IPS Security: Numbers of Sessions - *Revisited*

AEEC IPS MEETING 20
7-9 DECEMBER 2021

MICHAEL OLIVE

Honeywell

Summary from prior presentation on this topic

- The number of security contexts established and maintained by the aircraft may be influenced by the placement of the ground IPS and application layer security endpoint

Assumption	Ground IPS Placement Option	CM	CPDLC	ADS-C	AOC	Total
A separate secure session is required for every application	• End-System hosted • ANSP-hosted IPS GW • Service Provider-hosted IPS GW	3 (current, next, intermediate)	3 (current, next, + listener)	4 + 1 (active + listener)	2 ?	**13+**
A secure session between an Airborne IPS System and an IPS GW accommodates multiple applications	• ANSP-hosted IPS GW	4 + 1 (assume ADS-C is worst case)			2 ?	**7+**
	• Service Provider-hosted IPS GW	1				**1**

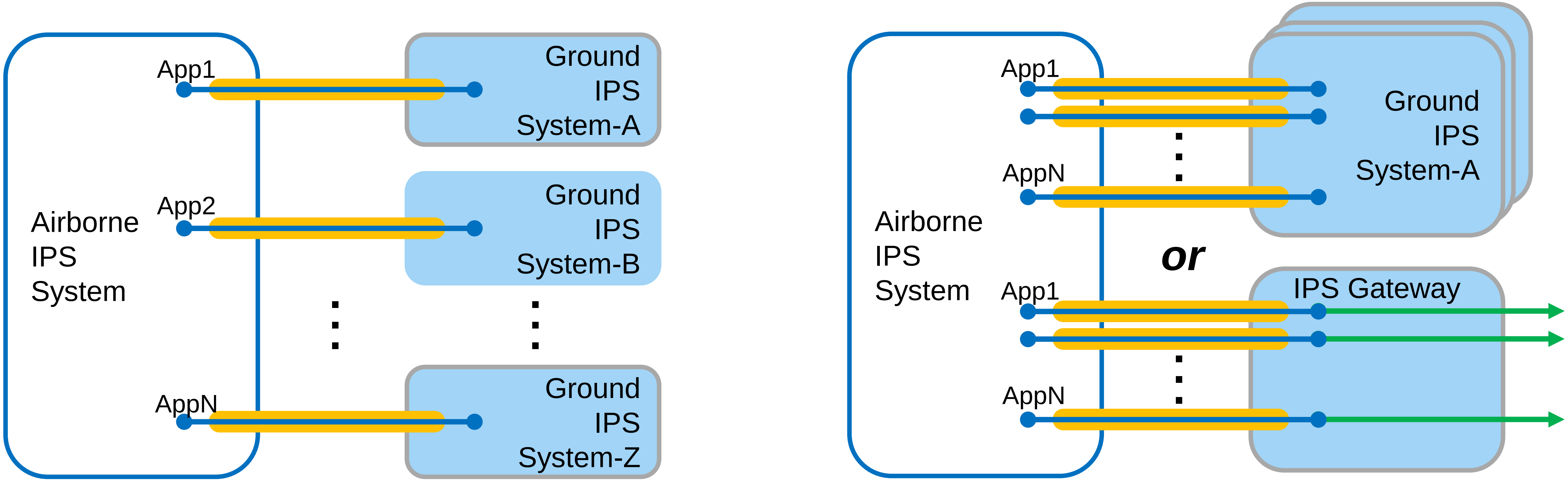
- IF a separate security session is mandatory for every application, then there may be opportunities to optimize DTLS session establishment overhead using the session resumption feature

  → Further consideration/investigation necessary

- Order of magnitude point-of-reference, not absolute
- Legacy apps only
- Does not yet consider Native IP apps

Secure Session per Application

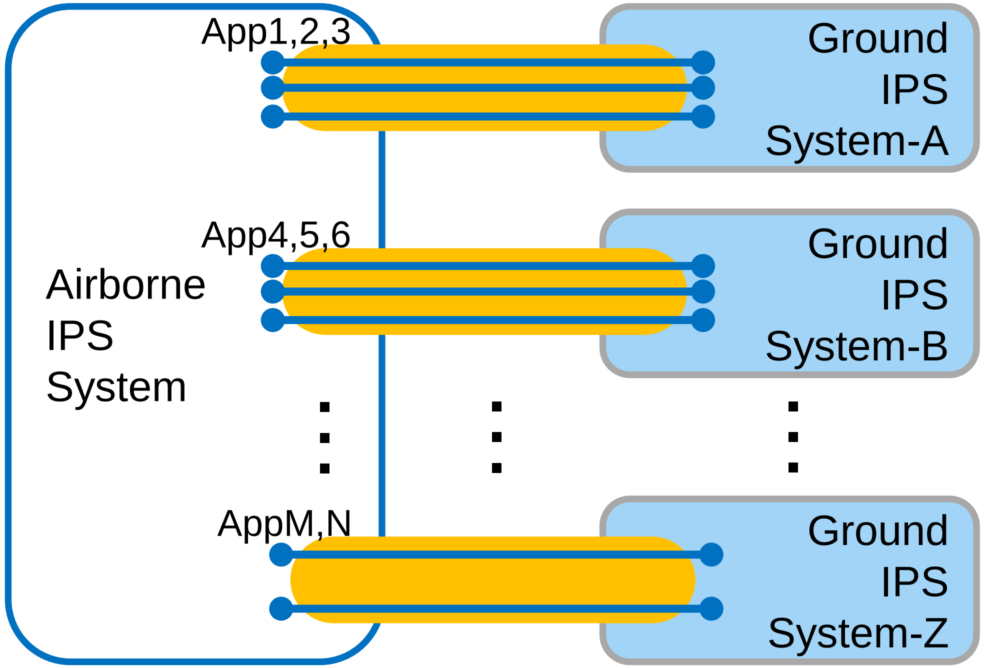
●—● App-over-IPS
→ App-over-Other
▬ DTLS

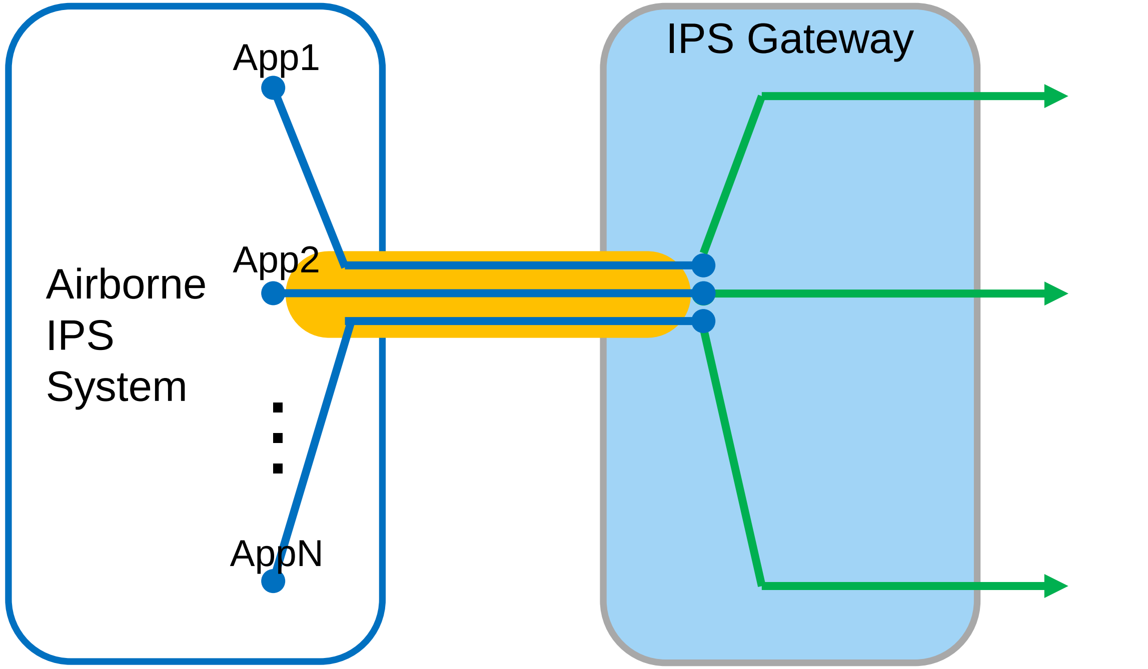


- DTLS terminates at a different Ground IPS System (e.g., ANSP, AOC) for each airborne application
- DTLS terminates at a Ground IPS System(s) (e.g., ANSP, AOC) ***or*** at an IPS Gateway for each airborne application

→ In either case, 13+ simultaneous sessions (CM/3, CPDLC/3, ADS-C/5, AOC/2+, ++)

Secure Session per IPS Entity





- DTLS terminates at one or more Ground IPS Systems (e.g., ANSP, AOC) and secures one or more airborne applications

  → 7+ simultaneous DTLS sessions (ADS-C/5, AOC/2+, ++), one per entity. Assumes that CM and CPDLC share ANSPs in common with ADS-C

- DTLS terminates at an IPS Gateway and secures all airborne applications

  → 1 DTLS session for all applications

HOWEVER,…

Feedback from Timo

I am very skeptical that a single session per A/C and ANSP / GW is technically feasible / reasonable. It would mean that a DTLS session spans multiple UDP ports and would not be bound to a particular application.

This seems to imply one of the following two approaches:

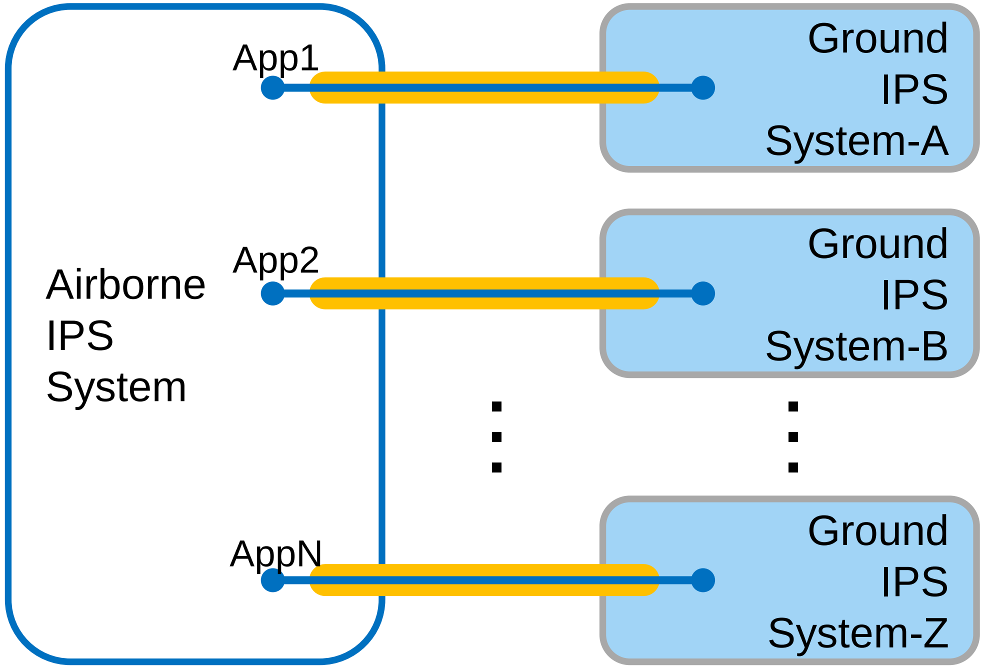
- When receiving a UDP datagram, the UDP port information is not relevant for making available the payload to an application. → That is, DTLS verifies (and possibly decrypts) the datagram, passes the payload to an upper layer, which decides (without port information, based on payload info only) which application shall receive the payload. In this case, the question is why we are using separate UDP ports for applications at all.
- When receiving a UDP datagram, the DTLS decrypts / verifies the datagram and passes the payload to an upper layer along with UDP port information. → That is, UDP port information has to be tracked across the DTLS layer. The need for ordering application messages / DTLS records seems to need some further evaluation for such an approach. To be checked, how well this is supported by DTLS implementations.

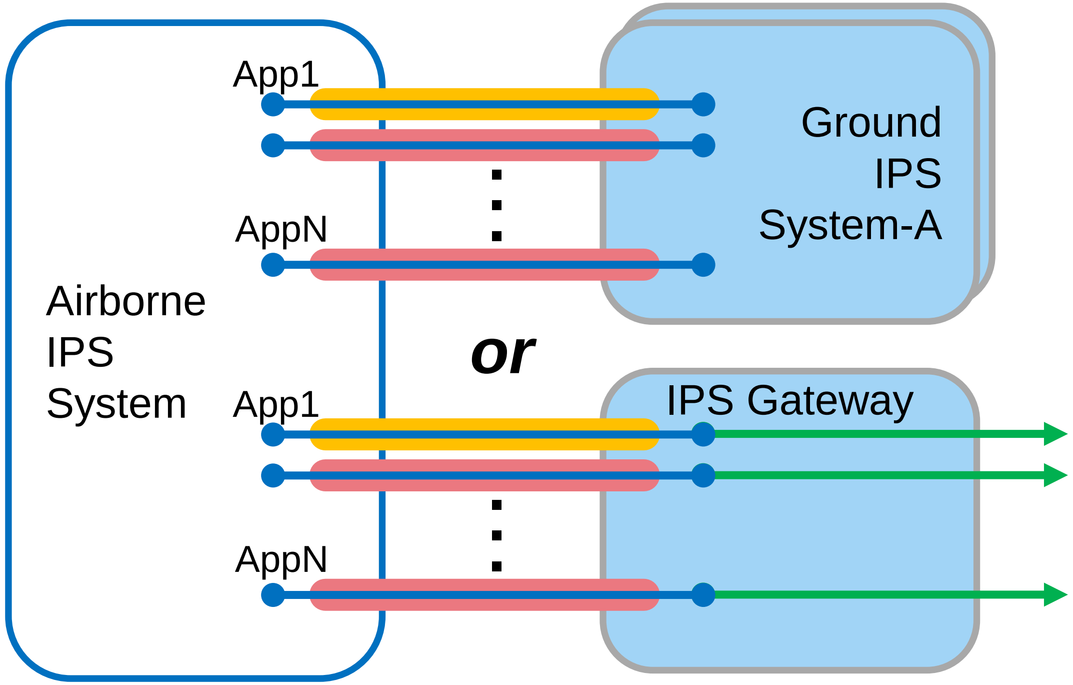
To some extent, these approaches seem to emulate a VPN with DTLS.

From my perspective, there may be some possibilities to avoid a full handshake for each session (e.g., using the session resumption mechanism even though the "previous" session is still running). Hence, we should be careful in distinguishing handshake overhead and number of sessions. We may be able to come up with a solution that minimizes handshake overhead, while still keeping separate DTLS sessions.

Secure Session per Application – Optimization [1/2]

- ●–● App-over-IPS
- → App-over-Other
- 🟨 DTLS
- 🟥 DTLS'





- Optimization does not change the math when DTLS terminates at a different Ground IPS System (e.g., ANSP, AOC) for each airborne application
  → 13+ simultaneous sessions (CM/3, CPDLC/3, ADS-C/5, AOC/2+, ++)

- Potential to minimize handshake overhead when DTLS terminates at a Ground IPS System(s) (e.g., ANSP, AOC) ***or*** at an IPS Gateway for one or more airborne applications.

  → *see next slide*

Secure Session per Application – Optimization [2/2]

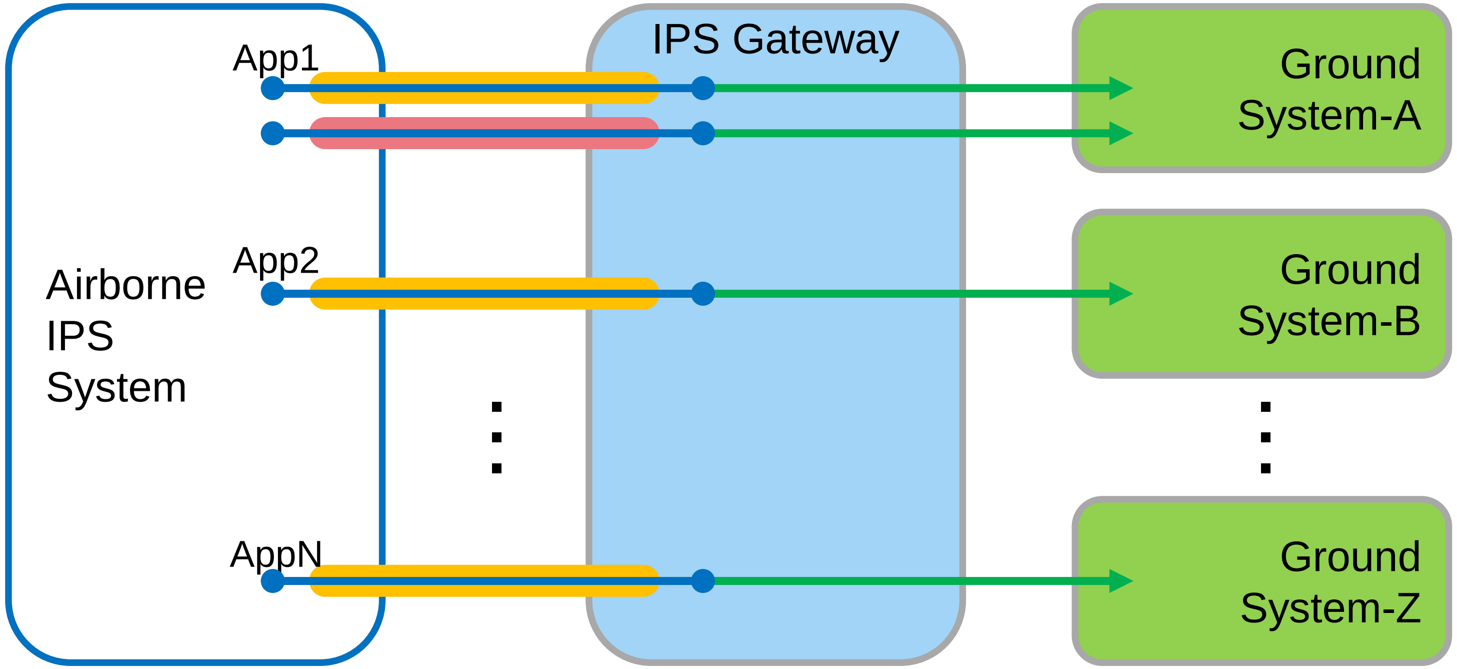
●━● App-over-IPS
━▶ App-over-Other
━ DTLS

- With potential optimization when DTLS terminates at

  → ANSP or AOC: up to 7+ simultaneous <u>sessions</u> (ADS-C/5, AOC/2+, ++)

  Assumes that CM and CPDLC share ANSPs in common with ADS-C

  → IPS Gateway: if there's a different ground system associated with each airborne application and <u>if each application must be secured on a per-end-entity basis</u>, then the worst-case is still up to 13+ simultaneous <u>sessions</u>



Is this the requirement??

Optimization may be possible technically, but it may not be desirable from a security and/or legal/liability perspective.

Discussion

- **DTLS optimization should be pursued to minimize overhead (bits over the air) and improve performance**
  - ICAO Doc. 9896 interoperability
    - Already includes considerations for session resumption
  - RTCA/EUROCAE IPS Profiles
  - RTCA/EUROCAE MASPS
    - Guidance on optimization with respect to deployment options
    - Still need to think about technical feasibility of spanning multiple ports (with least impact on standard behavior)
  - AEEC A858 → reference to those documents

- **Even if DTLS optimization is possible, the Airborne IPS System needs to accommodate the worst-case → a different Ground IPS System for every airborne application**
  - Resource dimensioning and performance to support a minimum of 13+ simultaneous DTLS sessions