Ensuring Flexibility and Security in SDN-Based Spacecraft Communication Networks through Risk Assessment

Dylan Z. Baker[†], Dr. Hong Liu[†], Christopher Roberts[*]

[†]*Department of Electrical and Computer Engineering*
University of Massachusetts Dartmouth

[*] *NASA Goddard Space Flight Center*

Frontier Technologies

OUTLINE

1. Overview of NASA Networks
2. SDN Integration in Space Networks
3. Flexibility vs Security Issues
4. SDN Testbed for Space Communications
5. Vulnerability Study
6. Conclusion & Future Direction

OVERVIEW OF NASA NETWORKS

Traditional Space Communication Networks

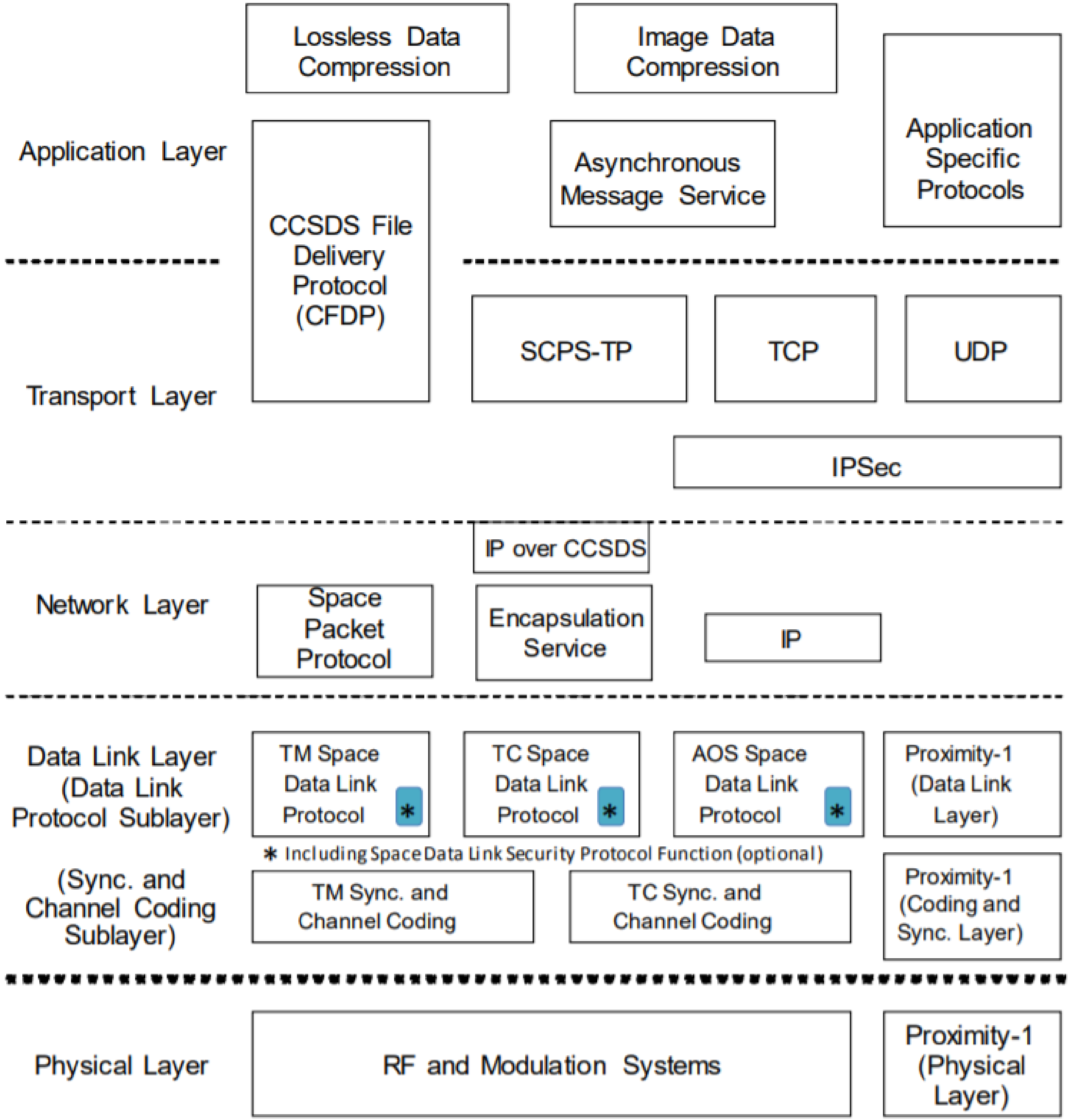
- Not fully networked (some ground networking)
  - End-to-end transmission relies on circuit switching
- RF/Microwave for ground-to-space
- “Relay satellites” (orbiting bent-pipe transponders)
- Consultative Committee for Space Data Systems (CCSDS) communications protocols
- Closed networks & manual configuration

Consultative Committee for Space Data Systems, "OVERVIEW OF SPACE COMMUNICATIONS PROTOCOLS - Green Book," Washington, DC, 2014.

M. Sanchez, D. Selva, B. Cameron, E. Crawley, A. Seas and B. Seery, "Exploring the Architectural Trade Space of NASAs Space Communication and Navigation Program," in IEEE Aerospace Conference, Big Sky MT, 2013.

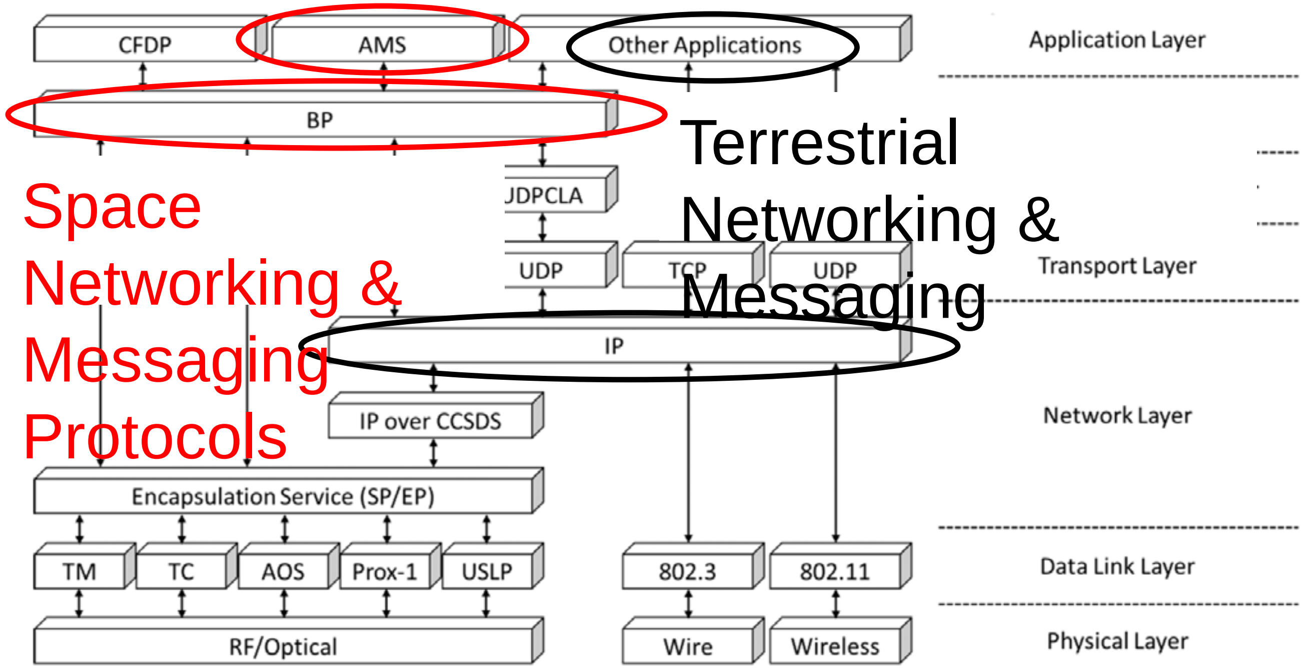
Space Communication Protocol Stack - Current

CCSDS Space Communications Reference Model ("OVERVIEW OF SPACE COMMUNICATIONS PROTOCOLS - Green Book” Fig. 2-1)



Space Communication Protocol Stack - Future

Baseline ICSIS Protocol Stack*



Bundle Protocol (CCSDS 734.2-B-1) provides "network functionality, e.g., network addressing, routing, and QoS management, in end-to-end communications environment of intermittent connectivity" enabling "multiplex/demultiplex capability to deal with multiple data streams from multiple sources over heterogeneous links." (ICSIS, Feb. 2018)

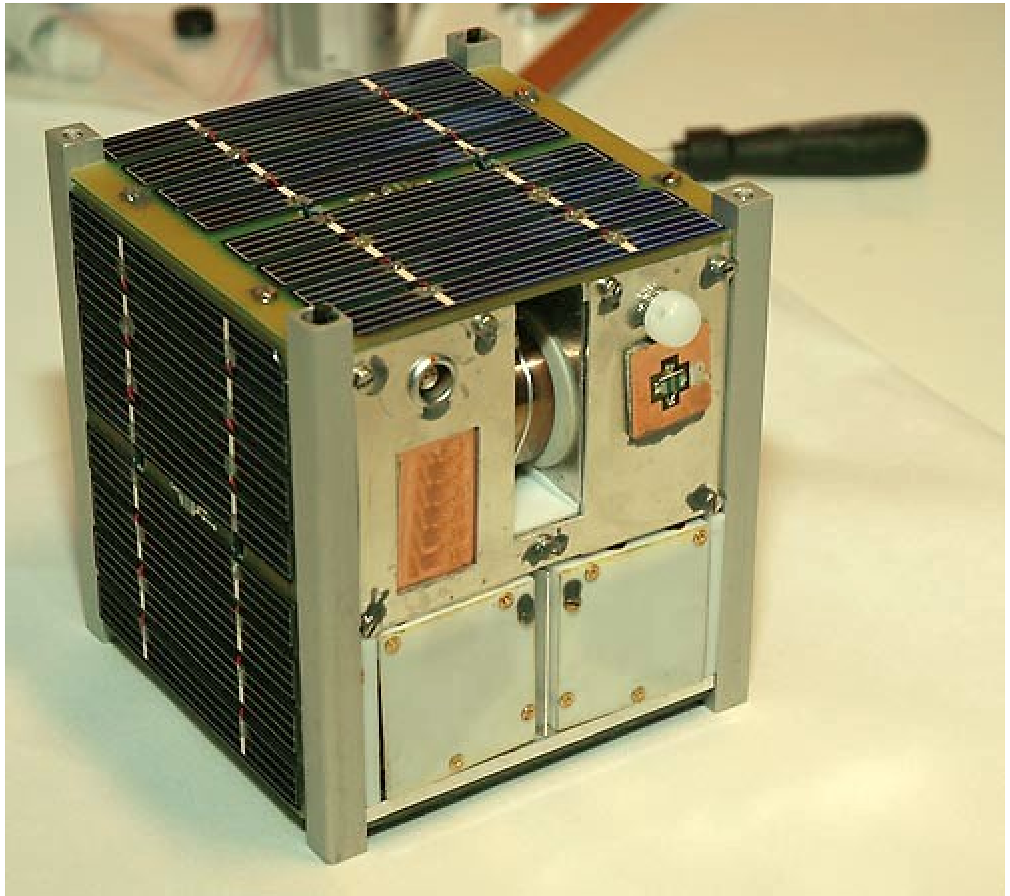
Asynchronous Message Service (CCSDS 735.1-B-1) "provides a standard, reusable infrastructure for the exchange of information among data system modules in a manner that is simple to use, highly automated, flexible, robust, scalable, and efficient. (ICSIS, Feb. 2018)

*International Communication System Interoperability Standards (ICSIS)
https://www.internationaldeepspacestandards.com/

Routable Multicast Data Flows Are Enabled by Networking; Asynchronous Messaging Enables Pub/Sub

Changes in the Space Industry

- Growing trends:
  - Commercial Space
  - SmallSats/CubeSats & large satellite constellations
- Growing communications requirements (throughput and number of nodes)



Example of a CubeSat (Pedersen)

G. J. Clark III, W. M. Eddy, S. K. Johnson, J. Barnes and D. Brooks, "Architecture for Cognitive Networking within NASA's Future Space Communications Infrastructure," in 34th AIAA International Communications Satellite Systems Conference, Cleveland, 2016.

Emerging Space Communication Trends

- New technologies driving future spacecraft missions
  - Laser Communications → Higher data rates
  - Delay/Disruption-Tolerant Networking (DTN) → Store-and-forward networking
- Integrated space communication/navigation networks
  - NASA Space Communications & Navigation (SCaN)
  - Integrating orbital, human exploration & deep-space network resources

M. Sanchez, D. Selva, B. Cameron, E. Crawley, A. Seas and B. Seery, "Exploring the Architectural Trade Space of NASAs Space Communication and Navigation Program," in IEEE Aerospace Conference, Big Sky MT, 2013.

V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall and H. Weiss, Delay-Tolerant Networking Architecture, Internet Engineering Task Force, 2007.

Future Space Networks

Software Defined Network (SDN)

- Technology used in cloud computing to abstract network resources
- Fundamentally: separates network's Control Plane from Data Plane
- Supports easier centralized network configuration through administrative applications

Role of SDN in Space Networks

- SDN can provide centralized view & control of a large space network for network managers and mission operators
- Time-dependent relay/antenna distribution & beamforming
- On-demand routing

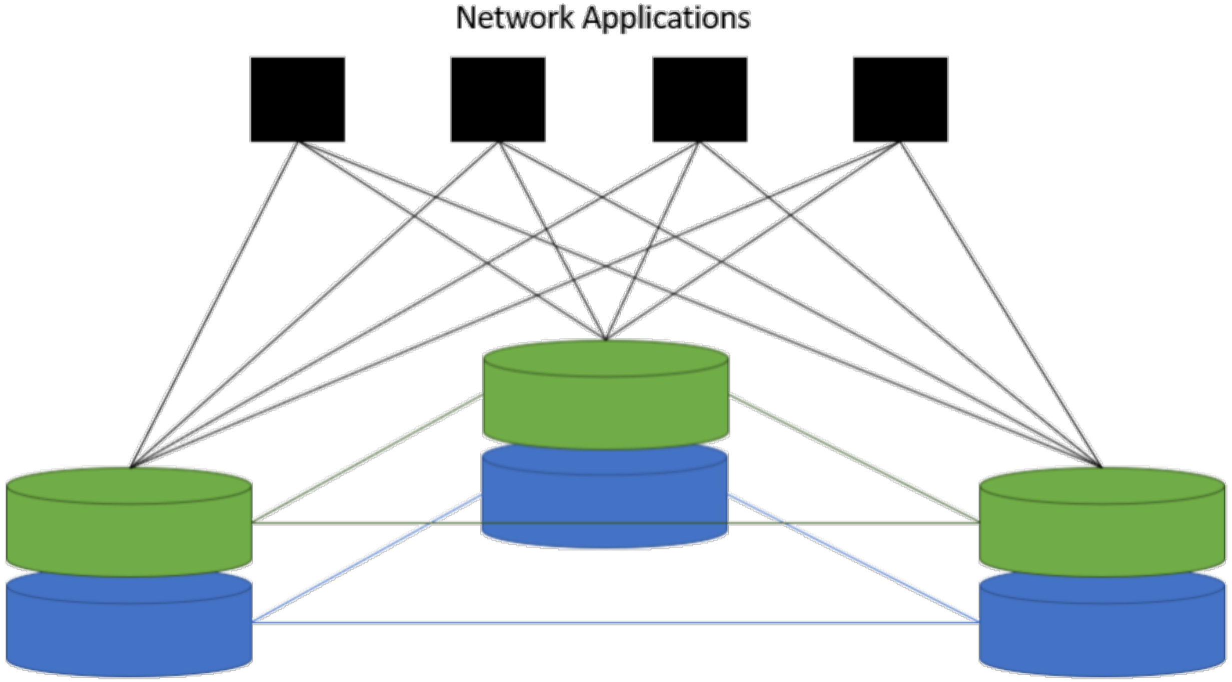
B. Barritt and V. Cerf, "Loon SDN: Applicability to NASA's Next-Generation Space Communications Architecture," in 2018 IEEE Aerospace Conference, Big Sky MT, 2018.

T. Li, H. Zhou, H. Luo and S. Yu, "SERvICE: A Software Defined Framework for Integrated Space-Terrestrial Satellite Communication," IEEE Transactions on Mobile Computing, vol. 17, no. 3, pp. 703-716, 2018.

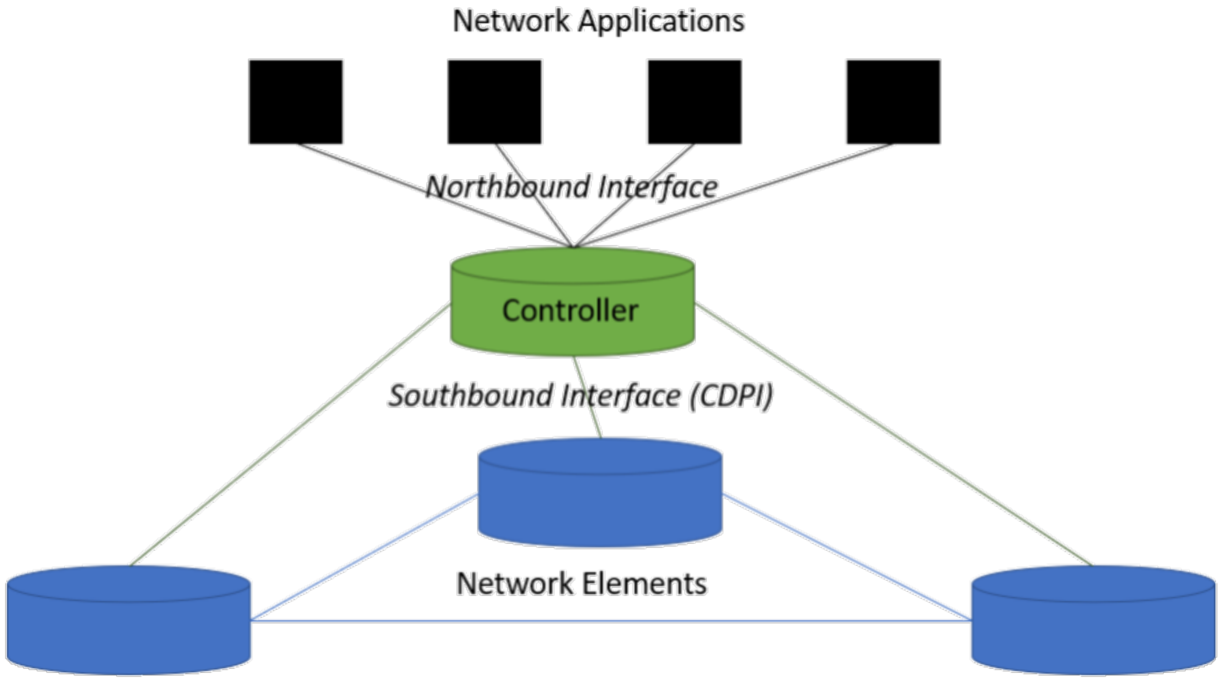
SDN INTEGRATION IN SPACE NETWORKS

Introduction to SDN

Without SDN

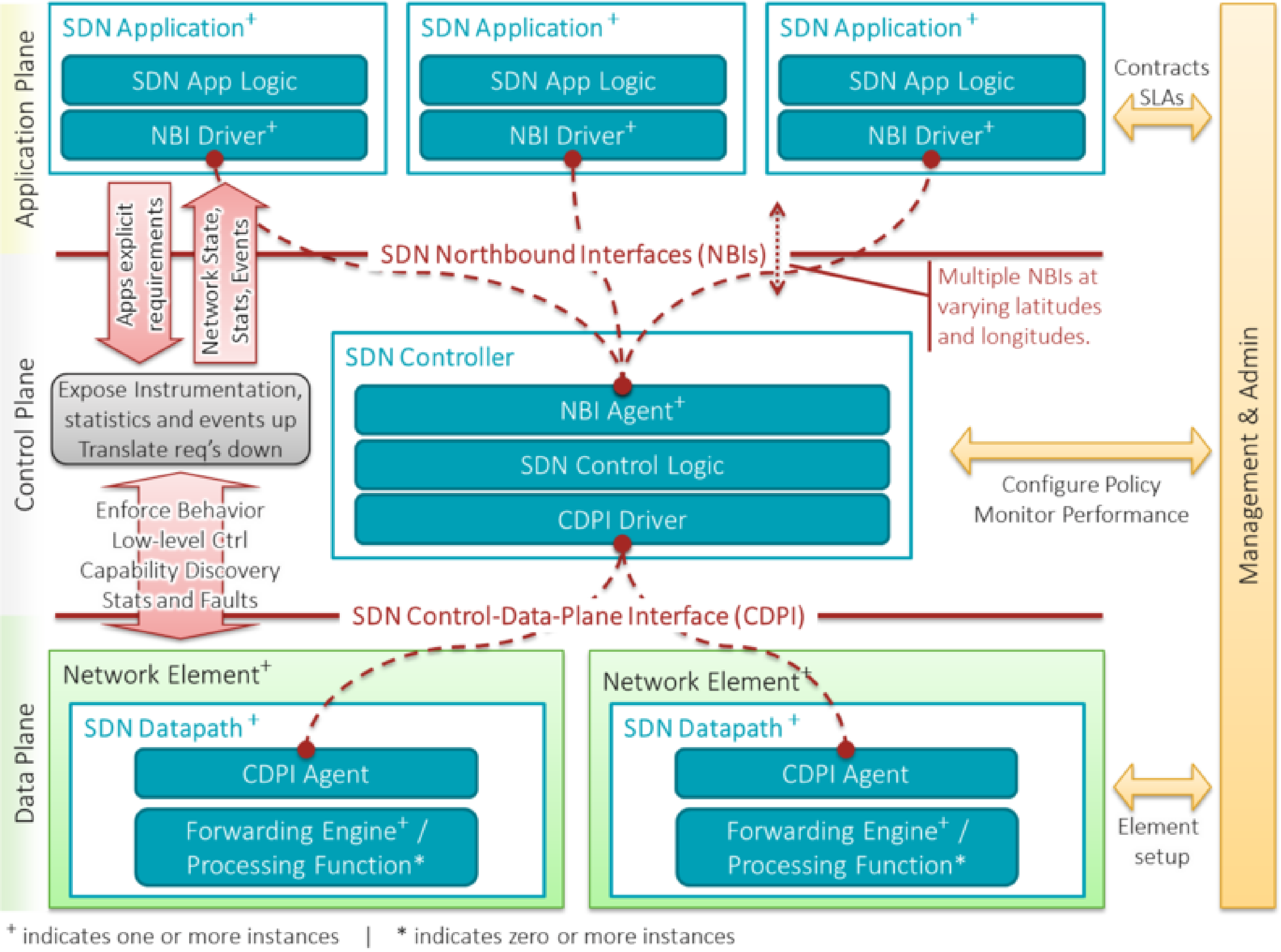


With SDN



Open Networking Foundation (ONF), "SDN Architecture Overview," Open Networking Foundation (ONF), 2013.

Introduction to SDN (cont.)



Logical Architecture of SDN (ONF Fig. 1)

Commercial SDN

- Open Networking Foundation (ONF): OpenFlow CDPI protocol
  - Enable/disable ports, modify QoS settings
  - Controller implementations: OpenDaylight, Ryu, Open Network Operating System (ONOS)
- Google: Espresso SDN routing infrastructure
- Cisco: Application Centric Infrastructure (ACI)

Cisco Systems, "Application Centric Infrastructure - Cisco," [Online]. Available: https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html. [Accessed 6 July 2019].

K.-K. Yap, M. Motiwala, J. Rahe, S. Padgett, M. Hilliman, G. Baldus, M. Hines, T. Kim, A. Narayan, A. Jain, V. Lin, C. Rice, B. Rogan, A. Singh, B. Tanaka, M. Verma, P. Sood, M. Tariq, M. Tierney, D. Trumic, V. Valancius, C. Ying, M. Kallahalla, B. Koley and A. Vahdat, "Taking the Edge off with Espresso: Scale, Reliability and Programmability for Global Internet Peering," in SIGCOMM, Los Angeles, 2017.

S. Scott-Hayward, S. Natarajan and S. Sezer, "A Survey of Security in Software Defined Networks," IEEE Communication Surveys & Tutorials, vol. 18, no. 1, pp. 623-654, 2016.

SDN Security Studies and Solutions

- Security Advantages/Capabilities:
  - Security policy & service deployment
  - Cyber forensics
  - Realtime intrusion detection & mitigation
- Security Challenges
  - DoS attacks on controller
    - AVANT-GUARD throttles control plane data to prevent this
    - CPRecovery controller failover
  - Malicious flow alteration
    - Trust systems and role-based authentication

G. Yao, J. Bi and P. Xiao, "Source Address Validation Solution with OpenFlow/NOX Architecture," in 19th IEEE International Conference on Network Protocols, Vancouver, 2011.

S. Scott-Hayward, S. Natarajan and S. Sezer, "A Survey of Security in Software Defined Networks," IEEE Communication Surveys & Tutorials, vol. 18, no. 1, pp. 623-654, 2016.

S. Shin, V. Yegneswaran, P. Porras and G. Gu, "AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks," in ACM Computer and Communications Security Conference (CCS), Berlin, 2013.

Integrating Space Communications

- NASA SCaN Program
  - Near-Earth Network (NEN), Deep Space Network (DSN) & Space Network (SN)
- Federated Satellite System
  - Distributed spacecraft collaborating to provide services
- Cognitive Networking
  - Identification & autonomous handling of network conditions
- Delay/Disruption-Tolerant Networking (DTN)
  - Internet-like networking across interplanetary distances (RFC 4838)
  - Bundle Protocol (BP)/RFC 5050: Transmitting “bundles” using store-and-forward paradigm

G. J. Clark III, W. M. Eddy, S. K. Johnson, J. Barnes and D. Brooks, "Architecture for Cognitive Networking within NASA’s Future Space Communications Infrastructure," in 34th AIAA International Communications Satellite Systems Conference, Cleveland, 2016.

K. Scott and S. Burleigh, Bundle Protocol Specification, Internet Engineering Task Force, 2007.

M. Sanchez, D. Selva, B. Cameron, E. Crawley, A. Seas and B. Seery, "Exploring the Architectural Trade Space of NASAs Space Communication and Navigation Program," in IEEE Aerospace Conference, Big Sky MT, 2013.

Sanchez Net, Marc, et al. "Architecting Information Security Services for Federated Satellite Systems." Journal of Aerospace Information Systems 14.8 (2017): 439-450.

V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall and H. Weiss, Delay-Tolerant Networking Architecture, Internet Engineering Task Force, 2007.

SDN For Space Networks

- Temporospatial SDN
  - Google Project Loon: Network nodes moving with respect to time & space
- Software Defined Naval Network for Satellite Communications (SDN-SAT)
  - U.S. Navy: Using OpenFlow & MPTCP to support satellite-based ship navigational networks
- Software dEfined fRamework for Integrated space tErrestrial satellite Communication (SERvICE)
  - China National Basic Research Program: Using SDN with NFV for satellite communications

B. Barritt and V. Cerf, "Loon SDN: Applicability to NASA's Next-Generation Space Communications Architecture," in 2018 IEEE Aerospace Conference, Big Sky MT, 2018.

S. Nazari, P. Du, M. Gerla, C. Hoffman, J. H. Kim and A. Capone, "Software Defined Naval Network for Satellite Communications (SDN-SAT)," in IEEE Military Communications Conference, Baltimore, 2016.

T. Li, H. Zhou, H. Luo and S. Yu, "SERvICE: A Software Defined Framework for Integrated Space-Terrestrial Satellite Communication," IEEE Transactions on Mobile Computing, vol. 17, no. 3, pp. 703-716, 2018.

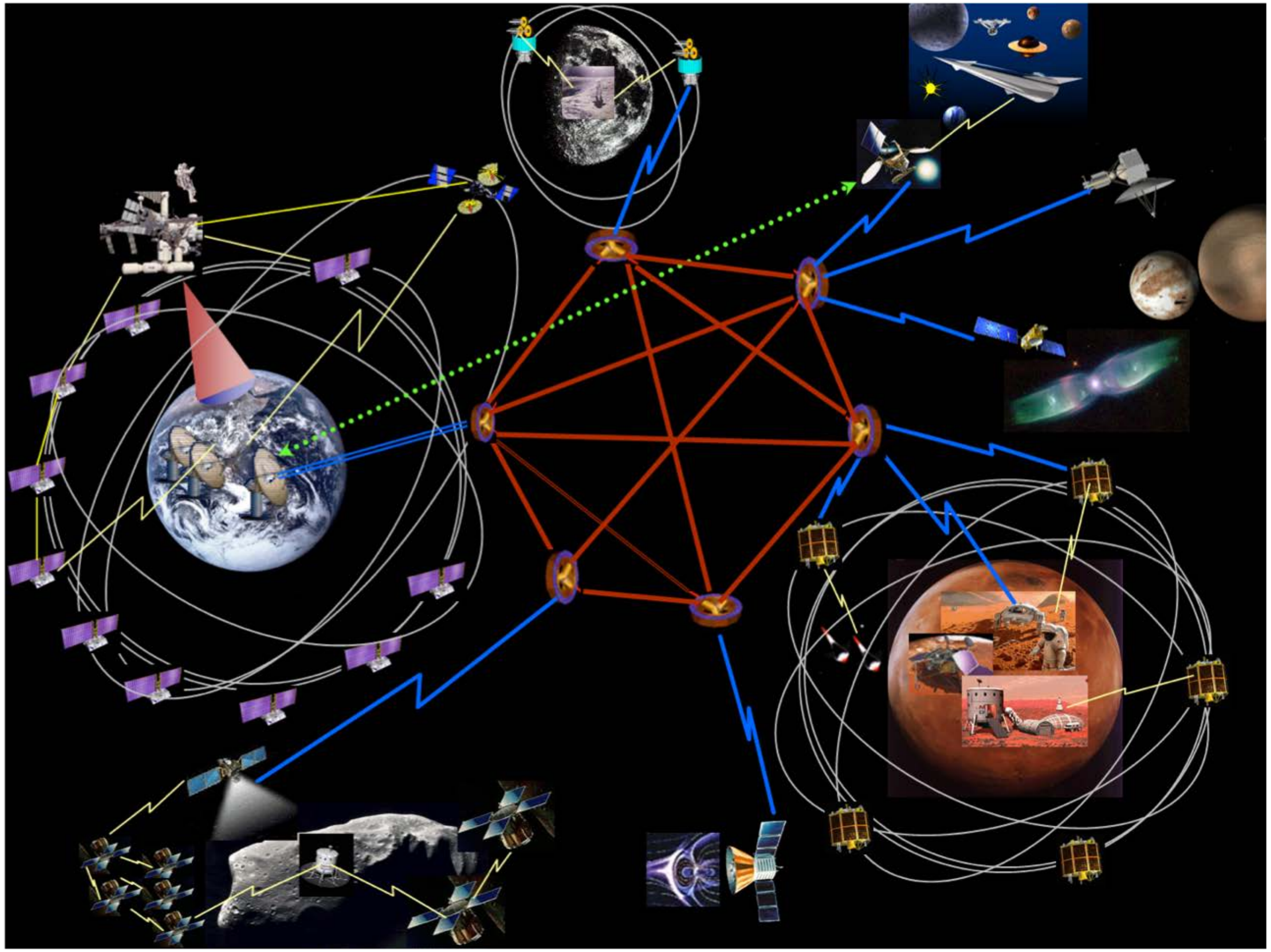
FLEXIBILITY VS SECURITY ISSUES

Combined Space Communication Networks (Near-Term)

- Diverse customers and missions using shared network resources, ranging from universities to human exploration
- Higher data requirements & larger number of nodes
- Scaling circuit-switched network segments may no longer be feasible

Solar System Internet (Long-Term)

- Long-term, space networking nodes may be distributed across the Solar System
- As with Internet, traffic may be forwarded through nodes unknown to endpoints



Depiction of a Solar System Internet ("Interplanetary Internet")

Limits to the Current Space Network Architecture

- Circuit switching requires dedicated connections
  - Packet switching: fuller bandwidth utilization
  - Increased connections & lower bandwidth utilization: higher cost
- Manual configuration & control: scalability challenges

SDN as a Solution

- Packet-switched networking & centralized network control
- Scalable with hierarchical controllers
- Synchronized spacecraft commanding & transponder control
- Automatic network reconfiguration
  - Traffic rerouting during cloud occlusion

Impact of an Open Network Architecture on Security

- Interconnected networks create more attack vectors
  - More interconnected nodes
  - A single compromise can have a greater reach
- Decoupled & centralized control plane can result in single point-of-failure

SDN TESTBED FOR SPACE COMMUNICATIONS

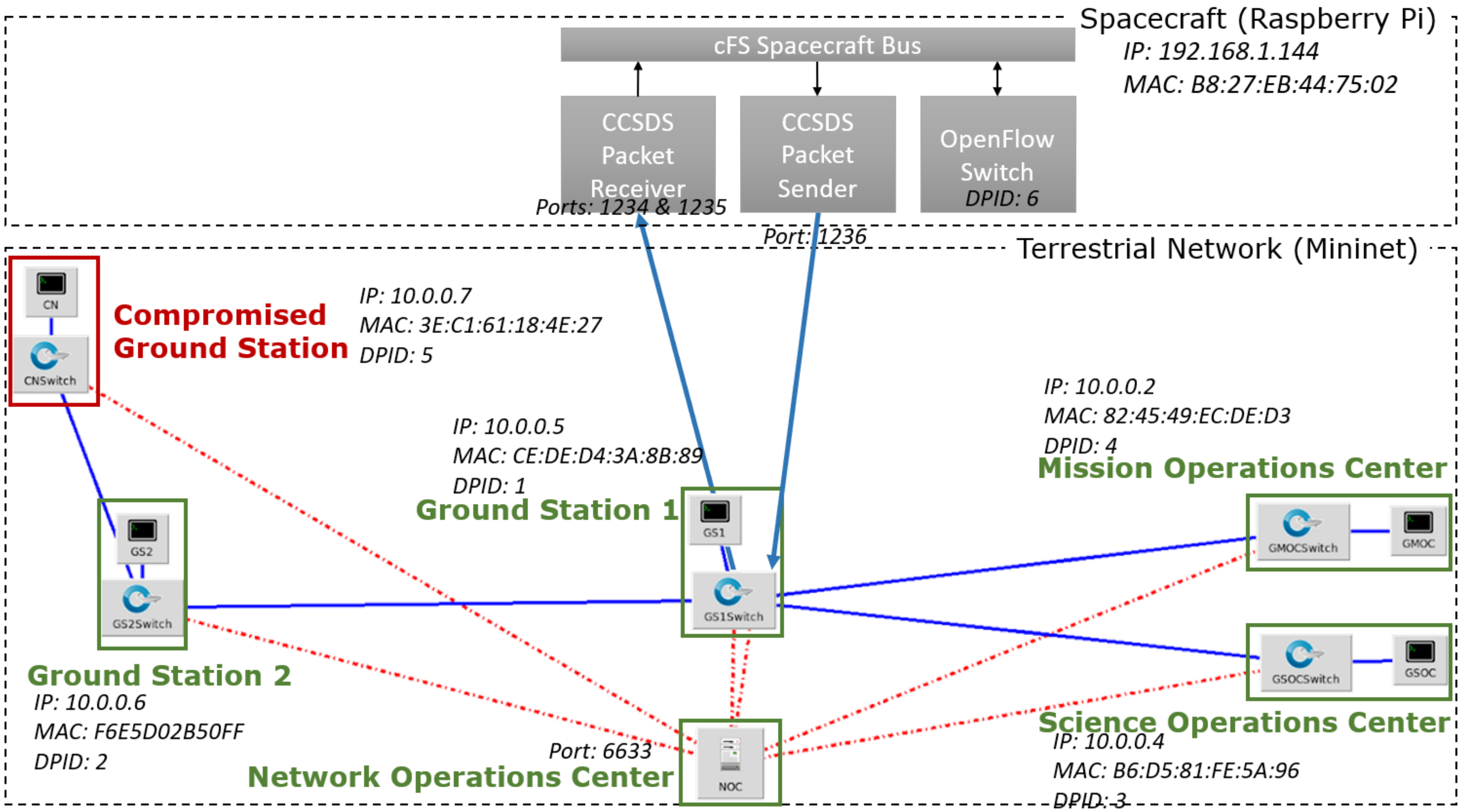
Experiment Environment Setup: Testbed with Mininet

- Mininet: Open-source network emulation tool
  - Uses Linux Kernel’s network stack
  - Capable of running real network device software/firmware
- SDN testbed:
  - Ground switches (OpenFlow)
  - OpenFlow controller
  - Raspberry Pi w/ core Flight System (cFS) & OpenFlow switch

Mininet, "Mininet: An Instant Virtual Network on your Laptop (or other PC)," [Online]. Available: mininet.org. [Accessed 13 July 2019].

National Aeronautics and Space Administration, "core Flight System: A paradigm shift in flight software development," 28 February 2019. [Online]. Available: https://cfs.gsfc.nasa.gov/. [Accessed 7 July 2019].

Experiment Environment Setup: Testbed with Mininet (cont.)



Mininet testbed topology

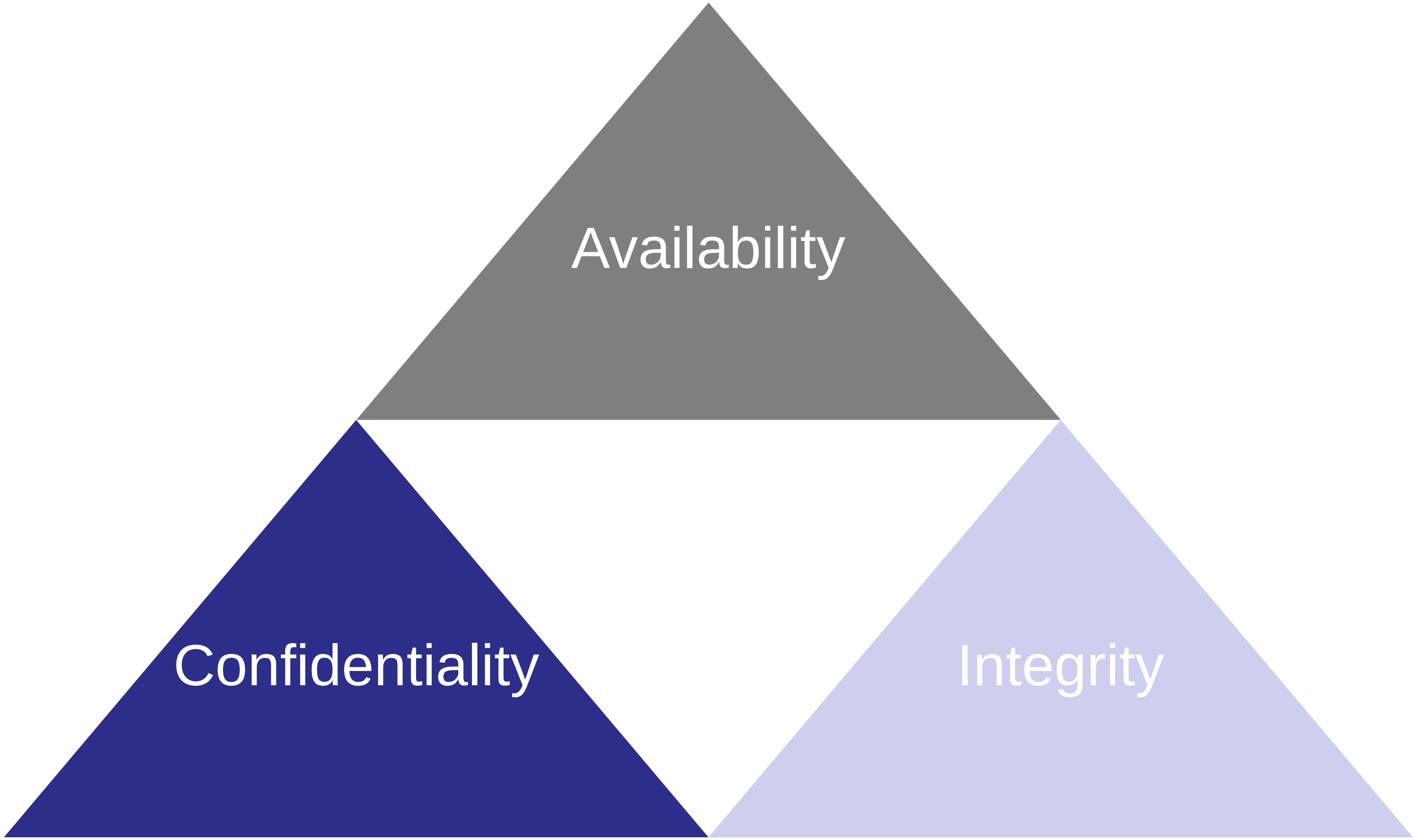
VULNERABILITY STUDY

ISO 27000 Series

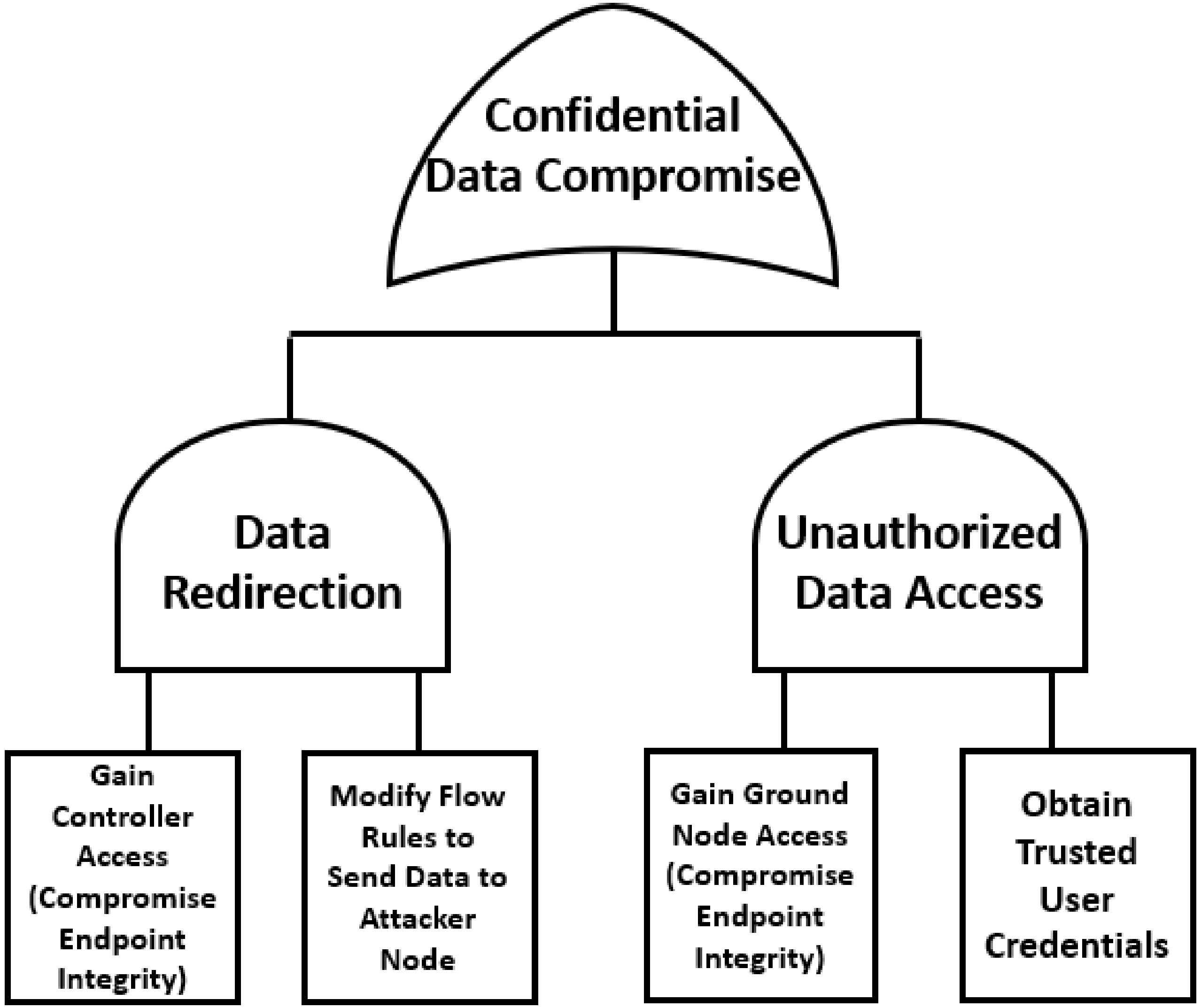
- ISO/IEC 27000 Series of Standards on IT Security Techniques

- Assets:
  - Ground stations & relays
  - Operations centers (mission, science, network)
  - Network
  - Data
  - Spacecraft

C.I.A. Triad

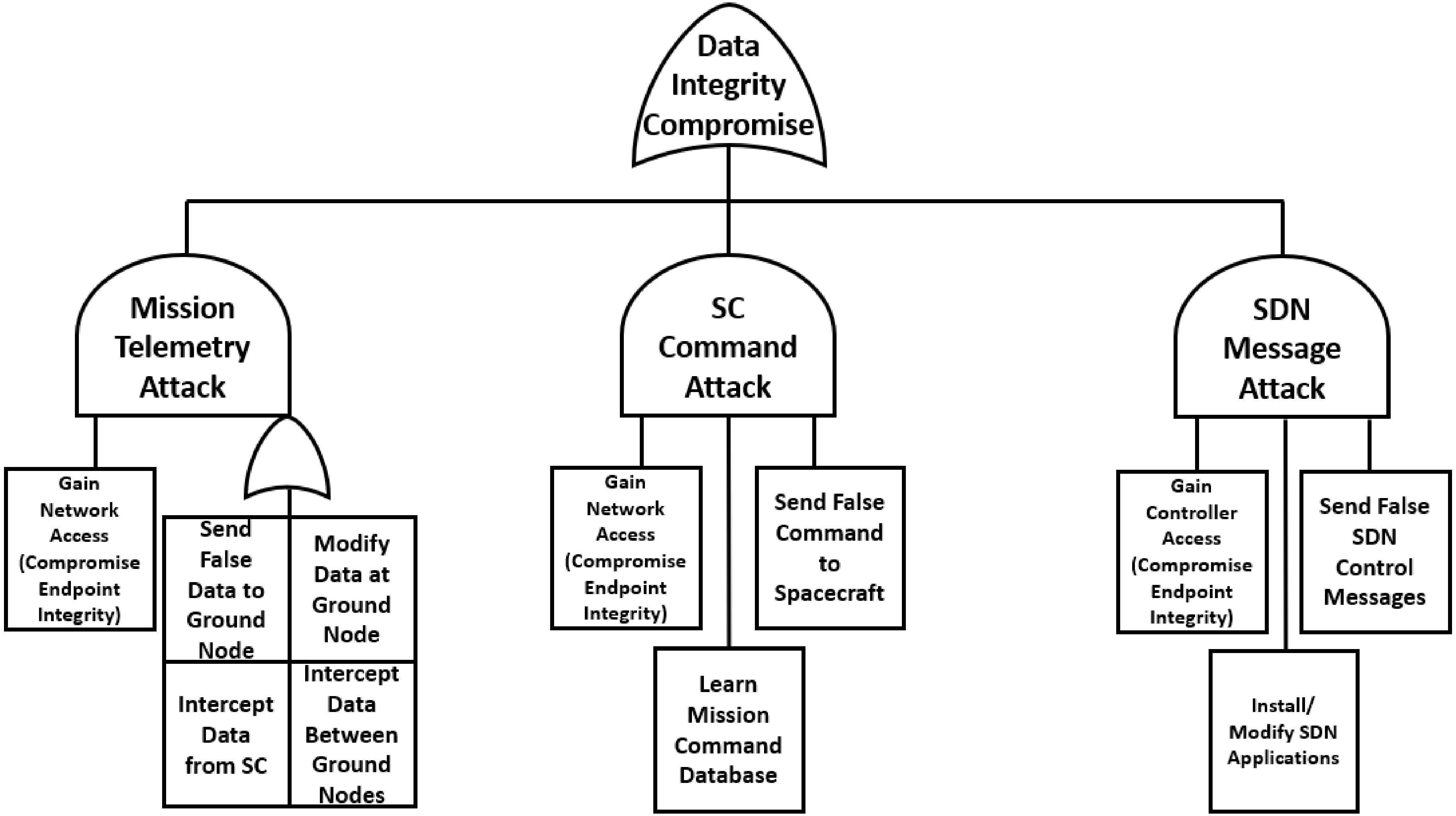


Confidentiality



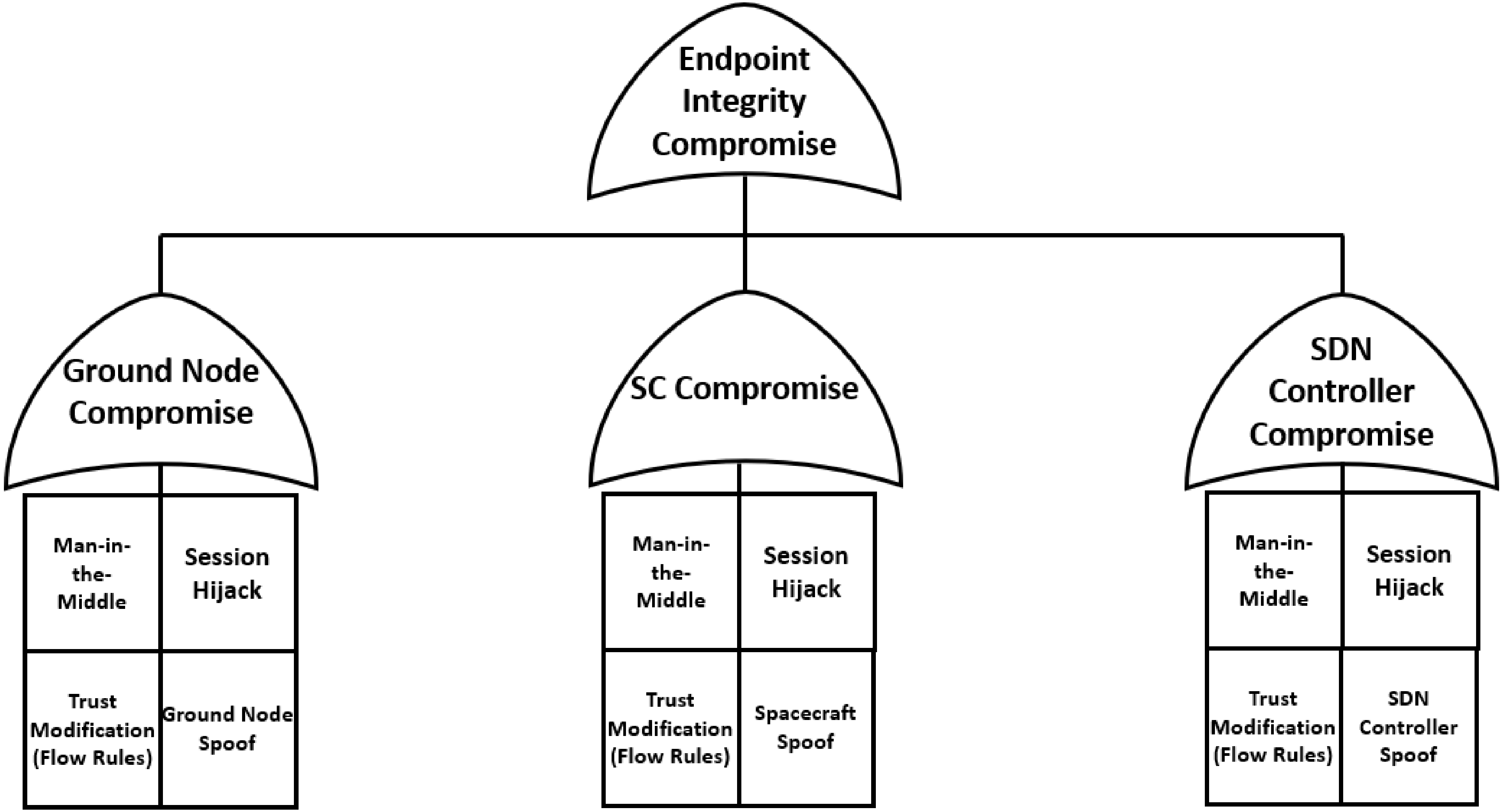
Attack tree for a confidentiality compromise.

Data Integrity



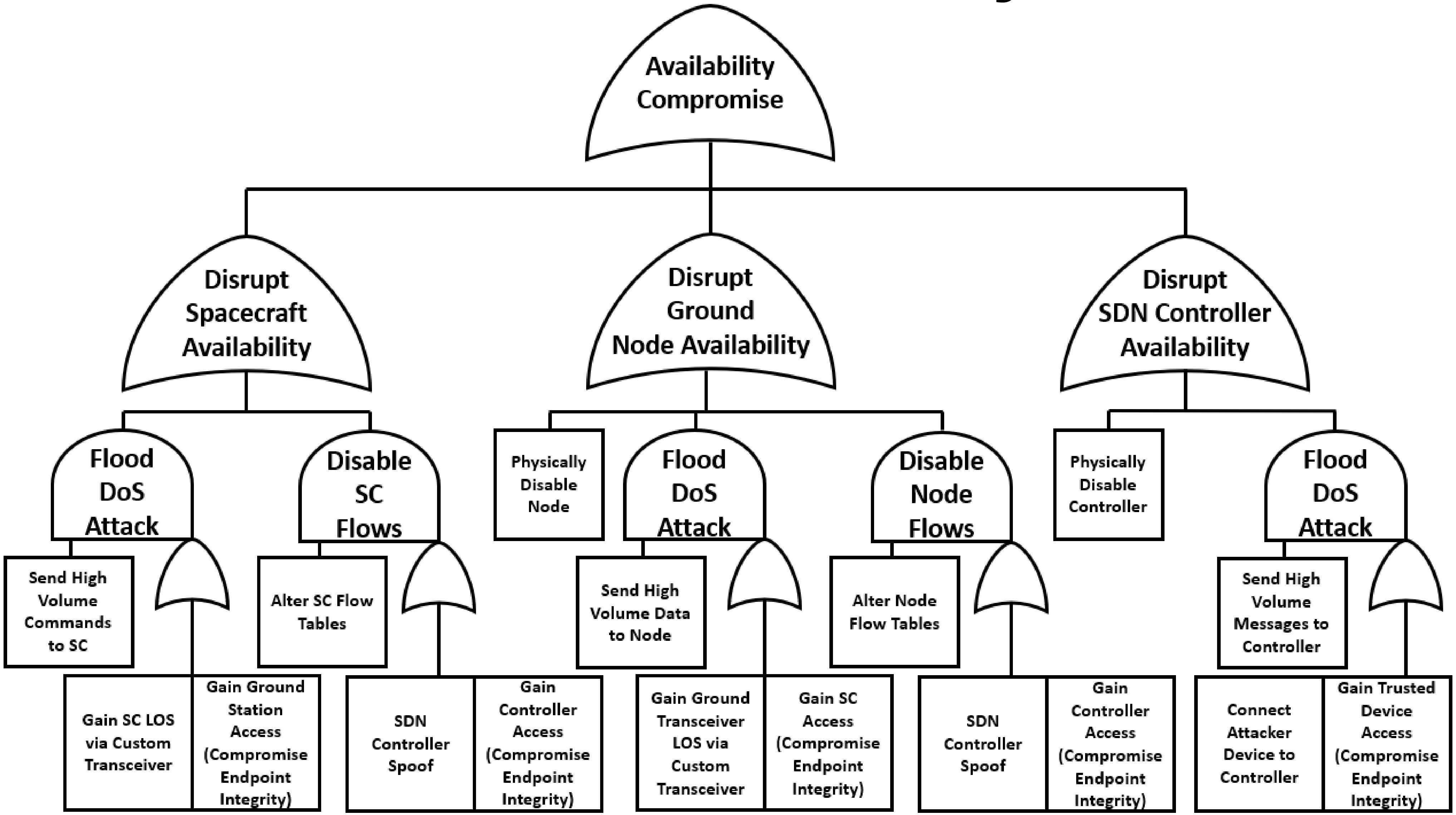
Attack tree for a data integrity compromise.

Endpoint Integrity



Attack tree for an endpoint integrity compromise.

Availability



Attack tree for an availability compromise.

Risk Register

Table 1: Classification of risks to spacecraft and associated assets

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability, availability and integrity of spacecraft	***Attacks/errors affecting spacecraft (i.e. DoS)***	***Space Data Link security; direct connection; command verification***	***Rare***	***Catastrophic/ Doomsday***	***Extreme***	***1***
Integrity and availability of ground nodes	Attacks/errors affecting ground nodes	Space Data Link security	Unlikely	Moderate	Medium	2
Confidentiality of spacecraft telemetry/ commands	Interception of telemetry or commands	Data encryption	Unlikely	Moderate	Medium	3
Integrity of spacecraft commands	Corruption or loss of command data	Error Detection & Correction codes	Possible	Minor	Medium	4

Risk Register (cont.)

Table 1: Classification of risks to spacecraft and associated assets

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Integrity of spacecraft telemetry	Corruption or loss of telemetry data	Error Detection & Correction Codes	Possible	Minor	Medium	5
Integrity and availability of SDN controller	***Attacks/errors affecting controller; corruption/loss of SDN control messages***	***Configuration; controller authentication***	***Possible***	***Moderate***	***High***	***6***

- 2 New Risks in SDN-based spacecraft network:
  - Spacecraft Availability
  - SDN Controller Integrity/Availability

Availability Challenges

- Spacecraft could be susceptible to DoS attacks
- Invalid messages sent to spacecraft at high data rate will consume clock cycles
- Compromised control plane can be made to flood spacecraft with messages or disconnect spacecraft

Controller Integrity and Availability

- Controller Integrity Compromise: Inauthentic controller and/or messages
  - Attacker has control over network configuration
- Loss of Controller Availability: Controller unable to update network configuration
  - No Control Plane functionality
- Vulnerabilities also prevalent in terrestrial SDN
  - AVANT-GUARD & CPRecovery
  - Trust Systems & Role-based Authentication

Need for DoS Attack-Resilient System

- Although rare, spacecraft DoS could be catastrophic
  - Asset Destruction
  - Mission Failure
  - Loss-of-Life
- Decreasing attack likelihood alone insufficient
- Detection and real-time DoS attack mitigation
  - Flow Sampling
  - Quality-of-Service (QoS)/network throttling

CONCLUSION & FUTURE DIRECTION

DoS and Control Plane Attacks

- Vulnerability study: these two attacks not handled by existing space networking security controls
- Impact of DoS attack on space systems makes DoS resiliency necessary
- Decoupled Control Plane → potential new vulnerabilities
  - Mitigation mechanisms (i.e. trust systems, role-based access control) for terrestrial implementations can apply

Future Work

- Controller-based active DoS attack mitigation
  - Flow sampling, heuristics
  - Network-wide attack handling
- Non-terrestrial SDN protocol implementation
- Flight hardware testing and hardware acceleration

Bibliography

B. Barritt and V. Cerf, "Loon SDN: Applicability to NASA's Next-Generation Space Communications Architecture," in 2018 IEEE Aerospace Conference, Big Sky MT, 2018.

Consultative Committee for Space Data Systems, "OVERVIEW OF SPACE COMMUNICATIONS PROTOCOLS - Green Book," Washington, DC, 2014.

Cisco Systems, "Application Centric Infrastructure - Cisco," [Online]. Available: https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html. [Accessed 6 July 2019].

G. J. Clark III, W. M. Eddy, S. K. Johnson, J. Barnes and D. Brooks, "Architecture for Cognitive Networking within NASA's Future Space Communications Infrastructure," in 34th AIAA International Communications Satellite Systems Conference, Cleveland, 2016.

G. Yao, J. Bi and P. Xiao, "Source Address Validation Solution with OpenFlow/NOX Architecture," in 19th IEEE International Conference on Network Protocols, Vancouver, 2011.

K.-K. Yap, M. Motiwala, J. Rahe, S. Padgett, M. Hilliman, G. Baldus, M. Hines, T. Kim, A. Narayan, A. Jain, V. Lin, C. Rice, B. Rogan, A. Singh, B. Tanaka, M. Verma, P. Sood, M. Tariq, M. Tierney, D. Trumic, V. Valancius, C. Ying, M. Kallahalla, B. Koley and A. Vahdat, "Taking the Edge off with Espresso: Scale, Reliability and Programmability for Global Internet Peering," in SIGCOMM, Los Angeles, 2017.

K. Scott and S. Burleigh, Bundle Protocol Specification, Internet Engineering Task Force, 2007.

M. Sanchez, D. Selva, B. Cameron, E. Crawley, A. Seas and B. Seery, "Exploring the Architectural Trade Space of NASAs Space Communication and Navigation Program," in IEEE Aerospace Conference, Big Sky MT, 2013.

Mininet, "Mininet: An Instant Virtual Network on your Laptop (or other PC)," [Online]. Available: mininet.org. [Accessed 13 July 2019].

National Aeronautics and Space Administration, Artist, Interplanetary Internet. [Art]. 2018.

National Aeronautics and Space Administration, "core Flight System: A paradigm shift in flight software development," 28 February 2019. [Online]. Available: https://cfs.gsfc.nasa.gov/. [Accessed 7 July 2019].

Bibliography (cont.)

Open Networking Foundation (ONF), "SDN Architecture Overview," Open Networking Foundation (ONF), 2013.

Pedersen, Bjørn. NCube2. European Space Agency. 2007.

S. Nazari, P. Du, M. Gerla, C. Hoffman, J. H. Kim and A. Capone, "Software Defined Naval Network for Satellite Communications (SDN-SAT)," in IEEE Military Communications Conference, Baltimore, 2016.

S. Scott-Hayward, S. Natarajan and S. Sezer, "A Survey of Security in Software Defined Networks," IEEE Communication Surveys & Tutorials, vol. 18, no. 1, pp. 623-654, 2016.

S. Shin, V. Yegneswaran, P. Porras and G. Gu, "AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks," in ACM Computer and Communications Security Conference (CCS), Berlin, 2013.

Sanchez Net, Marc, et al. "Architecting Information Security Services for Federated Satellite Systems." Journal of Aerospace Information Systems 14.8 (2017): 439-450.

G. J. Clark III, W. M. Eddy, S. K. Johnson, J. Barnes and D. Brooks, "Architecture for Cognitive Networking within NASA's Future Space Communications Infrastructure," in 34th AIAA International Communications Satellite Systems Conference, Cleveland, 2016.

T. Li, H. Zhou, H. Luo and S. Yu, "SERvICE: A Software Defined Framework for Integrated Space-Terrestrial Satellite Communication," IEEE Transactions on Mobile Computing, vol. 17, no. 3, pp. 703-716, 2018.

V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall and H. Weiss, Delay-Tolerant Networking Architecture, Internet Engineering Task Force, 2007.

Ensuring Flexibility and Security in SDN-Based Spacecraft Communication Networks through Risk Assessment

Dylan Z. Baker[†], Dr. Hong Liu[†], Christopher Roberts[*]

[†]*Department of Electrical and Computer Engineering*
University of Massachusetts Dartmouth

[*] *NASA Goddard Space Flight Center*

Frontier Technologies

THANK YOU **QUESTIONS?**