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


Space Communication Protocol Stack - Current

CCSDS Space Communications Reference Model ("OVERVIEW OF SPACE COMMUNICATIONS PROTOCOLS - Green Book" Fig. 2-1)
Routable Multicast Data Flows Are Enabled by Networking; Asynchronous Messaging Enables Pub/Sub

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

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)
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)

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


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


SDN INTEGRATION IN SPACE NETWORKS
Introduction to SDN

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)


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

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

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

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
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

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

- Availability
- Confidentiality
- Integrity
Confidentiality

Confidential Data Compromise

Data Redirection
- Gain Controller Access (Compromise Endpoint Integrity)
- Modify Flow Rules to Send Data to Attacker Node

Unauthorized Data Access
- Gain Ground Node Access (Compromise Endpoint Integrity)
- Obtain Trusted User Credentials

Attack tree for a confidentiality compromise.
Data Integrity

Attack tree for a data integrity compromise.
Attack tree for an endpoint integrity compromise.
Availability

Availability Compromise

Disrupt Spacecraft Availability
- Flood DoS Attack
  - Send High Volume Commands to SC
  - Gain SC LOS via Custom Transceiver
  - SDN Controller Spoof (Compromise Endpoint Integrity)

Disrupt Ground Node Availability
- Disable SC Flows
  - Alter SC Flow Tables
  - SDN Controller Access (Compromise Endpoint Integrity)
- Physically Disable Node
  - Gain Ground Station Access (Compromise Endpoint Integrity)

Disrupt SDN Controller Availability
- Disable Node Flows
  - Alter Node Flow Tables
  - Gain Controller Access (Compromise Endpoint Integrity)
  - Gain SC Access (Compromise Endpoint Integrity)
- Physically Disable Controller
  - SDN Controller Spoof
  - Gain Ground Transceiver LOS via Custom Transceiver

Flood DoS Attack
- Send High Volume Data to Node
  - Gain Controller Access (Compromise Endpoint Integrity)
  - Connect Attacker Device to Controller
  - Gain Trusted Device Access (Compromise Endpoint Integrity)

Attack tree for an availability compromise.
## Risk Register

### Table 1: Classification of risks to spacecraft and associated assets

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

Table 1: Classification of risks to spacecraft and associated assets

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

- 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


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

Pedersen, Bjørn. NCube2. European Space Agency. 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?