International Civil Aviation Organization

Fifth Meeting of the Surveillance Implementation Coordination Group (SURICG/5)

Web-conference, 22 – 24 September 2020

Agenda Item 5: Update on surveillance activities and explore potential cooperation opportunities

EXAMPLE OF ADS-B POSITION VERIFICATION PERFORMANCE

(Presented by Japan/Electronic Navigation Research Institute)

SUMMARY

ADS-B has a security concern of spoofing, which is transmissions of signals containing false aircraft information by an attacker. An effective countermeasure against spoofing is a position verification method using Time Difference of Arrival. Japan has conducted a performance evaluation of the position verification method in a spoofing experiment. This paper provides an example of performance evaluated in the spoofing experiment as information to contribute the SURICG activity.

1. INTRODUCTION

1.1 Automatic dependent surveillance–broadcast (ADS-B) is a new style aeronautical surveillance means for air traffic control (ATC) where aircraft periodically report their positions. Compared with conventional means of aeronautical surveillance such as secondary surveillance radar (SSR), ADS-B can provide a better positional accuracy and update rate; this is essential to support advanced operations in ATC to increase safety and capacity.

1.2 On the other hand, ADS-B has a security concern of spoofing, which is transmissions of signals containing false aircraft information by an attacker. An effective countermeasure against spoofing is a position verification method using Time Difference of Arrival (TDOA). This method determines whether the position contained in the ADS-B signal is valid or anomalous (spoofing).

1.3 Electronic Navigation Research Institute (ENRI) has been evaluating performance of the TDOA position verification method in a spoofing experiment. As a result of the experiment, a good probability of detection was observed. Also, the probability of a false alarm was consistent with the threshold design.

1.4 This paper provides an example of performance evaluated in the spoofing experiment using a prototype WAM/ADS-B system as information to contribute the SURICG activity. This information is useful for ADS-B Implementation and Operations Guidance Document (AIGD), as a guidance material for Security Issues Associated with ADS-B.

2. DISCUSSION

Attachment 1 presents the example of performance of the TDOA position verification method evaluated in the spoofing experiment conducted in Japan.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper; and

b) discuss to include this information into AIGD as a guidance material.

SURICG/5 – **WP/07**
Agenda Item 5
22-24/09/20

Example of ADS-B Position Verification Performance

Junichi Naganawa and Hiromi Miyazaki
Electronic Navigation Research Institute,
National Institute of Maritime, Port and Aviation Technology
Tokyo, Japan

1. Introduction

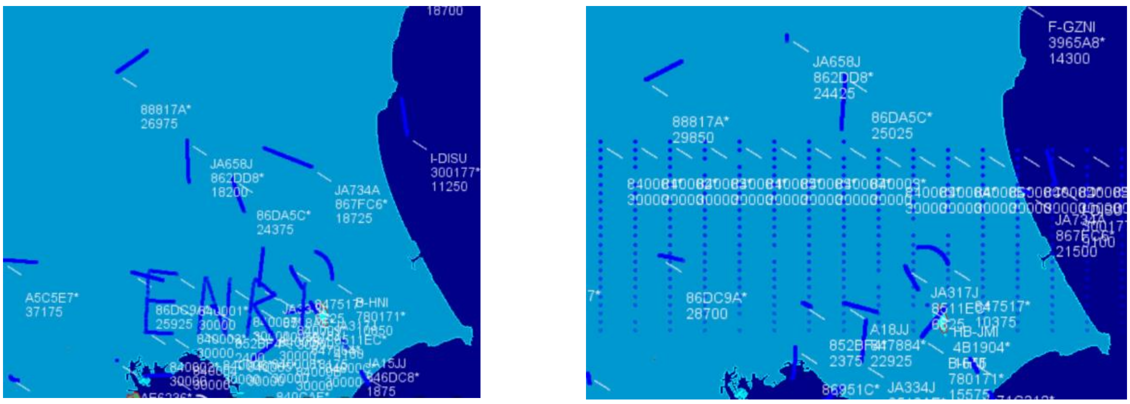
1.1 ADS-B has a security concern of spoofing, which is transmissions of signals containing false aircraft information by an attacker. An effective countermeasure against spoofing is a position verification method using Time Difference of Arrival (TDOA). The method determines whether the position contained in the ADS-B signal is valid or anomalous (spoofing).

1.2 Electronic Navigation Research Institute (ENRI) has been evaluating performance of the method.

1.3 This paper provides an example of performance evaluated in a spoofing experiment using a prototype WAM/ADS-B system as information to contribute the SURICG activity.

2. Enhancing ADS-B Security by a TDOA-based Position Verification Method

2.1 Spoofing is transmissions of signals containing false aircraft information by an attacker. As a result of spoofing, false targets may appear on the controller's display. To illustrate a threat of spoofing, Figure 1(a) and (b) show examples of false targets; these are results of an experiment conducted by ENRI.



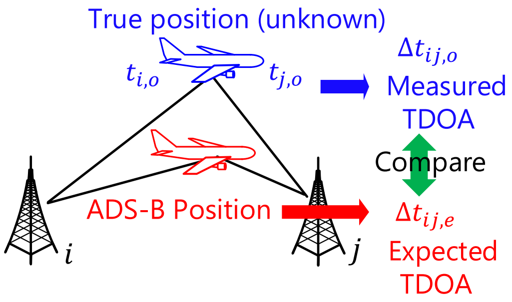
(a) (b)

Figure 1. False targets generated by spoofing experiment by ENRI: (a) a prank case and (b) a denial of service attack with flooding targets.

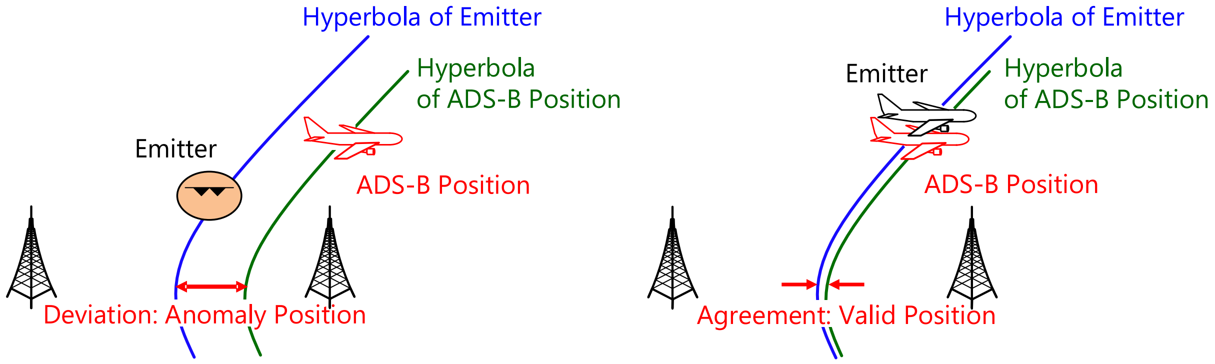
2.2 An effective countermeasure against spoofing is position verification. In a case of spoofing, the position of the emitter (attacker) is likely to differ from the position contained in the ADS-B signal. Such positional difference can be detected by means of TDOA.

2.3 Figure 2(a) explains the method. When an emitter (aircraft or spoofing emitter) transmits an ADS-B signal, (at least) two receivers detect the signal and measure the time of arrival (TOA). The difference of the TOAs between the two receivers is a TDOA. Next, decoding the ADS-B signal obtains the position contained in the signal. A calculation using the ADS-B position and the known receiver positions obtains the expected TDOA.

2.4 The measured and expected TDOAs are compared. The TDOA difference is large in a case of spoofing and small in a case of a legitimate aircraft, as illustrated in Figure 2(b) and (c), respectively. Therefore, a threshold can be used to make a decision; if the TDOA difference is smaller than the threshold, the position is determined as valid. If the TDOA difference is larger than the threshold, the position is determined as anomalous (spoofing).



(a)



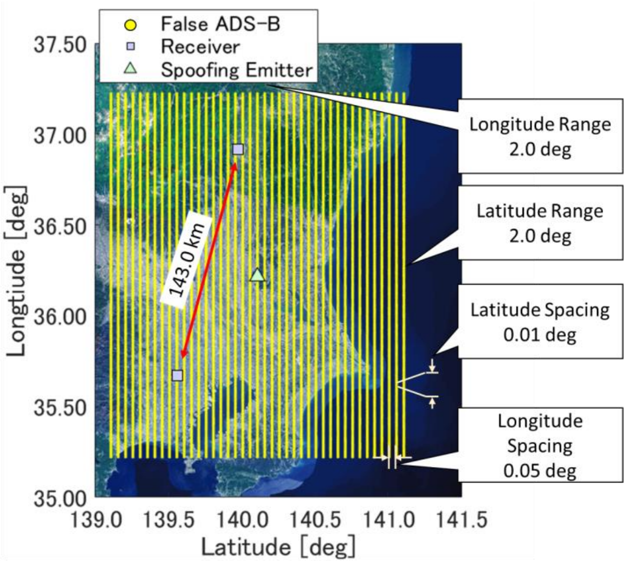
(b) (c)

Figure 2. Illustration of the TDOA method: (a) the procedure, (b) a case of spoofing, and (c) a case of a legitimate aircraft.

3. **Experiment**

3.1 Assumed Scenario

3.1.1 Figure 3 shows the scenario assumed in the experiment. The scenario had a spoofing emitter, targets of opportunity (all considered legitimate), and two receivers. En-route surveillance was assumed, and the two receivers are separated by 143 km. The positions generated by spoofing were uniform over a grid for the latitude and longitude at a fixed altitude. The position of the spoofing emitter was assumed to be on the top of a mountain. It should be noted that the spoofing emitter was not real; we did not actually transmit signal over the air.



Map data by Geospatial Information Authority of Japan was used. The data sources: Landsat 8 images (GSI,TSIC,GEO Grid/AIST), Landsat 8 images (courtesy of the U.S. Geological Survey), and bathymetric data (GEBCO). http://maps.gsi.go.jp/development/ichiran.html.

Figure 3. The scenario assumed in the spoofing experiment.

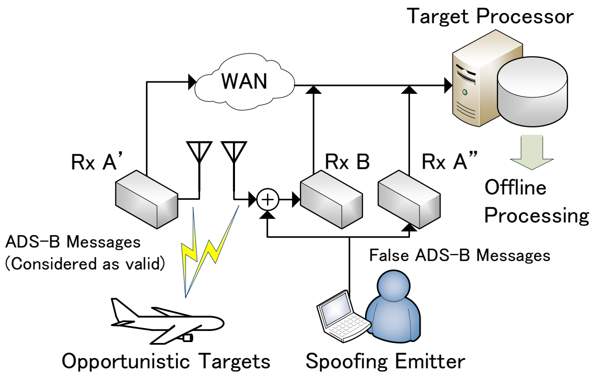


Figure 4. Schematic of the experiment.

3.2 Experiment Setup

3.2.1 A prototype WAM/ADS-B system developed by ENRI was used in the experiment. Figure 4 shows a schematic of the experiment. The experiment scenario was simulated by using two receivers at a local site (Rx B and Rx A"), a receiver at a remote site (Rx A'), and a signal generator as the spoofing emitter. The received messages were sent to a target processor and stored, and the stored messages were processed offline for evaluation.

3.2.2 Figure 5 shows the picture of the experiment system.

Figure 5. Photos of the experiment system.

3.2.3 The duration of the experiment is as follows: four hours from Oct 10, 2019 12:21:37 Japan Standard Time (JST) and 24 hours from Oct 10, 2019 18:13:44.

3.3 <u>Result</u>

3.3.1 Figure 6 shows the positions after applying the method. The left plot shows the positions determined as anomalous (spoofing), where most of the false positions (distributed as a grid) were successfully categorized here. The right plot shows the positions determined as valid, where most of the opportunistic signals were successfully categorized here.

3.3.2 The probability of detection was evaluated. 624889 signals were successfully detected as anomalous among 626053 false signals generated, which resulted in 99.81% of the probability of detection. This result demonstrated a good performance of the method.

3.3.3 The probability of a false alarm was evaluated. 27189 signals were wrongly detected as anomalous among 570152 opportunistic signals, which resulted in 4.8% of the probability of a false alarm. This value is consistent with our design of the experimental setup.

3.3.4 The detection threshold of 1019.4 nsec was used in this experiment. Actually, this value was empirically determined before this experiment as the value corresponding to the probability of a false alarm of 5%.

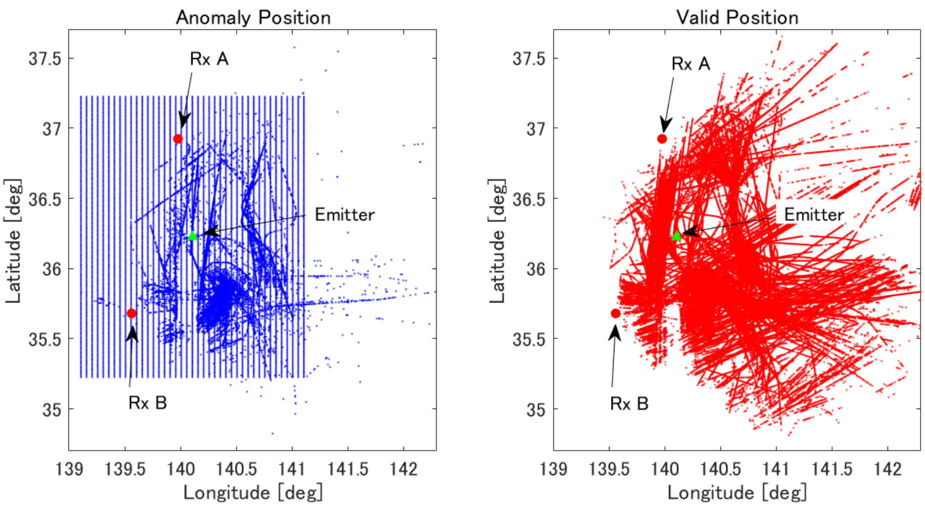


Figure 6. Result of the spoofing experiment: (left) the positions determined as anomalous and (right) the positions determined as valid.

4. Conclusion

4.1 Performance of an ADS-B position verification method using TDOA was evaluated by a spoofing experiment.

4.2 A good probability of detection was observed, and the probability of a false alarm was consistent with the threshold design.

4.3 ENRI continues evaluation of the position verification method.

5. Reference

5.1 J. Naganawa and H. Miyazaki, “Experimental Evaluation on TDOA-based Aircraft Position Verification,” 2020 14th European Conference on Antennas and Propagation (EuCAP), Copenhagen, Denmark, 2020.

5.2 M. Strohmeier, V. Lenders and I. Martinovic, “On the Security of the Automatic Dependent Surveillance-Broadcast Protocol,” in IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1066-1087, Secondquarter 2015.

5.3 G. Graziano, P. De Marco, F. Perilli, and L. Mene, “TDOA based ADS-B Validation,” 2013 International Symposium on Enhanced Solutions for Aircraft and Vehicle Surveillance Applications, Berlin, Germany, Mar. 2013.

5.4 SESAR Joint Undertaking, Final Project Report Surveillance Ground System Enhancements for ADS-B (Prototype Development), 15.04.05 b, D01, May 2015.

5.5 H. Neufeldt, “ADS-B Security,” 2016 International Symposium on Enhanced Solutions for Aircraft and Vehicle Surveillance Applications, Berlin, Germany, April 2016.