SSC21-X-04

Secure Space Mesh Networking

David Andaleon, Assi Friedman, Jonathan Wolff, Jeff Janicik
Innoflight
9985 Pacific Heights Blvd, Suite 250, San Diego, CA 92121; 858-638-1580
dandaleon@innoflight.com

ABSTRACT

Innoflight's Secure Space Mesh Networking development and prototyping efforts started at its incorporation over 15 years ago with a vision of establishing end-to-end Internet Protocol (IP) connectivity in and through space. A number of space industry trends have accelerated the demand for space networking: (a) the widespread adoption of enterprise-grade and cloud-based, IP-centric ground system architectures; (b) the accelerated growth of both commercial and government proliferated Low Earth Orbit (pLEO) constellations leveraging small satellites (SmallSats); (c) the maturation, miniaturization and commoditization of high-speed Radio Frequency (RF), Free Space Optical (FSO) Inter-Satellite Links (ISLs), and high-performance flight processors for aforementioned SmallSats; and (d) the need for All-Domain Operations (ADO) seamlessly and autonomously integrating space, airborne, terrestrial, maritime and underwater networks. Furthermore, data encryption, for reasons of either National Security or monetized mission data protection, creates additional challenges to effectively switch/route and encrypt/decrypt ciphertext data across a mesh network. Lastly, with the projection of multiple and multi-national pLEO constellations, it is critical to negotiate link security real-time for dynamic, trusted nodes, and prevent inadvertent or intentional networking with unknown/untrusted nodes.

Innoflight will discuss the aforementioned relevant space industry trends and commercial and government initiatives, including DARPA (Defense Advanced Research Projects Agency) Blackjack and Space Development Agency's (SDA) National Defense Space Architecture (NDSA), and then identify the technical challenges for secure space mesh networking and decompose these challenges with two popular frameworks: (a) the individual layers, especially Layer 2 (data/link layer) and Layer 3 (network layer), within the Open Systems Interconnection (OSI) model; and (b) the control and data planes within the Software Defined Networking (SDN) model. Innoflight will present its development and prototyping efforts, specific to these challenges, including recent work funded under a 2019 Space Pitch Day award and leveraging its general-purpose processing and networking CFC-400X platform, and conclude by identifying remaining gaps: including technical, commercial and policy; to fully realize interoperable secure space mesh networking..

INTRODUCTION

Future space communications are moving towards an enterprise architecture. While this visionary statement may mean different things to different people, the reason this is happening is to move away from stovepipe systems and decrease the amount of time it takes communications to travel end to end. Every space system developing and sustaining their own individual communications segments results in redundant costs and a communications and ground processing budget that is no longer affordable. A critical capability that enables the space community to move away from stovepipe systems is networking – not just space-to-space networking but transparent multi-domain networking from space to aerial and terrestrial systems as well. Per Joint Publication (JP) 3-12[1], the military cannot fight in Cyberspace without networking as "Cyberspace Operations are enabled by the Department of Defense (DoD) Information Networks (DoDIN)." The DoDIN has replaced the Global Information Grid (GIG) terminology and now represents the globally interconnected information capabilities for the DoD.

General Hyten said it best in an article that dates back to 2008[2]: "It's really all about the network. In the near future, our satellite capabilities will begin to look much different than today, and our operations will begin to look much different as well. Rather than single stove-piped satellites providing localized effects on the ground, our satellites will transition into part of a network. They will be even more joint and interoperable than we can imagine today. Everything we do will be on or through the joint network…" It is the near future, Space Enterprise is happening but, as usual, change or paradigm shifts in our space systems and operations can be excruciatingly slow.

Moving forward with networks in and through space we know that critical elements to success are interoperability and above all, security. The National Security Agency's High Assurance Internet Protocol Encryption Interoperability Specification (NSA's HAIPE® IS) and IPsec Minimum Essential Interoperability Requirements (IPMEIR) provide the framework to meet both of these elements.

Internet Protocol in Space

The use of Internet Protocol (IP) in space has many benefits that are largely associated with the fact that IP is so proven and widely proliferated in commercial and industrial hardware and software systems. In addition to an extensive number of applications and related standards/protocols that work directly with IP, there are encryption interoperability specifications associated with one of these protocols in particular – namely IPsec. There are two flavors of high assurance encryption specifications for IP -- HAIPE (restricted DoD communications) and IPMEIR (a configuration profile of commercial IPsec), which both support the use of the AES256 encryption algorithm. IP packet-based traffic can be divided into any number of "security associations" (SAs) that are protected with unique keys. A HAIPE and/or IPMEIR compliant system is designed to be fully compatible with a significant number of existing terrestrial boxes (e.g., radios, terminals) with each update of the specification designed to be backwards compatible to previous ones. Compliance with the specification means the abilty to operate and maintain secure IP communications end-to-end regardless of the communications medium.

A HAIPE/IPMEIR in space then is no different from a HAIPE/IPMEIR on the ground. If compliant with the specification, then interoperability is ensured. The physical waveform and signal characteristics will likely be different between space and non-space applications but those have no impact to the encryption/networking layer that is implemented into the individual system's communication and processing equipment. By enabling secure IP from a spacecraft to end user including any node within that network, traditional space communication applications that can now be accomplished as a result of secure addressing and associations of *all the data* instead of dedicated communication pipes or channels for each type of application (e.g., spacecraft command and control (C2), protection of spacecraft subsystem / payload data and/or control, protection of payload data and/or control traffic). While this is a well-understood and used concept for systems that rely on networking and packet-based protocols, space communication links are still stuck using traditional point-to-point serial communications protocols.

A secure space networking communications architecture maintains support for end-to-end native IP which could be easily interpreted as 'Wi-Fi for space' [See ***Figure 1***].

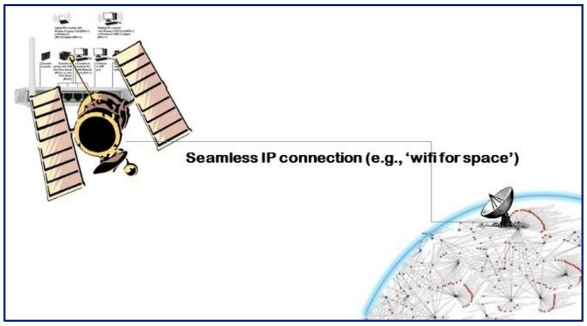

Figure 1. By using IP as the space communications transport, a satellite bus network and/or network of spacecraft can transparently "connect" to the DoDIN and any certified ground user.

While networking and service-oriented architecture (SOA) methods and protocols are more and more commonly used in space system architecture, the space communication links themselves have not migrated to a networking protocol or waveform thus adhering to legacy communications which result in "bridging" IP and performing IP-to-serial or serial-to-IP translations along the way [See ***Figure 2*****]**.

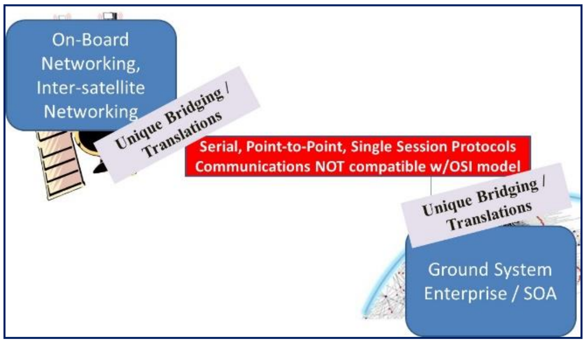
On-Board Networking, Inter-satellite Networking
Unique Bridging / Translations
Serial, Point-to-Point, Single Session Protocols Communications NOT compatible w/OSI model
Unique Bridging / Translations
Ground System Enterprise / SOA

Figure 2. Transparent routing between networks on-board spacecraft and amongst terrestrial users is severed by legacy serial-based communications.

Part of the reason for DoD space link communications to lag in adopting an IP-based physical architecture is the current reliance on bulk and usually custom encryption methods and the non-availability of a qualified packetized encryptor. For secure IP space communications, HAIPE / IPMEIR appliances should be adapted and certified since they meet existing NSA specifications based on Internet Engineering Task Force (IETF) protocols – the worldwide body for the development and promotion of IP-based specifications that frequently become standards.

The use of HAIPE or IPMEIR appliances in space will enable high assurance and/or NSA certified protection (with built-in authentication) of native IP space communication links. While this is a significant advantage to space system architecture, there is also the advantage of operating over a myriad of capable private and public networks and eliminating the serial 'daisy-chaining' with expensive and unique front-end processing equipment. Furthermore, compatible ground equipment for decryption (or uplink encryption) is quite prolific with an estimated 250,000+ HAIPE units in the field. From a cost perspective, a typical HAIPE is less than $10K/unit while the cost of space crypto boxes can easily run an order of magnitude higher with less availability and selection. The elimination of 'space unique' communication equipment from ground systems will ultimately allow more commercial and independent ground stations to become force multipliers for missions.

Mesh Network Definition

The network is defined as a "regular constellation mesh" network. In this network definition, a network node can be a spacecraft, a ground station, or a user. For the purposes of this architecture, Spacecraft Local Area Network (SLAN) refers to the devices within a single spacecraft that are capable of receiving or transmitting data to each other or to other nodes. A user is an endpoint of the network on the ground that is accessing the spacecraft network via a ground station. A regular constellation network is one where the orbits of spacecraft are constrained into many defined orbital planes, where there are several spacecraft in each orbit. The orbital planes are of different inclinations, and orbits may be of different altitudes. A regular constellation consists of rings of satellites where each satellite has a consistent node in front of and behind it. There are also neighboring rings where ring-to-ring (cross-plane) communication is possible. A node's neighbors are constantly changing due to the orbital planes having different altitude and inclinations, causing the need for frequency dynamic routing updates. The Starlink constellation in ***Figure 3*** is an example of a regular constellation.

A mesh network refers to a form of ad hoc network where nodes have rich interconnection with one another. However, each node will not be able to communicate directly with every other node in the network, therefore having only partial mesh visibility. Each node has partial network connectivity via direct link to its neighbors, yet the protocol for routing traffic enables full mesh network connectivity. The number of crosslinks per node depends on the constellation architecture. In an ad hoc network, nodes move in and out of range of each other. Old links of nodes moving out of range will be severed and new nodes coming into range will need to create new connections. Routes that existed on severed links must be rerouted onto different active links.

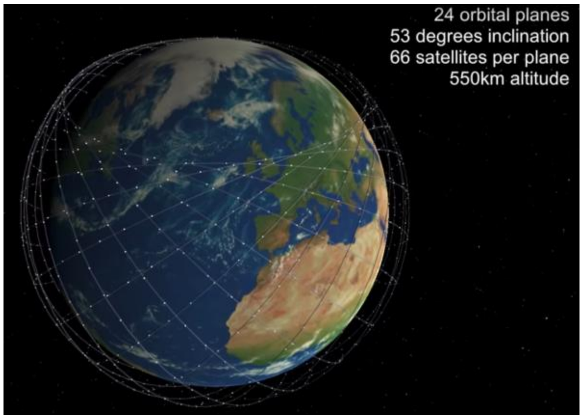

Figure 3: A Regular Constellation (Starlink)

IP-BASED SPACE MESH NETWORK

The space sector is currently undergoing a revolution where traditional "battlestar" style missions are transforming into constellations, swarms, and mega constellations. If we extrapolate this to the number of spacecraft predicted in the near future, it becomes clear that we lack the cyber secure space networking capability necessary to enable this transformation. On the ground side, it is also critical to enhance Mission Operations Centers to securely connect to commercial and other non-DoD controlled ground stations.

Current Space Mesh Network Efforts

Space Development Agency's Transport Layer Tranche 0 constellation consists of two planes of SVs in near-polar orbits.

Two types of SVs:

- Group A provides in-and out-of-plane crosslinks, as well as support of non-transport SVs and optical links to the ground
- Group B provides Link-16 capability and crosslinks in-plane to the Group A SVs

Each plane includes both types of SVs:

Parameter	Group A	Group B
Number of Planes	2	
SVs per Plane	7	3
Altitude	1000 km	
Inclination	80-100 degrees	
Node Separation	31.64 degrees	
Mean Anomaly Seperation	51.43 deg	36 deg
Interplane Phasing	25.71 deg	18 deg

OISLs per SV	4	2 In-Plane
Mission Payload(s)	IBS	Link 16, IBS
TT&C Downlink	Ka	Ka
Navigation	GPS	GPS

To implement SDA's mesh networking Innoflight has developed the generalized payload avionics architecture leveraging high TRL products (for both transport and tracking layers) in ***Figure 4***. Note that instantiations of this architecture are being used for SDA Tranche 0[4].

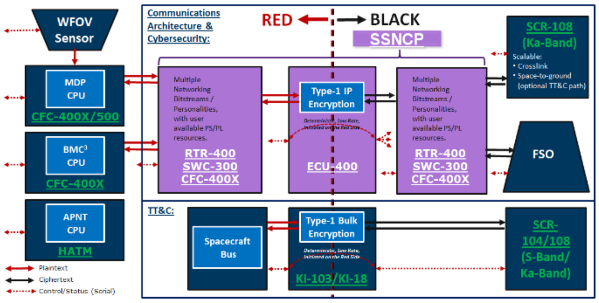
WFOV Sensor
MDP CPU
CFC-400X/500
BMC3 CPU
CFC-400X
APNT CPU
HATM
Plaintext
Ciphertext
Control/Status (Serial)
Communications Architecture & Cybersecurity:
RED
BLACK
SSNCP
Multiple Networking Bitstreams / Personalities, with user available PS/PL resources.
RTR-400
SWC-300
CFC-400X
Type-1 IP Encryption
Deterministic, Low Rate, Initiated on the Red Side
ECU-400
Multiple Networking Bitstreams / Personalities, with user available PS/PL resources.
RTR-400
SWC-300
CFC-400X
SCR-108 (Ka-Band)
Scalable:
• Crosslink
• Space-to-ground (optional TT&C path)
FSO
TT&C:
Spacecraft Bus
Type-1 Bulk Encryption
Deterministic, Low Rate, Initiated on the Red Side
KI-103/KI-18
SCR-104/108 (S-Band/ Ka-Band)

Figure 4: Innoflight's Generalized SDA Payload Avionics Architecture

Key to the architecture is Innoflight's CFC-400X platform product, which can be offered as a general-purpose processing and networking platform with full customer control, or in various networking & network encryption personalities, including Layer-2 switching (SWC-300), DSCP-capable routing (RTR-400) or mesh network HAIPE-compatible encryption (ECU-400). Collectively, the red-side SLAN, HAIPE encryption, and black-side SLAN is described as the Secure Space Networking Communications Processor (SSNCP) and discussed later, especially advanced black-side networking. The CFC-400X supports secure on-orbit reprogramming allowing for ground and on-orbit networking experiments.

The CFC-400X has its origins with DARPA System F6 as an F6 Technology Package (F6TP) providing hardware processing, common spacecraft & payload I/O, networking and crypto resources. With its four 1.2 GHz ARM Cortex-53 cores the CFC-400X also can serve as the Battle Management Command, Control and Communications (BMC3) processor and Mission Data Processor (MDP) functions. If additional processing is needed for a Wide Field of View (WFOV) sensor Innoflight also has its General-Purpose Graphics Processing Unit (GPGPU) based CFC-500 product.

While many of the interfaces are IP-centric, initially 1000BASE-T Gigabit Ethernt, the CFC-400X also supports the necessary I/O – including SpaceWire, LVDS and RS-422 – to interface to various mission links, such as K-Band via Innoflight's SCR-108 or third-party Free Space Optical (FSO) or Optical Inter-Satellite Link (OISL). For the Telemetry, Tracking and Command (TT&C) link to support existing DoD and commercial ground stations a more traditional serial communications with bulk encryption is shown in the architecture. However, in future tranches we anticipate TT&C as part of the SLAN with its own security association. Lastly, to enable advanced Assured (or Alternate) Pointing Navigation and Timing (APNT) features Innoflight offers a High Accuracy Timing Module (HATM) platform to source and sink 1PPS and 10 MHz timing signals, and perform timing functions, across signals from GPS receiver(s), RF & optical links and an internal Chip-Scale Atomic Clock (CSAC).

Innoflight's Research

Innoflight's objective is to introduce mesh networking technology for spacecraft constellations and allow them to be securely accessible via government and commercial gateway resources such as SATCOM and Remote Tracking Stations (RTS). The result is a mesh network of satellites, ground stations, and users. This objective will be achieved via two (2) major elements:

1. The Ground Station Gateway called the High Assurance Missions Operations Gateway (HAMOG), and
2. The Secure Space Networking Communications Processor (SSNCP) that establishes and maintains a secure network of satellites using a L2/L3 Router.

The HAMOG brings commercial ground stations into the mesh network by enabling a Spacecraft Operations Center (SOC) to securely access and communicate with the network of satellites via a commercial RTS in addition to its own space link capabilities. The SSNCP connects spacecraft to the mesh network via advanced networking and transport capabilities implemented on low Size Weight and Power (SWaP) hardware. ***Figure 5*** presents the concept of the space mesh network. Satellites that are not in view of the SOC can transfer/relay data over the network (via crosslinks), or by HAMOG via commercial RTS.

The SSNCP is a fully featured communications hardware stack. Each satellite in the network is equipped with an SSNCP, which creates a dynamic network, which is space-to-ground (ground link) and space-to-space (crosslink) capable. The SSNCP consists of a stack of three (3) Innoflight Compact Flight Computers CFC-400X platforms, each programmed with a different personality of software and firmware, and an Innoflight Software-defined Compact Radio (SCR) such as the SCR-104 (S-band), SCR-106 (X-band) or SCR-108 (K-band). The three (3) CFC-400Xs in the stack are the Space Ethernet Switch SWC-300, the Mesh Networking

HAIPE-compatible End Cryptographic Unit ECU-400, and the Layer 2 Space Node Processor (L2SNP).

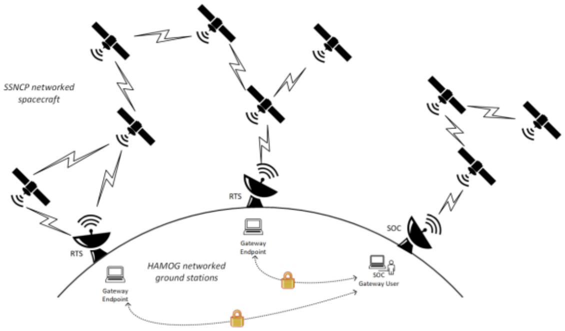

Figure 5: Secure Space Networking Concept

Figure 6 shows the end-to-end hardware architecture of a SOC user accessing the mesh network via an RTS. Satellites that are in view of one another and with active crosslinks are accessible via the SOC. The SOC encrypts traffic using a HAIPE at its location. The user at the SOC begins a secure session between the HAMOG-SOC and the HAMOG-RTS. The encrypted traffic destined for a spacecraft is then sent to an RTS over the HAMOG secured pipe. This provides two (2) layers of security for the traffic. The RTS then uplinks the traffic to any satellite within its range. Each link to spacecraft and between spacecraft are secured at the link level by the SSNCP, providing a second layer of security. The two (2) layers of security for HAMOG and SSNCP traffic is shown in ***Figure 7***.

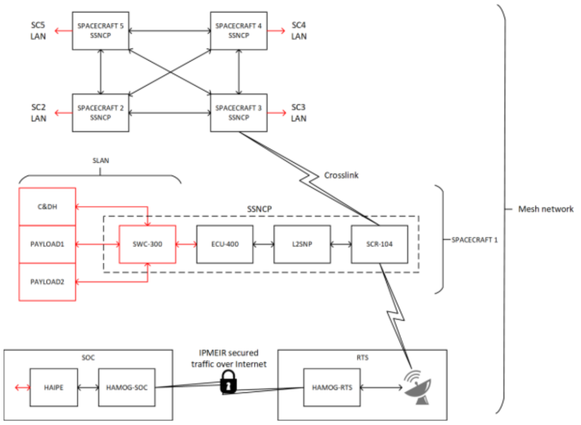

Figure 6: End-to-End System Architecture

The L2SNP decides if the traffic is destined for itself or a different satellite in the network. That satellite then forwards the traffic to the destination satellite within its network. Once the destination satellite receives the traffic, its L2SNP determines the destination is on the Spacecraft Local Area Network (SLAN) and forwards the traffic to the Space HAIPE (S-HAIPE) for decryption.

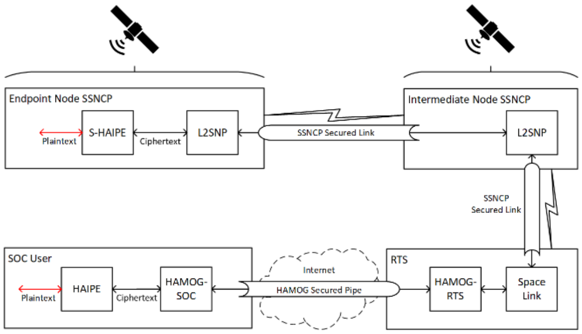

Figure 7: Two Layers of Security

This Innoflight research provides a cyber-secure space communications networking capability at the mission level that is integral to a resilient DoD Space Enterprise. This capability translates to satellite Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) expandability through secure operations with standard commercial Internet Protocol (IP)-based communications and infrastructure – something currently not possible with the DoD's dedicated satellite ground network and esoteric serial (point-to-point) communications interface equipment. A cyber-secure space networking capability for the DoD will be able to respond to emerging infrastructure threats, ensure resiliency, and provide ultimate flexibility to space asset mission operations. On the ground side, this research will provide the capability for DoD operation centers to securely connect to commercial and other non-DoD controlled ground stations without the need for COMSEC.

L2SNP OVERVIEW

The Layer 2 Secure Network Processor (L2SNP) contains the functionality for the L2 Router. It provides the interface between the Layer 1 (L1) devices and the L3 HAIPE and applications layers. It is responsible for generating and maintaining routes and switching network traffic. It also contains a certificate store for authenticating neighboring nodes and providing access to the network. A simplified layer diagram describing the L2SNP is provided in ***Figure 8***.

The application layer above the L2SNP is responsible for maintaining an address book, with each line containing a destination address, its identity, and rules for exchanging data. The L2SNP assumes that the application layer does not know how to reach the destination address. From the perspective of the L2SNP, packets to and from L3 only contain addresses and a payload. There is no additional exchange of information between L2 and L3 that helps the packet find its destination. When the L2SNP receives a packet from L3, it looks at the destination address and checks if it already knows a route to that address. If it does, then it attaches the appropriate labels, encrypts the packet, and begins transport of the packet.

If the L2SNP does not have a route to the destination, then it sends out network control packets to its neighbors to discover routes to the destinations. These network control packets go through link encryption and decryption at the L2/L1 interface. Once the other nodes in the network send back route information, the L2SNP then makes a determination of the best route to the destination. It creates a label switched path over that route to the destination, attaches those labels to the packet, then begins transport of the packet.

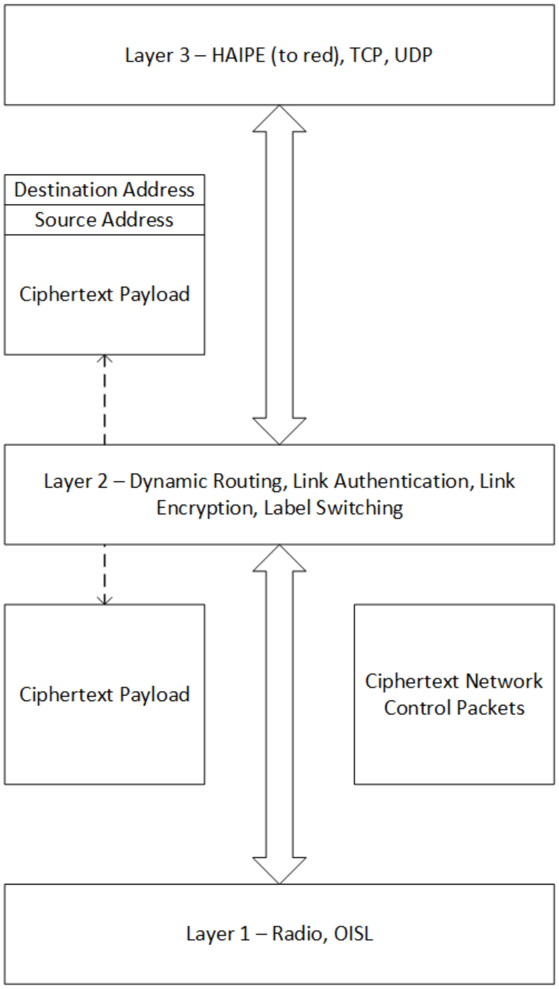
Layer 3 – HAIPE (to red), TCP, UDP
Destination Address
Source Address
Ciphertext Payload
Layer 2 – Dynamic Routing, Link Authentication, Link Encryption, Label Switching
Ciphertext Payload
Ciphertext Network Control Packets
Layer 1 – Radio, OISL

Figure 8: Simplified Layer Diagram

After transport has begun, L2SNP Link Encryption encrypts the entire packet including the labels, the destination address, the source address, and the ciphertext payload. L2SNP then sends the entirely encrypted packet to the appropriate L1 device to transmit the packet to the next node in the route. The next node's L2SNP receives the packet from its L1, decrypts the Link Encryption, and then observes the head label. If the label says it is not the destination, it pops the label, performs another Link Encryption, and forwards the entirely encrypted packet to the appropriate L1 to reach the next node in the route.

If a node observes that the head label is for itself, it pops off the label, and forwards the packet internally to be serviced. If the packet is a network control packet, then it stays in L2. If not, then it is a data packet destined for L3. The L3 and above then processes the destination address, the source address, and the data payload.

Key Performance Parameters

The key performance parameters of the L2SNP are latency, jitter, packets-per-second (PPS) and throughput. To achieve highest possible performance, the implementation of this architecture will be divided between hardware description language (HDL) implemented on a field programmable gate array (FPGA) and software (SW). Any function that can benefit from hardware acceleration will be evaluated for implementation in HDL. Realistically, some functions will be optimal for software implementation or for rapid prototyping in software.

Link Security

The L2SNP provides confidentiality, authentication, and integrity services at the link level with each of its neighboring nodes. Every Inter-Satellite Link (ISL) and ground station Primary Link is secured by the L2SNP. All data and network control traffic are secured at this link level.

The two L2SNP units on either end of an ISL will negotiate encryption keys for the Link Encryptor in a simplified process modeled after Internet Key Exchange v2 (IKEv2) to create Security Associations (SAs) with each other. Using this method, each link between neighboring nodes in the network is encrypted using a completely independent and ephemeral key. After some period of time, the key expires and a new SA must be negotiated.

The negotiation also securely exchanges certificates such that the two L2SNP units may authenticate each other's node identity. The certificates and temporary encryption key will be stored securely in the L2SNP.

Routing Algorithm

The space mesh environment is nothing like terrestrial and aerial networks due to vehicle dynamics and relative geometry. Inter satellite communication links range from just several kilometers to well over 40,000 km. Relative motion creates a network topology that is constantly evolving relative to itself and stations on the ground. To top it off, establishing and maintaining links on spacecraft platforms is no easy feat. Dynamic routing algorithms for ground systems assume a static physical network configuration. Since that model does not work for space based mesh networks, we propose a multi-variable model that considers: best path and orbit models.

Notionally, the mesh network utilizes a hybrid distance-vector and link-state routing algorithm to discover routes between two nodes and to determine the best path to the desired end node.

Orbit models are used to create a real time mesh diagram that allows each node to find the best path with a preexisting notion of what the network looks like. Last, schedule based access is supported to account for resources. Together, the system will provide a revolutionary "smart ad hoc" dynamic routing capability.

Key functions of the routing protocol implemented by the L2SNP are route discovery and distribution of data between network nodes. A key difference from terrestrial mesh networks is that orbits are predictable, and a satellite will generally know when it is in view of another satellite. The L2SNP executes a best-path algorithm based on its real-time knowledge of the network topology, then routes the packet accordingly.

Label Switching

Once a session is established and provisioned with the desired permissions by the secure session handler, it is provided with access into the mesh transport fabric of the system. The L2SNP employs a Label Switching Protocol as the underlying mesh transport protocol. Label switching is agnostic to higher level protocols and architected to make route decisions very efficiently. We leverage this to introduce hardware based routing cores that will support well over 1 Gbps of link throughput with aggregate routing throughput of at least 10 Gbps.

The label switching protocol generates Label Switched Paths (LSP) over the network by reading routes from the routing table. The routing protocol is responsible for filling the routing table, and label switching is responsible for the actual packet transport through routes read from the routing table. After the routing protocol finds a route to the destination node, and label protocol creates a LSP over that route, a packet can move through the route by a series of labels prepended to the packet. At each node in the LSP, a Label Switch pops off the head label and uses it to forward the packet to the next hop in the LSP.

Status of Research and Path Forward

Innoflight completed Hardware-In-The-Loop (HITL) testing of the initial L2SNP prototype. The prototype software and firmware was implemented on both CFC-400X hardware and virtual machines: each CFC-400X represented the black-side networking of a space vehicle (SV) and was running L2SNP, and the each virtual machine (VM) represented a Remote Ground Station (RGS). Innoflight based the orbital planes and network connections on SDA Transport Layer Tranche 0. This initial HITL test demonstrated secure link and route establishment. Future HITL testing includes modifying orbit and connectivity assumptions to SDA Transport Layer Trance 1 and scaling the number of nodes via SV and RGS VMs. Future HITL testing also will include Multi-Protocol Label Switching (MPLS), additional cyber security and more additional routing algorithm features. This future HITL testing is not yet funded. Ultimately the goal is to demonstrate SSNCP on-orbit including software updates based on improving models using on actual KPP data.

HAMOG will begin HITL testing in 2021 including a representative commercial ground system architecture. Also in 2021 Innoflight will work with a SV partner to define how SSNCP will be integrated for an on-orbit demonstration. The HITL testing is funded, and Innoflight is pursing transition partners for the on-orbit demo.

ACKNOWLEDGMENTS

The HAMOG and L2SNP research was supported by United States Space Force Space and Missile Systems Center (USSF SMC). The authors would like to thank Lt Tyler Albright, Lt Eduardo Garza and Mr Daniel Romm for their guidance and vision through the multiple programs.

REFERENCES

1. Joint Publication (JP) 3-12 (R) Cyberspace Operations 5 Feb 2013, pg vi.
2. Brig Gen John E. Hyten, *Fighting and Winning with Space*, High Frontier (Volume 4, Number 2), Air Force Space Command, Peterson AFB, CO, Feb 2008, pg 15.
3. Image credit: Mark Handley, University College London, https://youtu.be/QEIUdMiColU.
4. Innoflight teams with Lockheed Martin on avionics for Space Development Agency Transport Layer, https://www.innoflight.com/2021/04/21/innoflight-teams-with-lockheed-martin-on-avionics-for-space-development-agency-transport-layer/.