An ADS-B Message Authentication Method Based on Certificateless Short Signature

ZHIJUN WU
ANXIN GUO
MENG YUE
LIANG LIU
Civil Aviation University of China, Tianjin, China

The automatic dependent surveillance—broadcast (ADS-B) system adopts an open communication mode, and the lack of designed-in security measures in the ADS-B system makes it vulnerable to various types of attacks (jamming, spoofing, etc.). In view of the low-bandwidth and less-data-bit features of the ADS-B, this paper studies the integrity and authenticity of information by signing messages and proposes an ADS-B message authentication method based on certificateless short signature. This method uses short signature and does not require certificate management and has efficient performance. Compared with the existing approach, the computation costs of the proposed method in the signature phase are reduced by 1/2, and the signature length is reduced by 3/4. Additionally, we used the extended NS2 simulation platform to simulate 1090ES data link in different scenarios of the network; the simulation results show that our solution is suitable for minimum operational performance standard of ADS-B.

Manuscript received November 27, 2018; revised April 20, 2019 and July 22, 2019; released for publication July 24, 2019. Date of publication August 8, 2019; date of current version June 9, 2020.

DOI. No. 10.1109/TAES.2019.2933957

Refereeing of this contribution was handled by R. Sabatini.

This work was supported in part by the National Natural Science Foundation of China under Grant U1533107 and Grant 61601467, in part by the Key Program of Natural Science Foundation of Tianjin under Grant 17JCZDJC30900, and in part by the Fundamental Research Funds for the Central Universities of China under Grant 3122018D007.

Authors' address: Z. Wu, A. Guo, M. Yue, and L. Liu are with the School of Electronic Information and Automation, Civil Aviation University of China, Tianjin 300300, China, E-mail: (zjwu@cauc.edu.cn; guoanxin@outlook.com; myue@cauc.edu.cn; 1110510403@hit.edu.cn). *(Corresponding author: Zhijun Wu.)*

I. INTRODUCTION

Over the years, the aviation industry has rapidly advanced and the number of planes has been increasing dramatically. It is reported that the average number of registered flight movements over Europe is around 26 000 per day [1]. Airplane is currently the safest means of transportation with the lowest accident rate. With the development of economy, more and more people choose airplane as their primary forms of travel. According to the forecast of the International Civil Aviation Organization (ICAO), between 2005 and 2025, it is expected that the number of passenger-kilometers and the number of passengers carried to increase over 100% [2]. In addition, the International Air Transport Association also foresees that the number of passengers and tonnes of cargo that aviation will fly is going to be about 16 billion and 400 million, respectively, in the year 2050 [3]. It can be predicted that the number of airplane will continue to increase in the future, and airspace will become more and more crowded, which will pose great challenges to the conventional air traffic control (ATC) system. Due to the low precision and low refresh rate (4–10 s) of the conventional ATC system, it cannot meet the growth requirements of air traffic. Under this background, automatic dependent surveillance—broadcast (ADS-B) emerged.

A. ADS-B System Architecture

ADS-B is a new type of air surveillance technology by international aviation industry developed and will be the future development direction of the civil aviation. ADS-B systems are scheduled to be deployed in most airspace by 2020, as part of next-generation air transportation systems [4]. In the ADS-B system, there are two subsystems: ADS-B OUT and ADS-B IN. ADS-B OUT periodically broadcasts its messages, and the receiving subsystem, ADS-B IN, receives these messages. In the transmitter aircraft, the GPS receiver receives global navigation satellite system (GNSS) data, calculates its own position, speed, and other concerned information, packages the information into ADS-B message format, and broadcasts it continuously through the data link. The aircraft or ground stations equipped with the ADS-B IN receiver can know the relevant information of the aircraft by receiving the information. Compared with the conventional ground-based radar system, ADS-B provides real-time and more accurate aircraft position information with lower maintenance costs and longer service life, while construction and maintenance costs are only about one-tenth of the former [5]. A typical architecture of the ADS-B system is shown in Fig. 1.

Currently, ADS-B mainly uses two data links: universal access transceiver (UAT) and 1090 extended squitter (1090ES). As can be seen from Fig. 2, the typical size of the ADS-B message in the UAT is 272 bits, while the payload size of ADS-B in 1090ES is 56 bits only. The UAT operates at 978 MHz with a bandwidth of 1 Mb/s. Since the UAT requires installing new hardware, it is currently only used for general aviation. 1090ES is compatible with traditional Mode S transponders and mainly used in

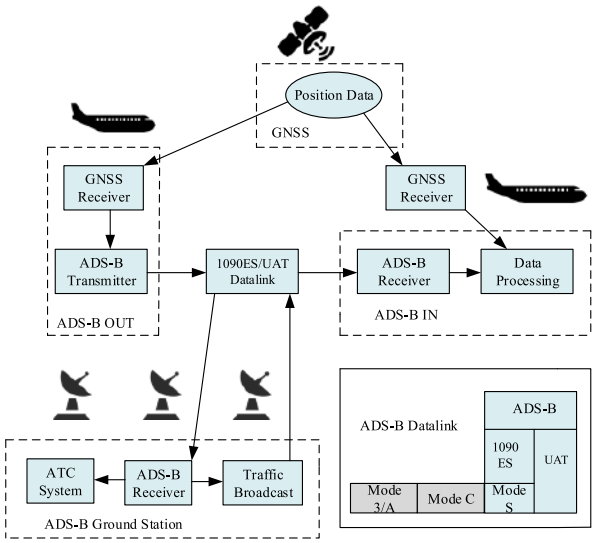


Fig. 1. ADS-B system architecture.

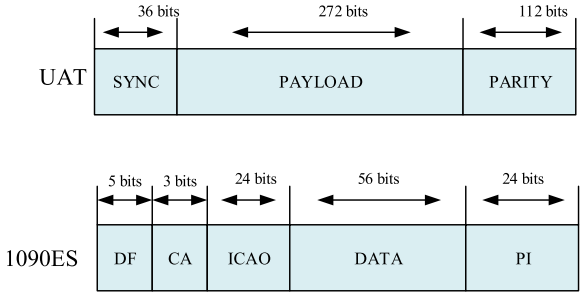


Fig. 2. ADS-B message structures.

commercial aircraft. In this paper, we focus only on the commercially used 1090ES data links, and the relationship between 1090ES and UAT data link can refer to the lower right of Fig. 1.

B. ADS-B Vulnerability

ADS-B uses an open unencrypted broadcast protocol. As the original designer pays more attention to the interoperability and compatibility design of the protocol, it may be less concerned with the encryption protection of the protocol. Therefore, the cost and engineering knowledge required for the attack makes it almost impossible for the designer to consider the protocol as a security mechanism for the ADS-B protocol. However, with the development of technology, especially the advent of software-defined radios over the past few years, the threat model has changed dramatically. As illustrated in Figs. 1 and 2, the transmitted ADS-B message is a plain text, and the data link it uses has no additional security measures; any third party with widely available standard hardware and software can eavesdrop, block, modify, insert, and delete ADS-B messages relatively easily, which brings a significant security risk for its practical application. Researchers have shown possible attacks on ADS-B equipment [4], [7], which will have fatal consequences in reality, for example, plane hijacking and air collision [8].

The vulnerabilities of ADS-B originate from the nature of an unencrypted wireless protocol. From a security perspective, the attack estimates for ADS-B can be divided into three categories: data integrity, message authenticity, and confidentiality. Data integrity requires that ADS-B data cannot be modified, deleted, inserted, and forged during transmission, and message authenticity guarantees that the received message is indeed from the aircraft which claimed. This can defend against message modification, insert, and delete attacks. Confidentiality means that messages are only accessed by authorized aircraft, and confidentiality is mainly against eavesdropping. Considering compatibility and interoperability, ADS-B gave up confidentiality at the beginning of design; the focus for this paper is on data integrity and message authenticity.

Therefore, the research focus of this paper is to ensure the integrity and authentication of ADS-B messages, while having better performance under the condition of using fewer data bits.

C. Our Contributions

For the case that there are few available data bits in the ADS-B message, we apply the certificateless short-signature cryptosystem [9] to the ADS-B field and propose an ADS-B message authentication method based on certificateless short signature, which modifies Tsai's CLSS scheme [10]. By signing the ADS-B message to ensure the integrity and authentication of the information, and without changing the original content of the message, any third party can correctly identify the message, thereby preserving the openness of the ADS-B system. Specifically, the contributions of this paper are as follows.

1) We proposed an ADS-B message authentication method based on certificateless short signature. To the best of the authors' knowledge, we first apply the certificateless short-signature cryptosystem to the ADS-B field, which provides integrity and authenticity in ADS-B messages.
2) The proposed approach overcomes the problem of the certificate management in the asymmetric encryption approach of ADS-B security. More importantly, compared with the related scheme, the key generation center (airport, ICAO, etc.) in our solution cannot obtain the aircraft's private key, and thus, it can offer true nonrepudiation.
3) Since our approach eliminates the costly map-to-point operations, the proposed approach is computationally efficient for on-board equipment with limited resources. Moreover, compared with the existing related scheme, our approach has lower communication cost, which is one-fourth of the compared scheme. Therefore, it is suitable for a low-bandwidth ADS-B data link.

II. RELATED WORK

Security of the ADS-B system has been receiving a great deal of attention recently. Much work has been

accomplished about security of ADS-B, mainly divided into two categories: noncryptographic approaches [11]–[14] and cryptographic approaches [15]–[25]. Noncryptographic approaches include Kalman filtering, time difference of arrival, multilateration, distance bounding, etc. In this paper, we focus only on the cryptographic approaches.

Krishna *et al.* [26] first studied security measures for verifying ADS-B messages using symmetric key encryption or digital signatures. Pan *et al.* [19] proposed an ADS-B data authentication scheme based on the elliptic curve cipher and X.509 certificate. The scheme requires the certification authority (CA) management certificate, which increases the operating cost of the ADS-B system, and in the certificate exchange protocol, the verification phase of the certificate requires high computation and communication costs, and thus, it is not suitable for a low-bandwidth ADS-B data link.

To overcome the shared key problem in symmetric cryptography, Baek *et al.* [21] proposed a confidentiality framework based on staged identity-based (ID-based) encryption. The scheme combines symmetric cryptography with ID-based encryption to overcome the key sharing problem in symmetric encryption.

In order to improve the efficiency of signatures in asymmetric encryption, Baek *et al.* [18] proposed an authentication framework based on online/offline ID-based signature. The scheme separates the operations of different complexity in the signature and completes the complex operations unrelated to the message to be signed in the offline phase. In the online phase, the airborne equipment only needs to do a small amount of low-complexity operations to obtain the signature of the message.

In view of the low-bandwidth characteristics of the ADS-B data link, Yang *et al.* [20] proposed a broadcast authentication scheme for ADS-B based on ID-based signature with message recovery. Because the message can be recovered from the signature, the length of the message is reduced indirectly, thus reducing the communication cost of the ADS-B message.

To more efficiently perform authentication, Yang *et al.* [22] proposed an ADS-B authentication framework based on hierarchical ID-based signature with batch verification. The scheme supports one-time authentication of a group of signatures. However, this scheme requires complex map-to-point operations during the authentication phase. To address the weaknesses in Yang *et al.*'s [22] scheme, He *et al.* [23] proposed a new hierarchical ID-based signature with batch verification. However, the signatures generated by these two schemes are longer, which increases the communication cost of the ADS-B data link.

Yang *et al.* [24] proposed a hybrid encryption scheme that combines format-preserving encryption with broadcast authentication protocol (TESLA) to provide confidentiality, authenticity, and integrity. In order to improve performance, recently, Gowri *et al.* [25] have proposed a new pairing-free ID-based ADS-B authentication scheme with batch verification.

Overall, there are two methods in cryptographic approaches to ensure ADS-B security: data encryption and digital signatures. Data encryption requires the communication parties to preshare a secret key, and the keys cannot be well distributed in real time, which makes its deployment difficult. Moreover, a single private key leak will destroy the entire system, and simply encrypting the ADS-B message is regarded conflicting with the open nature of the ADS-B system. For instance, concerning flight safety and operational requirements, the Federal Aviation Administration (FAA) claims the necessity of clear ADS-B data [6].

However, digital signature does not change the content of the ADS-B messages; it only appends the signatures to the end of the messages, guarantees the integrity and authentication of the data, and also preserves the openness of the ADS-B system. However, most current asymmetric encryption methods in the ADS-B system require the CA to manage certificates, which greatly increases the complexity and operating costs of the ADS-B system. Moreover, in the current related solution, the length of the signature is large and the amount of computation required is large, which is not suitable for the low-bandwidth data link of the ADS-B.

A. Requirements on the Message Authentication Method

In order to ensure ADS-B security, we consider the following security requirements needed to be satisfied.

1) *Integrity and Authenticity:* The ADS-B system adopts an open communication mode, and the lack of designed-in security measures in the ADS-B system makes it vulnerable to various types of attacks. Integrity requires that ADS-B data cannot be modified, deleted, and forged during transmission, and authenticity ensures that the transmitted messages is indeed sent by legitimate ADS-B equipment. Therefore, it can resist active adversarial threats such as spoofing, message modification, etc.

2) *Low Bandwidth:* In the ADS-B system, the communication costs should be as small as possible. First, the 1090-MHz band is crowded; apart from 1090ES, there are three modes, namely, modes A, C, and S transponders that currently use 1090 MHz as the downlink frequency. Moreover, the available data space is small and limited in the ADS-B data link. For instance, the payload size of ADS-B in 1090ES is 56 bits only. Second, in the ADS-B system, each aircraft periodically broadcasts its messages at a high frequency (0.5 s). Lower communication costs will reduce the impact on the ADS-B data link.

3) *Efficient Performance:* The performance of message authentication method should be efficient since onboard devices are usually resource constrained.

B. Adversary Model

McCallie *et al.* [27] show six ways of attacks that could damage the ADS-B system, ranging from the relatively easy disruption using jamming device to more difficult target ghost injects (spoofing) to flood denial. The focus for this paper is how to provide broadcast authentication and integrity for ADS-B. Jamming threat is a general wireless security problem, which does not directly threaten authenticity. Furthermore, as long as the ADS-B message

is not fully encrypted, it will inevitably face eavesdropping, and the open nature of ADS-B has been considered a desirable feature in most scenarios [4]. Therefore, in this paper, we do not consider eavesdropping and jamming. This paper considers an external adversary to the ADS-B system, which is capable of launching active adversarial threats to authenticity and integrity, such as spoofing ghost aircraft or damaging traffic data.

Although we do not consider eavesdropping, it is the first stepping stone for more sophisticated and problematic attacks. Eavesdropping can be used not only to collect sensitive flight information, but also to replay messages and the corresponding signatures. However, these attackers cannot forge a new signature, so it is not directly threatening authenticity. We can simply append a timestamp to the ADS-B message to prevent the replay attack, which is a tradeoff approach, since adding timestamps will increase communication overhead. However, it is a really important consideration for future air traffic communication protocol design.

In addition, considering a key compromise scenario, in the ID-based cryptography, private key generator (PKG) knows the private key of all aircraft; the FAA or ICAO could assume the role of PKG. ADS-B operates in a cryptographically untrusted environment. Once PKG is compromised, all private keys will be leaked; then, the adversary could forge any entity's signatures. So, it cannot offer true nonrepudiation. Our approach is based on certificateless public key cryptography that do not require the use of certificates. Furthermore, only part of the private key is generated by PKG, and the complete private key is generated by the aircraft itself, which eliminates the key escrow problem and enhances the overall security of the ADS-B system.

C. Motivation

In order to simplify the management of public key certificates, Shamir introduced the notion of ID-based public-key cryptography [28]. Most of the current schemes in ADS-B security are ID-based cryptography. However, the key escrow problem is an inherent problem of ID-based cryptography; the private key of any user is known to the PKGs, and usually, ICAO or Airport is assumed to be PKG. Since ADS-B operates in a cryptographically untrusted environment, whatever cryptographic hardware, software, and keys are ultimately employed will be accessible to malicious parties [6]. Once the PKG's master key is leaked, an adversary could forge any aircraft's signatures, and that means that all security measures are completely ineffective. In [29], Al-Riyami and Paterson introduce a new paradigm, namely, certificateless public key cryptography. In certificateless public key cryptography, PKG only knows user's partial private key, eliminating the key escrow problem. That is why, we apply the certificateless public key cryptography to the ADS-B field.

D. Organization

The rest of this paper is organized as follows. Section III presented some preliminaries. We proposes an ADS-B message authentication method based on short certificateless signatures and demonstrates the experiment results in Sections IV and V, respectively. Finally, we make a conclusion of this paper in Section VI.

III. PRELIMINARIES

In this section, we briefly review the basic concepts on bilinear pairings, some related mathematical problems, and definition of the proposed message authentication method. For more detailed information about cryptography, refer to [9].

A. Bilinear Pairings and Difficult Problems

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group with the same order q. Let $e : G_1 \times G_1 \to G_2$ be a map with the following properties.

1) *Bilinearity:* $e(aP, bQ) = e(P, Q)^{ab}$ for any $P, Q \in G_1$, and $a, b \in Z_q^*$.
2) *Nondegeneracy:* There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$; in other words, the map does not send all pairs in $G_1 \times G_1$ to the identity in G_2.
3) *Computability:* There exists an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

The proposed message authentication method is based on the following difficult problems:

1) *Computational Diffie–Hellman problem:* Given $P, aP, bP, \in G$, and $a, b \in Z_p$, there exists no algorithm that can compute $abP \in G$ with nonnegligible probability within polynomial time.
2) *Collusion attack algorithm with k traitors (k-CAA):* For an integer $a \in Z_p^*$, $P, Q = xP, h_1, \ldots, h_k \in Z_p^*, (1/(h_1 + x))P, \ldots (1/(h_k + x))P$, it is hard compute $1/(h + x)$ for some $h \notin h_1, \ldots, h_k$.

B. Definition of the Proposed ADS-B Message Authentication Method

The proposed ADS-B message authentication method consists of the following algorithms.

1) *Setup:* On input of a security parameter k, the Setup algorithm, which is run by the KGC, generates a master private key s, public parameters params, and its corresponding master public key P_{pub}. Then, this algorithm publishes the master public key P_{pub} and the public parameters params and keeps the master private key s secret.
2) *Set partial private key:* On input of system parameters $params$, master private key s, and FlightID, this algorithm, which is run by KGC, outputs a partial private key d_{ID}. The aircraft verify the legality while receiving a partial private key.
3) *Set secret value:* Take the system parameters params and FlightID as input, this algorithm, run by airplane, returns a secret-value x_{ID}.
4) *Set public key:* On input of system parameters params and secret value x_{ID}, this algorithm is run by airplane and returns the full public key PK_{ID}.

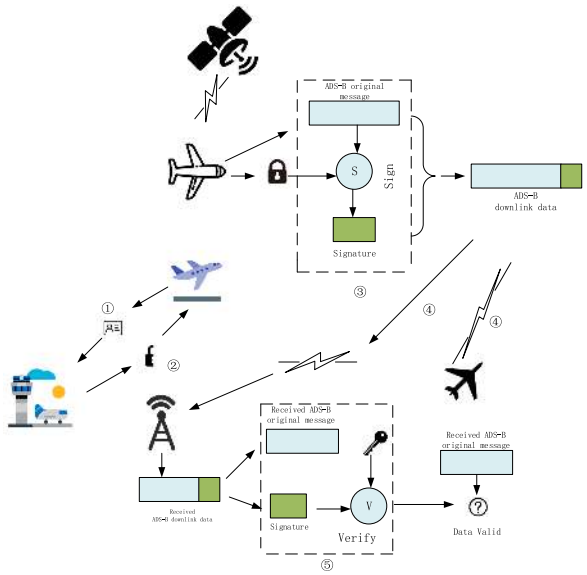


Fig. 3. Main idea of the message authentication method.

5) *CLSS-Sign:* This algorithm is run by airplane and takes public parameters params, message m, and the airplane full private key as inputs and then returns a signature σ.
6) *CLSS-Verify:* On input of system parameters params, message m, master public key P_{pub}, the signature σ, and the full public key PK_{ID}, this algorithm outputs "1" when the signature σ is valid. Otherwise, this algorithm outputs "0."

IV. PROPOSED ADS-B MESSAGE AUTHENTICATION METHOD

The design of our method is based on the communication process from the takeoff to the landing of the aircraft, combining the process of digital signature with the communication process of ADS-B messages. The main idea of the message authentication method is shown in Fig. 3. Before the aircraft takes off, it first submits identity information to the airport and obtains partial private key. Then, the aircraft calculates the corresponding public key and the complete private key, while it keeps the private key secret and publishes its public key. A complete list of all known public keys or a list of public keys that have changed since the last flight can be uploaded to the aircraft before the aircraft takes off. Real-time key or system parameters publication could be communicated over satellite or ground data links that are available on most commercial aircraft.

During the flight of the aircraft, the GPS receiver receives GNSS data, calculates its own position, speed, etc., and then packages the information into ADS-B message format. Afterwards, the airborne equipment uses the private key to sign the ADS-B messages to be transmitted and then broadcasts the message–signature pair. The surrounding aircraft, ground station, or any third part equipped with an ADS-B IN receiver can receive the messages. The receiver verifies the received messages with the published public key. If the verification passes, it indicates that the messages have not been changed or replaced by adversary. Moreover, regardless of whether they verify the signature or not, the broadcast messages can be seen by all participants, and thus, there remains the openness of the ADS-B system. If the message is changed during the propagation process, for example, an adversary spoofing ghost aircraft, and the verification fails, then the receiver drops the messages and thus ensures the integrity and authentication of the ADS-B message.

A. Proposed Method

This section presents the details of the ADS-B message authentication method based on certificateless short signature.

1) *Setup:* Let G_1, G_2 be bilinear groups of some prime on order $p \geq 2^k$, and k be the security parameters of the scheme. $e : G_1 \times G_1 \to G_2$ is an admissible bilinear pairing. Let $H_1 : \{0,1\} \times G_1 \times G_1 \to Z_q^*$, $H_2 : \{0,1\} \times G_1 \times G_1 \times G_1 \to Z_q^*$ be two secure cryptographic hash functions. KGC chooses a random number $s \in Z_q^*$ as a master private key and keeps it secretly, and an generator $P \in G_1$ then computes the corresponding master public key $P_{\text{pub}} = \{P_{\text{pub1}}, P_{\text{pub2}}, P_{\text{pub3}}\} = \{sP, s^{-1}, s^2P\}$ and publishes parameters $\{G_1, G_2, q, P, P_{\text{pub}}, H_1, H_2, e(P,P)\}$.
2) *Set partial private key:* Given the system parameters params, master private key s, and FilghtID, KGC chooses a random number r_{ID} and then computes the following equations:

$$R_{\text{ID}} = r_{\text{ID}} P_{\text{pub1}} \tag{1}$$

$$h_{\text{ID}} = H_1(\text{ID}, R_{\text{ID}}, P_{\text{pub}}) \tag{2}$$

$$s_{\text{ID}} = r_{\text{ID}} + h_{\text{ID}} s \mod q. \tag{3}$$

Each aircraft will be identified by a ID(FilghtID), which is of the following format ID = AR ‖ AD ‖ FN ‖ AUX, which denote aircraft registration (AR), 24-bit ICAO code, flight number (FN), and other auxiliary information (AUX), respectively. AUX may contain the date and duration of the flight, which can serve as additional information for unique identification of an aircraft [18]. KGC transmits partial private key $d_{\text{ID}} = (s_{\text{ID}}, R_{\text{ID}})$ to the plane. Upon receiving d_{ID}, the plane can verify its validity over the following equation:

$$s_{\text{ID}} P_{\text{pub1}} \stackrel{?}{=} R_{\text{ID}} + h_{\text{ID}} P_{\text{pub3}}. \tag{4}$$

3) *Set secret value:* Given the system parameters params, the plane chooses a random number x_{ID} as its secret value.
4) *Set public value:* Given the system parameters params and the secret value x_{ID}, the plane with identity ID(FlightID) computes $P_{\text{ID}} = x_{\text{ID}} P_{\text{pub1}}$ and sets $\text{PK}_{\text{ID}} = (P_{\text{ID}}, R_{\text{ID}})$ as the public key and publishes it.

5) *CLSS-Sign:* Given the system parameters params and a message m, the plane(signer) computes

$$\sigma = (k_{\mathrm{ID}} + x_{\mathrm{ID}})^{-1} P_{\mathrm{pub2}} \tag{5}$$

where $k_{\mathrm{ID}} = H_2(\mathrm{ID}, m, P_{\mathrm{ID}}, R_{\mathrm{ID}}, P_{\mathrm{pub}})$.

6) *CLSS-Verify:* Given the system parameters params, ID, $\mathrm{PK_{ID}}$, message m, and signature σ, the aircraft or ground station (verifier) computes the following equations:

$$h_{\mathrm{ID}} = H_1(\mathrm{ID}, R_{\mathrm{ID}}, P_{\mathrm{pub}}) \tag{6}$$

$$k_{\mathrm{ID}} = H_2(\mathrm{ID}, m, P_{\mathrm{ID}}, R_{\mathrm{ID}}, P_{\mathrm{pub}}). \tag{7}$$

Then, the verifier check the following equation:

$$e(\sigma, k_{\mathrm{ID}}(R_{\mathrm{ID}} + h_{\mathrm{ID}} P_{\mathrm{pub3}}) + P_{\mathrm{ID}}) \stackrel{?}{=} e(P, P). \tag{8}$$

If (8) holds and accepts the signature σ, the signature σ is invalid. We note that $e(P, P)$ is precomputed in the setup phase and only computed once.

Correctness: if σ is a valid signature on message m, then the correctness holds [see (9) shown at the bottom of this page].

B. Security Proof

For certificateless cryptosystems, there are two types of adversary with different capabilities [28]: A_I and A_{II}. Adversary A_I models a dishonest user who does not have access to the master private key and partial private key but has the ability to replace the public key. Adversary A_{II} models a malicious KGC who has access to the master private key but cannot replace the public key.

In this section, we briefly present the proposed method in the random oracle model, which is existential unforgeability against adaptive chosen message attack based on the k-CAA hard problem. The principle of proof is similar to [30]. To save space, we only give a summary proof about adversary A_I. For detailed proof, refer to [10].

The challenger C runs Setup to generate the system parameters and the master private key. The system parameters is sent to the adversary, and the master private key is kept secret.

Adversary makes the following queries.

1) H_1 *queries:* A_I can query the random oracle on $(\mathrm{ID}, R_{\mathrm{ID}}, P_{\mathrm{pub}})$; the challenger C returns H_1 and then adds $(\mathrm{ID}, R_{\mathrm{ID}}, P_{\mathrm{pub}}, H_1)$ to list L_{H_1}.
2) H_2 *queries:* A_I can query the random oracle on $(\mathrm{ID}, P_{\mathrm{ID}}, R_{\mathrm{ID}}, P_{\mathrm{pub}})$; the challenger C returns H_2 and then adds $(\mathrm{ID}, P_{\mathrm{ID}}, R_{\mathrm{ID}}, P_{\mathrm{pub}}, H_2)$ to list L_{H_2}.
3) *Partial key queries:* A_I query on his/her chosen ID, if $\mathrm{ID} \neq \mathrm{ID}^*$; the challenger computes partial key and return to adversary. If $\mathrm{ID} = \mathrm{ID}^*$, the challenger terminates partial-key queries.
4) *Replace public key:* A_I can request to replace public key with new public key $\mathrm{PK}^*_{\mathrm{ID}}$; the challenger replaces the original public key $\mathrm{PK_{ID}}$ with $\mathrm{PK}^*_{\mathrm{ID}}$ and then adds $(\mathrm{ID}, PK^*_{\mathrm{ID}})$ to list L_{PK}.
5) *Sign:* For each sign query on an input (m, ID), if $\mathrm{ID} \neq \mathrm{ID}^*$, the challenger generates the corresponding valid signature σ; otherwise, the challenger reports failure and terminates the simulation.

Finally, A_I outputs a signature σ^* for ID^* on a message m^*. The signature can pass the verification equation (8). Then, we show the probability that A_I successfully forges a signature as follows.

E_1: The challenger does not abort all partial key queries during the simulation.

E_2: A_I successfully forges a signature σ on m for ID.

E_3: The forged signature σ^* satisfies $\mathrm{ID} = \mathrm{ID}^*$.

Then, we have

$$\Pr[E_1] \geq \left(1 - \frac{q_{H_1}}{q}\right)^{q_{H_1}} \tag{10}$$

$$\Pr[E_2 \mid E_1] \geq \epsilon \tag{11}$$

$$\Pr[E_3 \mid E_1 \wedge E_2] \geq \frac{q_s}{q} \tag{12}$$

where q_{H_1} and q_s represent the number of H_1 queries and the sign queries, respectively. If adversary successfully forges the signature σ^* and the signature can pass (8), then the probability that adversary breaks the k-CAA problem is $\Pr[E_1] \geq (1 - \frac{q_{H_1}}{q})^{q_{H_1}} \cdot \frac{q_s}{q} \cdot \epsilon$

Because ϵ is nonnegligible, adversary cannot break the k-CAA problem. Hence, the proposed method is existential unforgeability against adaptive chosen message attack.

V. PERFORMANCE ANALYSIS

To evaluate the performance of the proposed method, this section compares the proposed method with current newer similar methods, in terms of computation cost and communication cost. Furthermore, we used the extended NS2 simulation platform to simulate the impact of our method on the 1090ES data link.

A. Computation Costs

First is the theoretical comparison of computational complexity. Table I gives a comparison of computational

$$\begin{aligned} e(\sigma, k_{\mathrm{ID}}(R_{\mathrm{ID}} + h_{\mathrm{ID}} P_{\mathrm{pub3}}) + P_{\mathrm{ID}}) &= e((k_{\mathrm{ID}} s_{\mathrm{ID}} + x_{\mathrm{ID}})^{-1} P_{\mathrm{pub2}}, k_{\mathrm{ID}}(R_{\mathrm{ID}} + h_{\mathrm{ID}} P_{\mathrm{pub3}}) + P_{\mathrm{ID}}) \\ &= e(((H_2(\bullet)(r_{\mathrm{ID}} + H_1(\bullet)s)) + x_{\mathrm{ID}})^{-1} s^{-1} p, H_2(\bullet)(r_{\mathrm{ID}} s P + H_1(\bullet)s^2 P) + x_{\mathrm{ID}} s P) \\ &= e(((H_2(\bullet)(r_{\mathrm{ID}} + H_1(\bullet)s)) + x_{\mathrm{ID}})^{-1} P, H_2(\bullet)(r_{\mathrm{ID}} P + H_1(\bullet) s P) + x_{\mathrm{ID}} P) \\ &= e(P, P)^{((H_2(\bullet)(r_{\mathrm{ID}} + H_1(\bullet)s)) + x_{\mathrm{ID}})^{-1} \cdot ((H_2(\bullet)(r_{\mathrm{ID}} + H_1(\bullet)s)) + x_{\mathrm{ID}})} \\ &= e(P, P) \end{aligned} \tag{9}$$

TABLE I
Efficiency Comparisons

Methods	Sign	Verify
HIBS-Y	$2T_m$	$5T_bp + 2T_{map} + T_m$
HIBS-H	$2T_m$	$2T_bp + 3T_m$
OURS	T_m	$T_bp + 2T_m$

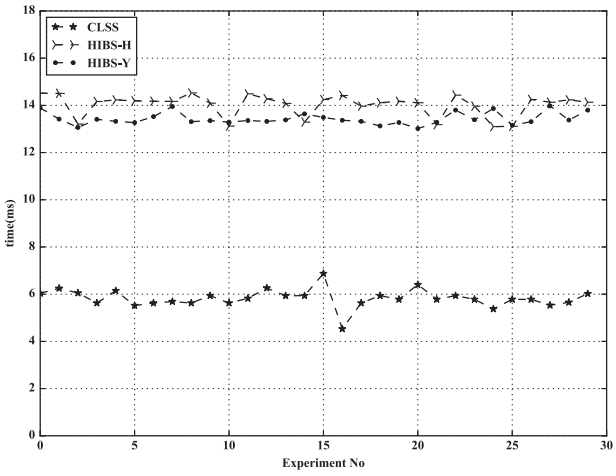


Fig. 4. Signature signing time for different experiments.

efforts required for our method with that of the signature method in [22] and [23]. Here, we only consider the costly operations, which are defined in the following, where T_m denotes the runtime of executing a point multiplication operation, T_{bp} denotes the runtime of executing a bilinear paring operation, and T_{map} denotes the runtime of executing a map-to-point operation. It can be observed from Table I that both [22] and [23] needs to execute two point multiplication in sign phase. In contrast, the proposed method only needs one-point multiplication. In the verification phase, the proposed method needs one bilinear paring operation and two-point multiplication and does not require map-to-point operation, which efficiently reduces the time of verification compared with [22] and [23].

In order to demonstrate the actual performance of the proposed method, we implemented the above schemes on a personal computer (Intel-i3 3.8-GHz processor, 4-GB memory. and Window 10 operating system) using the pairing-based cryptography library developed by Stanford University based on C language. We chose a super singular elliptic curve $E(F_p) : y^2 = X^3 + 1$ over on the finite field F_q for q is a 160-bit prime number, and p is a 512-bit prime number. To obtain more stable and accurate runtime, we ran each method 30 times to get an average value, and the statistical results are shown in Figs. 4 and 5, which illustrate the signature time and the corresponding verification time of different methods, respectively. From Fig. 4, we can see that the performance of [22] and [23] in the signature phase is not much different, and [23] is slightly better than [22]. The signature time of the proposed method is half of the compared scheme and is consistent with the theoretical analysis in Table I. It can be seen from Fig. 5 that in the verification

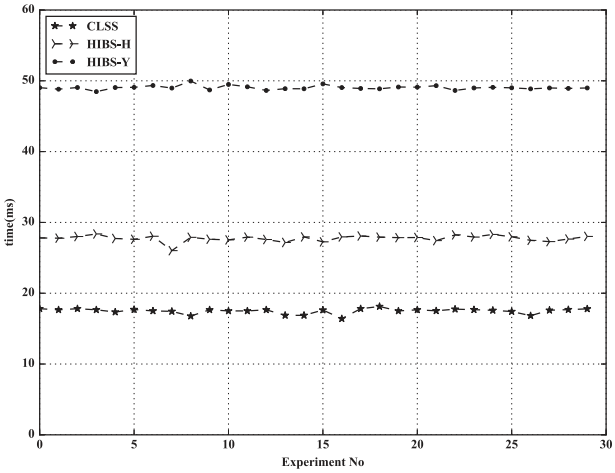


Fig. 5. Signature verification time for different experiments.

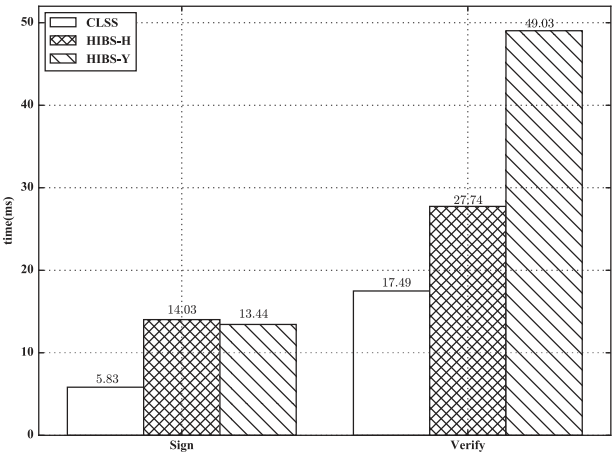


Fig. 6. Mean running time of different methods.

phase, the proposed method is still superior to the compared scheme. In order to compare the performance of different schemes more intuitively, we averaged 30 sets of data into a histogram of Fig. 6. It can be clearly seen from Fig. 6 that the proposed method is superior to the compared scheme in both the signature phase and the verification phase.

B. Communication Costs

In this section, we analyze the communication cost of the proposed method and compare its performance with [22] and [23]. According to the above analysis, we know that the ADS-B system has limited bandwidth, which means the amount of data transferred is small. It can be seen from Fig. 7 that the signature length of the proposed method is one-fourth of the compared scheme, which greatly reduces the communication cost of the ADS-B system. Note that L is the bit length of an element in an additive group G_1.

C. Simulation Results

For further performance analysis, we used the extended NS2 simulation platform to simulate 1090ES data link in different scenarios of the network. In this simulation, we simulated the scenario where the aircraft (flight altitude:

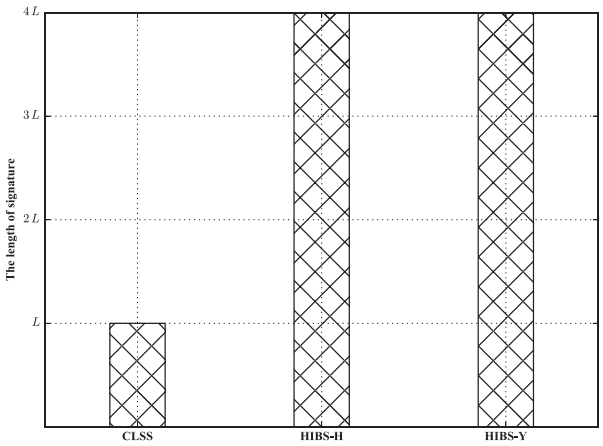


Fig. 7. Comparison of the communication costs of different methods.

TABLE II
Scene Parameter Setting

Scenario Size(Km)		15.347*15.347
Number of Nodes	Aircraft	10-200
	Ground Station	1
Node Distribution	Aircraft	evenly distributed
	Ground Station	center
Node Height	Aircraft	10 Km
	Ground Station	0 Km
Simulation Time		10 s

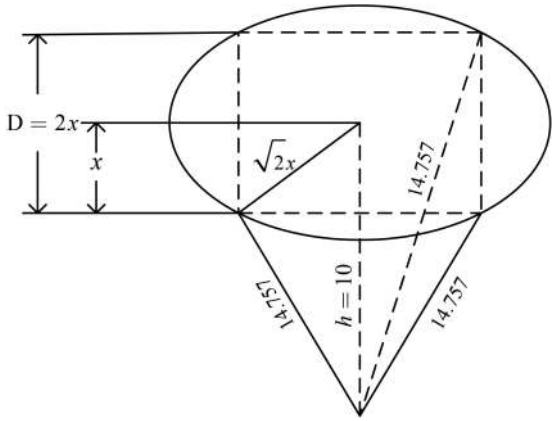


Fig. 8. Map of ground station coverage.

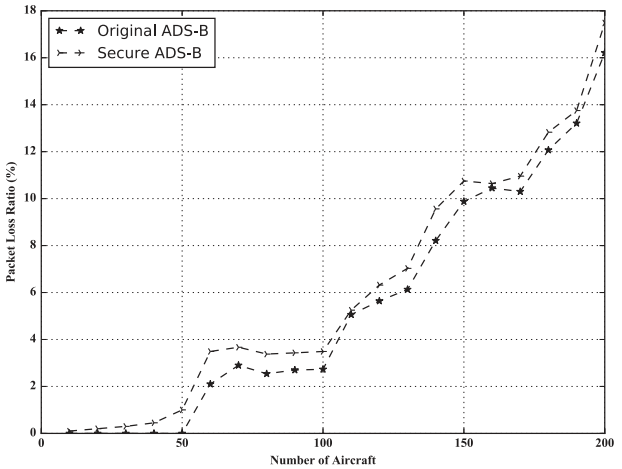


Fig. 9. Trend of the packet loss ratio with the increase in the number of aircraft.

10 km) communicates with the ground station, and the messages are sent every half second. We used the 1090ES A1 device with a communication range of 20 nmi (37.04 km) [31]. The most important assumption taken to develop the simulation model was that every transmission message within a communication range would be received by the ground station. In order to ensure that the ground station can receive messages from all aircraft within the communication range, in the multipath fading environment, the actual communication distance is 14.757 km. The ground station coverage area depends on the flight altitude h and the maximum communication range. Hence, it is necessary to know the coverage of a single ground station. As we can see from Fig. 8, the coverage of the ground station can be abstracted into a square, where the side length $D=2x=2\sqrt{\frac{(7.968\times1.852)^2-10^2}{2}}=15.347$. Table II shows the parameter setting for NS2.

In order to reduce the complexity, we set the simulation topology to a square area of 15 km $\times$ 15 km. All the mobile nodes in the scenario are randomly moving at a constant speed in the horizontal area with a vertical height of 10 km. The number of node increases from 10 to 200. All mobile nodes are produced by the NS2 stochastic production scene. The mobile node broadcasts an ADS-B position message and an airspeed message every 0.5 s. The ground station has a height of 0 km and is located at the center of the topology.

Fig. 9 shows the packet loss ratio under different network scenarios. With the increase of aircraft number, which means that message collision probability will become larger. So, the original ADS-B packet loss rate also increases. When the number of aircraft reaches 200, the packet loss ratio is about 17%. Additionally, our method implies additional processing time to sign or verify a packet; it will be discussed later, which also increase packet collision probability. That is why, the secure ADS-B packet loss ratio is slightly larger than the original ADS-B packet loss ratio. Note that we did not consider the interference of the Mode S transponder. Namely, in this paper, we only consider the case of packet collision due to the broadcast or receive time interval from two separate messages that overlap partially or completely.

End-to-end delay refers to the time between the sending node signing the message and the receiving node successfully verifying the signature. End-to-end delay under different network scenarios is shown in Fig. 10. End-to-end delay mainly includes transmission delay, propagation delay, and reception delay. The propagation delay is related to the height of the aircraft. When the altitude of the aircraft is

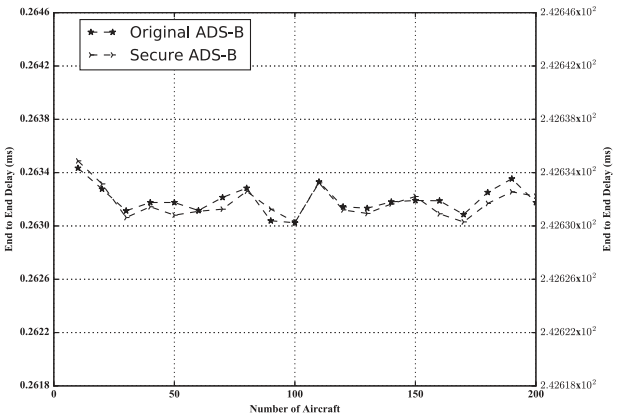


Fig. 10. Trend of end-to-end delay with the increase in the number of aircraft.

TABLE III
Comparative Summary: Attributes and Features

Methods	Data Integrity	Source Integrity	Non Reputation	Complex Operation
HIBS-Y	Yes	Yes	No	Yes
HIBS-H	Yes	Yes	No	No
OURS	Yes	Yes	Yes	No

10 km, the mathematical expectation of the propagation delay is 0.042 ms. The transmission delay and reception delay are calculated in the same way: $\frac{\text{packetsize}}{\text{bandwidth}} = \frac{112\,\text{bit}}{1\,\text{Mbit/s}} = 0.112$ ms. So, the total end to end delay expectation is 0.266 ms. As can be seen from Fig. 10, the end-to-end delay is independent of the number of nodes in the network. With the increase in the number of aircraft, the end-to-end delay fluctuates around 0.266 ms. However, our method has a higher end-to-end delay compared to the original ADS-B. When using the proposed method, the end-to-end delay is increased by about 24 ms. As mentioned above, the average running time of the proposed method is 23.32 ms. It can be seen that the increased end-to-end delay is almost the same as the running time of the proposed approach. This is because securing data packets in our approach means that additional processing time is required to sign or verify a packet. Although the method used in this paper increases the end-to-end delay, its value is still less than the highest Required Communication Technical Performances delay constraint specified (740 ms) by Eurocontrol and FAA for AOC services [32].

A comparison of different methods is shown in Table III, where complex operation denotes map-to-point operation. Data integrity ensures that ADS-B messages have not been modified during the broadcast process. Source integrity ensures that the transmitted messages are indeed sent by legitimate ADS-B equipment. Like our solution, the compared schemes also ensure the security of ADS-B by signing the message, thus ensuring data integrity and source integrity. However, compared schemes are based on identity encryption; the PKG can forge any aircraft's signatures, so it cannot offer true nonreputation. Our approach is based on certificateless public key cryptography, and the PKG only generates partial private key of aircraft, thus providing nonrepudiation. Map-to-point operation is an expensive cryptographic operation and requires more computing resources. In our method, we remove the complex operation, which greatly improved the efficiency of the signature.

VI. DISCUSSION

In this section, we briefly discuss the advantages and disadvantages of our approach and its impact on the ADS-B system.

A. Communication Overhead

The communication overhead of our approach is L, where L is the bit length of an element in an additive group G_1. To achieve a security level of 1024-bit RSA algorithm, the size of P is 512 bits. Therefore, the size of an element in G_1 is $512 + 512 = 1024$ bits. The communication overhead of our approach is $L = 1024$ bits, which is larger than the maximum payloads of the ADS-B message specified in 1090ES (56 bits). Note that the communication overhead of Yang *et al.* [22] and He *et al.* [23] are $4L = 4096$ bits. There are two alternative broadcast methods: 1) broadcasting the message-signature pair together; and 2) broadcasting a sequence of ADS-B 112 bit standard messages, where the first is the standard ADS-B message followed with several ADS-B messages that package the divided signature segments in the ADS-B data blocks. The former method requires altering the ADS-B message format, and extending the ADS-B message length will increase the potential of interference. The latter method preserves the format of the ADS-B message. The disadvantage of the latter method is that it increases the delay between the original message transmission and the message's authentication. In order to secure ADS-B operations, the incurred latency is worthwhile compared to no security at all. To avoid these difficulties mentioned above, a possible alternative would be to broadcast signed ADS-B messages over the aviation-protected L-band at 960–1215 MHz [6].

B. Key Management

System parameters and public keys are public. There are two alternative published methods: 1) broadcasting the message–public keys pair together; and 2) uploading a complete list of public keys before the aircraft takes off. The former method occupies the already crowded bandwidth and reduces the update frequency of messages, which is critical for ADS-B. Hence, we chose the latter method. To reduce the occupation of the crowded 1090ES data link, before the aircraft takes off, a complete list of all known public keys or a list of public keys that have changed since the last flight can be uploaded to the aircraft, while real-time key or system parameters publication could be communicated over ground data links that are available on most commercial aircraft.

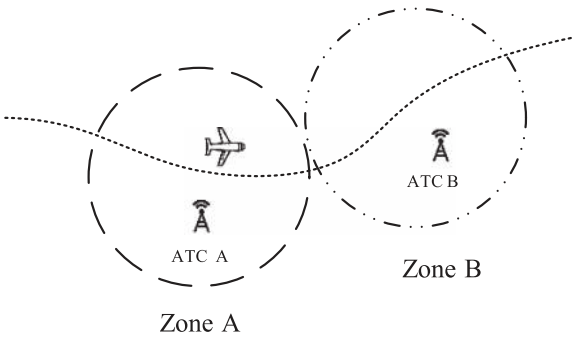


Fig. 11. Key publishing principle.

During the flight of the aircraft, in nonradar airspace, there is no ground station, so the key publication could be communicated over satellite data links. In radar airspace, a simplified example is illustrated in Fig. 11. Zone A is under control of ATC A, while zone B is under control of ATC B. The dotted line represents the trajectory of the aircraft. When the aircraft passes through the management area of different ATCs, it will be given the public key that has been changed in the area while being granted permissions. Because the ATC that manages each area is geographically well defined, the aircraft can choose the appropriate public key. In order to reduce the occupation of the 1090ES data link, Flight Information Service Bulletin (FIS-B) is an optional solution. One major tradeoff to be considered when implementing this solution is the cost. One is the installation cost. FIS-B is broadcast over the UAT frequency; to facilitate interoperability between aircraft using different frequencies, the FAA will install ADS-R (Rebroadcast) capabilities in ADS-B ground stations to rebroadcast 1090ES messages in the UAT format and vice versa. The other is the cost of use. The aircraft needs more storage space to store a large number of public keys. To save storage space, the aircraft can only store the public keys of area where it passing through.

VII. CONCLUSION

Considering the low bandwidth and limited available data bits of the ADS-B system, in this paper, we proposed an ADS-B message authentication method based on certificateless short signature. Compared with the related scheme, the signature length of the proposed method in the signature phase is reduced by 3/4, and the overall performance is also improved to a certain extent. The performance of the signature phase is nearly doubled. In addition, our method does not need to manage certificates; at the same time, it eliminates the key escrow problem, which greatly reduces the burden on the ADS-B system and enhances the usability and overall security of the system. Additionally, we conducted a simulation under the extended NS2 simulation platform, and the simulation results show that the proposed method is suitable for minimum operational performance standard of ADS-B. The next step is to demonstrate the feasibility of its application in the actual ADS-B network [33]. In addition, we noticed that ADS-B messages are sent at a high frequency, and it is crucial for the receiver to be able to quickly verify ADS-B messages. Hence, future work will include extending the method to provide batch verification.

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, May 2014.

[2] ICAO, *Outlook For Air Transport to the Year 2025*. Montreal, QC, Canada: Int. Civil Aviation Org., Sep. 2007.

[3] IATA, Vision 2050, Int. Air Transp. Assoc., Montreal, QC, Canada, Feb. 2011. [Online]. Available: https://www.iata.org/pressroom/facts_figures/documents/vision-2050.pdf

[4] M. Strohmeier, V. Lenders, and I. Martinovic
On the security of the automatic dependent surveillance-broadcast protocol
IEEE Commun. Surv. Tut., vol. 17, no. 2, pp. 1066–1087, Second Quarter 2015.

[5] E. Atienza, R. Falah, S. Garca, L. Gutiérrez, and O. Robles
ADS-B: An air navigation revolution
Rey Juan Carlos Univ.–Fuenlabrada Campus, Madrid, Spain, Rep., Apr. 2013.

[6] K. D. Wesson, T. E. Humphreys, and B. L. Evans
Can cryptography secure next generation air traffic surveillance 2014. [Online]. Available: https://radionavlab.ae.utexas.edu/images/stories/files/papers/adsb_for_submission.pdf

[7] A. Costin and A. Francillon
Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices
In *Proc. BlackHat USA*, 2012, pp. 1–12.

[8] M. Schäfer, V. Lenders, and I. Martinovic
Experimental analysis of attacks on next generation air traffic communication
In *Proc. Int. Conf. Appl. Cryptography Netw. Secur.*, 2013, pp. 253–271.

[9] D. Boneh and M. Franklin
Identity-based encryption from the weil pairing
In *Proc. Annu. Int. Cryptol. Conf.*, 2001, pp. 213–229.

[10] J.-L. Tsai
A new efficient certificateless short signature scheme using bilinear pairings
IEEE Syst. J., vol. 11, no. 4, pp. 2395–2402, Dec. 2017.

[11] I. A. Mantilla-Gaviria, M. Leonardi, G. Galati, and J. V. Balbastre-Tejedor
Localization algorithms for multilateration (MLAT) systems in airport surface surveillance
Signal, Image Video Process., vol. 9, no. 7, pp. 1549–1558, Oct. 2015.

[12] Y. Kim, J.-Y. Jo, and S. Lee
ADS-B vulnerabilities and a security solution with a timestamp
IEEE Aerosp. Electron. Syst. Mag., vol. 32, no. 11, pp. 52–61, Nov. 2017.

[13] L. Mauro, E. Piracci, and G. Galati
ADS-B jamming mitigation: A solution based on a multichannel receiver
IEEE Aerosp. Electron. Syst. Mag., vol. 32, no. 11, pp. 44–51, Nov. 2017.

[14] M. Leonardi
ADS-B anomalies and intrusions detection by sensor clocks tracking
IEEE Trans. Aerosp. Electron. Syst., to be published, doi: 10.1109/TAES.2018.2886616.

[15] V. Edward
Enhanced ADS-B research
IEEE Aerosp. Electron. Syst. Mag., vol. 22, no. 5, pp. 35–38, Oct. 2007.

[16] T. Kacem, D. Wijesekera, and P. Costa
Integrity and authenticity of ADS-B broadcasts
In *Proc. IEEE Aerosp. Conf.*, Mar. 2015, pp. 1–8.

[17] R. V. Robinson, K. Sampigethaya, M. Li, S. Lintelman, R. Poovendran, and D. von Oheimb
Secure network-enabled commercial airplane operations: It support infrastructure challenges
In *Proc. 1st CEAS Eur. Air Space Conf. Century Perspectives*, 2007, pp. 1–10.

[18] J. Baek, Y.-J. Byon, E. Hableel, and M. Al-Qutayri
An authentication framework for automatic dependent surveillance-broadcast based on online/offline identity-based signature
In *Proc. 8th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, Oct. 2013, pp. 358–363.

[19] W. Pan, Z. Feng, and Y. Wang
ADS-B data authentication based on ECC and X.509 certificate
J. Electron. Sci. Technol., vol. 10, pp. 51–55, Jan. 2012.

[20] H. Yang, R. Huang, X. Wang, J. Deng, and R. Chen
EBAA: An efficient broadcast authentication scheme for ADS-B communication based on IBS-MR
Chin. J. Aeronaut., vol. 27, no. 3, pp. 688–696, 2014.

[21] J. Baek, E. Hableel, Y.-J. Byon, D. S. Wong, K. Jang, and H. Yeo
How to protect ADS-B: Confidentiality framework and efficient realization based on staged identity-based encryption
IEEE Trans. Intell. Transp. Syst., vol. 18, no. 3, pp. 690–700, Mar. 2017.

[22] A. Yang, X. Tan, J. Baek, and D. S. Wong
A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification
IEEE Trans. Services Comput., vol. 10, no. 2, pp. 165–175, Mar. 2017.

[23] D. He, N. Kumar, K.-K. R. Choo, and W. Wu
Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system
IEEE Trans. Inf. Forensics Secur., vol. 12, no. 2, pp. 454–464, Feb. 2017.

[24] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang
A practical and compatible cryptographic solution to ADS-B security
IEEE Internet Things J., vol. 6, no. 2, pp. 3322–3334, Apr. 2019.

[25] T. Gowri, N. Gayathri, R. P. Vasudeva, R. M. Zia, and L.-E. Aime
Efficient pairing-free identity-based ADS-B authentication scheme with batch verification
IEEE Trans. Aerosp. Electron. Syst., to be published, doi: 10.1109/TAES.2018.2890354.

[26] S. Krishna, P. Radha, S. Sudhakar, D. Terry, and R. Chuck
Future e-enabled aircraft communications and security: The next 20 years and beyond
Proc. IEEE, vol. 99, no. 11, pp. 2040–2055, Nov. 2011.

[27] D. McCallie, J. Butts, and R. Mills
Security analysis of the ADS-B implementation in the next generation air transportation system
Int. J. Crit. Infrastructure Protection, vol. 4, pp. 78–87, Aug. 2011.

[28] A. Shamir
Identity based cryptosystems and signature schemes
Adv. Cryptology-Crypto, Lecture Notes in Computer Science, Springer-Verlag, vol. 196, pp. 47–53, 1984.

[29] S. S. Al-Riyami and K. G. Paterson
Certificateless public key cryptography
In *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2003, pp. 452–473.

[30] R. Tso, X. Yi, and X. Huang
Efficient and short certificateless signature
In *Proc. Int. Conf. Cryptol. Netw. Secur.*, 2008, vol. 5339, pp. 64–79.

[31] *Minimum Operational Performance Standards for 1090 MHz Extended Squitter: Automatic Dependent Surveillance-Broadcast (ADS-B) and Traffic Information Services-Broadcast (TIS-B)/RTCA*, SC-186, 2006.

[32] EUROCONTROL/FAA, Communications Operating Concept and Requirements for the Future Radio System (COCR), pp. 90–93. [Online]. Available: https://www.eurocontrol.int/sites/default/files/field_tabs/content/documents/communications/cocr-future-radio-system-v.2.pdf

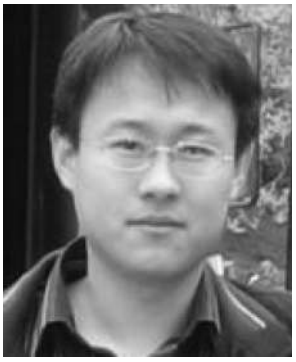
[33] R. Barhydt, M. T. Palmer, W. W. Chung, and G. W. Loveness
ADS-B within a multi-aircraft simulation for distributed air-ground traffic management
In *Proc. 23rd Digit. Avionics Syst. Conf.*, 2004, vol. 1, pp. 490–531.

Zhijun Wu received the B.S. and M.S. degrees in information processing from Xidian University, Xi'an, China, in 1988 and 1996, respectively, and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, Beijing, China, in 2004.

He was a Professor with the Department of Communication Engineering, Civil Aviation University of China. His research interests include denial-of-service attacks, security in ADS-B system, and BeiDou navigation satellite system.

Anxin Guo received the B.S. degree in electronic information engineering from Zhengzhou University of Light Industry, Zhengzhou, China, in 2015, and the M.S. degree in information security from the Civil Aviation University of China, Tianjin, China, in 2019.

His research interests include information security.



Meng Yue received the B.S. degree in electronic information engineering from the Hebei University of Science and Technology, Shijiazhuang, China, in 2006, and the M.S. degree in information security from the Civil Aviation University of China, Tianjin, China, in 2009.

He is currently an Associate Professor with the Department of Communication Engineering, Civil Aviation University of China. His research interests include denial-of-service attacks.

Liang Liu received the B.S. degree in communication engineering from the Harbin Institute of Technology, Harbin, China, in 2015, and the M.S. degree in information security from the Civil Aviation University of China, Tianjin, China, in 2018.

He is currently a Technician with the Department of Communication Engineering, Civil Aviation University of China. His research interests include denial-of-service attacks, system wide information management, and future networks.