Paper ID: 99345
oral

IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Advances in Space-based Communication Technologies (7)

Author: Mr. Andrew Savchenko
University of Technology Sydney (UTS), Australia

AUTHENTICATED ENCRYPTION FOR SPACE TELEMETRY

Abstract

Keywords: Communications security, telemetry, authenticated encryption

This paper presents a lightweight authenticated encryption implementation for space telemetry applications, addressing NASA-STD-1006A requirements while maintaining operational simplicity. Our approach prioritises robust security without sacrificing performance in resource-constrained environments. Our solution produces fixed-length messages, maintaining compatibility with Space Packet Protocol (SPP), SpaceWire and Delay/Disruption Tolerant Networking (DTN) protocols.

Methodologically, proposed scheme leverages a well-tested stream cipher which is accelerated in hardware across multiple platforms, making it ideal for space applications with limited power and computational resources. To defend against side-channel attacks, we incorporate various normalisation techniques, denying adversaries the opportunity to infer underlying information through temporal pattern and message content analyses. Additional enhancements include a sliding timing window to account for varying clock drifts, a key ratchet mechanism with rotation during heartbeat roundtrips, terminal-specific nonce generation as well as the key revocation procedure.

Our threat model assumes that adversaries can observe, modify, and replay traffic but are unable to physically tamper with TX/RX terminals. The security analysis acknowledges theoretical vulnerabilities, but demonstrates why practical exploitation remains improbable within the limits of space systems. By focusing on predictable properties and robust authentication, our solution balances security requirements with operational constraints of space telemetry applications where protection of sensitive data and prevention of unauthorised commands remain critical concerns.

An implementation in one of the popular programming languages will be made available for download.