NASA/TM—2015-218821

Control and Non-Payload Communications (CNPC) Prototype Radio—Generation 2 Security Flight Test Report

Dennis C. Iannicca, Joseph A. Ishac, and Kurt A. Shalkhauser
Glenn Research Center, Cleveland, Ohio

June 2015

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI Program provides access to the NASA Technical Report Server—Registered (NTRS Reg) and NASA Technical Report Server—Public (NTRS) thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers, but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., "quick-release" reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- E-mail your question to help@sti.nasa.gov

- Fax your question to the NASA STI Information Desk at 757-864-6500

- Telephone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Program
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM—2015-218821

Control and Non-Payload Communications (CNPC) Prototype Radio—Generation 2 Security Flight Test Report

Dennis C. Iannicca, Joseph A. Ishac, and Kurt A. Shalkhauser
Glenn Research Center, Cleveland, Ohio

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

June 2015

Acknowledgments

The National Aeronautics and Space Administration thanks the faculty and staff of the Avionics Engineering Center at the Ohio University Russ College of Engineering for their generous logistical and institutional support, enabling us to successfully install and operate the Albany, Ohio, ground station described in this report.

This report is a formal draft or working paper, intended to solicit comments and ideas from a technical peer group.

This report contains preliminary findings, subject to revision as analysis proceeds.

Trade names and trademarks are used in this report for identification only. Their usage does not constitute an official endorsement, either expressed or implied, by the National Aeronautics and Space Administration.

Level of Review: This material has been technically reviewed by technical management.

Available from

NASA STI Program
Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
703-605-6000

This report is available in electronic form at http://www.sti.nasa.gov/ and http://ntrs.nasa.gov/

Contents

Control and Non-Payload Communications (CNPC) Prototype Radio—Generation 2 Security Flight Test Report

Dennis C. Iannicca, Joseph A. Ishac, and Kurt A. Shalkhauser
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Abstract

NASA Glenn Research Center (GRC), in cooperation with Rockwell Collins, is working to develop a prototype Control and Non-Payload Communications (CNPC) radio platform as part of NASA Integrated Systems Research Program's (ISRP) Unmanned Aircraft Systems (UAS) Integration in the National Airspace System (NAS) project. A primary focus of the project is to work with the Federal Aviation Administration (FAA) and industry standards bodies to build and demonstrate a safe, secure, and efficient CNPC architecture that can be used by industry to evaluate the feasibility of deploying a system using these technologies in an operational capacity. GRC has been working in conjunction with these groups to assess threats, identify security requirements, and to develop a system of standards-based security controls that can be applied to the GRC prototype CNPC architecture as a demonstration platform.

The proposed security controls were integrated into the GRC flight test system aboard our S-3B Viking surrogate aircraft and several network tests were conducted during a flight on November 15th, 2014 to determine whether the controls were working properly within the flight environment. The flight test was also the first to integrate Robust Header Compression (ROHC) as a means of reducing the additional overhead introduced by the security controls and Mobile IPv6. The effort demonstrated the complete end-to-end secure CNPC link in a relevant flight environment.

1.0 Introduction

NASA is currently working with the Federal Aviation Administration (FAA), RTCA Inc. (a Federal Advisory Committee), and other organizations to develop technologies and procedures to allow Government (public) and commercial (civil) unmanned aircraft (UA) to operate safely in the National Airspace System (NAS). One aspect of this effort is to design and test a concept prototype network that will allow a UA to fly in the NAS while being controlled by a Pilot in Command (PIC) from a Control Element (CE) located elsewhere on the ground, thus creating an Unmanned Aircraft System (UAS). An essential element of this new national capability is the radio communications channel linking each UA to a network of fixed ground stations (GSs). Data communication necessary for flight is referred to as Control and Non-Payload Communication (CNPC) and is exchanged between each UA and a CE to ensure safe, reliable, and effective UA flight operation.

This report focuses on the research effort to better understand the requirements for secure communications over the concept prototype network and assesses standards-based cryptographic security controls that allow for confidentiality, integrity, non-repudiation, and anti-replay capabilities. The overarching goal of secure communications is to provide safety of flight.

Figure 1 depicts a diagram of GRC's UAS flight network environment. The network consists of one UA connected to one or more GS using Rockwell Collins prototype radios providing the air-ground RF

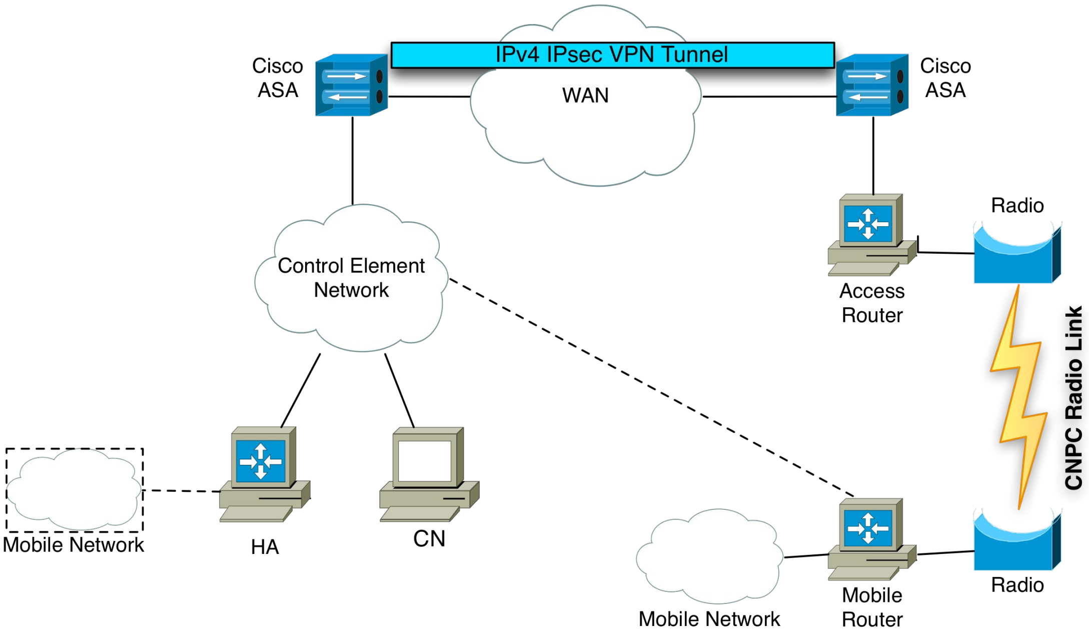

Figure 1.—UAS Networked Reference Implementation

link. Networking equipment to support the mobile routing of information from the CE to the UA was also used to verify that messaging from a PIC to a UA is achieved seamlessly during handover procedures between towers.

To implement the end-to-end security controls, a standards-based cryptographic security extension to the Internet Protocol (IP) called IPsec is used to secure the communications transmission through the network and over the air-ground RF link. Cryptographic techniques inherently add an overhead to the transmission of information and can adversely affect the throughput and overall capacity of the network so techniques like header compression are used to offset the overhead of such cryptography.

2.0 Environment Description

2.1 Overview

The flight architecture consists of three major components: the control element network, the ground station(s), and the mobile node or router aboard the aircraft. Within the control element network is the Mobile IPv6 home agent and one or more correspondent nodes that need to communicate with the mobile node.

A home agent (HA) is placed in the control element network, or “home network”, and is used as a central communications point for contacting the mobile node. The HA maintains a binding database of a mobile node's current foreign network address, or care-of address (CoA). The bindings map the home address, a known address in the home network, to the shifting care-of address in the foreign network in order to transparently reroute traffic from external users.

Each GS serves as a broker providing a UAV with its foreign network IPv6 address. This is done by means of an IPv6 access router (AR) which communicates with the aircraft through the prototype CNPC radio. Router advertisements or other dynamic host configuration methods can then be used to provide the UAV with a network address. The ground station does not need to be owned by the same agency as the aircraft and will have address space associated with the terrestrial service provider used at that location.

The aircraft communicates to the ground station using the same CNPC radio link. A Mobile IPv6 router (MR) attached to the radio allows the mobile network to communicate with the home network seamlessly. This allows the various components behind the mobile router to be addressed directly by using a predefined static mobile network prefix. Users would not need to know the dynamic addressing schemes used at the various ground stations as the devices can always be reached via their mobile network prefix address.

2.2 Internetworking

In a deployed environment communication between endpoints would be expected to eventually utilize IPv6 end-to-end, without the need for any encapsulation of traffic within legacy IPv4 packets for transmission across the Internet. However, the perimeter network in use does not currently route IPv6 traffic natively. In order to emulate a native IPv6 environment, “6in4” (IP Protocol 41) tunnels were created between the home agent and the ground station computer system to allow for utilization of the readily available IPv4 backhaul communications networks. While there are several alternative ways to configure the test architecture to transmit IPv6 packets across an IPv4 network, the 6in4 approach reduced configuration complexity and eliminated the need for devices between the home agent and ground station computer to be IPv6-compatible.

The home network and the ground stations are each protected by a dedicated firewall system that serves as both an IPv4 network firewall as well as a virtual private network (VPN) gateway to secure the transmission of data across the Internet. Each GS utilizes an IPv4 IPsec VPN connection to communicate with the home network and carry the 6in4 traffic between the home agent and the ground station computer where it is unencapsulated back to native IPv6 packets.

While the prototype flight architecture implements this "6in4" encapsulation in order to ensure complete compatibility with an expected future implementation, the terrestrial IPv4 IPsec VPN link over the "Internet" has no design relevance to the CNPC security architecture recommendations under evaluation by this experiment. The additional overhead of the VPN gateways and IPv4 VPN link are negligible across terrestrial links.

2.3 Addressing Scheme

The home network and ground stations were designed to support a dual-stack IPv4/IPv6 environment in order to support direct communications with legacy devices such as uninterruptible power supply (UPS) battery backup network interfaces or out-of-band management interfaces on the ground station computers that may not support IPv6. In addition, an IPv4 addressing scheme was needed to serve as an endpoint for the 6in4 tunnels between the home agent and the ground station computer.

The ground station computers were configured to use the radvd (router advertisement) daemon in order to support IPv6 neighbor discovery across the RF link by multicasting periodic Router Advertisement (RA) packets every 10 sec. The remote aircraft computer, upon receipt of one of these RA packets, would be able to self-configure its IPv6 Care-of Address (CoA) and begin communicating with the ground station, and thus the home agent, at the network layer.

2.4 Network Mobility Concept

The Mobile IPv6 design allows the aircraft to maintain seamless network-layer communications between the pilot’s ground control station and the onboard avionics systems as the unmanned aircraft transitions between ground stations. This design will result in a few dropped packets during the transition, but established sessions should usually continue on without needing to reconnect. This method eliminates the costly procedure of tearing down and re-establishing active IPsec sessions.

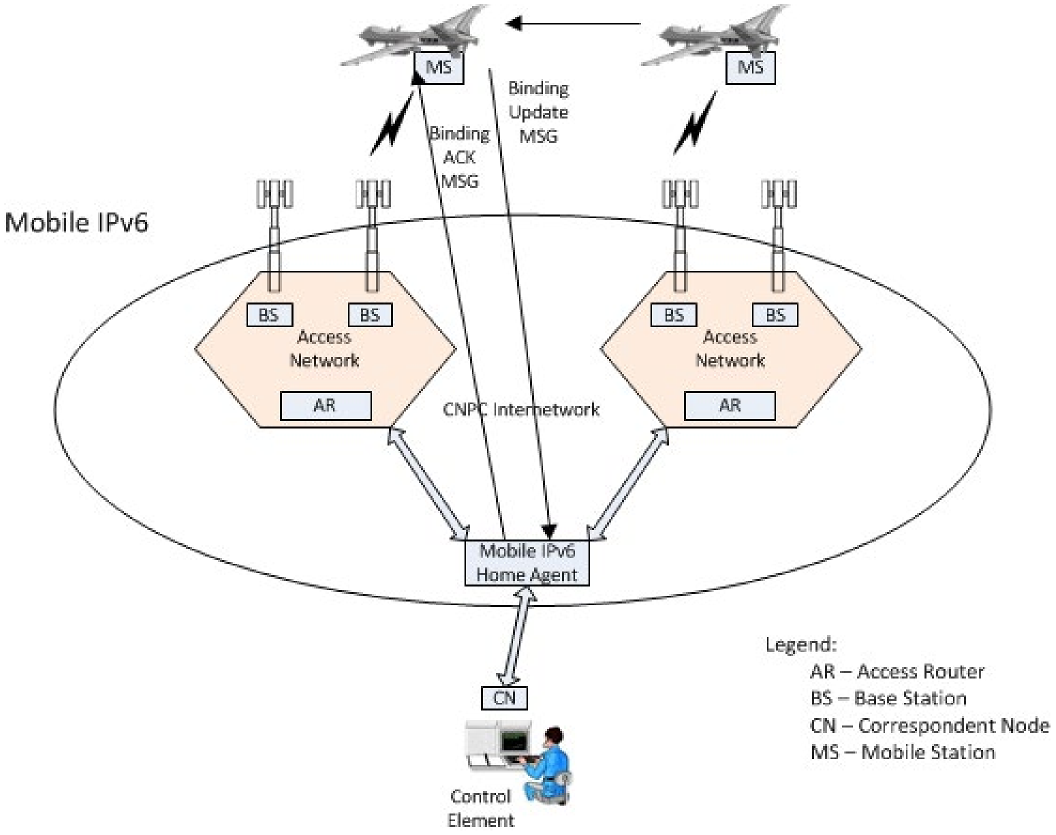

Figure 2.—Mobile IPv6 Layer-3 Handoffs

The Mobile IPv6 network shown in Figure 2 starts configuring after the CNPC radios connect. Then the ground station AR sends a RA via the CNPC radios to the MR. The MR using the RA creates a care-of-address (CoA), providing the MR with a global address that allows communication between the MR and HA.

The MR then sends a Binding Update (BU) that contains the MR's Home Address (HoA) and CoA to the HA, providing the HA with MR's latest point of attachment to the network. The HoA is a global address from the home network (located in the Control Element) address space and is used by the HA to identify the MR. After authenticating the BU, the HA replies with a Binding Acknowledgement (BA) and creates an IPv6 dynamic tunnel between the HA and the MR through which any traffic between the Correspondent Node (CN) and the MR travels.

2.5 Robust Header Compression (ROHC)

ROHC is a 2001 specification used to reduce the size of network protocol headers across a single data communication link. There has been significant interest in compressing headers in situations where communication links have limited capacity or where the ratio of header to payload is large. In the UAS CNPC waveform, reducing this overhead is of critical importance as the link is both limited in capacity and the anticipated nature of communication is a large number of relatively short messages, each message with an associated set of protocol headers. Given the degree of realtime sensitivity, the traffic should be moved forward expeditiously.

The ROHC specification defines a process that will, under ideal circumstances, compress the IPv6 header to 1 or 2 bytes. It does this by establishing "sessions" between the ROHC compressor and ROHC decompressor operating at the two endpoints. State is maintained at both endpoints and the compressor begins removing invariant or predictable components in the header obviating the need to pass those fields across the communication link. Since the decompressor shares the same session and state as the compressor it can reconstruct those headers upon arrival.

2.6 End-to-End Network Security

IPsec is a security extension to the Internet Protocol (IP) that provides end-to-end security protection of network layer traffic in a standard fashion. It allows for mutual authentication of nodes at the establishment of a session and periodic renegotiation of cryptographic keys used during an ongoing session. Mechanisms are available to provide confidentiality, data integrity, data-origin authentication, non-repudiation, and anti-replay capabilities. IPsec can be used in two different modes: “transport”, which protects data communications between two hosts, and “tunnel” which protects communications between two gateways allowing for secure communications between one or more hosts on each side of the tunnel. In addition, IPsec offers transport and tunnel mode with two protocols: Authentication Headers (AH) and Encapsulating Security Payloads (ESP).

For the architecture to provide secure transmission over the CNPC network while maximizing the capability of ROHC to compress as much of the header stack as possible, IPsec ESP transport mode is utilized to transmit packets between the CN (behind the HA) and the MR or other destination aboard the UA. Once the Mobile IPv6 tunnel is established between the HA and the MR and traffic destined for one of the pre-configured security endpoints is detected by the operating system, an Internet Key Exchange version 2 (IKEv2) session is automatically established to negotiate a set of IPsec security associations between the CE and the UA system(s). All packets subsequently transmitted over this Mobile IPv6 tunnel after IPsec ESP transport mode security associations are established will be encrypted and the communications will be securely authenticated using strong cryptographic algorithms.

The testing utilized 256-bit Elliptic Curve Digital Signature Algorithm (ECDSA) certificates on the endpoint systems for authentication of the CNPC link. IKEv2 negotiation used 128-bit Advanced Encryption Standard-Galois Counter Mode (AES-GCM) with a 64-bit Cryptographic Message Authentication Code (CMAC) for session establishment. ESP was also configured to use 128-bit AES-GCM for encryption and 64-bit CMAC for authentication of packets.

3.0 Test Setup

3.1 Data Generation

A simple User Datagram Protocol (UDP) based utility was used to generate the simulated test traffic. It features adjustable payload size and adjustable generation rate. After different payload sizes and packet intervals were tested in the lab, a payload size of 40 bytes and a fixed rate of two packets per second (0.5 sec interval) was determined to be ideal for testing purposes. These payload parameters were selected to prevent dropped packets.

Udp_ping was written to emulate the anticipated type of traffic the CNPC network will see when real equipment is configured to use the CNPC links. The initial concern with using Internet Control Message Protocol (ICMP) echo request/echo reply “ping” traffic was with how the ROHC algorithm would handle ICMP traffic. ROHC defined several profiles, each of which is specific to a particular type of traffic. The profile used for ICMP traffic is different from the one used for UDP traffic. As UDP traffic will predominate in actual use scenarios, it was felt using UDP test traffic would yield more realistic measurements in test simulations. In the end the concerns were unwarranted as the UDP traffic was encapsulated within an encrypted ESP packet that obscured the transmitted UDP header and payload from the ROHC profile optimizations.

The *udp_ping* program carefully maintains synchronization with the system clock, which had a significant effect on how traffic flows to the radio. A sawtooth pattern was observed during earlier latency tests (Ref. 1) as a result of the ICMP-based ping utility's lack of clock synchronization for sending packets at exact intervals to sync to the radio frames. Our overall understanding of how traffic might potentially interact with the CNPC RF radio links was increased. Note, this observation is specific to the particular model of radios used in the test, but the considerations might well apply to any radio that depends on closely time-synchronized operations.

3.2 Data Capture

The standard Linux *tcpdump* utility was used to monitor the test traffic at several points in the network. Arguably this could be described as the Swiss-army-knife of network traffic monitoring utilities, it features a wealth of configurable options that allow capture of different types of network traffic coupled with accurate recording (logging) and time stamping of that traffic. Post-test, the recorded logs were re-processed by *tcpdump* to extract data used to produce the charts and measurements.

3.3 Mobile IPv6

The software used to provide layer-three IPv6 network mobility was *UMIP* (Ref. 2), an open source implementation compatible with Request for Comments (RFC) 6275 (Ref. 3) (Mobile IPv6), RFC 3963 (Ref. 4) (NEMO), RFC 3776 (Ref. 5) and RFC 4877 (Ref. 6) (IPsec and IKEv2).

3.4 IPsec Software

The open source *StrongSwan* (Ref. 7) IPsec VPN software was used to provide the IPsec and IKEv2 implementation for the end-to-end security testing on an Ubuntu Linux-based platform. Its support for authentication and encryption suites is extensive, among which are support for AES-GCM, elliptic curve Diffie-Hellman (DH) groups and ECDSA certificates (Suite B, RFC 4869 (Ref. 8)) and Extensible Authentication Protocol (EAP) user authentication. It also supports IKEv2 MOBIKE (RFC 4555 (Ref. 9)) support for dynamic IP address and interface updating.

3.5 Network Preparation

The following steps were used to configure the components of the Mobile IPv6 network.

- Upload configuration files to the radios that set up link streams and establish link stream identification numbers.
- Start the radio connection software that brings up the Linux tunnel interfaces on the GS AR and aircraft MR and establishes a data connection to the radio interface using the configured link stream IDs. [The radio connection software is also where the ROHC option is enabled if needed.]
- Ensure the *mip6d* daemons on the home agent and mobile router are running.
- Ensure the *StrongSwan* IPsec configuration is loaded and running in the background. [Security associations will be created dynamically when traffic is detected destined for one of the endpoints. Authentication certificates and certificate authority certificates are preloaded appropriately on each end node.]
- Start *tcpdump* captures on the following interfaces:

Correspondent Node Interface:
tcpdump -i eth0 [capture the udp-pings response and request packets.]

Home Agent Interface:
tcpdump -i eth0 [capture all traffic passing thru the HA for reference, in case of unexplained event in data.]

GS AR interface:
tcpdump -i six0 [capture all IPv6 traffic passing thru GS AR from the HA.]
tcpdump -i rftun0 [the aforementioned Linux tunnel established between the computer and the radio. This should capture all traffic being passed to/from the radio connection software for the CNPC radio.]

Aircraft MR Interface:
tcpdump -i rftun0 [capture all traffic being passed to/from the radio connection software for the CNPC radio destined to ground station 1.]
tcpdump -i rftun1 [capture all traffic being passed to/from the radio connection software for the CNPC radio destined to ground station 2.]

3.6 Aircraft Operations and Flight Path

Test conditions for demonstrating the system security controls were established in a single flight test sequence using one research aircraft and two ground stations. Using this arrangement, all elements of the communications network would be part of the investigation, including the actual radio-to-radio link, which would provide assessment of losses and latencies throughout the entire system. For this test the aircraft, its CNPC radio, and the associated airborne equipment serve as the mobile network. Two identical ground stations were used in the stationary system, each with a network connection to the home agent and test control location. While only one ground station was necessary to complete the security tests, the second ground station provided additional test opportunities including measurement of different terrestrial latencies and the ability to perform in-flight hand-offs between the spatially-separated ground stations.

The flight test was performed on November 15, 2014, in the airspace above south-central Ohio (Figure 3). The primary CNPC communications path utilized a ground station installed at the Ohio University Gordon K. Bush Airport in Albany, Ohio, shown as GS2 in the figure. The terrain in the local area is generally hilly, but the radio line-of-sight path between aircraft and ground station has been well characterized and the shown to be free of obstructions for the flight altitude of 11,000 ft (Ref. 1). The flight path for the security test is shown as a red trace, which begins at UTC 17:30 at a point directly east of the GS2 location. From 17:30 until approximately 18:03 the aircraft travelled in a counterclockwise circular path at a radial distance of nominally 25 nmi from GS2. At approximately 18:03 the aircraft turned northbound, allowing it to fly directly overhead of the GS2 location then towards ground station 1 (GS1) in Cleveland, Ohio. All security testing was completed at UTC 18:25 and approximately 56 nmi south of Cleveland.

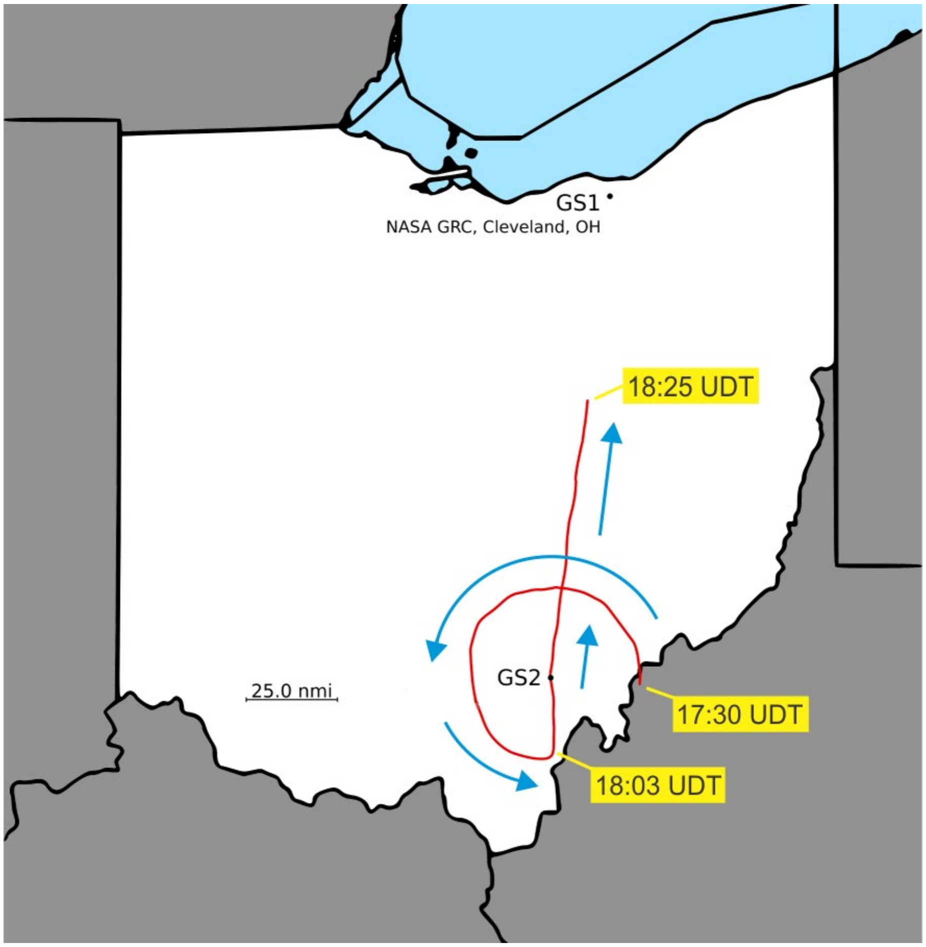

Figure 3.—Research Flight Track for November 15, 2014; GS, ground station. Map created using GPSVisualizer.com.

4.0 Test Results

4.1 Radiofrequency Link Performance

Figure 4 presents radio link and flight data for the entire 17:30 to 18:30 security test period, with time annotated along the horizontal axis. Received signal strengths at the aircraft radio and at the ground stations are plotted along the vertical axis in the uppermost section of the figure. Signal strength data for the first half of the test (17:30 to 18:03) generally varies between –80 and –100 dBm. This corresponds to the time period during which ROHC was disabled. With the aircraft performing rudder turns (minimal roll) during the orbital flight path, the CNPC radio connection to GS2 remained unbroken throughout the 33-min subtest period.

The next four traces in Figure 4 present data on the percentage of frame data loss averaged over 1 sec at the ground and aircraft receivers. Individual traces for uplink (UL1) and downlink (DLC2) channels are shown. Where the CNPC communications path was transferring all data without error, the data are represented as 0-percent loss. Where errors occurred in the radio link, the lost frame data trace created a visible trace ranging from 0 to 100 percent, with the latter representing total loss of the radio link. During the 17:30 to 18:03 period, both uplink and downlink between the test aircraft and GS2 remained essentially lossless.

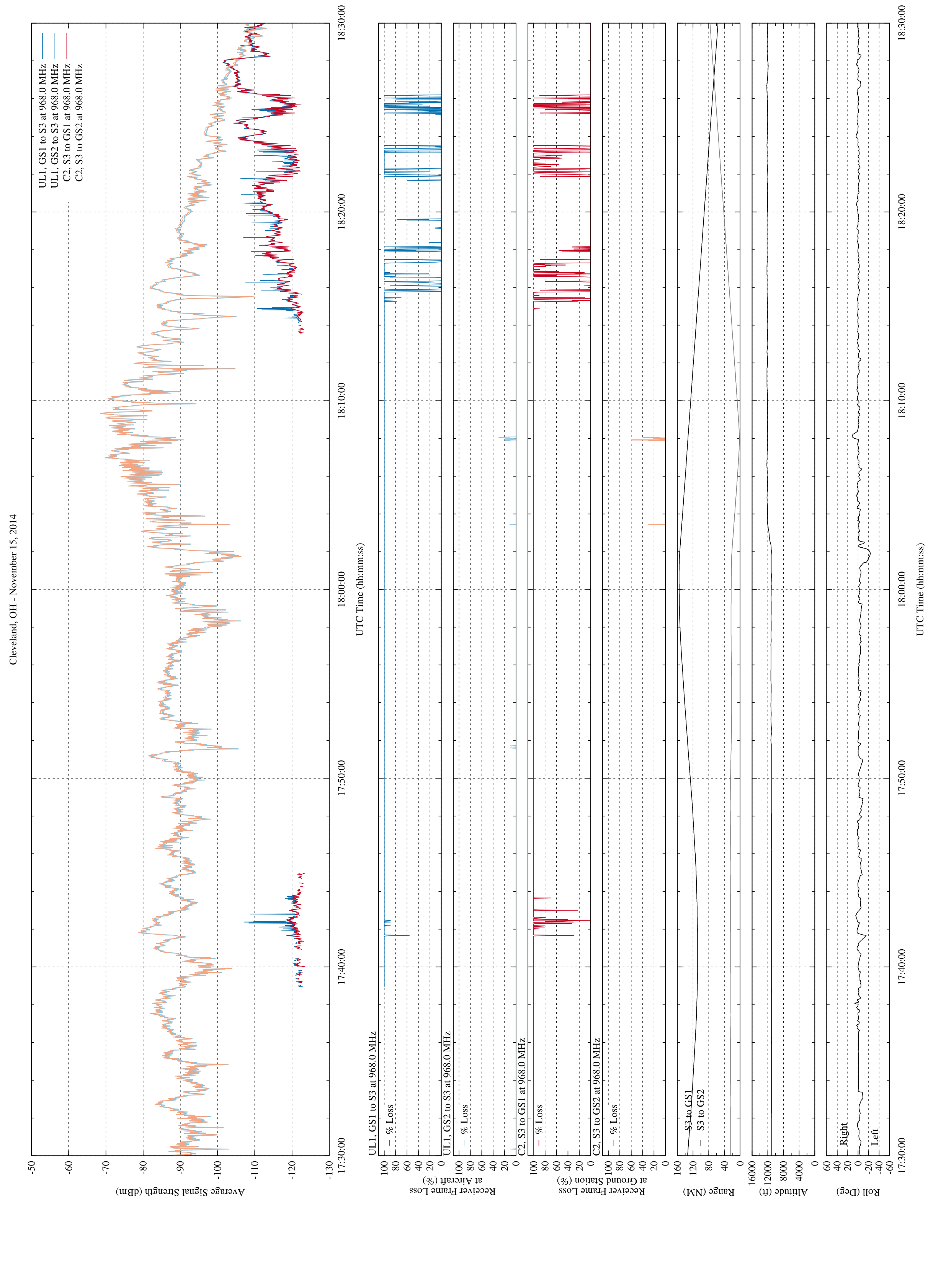

Figure 4.—RF Link Performance

Aircraft flight data is presented in the lowest three traces of Figure 4. Slant range between the GS and aircraft, aircraft altitude, and roll angle are presented to correlate to CNPC radio link performance.

Once the aircraft completed approximately ¾ of the full orbital circle (near 18:02 and directly south of GS2), it turned northbound to fly overhead of GS2 and then on a vector toward GS1 in Cleveland, Ohio. Figure 4 shows a small burst of packet losses as the aircraft flew directly overhead of GS2 (immediately prior to 18:07) and executed a small course correction maneuver. After the overflight, the radio signal strength progressively declined from a peak value near –70 dBm toward –110 dBm near the end of the security test. The CNPC communications link to GS2 was maintained throughout this second test period, allowing ROHC to be activated and operated.

As the aircraft approached Cleveland, Ohio, low-level signals started being communicated between the aircraft and GS1 (approximately 18:14). By 18:18 the signals to GS1 in Cleveland, Ohio, were sufficiently strong to produce 0 percent packet errors, while at the same time the aircraft radio remained in full contact with GS2. For the periods when lossless connections were available to both ground stations, hand-off testing was performed.

4.2 Authentication

When the *udp_ping* data generation program is started on the CN ground system, the CN system's *StrongSwan* implementation sends an IKEv2 security association (SA) initialization request to the UA's node. In this portion of the test, the UA received this IKE_SA_INIT request via its Mobile IPv6 home address through GS2 and compared it against the UA's *StrongSwan* configuration file to determine if the requestor's identifier, "C=US, O=NASA, CN=vsm", was authorized to connect to it.

The UA then validated the request to ensure that a trusted certificate authority (CA) signed it by verifying the certificate's ECDSA-256 signature. In this case a self-signed certificate authority was created in the lab for all public key infrastructure purposes and was used to sign all the end-node certificates used during testing. The CA's self-signed root certificate was preloaded onto each of the end-nodes prior to flight.

Once the authentication phase was completed, a security association between the CN system and the UA was established. All subsequent traffic between the nodes (aside from IKE communications) was encrypted and integrity-protected using ESP transport mode. The *StrongSwan* authentication log of this example IKE_SA_INIT event is included below. Note: These tests were conducted while the UA was loitering within communications range of GS2, with Mobile IPv6 enabled, and with Robust Header Compression disabled.

```
Nov 15 17:24:09 Aircraft1 charon: 13[NET] received packet: from CN[500] to UA[500] (232 bytes)
Nov 15 17:24:09 Aircraft1 charon: 13[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
Nov 15 17:24:09 Aircraft1 charon: 13[IKE] CN is initiating an IKE_SA
Nov 15 17:24:09 Aircraft1 charon: 13[IKE] sending cert request for "C=US, O=NASA, CN=UAS CA"
Nov 15 17:24:09 Aircraft1 charon: 13[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ
N(MULT_AUTH) ]
Nov 15 17:24:09 Aircraft1 charon: 13[NET] sending packet: from UA[500] to CN[500] (265 bytes)
Nov 15 17:24:11 Aircraft1 charon: 14[NET] received packet: from CN[4500] to UA[4500] (936 bytes)
Nov 15 17:24:11 Aircraft1 charon: 14[ENC] parsed IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ IDr AUTH N(USE_TRANSP) SA TSi
TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] received cert request for "C=US, O=NASA, CN=UAS CA"
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] received end entity cert "C=US, O=NASA, CN=vsm"
Nov 15 17:24:11 Aircraft1 charon: 14[CFG] looking for peer configs matching UA[C=US, O=NASA, CN=s3]...CN[C=US, O=NASA, CN=vsm]
Nov 15 17:24:11 Aircraft1 charon: 14[CFG] selected peer config 's3-hoa-vsm'
Nov 15 17:24:11 Aircraft1 charon: 14[CFG]   using certificate "C=US, O=NASA, CN=vsm"
Nov 15 17:24:11 Aircraft1 charon: 14[CFG]   using trusted ca certificate "C=US, O=NASA, CN=UAS CA"
Nov 15 17:24:11 Aircraft1 charon: 14[CFG] checking certificate status of "C=US, O=NASA, CN=vsm"
Nov 15 17:24:11 Aircraft1 charon: 14[CFG] certificate status is not available
Nov 15 17:24:11 Aircraft1 charon: 14[CFG]   reached self-signed root ca with a path length of 0
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] authentication of 'C=US, O=NASA, CN=vsm' with ECDSA-256 signature successful
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] peer supports MOBIKE
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] authentication of 'C=US, O=NASA, CN=s3' (myself) with ECDSA-256 signature successful
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] IKE_SA s3-hoa-vsm[3] established between UA[C=US, O=NASA, CN=s3]...CN[C=US, O=NASA, CN=vsm]
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] scheduling reauthentication in 3295s
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] maximum IKE_SA lifetime 3475s
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] sending end entity cert "C=US, O=NASA, CN=s3"
Nov 15 17:24:11 Aircraft1 charon: 14[IKE] CHILD_SA s3-hoa-vsm{2} established with SPIs c24a5a3d_i c8fd1db1_o and TS UA/128 === CN/128
Nov 15 17:24:11 Aircraft1 charon: 14[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH N(USE_TRANSP) SA TSi TSr N(AUTH_LFT)
N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR)
N(ADD_6_ADDR) ]
Nov 15 17:24:11 Aircraft1 charon: 14[NET] sending packet: from UA[4500] to CN[4500] (813 bytes)
```

The corresponding *tcpdump* capture of this IKE_SA_INIT authentication request as viewed from the perspective of the CN is:

```
17:24:09.500980 IP6 CN.isakmp > UA.isakmp: isakmp: parent_sa ikev2_init[I]
17:24:10.319071 IP6 UA.isakmp > CN.isakmp: isakmp: parent_sa ikev2_init[R]
17:24:10.320767 IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  ikev2_auth[I]
17:24:12.420175 IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  ikev2_auth[R]
```

4.3 Data Flow

Once the IPsec ESP security association has been established, subsequent traffic begins to flow over encapsulated packets via ground station 2, which will serve to both, in our configuration’s case, encrypt and protect the integrity of the payload carried within. The protected data transmission can be verified by looking at the *tcpdump* packet captures after the security association has been established. This sample of traffic is captured on the CN node:

```
17:24:12.500099 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x1), length 76
17:24:12.919634 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0x1), length 76
17:24:13.000134 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x2), length 76
17:24:13.418898 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0x2), length 76
17:24:13.500125 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x3), length 76
17:24:13.918828 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0x3), length 76
17:24:14.000163 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x4), length 76
17:24:14.418903 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0x4), length 76
17:24:14.500129 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x5), length 76
17:24:14.918887 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0x5), length 76
17:24:15.000145 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x6), length 76
17:24:15.420418 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0x6), length 76
17:24:15.500159 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x7), length 76
17:24:15.919660 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0x7), length 76
17:24:16.000158 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x8), length 76
17:24:16.418761 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0x8), length 76
17:24:16.500155 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x9), length 76
17:24:16.919336 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0x9), length 76
17:24:17.000164 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0xa), length 76
17:24:17.419567 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0xa), length 76
17:24:17.500159 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0xb), length 76
17:24:17.919631 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0xb), length 76
17:24:18.000159 IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0xc), length 76
17:24:18.419655 IP6 UA > CN: ESP(spi=0xc8fd1db1,seq=0xc), length 76
```

With IPsec ESP, a unidirectional security association is created between the two nodes and is subsequently identified by a Security Parameter Index (SPI). An incrementing sequence number unique to this SPI is kept by the systems to track state. Aside from this, no other identifying information regarding the type of data encapsulated within the IPsec ESP payload is visible to outside observers that may be able to intercept and observe the traffic flow when using network-layer encryption, for example, over an otherwise unprotected and unencrypted RF CNPC link.

4.4 Rekeying

Periodically the two endpoints will attempt to re-establish their temporary session keys for the unidirectional security associations in order to reduce the chances that an adversary that is able to observe the channel has been able to crack the old key based upon traffic analysis. Several example *StrongSwan* log events as well as their corresponding *tcpdump* captures from the network interfaces are shown below.

A rekeying request initiated by the CN to the UA to rekey the security association:

```
Nov 15 17:38:37 Aircraft1 charon: 05[NET] received packet: from CN[4500] to UA[4500] (317 bytes)
Nov 15 17:38:37 Aircraft1 charon: 05[ENC] parsed CREATE_CHILD_SA request 2 [ N(REKEY_SA) N(USE_TRANSP) SA No KE TSi TSr ]
Nov 15 17:38:37 Aircraft1 charon: 05[IKE] CHILD_SA s3-hoa-vsm{2} established with SPIs ccdf6c0b_i c2215003_o and TS UA/128 === CN/128
Nov 15 17:38:37 Aircraft1 charon: 05[ENC] generating CREATE_CHILD_SA response 2 [ N(USE_TRANSP) SA No KE TSi TSr ]
Nov 15 17:38:37 Aircraft1 charon: 05[NET] sending packet: from UA[4500] to CN[4500] (305 bytes)
Nov 15 17:38:38 Aircraft1 charon: 15[NET] received packet: from CN[4500] to UA[4500] (61 bytes)
Nov 15 17:38:38 Aircraft1 charon: 15[ENC] parsed INFORMATIONAL request 3 [ D ]
Nov 15 17:38:38 Aircraft1 charon: 15[IKE] received DELETE for ESP CHILD_SA with SPI c8fd1db1
Nov 15 17:38:38 Aircraft1 charon: 15[IKE] closing CHILD_SA s3-hoa-vsm{2} with SPIs c24a5a3d_i (83088 bytes) c8fd1db1_o (82992 bytes) and
TS UA/128 === CN/128
Nov 15 17:38:38 Aircraft1 charon: 15[IKE] sending DELETE for ESP CHILD_SA with SPI c24a5a3d
Nov 15 17:38:38 Aircraft1 charon: 15[IKE] CHILD_SA closed
Nov 15 17:38:38 Aircraft1 charon: 15[ENC] generating INFORMATIONAL response 3 [ D ]
Nov 15 17:38:38 Aircraft1 charon: 15[NET] sending packet: from UA[4500] to CN[4500] (61 bytes)
```

The *tcpdump* on the aircraft rftun1 (GS2) interface captures the traffic:

```
17:38:37.884834 IP6 HA > 2001:db8::22e4:601:6e00:4ca2:3f7e: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  child_sa[I]
17:38:37.885980 IP6 2001:db8::22e4:601:6e00:4ca2:3f7e > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  child_sa[R]
17:38:38.121878 IP6 HA > 2001:db8::22e4:601:6e00:4ca2:3f7e: IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x6c3), length 76
17:38:38.122193 IP6 2001:db8::22e4:601:6e00:4ca2:3f7e > HA: IP6 UA > CN: ESP(spi=0xc2215003,seq=0x1), length 76
17:38:38.284874 IP6 HA > 2001:db8::22e4:601:6e00:4ca2:3f7e: IP6 CN > UA: ESP(spi=0xc24a5a3d,seq=0x6c4), length 76
17:38:38.285159 IP6 2001:db8::22e4:601:6e00:4ca2:3f7e > HA: IP6 UA > CN: ESP(spi=0xc2215003,seq=0x2), length 76
17:38:38.584774 IP6 HA > 2001:db8::22e4:601:6e00:4ca2:3f7e: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  inf2[I]
17:38:38.585523 IP6 2001:db8::22e4:601:6e00:4ca2:3f7e > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  inf2[R]
```

As can be observed, normal ESP communications is not interrupted during the rekeying of the security association. The only detrimental effects are the additional overhead of the IKE traffic, which may cause periodic spikes in the latency while the rekeying is occurring.

A rekeying request is initiated by the UA to the CN to rekey the security association:

```
Nov 15 17:52:51 Aircraft1 charon: 07[KNL] creating rekey job for ESP CHILD_SA with SPI ccdf6c0b and reqid {2}
Nov 15 17:52:51 Aircraft1 charon: 07[IKE] establishing CHILD_SA s3-hoa-vsm{2}
Nov 15 17:52:51 Aircraft1 charon: 07[ENC] generating CREATE_CHILD_SA request 0 [ N(REKEY_SA) N(USE_TRANSP) SA No KE TSi TSr ]
Nov 15 17:52:51 Aircraft1 charon: 07[NET] sending packet: from UA[4500] to CN[4500] (317 bytes)
Nov 15 17:52:52 Aircraft1 charon: 06[NET] received packet: from CN[4500] to UA[4500] (305 bytes)
Nov 15 17:52:52 Aircraft1 charon: 06[ENC] parsed CREATE_CHILD_SA response 0 [ N(USE_TRANSP) SA No KE TSi TSr ]
Nov 15 17:52:52 Aircraft1 charon: 06[IKE] CHILD_SA s3-hoa-vsm{2} established with SPIs c5129432_i c9b745b2_o and TS UA/128 === CN/128
Nov 15 17:52:52 Aircraft1 charon: 06[IKE] closing CHILD_SA s3-hoa-vsm{2} with SPIs ccdf6c0b_i (81792 bytes) c2215003_o (81888 bytes) and TS
UA/128 === CN/128
Nov 15 17:52:52 Aircraft1 charon: 06[IKE] sending DELETE for ESP CHILD_SA with SPI ccdf6c0b
Nov 15 17:52:52 Aircraft1 charon: 06[ENC] generating INFORMATIONAL request 1 [ D ]
Nov 15 17:52:52 Aircraft1 charon: 06[NET] sending packet: from UA[4500] to CN[4500] (61 bytes)
Nov 15 17:52:53 Aircraft1 charon: 04[NET] received packet: from CN[4500] to UA[4500] (61 bytes)
Nov 15 17:52:53 Aircraft1 charon: 04[ENC] parsed INFORMATIONAL response 1 [ D ]
Nov 15 17:52:53 Aircraft1 charon: 04[IKE] received DELETE for ESP CHILD_SA with SPI c2215003
Nov 15 17:52:53 Aircraft1 charon: 04[IKE] CHILD_SA closed
```

The *tcpdump* on rftun1 (GS2) of the UA:

```
17:52:51.886712 IP6 2001:db8::22e4:601:6e00:4ca2:3f7e > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: parent_sa child_sa
17:52:52.182675 IP6 HA > 2001:db8::22e4:601:6e00:4ca2:3f7e: IP6 CN > UA: ESP(spi=0xccdf6c0b,seq=0x6ac), length 76
17:52:52.182967 IP6 2001:db8::22e4:601:6e00:4ca2:3f7e > HA: IP6 UA > CN: ESP(spi=0xc2215003,seq=0x6aa), length 76
17:52:52.882744 IP6 HA > 2001:db8::22e4:601:6e00:4ca2:3f7e: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: parent_sa child_sa[IR]
17:52:52.884432 IP6 2001:db8::22e4:601:6e00:4ca2:3f7e > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  inf2
17:52:53.121820 IP6 HA > 2001:db8::22e4:601:6e00:4ca2:3f7e: IP6 CN > UA: ESP(spi=0xc5129432,seq=0x1), length 76
17:52:53.122135 IP6 2001:db8::22e4:601:6e00:4ca2:3f7e > HA: IP6 UA > CN: ESP(spi=0xc9b745b2,seq=0x1), length 76
17:52:53.282024 IP6 HA > 2001:db8::22e4:601:6e00:4ca2:3f7e: IP6 CN > UA: ESP(spi=0xc5129432,seq=0x2), length 76
17:52:53.282259 IP6 2001:db8::22e4:601:6e00:4ca2:3f7e > HA: IP6 UA > CN: ESP(spi=0xc9b745b2,seq=0x2), length 76
17:52:53.382687 IP6 HA > 2001:db8::22e4:601:6e00:4ca2:3f7e: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  inf2[IR]
```

4.5 Enabling ROHC

In previous tests, the *StrongSwan* logs and *tcpdump* data captures had shown examples of the security controls applied to a baseline Mobile IPv6 link without Robust Header Compression. The next phase of testing restarted everything and activated ROHC while continuing to use Mobile IPv6. Restarting everything from scratch required that the IKE session also restart from scratch and mutually authenticate the nodes as it had done during the initial non-ROHC tests above. Note: At this point the UA continues to loiter within range of GS2 for testing purposes.

```
Nov 15 18:06:38 Aircraft1 charon: 08[NET] received packet: from CN[4500] to UA[4500] (57 bytes)
Nov 15 18:06:38 Aircraft1 charon: 08[ENC] parsed INFORMATIONAL request 4 [ D ]
Nov 15 18:06:38 Aircraft1 charon: 08[IKE] received DELETE for IKE_SA s3-hoa-vsm[3]
Nov 15 18:06:38 Aircraft1 charon: 08[IKE] deleting IKE_SA s3-hoa-vsm[3] between UA[C=US, O=NASA, CN=s3]...CN[C=US, O=NASA, CN=vsm]
Nov 15 18:06:38 Aircraft1 charon: 08[IKE] IKE_SA deleted
Nov 15 18:06:38 Aircraft1 charon: 08[ENC] generating INFORMATIONAL response 4 [ ]
Nov 15 18:06:38 Aircraft1 charon: 08[NET] sending packet: from UA[4500] to CN[4500] (49 bytes)
Nov 15 18:07:02 Aircraft1 charon: 04[NET] received packet: from CN[500] to UA[500] (232 bytes)
Nov 15 18:07:02 Aircraft1 charon: 04[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
Nov 15 18:07:02 Aircraft1 charon: 04[IKE] CN is initiating an IKE_SA
Nov 15 18:07:02 Aircraft1 charon: 04[IKE] sending cert request for "C=US, O=NASA, CN=UAS CA"
Nov 15 18:07:02 Aircraft1 charon: 04[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ
N(MULT_AUTH) ]
Nov 15 18:07:02 Aircraft1 charon: 04[NET] sending packet: from UA[500] to CN[500] (265 bytes)
Nov 15 18:07:04 Aircraft1 charon: 09[NET] received packet: from CN[4500] to UA[4500] (936 bytes)
Nov 15 18:07:04 Aircraft1 charon: 09[ENC] parsed IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ IDr AUTH N(USE_TRANSP) SA TSi
TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] received cert request for "C=US, O=NASA, CN=UAS CA"
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] received end entity cert "C=US, O=NASA, CN=vsm"
Nov 15 18:07:04 Aircraft1 charon: 09[CFG] looking for peer configs matching UA[C=US, O=NASA, CN=s3]...CN[C=US, O=NASA, CN=vsm]
Nov 15 18:07:04 Aircraft1 charon: 09[CFG] selected peer config 's3-hoa-vsm'
Nov 15 18:07:04 Aircraft1 charon: 09[CFG]   using certificate "C=US, O=NASA, CN=vsm"
Nov 15 18:07:04 Aircraft1 charon: 09[CFG]   using trusted ca certificate "C=US, O=NASA, CN=UAS CA"
Nov 15 18:07:04 Aircraft1 charon: 09[CFG] checking certificate status of "C=US, O=NASA, CN=vsm"
Nov 15 18:07:04 Aircraft1 charon: 09[CFG] certificate status is not available
Nov 15 18:07:04 Aircraft1 charon: 09[CFG]   reached self-signed root ca with a path length of 0
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] authentication of 'C=US, O=NASA, CN=vsm' with ECDSA-256 signature successful
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] peer supports MOBIKE
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] authentication of 'C=US, O=NASA, CN=s3' (myself) with ECDSA-256 signature successful
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] IKE_SA s3-hoa-vsm[4] established between UA[C=US, O=NASA, CN=s3]...CN[C=US, O=NASA, CN=vsm]
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] scheduling reauthentication in 3250s
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] maximum IKE_SA lifetime 3430s
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] sending end entity cert "C=US, O=NASA, CN=s3"
Nov 15 18:07:04 Aircraft1 charon: 09[IKE] CHILD_SA s3-hoa-vsm{2} established with SPIs cfb5a5e2_i c6799f14_o and TS UA/128 === CN/128
Nov 15 18:07:04 Aircraft1 charon: 09[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH N(USE_TRANSP) SA TSi TSr N(AUTH_LFT)
N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR)
N(ADD_6_ADDR) ]
Nov 15 18:07:04 Aircraft1 charon: 09[NET] sending packet: from UA[4500] to CN[4500] (813 bytes)
```

The *tcpdump* data capture from the UA's rftun1 (GS2) interface shows the IKEv2 IKE_SA_INIT request being processed and subsequently shows the new ESP security association SPIs starting with sequence number 0x1. In the mean time, the *udp_ping* traffic generator continued to send data without interruption and the security associations were established automatically behind the scenes:

```
18:06:38.181525 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  inf2[I]
18:06:38.182164 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  inf2[R]
18:06:38.681699 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN > UA: ICMP6, destination unreachable, unreachable port, CN udp port
4500, length 109
18:07:02.881737 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN.500 > UA.500: isakmp: parent_sa ikev2_init[I]
18:07:02.883666 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA.500 > CN.500: isakmp: parent_sa ikev2_init[R]
18:07:04.380780 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  ikev2_auth[I]
18:07:04.384125 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  ikev2_auth[R]
18:07:05.681717 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN > UA: ESP(spi=0xcfb5a5e2,seq=0x1), length 76
18:07:05.682046 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA > CN: ESP(spi=0xc6799f14,seq=0x1), length 76
18:07:06.181609 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN > UA: ESP(spi=0xcfb5a5e2,seq=0x2), length 76
18:07:06.181889 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA > CN: ESP(spi=0xc6799f14,seq=0x2), length 76
```

At 18:16:25 an informational message is sent using MOBIKE (Mobile IKE) from the UA to the CN upon the UA acquiring a new IP address on its rftun0 interface listening for GS1. This message is sent from the UA to the CN in order to update it on the available UA communication interfaces.

```
Nov 15 18:16:25 Aircraft1 charon: 08[KNL] 2001:db8::1ce8:601:2ca5:415d:79ee appeared on rftun0
Nov 15 18:16:25 Aircraft1 charon: 06[IKE] sending address list update using MOBIKE
Nov 15 18:16:25 Aircraft1 charon: 06[ENC] generating INFORMATIONAL request 0 [ N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_4_ADDR)
N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) ]
Nov 15 18:16:25 Aircraft1 charon: 06[NET] sending packet: from UA[4500] to CN[4500] (157 bytes)
Nov 15 18:16:25 Aircraft1 charon: 11[NET] received packet: from CN[4500] to UA[4500] (49 bytes)
Nov 15 18:16:25 Aircraft1 charon: 11[ENC] parsed INFORMATIONAL response 0 [ ]
```

The *tcpdump* data capture on rftun1 (GS2) shows the traffic being relayed to the CN:

```
18:16:25.233813 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: parent_sa inf2
18:16:25.582768 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: parent_sa inf2[IR]
```

At 18:21:32 a request from the CN to the UA to rekey the security association:

```
Nov 15 18:21:32 Aircraft1 charon: 09[NET] received packet: from CN[4500] to UA[4500] (317 bytes)
Nov 15 18:21:32 Aircraft1 charon: 09[ENC] parsed CREATE_CHILD_SA request 2 [ N(REKEY_SA) N(USE_TRANSP) SA No KE TSi TSr ]
Nov 15 18:21:32 Aircraft1 charon: 09[IKE] CHILD_SA s3-hoa-vsm{2} established with SPIs c6043759_i c5d267a6_o and TS UA/128 === CN/128
Nov 15 18:21:32 Aircraft1 charon: 09[ENC] generating CREATE_CHILD_SA response 2 [ N(USE_TRANSP) SA No KE TSi TSr ]
Nov 15 18:21:32 Aircraft1 charon: 09[NET] sending packet: from UA[4500] to CN[4500] (305 bytes)
Nov 15 18:21:33 Aircraft1 charon: 11[NET] received packet: from CN[4500] to UA[4500] (61 bytes)
Nov 15 18:21:33 Aircraft1 charon: 11[ENC] parsed INFORMATIONAL request 3 [ D ]
Nov 15 18:21:33 Aircraft1 charon: 11[IKE] received DELETE for ESP CHILD_SA with SPI c6799f14
Nov 15 18:21:33 Aircraft1 charon: 11[IKE] closing CHILD_SA s3-hoa-vsm{2} with SPIs cfb5a5e2_i (82896 bytes) c6799f14_o (82848 bytes) and TS
UA/128 === CN/128
Nov 15 18:21:33 Aircraft1 charon: 11[IKE] sending DELETE for ESP CHILD_SA with SPI cfb5a5e2
Nov 15 18:21:33 Aircraft1 charon: 11[IKE] CHILD_SA closed
Nov 15 18:21:33 Aircraft1 charon: 11[ENC] generating INFORMATIONAL response 3 [ D ]
Nov 15 18:21:33 Aircraft1 charon: 11[NET] sending packet: from UA[4500] to CN[4500] (61 bytes)
```

The *tcpdump* data capture from rftun1 (GS2) on the UA shows the corresponding traffic:

```
18:21:32.783557 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  child_sa[I]
18:21:32.784431 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN > UA: ESP(spi=0xcfb5a5e2,seq=0x6c7), length 76
18:21:32.784716 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA > CN: ESP(spi=0xc6799f14,seq=0x6be), length 76
18:21:32.785735 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  child_sa[R]
18:21:33.122085 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN > UA: ESP(spi=0xcfb5a5e2,seq=0x6c8), length 76
18:21:33.122332 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1), length 76
18:21:33.382442 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  inf2[I]
```

```
18:21:33.383158 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  inf2[R]
18:21:33.682579 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x1), length 76
18:21:33.682824 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x2), length 76
18:21:34.182447 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x2), length 76
18:21:34.182711 IP6 2001:db8::2d45:601:6fe2:6e8d:70da > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x3), length 76
18:21:34.483397 IP6 fe80::2000:15a9:11cd:385e > ff02::1: ICMP6, router advertisement, length 128
18:21:34.682131 IP6 HA > 2001:db8::2d45:601:6fe2:6e8d:70da: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x3), length 76
```

4.6 Tower Handoffs

Over the time period of approximately 18:24 through 18:26, the aircraft traversed a region where the airborne CNPC radio could communicate simultaneously with ground radios at both GS1 and GS2. At this point the flight research began a series of manual "handoffs" to iteratively make and break the data flow stream between GS1 and GS2.

The procedure to perform a layer-3 manual handoff between towers is:

1. Bring up an idle rftun interface.
2. Wait for a router advertisement to be broadcast from the tower to the aircraft.
3. Once received, the aircraft computer uses the router advertisement, which contains the ground station's IPv6 prefix, to automatically configure its IPv6 address.
4. *StrongSwan* will send a MOBIKE informational message to its active security association peer that its interfaces have changed.
5. Shutdown the active rftun interface.
6. *StrongSwan* will send a MOBIKE informational message to its active security association peer that its interfaces have changed.
7. The Mobile IPv6 daemon will sense the active interface is no longer available and switch over to using the next available interface listed in its configuration.
8. The Mobile IPv6 daemon will send a binding update to the home agent with the new active interface's care-of address.
9. Upon the aircraft receiving a binding update acknowledgement, the two Mobile IPv6 endpoints re-establish the tunnel between the home agent address and the new active interface on the aircraft.
10. Communications destined for the aircraft's HoA begin to flow over the new link.

Several optimizations to this procedure are being evaluated for future test flights. First, the router advertisement daemon on the ground station will be configured with the *UnicastOnly* option enabled so that it will no longer send periodic router advertisement broadcasts. These broadcasts result in unnecessary traffic being sent over the air once the aircraft's interface has been configured. The daemon will be configured to only respond to router solicitation requests from the aircraft when it is initially setting up its rftun interface using IPv6 autoconfiguration. Second, MOBIKE will be disabled in the *StrongSwan* configuration as it generates unnecessary overhead via informational messages it sends to its peer when interfaces change state. Since the security association is between a static IP address in the control element network and the HoA of the aircraft, the MOBIKE extensions are unnecessary when using a full Mobile IPv6 configuration with tunneling.

The following *StrongSwan* log shows the information messages recorded by the daemon during the tower handoffs as the active interface is switched from rftun1 to rftun0 and then back to rftun1:

```
Nov 15 18:24:28 Aircraft1 charon: 05[KNL] interface rftun1 deactivated
Nov 15 18:24:28 Aircraft1 charon: 10[KNL] 2001:db8::2d45:601:6fe2:6e8d:70da disappeared from rftun1
Nov 15 18:24:28 Aircraft1 kernel: [13151.996100] device rftun1 left promiscuous mode
Nov 15 18:24:28 Aircraft1 charon: 13[KNL] fe80::601:6fe2:6e8d:70da disappeared from rftun1
Nov 15 18:24:28 Aircraft1 charon: 14[IKE] sending address list update using MOBIKE
Nov 15 18:24:28 Aircraft1 charon: 14[ENC] generating INFORMATIONAL request 1 [ N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_4_ADDR)
N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) ]
Nov 15 18:24:28 Aircraft1 charon: 14[NET] sending packet: from UA[4500] to CN[4500] (157 bytes)
Nov 15 18:24:32 Aircraft1 charon: 11[IKE] retransmit 1 of request with message ID 1
Nov 15 18:24:32 Aircraft1 charon: 11[NET] sending packet: from UA[4500] to CN[4500] (157 bytes)
Nov 15 18:24:32 Aircraft1 charon: 12[NET] received packet: from CN[4500] to UA[4500] (49 bytes)
Nov 15 18:24:32 Aircraft1 charon: 12[ENC] parsed INFORMATIONAL response 1 [ ]
Nov 15 18:24:53 Aircraft1 charon: 06[KNL] fe80::601:457b:47de:4ca5 appeared on rftun1
Nov 15 18:24:53 Aircraft1 charon: 09[KNL] interface rftun1 activated
Nov 15 18:24:53 Aircraft1 kernel: [13176.873379] IPv6: ADDRCONF(NETDEV_UP): rftun1: link is not ready
Nov 15 18:24:53 Aircraft1 kernel: [13176.888420] IPv6: ADDRCONF(NETDEV_CHANGE): rftun1: link becomes ready
Nov 15 18:24:53 Aircraft1 charon: 12[IKE] sending address list update using MOBIKE
Nov 15 18:24:53 Aircraft1 charon: 12[ENC] generating INFORMATIONAL request 2 [ N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_4_ADDR)
N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) ]
Nov 15 18:24:53 Aircraft1 charon: 12[NET] sending packet: from UA[4500] to CN[4500] (157 bytes)
Nov 15 18:24:53 Aircraft1 charon: 13[NET] received packet: from CN[4500] to UA[4500] (49 bytes)
Nov 15 18:24:53 Aircraft1 charon: 13[ENC] parsed INFORMATIONAL response 2 [ ]
Nov 15 18:25:05 Aircraft1 charon: 15[KNL] 2001:db8::2d45:601:457b:47de:4ca5 appeared on rftun1
Nov 15 18:25:05 Aircraft1 charon: 05[IKE] sending address list update using MOBIKE
Nov 15 18:25:05 Aircraft1 charon: 05[ENC] generating INFORMATIONAL request 3 [ N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_4_ADDR)
N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) ]
Nov 15 18:25:05 Aircraft1 charon: 05[NET] sending packet: from UA[4500] to CN[4500] (157 bytes)
Nov 15 18:25:06 Aircraft1 charon: 14[NET] received packet: from CN[4500] to UA[4500] (49 bytes)
Nov 15 18:25:06 Aircraft1 charon: 14[ENC] parsed INFORMATIONAL response 3 [ ]
Nov 15 18:25:51 Aircraft1 charon: 07[KNL] interface rftun0 deactivated
Nov 15 18:25:51 Aircraft1 charon: 13[KNL] 2001:db8::1ce8:601:2ca5:415d:79ee disappeared from rftun0
Nov 15 18:25:51 Aircraft1 charon: 05[KNL] fe80::601:2ca5:415d:79ee disappeared from rftun0
Nov 15 18:25:51 Aircraft1 charon: 06[IKE] sending address list update using MOBIKE
Nov 15 18:25:51 Aircraft1 charon: 06[ENC] generating INFORMATIONAL request 4 [ N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_4_ADDR)
N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) ]
Nov 15 18:25:51 Aircraft1 charon: 06[NET] sending packet: from UA[4500] to CN[4500] (157 bytes)
Nov 15 18:25:55 Aircraft1 charon: 13[IKE] retransmit 1 of request with message ID 4
Nov 15 18:25:55 Aircraft1 charon: 13[NET] sending packet: from UA[4500] to CN[4500] (157 bytes)
Nov 15 18:25:55 Aircraft1 charon: 08[NET] received packet: from CN[4500] to UA[4500] (49 bytes)
Nov 15 18:25:55 Aircraft1 charon: 08[ENC] parsed INFORMATIONAL response 4 [ ]
```

These *tcpdump* data capture samples on the CN system show the effects of the handoffs and how the system is able to cope with rapid transitioning between two active interfaces (or ground stations) without needing to renegotiate the entire security association. Notice that the security association Security Parameter Indexes (SPIs) do not change and that the sequence numbers do not reset. The addresses are just updated via the IKEv2 protocol:

RFTUN0 *tcpdump* [Link to Ground Station 1]:

```
18:24:26.332065 IP6 fe80::1000:1bc:9fd:7fec > ff02::1: ICMP6, router advertisement, length 128
18:24:29.382218 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: DSTOPT mobility: BU seq#=41097 AH lifetime=75660
18:24:29.632372 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: srcrt (len=2, type=2, segleft=1, [0]UA) mobility: BA status=0 seq#=41097
lifetime=75660
18:24:30.232055 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x162), length 76
18:24:30.232378 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x160), length 76
18:24:30.732872 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x163), length 76
18:24:30.733132 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x161), length 76
18:24:31.232803 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x164), length 76
18:24:31.233035 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x162), length 76
18:24:31.632141 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x165), length 76
18:24:31.632354 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x163), length 76
18:24:32.132737 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x166), length 76
18:24:32.132972 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x164), length 76
18:24:32.484204 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  inf2
18:24:32.632851 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x167), length 76
18:24:32.633097 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x165), length 76
18:24:32.933059 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  inf2[IR]
18:24:33.132690 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x168), length 76
18:24:33.132920 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x166), length 76
```

```
18:24:34.731870 IP6 fe80::1000:1bc:9fd:7fec > ff02::1: ICMP6, router advertisement, length 128
18:24:44.432890 IP6 fe80::1000:1bc:9fd:7fec > ff02::1: ICMP6, router advertisement, length 128
18:24:53.385938 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  inf2
18:24:53.631904 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x191), length 76
18:24:53.632218 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x18f), length 76
18:24:53.832878 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  inf2[IR]
18:24:54.132711 IP6 HA > 2001:db8::1ce8:601:2ca5:415d:79ee: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x192), length 76
18:24:54.133001 IP6 2001:db8::1ce8:601:2ca5:415d:79ee > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x190), length 76
```

RFTUN1 *tcpdump* [Link to Ground Station 2]:

```
18:25:33.582476 IP6 fe80::2000:15a9:11cd:385e > ff02::1: ICMP6, router advertisement, length 128
18:25:52.252155 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: DSTOPT mobility: BU seq#=41099 AH lifetime=75576
18:25:52.582284 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: srcrt (len=2, type=2, segleft=1, [0]UA) mobility: BA status=0 seq#=41099
lifetime=75576
18:25:52.782256 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x207), length 76
18:25:52.782621 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1dd), length 76
18:25:53.182020 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x208), length 76
18:25:53.182301 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1de), length 76
18:25:53.482869 IP6 fe80::2000:15a9:11cd:385e > ff02::1: ICMP6, router advertisement, length 128
18:25:53.682116 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x209), length 76
18:25:53.682400 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1df), length 76
18:25:54.122092 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x20a), length 76
18:25:54.122375 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1e0), length 76
18:25:54.581928 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x20b), length 76
18:25:54.582204 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1e1), length 76
18:25:55.122144 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x20c), length 76
18:25:55.122433 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1e2), length 76
18:25:55.354368 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA.4500 > CN.4500: NONESP-encap: isakmp: child_sa  inf2
18:25:55.582095 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x20d), length 76
18:25:55.582377 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1e3), length 76
18:25:55.883027 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN.4500 > UA.4500: NONESP-encap: isakmp: child_sa  inf2[IR]
18:25:56.083425 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x20e), length 76
18:25:56.083719 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1e4), length 76
18:25:56.581916 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x20f), length 76
18:25:56.582193 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1e5), length 76
18:25:57.122118 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x210), length 76
18:25:57.122413 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1e6), length 76
18:25:57.582922 IP6 HA > 2001:db8::2d45:601:457b:47de:4ca5: IP6 CN > UA: ESP(spi=0xc6043759,seq=0x211), length 76
18:25:57.583196 IP6 2001:db8::2d45:601:457b:47de:4ca5 > HA: IP6 UA > CN: ESP(spi=0xc5d267a6,seq=0x1e7), length 76
18:25:58.882881 IP6 fe80::2000:15a9:11cd:385e > ff02::1: ICMP6, router advertisement, length 128
```

4.7 Network Performance

Figure 5 shows a summary of the round trip times over the course of an hour of the flight test run. All traffic from 17:30:00 to 18:24:00 was communicated between the UA and the CN via GS2. The first portion of the run (17:30:00 to 18:00:00 UTC) was with ROHC disabled and shows average round trip times of approximately 410 ms including 36 ms RTT caused by terrestrial latency between the CN and GS2. This is to be expected with the large overhead needed to accommodate the additional IPv6 headers for Mobile IPv6 tunneling and the ESP security headers for the encryption and integrity protection.

To reduce latency we enabled ROHC (around 18:03:00 UTC) which nearly cut the RTT average in half to about 215 ms. Again, these times included an additional terrestrial latency of 36 ms RTT between the CN and GS2. The generated traffic was sent at a rate of two 40-byte packets per second.

The periodic spikes in the graph are a result of extraneous traffic being transmitted over the channel and is mostly comprised of 128-byte IPv6 router advertisements sent from the ground station system every 10 to 15 sec. The additional semi-random traffic transmissions cause issues with the radio queue and results in these observed spikes in the latency. Implementation of a priority system in the data transmission channel is underway and should alleviate this issue. These periodic router advertisements will be eliminated in future tests by reconfiguring the system so that the ground station only sends a unicast router advertisement message upon receiving a router solicitation request from a remote system aboard the aircraft upon initial network entry and handovers.

This modification should completely eliminate the extraneous router advertisement spikes seen in the round trip time graph shown in Figure 5, and result in a much smoother graph. Figure 6 breaks out the ROHC disabled portion of Figure 5. Figure 7 breaks out the ROHC enabled portion of Figure 5. Finally, Figure 8 breaks out the tower handoff portion of Figure 5.

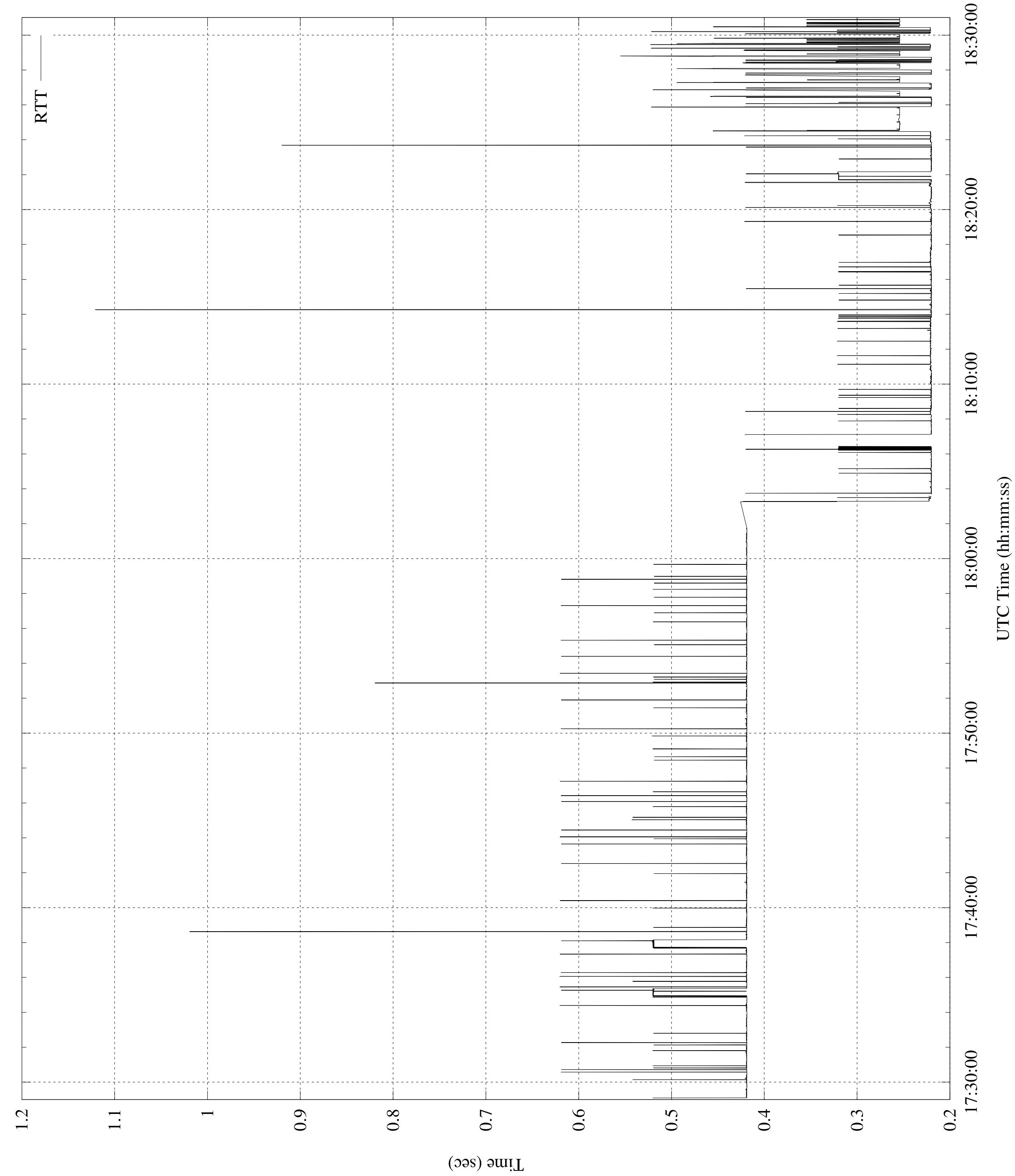

Figure 5.—Round Trip Times

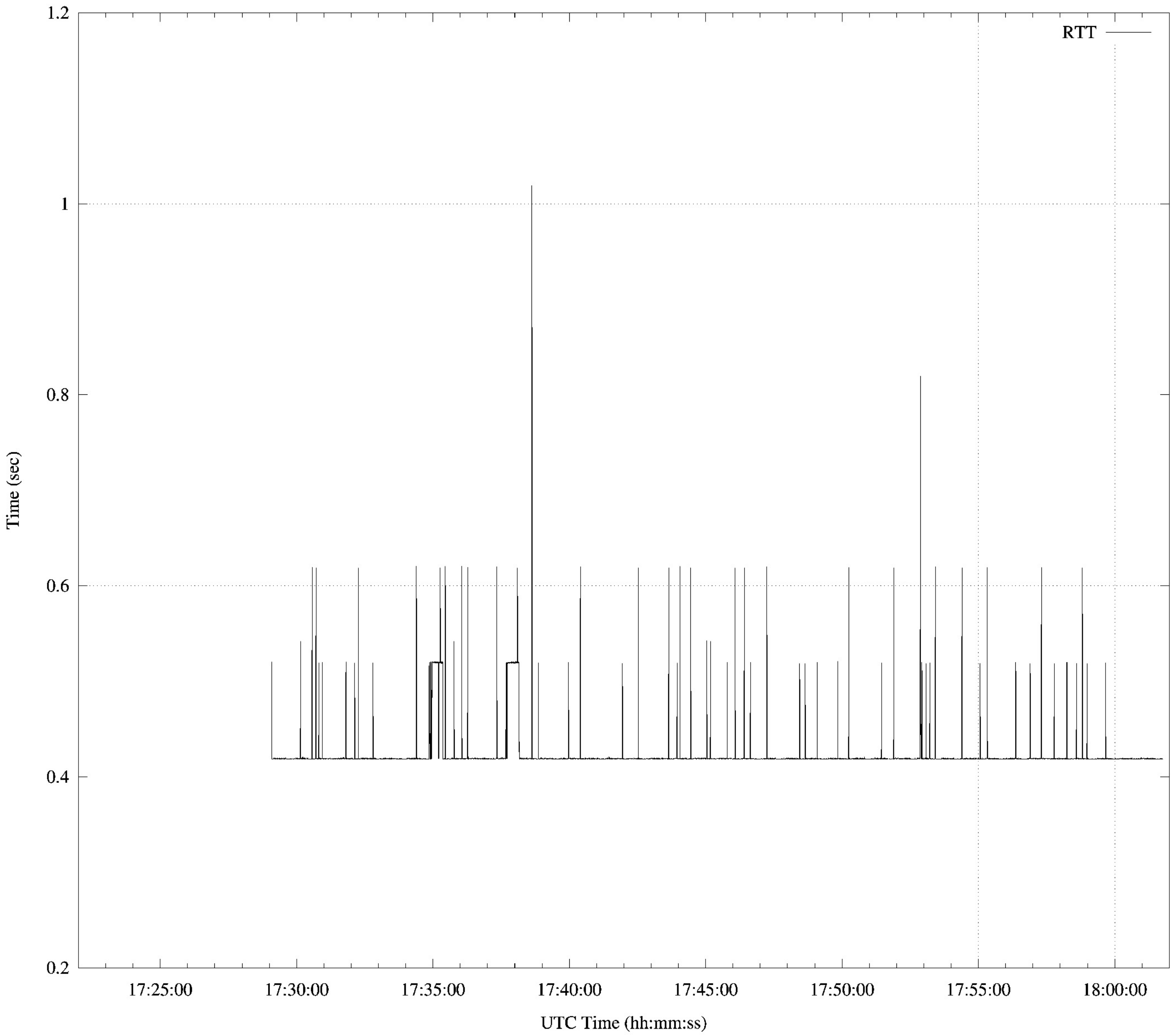

Figure 6.—Round Trip Time (ROHC Disabled)

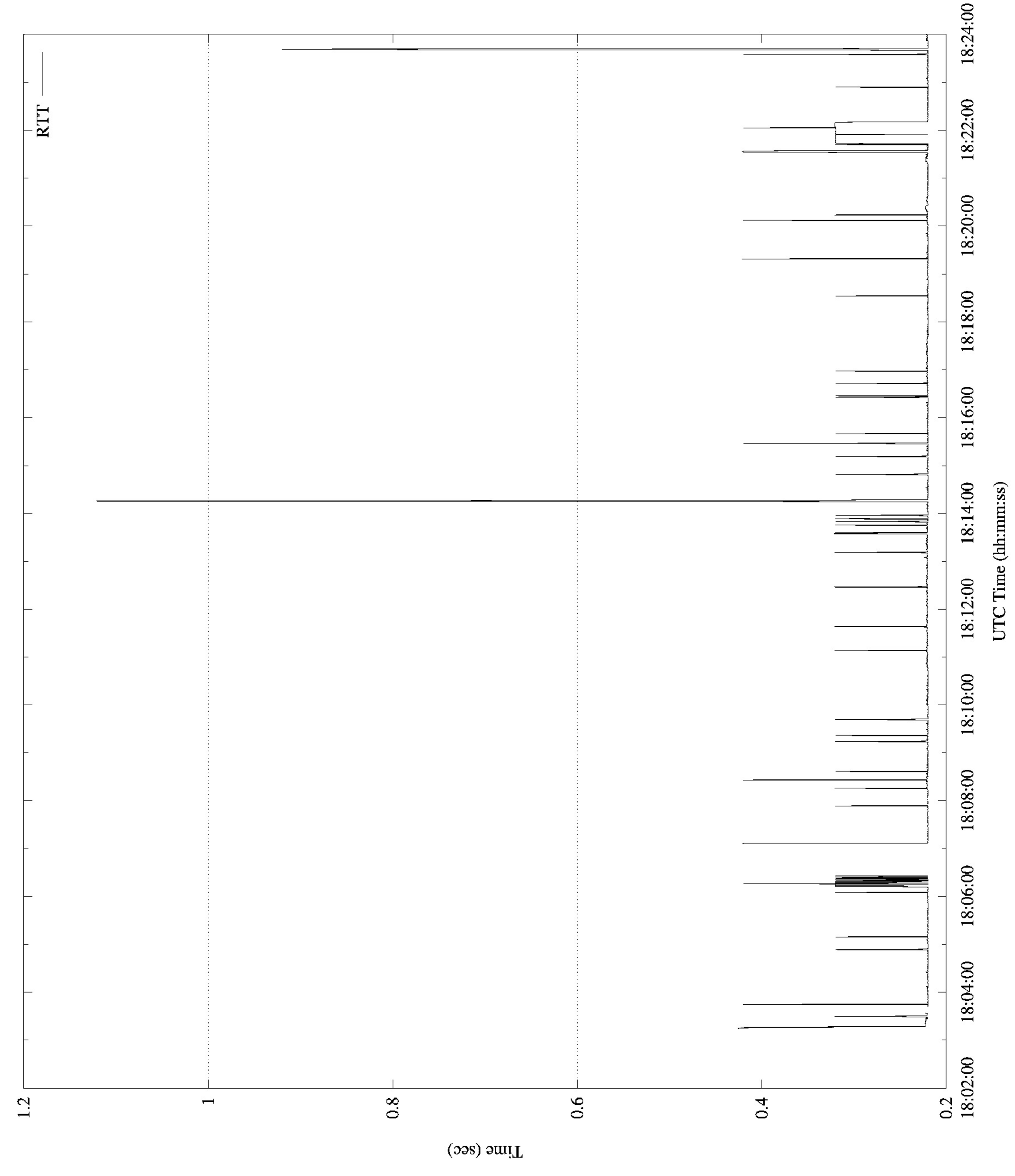

Figure 7.—Round Trip Time (ROHC Enabled)

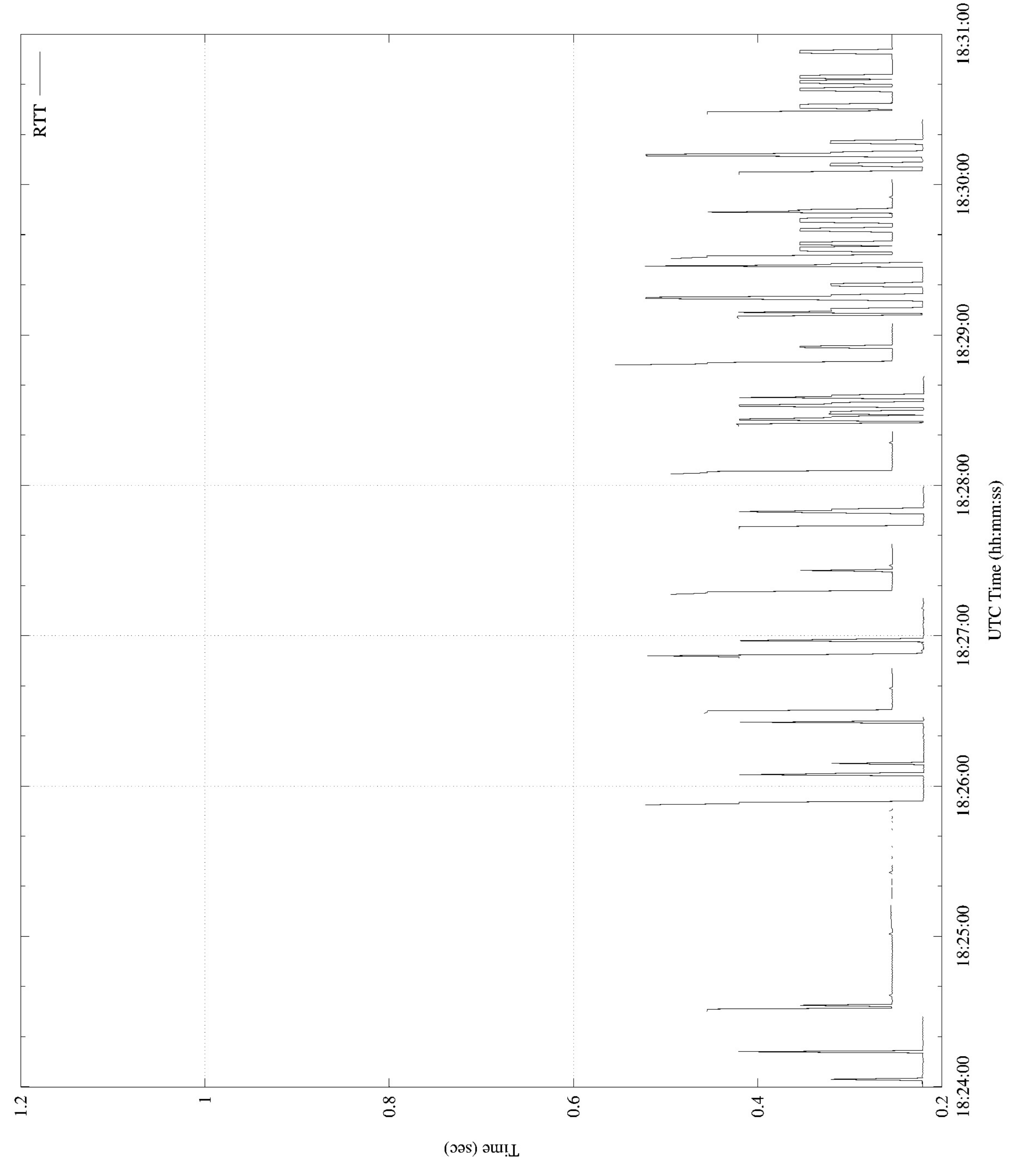

Figure 8.—Round Trip Time (Tower Handoffs)

5.0 Conclusion

The observed results of the test flight have conclusively shown that the system security controls developed over the course of the project to provide end-to-end network security could be successfully integrated into the relevant flight environment aboard NASA’s S-3B Viking surrogate unmanned aircraft. As required by the draft SC-228 MOPS security requirements, strong mutual authentication between the end nodes was demonstrated and end-to-end confidentiality and integrity protection was supplied by utilizing the standards-based IPsec ESP protocol in transport mode with 256-bit ECDSA certificates for

IKEv2-based authentication, 128-bit AES-GCM for encryption, and 64-bit CMAC for authentication codes to provide data integrity. In normal operation the system functions seamlessly to the end users and will dynamically create security associations as required to protect network flows.

As expected after analyzing the results from earlier lab testing, Mobile IPv6 and IPsec ESP in either tunnel or transport mode add a significant amount of overhead to accommodate the additional protocol headers required for operation. This additional overhead in turn adds a large amount of additional latency to the round-trip time for CNPC communications, as the IP packets must be fragmented into multiple radio frames to be transmitted across the radio frequency (RF) link. By introducing Robust Header Compression, the effects of this additional overhead were mitigated by virtually eliminating the vast majority of the header information in normal communications and in turn, this reduced the amount of traffic that needs to be transmitted to acceptable levels that are expected to meet FAA requirements.

Furthermore, it can be shown that additional optimizations can be made to the link performance by eliminating the periodic router advertisement broadcasts being sent across the air by configuring the ground station to operate in “UnicastOnly” mode and only respond to router solicitation packets from the aircraft. In addition, disabling the MOBIKE support in the *StrongSwan* daemon can eliminate unnecessary IKE informational messages from being broadcast to the security peer during layer-3 handoffs. Testing has determined it is unnecessary to maintain seamless secure communications when deployed in a full Mobile IPv6 tunneled architecture.

Future work with Rockwell-Collins will include enhancing the security controls of the current architecture by adding WiMAX-like datalink security controls like PKMv2 EAP authentication of control-plane traffic. Work is being planned to integrate this functionality into the next generation prototype radio system.

6.0 References

1. Ishac, J., Iannicca, D., Shalkhauser, K., and B. Kachmar: Control and Non-Payload Communications (CNPC) Prototype Radio - Generation 2 Flight Test Report. NASA/TM—2014-218391, 2014.
2. UMIP Development Team (2014), “UMIP,” Computer Software, http://www.umip.org
3. C. Perkins, Ed., Johnson, D., and J. Arkko, “Mobility Support in IPv6,” RFC 6275, July 2011. [Online]. Available: http://www.rfceditor.org/rfc/rfc6275.txt
4. Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, “Network Mobility (NEMO) Basic Support Protocol,” RFC 3963, January 2005. [Online]. Available: http://www.rfceditor.org/rfc/rfc3963.txt
5. Arkko, J., Devarapalli, V., and F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents,” RFC 3776, June 2004. [Online]. Available: http://www.rfceditor.org/rfc/rfc3776.txt
6. Devarapalli, V. and F. Dupont, “Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture”, RFC 4877, April 2007. [Online]. Available: http://www.rfceditor.org/rfc/rfc4877.txt
7. Steffen, A., “strongSwan,” Computer Software, http://www.strongswan.org
8. Law, L., Solinas, J., “Suite B Cryptographic Suites for IPsec”, RFC 4869, May 2007. [Online]. Available: http://www.rfceditor.org/rfc/rfc4869.txt
9. P. Eronen, Ed., “IKEv2 Mobility and Multihoming Protocol (MOBIKE),” RFC 4555, June 2006. [Online]. Available: http://www.rfceditor.org/rfc/rfc4555.txt