Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 2, Number 13; April-June, 2015 pp. 1159-1162
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Evaluation of Protocols to Support IP Mobility in Aeronautical Communications

Kapil Sharma

Delhi Technological University
E-mail: kapil@ieee.org

Abstract— *The aviation trade is presently at the opening of a modernization phase about its communication systems. This involves a transition to IP-based networks for Air Traffic Manage and Airline Operational Communications. Due to the heterogeneous nature of the communication environment, support for mobility among dissimilar access technologies and access networks becomes required. We initial introduce the aeronautical communications environment and their domain specific requirements. The major part of this article is a survey of dissimilar protocols that can be used to solve the IP mobility difficulty in the aeronautical environment. These protocols are assessed with regard to the introduced requirements.*

Keywords: *Aeronautical Access Technologies, Mobility, IPv6, Mobile IP.*

1. INTRODUCTION

The communication infrastructure currently used for civil aeronautical communications is based on an analogue voice system that can neither cope with the expected improve in air traffic nor support the envisaged paradigm shift towards data or packet oriented communications. The digitalization effort is supposed to free-up the at this time congested analogue voice based system and to improves, operational efficiency. The Internet Protocol IPv6 has been select as the basis for the Aeronautical Telecommunications Network (ATN/IP) as:

- It is a widely used industry standard in telecommunications
- It is actively maintained and extended by the accountable standardization organization, the Internet Engineering Task Force (IETF).
- It provides sufficient address space for a world-wide deployment in each national state and aircraft.

2. THE AERONAUTICAL ENVIRONMENT

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of Units

3. AERONAUTICAL ACCESS TECHNOLOGIES

The future ATN will employ dissimilar access technologies for carrying IP-based traffic that makes this network ("greatly" heterogeneous. At airports standard IEEE 802.11 [1] (WiFi) equipment is already in use for providing wireless connectivity for AAC communications when the aircraft is standing at the gate.. This technology will provide some Mbit/sec per radio cell for ATS and AOC traffic. Standard WiMAX can be used to provide connectivity for AAC and APC. Most of the ATS traffic more continental areas, as well as AOC traffic, will be carried by the L-Band Digital Aeronautical Communications System L-DACS, a technology that is at present¬ in development.

4. MOBILITY REQUIREMENTS

In this section, we specify inherent, primary and secondary needs that have to be fulfilled by a mobility protocol used in the aeronautical environment. The word "aircraft" refers to a total mobile network, consisting of an airborne router and at least one network prefix. Some end-system (MNNs) are connected to this airborne router. The inherent requirements that must be completely fulfilled by all candidates are as follows.

a. Session continuity: This property provides a stable IP address for use to higher layer protocols, even in case of handovers.
b. Mobile Network support: Mobility should not only be provided for a single mobile host, but for a complete onboard network. More specifically, instead of providing a constant IP address (as the case for the previous requirement) one or some constant network prefixes should be provided. "Session continuity" is automatically fulfilled by all mobility protocols investigated later.

The requirements that should all be fulfilled by the candidate protocols are as follows:

Multihoming: The aircraft should be capable of routing data simultaneously over different interfaces/ paths from the aircraft to the ground. This requirement covers both load-balancing and fault-tolerance. The latter addresses the main issue of reliability/availability

Security 1 (masquerading): An attacker must not be able to claim the constant addresses/prefixes of an aircraft, e.g. by means of man-in-the-middle attacks.

Security 2 (DoS): The mobility protocol itself should not introduce any new denial of service vulnerabilities.

End-to-end delay: The delay among the communication peers should be kept minimal.

Scalability: The impact of the mobility protocol on the universal routing infrastructure should be kept to a minimum, meaning that frequent route announcements/ withdrawals for each individual aircraft should be avoided.

Applicability to AAC/APC: Specifies whether the solution is also applicable to non-safety related services. This indicates whether the protocol stack on the last systems has to be modified in order to support mobility.

Secondary requirements are desirable and their fulfilment is a bonus:

1. Efficiency 1: The overhead incurred by the mobility protocol itself should be limited. The number of roundtrip times (RTTs) needed for mobility-related signalling should therefore be kept minimal.
2. Efficiency 2: The overhead imposed upon each individual packet with payload from the MNNs or CNs should be limited. The number of additional protocol headers, needed to support mobility, should therefore be kept minimal.
3. Convergence time: Convergence time is also influenced by the number of exchanged signalling messages as described by Efficiency 1, this need is restricted to the time it takes to propagate the new mobility state throughout the (routing) system.

Support for ground-initiated communications: End systems on the ground should be capable of sending packets to an aircraft they have not yet communicated with. This means that a routing path to the current location of an aircraft has to be available for these nodes. It is preferable to have a single protocol (family) as a solution for all domains, ATS/AOC/AAC/APC.

5. MOBILITY OPTIONS

The Protocols for providing IP mobility are also discussed in [2], [3], with a focus on the aeronautical environment in [4]. Our investigation is different from the previous ones by (a) having introduced numerous needs and (b) by assessing the protocols based on those requirements. While the work performed in [4] also specifies certain requirements, many of them are high level. We investigate the protocols and perform our analysis with a higher degree of detail. Also, the second addresses an main optimization problem that is not covered at all by [4]. We therefore focussed on protocols between the network and transport layer for our investigation. We identify dissimilar protocols that can be categorized as follows:

- Routing protocol based approach (network layer), with the example of the Border Gateway Protocol.
- Tunnelling based approaches (network layer), with the examples of the IPsec and Mobile IP protocol families.
- A transport protocol approach, with the example of the Stream Control Transmission Protocol.
- Locater-identifier split (between network and transport layer), with the example of the Host Identity Protocol.

6. BORDER GATEWAY PROTOCOL (BGPV4)

The Border Gateway Protocol Version 4 (BGPv4) [5] is the inter-domain routing protocol mostly used in the Internet. BGP is used between autonomous systems for exchanging information on routing paths to specific destination prefixes. Routing information is distributed to neigh boring routers that fill in their routing tables and forward the routing information to other selected routers. BGP has already been used in the past for providing (IPv4) Internet Connectivity to the APC domain via GEO satellites.

7. BORDER GATEWAY PROTOCOL (BGPV4)

IPSec [6] is a well known protocol providing confidentiality, data integrity and data source authentication. These services are provided by maintaining a joint state among the two communication peers, also called Security Association (SA). Establishing such a SA manually would not be scalable, hence the Internet Key Exchange (IKEv2) protocol [7] provides the means to create and manage them dynamically. IKE mutually authenticates the two peers, based on either pre-shared secrets, certificates or the Extensible Authentication Protocol (EAP) [8]. In case of a VPN-like approach where an IP-in-IP tunnel is established, if one of the two IPSec peers moves to a different network and configures a new IP address, the established SAs would not be usable anymore.

8. NETWORK MOBILITY (NEMO)

Text The Network Mobility (NEMO) protocol [9] is an extension to Mobile IPv6 (MIPv6) [10]. NEMO extends the concept of a mobile node to that of a Mobile Router (MR) with one or some mobile network prefixes. As soon as the MR attaches to a foreign network it registers the new CoA with its Home Agent (HA) in the home network and creates a bi-directional tunnel for forwarding traffic between the nodes of the mobile network and the communication peers on the ground via the HA.

9. NETWORK MOBILITY (NEMO)

SCTP is a connection-oriented transport layer protocol comparable to TCP, but with additional features such as multihoming. The original SCTP specification allows specifying several IP addresses during connection setup time only. This limitation has been removed with [11] where newly configured IP addresses can be dynamically added to or deleted from an SCTP association by one of the two communication peers. This is particularly useful for a mobile node where IP addresses appear and disappear due to handovers between different access networks. The original SCTP specification allows specifying some IP addresses during connection setup time only. This limitation has been removed with [11] where newly configured IP addresses can be dynamically added to or deleted from an SCTP association by one of the two communication peers.

10. HOST IDENTITY PROTOCOL (HIP)

Another, more radical, approach for supporting mobility is the locator-identifier split, where a new shim layer between the network and the transport layer is introduced. This layer also introduces a new namespace on top of the IP address space. In HIP, Host Identity Tags (HITs - the identifiers) are mapped to the available IP addresses (locators) with the help of IPSec. The HITs are generated from the public key and therefore cryptographically bound to it. Only the owner of the corresponding private key can make use of the related HIT in the HIP protocol exchanges. If the HIP-enabled mobile node attempts to communicate with a HIP correspondent node, it initiates a message exchange to establish a common session based on the HITs of the two nodes and the IP addresses they want to use for message exchange

11. HOST IDENTITY PROTOCOL (HIP)

WINMO which stands for Wide-Area IP Network Mobility was introduced in 2008 to address the routing update overhead problem of Connexion. Like Connexion, WINMO also assigns each mobile network a stable prefix. However, through two new approaches, WINMO can reduce the BGP updates overhead for mobile networks by orders of magnitude lower than those of Connexion. Thus, packets destined to mobile networks are forwarded to DBR after they enter the border of an AS, and DBR will tunnel them to the current locations of mobile networks.

12. HOST IDENTITY PROTOCOL (HIP)

The discussion of all the various protocols shows that there is no optimal solution that is capable of fulfilling all requirements”out of the box”. In the following, we give idea a how the requirements are graded and discuss how they are fulfilled by each protocol.

13. GRADING OF MOBILITY REQUIREMENTS

The grading of the property Multihoming is either completely fulfilled/Optional (C.F/O.), Basically Fullfield/Fair fullfield with limitations (B.F/F.) or not Unsupported/Poor not fulfilled (U/P.). The latter is applied if load-balancing is not supported.

Security 1 is either completely fulfilled (C.F/O.), or not fulfilled (U/P.).

Security 2 has the additional grading levels (B.F/F.) and (U/P.) that point to those vulnerabilities exist but the probability for an attacker to exploit them is very small, given that sure precautions are taken.

The end-to-end delay can be either optimal (C.F/O) or suboptimal (U/P).

Scalability always refers to the entries in the BGP routing tables, except for HIP that only creates entries in the DNS (U/P.) indicates linear scalability with number of mobile nodes and (B.F/F.) Indicates linear scalability with number of aggregated prefixes. Finally Limitation/Average (L/A.) for HIP is scalability with number of mobile nodes, but graded better because it only impacts the DNS. More precisely, the DNS entry of a mobile node is only stored at a single DNS server.

Applicability to AAC/APC is either possible (C.F/O.) or not possible (U/P.).

Convergence time is either limited to the time it takes to signal the new location to a single node (C.F/O.), influenced by DNS lookup and forwarding of the initial packet by a rendezvous server (B.F/F.) or depending on the convergence time of the global routing tables (L/P.) for an inter network of limited size, such as the ATN.

The gradins of the individual protocols for Efficiency 1 and Efficiency 2 are relative to each other.

Ground-initiated communications is either fully supported (C.F/O.), supported with a dependency on the DNS (B.F/F.) or not supported at all (U/P.). Table 1 shows a brief comparison of six mobility protocol of Aeronautical Environment.

Table 1: Comparisons many type of protocol under the Aeronautical Environment

Protocol	BGP	IPSec	NEMO
Session Continuity	(C.F/O)	(C.F/O)	(C.F/O)
Mobile Network Support	(C.F/O)	(C.F/O)	(C.F/O)
Multihoming	(L/A)	(U/P)	(C.F/O)
Security 1	(C.F/O)	(C.F/O)	(C.F/O
Security 2	(B.F/F)/(L/A)	(C.F/O)	(C.F/O)
End-to-end delay	(C.F/O)	(U/P)	(U/P)
Scalability	(U/P)	(B.F/F)	(B.F/F)
Applicability to AAC/APC	(C.F/O)	(C.F/O)	(C.F/O)
Convergence time	(L/A)	(C.F/O)	(C.F/O)
Efficiency 1	(U/P)	(B.F/F)	(B.F/F)
Efficiency 2	(B.F/F)	(U/P).(U/P)	(U/P)
Ground -initiated comms	(C.F/O)	(C.F/O)	(C.F/O)

Protocol	SCTP	HIP	WINMO
Session Continuity	(C.F/O)	(C.F/O)	(C.F/O)
Mobile Network Support	(U/P)	(C.F/O)	(C.F/O)

Multihoming	(U/P)	(L/A)	(B.F/F)
Security 1	(U/P)	(C.F/O)	(C.F/O)
Security 2	(L/A)	(L/A)	(B.F/F)
End-to-end delay	(C.F/O)	(C.F/O)	(C.F/O)
Scalability	(C.F/O)	(L/A)(for DNS)	(B.F/F)
Applicability to AAC/APC	(U/P)	(U/P)	(C.F/O)
Convergence time	(C.F/O)	(B.F/F)	(B.F/F)
Efficiency 1	(B.F/F)	(L/A)	(L/A)
Efficiency 2	(B.F/F)	(L/A)	(B.F/F)
Ground -initiated comms	(U/P)	(B.F/F)	(L/A)

14. CONCLUSION

In this paper, we use an aeronautical access technology that provides some Mbit/sec per radio cell for ATS and AOC traffic and Standard WiMAX can be used to provide connectivity for AAC and APC. we have described the various protocols and its mobility requirements We also enhanced a protocol WINMO and give the details of it and its requirements. This identifies it as the most promising approach among all the studied RO protocols. An advantage of the MR-to-HA approach though is the applicability to the AAC and APC domains where passenger owned devices have to be supported and data is routed over the public Internet. As mobility signalling is only performed between mobile router and home agent, both MNNs and CNs remain unaffected. In fact, the mobility protocol is completely transparent to these end-systems and they do not require any mobility extensions.

REFERENCES

[1] "IEEE Standard for Local and metropolitan area network. Wirless LAN Medium Access Cantrol (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2007, pp. C1–1184, 2007.

[2] D. Le, X. Fu, and D. Hogrefe, "A review of mobility support paradigms for the Internet," IEEE Commun. Surveys and Tutorials, vol. 8, no. 1-4, pp. 38–51, 2006.

[3] E. Perera, V. Sivaraman, and A. Seneviratne, "Survey on network mobility support," SIGMOBILE Mob. Comput. Commun. Rev., vol. 8, no. 2, pp. 7-19, 2004.

[4] ICAO Aeronautical Communications Panel, WG I, "Analysis of Candidate Mobility Solutions," 13th meeting of the working group N-SWGI, Montreal, Canada.

[5] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," RFC 4271, Jan. 2006.

[6] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, Dec. 2005.

[7] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," RFC 4306, Dec. 2005.

[8] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, Jun. 2004.

[9] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," RFC 3963, Jan. 2005.

[10] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775, Jun. 2004

[11] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration, RFC 5061, Sep. 2007.