Effective Security Techniques for Automatic Dependent Surveillance-Broadcast (ADS-B)

Fatimah Alghamdi
Faculty of Computing and Information Technology, King Abdul-Aziz University
B.P. 42808 Zip Code 21551 Girl Section, Jeddah, KSA

Amal Alshhrani
Faculty of Computing and Information Technology, King Abdul-Aziz University
B.P. 42808 Zip Code 21551 Girl Section, Jeddah, KSA

Nermin Hamza
Faculty of Computing and Information Technology, King Abdul-Aziz University,
B.P. 42808 Zip Code 21551 Girl Section, Jeddah, KSA
* Institute of Statistical Studies and Research, Cairo University Cairo, Egypt

ABSTRACT
Although air traffic is continuously increasing on a global scale, the next generation of management in this field is successfully handling this expansion and improving the safety of billions of future passengers. In this paper, Automatic Dependent Surveillance-Broadcast (ADS-B) was examined, which is a primary system, unlike traditional radar. This technology allows aircraft to automatically broadcast their intentions and location; however, it faces certain threats from which it requires some manner of protection. This paper discussed some techniques to encrypt and protect ADS-B messages. Staged Identity-Based Encryption (SIBE) was the most suitable means of solving the issues, providing, as it does, a sufficient level of security for ADS-B messages. In addition, the technique has attractive characteristics, such as confidentiality, efficiency, and a high enough degree of flexibility for effective key management and frequent encryption. This last attribute distinguishes the approach and renders it more popular than its peers.

Keywords
ADS-B, identity-based encryption, Staged Identity-Based Encryption(SIBE). encryption technique

1. INTRODUCTION
Globally, air traffic has moved from the traditional independent stage (primary surveillance radar) to an advanced dependent stage (secondary surveillance radar). This shift has reduced the cost of deployment and improved the detection precision of aircraft.

PSR (primary surveillance radar) is used to survey the routes, and detect the positions, of aircraft. It works by sending out a beam of energy that, when it hits the aircraft, reflects a time to the radar in the form of an echo. By measuring the time, it takes the beam to do this, the PSR can detect the position of the aircraft, which is then sent to the control center where it is displayed as a radar blip. This surveillance is independent, meaning that no aircraft can remain invisible to the air traffic controller **[1].**

SSR (secondary surveillance radar) is used for the same purposes as its primary counterpart, while also gathering information about altitude and identity. SSR requires aircraft to be fixed with an onboard transponder that continually takes the antenna into consideration. The SSR sends beam of energy that hits the aircraft; a coded replay is then sent at a later time to the radar. This replay contains the altitude and aircraft identification. The SSR does not depend on the responder for the position of aircraft; it determines the position itself by measuring the time taken to receive the replay. Thereafter, all of this information is transmitted to the aircraft control center, where it is displayed as an air traffic label. Additionally, the secondary radar installed in aircraft is used to transmit the pulses on 1030 MHZ and responses on 1090 MHZ [1]

The Automatic Dependent Surveillance-Broadcast (ADS-B) system is one of the most widely used secondary surveillance radar systems. ADS-B has become a primary component of next-generation air traffic. This surveillance and security technology will be widespread globally by 2020 as every aircraft will be equipped with an ADS-B device. This system broadcasts plain-text messages to other aircraft and ground station controllers one or two per second. However, a loss of security in ADS-B systems could result from different attacks which require responses using various security techniques. [2]

This paper compared the different encryption techniques available in order to identify the optimum method of protecting ADS-B messages from such threats.

As will be discussed further in the next Sections, Staged Identity-Based Encryption was concluded, that is the most suitable technique for this purpose.

This paper is organized as follows: Section 2 is overview about ADS-B system, Section 3 summarizes the related research that has discussed the most popular techniques used in aircraft security; Section 4 describes the contribution of this work; last Section offers conclusions and suggestions for future research.

2. OVERVIEW
As mentioned before, The Automatic Dependent Surveillance-Broadcast (ADS-B) system is one of the most widely used secondary surveillance radar systems. ADS-B has become a primary component of next-generation air traffic.

.

ADS-B can be used for control and surveillance of aircraft, whether it is on the ground or airborne. The reports transmitted for each position have integrity of data. Users can determine and select which applications support the data's immunity to multiple paths. [1,2]

2.1 (ADS-B) architecture

Primary surveillance radar is very simple but is also very costly and difficult to maintain and operation. Secondary surveillance radar systems, such as ADS-B, can be used by airlines and air traffic managers, and their improved accuracy increases security and reduces the odds of accidents. However, sometimes these systems can be exposed to attacks which result in serious damage to the security of individuals and information [3].

The two modes of operation offered by ADS-B are ADSB OUT and ADSB IN. see Figure 1 illustrate the two-operation mode.

The former directs a communication mode whereby ADS-B messages are sent to the ground controllers and sometimes to other aircraft, with the help of ABS-B transponders installed in said vehicles. Meanwhile, the latter directs a communication mode whereby ADS-B messages are received by the aircraft from ground controllers and sometimes from other aircraft [4].

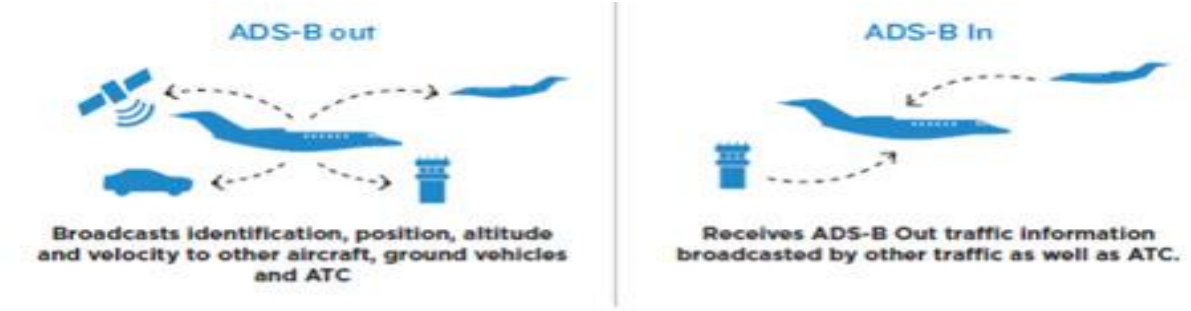

Fig 1: Operation mode of ADS-B [5]

For ADS-B OUT to work, it requires ATC (air traffic control) transponders, at the very minimum, to get the aircraft off the ground and through controlled airspace. In addition, advisory services to the aircraft can be provided in non-controlled airspace.

The other mode, ADS-B IN works with a TCAS (Traffic Collision Avoidance System), which is used to reduce the frequency of mid-air collisions between aircraft. Additional wiring and traffic selectors are needed in cockpit for ADS-B IN to work. A capable EIS2 and OANC (on board navigation computer) are also required.

Despite the fact that ADS-B messages can contain certain sensitive information, especially when communication takes place between mission-critical civil airplanes, use of the mode can raise security alarms as channels between ground controllers and aircraft for ADS-B communication are not secured. This means that any random individual who has an ADSB receiver can capture these messages. It is therefore necessary to protect the interactions from unwanted eavesdropping [4].

2.2 ADS-B Messages

The messages of ADS-B contain 112 bits that move through 1090 MHz data links and are distributed as follows. The first 5 bits are in message type (format). The second 3 bits contain Mode S transponder information. The third 24 bits contain the aircrafts unique address. The next 56 bits consist of ADS-B field data, which include information about the aircrafts identity, position, and velocity, altitude, latitude, and longitude of the aircraft. The last 24 bits include a parity check that detects and corrects transmission errors in the messages, so ADS-B messages are unencrypted [6]. In the modern era, ADS-B messages are constantly being broadcast by a great variety of aircraft. The abovementioned interlopers use a range of programs, such as Modes Beast, Radar Space, and so on, to setup their own receiver and antenna to start tapping into these signals.

2.3 Threats to ADS-B

ADS-B signals are public and use known frequencies. As a result, the signals are becoming vulnerable to jamming and spoofing [7].

Some papers have discussed the ADS-B vulnerabilities caused by the nature of RF communication if used without sufficient security measures. Wired networks have less vulnerability to access attacks, while wireless networks pose numerous access, monitoring, and security issues.

ADS-B threats can be summarized as consisting of either entity message authentication, authorization, such as medium range access with temporary privacy or identifiers, and encrypted messages Table 1 summarizes the most well-known vulnerabilities that threaten system security

The security problems that face ADS-B are on channels between ground controllers and aircraft. if this channel is not secure, ADS-B messages could be captured by third parties whom may be authorized or unauthorized person. it is very problem when ADS-B messages interruption or eavesdropping specially when include sensitive information for mission-critical civil airplanes. so, the ADS-B message need protection.

3. LITERATURE REVIEW

Cook [8] presents a scheme for authentication message using PKI and asymmetric and symmetric encryption. First, public key infrastructure (PKI) ensures that all ADS-B signals are registered with aircraft monitors. After this verification, asymmetric encryption with distributed symmetric session keys is used to prove the authenticity and integrity of exchanged information. It is intended to ensure the security, feasibility, and scalability of ADS-B and to limit use of digital signatures to reduce overhead.

Amin et al. [9] designed a secure framework that can prevent the ADS-B signal from being jammed or spoofed. He used different techniques to detect and avoid spoofing attacks on ADS-B messages during transmission, then compared between them in order to select best one. The first technique used was adding a hashing algorithm to the end of messages to distinguish the source of the message. The researchers also used symmetric and asymmetric encryption to guarantee message confidentiality, non-repudiation, authentication, and integrity. Asymmetric encryption used only public keys, while asymmetric encryption used both public and private keys. The researchers found that the best technique to avoiding spoofing attacks is symmetric encryption [9]. The ADS-B protocol was discussed by Strohmeier et al. [7] in the context of identifying important related issues using a sensor network (Open Sky).

Table 1 summarize of ADS-B threats [12]

Attacks	Layer	Method	Security	Complexity
Aircraft Reconnaissance	PHY+APP	Eavesdropping	Low	Lowest
Ground Station Flood Denial	PHY	Signal Jamming	Medium	Lower
Aircraft Flood Denial	PHY	Signal Jamming	Medium	Low-Medium
Ground Station Trager Ghost Injection/ Flooding	App	Message Injection	High	Low
Aircraft Station Trager Ghost Injection/ Flooding	App	Message Injection	Medium	Low-Medium
Visual Aircraft Hijacking	PHY+APP	Message Modification	High	Medium
Virtual Trajectory Modification	PHY+APP	Message Modification	High	Medium
Aircraft Disappearance	PHY	Message Deletion	High	Low
Aircraft Spoofing	PHY+APP	Message Modification	High	Low

Hableel et al. [6] proposed the SIBE scheme that defines identifiers for ground controllers and generates private keys for them. When the aircraft reaches the corresponding airspace, the aircraft encrypts the symmetric keys defined by the ground controller and then uses symmetric encryption in cyber messages. When a cipher text reaches the ground controller, the system decrypts the message using the private key connected to the identifier and decrypts subsequent cipher texts [6].

Yung et al. [10] proposed a new framework for ADSB which performs authentication based on a three-level hierarchal identity-based signature. ADS-B can be focused on efficiently making signatures while reducing the cost of schemes and verification. The plan for this idea draws from the design of two concrete schemes and supports verification. Three secure

methods hashing, asymmetric, and symmetric encryption are used to create high-level security for ADS-B signals.

The Diffie-Hellmanin assumption was deployed by these authors [11] to construct a new HIBE scheme in a generic leveled drawing map setting and prove its security. Meanwhile, The Lewko technique was considered by Liu et al. [12]; through this approach, one can look into the memory leakage flexibility in anonymous identity-based encryption schemes. Anonymity of leakage flexibility can be achieved using this scheme, while fully adaptive ID attacks can be resisted.

While ATC can detect objectives and identify collaboration aircraft, it cannot assure full security and coverage at low altitude. Accordingly, Annibalia et al. [13] proposed a new ATC architecture (ARGUS 3D) to address this problem, especially in the absence of PSR coverage. The following steps will discuss the main security techniques was used in the

comparisons. Table 2 discuss presents a summarization for the advantages and dis advantages for the security techniques.

The security techniques are:

1) Public Key Infrastructure (PKI): is a system that uses public key encryption and a digital certificate to yield secure internet services [14].

2) Hash algorithms: Hash algorithms on ADS-B signals are used to confirm, ensure, and identify the source message and generate the output signal, before comparing the latter with its input counterpart.

3) Asymmetric encryption: Asymmetric encryption on ADS-B signals: This is a type of encryption where different keys are used for encrypting and decrypting messages.

4) Symmetric encryption: This is where the same key is used for encrypting and decrypting messages.

5) Staged Identity-Based Encryption (SIBE): A type of public key encryption in which the public key of a user carries unique information about the identity of the user, such as their email address [6].

6) Hierarchical Identity-Based Signature (HIBS): This scheme was first suggested by Gentry and Silverberg in 2002, while Chow et al. proposed the first provable protected HIBS scheme. It requires random oracles to prove its security. It was observed by Yuen and Wei that by using a hierarchical authentication tree and one-time signature, HIBS can be constructed, though it will be ineffective. A direct construction was also provided by the same authors, wherein the number of levels was independent of the size of the signature. Despite the fact that their scheme can be proven without random oracles, it is either demonstrably secure under an even weaker module called the gauntlet-ID model or requires a specially designed strong assumption [10].

7) Batch verification: A technique that determines whether a set of signatures contains any invalid examples [10].

8) Hierarchical Identity-Based Encryption (HIBE): This forms levels of an organizational hierarchy, thereby providing increased functionality. Secret keys can be delegated to descendant characters at lower levels by the user, but messages cannot be decrypted that are intended for a recipient that is not among its descendants [10].

9) Diffie-Hellman (DDH): An assumption that is actually a computational hardness assumption, which is about a certain problem involving distinct logarithms in a cyclic group. Used as a basis from which to prove the security many cryptographic protocols such as EIGamal and Cramer- Shoup cryptosystems.

10) Lewko: This shows that fully secure leakage resilience can be gained using the techniques of dual system encryption [12].

11) NextGen (ATC): This is the next generation air transportation system, which is already saving air carriers and reducing the exhaust emitted by aircraft using an accurate system [7]

12) ARGUS(3D): collaborative project to enhance the security of European citizens by managing 3Ddata positions in all regions, 24/7, in all weather conditions. An enhanced version of the existing PSR [13].

4. THE CONTRIBUTION

4.1. Discussion

In this comparative study, we found that Staged Identity Based Encryption (SIBE) is the most suitable technique for solving the problems inherent in ADS-B. Security, confidentiality, and efficiency requirements can be met by using the SIBE framework. It is sufficiently flexible for effective key management, while being fast enough for highly frequent encryption. To achieve superior overall efficiency, SIBE minimizes heavy IBE operations by effectively deploying a symmetric encryption scheme.

Table 2 Summarization of Activities in Assignment Example.

Techniques	Finding	Limitation
E. Cook, [8] used PKI, symmetric and asymmetric encryption techniques. He used a Public Key Infrastructure (PKI) to verify all ADS-B signals from FAA registered aircraft, asymmetric encryption to exchange a symmetric session key, and used the symmetric session key to validate data authenticity and integrity.	Verifies aircraft identity and authenticates ADS-B messages; avoids public key snooping by third parties; Uses fewer digital signatures. Presents authentication scheme for ADS-B messages	Requires software updates and MAC on packet; increased workload for generating public keys; presents threat in case private key are used.
S. Amin, et al, [9] used Hash algorithms, asymmetric and symmetric encryption on ADS-B signals. They designed a secure transmission framework that prevents ADS-B signals from being spoofed. Three alternative methods were evaluated for securing ADS-B signals: hashing, symmetric encryption, and asymmetric encryption.	1. Hashing algorithms run very quickly and only require software upgrades 2. None of the security issues of key exchanges 3. Provides high-level security system with fewer collisions; needs software upgrades with limited hardware. Secure framework to protect ADS-B signals	1. Needs additional bits in ADS-B messages that are fully used 2. Difficulty sharing public keys between nodes which require knowing the recipient before sending the message 3. Presents security issues in key distribution. Needs more trials in field collision and simulation
E. Hableel et al. [6] used staged identity-based encryption (SIBE). The Staged Identity Based Encryption (SIBE) scheme, is an extended version of hybrid Identity-Based Encryption. They introduced a confidentiality framework for future e-Enabled aircrafts with ADS-B capability.	Proposed framework matches security and efficiency requirements.	Does not match authentication requirements
A. Yang et al. [10] used Three-level HIBS. They proposed a framework for providing authenticated ADS-B based on three-level hierarchical identity-based signature (HIBS).	Proposed a framework supports authentication for ADS-B based on HIBS. Their schemes can significantly reduce the verification cost, so at any time an ADS-B receiver may receive many of signatures.	Requires expensive materials and more time and higher accuracy in the accounts

H. Wang, et al [11] used HIBE with Diffie-Hellmanin assumption. They construct a HIBE scheme in a generic leveled multilinear map setting, they proved its security under multilinear decisional Diffie-Hellmanin assumption in the selective-ID model.	Provides security.	Inefficient

Continued: Table 2 Summarization of Activities in Assignment Example.

Techniques	Finding	Limitation
P. Liu, et al. [12] used Lewko Technique with anonymous identity-based encryption schemes. Their scheme is built in merged order groups which have four prime order subgroups, blind the public parameters and cipher texts using the random elements of same subgroup to achieve the anonymity.	Anonymity leakage flexibility can be achieved through this scheme and full adaptive ID attacks can be resisted	This technique can lead to master key leakage if used by unreliable sources
M. Strohmeier et al. [7] discussed the Integration of ADS-B as part of NextGen ATC system. They reported from their OpenSky sensor network in Central Europe., this sensor is able to capture around 30 percent of the European commercial air traffic.	The issues of ADS-B will be addressed by ATC authorities and the academic community; accordingly, a replacement PSR with ADS-B will be taken into consideration	Server dangers and limitations of final integration between ADS-B and NextGen ATC
E. Anniballi and R. Cardinali [13] used ARGUS(3D) as air guidance and surveillance in 3D. They proposed a ATC (Air Traffic Control) architecture foresees the combined use of conventional system, such as Primary and Secondary Radar, ADSB, etc., and innovative systems such as a new enhanced PSR, passive and bistatic radar network.	Could improve security over a large area, with appropriate cost and accurate determination of the position the position by accuracy way.	The overall performance of the system, and accuracy of data analysis, needs to be improved to obtain better results.

4.2. Case study

Step 1: An assumption is made that all ground controllers are identified by unique identifiers and private keys that are associated with them have been obtained from the corresponding authority, which acts as a Private Key Generator (PKG). (ensure authorization).

Step2: When an aircraft enters a section of airspace that is managed by one ground controller, a securely generated random symmetric key is encrypted by the aircraft with that individual's identity. (create secure channel).

Step 3: Subsequent messages are then encrypted using a secure symmetric encryption scheme under the previously selected random key. (message encryption)

Step 4: After the random symmetric key is encrypted, a cipher text is received, which we call the key cipher text; the ground controller decrypt this using the private key associated with its identity and decrypts subsequent cipher texts, which we call data cipher texts, from the aircraft. (message decryption using private key).

Step 5: With the list of identities of the ground controllers on its flight path, each identity will be used by the aircraft to encrypt a random symmetric key of its choice and the resulting ADS-B messages will be encrypted by said key.

Step 6: A new symmetric key will be chosen and subsequent ADS-B messages for that ground controller will be encrypted by said key when the aircraft communicates with a new ground controller on its flight path. Then, the encrypted key sent by the aircraft will be decrypted by the ground controlle

who is in control of the private key associated with their identity.

5. CONCLUSION

The implementation of ADS-B is moving from a worldwide plan to reality. ADS-B uses a range of technologies to protect

itself from any threats. In this study, we have discussed certain types of this technology, reaching the conclusion that

Staged Identity-Based Encryption (SIBE) is the optimum specimen.

In future research, we will attempt to build on this technique to enhance the security of all types of air traffic.

6. REFERENCES

[1]. THALES AIR SYSTEMS. air traffic management A guide to global surveillance, Parc tertiaire Silic ,

[2]. ICAO. 2007 Guidance Material on Comparison of Surveillance Technologies (GMST). International Civil Aviation Organization Asia and Pacific, (Sept 2007)

[3]. Martin, S., Vincent, L. and Ivan, M. 2015. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. In IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1066-1087, Second quarter.

[4]. Christine, V. Automatic Dependent Surveillance Broadcast (ADS-B) Surveillance development for Air Traffic Management. AirBus

[5]. TextRon Aviation. Mandate and NextGen is 2020 ADS-B out mandate on your radar? Retrieved at: http://txtav.com/en/service/mandates-and-nextgen

[6]. Eman, H., Joonsang, B., Young-Ji, B. and Duncan S. 2015. How to protect ADS-B: Confidentiality framework for future air traffic communication. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Hong Kong, 2015, pp. 155-160.

[7]. Martin, S., Matthias, S., Vincent, L. and Ivan, M. 2014. Realities and challenges of NexGen air traffic management: the case of ADS-B. In IEEE Communications Magazine, vol. 52, no. 5, pp. 111-118, (May 2014).

[8]. Emily, C. 2015. ADS-B, Friend or Foe: ADS-B Message Authentication for NexGen Aircraft. In IEEE 17th International Conference on High Performance Computing and Communications. IEEE 7th

[9]. International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, New York, NY, pp. 1256-1261.

[10]. Sahar, A., Tyler, C., Rennix, O. and Kate, S. 2014. Design of a cyber security framework for ADS-B based surveillance systems. Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, pp. 304-309.

[11]. Anjia, Y., Xiao, T., Joonsang, B.and Duncan S. W. 2017. A New ADS-B Authentication Framework Based on Efficient Hierarchical Identity-Based Signature with Batch Verification. In IEEE Transactions on Services Computing, vol. 10, no. 2, pp. 165-175, March-April.

[12]. Hao, W., Zhihua, Z. and Lei, W. 2014. Hierarchial Identity-Based Encryption Scheme from Multilinear Maps. Tenth International Conference on Computational Intelligence and Security, Kunming, pp. 455-458.

[13]. Pengtao, L., Chengyu, H., Shanqing, G. and Yilei W. 2015. Anonymous Identity-Based Encryption with Bounded Leakage Resilience. IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangiu, pp. 287-292

[14]. Enrico, A. and Roberta, C. 2011. A new architecture to increase security of Air Traffic Control system. 8th European Radar Conference, Manchester, pp. 357-360

[15]. Sufyan, F.A. and Amer, K. O. 2012. Development of Certificate Authority services for web applications. International Conference on Future Communication Networks, Baghdad, pp. 135-140.