Modeling and Design of a Communication Architecture Supporting Lunar Exploration

Ayan Roy-Chowdhury*, Michael Hadjitheodosiou† and John S. Baras‡
Center for Satellite and Hybrid Communication Networks, University of Maryland, College Park, MD, 20742, USA

and

Nicolas Rentz§
INP Grenoble Telecom, St Martin d' Heres, Isère, 38402, France

We discuss some basic requirements and trade-offs for designing a communication network supporting the needs of lunar exploration missions. We describe the unique characteristics of this network and outline a prototype network architecture. The proposed network consists of three distinct segments - a terrestrial network on Earth, a network on the lunar surface, and a space segment comprising a satellite constellation that connect the two surface networks.. We develop a simulation platform that includes the network topology, node orbits and mobility, and test the network performance with different applications and traffic loads. We present simulation results obtained with our models that illustrate the network connectivity and delay for varying satellite orbital patterns and traffic characteristics. We also discuss the requirements and constraints for providing a secure infrastructure for end-to-end communication in space exploration networks, and suggest algorithms and protocols for implementing end-to-end encryption, authentication and secure group 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 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 and also broadband capability to download collected data back to Earth.

Several network topologies that involve a space component are possible. 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, and to ensure secure communication between users.

In this paper we present several issues related to designing a communication network for space exploration. We discuss the important requirements for future space missions that influence the design of the communication network. We list some characteristics of the network, and highlight important issues and constraints related to

*Ph.D. student, Electrical and Computer Engineering, University of Maryland College Park, AIAA student member.
†Research Scientist, Institute for Systems Research, University of Maryland College Park, AIAA member.
‡Professor, Electrical and Computer Engineering and Institute for Systems Research, University of Maryland College Park, AIAA member.
§M. S. student, Telecommunications, INP Grenoble Telecom, AIAA student member.

performance, cost, and future network evolution, among others. We also consider a lunar exploration scenario, and design the network architecture to connect a network on the Moon to a network on Earth. The proposed network can be considered a prototype for future missions to the Moon and beyond. This network shares similarities with terrestrial wireless networks 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 simulate the lunar mission network in software and provide a few performance results. We also discuss the security issues for the space exploration networks and suggest algorithms and protocols that can be implemented for ensuring secure communication while maintaining the performance of such networks.

The rest of this paper is organized as follows. In section II we discuss the design requirements and characteristics of space exploration networks. Design and performance tradeoffs associated with the space mission network are discussed in section III. In section IV we describe in detail a lunar mission network topology that we have designed and simulated in software. The simulation setup of the proposed network is given in section V, along with preliminary results for network delay. A discussion of the issues for secure communication for space missions is in section VI, along with suggestions for implementation of security protocols for efficient encryption, authentication and secure group communication. We subsequently conclude the paper with a discussion of our current and future research.

II. Requirements and Space Exploration Network Characteristics

In order to design and analyze the space exploration network, we make certain assumptions about the mission characteristics, since the specific details and requirements for such missions are not determined yet. We define the unique constraints and complexities associated with an inter-planetary space network, and subsequently we try to adapt solutions from comparable space-terrestrial networks, while addressing the specific requirements wherever necessary. In our view, a space network will consist of one or more small clusters of wireless networks on the remote planetary surface, which will be connected by long-distance broadband links to heterogeneous terrestrial networks. Some important design considerations for such a space exploration network include the following.

- The number of missions might grow and any mission might evolve, with varying communication and service requirements. Evolution of a mission would impact the size and/or topology of the network.
- On the remote planetary surface, the areas of concentrated activities would require continuous coverage by the satellites.
- There might be orbiting missions of single spacecraft or constellations.
- The long-distance broadband backbone should have the capability to upload mission telemetry and control data to the remote outposts, and download collected mission data to the command centers on Earth. There might also be the requirement for coordination between different missions using the satellite broadband backbone.
- The space network would consist of both stationary and mobile nodes. In case of the latter, we assume that the mobility would be highly predictable.
- The network backbone should be capable of supporting a wide range of data rates – from a few *kilobits per second* in case of command and telemetry traffic to several *gigabits per second* in case of collected science data downloaded to Earth centers.
- The utilization of the network links would be variable in time – there would be periods of idle time or low keep-alive interchanges, followed by periods of full utilization.
- The link delays would vary from a few milliseconds (for example, in case of surface wired/wireless links) to a few seconds or even minutes (for example, in case of inter-planetary link between Earth and a remote planet).
- The link error characteristics would be different between the wired/wireless links in the surface networks, and the space satellite links, requiring different error correction algorithms.
- The security requirements might be different in different segments of the overall network, and on the different links, which would influence implementation of a heterogeneous set of security algorithms and policies.

III. Design and Performance Trade-offs

Based on the design requirements and characteristics of a space exploration network as discussed in section II, several fundamental issues need to be addressed with respect to the network design and its performance. In particular we are working on five specific related studies focusing on:

- Overlaying communications architecture: packet or circuit switching, Internet/standard protocols like IP or National Aeronautics and Space Administration (NASA)-specific solutions like CCSDS[1], end-to-end optimization of hybrid networks.
- Security: technologies and procedures to ensure the end-to-end secure delivery of information across different links or network subnets.
- Network topology options: investigate different topologies, surface vs. multihop options.
- Relay network options: investigate service coverage and optimization, option of on-board processing/routing satellites, cross links.
- Path redundancy and reliability analysis: investigate performance implications of nodes being lost or unavailable, timing of new path discovery.

A. Link Switching Characteristics

Most space missions to date have used static switching for the transfer of data over the satellite links. The networks used mostly dedicated circuits for the duration of a satellite contact. After a contact with one satellite, the ground terminal required time to point to a different satellite in a different location before signal acquisition and download from that satellite. The ground network did circuit switching but the switching time was dominated by physical antenna slewing (in seconds), not electronic circuit switching (in micro- to milliseconds). Circuit switching satisfied the traffic requirements for these missions, since the traffic was highly predictable and pre-scheduled, so that the satellite link bandwidth could be dedicated to specific traffic sources at different instances in time. This ensured that the link utilization was maximized, and the resource wastage and delay were minimized. However, dynamic mission operation is not possible using this pre-scheduled approach nor are any changes in the topology or size of the network easily accommodated. We envision that the traffic for future missions would be heterogeneous, with less predictability, which is better suited in a packet switching environment. Important design and performance considerations in this case include the following.

1) Bandwidth efficiency: For bursty data traffic or variable traffic services, packet switching would have better bandwidth use. On the other hand, for continuous streams of similar traffic sources (for example, constant bit rate or CBR traffic) with *apriori* allocation, circuit switching would be more useful.
2) Delay performance: Results show that mean delay is better for packet switching under the above traffic assumptions. The variance in delay might be better for circuit switching, but by buffering the traffic, this problem can be alleviated for packet switching (this is important for real-time traffic only). It is to be noted that the large propagation delay over the satellite links (in the order of 1-2 seconds between a lunar satellite and the Earth) would dwarf any other delay component.
3) Network flexibility:
    a. Path redundancy: packet switching is adaptive in discovering new routes if/when a link fails, whereas in the case of circuit switching, links and bandwidth have to be allocated *apriori* for redundant paths to be available.
    b. Link cascading: heterogeneous cascaded links are a problem in circuit switching, since a bottleneck at any link in the end-to-end path would limit the bandwidth utilization of the entire path. Circuit switching would also require that capacity be allocated in advance for all the cascaded links, including the redundant idle links.
    c. Reconfigurability: antennas and physical links are more rigid in the case of circuit switching and therefore it might be more difficult to reconfigure links.
4) Cost and deployment: circuit switching would require a higher amount of hardware, therefore leading to higher expense in deployment. Packet switching, on the other hand, is more adaptive to implementation in software.
5) Quality of service (QoS) support: packet switching-based protocols like IP allow different priorities to be set for different services based on QoS requirements. In the case circuit switching, once bandwidth is allocated, no overwrite of traffic priority is possible.
6) Autonomy support: autonomous, self-configurable networks are a part of the vision for space exploration. This will be difficult to achieve using a circuit-switched dedicated approach.

7) Program Development: NASA's Exploration Systems Mission Directorate's Office of Space Exploration objective is to develop a technology infrastructure that can be adapted and reused in future settings where more flexibility is required. Even if certain limited short term needs of lunar network can be met with other solutions, it will pay to develop an approach that can be scaled up or carried over to future planetary missions.

B. Protocols for space networks

If packet switching is adopted, the next important question is whether to implement commercial protocols like IP, or to go for solutions specific to space networks, such as the ones defined by the Consultative Committee for Space Data Systems (CCSDS). Associated with this issue is the definition of metrics to quantify the performance of the different protocols. If the network design requires that provisions be made for end-to-end communication in the future, where one end node might be in a terrestrial public network, then IP might be useful, since most public networks are IP-based. Use of CCSDS in the satellite links would require implementation of protocol interfaces at the gateways to support the protocol conversion. This could introduce additional cost, computation and power consumption and delay.

C. Power issue

The lunar/remote planetary surface network would include nodes with limited, albeit renewable, energy source. The same holds true for the satellites in orbit. We envision that the planetary network would have a large number of sensor nodes with constrained energy. The design and implementation of the communication network and protocols should take into account this energy limitation – the protocols should not be such that they deplete the node energy before it can be renewed. This consideration is also very important in the design of security algorithms and protocols for the space network, as discussed later in section VI.

IV. A Network Architecture for Space Exploration

In this section we outline a lunar mission network, which can be considered as representative of future inter-planetary missions. We segment the network into three components - a lunar surface network, a “space” component connecting the lunar network to the networks on Earth, and the terrestrial networks. We follow a modular, “bottom-up” approach, by starting with designing the lunar network, optimizing the system components and then focusing on the end-to-end system.

A. Description of the lunar network

The topology of the lunar network is the critical component since it influences the architecture of the space segment. The lunar network specification depends largely on the type of the mission. One mission type would be to have a large single base on the lunar surface (e.g. at the lunar South Pole), from which the network nodes would go out and explore different regions on the Moon. An alternative to that would be to have several small outposts scattered at different geographical positions on the lunar surface, from which explorations of the surrounding regions would take place. In the former case, the coverage area of the satellites in the space component would be concentrated in one small area of the lunar surface; while in the latter case, the satellites would cover a much larger area of the Moon, and possibly the entire lunar surface. The lunar nodes would include both biological nodes (human astronauts), and mechanical nodes (sensors, robotic vehicles, etc.). In our network design, we abstract the astronauts to mobile nodes without any loss of generality. We therefore design the lunar surface network to be comprised of sensor nodes serviced by stationary gateways and mobile robotic vehicles with sensing capability. The sensors are grouped into clusters based on their geographical location and radio range proximity to one another. Each group of sensor nodes would have a

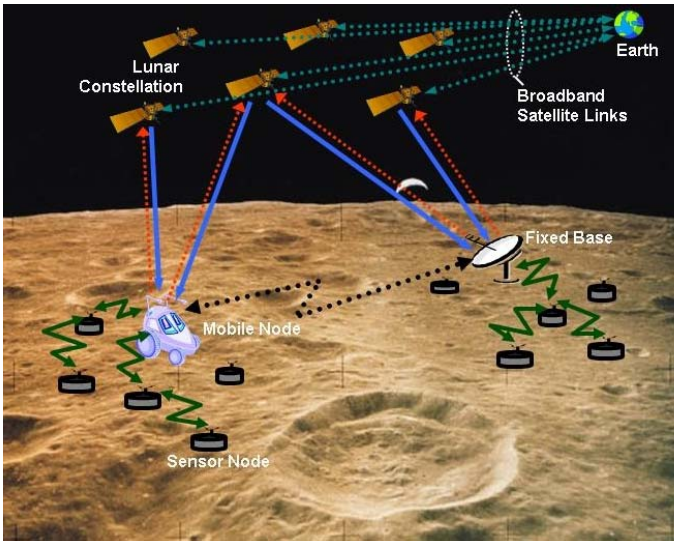

Figure 1. Schematic of lunar surface network.

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 one another. The base stations can also communicate with a lunar satellite constellation orbiting the moon. The satellite constellation relays the data collected from the base stations to networks on Earth. We assume that 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. The network is managed from a dedicated control center on Earth that can send remote commands via satellite uplink. A schematic of the lunar network is given in Fig. 1.

The sensor nodes "sense" various physical phenomena on the lunar surface and collect data on the observed phenomena periodically. They could be anywhere from orbiting nodes around the Moon to probes embedded in the surface sensing seismic conditions. The collected data is transmitted to the base station at periodic intervals through wireless channels. 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. We make the important assumption that the network supports IP protocol in our model, although other types of addressing are possible. Therefore, an IP address is associated with each node, and each also supports ad hoc routing protocols. 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.

Each base station can also act as a sensor and collect data itself, which it sends to the orbiting constellation. 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. 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. 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. The base stations support both public key cryptographic operations and symmetric cryptographic operations.

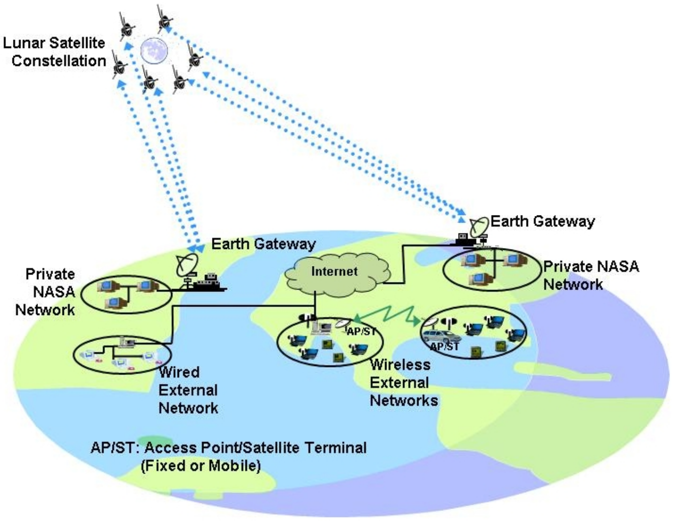
Lunar Satellite Constellation
Earth Gateway
Earth Gateway
Private NASA Network
Internet
Private NASA Network
AP/ST
AP/ST
Wired External Network
Wireless External Networks
AP/ST: Access Point/Satellite Terminal (Fixed or Mobile)

Figure 2. Schematic of the Earth surface network.

B. The space network

Some type of lunar relay constellation is required to relay data from the surface back to Earth. The specific design might depend on science requirements and location of the exploration missions. This could offer total surface continuous coverage or just specific location spot coverage. For an architecture that supports total surface coverage we assume a possible constellation of six satellites in orbit around the moon. The satellites collect data from the base stations, and relay the collected data directly to the gateways on Earth. The satellites also relay command and control data from Earth to the base stations, and subsequently downloaded to the sensor nodes as needed. Each lunar satellite supports multiple spot-beams, and has a switch for onboard processing of the data. Each satellite is associated with an IP address, is capable of supporting security functionalities for both public key and symmetric cryptography and is also capable of content caching.

C. Terrestrial network

A schematic of the terrestrial network that we design is given in Fig. 2. There are multiple satellite gateways on Earth connected to the lunar constellation. The gateways are also 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. 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.

Communication Segment / Delay (sec)	Moon Facility to Satellite	Satellite to Earth	Total
Min Path Delay	**0.025**	**1.147**	**1.172**
Max Path Delay	**0.031**	**1.384**	**1.415**
Mean Path Delay	**0.027**	**1.270**	**1.297**
Max Delay Variation	**0.006**	**0.237**	**0.243**

Figure 4. Propagation delay for polar orbit configuration

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.

D. Constraints of the network architecture

The sensor nodes in the lunar network 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[2].

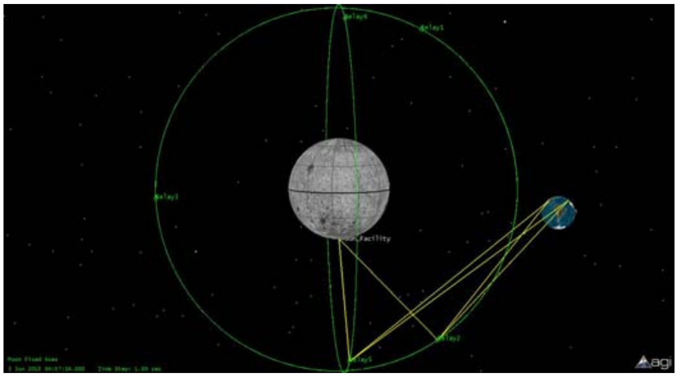

Figure 3. STK model with polar orbit.

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.

Similarly, to avoid data loss in case of interruption in connectivity between the gateways on the lunar network and the satellite constellation, or between the constellation and the terrestrial gateways, both the lunar gateways and the satellites should have the provision for *data caching*.

A critical requirement for the space mission is to ensure that communication between the command center on Earth and the planetary surface network is *always available*, and also that 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.

V. Space Exploration Network Simulation and Results

We have modeled the network described in section IV in the Satellite Tool Kit[3] (STK) version 6.1 and collected statistics for the network delay by considering three different orbit configurations for the lunar satellite constellation. The orbit configurations are polar, elliptical and inclined. The polar orbits have a semi-major axis of 9250km (altitude from lunar surface is 7511.8 km) at an inclination of 90 degrees, with 3 satellites on each of the two orbits

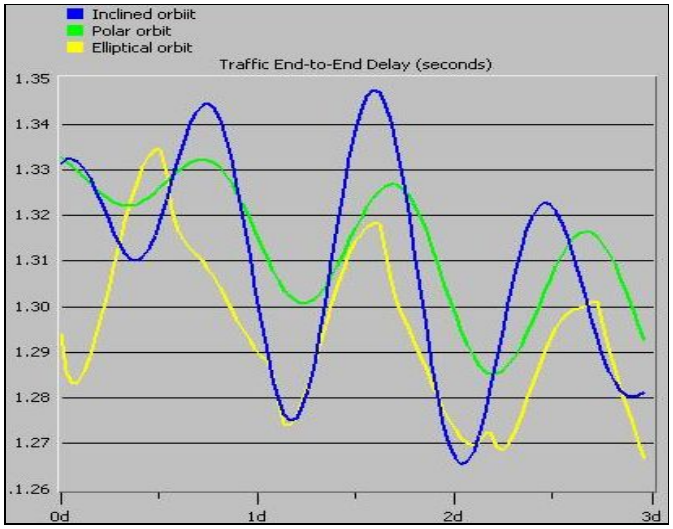

Figure 5. Opnet model: propagation delay without connectivity breaks. *X-axis represents the simulation duration in days; Y-axis represents the delay in seconds.*

(fig. 3). The elliptical orbits are inclined at 56.1 degrees, with semi-major axis of 6541.2km (altitude: 4803km) and eccentricity of 0.6. The lunar surface network for these two configurations is located at the lunar South Pole, which receives full coverage from the constellation in either case. The inclined orbit configuration has semi-major axis of 8050km (altitude: 6311.8km) at an inclination of 52.2 degrees. In this case, the lunar network is located in the Sea of Tranquility, close to the lunar equator to have continuous coverage. In the Earth segment, the gateways are at Guam, Wallops and White Sands in the US, and Madrid. The simulation is made between June 1st, 2015 and December 1, 2015 to get a long-term understanding of the delay. Fig. 4 gives the delay values for the polar orbit configuration. The results are similar for the other orbit configurations.

We have also modeled the network in Opnet Modeler 11.0.A[4]. Fig. 5 gives the end-to-end traffic delay for transmission from a lunar node to the Earth gateway at Guam, for the case when the model does not account for the break in satellite link connectivity due to the movement of the Earth and the Moon with the satellite constellation. The graph suggests that the variation in delay would be the least in case of the polar orbit. Fig. 6 gives the delay figures for the case where the break in connectivity is considered. This is a more realistic scenario that shows that it would be necessary for the satellites (and/or the lunar nodes) to have *store-and-forward* mechanisms so that the traffic can be locally cached when the connectivity breaks, and is transmitted from the local cache when the links are re-established. For the above model, we have considered the satellites to be simple reflectors without any protocol stack. We are also modeling the network topology that has satellites with full IP routing functionality (currently under implementation).

VI. Communication Security for Space Exploration Networks

Security is a major component of any network and in this case is a critical and complex requirement. NASA has recently developed a number of policy decisions for all its missions that have several implications for mission security:

- NASA needs to comply with policies outlined in governing documents like NPD 2810.1C[5].
- Security solutions need to be approved by the US National Institute of Standards and Technology (NIST).
- There is a need to be able to interoperate with commercial networks and international partners while at the same time adhering to the above security requirements.
- The International Space Station and TDRS are NASA legacy systems that need to be included in this infrastructure.

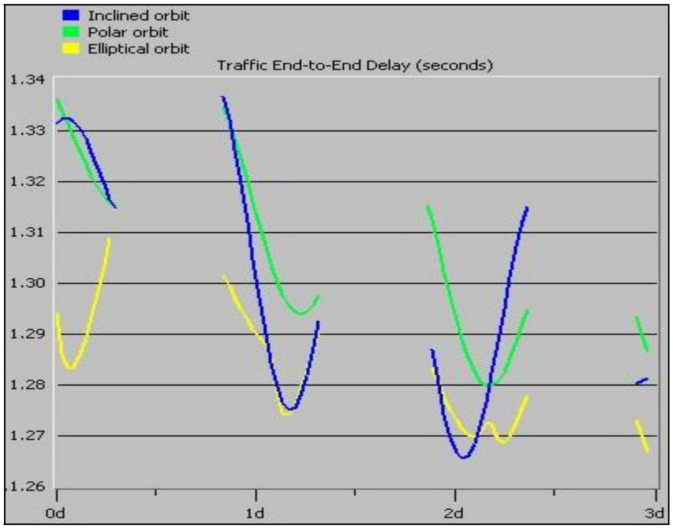

Figure 6. Opnet model: propagation delay with connectivity breaks. *X-axis represents the simulation duration in days; Y-axis represents the delay in seconds.*

It is therefore important to develop for this network security protocols that operate within the constraints of space environment (limited power/computational ability of the nodes). We outline next some basic security procedures and possible approaches that might be relevant.

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 so that unauthorized entities cannot read anything meaningful from the satellite broadcast. An important issue here is whether the encryption should be done end-to-end (source encryption), or whether the encryption should be done separately at different sections on the communication path (link encryption). Source encryption is highly secure, but it creates performance problems by disabling the functionalities of various intermediate servers, as discussed later. Link encryption, on the other hand, requires added functionality in some nodes to decrypt/re-encrypt the traffic.

An important question related to encryption is the type of cryptographic algorithms to use. As stated earlier, NASA policy requires that the security functionalities should be inter-operable with those of international partners who might be contributing to the mission. This creates new complications since due to export-control rules many security algorithms cannot be made available to non-US entities. Therefore algorithms are needed that would could be shared with mission partners while simultaneously maintaining strong security.

The implementation of security algorithms in hardware or software is another important issue. Hardware implementation is arguably more secure, and is traditionally favored by standards bodies like NIST, but it is also inflexible. Software solutions have the advantage that they can be upgraded at a later point in time if necessary. Software is also lighter, and therefore cheaper for deployment.

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 be 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[6] 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[7]. 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 variant SCPS-SP[8], 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.

1) 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.
2) 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.
3) 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.
4) 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.
5) 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[9]. Named *extended TESLA certificates*, the algorithm is based on authentication using TESLA key hash chains[10] and its extension to a certificate infrastructure[11]. 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 algorithm can be implemented also in a hierarchical manner, with one infrastructure at the level of the sensor nodes, and a second infrastructure at a higher level involving the base stations and the satellite constellation. 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[12,13]. 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[14], described in Ref. 7.

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[15,16]. 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 the lunar satellites would transmit 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 Ref. 17. 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 Centers (NOC), and the satellite gateways, which together form an *overlay* interconnecting the terrestrial LANs. The gateways act as the “bridge” between the two levels. Key management is done separately in the two levels, using the Logical Key Hierarchy (LKH)[18,19] algorithm. 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 described 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.

VII. Conclusion

In this paper we have treated the topic of a future space exploration mission. We have discussed the communication requirements for such a mission, highlighted some important issues related to the design of the communication network that are unique to the space environment, and analyzed a few important constraints of the mission. We have also described the design of a prototype network architecture for supporting a space exploration to the Moon, and provided several simulation results. We have also laid out a case for secure communication in this architecture, discussed the unique performance issues in the security context in such networks, and suggested approaches for security without sacrificing performance.

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 work on this topic.

Acknowledgments

Part of this work is supported by the Center for Satellite and Hybrid Communication Networks (CSHCN) under NASA award number NCC8-235. The views expressed in this paper are solely that of the authors and do not reflect the views or positions of NASA.

The authors would like to thank Dan Williams and Jim Schier of NASA, Lloyd Wood of Cisco Systems, and Majid Raissi-Dehkordi, Gun Akkor and Hui Zengh of CSHCN, for useful discussions on this topic.

References

[1]"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.

[2]Y. Chen and M. Hadjitheodosiou, "Joint Energy Management and Routing in Sensor Networks for Space Exploration," *Proc. 22nd AIAA International Communications Satellite Systems Conference And Exhibit 2004*. AIAA, Monterey, California, May 2004.

[3]"Satellite tool kit," URL: http://www.agi.com/products/desktopApp/stkFamily/modules/core/stk/.

[4]"Opnet Modeler," URL: http://www.opnet.com/products/modeler/home.html.

[5]Office of the Chief Information Officer, National Aeronautics and Space Administration, "NASA Policy Directive NPD 2810.1C," URL: http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_2810_001C_&page_name=main

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

[7]A. Roy-Chowdhury, J. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security Issues in Hybrid Satellite Networks," *Submitted for publication, IEEE Wireless Communications*, 2005.

[8]"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.

[9]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.

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

[11]M. Bohge and W. Trappe, "TESLA Certificates: An Authentication Tool for Networks of Compute-constrained Devices," in *Proc. of 6th International Symposium on Wireless Personal Multimedia Communications (WPMC '03)*, Yokosuka, Kanagawa, Japan, October 2003.

[12]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, May 2004, pp.767–776.

[13]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.

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

[15]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.

[16]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, February 2004, pp.308–319.

[17]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.

[18]C. Wong, M. Gouda, and S. S. Lam, "Secure Group Communications using Key Graphs," *IEEE/ACM Transactions on Networking*, Vol. 8, February 200, pp.16–30.

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