*International Civil Aviation Organization*

**AUTOMATIC DEPENDENT SURVEILLANCE – BROADCAST SEMINAR AND THIRTEENTH MEETING OF AUTOMATIC DEPENDENT SURVEILLANCE – BROADCAST (ADS-B) STUDY AND IMPLEMENTATION TASK FORCE (ADS-B SITF/13)**

Hong Kong, China, 22-25 April 2014

---

**Agenda Item 7: Any other Business - Security Issues**

# SECURITY ISSUES OF ADS-B OPERATIONS

(Presented by Airports Authority of India)

**SUMMARY**

This paper presents the security aspects of Automatic Dependent Surveillance – Broadcast (ADS-B) protocol. Referring to Aviation Security Manual Doc 8973/8, states have been urged to include provisions for protection of critical information and communication technology systems against cyber-attacks and interference. Further, in the recently issued Air Traffic Management Security Manual Doc 9985 AN/492 First Edition – 2013 emphasis has been laid on protection of Air Traffic Management Systems against cyber-attacks. In this context, attempt has been made through this paper to highlight the importance of security aspects of ADS-B protocol with mitigation policy to be adopted uniformly across the states.

## 1. INTRODUCTION

1.1 Referring to Aviation Security Manual Doc 8973/8, states have been urged to include provisions for protection of critical information and communication technology systems against cyber-attacks and interference. Further, in the recently issued Air Traffic Management Security Manual Doc 9985 AN/492 First Edition – 2013, emphasis has been laid on protection of Air Traffic Management Systems against cyber-attacks.

1.2 One of the goals of ADS-B is to increase safety of air traffic. However, considering the high dependency of data links for transportation of surveillance data, the possibilities of attacks ranging from passive attacks (eavesdropping) to active attacks (message jamming, replaying of injection) need to be deliberated.

## 2. DISCUSSION

2.1 Reference is drawn to various published papers available on the public media, wherein the vulnerabilities of ADS-B have been discussed.

2.2 As there are no cryptographic mechanisms implemented in the ADS-B protocol, messages can be trivially injected, modified or deleted by an attacker who has full control over the wireless channel. Generally, two patterns of attacks may be considered: Passive Attacks and Active Attacks.

2.3 Passive Attacks: Inherent characteristic of wireless networks is the broadcast nature of RF communication. Since ADS-B messages are not encrypted, they can be recorded and misused to obtain unique identifiers of aircraft as well as accurate position trajectories. Besides commercially available ADS-B receivers, there are even services available on the Internet which provide digitized live ADS-B data to the public. For more sophisticated traffic analyses, there is e.g. a Mode S and ADS-B capable open-source GNU Radio module available. Such provisions may be used to eavesdrop and analyze ADS-B traffic and signals.

2.4 This brings important area of vulnerability wherein the movement of VIP aircrafts can be easily tracked by agencies and is highly undesirable from the national security aspect.

2.5 Active Attacks: While passive attacks are mainly affecting privacy and might not result in severe risks for air-traffic safety, active attacks could be matter of concern. Active attacks may result in severe threats to air traffic safety including attacks on air traffic monitors and automated assisting systems like collision avoidance (TCAS) and pilots.

2.6 Active attacks could be based on three basic primitives: message injection, message deletion and message modification. The assumption here is that the attacker has full control over the wireless communication channel and is able to inject, delete and modify any ADS-B message. Ghost Aircraft Injection (ADS-B messages of non-existing (ghost) aircraft could be broadcasted on ADS-B channel) and Ghost Aircraft Flooding (injection of multiple aircraft simultaneously) could be possible threats. These could lead to undesired decisions by controllers or denial of service due to excessive ghost targets on surveillance system.

2.7 The security issues associated with ADS-B have been recognized by ICAO under the ADS-B Implementation and Guidance Document (AIGD). It even refers that nature and complexity of ATC systems as a whole need to be considered while contemplating over the much publicized security issues. Even recommendations have been laid down for the states to handle the ADS-B security issues in coordination with the respective appropriate national organizations and ANSPs.

2.8 In accordance with the recommendations mentioned in the AIGD, it is proposed that working group within the ADS-B Task Force could be formulated to look into specific security measures with respect to identify potential encryption and authentication techniques, so that the ADS-B security issues could be addressed uniformly across the states, instead of implementing respective state-wise policies.

2.9 It is further proposed that the meeting upon discussion may recommend formation of a working group to devise mitigation measures to counter various identified vulnerabilities in ADS-B operations. Specific Identification, encryption and authorization of ADS-B equipment could be some of the possible measures.

## 3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) recommend formation of working group to devise mitigation measures to counter ADS-B vulnerabilities; and

c) upon suitable discussion on the topic, consider to formulate mitigation policy on the various ADS-B security issues to be adopted uniformly across the states instead of implementing respective state-wise policies as recommended in the AIGD.

– – – – – – – – – – – – – – –