Recent Developments in Space Communication Architectures

Omar Y. Tahboub & Javed I. Khan
Media Communications and Networking Research Laboratory
Kent State University

otahboub|javed@kent.edu

Abstract

A revived interest in space communication has been initiated by major space agencies since the early of this millennium. Globally, a significant growth of national space programs has been achieved by a number of nations including the USA, Europe, Russia, India and China. Industrially, there is a trend for privatizing the space industry. This will lead to new space communication age opening new horizons for multi-billion dollars space communication enterprises. Recently, there has become a global interest for establishing a new generation of commercial space communication architectures. A number of space communication architectures and protocols have been proposed by NASA, JPL, CCSDS and BBN. All of these architectures aim to provide an extensive multi-party access to space explorations deployed at three geographical zones: earth, near space and deep space. In paper, seminar, we present some of the recent developments in space communication architectures. First, we describe the space communication environments in terms of their geography, and features. Second we survey four leading space communication architectures namely OMNI, CCSDS, Hi-DSN and SpaceVPN. Finally, we provide a detailed evaluation discussion demonstrating the points of strengths and weakness of each of these architectures. Finally, it is shown that the OMNI architecture will serve the demands of future near space missions, while SpaceVPN will be the de facto architecture serving the demands of deep space explorations.

I. Introduction

A nationally renewed interest in space communication has been witnessed since the early of this millennium. This special interest will lead communication industries to a new space age [1]. Recently, a strong trend has been observed towards privatizing the space industry. In the near future, the private sector will play a key role in drawing the future of the space industry. Emergent space applications such as global precipitation measurement [2], astrobiology [3] and space tourism will open new industrial markets in the near future.

Future space industries will serve two classes of clients: public and private. The former class includes governmental organizations, while the latter includes private organizations and individuals. For instance, public organizations would benefit from global precipitation measurement for aviation and natural disaster prevention purposes. On the other hand, traveling agencies and individuals would benefit from space tourism. Furthermore, medical and pharmaceutical industries will have new opportunities to conduct astrobiological experiments in space [3].

One remarkable aspect of this age is the communication-centric nature of both space missions and applications. This implies the existence of integrated communication architectures along with protocol architectures

Space communication architectures will provide reusable and yet sharable physical infrastructures accommodating the communication needs of various space missions operated by different national parties [1]. These architectures will link network assets at three geographical (galactic) zones: earth, orbiting and deep space [1].

Space protocol architectures will transparently provide end-to-end communication services to space networks. These architectures also describe the design of the protocol suite applied by all assets such as satellites, rovers, and scientific equipments deployed in the space network [4]. It is anticipated that these architectures will be interoperable with standard terrestrial communication protocols enabling both secured and real-time Internet-based access to on-going space missions[4].

The space communication environment raises a set of interesting design challenges must be addressed by future protocol architectures. These challenges include long propagation delays, network mobility, link intermittency, limited resource allocation, extreme reliability and security. As a consequence, major space agencies and research labs have undergone design exploration for a new generation of space protocol architectures[1,4] addressing these design challenges.

In this paper, we present some recent developments in space communication architectures. First we describe the space communication environment in terms of its hierarchal organization - galactic geography-[1], services and environmental constraints. Second we survey four leading architectures namely OMNI[5], CCSDS[6], Hi-DSN[7] and SpaceVPN[8]. Third, analytically demonstrate their extent of completeness, strength and weakness and what design challenges they address and they do not.

The complete paper will describe the space communication environment, then survey the four leading architectures, and finally provide the analytical discussion of these architectures.

The rest of the paper is organized as follows, section II describes the space communication environment, section III surveys the four space communication architectures, and section IV provides the evaluation discussion of SpaceVPN, and section V concludes the paper.

II. The Space Communication Environment

In this section we describe the common characteristics of space communication environments that distinguish space communication from conventional terrestrial communication. Space communication environments commonly share two characteristics: galactic geography, a set of standard features that consists of service constraints and environmental constraints.

A. Galactic Geography

The geography of space communication architectures is broken into three zones: earth, orbital and deep space. The earth zone represents the all terrestrial network assets deployed for space communication purposes. As shown in Figure1, these network assets collectively provide a secured broadband network backbone that links scientist and investigators to mission operation centers (MOC). These MOCs are further linked to access networks that consist of gateways to space network assets. The orbiting zone forms an intermediary region that enables access to deep space mission. As shown in Figure1, this zone contains all network assets that includes deployed at the earth and lunar orbital ranges. The orbiting zone network assets

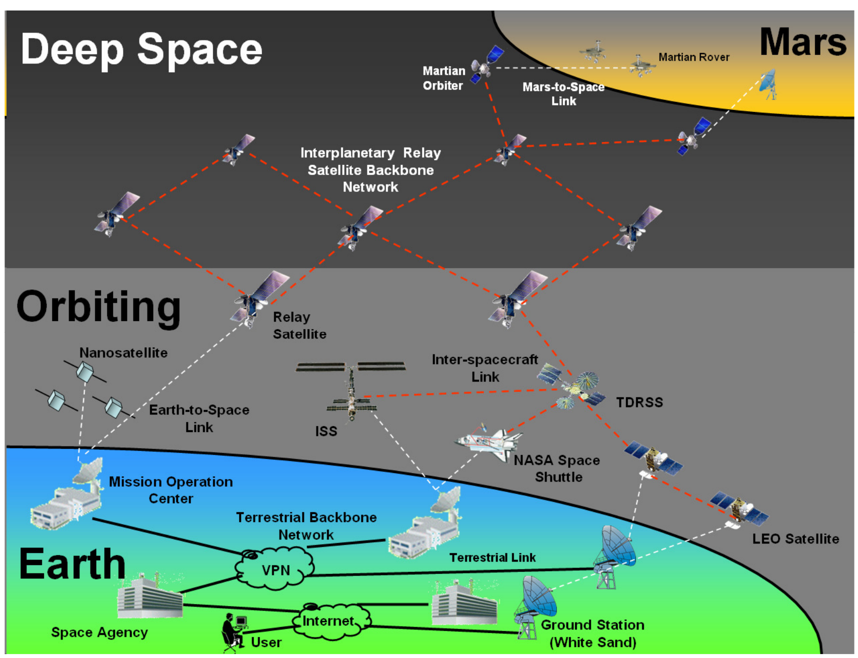

Figure 1: The three-zone galactic space communication geography

contain various satellites scales (LEO, MEO, GEO, micro, and nano satellites), space shuttles, ISS, and lunar orbiters.

The deep space zone provides a long hull interplanetary network infrastructure that will service the entire solar system. It shown in Figure1 that three types of networks are to be supported by this zone: satellite formations, interplanetary satellites and planetary colony networks.

This galactic geography is further broken into five-zonal hops described as follows. The home colony zonal hop represents the earth zone. The home orbital zonal hop represents the earth orbital range. The space backbone zonal hop represents regions between the planets. This zonal hop consists of a set of relay satellites acting as an interplanetary communication backbone, which aims to interconnect different planetary networks into a global space network. Similar to the home zonal hop, foreign orbital zonal hop also represents the orbiting range of spacecrafts deployed at different planets like Mars. The foreign colony zonal hop is the network deployed at the surface of planet other than the earth. One feature distinguishes this zonal hop from its earth counterpart is the type of network assets deployed there, which include scientific equipments, rovers, and in-situ sensors**.**

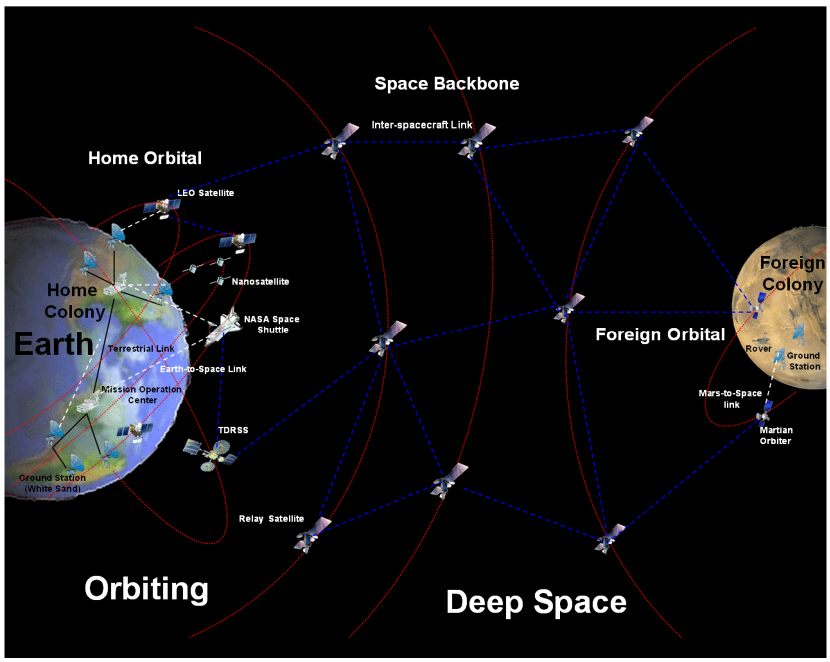

Figure 2: The five-zonal hops

B. Features

1) Long propagation delays

This service is related to the connectivity established under a wide range of propagation delays and relative velocity. By referring to the space network infrastructure shown at Figures 1 and 2, it can be noticed that the inter-zonal hop distances (listed in Table 1) are remarkably long.

Inter-zonal hop range	Approximate Distance (Km)
Home colony - Home orbital	250-2000[9]
Home orbital - Space Backbone Network	1-2800[9]
Space Backbone Network- Foreign orbital	1-100,000[10]
Foreign orbital - Foreign colony orbital	800[11]

Table 1: The inter-zonal hops distances

2) Mobility

Three types of types of mobility patters exit in this space communication environments: zero-dynamicity (static), semi-dynamicity (semi-dynamic) and total-dynamicity (fully-dynamic). In the first type, the topology of space network entities is completely static (stationary). The context of network entities is related to hardware assets that are further broken into two types: end-systems (end-points) and intermediate-systems. In the second type, the topology is dynamic but predictable; hence the mobility of the network entities can be predicted with high precision. On the hand, in the third type the mobility of space network entities is ad hoc, and hence unpredictable. The mobility patters of three-zone architectures is given by Table 1.

Space Network Entity Type	Earth Internet	Earth Proximity	Space backbone	Planetary Proximity	Planetary Colony
End-Systems	Zero/Semi-Dynamicity	Semi-Dynamicity	Fully-Dynamicity	Semi-Dynamicity	Zero/Semi-Dynamicity
Intermediate-Systems	Zero-Dynamicity	Semi-Dynamicity	Fully-Dynamicity	Semi-Dynamicity	Zero-Dynamicity

Table 1: The mobility patters in space communication environments

3) Extreme Protocol Reliability

Generally, the spending budgets allocated for space missions tend to be in the scale of Billions of dollars. The fact behind this aspect is attributed to high expense of spacecrafts, launching facilities, scientific equipment and personnel. Moreover, deploying a space mission at the orbiting or deep space zone would involve a series of activities that include launching a spacecraft, deploying scientific equipment deployment and commanding and controlling its operations. It universally agreed that spacecrafts are the most expensive transportation systems costing hundreds millions of dollars. The high cost space mission entities impose the demand for extremely reliable communication protocols performing the command and control activities. For instance losing a spacecraft due to miss-control be a multi-hundred million dollars fault; hence intolerable.

The deployment of space missions is one of the level of reliability guaranteed by the space protocol to deliver mission data and control signals between base-stations and spacecrafts, and among spacecrafts themselves. Moreover, reliability in this context is also related to degree to fault-tolerance and self-stabilization the protocol provides in the cases of sudden failures or crashes. In space networks, the degree of protocol reliability is required to be extremely high due to the extremely high expense of mission redeployment. For instance, loosing control of a spacecraft orbiting around a specific planet would incur a prohibitive cost in the order of millions of dollars, and hence it would be in tolerable. Conventional standard terrestrial network protocol architectures do not provide this degree of fault tolerance.

4) Link Intermittency

Link intermittency is a direct consequence of the dynamicity of the space network topology. This aspect is can be clearly observed at the space backbone network zonal hop, where communication links have limited age. In other words, links are active only for a limited period of time due to the constant node mobility. The concept of link intermittency is elaborated for a time-varying connected graph in Figure 3.

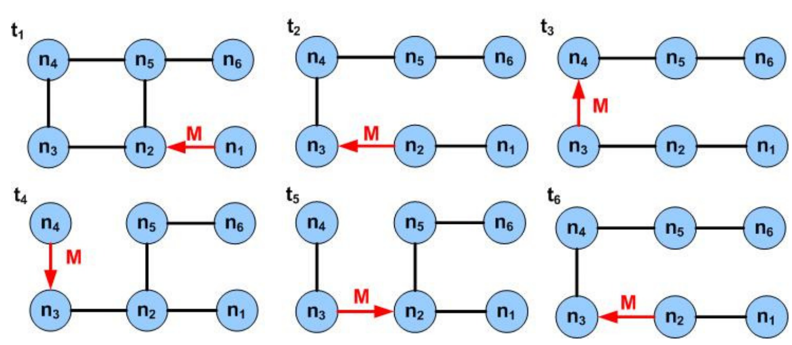

Figure 3: Link Intermittency Scenario in Time-Varying Graphs

The entire set of edges is intact in initial graph at time t_1, n_1 intends to send a message M to n_6 through the path (n_1, n_2, n_5, n_6). At t_2, the message is received by n_2, the link (n_2, n_5) goes down, and n_2 reroutes M to n_3 through the path (n_2, n_3, n_4, n_5, n_6). At t_3, M is received by n_3 and forwarded to n_4.At t_4, M is received by n_4, the link (n_4, n_5) while the link (n_2, n_5) returns up. Therefore n_4 reroutes M to n_3 through the path (n_3, n_2, n_5, n_6). At t_5, M is received by n_3 and forwarded to n_2. At t_6, M is received by n2, the link (n_2, n_5) goes down again, and n_2 reroutes M to n_3 through the path (n_2, n_3, n_4, n_5, n_6). The links (n_2, n_5) and (n_2, n_5) will interchangeably keep going up and down keeping M to be rerouted back and forth between n_2 and n_4 causing and message trap.

In order to avoid such message traps the design of space communication architecture should be aware of link intermittency and provide both prevention and avoidance message trap policies

5) Security

The principle mechanism needed to thwart such threat is authentication and encryption. However, unlike earth, some information cannot be hidden. The orbit and location information of most of the assets along with overall routing and topology scenario will remain exposed. It will be vulnerable to jamming, denial of service attacks or even physical destruction. It is likely that different countries (or agencies within a country) will have complementary assets, and there will be mission scenarios under which communication routes have to be established using assets from multiple administrative domains. BGP like selective asset advertisement and filtered asset disclosure protocols have to be developed to support such scenarios. The current BGP have to be extended to include schedulablity and dynamic topology support. Further, two sub-scenarios might arise in inter agency information exchange. Like earth, the information may be filtered and exchanged directly in space. However, it is also possible that the agencies will exchange all such information via a gateway server on earth, where proper filtering and security checks enforced here.

III. Recently Proposed Communication Architectures

In this section we present the four of the leading space communication architectures namely OMNI[2], CCSDS, Hi-DSN and SpaceVPN. The layered approach provides is considered allows a clean isolation of special space problems in order to be solved as needed. Moreover, it facilitates modular protocol layer design, which further allows having independent implementations.

A. OMNI

The **Operating Missions as Nodes on the Internet**[1] (**OMNI**) architecture proposed by NASA/GSFC to provide a simple and cost-effective communication infrastructure for NASA future missions. This architecture aims to integrate terrestrial networks to space networks to enable mission operations that organize network assets as Internet nodes. Moreover, such organization facilitates access to on-board spacecraft equipments though standard remote access protocols. One design breakthrough this architecture attempted to achieve is the adoption of standard Internet technologies which in effect broadens the use of COTS hardware. Furthermore, the use of COTS technologies will play a key role in reducing the development time and costs of future space mission development.

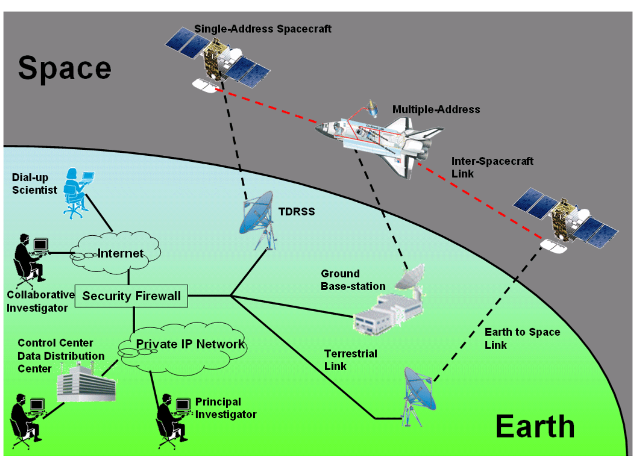

Figure 4: OMNI communication architecture

The OMNI communication architecture consists of two segments that correspond to earth and orbiting galactic zones. The earth zone is the network backbone connecting three types of network assets: space missions and control centers, ground base-stations and users. The orbiting zone consists of satellite networks orbiting within the earth vicinity. The OMNI space communication architecture is illustrated in Figure 4.

The OMNI protocol architecture is illustrated in Figure 5. The design OMNI protocol architecture depicts the standard five protocol layers of the OSI-ISO reference model.

The mechanisms for delivering bits across media like copper, fiber and RF are provided by the physical layer. This layer provides modulation, coding and forward error coding services along with the bit delivery mechanisms. The transmitted data (bits) are recovered by sampling the data line at each clock cycle, such type of signaling is commonly used in serial line protocols as RS-449/422 and V.35. Moreover, this layer also used a set of reliable coding and modulation techniques the perform data recovery over serial link lines with an embedded clock signal. Manchester coding is used for 10 Mbps Ethernet, 4B/5B for 100 Mbps FDDI, 8B/10B for Gigabit SONET, and BPSK and QPSK for RF systems. The RF systems of NASA missions are designed to provide 10-5 or better BER after coding.

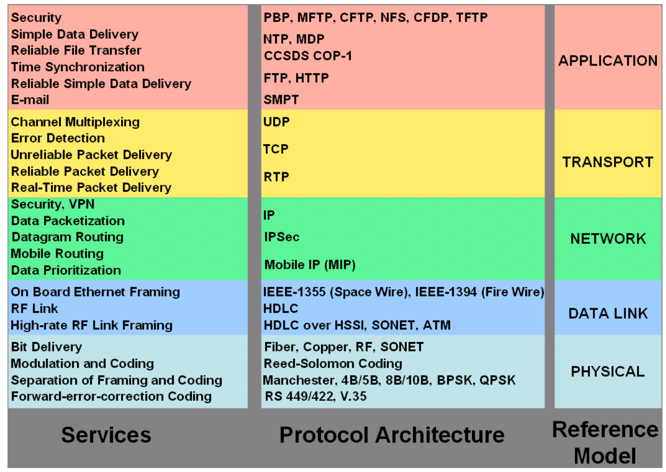

Figure 5: OMNI protocol architecture

The data link layer handles frame transmission and reception at the earth and space (on-board spacecraft) network segments. The data link layer first puts the upper protocol data units (mostly packets) into frames to be transmitted over the physical layer. For frame reception, this layer extracts frames from the bitstream coming from the physical layer and then passes them to the upper layer. Prior to passing a frame to its upper layer it performs the error detection on the information associated with the frame. This layer supports IEEE-1394 and Ethernet for ground and on-board links, HDLC for RF links, and HDLC over ATM and SONET high rate links.

Global end-to-end addressing, datagram routing, data prioritization and security services are provided at the network layer. This layer uses Internet IP-based protocols such as Routing Information Routing (RIP) and Open Shortest Path First (OSPF) for end-to-end packet and datagram routing at the earth network segment. In addition, Mobile IP (MIP) is supported to continuously communicate with spacecrafts since they orbit around the earth in different velocities. When a spacecraft in its orbit course it crosses over different ground base-stations, the spacecraft is assigned a home agent the rest of base-stations are considered foreign-agents. When a spacecraft is accessed through a foreign-agent base-station, its home-agent establishes an IP tunnel with that foreign-agent. Authentication and packet encryption services are provided by IPSec protocol suite.

Channel multiplexing, error detection and end-to-end packet delivery services are the responsibility of the transport layer. This layer applies UDP for unreliable end-to-end data delivery and TCP for reliable end-to-end data delivery. UDP is strongly recommended when the timeliness is more critical than guaranteeing the delivery of each packet. This can be sensed when transmitting spacecraft engineering data, health and safety telemetry, and blind commanding. UDP is also a “send-and-forget” transport protocol where connection setup or handshaking phase is inexistent. UDP properly operates with asymmetric or unidirectional links, is delay in-sensitive and supports multicasting. On the other hand, TCP is a connection-oriented transport protocol, which provides reliable data delivery. For reliability and flow control purposes, TCP mandates status information to be sent with each packet and acknowledgement to be received back. However, TCP still suffer from a number of limitations. TCP handshaking and flow control requires bi-directional link that moderately exhibits link asymmetry approximately 50:1 before the throughput is affected.

E-mail, reliable files transfer, web access, time synchronization and other user application services are provided by the application layer. This layer supports two types of applications: UDP-based and TCP-based applications. UDP-based applications include simple data delivery protocols, reliable file transfer protocols and time synchronization protocols. Simple file delivery is performed through warping custom user application data in a self-defined protocol. Time synchronization protocol (NTP) is used for synchronizing the time of a client computer or server to another server or reference time path. TCP-based application protocols include reliable simple data delivery, reliable file transfer, and E-mail. Reliable simple data delivery is similarly implemented as the UDP-based with additional feature of guaranteed byte-by-byte data delivery; hence automatic packet retransmission is supported in case of data loss or damage. The e-mail service is performed by the Short Mail Transfer Protocol (SMTP), which is specified for sending electronic mails among TCP/IP hosts. SMTP enables scientists and spacecraft operators to communicate with spacecrafts. This also enables space mission scientists and operators can send commands and receive telemetry data in an offline fashion.

B. CCSDS

The CCSDS was among the pioneering organizations that aimed to standardize space network protocols. The CCSDS has accomplished that through providing protocol recommendations covering four categories. The first category includes telemetry, tracking, and command, and second includes information interchange processes, the third includes cross-support potations, and the fourth includes radio-metric and orbit data. Furthermore, these recommendations are motivated to serve the growing demand for interplanetary communication for current and future space missions. The fundamental concept of IPN stems from the fact that Internet is an interconnection of networks and hence it is a "Network of Networks". IPN extends this concept to higher level of abstraction, which envisions the entire Internet on a planet as single network, and the interconnection among these disconnected planetary Internets constitutes the IPN. Therefore, the major goal of IPN is to expand the use of standard Internet protocols to serve in space and deep space missions. Since the beginning of this millennium, the CCSDS has been proposing an integrated IPN protocol architecture. The sole concept behind the CCSDS architecture is the incremental use of "internationally standardized" space data communication protocols in space missions[6].

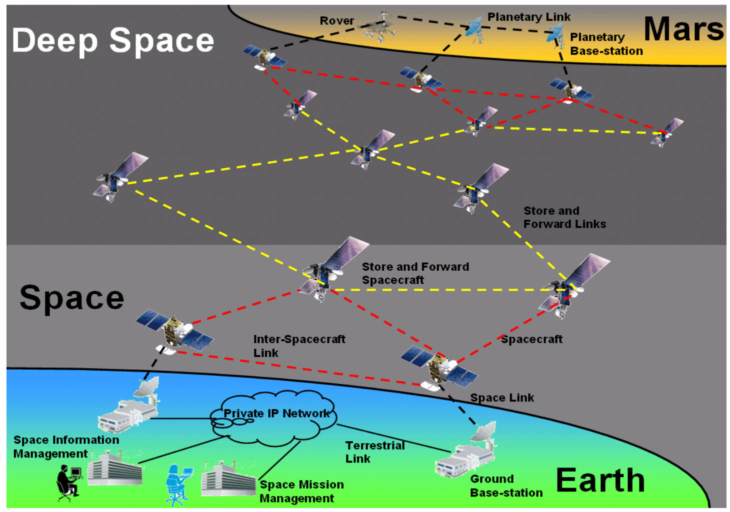

Figure 6: CCSDS communication architecture

The space communication architecture of CCSDS consists of three zones: earth, orbiting and deep space. The first and the second segments are similar to the ones that belong to OMIN architecture in terms of the purpose and the contents. The deep space zone consists of "store-and-forward" relay satellites, communication, science spacecrafts (orbiters) and planetary colony networks (in-situ Internet).

Services	Protocol Architecture	CCSDS Reference Model
Reliable File Transfer Data Compression Security (End-to-End Data Protection)	SCPS-FP FTP Lossless Data Compression	APPLICATION
Channel Multiplexing Security (End-to-End Data Protection) End-to-End On-board Data Transport End-to-End Reliable Packet Delivery	UDP TCP SCPS-TP, SCPS-SP	TRANSPORT
Addressing Security (End-to-End Data Protection) Data Packetization Datagram Routing On-board Packet Routing End-to-End Routing	IPv4, IPv6 Space Packet Protocol, SCPS-NP IPSec	NETWORK
Frame Transfer Framing (Packet Encapsulation) Synchronization and Channel Coding Error Detection and Correction Security (End-to-End Data Protection)	Ethernet ,HDLC, SONET, ATM TM, TC, AOS Proximity-1 Data Link	DATA LINK SYNCH AND CHANNEL CODING
Bit Delivery Modulation, Synchronization, Coding Error Detection	Fiber, Copper, RF, SONET Reed-Solomon Coding, Convolutional, Proximity-1 Physical	PHYSICAL

Figure 7: CCSDS protocol architecture

The CCSDS physical layer provides the standard bitstream delivery service, which consists of bitstream transmission, modulation, coding, and error detection. Modulation and coding, and error detection and correction services are provided by Proximity-1 physical protocol.

The CCSDS data link layer provides standard data transfer along with security services to the three geographic zones. This layer is further broken into two sublayers: synchronization and channel coding, and data link protocol. Standard data transfer services implemented by Proximity-1 Data Link, TM, TC and AOS. At the earth zone, this layer applies IEEE-1394 and Ethernet for ground and on-board links, HDLC

for RF links, ATM and SONET for high rate links. On the other hand, at both of the space and deep space segments, Proximity-1 data link, TM, TC, and AOS protocols are used.
The CCSDS network layer provides four standard services to the three geographic zones. These services include data unit packetization, addressing, end-to-end packet routing and security. At the earth zone CCSDS performs data unit packetization, addressing and end-to-end routing through IPv4 and IPv6 and further supports security through IPSec. At the space and deep space segments, CCSDS uses space packet protocol SPP, SCPS network protocol SCPS-NP, IPv4 and IPv6. SCPS-NP supports connectionless and managed connections operations, priority-based handling, datagram lifetime control, and multiple routing operations. It also is also compatible with IP addressing. Further, this layer also provides end-to-end services through SCPS security protocol SCPS-SP. SCPS-SP perform the confidentiality, integrity, authentication, and access control operations.
The CCSDS transport layer is responsible of provided end-to-end data delivery along with security to thee galactic zones. For the earth zone, TCP and UDP are used for end-to-end data delivery. TCP is applied for reliable data delivery, while UDP is applied for unreliable datagram delivery. For both of space and deep space zones, CCSDS applies SCPS-TP protocol for end-to-end data delivery. For security services, SCPS-TP is used.
The CCSDS application layer has three services to provide the users at three segments. These services include reliable data transfer, lossless data compression and security. For reliable files transfer service, CCSDS has proposed SCPS-FP, which handles all file transfer operations (primitives). Moreover, FTP can be used on the top of SCPS-TP, TCP and UDP.

C. Hi-DSN

The Hi-DSN architecture[7] integrates both space and terrestrial networks with each other to provide an ad hoc space communications infrastructure. This infrastructure is intended to support a wide range of space missions and spacecraft configurations. Hi-DSN infrastructure will be relevant for integrating various space missions to share their assets and mission data. Hi-DSN is planned to be applied for establishing communication with ground base-stations, planet rovers and low-flying probes. Hi-DSN is also applied for inter-spacecraft networking that include formation and clusters. In addition, Hi-DSN will provide support for real-time applications and multiple self-forming space network topologies.
The Hi-DSN space communication architecture is illustrated in Figure 8
Hi-DSN is three-zone architecture. The first zone represents the Earth tier which consists of space network assets deployed on earth such as base-stations. The second segment (middle) is the space network that consists of the spacecraft network, which consists of the spacecrafts that within the vicinity of the earth and the Moon. The third tier (highest) is the deep space network, which consists the interplanetary relay satellites that relay data among different planets in the solar system.

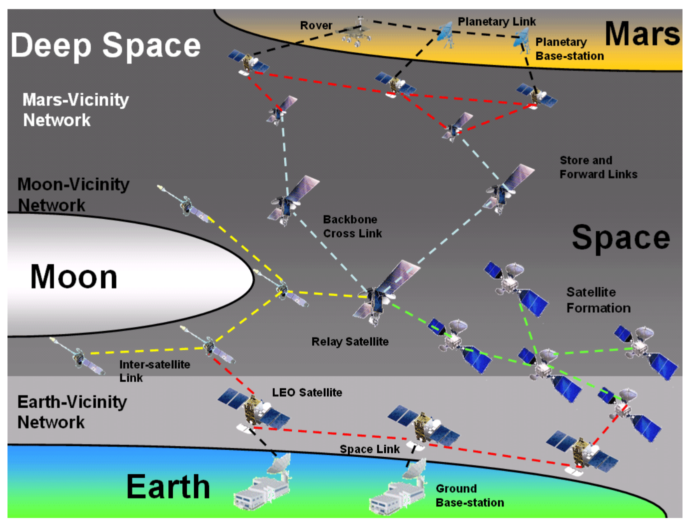

Figure 8: Hi-DSN communication architecture

Services	Protocol Architecture	Reference Model
Addressing Data Packetization Constellation Management Inter-Constellation Routing Intra-Constellation Routing On-board Instrument Security Routing	IP IPSec	NETWORK
Packet Forwarding Node Affiliation	Node Affiliation Protocol	SUB-NETWORK
Frame Transfer Neighbor Discovery Bandwidth Allocation Temporal and Spatial Synchronization Channel Coding Error Detection and Correction Carrier Sensing/Multiple Access	TCeMA Reed-Solomon Coding	DATA LINK
Bit Delivery (Variable Rate Links) Modulation and Coding Error Detection and Correction Digital Beam Forming Burst Assembly and Transmission Time and Code Multiplexing	Null-Steered RF Reed-Solomon Coding BPSK, 256 QAM, KPSK Modulation	PHYSICAL

Figure 9: Hi-DSN protocol architecture

The Hi-DSN protocol architecture is the outcome of the collaboration project between NASA and BBN that aims to provide future Internet-friendly planet vicinity architecture. The main focus of this architecture is only on the space and deep space zones.

The key layer of this architecture is the physical layer, which is uniformly deployed at spacecrafts. This layer provides two types of services standard and specialized. Standard services include bitstream delivery, modulation and coding, and error detection. Specialized services include digital beam forming and, constant burst transmission and reception. Bitstream transmission is performed at the Ka-band, which allows high data rate transmission, spatial reuse of the available spectrum, and the use of high gain antenna arrays. This layer assumes that transmit-and-receive antennas are spatially isolated in order to achieve full reuse of the spectrum. One significant capability of this layer is the predictability of arbitrary network topologies, which in place facilitates the use of null-steered digital beam-forming to establish a variable number of cross-links per spacecraft. In addition, two types of null-steered beam forming are supported: broadcast and point-to-point. To cope with the long inter-spacecraft distances, a novel BBN-based multi-code multi-bit modulation-and coding technique is used. This multi-code modulation-and-coding technique is used on each cross link in order to achieve high bit rates up to four-order-of-magnitude.

The Hi-DSN data link layer is responsible of controlling the use and access to the shared media (space link) among multiple spacecrafts. Therefore the services of this layer are focused on multiple access control functionalities, since this layer has proposed a novel multiplexing called TCeMA as combination of spatial, time, and code multiplexing. This layer also performs two classes of services: standard and specialized, Standard services include frame transmission and reception, channel coding, and error detection and correction. Hi-DSN defines a space link frame structure, which supports for space-and-time synchronization and intermittent (bursty) traffic. On the other hand, specialized services include neighbor discovery, spatial-temporal synchronization, spatial multiplexing control, cross-link level control, and receiver-direct burst synchronization. First, neighbor discovery service is performed by exchanging HELLO and FOUND_YOU busts in the discovery DISC time-slot. This operation further incurs a series of computation-intensive measurements for relative spatial direction, frame-time alignment and carrier frequency synchronization. Second, spatial-temporal synchronization service maintains both the spatial and frame alignment of each node is synchronized with the other nodes. Third, spatial multiplexing control service is supervises the spatial alignment between nodes and the negotiation that takes place between them (aligned nodes) for creating a non-interfering cross-links. Fourth, cross-link level control service performs two tasks: post bust-reception measurements of link performance and of the relative frequency, and using these measurements to monitor the quality of cross-links. The quality of cross-links determines the achievable throughput as a function of the BER encoding and the required PER. Fifth, receiver-direct burst synchronization service schedules burst transmission between the nodes (between a node and its neighbors). Burst transmission schedule is required to guarantee that nodes transmissions do not overlap at the transmitter and the burst is received time-aligned with the both of the receiver's time-slots and carrier frequency.

Global addressing, data packetization and end-to-end routing are handled by the Hi-DSN network layer. This layer is further extended to an additional sublayer which provides more specialized services to include neighbor discovery, network synchronization and terminal affiliation. The end-to-end routing service provided by this layer covers the routing at the on-board spacecraft, formation, intra-constellation, and inter-constellation topological levels. BBN has proposed five related protocols to serve this purpose. First, the neighbor discovery protocol handles node self-advertisement and time-slot synchronization with other nodes within its range. Second, global node frame-epoch synchronization is performed by the network synchronization protocol. Third, end-to-end routing is performed by the distributed routing protocol, which maintains the network topological information database and manages the link state information for each destination node. Fourth, the decisions a node takes to forward a packet to specific destination node is performed by the packet forwarding protocol. Finally, the node affiliation protocol enables an endpoint router to find affiliate routers on the path to a destination node and dynamically handover network topological information over time.

D. SpaceVPN

The SpaceVPN[8] architecture extends the Hi-DSN with the architectural specifications of the earth zone, which focuses on enabling both secured real-time access to both onboard spacecraft resources. According the contest of SpaceVPN, the spacecraft resources include science data, instruments and sensors.

The SpaceVPN protocol architecture illustrated in Figure 10 extends the Hi-DSN architecture shown in Figure 8 with the earth network segment by which users (experimenters) gain access to space missions

Given the fact that SpaceVPN is based on the Hi-DSN, SpaceVPN is three-zone architecture. Moreover, the orbiting and deep space zones are equivalent to the ones belonging to the Hi-DSN. Therefore, the preceding discussion only describes the earth segment.

The main task of the earth segment is to provide experimenters (users) secure and real-time access to spacecraft resources. Generally experimenters gain access to different space missions through Missions Operations Centers (MOC) using secure Internet connections. These centers host network access servers securely connected to ground stations. The earth segment shown in Figure5 illustrates the scenario by which an experimenter is transparently linked to the on-board spacecraft sensor hardware through an encrypted tunnel.

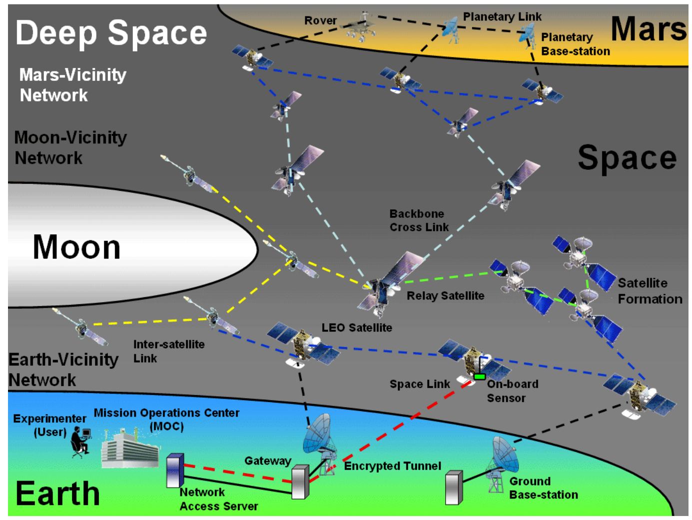

Figure 10: SpaceVPN communication architecture

The SpaceVPN protocol architecture is illustrated in Figure 11, note that the lower four layers corresponds to the Hi-DSN architecture described previously. However, the network layer additionally provides security services through IPSec protocol suite. Therefore we only describe the transport and application layers of the SpaceVPN architecture.

The standard channel multiplexing and data delivery services are provided by transport layer. For unreliable end-to-end data transport UDP is used, while TCP is used for reliable end-to-end data transport. Reliable file transfer and secured remote login services are provided by the application layer, which supports FTP and SCP for file transfer services and SSH for remote login to on-board spacecraft computers

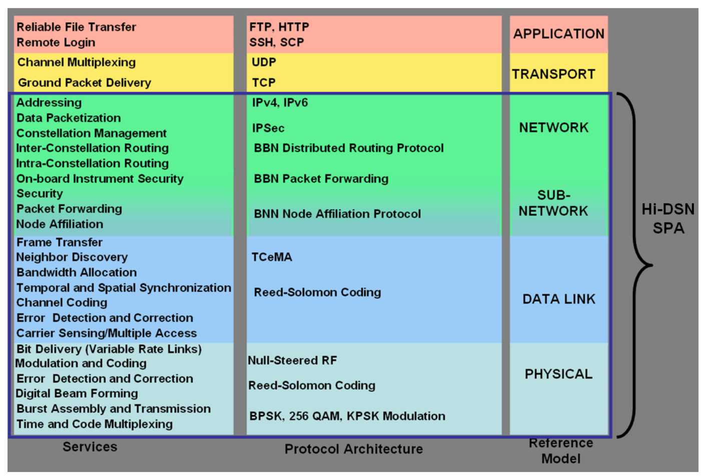

Figure 11: SpaceVPN protocol architecture

IV. Discussion

In this section we provide a brief discussion of the features provided by the four architectures surveyed in this paper summary for both architectures through the related discussion of space communication environment described in section III.

The galactic geography of the surveyed architectures fall into two categories: two- and three-zone architectures. OMNI is a two-zone, while CCSCS Hi-DSN and SpaceVPN are three-zone architectures.

The table shown below provides a detailed comparison of the features supported by the four space protocol architectures. First, OMNI architecture is targeted towards near earth exploration missions. This architecture is both IP-based and application-centric. The OMNI architecture is IP-based, which lends itself the flexibility of levering technological advancement of standard Internet protocols. This is evident through the standard services provided by each of its five layers. The design of this protocol architecture is focused on the application aspects of space missions such command and control, telemetry data access. This is seen through the services provided by the transport and application layers. For command and control operations TCP/IP is applied for reliable connection, while UDP can be used for telemetry data access. Onboard spacecraft scientific equipments can be accessed through standard remote login protocol like SSH.

Protocol Layer	Services	OMNI	CCSDS	Hi-DSN	SpaceVPN
Application	• Security	☑	☑		☑
	• File transfer	☑	☑		
	• Remote access	☑	☑		
Transport	• Channel multiplexing	☑	☑		☑
	• Reliable end-to-end transportation	☑	☑		☑
	• Unreliable end-to-end transportation	☑	☑		☑
Network	• Global addressing	☑	☑	☑	☑
	• Security	☑	☑	☑	☑
	• Ground end-to-end routing	☑	☑	☑	☑
	• Constellation management		☑	☑	☑
	• Intra-Constellation routing			☑	☑
	• Inter-Constellation routing			☑	☑
	• Packet Forwarding	☑	☑	☑	☑
	• Node Affiliation			☑	☑
Data Link	• Packet encapsulation (Framing)	☑	☑	☑	☑
	• Frame transmission and reception	☑	☑	☑	☑
	• Error detection and correction	☑	☑	☑	☑
	• Neighbor Discovery			☑	☑
	• Temporal and Spatial Synchronization			☑	☑
	• Carrier Sensing	☑	☑	☑	☑
	• Bandwidth Allocation	☑	☑	☑	☑
Physical	• Bit delivery (variable rate links)	☑	☑	☑	☑
	• Modulation and coding	☑	☑	☑	☑
	• Error detection	☑	☑	☑	☑
	• Digital beam forming			☑	☑
	• Burst assembly and transmission			☑	☑
	• Time and code multiplexing			☑	☑

Table 8: The feature supported by OMNI, CCSDS, Hi-DSN and SpaceVPN architectures

The OMNI architecture sufficiently addresses the mobility, long propagation delay and security issues. Due to the fact that it is an IP-based architecture, Mobile IP is used for handling spacecraft mobility.

Furthermore, long propagation delay is handled at the network and transport due to fact OMNI is applied at the near space where propagation delays are . Security is supported at the application and network layers. On the other hand, OMNI architecture is not expandable for deep space missions based on the fact that IP-based protocols are obsolete for deep space communications due to long propagation delay, mobility and link intermittency.

Second, the CCSDS architecture is intended as reference specification from near and deep space communication networks. Similar to the OMNI architecture, CCSDS implements the standard ISO-OSI reference model at wider scale supporting the deep space galactic zone. The CCSDS architecture is IP-based at the earth zone and IP-interoperable at the orbiting and deep space zones. For instance, CCSDS employs IP for terrestrial communications and IP-compatible protocols including SCPS-NP, -TP, and –FP at the orbiting and deep space zones. Security services at the earth zone are provided by standard authentication and data encryption mechanisms, while these services are provided by SCPS-SP at remaining zones. In addition, long propagation delay, mobility and link intermittency from crucial design issues especially at the deep space zone. The design of both SCPS-NP and –TP address the issues of long propagation delays especially at the deep space zone. One the other hand, SCPS-NP does not address the mobility issues related to routing satellites in continuous motion. Furthermore, SCPS-TP does not provide mechanisms for preventing message trapping due to link intermittency.

Third, Hi-DSN forms a technological leap towards deep space communication. One remarkable feature of Hi-DSN is its communication-centric nature. The services provided by the Hi-DSN architecture are focused on orbiting and deep space zones. Hi-DSN provides special class of services at the physical, data link and network layers. For instance, beam-forming and burst assembly services are provided by the physical layer, neighbor discovery and burst synchronization are provided by the data link layer. Yet, Hi-DSN introduces a special sub-network layer that provides multi-hop distributed intra/inter-constellation routing, node affiliation and constellation management services. Hi-DSN addresses both mobility and link intermittency issues through the services provided by the sub-network layer. Hi-DSN organizes spacecrafts into clusters and ad hoc formations topologies facilitating intra-/inter-formation routing. Furthermore, satellite formation topologies are deterministic providing a high degree of link predictability that lessens the effect of link intermittency. Furthermore, one major advantage gained from Hi-DSN topological organization is the mitigation of long propagation delay provided by its multi-hop topologies. However, the design of the sub-network protocol does not precisely address routing in non-deterministic topologies and message trapping.

Fourth, SpaceVPN is an architectural extension of Hi-DSN emphasizing the earth zone. SpaceVPN additionally provide the standard IP-based services to the space network assets deployed in the earth zone. Unlike Hi-DSN, SpaceVPN architecture supports security through its application and network layers using IPSec protocol. Finally, due to the fact SpaceVPN is based on Hi-DSN, this architecture shares the similar issues at the orbiting and deep space zones.

V. Conclusion

In this paper, we presented some of the recent development in space communication architectures. We first described the space communication environment by means of its galactic geography and common features – service constraints-. Second, we presented two of the most recent space communication architectures Hi-DSN and SpaceVPN. For each architectures, we provided a detailed description if its communication and protocol architectures. Third, we provided a detailed discussion emphasizing the points of strengths and weaknesses of each of the four protocol architectures. Future emergent space missions will pose a demand for robust and yet scalable communication-centric protocols at three the three galactic zones. Two classes of space protocol architectures are likely to exist: two and thee-zone architectures. Based on the discussion carried out, it is shown that OMNI architecture provides a sustainable architecture serving future near space exploration demands. The CCSDS architecture will remain the most reliable standardization reference for future of interplanetary communication architectures. On the other hand, Hi-DSN and SpaceVPN provide robust and yet scalable architectural design that will serve the growing demands of future deep space explorations. That is sensed through specialized features provided by their physical, link and network protocol layer. Finally, it can also be concluded that the Hi-DSN and SpaceVPN will be the future *de facto* space protocol architectures of the next space age.

VI. References

[1] Khan, J., Tahboub, O., “A Reference Framework for Emergent Space Communication Architectures oriented on Galactic Geography”, to appear in AIAA Space Operations ‘08, Heidelberg, 2008.

[2] Hogie, K., Criscuolo, E., and Parise, R., “Using Standard Internet Protocols and applications in space”, Computer Networks, Vol. 47, No. 5, Elsevier, 2005.

[3] Pohorille, A., Shrager, J., Racunas, S. and Schweighofer, K., “An Integrated System for Synthesis and Evaluation of Biological Models”, NASA Science and Technology Conference 07, Baltimore, Maryland, 2007.

[4] Tahboub, O. Y., and Khan, J. I.,“A Critical Design Evaluation of the Next Generation Space Network Architectures”, technical report TR-2007-09-01, Medianet Lab, July, 2007.

[5] Rash, J., Hogie, K., and Casasanta, R., “Internet technology for future space missions”, Computer Networks, Vol. 47, No. 5, Elsevier, 2005.

[6] Burleigh, S., Cerf, V., Durst, R,. Fall, K., Hooke, A,, Scott, K., Weiss, H., “The Interplanetary Internet: a communications infrastructure for Mars exploration”, 53 International Astronautical Congress The World Space Congress, 2002.

[7] Bergamo, M. AS., “High-Throughput Distributed Spacecraft Network: architecture and multiple access technologies”, Computer Networks, Vol. 47, No. 5, Elsevier, 2005.

[8] Lapsly, D., Bergamo, M., “An integrated approach to the development of wireless network protocols”, Proceedings of the 1st international workshop on Wireless network Testbeds, experimental evaluation & characterization, Los Angeles, CA, USA, p.10-17, 2006.

[9] Christopher R., “Overview of LEO Satellite Systems”, 1999 second annual International Symposium on Advanced Radio Technologies, Sept. 8-10, 1999.

[10] Bhasin, K., and Hayden, J. L., “Space Internet Architectures and Technologies for NASA Enterprises” Int. J. Satell. Commun. 2002; 20, 311-332.

[11] Bell, D.J.; Cesarone, R.; Ely, T.; Edwards, C.; Townes, S., “Mars network: a Mars orbiting communications and navigation satellite constellation”, IEEE Aerospace Conference Proceedings, Volume 7, Issue , 2000 Page(s):75 - 88 vol.7.