. Hadjitheodosiou, “”Joint energy management and routing in sensor networks for space exploration”,” in *Proc. 22nd AIAA International Communications Satellite Systems Conference And Exhibit 2004*. Monterey, California: AIAA, May 2004.

[7] R. Atkinson and S. Kent, *”Security Architecture for the Internet Protocol”*, IETF RFC 2401, November 1998.

[8] A. Roy-Chowdhury, J. Baras, M. Hadjitheodosiou, and S. Papademetriou, “”Security issues in hybrid satellite networks”,” *Submitted for publication, IEEE Wireless Communications*, 2005.

[9] “”Implementation Guide for the Use of the Internet Protocol Suite in Space Mission Communications”,” National Aeronautics and Space Administration - Goddard Space Flight Center, Greenbelt, MD, USA, Tech. Rep., September 2003.

[10] “”Space Communications Protocol Specification (SCPS) - Security Protocol (SCPS-SP)”,” National Aeronautics and Space Administration - CCSDS Secretariat, Washington DC, USA, Tech. Rep. CCSDS 713.5-B-1, May 1999.

[11] A. Roy-Chowdhury and J. Baras, “”A certificate-based light-weight authentication algorithm for resource-constrained devices”,” Center for Satellite and Hybrid Communication Networks, University of Maryland College Park, Tech. Rep. CSHCN TR 2005-4, 2005.

[12] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, “”The TESLA Broadcast Authentication Protocol”,” *RSA Cryptobytes*, Summer 2002.

[13] M. Bohge and W. Trappe, “”TESLA certificates: an authentication tool for networks of compute-constrained devices”,” in *Proc. of 6th international symposium on wirless personal multimedia communications (WPMC ’03)*, Yokosuka, Kanagawa, Japan, October 2003.

[14] Y. Zhang, “”A Multilayer IP Security Protocol for TCP Performance Enhancement in Wireless Networks”,” *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 4, pp. 767–776, May 2004.

[15] M. Karir and J. Baras, “”LES: Layered Encryption Security”,” in *Proceedings of the Third International Conference on Networking (ICN’04)*, Guadeloupe, French Caribbean, March 2004.

[16] *”The SSL Protocol Version 3.0”*, IETF Transport Layer Security Working Group, http://wp.netscape.com/eng/ssl3/draft302.txt, November 1996.

[17] L. Duquerroy, S. Josset, O. Alphand, P. Berthou, and T. Gayraud, “”SatIPSec: an optimized solution for securing multicast and unicast satellite transmissions”,” in *22nd AIAA International Communications Satellite Systems Conference and Exhibit 2004*, no. AIAA-2004-3177, Monterey, California, 9-12 May 2004.

[18] M. P. Howarth, S. Iyengar, Z. Sun, and H. Cruickshank, “”Dynamics of Key Management in Secure Satellite Multicast”,” *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 2, pp. 308–319, February 2004.

[19] A. Roy-Chowdhury and J. Baras, “”Key Management for Secure Multicast in Hybrid Satellite Networks”,” in *19th IFIP Information Security Conference (SEC 2004)*, Toulouse, France, August 23-26 2004.

[20] C. Wong, M. Gouda, and S. S. Lam, “”Secure Group Communications using Key Graphs”,” *IEEE/ACM Transactions on Networking*, vol. 8, pp. 16–30, February 2000.

[21] D. Wallner, E. Harder, and R. Agee, *”Key Management for Multicast: Issues and Architectures”*, IETF RFC 2627, http://www.apps.ietf.org/rfc/rfc2627.html, June 1999.

[22] “Satellite tool kit,” http://www.agi.com/products/desktopApp/stkFamily/modules/core/stk/.

[23] “Opnet Modeler,” http://www.opnet.com/products/modeler/home.html.