Workgroup: DRIP
Internet-Draft:
draft-moskowitz-drip-efficient-a2g-comm-00
Published: 4 April 2023
Intended Status: Standards Track
Expires: 6 October 2023
Authors: R. Moskowitz HTT Consulting
S. Card AX Enterprize
A. Gurtov Linköping University

Efficient Air-Ground Communications

Abstract

This document defines protocols to provide efficient air-ground communications without associated need for aircraft to maintain stateful connection to ground-tower infrastructure. Instead, a secure source-routed ground infrastructure will not only provide the needed routing intelligence, but also reliable packet delivery through inclusion of Automatic Repeat reQuest (ARQ) and Forward Error Correction (FEC) to address both reliable wireless packet delivery, and assured terrestrial packet delivery.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 6 October 2023.

Table of Contents

1. Introduction

The goal of this design approach is to place minimal network intelligence in the aircraft and even the wireless towers. Practically all the networking intelligence is placed within the Ground Station (GS). The justification for this approach is intelligence in the aircraft has disproportional costs to that in the GS; there are many factors in this claim. Lower intelligence requirements in the towers will make the technology more attractive to tower owners, provided there is an associated functional payment mechanism for them for the service.

The wireless downlink from the aircraft is treated as a broadcast message, with every receiving tower forwarding messages to the GS. The GS, in turns, notes which towers are in contact with the aircraft and sends uplink messages through them to the aircraft. There is no need for complex aircraft/tower connection technologies. At most, for billing purposes, the towers are aware of aircraft and

GS that will use their connectivity services via their source IP addresses.

2. Terms and Definitions

2.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Definitions

A2G
: Communications from an aircraft to some ground equipment. Also somethings GS.

3. Enabling and Enhancing Functions

The following is a list of enabling and enhancing functions.

3.1. Enabling Requirements

The aircraft:

* Support end-to-end secure communications with the GS and start the operation with the pre-configured GS IP address. The aircraft sends the first message, to the GS, to establish the routing knowledge in the GS,

* Use a fixed IP address for itself for the duration of the operation, and

* be able to process multiple copies of messages from the GS, received potentially from multiple towers.

The tower:

* Support digital signing of messages from the aircraft, and the tower's IP address, and forward these objects to the GS.

The GS:

* Support end-to-end secure communications with the aircraft,

* support processing multiple copies of messages from the aircraft,

* support digital signing by the tower, and

*maintain a list/map of towers forwarding aircraft messages from the aircraft for messaging to the aircraft. The list of trusted tower IP addresses is constructed from within the tower signed objects.

3.2. Enhancing Security Requirement

The GS should:

*Support digital signing for the tower to trust messages from the GS.

3.3. Enhancing Performance Requirements

The aircraft may:

*Support uplink usage optimizations like FEC and ARQ, and

*support GS IP address mobility (e.g. via HIP, [RFC7401]).

The tower may:

*Include information like timestamp and its GPS-derived location (and accuracy of same) in the signed object delivered to the GS,

*may be IP address mobile, if so, then MUST provide its IP address within the signed object,

*support multicast and DETNET (rfc8938) for efficient and reliable communications with the GS, and

*use a subscription model to filter messages supported for forwarding. If done with a list of registered IP addresses it MUST support GS IP address mobility.

The GS may:

*Support intelligent operation routing and tower contact information to select towers to use to send messages to the aircraft,

*support tower subscription for tower communication filtering,

*support multicast and DETNET for efficient communications with the towers,and

*support FEC and ARQ for efficient use of uplinks to the aircraft.

4. Background Discussion

The following considers the possible technologies, some challenges, and final proposed solution.

4.1. The problem and simple solution using IPnIP

Internet Protocol (IP) transmissions from the aircraft to ground, though unicast in construction (i.e. IP destination/source paired), are really broadcasts, as a practical matter, to all available ground towers. Such towers can simply send the packets on their way and they will naturally get routed, i.e. relayed, to the GS which correspondingly simply recognizes and processes potential multiple receipts via the many relaying towers. The problem is only the uplink: how to get IP transmissions from the GS to the aircraft.

The GS needs to ‘know’ which towers can likely transmit up to the aircraft and how to route packets through them. A simple solution is to use IP-in-IP (IPnIP) tunneling protocol [RFC1853]. Here, each receiving tower wraps the downlink message in IPnIP with the outer source address being the the tower’s address. The aircraft always uses a fixed source address (e.g. their respective DET [RFC9374]). The GS maintains an IPnIP tunneling table for each aircraft DET of the tower addresses. Packets inbound to the GS update this table (stale entries are purged) and the IPnIP service unwraps and forwards the inner content back through the IP kernel for sending up to the application. Packets outbound to the aircraft address get routed internally to the IPnIP process which ends up sending out multiple copies to each of the tower addresses in the table. Each receiving tower then simply unwarps and uplinks the content to the aircraft.

Though this approach works, it has security and traffic management challenges. First and foremost, the aircraft must know the GS IP address. It either needs to be fixed or the aircraft needs a separate process to update its knowledge of the GS address. The GS should have the aircraft address prior to operation start or can simply learn them through received messages.

There are two security issues associated with the GS processing messages from any random aircraft address:

* either these addresses are preset (e.g. registered DET), or there is some process for the GS to dynamically learn which to trust.

* a larger security challenge is why should the GS trust the address for the towers as a route to the aircraft. A malicious source could provide bad tower addresses resulting in loss of aircraft contact at worst, or consumption, through DOS attacks, of both GS processing resources and tower uplink bandwidth.

An additional challenge for the GS is determining which set of towers to use to send messages uplinked to the aircraft. Which of the towers last sending messages from the aircraft are still in RF reach of the aircraft and are there now towers better able to message the aircraft? If the GS can trust the towers and know their GPS location and the signal strengths of messages from the aircraft, the GS can use this map along with the map of the planned operation to better select towers for uplinking messages.

With all these stated concerns, the IPnIP approach should only be used for PoC and general testing. It presents too good of a DOS attack scenario for production deployments.

4.2. Improved tower trust through digital signing

Trust in tower messaging can be achieved by each tower cryptographically signing the received aircraft messages before forwarding them to the GS. This must be a specific signed object, perhaps in COSE format [RFC8152]. Not only would it contain the aircraft message with the tower's digital ID and signature, it should also minimally include a timestamp, the tower's GPS location plus GPS accuracy, and signal strength. With this information, a process on the GS can put the tower on a map with the planned aircraft flight plan. If three or more towers forwarded the message, the GS can also multilaterate the aircraft location for accurate location on the map. This information would allow the GS to predict which towers are still in range, or soon in range (i.e. predicting new towers for communications) of the aircraft for uplink messaging.

This signing method is preferable to secure tunnels from the tower to the GS as there will be thousands of GS using a small number of towers. How should tunnels be set up and torn down recognizing the cost to the tower system? It is preferable for the towers to be stateless in their forwarding to the GS. Also, it is questionable whether the GS should sign messages for the uplink. Doing so would potentially place the burden of processing cost on the tower, and analysis would be needed to avoid denial of service (DOS) attacks against towers and their uplink capacity.

The inclusion of GPS accuracy supports improved mobile tower multilateration. The timestamp also enables multilateration, in aging towers out of the reachable list of towers against the flight plan.

Thus, inbound processing on the GS would first place tower information into the aircraft reachable table mentioned above, then forward the aircraft message up to the application. For outbound, the aircraft address could result in passing the message to an IPnIP

service for simple forwarding to the tower as above, but as mentioned above IPnIP has DOS risks.

4.3. Inclusion of mobile ground systems

If the air-ground communications are secured with the Host Identity Protocol (HIP, [RFC7401]), the HIP mobility function can update the aircraft with any changes in the GS IP address. DTLS 1.3 [RFC9147] can be used only if the aircraft is the server as these support client, not server, mobility and the aircraft can learn of new GS addressing as it processes uplinked messages from the new addresses.

In any case, the aircraft address should be its DET and be unchanging for the flight duration.

4.4. Improved uplink reliability

If three or more towers provide the uplink, the GS can use Forward Error Correction (FEC) and send the fragments to different towers. The aircraft need only receive the proper set of fragments to reconstruct the full message. This both reduces the packet size on the uplink, conserving uplink capacity and increases both ground and wireless delivery reliability. Static Context Header Compression (SCHC, [RFC8724]) should also be used to reduce the size of the aircraft-ground messages. SCHC Automatic Repeat reQuest (ARQ) may also be used and will soon directly support FEC.

The ground communications path reliability can be further improved through use of a subset of Deterministic Networking (DETNET) (tbd) and Bit Indexing Explicit Replication (BIER) multicasting from the GS to the towers.

4.5. Alternative dedicated Tower-GS tunneling

There will be areas where significant traffic exists between a tower (or group of towers) and a GS. An example of such an area is around an aerodrome and its supporting systems. Here it makes performance sense that a secure tunneling technology (e.g ESP, [RFC4303]) be used between the tower(s) and GS(s) rather than digitally signing individual messages. Often, in such cases the ground network can be deployed to ensure reliable delivery.

5. Aircraft to GS Messaging

The aircraft and GS MAY have a pre-configured secure connection using technologies like DTLS, IPsec, or HIP. The aircraft SHOULD use its DET as its IPv6 address, and underlying HI for the rawPublicKey to establish the connection. Examples of this type of secure aircraft to GS is discussed in [drip-secure-nrid-c2].

There is a bit of chicken-and-egg here if the initial connection setup is not over a single link, as DETs are not easy to route over an IPv6 network. In such a case a tunnel, as discussed later, needs to be in place between the first hop from the aircraft (e.g. WiFi Access Point) and the GS.

In some instances, a pre-established aircraft-GS session is not practical (e.g. aircraft to airport traffic control). A variant of Section 3.2 of [drip-a2x-adhoc-session] (Compressed UA Signed Evidence of the A2X message) can be sent to the pre-configured GS IPv6 address:

Bytes	Name	Explanation
16	DET of Aircraft	DRIP Entity Tag of Aircraft
16	Destination Address	IPv6 address of GS
4	VNA Timestamp	Timestamp denoting recommended time to trust Evidence
1	Message ID	A2G Message ID Number
n	A2G Message	Actual A2G Message
64	Signature by Aircraft	Signature over preceding fields using the keypair of the Aircraft DET

Table 1: 101+n Byte Aircraft Signed A2G message

This message is a SCHC compressed IPv6/UDP datagram. The signature is on the whole datagram. The wireless transport will have some mechanism (e.g. SCHC as Ethertype) to trigger the SCHC rule processing to compress the datagram for transmission. Depending on the wireless technology there will be a 1-byte SCHC RuleID after the SCHC Ethertype (or equivalent). If the IP Header is sent without SCHC compression, then SCHC will need to be the Next Header in the IPv6 Header and the SCHC RuleID will immediately follow the IPv6 Header.

The full uncompressed message is:

Bytes	Name	Explanation
40	IPv6 Header	IPv6 Header from Aircraft to GS
8	UDP Header	Full UDP Header
4	VNA Timestamp	Timestamp denoting recommended time to trust Evidence
1	Message ID	A2G Message ID Number
n	A2G Message	Actual A2G Message
64	Signature by Aircraft	Signature over preceding fields using the keypair of the Aircraft DET

Table 2: IPv6 117+m+n Byte Aircraft Signed A2G message

Any tower that receives these messages and has a tunnel to the destination IPv6 address uses it to forward the message to the GS. The GS will use the aircraft DET to retrieve, via DNS, the HDA Endorsement of the DET. This will provide the aircraft HI to validate the signature.

A tower MAY validate the signature by using the aircraft DET to retrieve via DNS the HDA Endorsement of the aircraft DET. The tower may choose to leave this validation to the GS as it is terrestrial network that may be DOSed from wireless transmissions.

5.1. The Tower to GS tunnel

It is impractical for most towers to maintain long-lived static tunnels as described in Section 4.5. Too many towers will need to forward messages to too many GS for static tunneling. Rather, per-packet tunneling will be frequently used. These tunnels are the Aircraft-GS packets wrapped in a signed IPv6 datagram from the tower's IPv6 address to the GS's address that is in the A-GS packet:

Bytes	Name	Explanation
40	IPv6 Header	IPv6 Header from Tower to GS
8	UDP Header	Full UDP Header
16	DET of Tower	DRIP Entity Tag of Tower
4	VNA Timestamp	Timestamp from tower denoting recommended time to trust Evidence
m	Tower Location	Optional tower location
m	A2G Message	Full A2G Message
64	Signature by Tower	Signature over preceding fields using the keypair of the Tower DET

Table 3: IPv6 117+n Byte Aircraft Signed tunnel message

The GS will use the tower DET to retrieve, via DNS, the HDA Endorsement of the tower. This will provide the tower HI to validate the signature.

The UDP Destination Port can be the indicator of the presence of the Tower Location information. If absent, this information needs to be accessible via DNS using the Tower's DET (or pre-configured in the GS). If the tower is physically mobile, this information SHOULD be included.

The GS MUST be able to handle multiple copies of the A2G message. It MUST use the Tower location information to maintain a mapping for routing messages to the aircraft. It MAY use knowledge of the aircraft's planned flight to adjust this routing information as to which tower's are likely to be within reach of the aircraft.

6. GS to Aircraft Messaging

In most cases, the GS to aircraft messaging is the mirror of aircraft to GS. The important difference is how the GS selects towers for forwarding G2A messages and how the towers pre-process these messages before using precious wireless bandwidth in sending messages.

The GS uses some process to select towers from the list of towers last forwarding aircraft messages to the GS plus knowledge of the aircraft flight and other towers in the area.

The GS to tower tunnel is the mirror of Section 5.1 without the location information. The tower SHOULD validate the authenticity of the GS via DNS retrieved HDA Endorsement of the GS DET. It MAY also filter messages based on having recently received aircraft to GS messages.

The tower takes the G2A message from within the tunnel, adding any needed wireless heading and transmits the datagram.

The aircraft MUST be able to process multiple copies of an G2A message coming from multiple towers.

7. IANA Considerations

TBD

8. Security Considerations

TBD

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9374] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)", RFC 9374, DOI 10.17487/RFC9374, March 2023, <https://www.rfc-editor.org/info/rfc9374>.

9.2. Informative References

[drip-a2x-adhoc-session] Moskowitz, R., Card, S. W., and A. Gurtov, "Aircraft to Anything AdHoc Broadcasts and Session", Work in Progress, Internet-Draft, draft-moskowitz-drip-a2x-adhoc-session-01, 4 April 2023, <https://datatracker.ietf.org/doc/html/draft-moskowitz-drip-a2x-adhoc-session-01>.

[drip-secure-nrid-c2] Moskowitz, R., Card, S. W., Wiethuechter, A., and A. Gurtov, "Secure UAS Network RID and C2 Transport", Work in Progress, Internet-Draft, draft-moskowitz-drip-secure-nrid-c2-12, 26 March 2023, <https://datatracker.ietf.org/doc/html/draft-moskowitz-drip-secure-nrid-c2-12>.

[RFC1853] Simpson, W., "IP in IP Tunneling", RFC 1853, DOI 10.17487/RFC1853, October 1995, <https://www.rfc-editor.org/info/rfc1853>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[RFC8724] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <https://www.rfc-editor.org/info/rfc8724>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/info/rfc9147>.

Acknowledgments

Adam Wiethuechter of AX Enterprize provided review and implementation insights. Michael Baum provided extensive review of the contents in chapters 3 and 4 in a prior white paper.

Authors' Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America

Email: rgm@labs.htt-consult.com

Stuart W. Card
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: stu.card@axenterprize.com

Andrei Gurtov
Linköping University
IDA
SE-58183 Linköping
Sweden

Email: gurtov@acm.org