ELEKTROTEHNIŠKI VESTNIK 82(5): 297-301, 2015
REVIEW SCIENTIFIC PAPER

Security of the ADS-B system in heavy multipath propagation environments

Uroš Šolar

Faculty of Electrical Engineering, University of Ljubljana, Tržaška 25, 1000 Ljubljana, Slovenia
E-mail: solar.uros@gmail.com

Implementation of the ADS-B system for identification and localization of airplanes has presented a number of technological and regulatory challenges. The system is based on an automatic and continuous broadcasting mechanism of the location, speed and identification of the airplane and together with the traditional radar systems brings better capabilities to air traffic management. Unfortunately, the system also has its flaws in the form of security vulnerabilities. The paper focuses on presenting these vulnerabilities which stem from the system's lack of cryptographic and authentication procedures. Moreover, the existing mitigating techniques are presented and analyzed in new operating environments with strong multipath signal propagation. The current mitigation techniques might not be sufficiently effective in these non-line-of-sight; urban or mountainous low-altitude environments which present a serious security issue. The disparity of the line-of-sight and non-line-of-sight channels is presented for being the main factor when differentiating between the two operational environments. The system is already used with helicopters which operate in such non-line-of-sight environments and, in future, it may be even used with unmanned aircraft. For this purpose, the potential vulnerabilities of the current ADS-B implementation are presented and solutions are proposed based on signal propagation modeling and good ground-station infrastructure.

Keywords: Multipath propagation, ADS-B security, ADS-B vulnerabilities, ADS-B spoofing, ADS-B injection

Varnost sistema ADS-B v okolju z močnim večpotnim razširjanjem signalov

Implementacija sistema ADS-B za identifikacijo in lokalizacijo potniških letal je predstavila kopico tehnoloških in regulacijskih izzivov. Sistem ADS-B se trenutno že uporablja in temelji na avtomatičnem in kontinuiranem oddajanju lokacije, hitrosti in imena letal ter skupaj s tradicionalnimi radarskimi sistemi prinaša boljše sposobnosti obvladovanja zračnega prometa. Skupaj s prednostmi pa se pojavljajo tudi slabosti. Članek usmeri pozornost k varnostnim problemom sistema ADS-B, ki izhajajo iz neuporabe šifrirnega in avtentikacijskega postopka. Predstavijo se ranljivosti sistema in tehnike, ki lajšajo nevarnost v trenutnem načinu uporabe. Tehnike, ki pa morda niso enako učinkovite v okoljih z močnim večpotnim razširjanjem valov. Tu govorimo o mestnih ali pa gorskih okoljih predvsem pri nizkih višinah letenja. Predstavijo se razlike komunikacijskih kanalov za neposredno-vidna in posredno-vidna področja delovanja, saj v največji meri pripomorejo k razlikovanju med omenjenimi okolji. V takih okoljih se trenutno že uporabljajo helikopterji, potencialno pa bi se lahko pojavila tudi brezpilotna letala. Prav zato članek opiše varnostne luknje trenutne implementacije sistema ADS-B in predstavi mogoče rešitve, ki pa temeljijo na sestavljanju propagacijskih modelov in močni infrastrukturi zemeljskih postaj.

1 INTRODUCTION

Traditionally, any aerial vehicle localization relies on radar systems originally developed for military applications (IFF). These systems can be classified as primary (PSR) and secondary (SSR) surveillance radars. PSRs transmit high frequency signals which are reflected by targets. Reflections are received and evaluated to determine the direction, velocity, shape and size. In contrast, SSRs require cooperation from aerial vehicles as these systems are dependent on on-board identification transponders. By responding to interrogation enquiries from ground stations all the relevant information is transmitted to air traffic controllers [1].

The increasing density of air traffic and relatively low precision and detection accuracy of the current localization systems [2] have sparked the development of a new technology for traffic monitoring called Automatic Dependent Surveillance-Broadcast (ADS-B). It combines satellite positioning information with the ground-based reference stations and inertial sensors (US: WAAS or EU: EGNOS) to repeatedly and automatically transmit location updates to airplanes and ground stations in proximity [3]. The model is presented in Figure 1. On the other hand, the older system (Mode S) which is still in use today, only responds to interrogation enquiries.

Received 10 November 2015
Accepted 25 November 2015

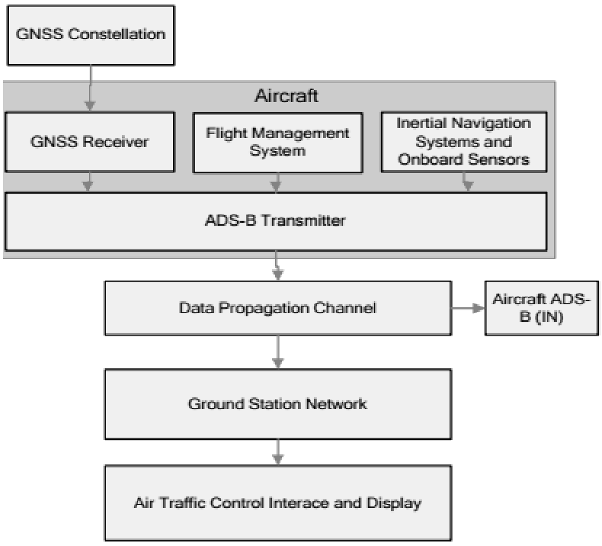

Figure 1: ADS-B system structure [15].

ADS-B is already standardized with aviation authorities in Europe (EUROCONTROL) and the USA (FAA). Both organizations have mandated its deployment; the USA for 2020 and Europe for 2017. Airliners have already begun equipping airplanes with ADS-B in preparation for these mandates. ADS-B messages are unencrypted for the purpose of being available to anyone in the airspace but because of it, the messages can be actively collected from all over the world. This data is decoded, visualized and offered as a real-time online aircraft tracking service. One such example is flightradar24.

Although ADS-B presents a lot of desirable new features such as; better ATC traffic flow management, merging and spacing, enhanced operations in lower visibility, etc., it also poses some security concerns directly attributed to the protocol's lack of message authentication and encryption. It allows a potential attacker to change the integrity and origin of data without much effort [4]. All attack venues will be described in further chapters.

Mitigation techniques exist when ADS-B is used in the line-of-sight (LOS) environments where conventional airline aircraft are used [5, 6]. These techniques use machine learning procedures on the obtained messages. Patterns of real and injected air-traffic signal data are analyzed to determine potential attacks. Methods based on the received signal strength (RSS) are not sufficiently effective in non-line-of-sight (NLOS) urban environments where signals don't propagate predictably and multipath signal propagation becomes a factor.

A potentially wide-spread use in crowded environments presents a problem in the field of Air Traffic Management and Control. Resulting from a continuous transmission of data packets at all times during the aircraft operation, thus causing congestion of the radio channel. The conventional air-traffic control has already experienced an astounding growth with no signs of stopping. The largest airports in Europe can get more than 1,500 daily takeoffs and landings [1].

Introducing the system in low-altitude and NLOS environments where heavy multipath propagation becomes a factor and where helicopters and potentially UAVs [7, 8] might operate only amplifies the problem of congestion and mitigation of vulnerabilities.

2 ADS-B SYSTEM OVERVIEW

The ADS-B system consists of three main components, the first is the ADS-B Out which periodically and automatically broadcasts the position, velocity, route and identity of the equipped aircraft. The second is the transport protocol, both of which are listed in the next paragraph. The third is the receiving subsystem, i.e. ADS-B In system which includes message reception and assembly at the receiving destination. [8].

There are two competing ADS-B data link standards: Universal Access Transceiver (UAT) and 1090 MHz Extended Squitter (1090ES) [12]. The difference between the two standards is in the used frequency of 1090 MHz for 1090ES and of 987 MHz for UAT. 1090ES uses the existing radio channel for the Mode-S data which is based on interrogation techniques for message broadcasting. It includes the ADS-B data as an addition to the existing Mode-S messages, hence the ‘extended squitter (ES)’. Between both, it is also the only one allowed in the Class A airspace and is therefore used as the International Civil Aviation Organization’s (ICAO) standard for airliners and other large aircraft [10]. A major problem with using 1090ES is congestion of the 1090 MHz radio channel. The message specification is presented in Figure 2.

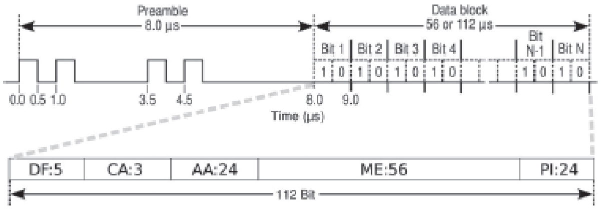

Figure 2: 1090ES data link message format [12].

Mode-S reply protocol messages start with a known, eight-bit long preamble which allows the decoder to synchronize and decode messages correctly. DF indicates the structure of the message (DF17 is used for 1090ES), CA indicates the capabilities of the primary transponder, AA carries the unique 24 bit ICAO address which enables aircraft identification, ME is reserved for the 56-bit arbitrary data (e.g. the position, velocity, urgency code, quality level), lastly, PI field provides a 24-bit CRC to detect and correct up to five-bit errors.

Messages are encoded and transmitted with a pulse position modulation scheme (PPM) with the transmission rates reaching 1 Mbit/s. Unfortunately, PPM is very sensitive to the reflected signals and multipath propagation [9] which is often observed in the NLOS environments. This needs to be acknowledged when contemplating the protocol security concerns.

UAT is a data link standard developed and used in the US to resolve the 1090 MHz channel congestion since it operates on 978 MHz. It is designed to be an alternative to 1090ES, to be used for aircraft other than airliners and to support additional services than just ADS-B i.e. services such as Traffic Information Service – Broadcast (TIS-B) and Flight Information Service – Broadcast (FIS-B). The standard defines two distinct message segments for the ground and ADS-B communication. It uses a continuous phase-frequency shift keying modulation scheme (CPFSK) to transmit at a speed reaching 1 Mbit/s. The message is presented in Figure 3.

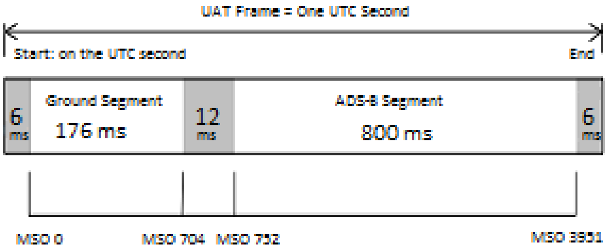

Figure 3: UAT data link message format [10].

As seen in the figure below, each UAT frame is 0.8 s long and spans 3200 message start opportunities (MSOs). Each aircraft makes one UAT ADS-B message transmission per frame from a pseudo-random selection among the 3200 MSOs to start a transmission. This mechanism is used to prevent interference with other UAT messages. Some schemes use this mechanism to determine the range of the UAT equipment transmitting the message [10]. The ADS-B Message format contains a synchronization preamble, payload and forward error correction (FEC) parity.

ADS-B increases safety of the air-traffic management control by improving the aircraft situational awareness. Enhanced conflict detection and resolution allows each individual plane to know their position regardless of infrastructure, and to optimize the use of the airspace by minimizing the load on air-traffic control centers since vehicles can broadcast their positions and velocities directly to each other.

Despite of all these positive sides, there are known major security vulnerabilities which make attacks on the system possible. These attacks are listed and described in the next chapters with regard to the use in a heavy multipath propagation environment.

3 ADS-B SECURITY VULNERABILITIES

Assessing security of the communication protocols typically consists of analyzing the ability of a system to maintain the integrity, availability and confidentiality. These three principles are at the heart of information security and in case of ADS-B highly neglected.

Openly broadcasting unencrypted messages neglects confidentiality. The lack of message authentication mechanisms impacts the data integrity and the possibility of jamming the ADS-B signals affects the protocol's availability. The consequences of not properly adhering to these principles can be exploited by malicious users to perform the attacks listed in Table 1.

Table 1: Potential attacks on the ADS-B protocol [12].

Attacks	Method
Aircraft Disappearance	Message Deletion
Aircraft Flood Denial	Signal Jamming
Aircraft Reconnaissance	Eavesdropping
Aircraft Spoofing	Message Modification
Aircraft Ghost Injection	Message Injection
Ground Station Ghost Injection	Message Injection
Ground Station Flood Denial	Signal Jamming
Virtual Aircraft Hijacking	Message Modification
Virtual Trajectory Modification	Message Modification

The attacks can be categorized into broader groups based on their method of operation [12].

1. **Eavesdropping**: Anyone can decode the ADS-B messages with cheap SDRs due to being openly broadcasted and unencrypted.
2. **Message Deletion**: Transmission of the protocol messages can be interfered on the physical-wireless medium by broadcasting legitimate but inverse signals. Superposition of these waves results in a destructive interference which highly attenuates legitimate messages.
3. **Message Injection**: Correctly modulated and constructed ADS-B messages can be transmitted on the network without a proper authorization procedure. These messages can mimic any real aerial vehicle with the desired position and velocity parameters.
4. **Message Modification**: Messages can be modified without any participants' knowledge by sending a strong signal to override a part or the whole message (overshadowing). Data can also be modified by superimposing a signal with the intent to convert any number of bits from 0 to 1 or vice versa (bit-flipping). These attacks can be especially sinister since a legitimate message is manipulated.

5. **Signal Jamming**: Signals can be transmitted at the frequencies used by ADS-B to make legitimate protocol messages imperceptible. Such jamming techniques can be directed at the aircraft or ground stations.

These techniques apply to both the LOS and NLOS environments. The system's easily exploitable security vulnerabilities with cheap and available software-defined radios (SDR) urge the need to address such issues before ADS-B is more widely used in vulnerable environments.

Current techniques for resolving these issues are primarily designed for the manned passenger flights in the LOS environments. Besides using the PSR solutions, these methods primarily involve the use of multilateration or ADS-B message RSS analysis [12] both of which are vulnerable to multipath propagation in the NLOS urban environments.

3.1 LOS and NLOS channel differences

The discussed difference between the operational environments needs to be addressed directly. This is done by comparing both, the NLOS (Figure 4) and the LOS (Figure 5) channel characteristics [14, 15]. This difference needs to be defined to understand the importance it has in applying mitigation techniques for the presented vulnerabilities of the ADS-B protocol system.

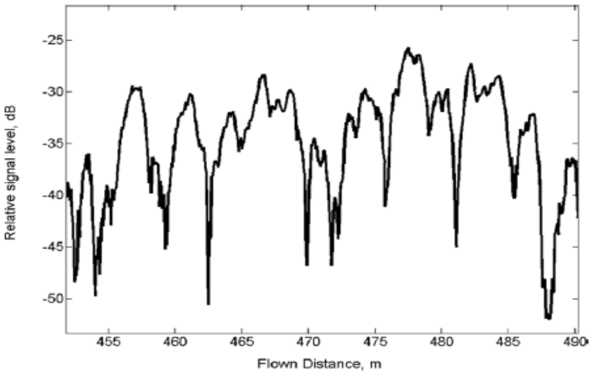

Figure 4: Channel characteristics at 2 GHz in an NLOS environment [14].

Figure 4 was obtained by measuring the received power of a flying UAV in an urban environment. It shows the result of a multipath effect (i.e. fading) a signal experienced by reflecting and diffracting in a NLOS environment.

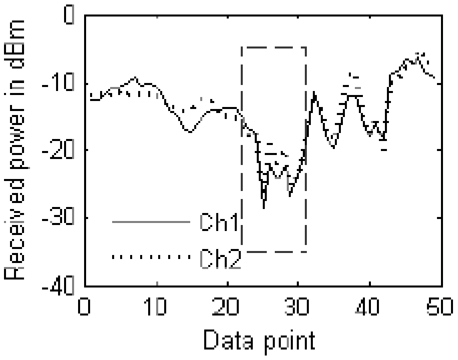

Figure 5: Channel characteristic at 5 GHz in an LOS environment [15].

Contrary, the Figure 5 shows that the LOS signal propagation experienced less severe fluctuations even at a much higher frequency with the exception of the shadowing effect (highlighted in the dotted rectangle) since the aircraft flew relatively close to the ground station and the signal transmitted did not additionally refract around the shadowing profile [15].

These differences affect the way the mitigating techniques can be applied in both scenarios since multilateration and RSS analysis works best in a predictable environment. In case of NLOS, additional procedures [16, 17] must be implemented to ensure signal propagation predictability.

3.2 Mitigation techniques

Mitigating techniques are already in use for the commercial airline flight operation. They target different layers and various vulnerabilities but there isn't a single method that would address all security concerns at the same time [12]. Problems arise when the existing techniques are applied to a low-altitude and NLOS environment since ADS-B messages are subjected to heavy multipath propagation.

All the techniques assume a good ground-station infrastructure, as in the case of commercial flights. The effects described in the previous chapter emphasize this importance. These are the techniques that don't completely change the way the ADS-B system functions and they are:

1. **Multilateration:** By knowing the precise distance between four or more ground stations we can identify the unknown location. All stations receive the same signal with different times of arrival (TDOA) which allows us to construct hyperboloids that determine the aircraft's location. It is very vulnerable to multipath propagation in its basic form but some success has been achieved by applying additional procedures [17].

2. **Group Verification:** This technique is used in conjunction with the ADS-B In system. Additional airborne and trusted airplanes are used together to employ the same multilateration techniques as the ground stations. Its negative consequence is its need of an established trust and verification process.
3. **Traffic Modeling / RSS Analysis:** It is a collection of the methods used to detect abnormal variations in the received signal power. A heat-map model can be built from the previously obtained aircraft data and machine learning methods. It provides a basis upon which the ADS-B location claims can be verified. Such a model is created for all ground stations in an environment and is used to cross-correlate the location claims.

The ADS-B system in its current form presents a considerably big attack surface that the listed techniques cannot prevent attacks easily. These techniques have only been tested in high-altitude LOS environments where the signal propagation is easily predictable and multipath effects are small. There is some evidence that the 1090ES and UAT signals are vulnerable to these effects [15].

PSRs provide support to the ADS-B system since it isn't designed to operate alone. Not much can be done without changing the whole ADS-B system. Also, the methods listed above only focus on the mitigation of spoofing attacks (message injection, message modification).

Conclusion

The ADS-B system's most desirable feature is its openness which is also its greatest security vulnerability. By not adhering to the security principles it makes itself vulnerable to attacks. To prevent these vulnerabilities and detect if a malicious attack is being performed on the network, a good ground-station infrastructure is needed. The mitigation techniques are currently only used in the LOS conditions since it is the system's only operational environment. Optimally, the whole message broadcasting procedure should be changed drastically to ensure confidentiality, integrity and to some extent availability.

Currently, the ADS-B Out system is only mandated in flight operations at higher altitudes where LOS conditions exist and mitigation techniques work but changes need to be implemented to have the ADS-B system used in the low-altitude NLOS environments as well. The use of PSRs in the urban and mountainous environments is not ideal. An SSR system such as the ADS-B system would be the second best choice but the system itself needs to be secure and trusted to be used in such an environment.

In conclusion, the paper presents the inherent differences between the aircraft operational environments and their effects on the ADS-B system's security. It defines the problems of applying the same mitigation techniques to both the LOS and NLOS environments. Identification of these differences serves as a reference point for further research into these specific ADS-B security issues.

References

[1] M. Strohmeier, M. Schafer, V. Lenders and I. Martinovic, 'Realities and challenges of nextgen air traffic management: the case of ADS-B', *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 111-118, 2014.

[2] RTCA Inc., 'Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B),' DO-242A (including Change 1), Dec. 2006.

[3] EUROCONTROL, 'Policy on GNSS for Navigation Applications in the Civil Aviation Domain', EUROCONTROL Headquarters, Haren, 2008.

[4] A. Costin, A. Francillon, 'Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices', *Black Hat USA*, 2012.

[5] M. Strohmeier, I. Martinovic, 'Detecting False-Data Injection Attacks on Air Traffic Control Protocols', *Proc. of the 7th ACM Conf. on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2014.

[6] M. Strohmeier, V. Lenders and I. Martinovic, 'On the Security of the Automatic Dependent Surveillance-Broadcast Protocol', *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1066-1087, 2015.

[7] B. Stark, B. Stevenson and Y. Chen, 'ADS-B for small Unmanned Aerial Systems: Case study and regulatory practices', *2013 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2013.

[8] S. Trimble, 'Google targets low-cost ADS-B Out avionics market', *Flightglobal.com*, 2015. Available: https://www.flightglobal.com/news/articles/google-targets-low-cost-ads-b-out-avionics-market-410473/.

[9] M. Simunek, F. Fontan and P. Pechac, 'The UAV Low Elevation Propagation Channel in Urban Areas: Statistical Analysis and Time-Series Generator', *IEEE Trans. Antennas Propagat.*, vol. 61, no. 7, pp. 3850-3858, 2013.

[10] ICAO, 'Manual for the Universal Access Transceiver (UAT)', 2003

[11] Y. Meng and Y. Lee, 'Study of shadowing effect by aircraft maneuvering for air-to-ground communication', *AEU - International Journal of Electronics and Communications*, vol. 66, no. 1, pp. 7-11, 2012.

[12] Y. Wang, L. Cheng, G. Han, H. Wu and B. Jiang, 'RSS Localization Algorithm Based on Nonline of Sight Identification for Wireless Sensor Network', *International Journal of Distributed Sensor Networks*, vol. 2014, pp. 1-8, 2014.

[13] S. Nawaz and N. Trigoni, Robust Localization in Cluttered Environments with NLOS Propagation, *IEEE 7th International Conference on Mobile Adhoc & Sensor Systems (MASS)*, pp. 166-175, 2010

[14] C. Yu Hasan, L. Sherman, E. Per and J. Shau Shiun, 'Evaluation & comparison of ranging using Universal Access Transceiver (UAT) and 1090 MHz Mode S Extended Squitter (Mode S ES)', *IEEE Position, Location & Navigation Symposium – PLANS 2014*, pp. 915-925, 2014.

[15] L. Purton, et al. 'Identification of ADS-B System Vulnerabilities and Threats', *Australasaian Transport Research Forum proceedings*, 2010