

Security Considerations for Space Settings

IETF Security Area Open Meeting

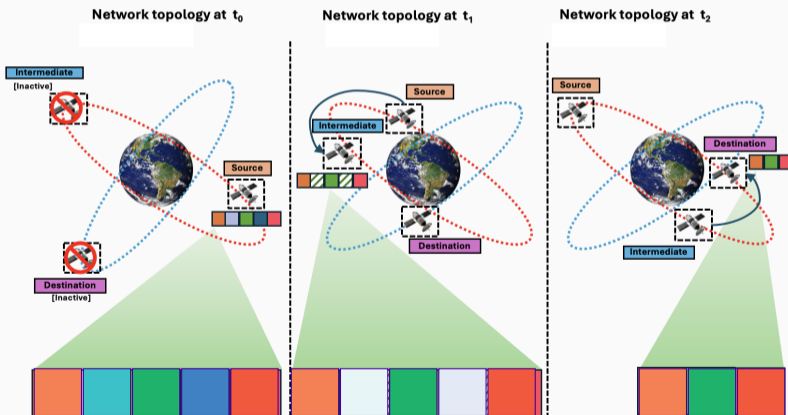
Benjamin Dowling

March 20, 2026

benjamin.dowling@kcl.ac.uk

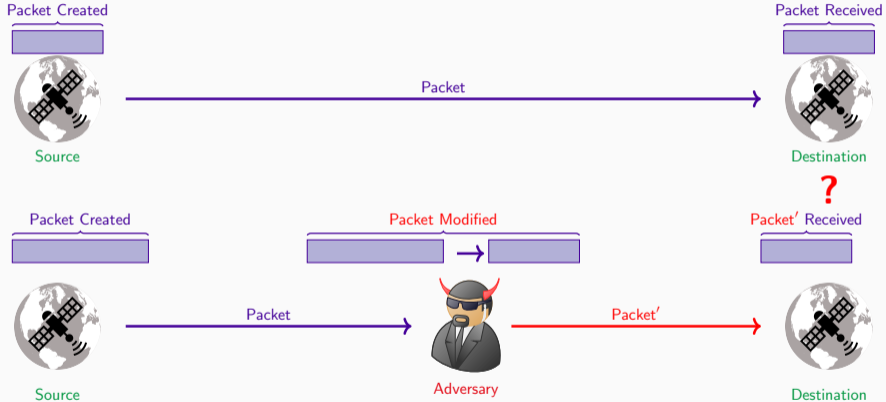
Functional Requirements

“Until full coverage..., the orbiters and other assets that are facing intermittent communications should provide store-and-forward capability.” - IP in Deep Space: Key Characteristics, Use Cases and Requirements



Security Requirements

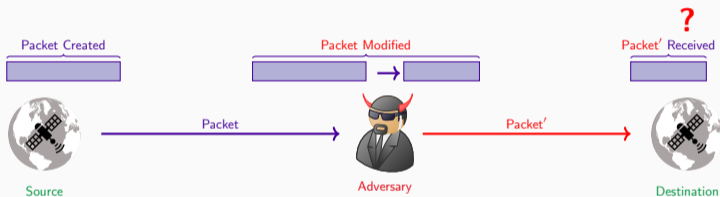
Need a mechanism to ensure confidentiality / authenticity.



But these properties can be quite fine-grained. Will address soon!

Realistic Threat Model?

“... over time **it is possible that connectivity to the Internet may become available** for some mission assets, and eventually interplanetary networks could become part of the Internet.”

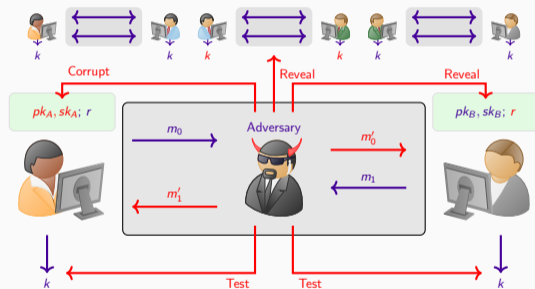


“Space exploration is more than ever carried by multiple stakeholders. A mixture of assets operated by government, commercial, and academic/research organizations **from multiple nations** are deployed.” - **IP in Deep Space: Key Characteristics, Use Cases and Requirements**

Threat Modelling for Space

Security properties inform the design of the protocols we will use. What is an appropriate threat model? Typically, in the analysis of real-world cryptographic protocols (TLS, SSH, Signal, etc) we tend to consider security against an attacker that:

- is in complete control of the network,
 - Cryptographic modelling norm for network adversaries
- can **Compromise** derived keys k ,
- can **Corrupt** long-term secrets (pk, sk) ,
- can **Exploit** bad randomness r



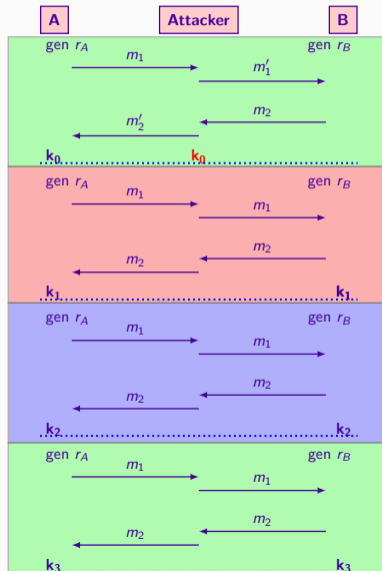
Threat: Network adversary capable of compromising one or more of the endpoints. Security should be resilient against such an adversary.

Fine-grained Security Considerations

Secure Channel protocols today realise advanced security properties:

- **Perfect Forward Secrecy**
 - The adversary cannot read ciphertexts sent before a compromise.
- **Post Compromise Security**
 - The adversary cannot read ciphertexts sent after a “healing” period post-compromise.

Both consider security in the face of adversary compromise, and both are standard expectations of security for long-lived protocols, such as those used in the space setting.

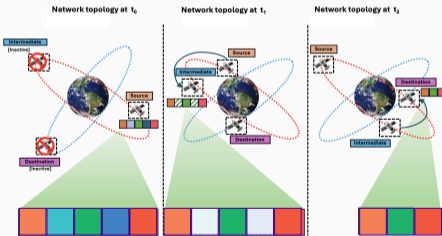


Space Setting Challenges

“Compared to Internet on Earth, deep space communications and networking have multiple challenges, such as:

- **Significant and variable delays** (e.g. ... multiple seconds, minutes, or hours).
- **Frequent and long interruptions** of communications, often with no alternate path.”

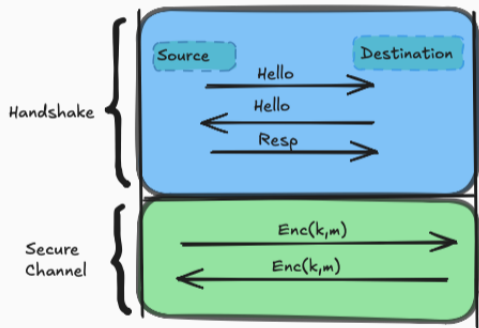
- IP in Deep Space: Key Characteristics, Use Cases and Requirements



Packet loss is even more difficult to address in space setting, since the **delays and interruptions** hide whether packet loss occurred (and lead to incomplete secure channel establishment).

Handshakes and Packet Loss

To achieve confidentiality and authentication, we need to establish keys for secure communication. In secure communication these are typically called handshakes



Any delay or dropping of packets prevents key establishment.

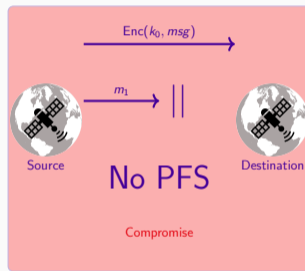
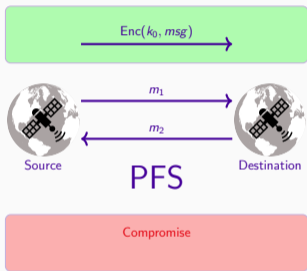
Let's assume you have some probability of packet loss P_{pl} . Logically, as the number of messages in the handshake increases, then so too does the probability of the handshake failing due to packet loss:

$$(1 - P_{pl}), (1 - P_{pl})^2, (1 - P_{pl})^3, \dots$$

Thus, **delays or dropping** of handshake messages **extends impact of compromise** due to delayed secure payload communication.

Impact of Delay/Dropping on Security

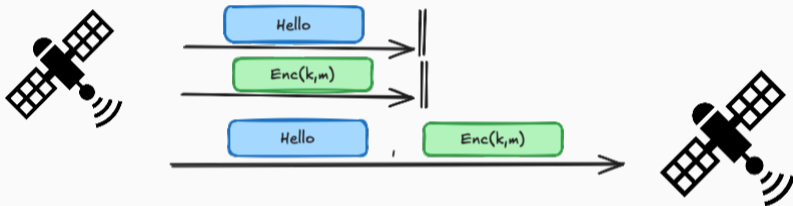
Any delay in a handshake extends the window/impact of compromise.



More communication needed to establish goals gives more changes for delays to key refresh, and thus extends the impact of compromise.

Async vs Sync Handshakes

Asynchronous support allows for entities to be offline, thus massive delays in handshake messages can be resolved.



Asynchronous handshakes allow for key establishment (and key refresh) without both parties being interactive.

This allows for **resilience against packet loss during key establishment**, shortening the impact of the window of compromise.

What would an appropriate protocol look like?

Goals – Setting

- **Asynchronous key agreement protocol**
- **Standardised**, composes with different symmetric protocols
- **Sessions are long-lasting** to avoid costly handshake authentication
- Low bandwidth & complexity
- (Optional) Can handle groups of devices and dynamic group membership

Goals – Security

- E2E Authenticity and Confidentiality
- Adversarial Model
 - MiTM: Network, Delivery Service compromised
 - Corruption: Can heal from state compromise
 - Adaptive and Active Adversary
- **Forward and Post-Compromise Security**

So, what now?

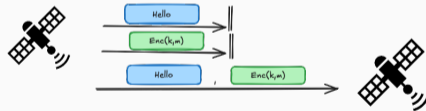
There are a number of Working Groups that are starting to look at what network protocols should be used in space settings:

- **TIPTOP: Taking IP to Other Planets**

- IP in Deep Space: Key Characteristics, Use Cases and Requirements
- An Architecture for IP in Deep Space
- QUIC Profile for Deep Space

- **DTN: Delay Tolerant Networking**

- **SPACERG: Systems and Protocol Aspects for Circumstellar Environments Research Group**



Whatever security we put up there in space will be hard to upgrade and replace, so let's make sure that we get it right the first time.

Thank you for your time.