An Efficient Broadcast Authentication Scheme with Batch Verification for ADS-B Messages

Haomiao Yang [1], Hyunsung Kim [2], Hongwei Li [1], Eunjun Yoon [2], Xiaofen Wang [1] and Xuefeng Ding [3]

[1] School of Computer Science & Engineering, UESTC
Chengdu, 610054 - China
[e-mail: haomyang@uestc.edu.cn, hongwei.uestc@gmail.com, wangxuedou@sina.com]
[2] Dept. of Cyber Security, Kyungil University
Kyungsansi, 712-701 - Republic of Korea
[e-mail: kim@kiu.ac.kr, ejyoon@kiu.ac.kr]
[3] Information Management Center, Sichuan University
Chengdu, 610041 - China
[e-mail: 65576387@qq.com]
*Corresponding author: Xuefeng Ding

Received June 3, 2013; revised August 27, 2013; accepted September 21, 2013; published October 29, 2013

Abstract

As a cornerstone of the next generation air traffic management (ATM), automatic dependent surveillance-broadcast (ADS-B) system can provide continual broadcast of aircraft position, identity, velocity and other messages over unencrypted data links to generate a common situational awareness picture for ATM. However, since ADS-B messages are unauthenticated, it is easy to insert fake aircrafts into the system via spoofing or insertion of false messages. Unfortunately, the authentication for ADS-B messages has not yet been well studied. In this paper, we propose an efficient broadcast authentication scheme with batch verification for ADS-B messages which employs an identity-based signature (IBS). Security analysis indicates that our scheme can achieve integrity and authenticity of ADS-B messages, batch verification, and resilience to key leakage. Performance evaluation demonstrates that our scheme is computationally efficient for the typical avionics devices with limited resources, and it has low communication overhead well suitable for low-bandwidth ADS-B data link.

Keywords: ADS-B, broadcast authentication, identity-based signature, batch verification, key evolution

This work is supported by the National Natural Science Foundation of China under Grants U1233108 and 61103207, the 2011 Korea-China Young Scientist Exchange Program, the Fundamental Research Funds for Chinese Central Universities under Grant ZYGX2011J059, the Research Funds for Science &Technology Department of Sichuan Province under Grant 2012GZ0024, the Shanghai Science and Technology Committee under Grant 11511505300, and the National Research Foundation of Korea Grant funded by the Korea Government (MEST) (NRF-2010-0021575).

http://dx.doi.org/10.3837/tiis.2013.10.013

1. Introduction

ADS-B is a surveillance system for ATM, which is intended to replace traditional radar systems to become a cornerstone of the next generation ATM. The idea of ADS-B can be summarized as follows: ADS-B avionics periodically broadcast the satellite-based aircraft position, identification, capability, etc. Furthermore, with availability of ADS-B messages, ground stations or aircrafts can monitor and track the location and path of flight [1]. However, ADS-B signals over radio data links are not authenticated, and thus it is easy to spoof fake aircrafts into ADS-B system by transmitting signals on ADS-B frequencies [2]. Therefore, ADS-B data spoofing becomes a severe potential threat to safety of air traffic, and the critical ATM tasks depend on the integrity of ADS-B data delivered over a shared data link.

Although the spoofing threat can be alleviated with some traditional aviation surveillance technologies, the existing solutions cannot directly apply to preservation of ADS-B data integrity. For instance, secondary surveillance radars can serve to verify integrity of ADS-B messages if the filtered fake targets are not too many. However, as early as 2006, concerns were raised about the ability of hackers to introduce as many as 50 false targets onto controllers' radar screens, which is beyond the processing capability of common radars [3].

Cryptography can protect ADS-B data link against spoofing. Unfortunately, simply using encryption to prevent ADS-B data spoofing is not applicable, because the encrypted broadcast messages could not be decoded correctly by the public, and this would also violate the original openness intention of ADS-B system design. As we know, encryption changes messages, while authentication does not change messages (only append authentication data). Hence, if authentication method is used, the message is sent in the clear for view by all participants, but the message authentication code (MAC) or the digital signature is appended to the message to provide authentication for those participants for which security is important. Therefore, authentication is introduced to prevent ADS-B data from being spoofed. The key benefit is that whether you are checking the authentication or not, the data can be seen by all participants and thus the fundamental openness of ADS-B system is maintained.

Despite the importance of ADS-B broadcast authentication, it has not been well researched in civil aviation due to unique properties of aviation communications. For example, TESLA is widely known as a lightweight broadcast authentication scheme [4], but it could not directly apply to authentication of ADS-B messages since TESLA may not play well for authenticity of emergency broadcast due to the heavy dependence on time delay.

Recently, Sampigethaya et al. first considered cryptographic solutions for authenticity of ADS-B messages [5-6]. However their solutions, either require pre-shared secret between aircraft and air traffic controller, or require availability of public key infrastructure (PKI), which may pose scalability and cost-benefit challenges for ATM systems. Hence, their solutions are not suitable for the low-bandwidth and not well-connected ADS-B data links.

Therefore, in this paper, we will tackle the problem, i.e., how to enable efficient broadcast authentication. The IBS crypto-primitive provides an alternative solution for the problem [7]. The advantage of IBS is that the user's public key can be directly derived from the identity string so that PKI is not necessary. In addition, such system needs a trusted authority called the private key generator (PKG) whose task is to extract user's private key from user's identity information. Therefore, when IBS is applied to broadcast authentication for ADS-B messages, its advantages are as follows. On one hand, a broadcaster attaches an IBS to every piece of

ADS-B messages by use of her private key, where the signature enables recipients to detect the falsification or corruption by verifying it. On the other hand, IBS can simplify key management and distribution, compared with the traditional certificate-based signature.

However, direct application of IBS to broadcast authentication of ADS-B messages would not be necessarily suitable, as IBS is developed as crypto-primitive and cannot accommodate such high service-level requirements of security and efficiency, considering unique properties of aviation communications. Especially, there are two issues to be considered: (i) The side-channel attack poses significant threats to ADS-B space communications by exploiting various forms of unintended key information leakage (e.g., electromagnetic radiation) [8], where an adversary observing information leakage from computation on the key can potentially accumulate enough data over time to compromise the security of IBS scheme. (ii) Generally, a broadcaster verifies each signature individually. When the arrival rate of signatures is high (e.g. in taking off or landing), a scalability problem emerges immediately, where the recipient has much less time to verify each received signature, especially for that the verification of the IBS signature involves costly pairing operations.

As above, we discuss the primitive of IBS and its pros and cons. Then, we show how we can adapt it to suit our purpose briefly. On one hand, we use batch verification technique to decrease the computational cost of verification where each recipient can simultaneously verify multiple received signatures. On the other hand, we adapt key evolving technique to reduce damage caused by private key exposure in which time is divided into distinct periods 1,…, N and private keys evolve over time.

Our Contributions. In this paper, we study aforementioned points and our contributions can be summarized as follows:

- Firstly, we propose an efficient broadcast authentication scheme with batch verification for ADS-B messages by modifying the Kurosawa-Heng IBS scheme [9]. The security analysis demonstrates that our scheme can achieve integrity and authenticity of ADS-B messages, batch verification, and resilience to key leakage.
- Secondly, we compare our scheme with existing schemes in [10] and [11] which also achieve batch verification. The comparison results show that our scheme is more efficient in terms of computation and communication overheads. Therefore, it is more suitable for ADS-B data link communication.

Organization. The rest of the paper is organized as follows: we review the related works in Section 2. Section 3 gives system and threat models, design goals, notations, and preliminaries. Then, we propose an broadcast authentication scheme with batch verification based on IBS in Section 4. The security analysis and performance evaluation are given in Section 5 and Section 6, respectively. Finally, Section 7 gives the concluding remark of the paper.

2. Related Work

To provide integrity and authenticity of ADS-B messages, cryptography can be used in ADS-B data communications. Sampigethaya et al. first considered possible cryptographic solutions for authentication of ADS-B messages [5-6], either by using symmetric-key encryptions or digital signatures. Following their ideas, two authentication schemes are proposed respectively. At CSQRWC 2012, Chen proposed a data link authenticated

encryption scheme based on symmetric block ciphers [12]. However, the difficulty in this scheme is the distribution of symmetric keys, because ADS-B system is not a well-connected network and the keys cannot be well distributed in real time. In addition, encrypting ADS-B messages conflicts with the openness of ADS-B design. Also in 2012, Pan et al. provided an ADS-B data authentication scheme based on the elliptic curve data signature algorithm (ECDSA) and X.509 public certificates [11]. However the traditional certificate-based signature requires expensive communication and computation costs for certificate transmission and verification, and thus it is not suitable for low-bandwidth ADS-B communications.

As introduced above, IBS with batch verification provides an alternative solution for efficient broadcast authentication of ADS-B messages. Instead of verifying the signature for one message every time, the batch verification authenticates multiple messages one time. In this way, the cost of verification is amortized over multiple messages.

Although several IBS schemes have been proposed, batch verifications for these schemes have some weaknesses either in efficiency or in security, and thus they are not suitable for ADS-B broadcast authentication [10, 13-14]. For exmaple, the batch verification in [10] is not efficient, since it needs n+1 expensive pairing operations for n messages. And the batch verification in [13] is not secure, since an adversary can forge signatures which pass the batch verification with the honest user. Additionally, the security of batch verification in [14] depends heavily on the random oracle model which is only an ideal model and not essentially secure in the reality world.

In this paper, our broadcast authentication scheme is based on the Kurosawa-Heng IBS scheme [9], where the security could be proved without random oracles and the verification for the signature only uses one pairing (Kurosawa-Heng only proposed an identity-based identification scheme, and we can derive the corresponding IBS scheme using the Fiat-Shamir heuristic [15]). Furthermore, we can properly modify it to develop an efficient broadcast authentication scheme with batch verification for ADS-B messages for our purpose.

3. Problem Statement

In this section, we give the problem statement, including system and threat models, design goals, notations, and preliminaries

3.1 System and Threat Models

As shown in **Fig. 1**, each aircraft is equipped with the global position system (GPS) as a primary information source for navigation. Aircrafts move in airspace with sharing information as well as communicating with ADS-B ground stations. Moreover, each aircraft periodically broadcasts traffic beacons by using the ADS-B-Out capability, once or twice per second. Ground stations and aircrafts of one communication hop away use the ADS-B-In capability for the ground surveillance and airborne surveillance. On the other hand, ADS-B data link standards mainly include the universal access transceiver (UAT) and the 1090 MHz Extended Squitters (1090 ES) [16-17]. Since 1090 ES is highly congested, due to its current use by the air traffic control radar beacon system [18], this paper only considers authentication of ADS-B messages upon the UAT data link. Additionally, each aircraft possesses a globally coordinated permanent unique digital identifier, such as the 24-bit international civil aviation organization address, which can be considered as the unique identity in the identity-based setting of our broadcast authentication scheme.

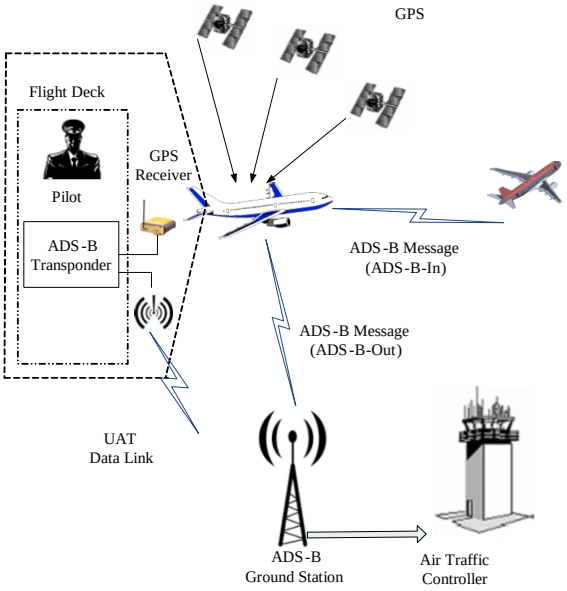


Fig. 1. System Model

Since ADS-B data link is a broadcast-type shared link and messages are broadcasted in the form of plaintexts, they are vulnerable in all kinds of attacks. McCallie et al. summarized six main ways for attackers to harm ADS-B system, ranging from relatively easy disruptions using jamming equipment to more difficult target ghost inject (spoofing) to flood denial [19]. This paper mainly focuses on how to provide authenticity of ADS-B broadcast messages. Therefore in this paper, we only consider that the adversary is capable of launching active adversarial threats such as spoofing false target aircraft or corruption of traffic data. Here, we do not consider attacks of passive eavesdropping and recording all broadcasts. Also, we consider communication jamming threats not to directly threaten authenticity.

Additionally, side-channel attacks expose crucial vulnerabilities to ADS-B broadcast authentication scheme by exploiting various forms of unintended key information leakage (e.g., emitted radiation) [8]. Especially, we consider that exposure of private keys in cryptographic mechanisms (e.g., digital signature) is the greatest harm to users and means that all security goals are entirely lost. In this paper, the key evolving technique is adopted to reduce damage caused by private key exposure.

3.2 Design Goals

For the broadcast authentication of ADS-B messages, we consider the following required features needed to be satisfied.

- Authenticity and integrity of ADS-B messages: To cope with active adversarial threats such as insertion of false targets or corruption of traffic data, authenticity and integrity of ADS-B broadcast messages should be preserved, i.e., the transmitted messages are really sent by legitimate ADS-B-equipped aircrafts or ground stations, and have not been forged or modified during the communication.
- Resilience to key leakage: To preserve resilience to key leakage, the indepence of private key evolving should be achieved, i.e., if an adversary $\mathcal{A}$ compromises any previous private key of a broadcaster, $\mathcal{A}$ cannot use it currently or in the future.

- Low cost of communication: The communication cost should be low, becasue the available ADS-B-Out data space is small and limited in UAT data link.
- Low cost of computation: The computation cost should be low, because participants are usually avionics devices with limited resources.

3.3 Notations and Preliminaries

In this subsection, we introduce notations (**Table 1**) used throughout the remainder of this paper and review bilinear maps and UAT ADS-B message structures.

Table 1. Notations

Notation	Meaning
λ	Security Parameter
G_1, G_2, G_T	Cyclic groups of the same order q
P, Q	Generators of G_1, G_2, respectively
g	Value of $\hat{e}(P, Q)$
$\hat{e}: G_1 \times G_2 \to G_T$	Admissible bilinear map
$H_1: \{0,1\}^* \to \mathbb{Z}_q^*$	Cryptographic one-way hash function
$H_2: \{0,1\}^* \times G_T \to \mathbb{Z}_q^*$	Cryptographic one-way hash function
N	Number of periods for private key evolving
T	Length of each period
$\|\|$	Concatenation operator
$\|\cdot\|$	Bit length of a message

Firstly, we briefly recall bilinear maps as in [20]. Let G_1 and G_2 be two additive groups, and G_T be a multiplicative group of the same prime order q. Let P be a generator of G_1, Q be a generator of G_2, and ψ be an efficiently computable isomorphism from G_2 to G_1, with $\psi(Q) = P$. An admissible bilinear map is a map $\hat{e}: G_1 \times G_2 \to G_T$ with the following properties: (i) Bilinearity: for all $U \in G_1, V \in G_2$ and $a, b \in \mathbb{Z}_q^*$, $\hat{e}(aU, bV) = \hat{e}(U, V)^{ab}$; (ii) Non-degeneracy: $\hat{e}(P, Q) \neq 1_{G_T}$; (iii) Computability: $\hat{e}$ can be computed efficiently.

Definition 1. An asymmetric bilinear parameter generator $\mathcal{G}(\lambda)$ is a probabilistic algorithm that takes a security parameter $\lambda \in \mathbb{Z}^+$ as input, and outputs a 7-tuple $(q, P, Q, G_1, G_2, G_T, \hat{e})$ where q is a λ-bit prime number, G_1, G_2, and G_T are three cyclic groups of the same order q with $G_1 \neq G_2$, P is a generator of G_1, Q is a generator of G_2, and $\hat{e}: G_1 \times G_2 \to G_T$ is an admissible bilinear map.

Then, we give a brief overview of UAT ADS-B message structures [16], which give a conceptual illustration of the payload structures of the two defined types of UAT ADS-B messages, namely the basic ADS-B message and the long ADS-B messages. All UAT ADS-B messages include a message header (HDR), which provides one way to correlate different messages received from a given aircraft. The HDR also contains a five-bit field to indicate the type of information provided in the message. This enables designation of up to 32 different payload types (labeled from 0 to 31), which are shown parenthetically in **Fig. 2**. Note that in our scheme, we use the ADS-B message of Type 30 to accommodate the signature data.

Basic ADS-B Message

(0*) HDR	STATE VECTOR

Long ADS-B Messages

(1-6) HDR	STATE VECTOR	Mode Status/Intent Data
(7-10) HDR	STATE VECTOR	Reserved
(11-29) HDR	Reserved for Future Definition	
(30, 31) HDR	Reserved for Developmental/Experimental Use	

*Payload type codes are part of HDR and are indicated in parentheses.

Fig. 2. UAT ADS-B Message Structures

4. Proposed Scheme

In this section, we propose a broadcast authentication scheme with batch verification for ADS-B messages. To begin with, the main ideas and ADS-B-Out data format of our scheme are given in subsection 4.1 and 4.2, respectively.

4.1 Main Ideas

Fig. 3 shows the main ideas of our scheme. A broadcaster B with the identity ID_B attaches an IBS signature (r, S) to the ADS-B messages m by use of her private key S_{ID_B}. This allows recipients to easily verify integrity and authenticity of received messages. Note that the message is sent in the clear for view by all participants, but the IBS signature is appended to the message to provide authentication for those participants for which security is important and who have the desire to verify authenticity. Consequently, whether you are checking authentication or not, the broadcast messages can be seen by all participants and thus our scheme is compatible with the openness of ADS-B system.

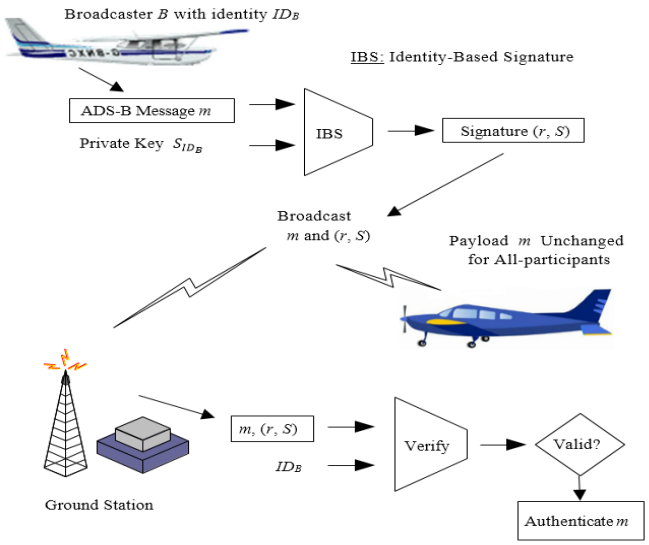
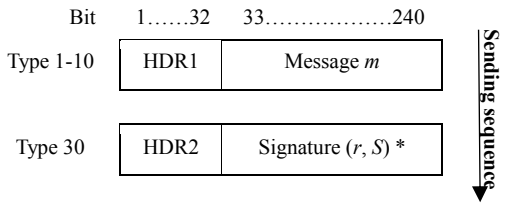


Fig. 3. Main Ideas

4.2 ADS-B-Out Data Format

In this subsection, we illustrate the encapsulated data format and package sending sequence in **Fig. 4**. First of all, considering the typical data block size of payload in UAT, there are only 272 bits of data space left, in which with the 32-bit HDR there is only 240-bit data space that can be used as the payload [16]. As shown in **Fig. 2**, Type 30 is defined to accommodate the IBS signature data. It is transmitted after any other original ADS-B data types. Therefore, our scheme does not change the ADS-B data of original types (Type 1-10), but only append IBS signatures of Type 30. Additionally, to prevent from replay attack, timestamps or random numbers can be appended into the messages as usual. Here we omit the details. Interested readers are referred to [11].



* Type 30 is defined to accommodate the signature data (r, S).

Fig. 4. UAT Data Composition of New Type 30

4.3 Phases of Proposed Scheme

The scheme consists of the following five phases: *System Initialization*, *Broadcaster Registration*, *Message Broadcast*, *Signature Verification and Batch Verification*, and *Private Key Evolution*.

(1) *System Initialization*

The air traffic controller can act as PKG to set up all parameters as follows.

- *Step-1:* Given the security parameter λ, runs $\mathcal{G}(\lambda)$ to generate a 7-tuple $(q, P, Q, G_1, G_2, G_T, \hat{e})$.
- *Step-2:* Chooses a random $b \in \mathbb{Z}_q^*$, keeps it as the system master key secretly, and computes $Q_{Pub} = bQ$ and $g = \hat{e}(P, Q)$.
- *Step-3:* Chooses two secure cryptographic one-way hash functions $H_1: \{0,1\}^* \to \mathbb{Z}_q^*$ and $H_2: \{0,1\}^* \times G_T \to \mathbb{Z}_q^*$.
- *Step-4:* Publishes the public parameters as

$$\{q, P, Q, G_1, G_2, G_T, \hat{e}, Q_{Pub}, g, H_1, H_2\} \tag{1}$$

(2) *Broadcaster Registration*

When a broadcaster B registers her identity ID_B to the system, PKG works as follows.

- *Step-1:* Checks if ID_B is valid.
- *Step-2:* Computes the private key S_{ID_B} of ID_B as

$$S_{ID_B} = \left(b + H_1(ID_B)\right)^{-1} P \tag{2}$$

- *Step-3:* Sends S_{ID_B} to B through a secure channel.

Remark 1. Assume that the secure channel for transmitting the private key can be properly established via additional cryptographic tools such as wired or wireless secure socket layer protocol, as suggested in [21].

(3) *Message Broadcast*

A broadcaster B with the private key S_{ID_B} signs a message $m \in \{0,1\}^*$ and broadcasts it as follows.

- *Step-1:* Chooses a random $k \in \mathbb{Z}_q^*$ and computes

$$r = \hat{e}(P, Q_{Pub} + H_1(ID_B)Q)^k \tag{3}$$

- *Step-2:* Sets

$$h = H_2(m, r) \tag{4}$$

- *Step-3:* Computes

$$S = kP + hS_{ID_B} \tag{5}$$

- *Step-4:* Broadcasts the signature (r, S) through ADS-B data link.

Remark 2. Note that $\hat{e}(P, Q_{Pub} + H_1(ID_B)Q)$ can be pre-computed by the broadcaster B.

(4) *Signature Verification and Batch Verification*

Upon the receipt of a signature (r, S) of a message m from the broadcaster B, each recipient verifies it as follows.

- *Step-1:* Sets

$$h = H_2(m, r) \tag{6}$$

- *Step-2:* Checks if

$$rg^h = \hat{e}(S, Q_{Pub} + H_1(ID_B)Q) \tag{7}$$

If it holds, then the recipient accepts the signature and outputs **true**. Otherwise, the recipient outputs **false**.

When a recipient receives ADS-B broadcast messages from different aircrafts at the same time, the recipient can verify the signatures of the messages in a batch manner. Given l tuples (ID_1, m_1, r_1, S_1), $\cdots$, (ID_l, m_l, r_l, S_l), we can perform batch verification as follows:

- *Step-1:* Sets for all $i = 1, \cdots, l$.

$$h_i = H_2(m_i, r_i) \tag{8}$$

- *Step-2:* Checks if

$$\left(\prod_{i=1}^{l} r_i\right)\left(g^{\sum_{i=1}^{l} h_i}\right) = \hat{e}\left(\sum_{i=1}^{l} S_i, Q_{Pub}\right)\hat{e}\left(\sum_{i=1}^{l} H_1(ID_i)S_i, Q\right) \tag{9}$$

If it holds, then the recipient accepts all signatures and outputs **true**. Otherwise, the recipient outputs **false**.

Remark 3. From the above batch verification, the computation cost that the recipient spends on verifying n signatures is dominantly comprised of n point multiplications and 2 pairing operations. Therefore, the time for a recipient to verify a large number of signatures from multiple broadcasters can be dramatically reduced.

(5) *Private Key Evolving*

To reduce the damage caused by private key exposure, the lifetime of the proposed scheme is divided into N distinct time periods: $1, \cdots, N$ (the time periods are of the same length T, e.g. one day). The private key evolving can be performed by the following steps:

- *Step-1:* At the end of period i, the broadcaster B sends a request for the private key of next period through a secure channel.
- *Step-2:* After receiving the request, PKG checks the validity of B. If B is still a legitimate user, then PKG generates the private key of period $i+1$ as

$$S_{ID_B \| i+1} = \left(b + H_1\left(ID_B \| (d + (i+1) * T)\right)\right)^{-1} P \tag{11}$$

, where d is the initial date and T is the length of the period.

- *Step-3:* PKG sends $S_{ID_B \| i+1}$ back to B through a secure channel.

Remark 4. If B is not yet a legitimate user, no new private key is issued by PKG and the old one is automatically revoked.

5. Security Analysis

In this section, we give the security analysis of the proposed scheme.

5.1 Correctness of Verification and Batch Verification

The correctness of verification and batch verification can be illustrated in the following two theorems, respectively.

Theorem 1. *The verification for the broadcast message is correct.*

Proof. The correctness of the verification in Eq. (7) is justified as follows. For simplicity, we denote $Q_{Pub}+H_1(ID_B)Q$ by Q_{ID_B}.

Firstly, we have

$$\begin{aligned}
&\hat{e}(P,Q)^h = \hat{e}\left(h\left(b + H_1(ID_B)\right)^{-1} P, \left(b + H_1(ID_B)\right)Q\right) \\
&= \hat{e}\left(h\left(b + H_1(ID_B)\right)^{-1} P, Q_{Pub}+H_1(ID_B)Q\right) \\
&= \hat{e}\left(hS_{ID_B}, Q_{ID_B}\right).
\end{aligned}$$

Then, we have

$$\begin{aligned}
&\hat{e}\left(kP, Q_{ID_B}\right)\hat{e}(P,Q)^h = \hat{e}\left(kP, Q_{ID_B}\right)\hat{e}\left(hS_{ID_B}, Q_{ID_B}\right) \\
&\Rightarrow \hat{e}\left(P, Q_{ID_B}\right)^k \hat{e}(P,Q)^h = \hat{e}\left(kP + hS_{ID_B}, Q_{ID_B}\right) \\
&\Rightarrow rg^h = \hat{e}\left(S, Q_{ID_B}\right) \\
&\Rightarrow rg^h = \hat{e}\left(S, Q_{Pub}+H_1(ID_B)Q\right).
\end{aligned}$$

Theorem 2. *The batch verification for the broadcast messages is correct.*

Proof. The correctness of the batch verification in Eq. (9) is justified as follows.

$$
\begin{aligned}
&\hat{e}\left(\sum_{i=1}^{l} S_i, Q_{Pub}\right)\hat{e}\left(\sum_{i=1}^{l} H_1(ID_i)S_i, Q\right)\\
&= \hat{e}\left(\sum_{i=1}^{l} S_i, bQ\right)\hat{e}\left(\sum_{i=1}^{l} H_1(ID_i)S_i, Q\right)\\
&= \hat{e}\left(\sum_{i=1}^{l} bS_i, Q\right)\hat{e}\left(\sum_{i=1}^{l} H_1(ID_i)S_i, Q\right)\\
&= \hat{e}\left(\sum_{i=1}^{l} \left(b + H_1(ID_i)\right)S_i, Q\right)\\
&= \hat{e}\left(\sum_{i=1}^{l} \left(b + H_1(ID_i)\right)\left(k_iP + h_iS_{ID_i}\right), Q\right)\\
&= \hat{e}\left(\sum_{i=1}^{l} \left(b + H_1(ID_i)\right)(k_iP), Q\right)\hat{e}\left(\sum_{i=1}^{l} \left(b + H_1(ID_i)\right)\left(h_iS_{ID_i}\right), Q\right)\\
&= \left(\prod_{i=1}^{l} \hat{e}\left(\left(b + H_1(ID_i)\right)(k_iP), Q\right)\right)\left(\prod_{i=1}^{l} \hat{e}\left(\left(b + H_1(ID_i)\right)(S_{ID_i}), h_iQ\right)\right)\\
&= \left(\prod_{i=1}^{l} \hat{e}\left((k_iP), \left(b + H_1(ID_i)\right)Q\right)\right)\left(\prod_{i=1}^{l} \hat{e}(P, h_iQ)\right)\\
&= \left(\prod_{i=1}^{l} \left(\hat{e}\left(P, Q_{Pub} + H_1(ID_i)Q\right)\right)^{k_i}\right)\left(\prod_{i=1}^{l} \left(\hat{e}(P, Q)\right)^{h_i}\right)\\
&= \left(\prod_{i=1}^{l} r_i\right)\left(g^{\sum_{i=1}^{l} h_i}\right).
\end{aligned}
$$

5.2 Authenticity and Integrity of ADS-B messages

In the proposed scheme, the authentication for ADS-B messages is implemented with IBS. Hence, the security of our scheme is based on the underlined Kurosawa-Heng IBS scheme [9]. As we know, the Kurosawa-Heng IBS scheme is existentially unforgeable under chosen-message attacks without random oracles. As a result, authenticity and integrity of ADS-B messages can be achieved in the proposed scheme.

5.3 Resilience to Key Leakage

In *Private Key Evolving* phase, the broadcaster B firstly sends a request for the private key of next period through secure channel. Then PKG generates $S_{ID_B\|i+1}$ and further sends it back to B through secure channel. Thus, even if an adversary $\mathcal{A}$ eavesdrops the communication between B and PKG, she cannot get any information about $S_{ID_B\|i+1}$. On the other hand, even if an adversary $\mathcal{A}$ compromises any previous private key, she cannot deduce current or future private keys since the discrete logarithm problem ensures the private keys' security [21]. Therefore, the key resilience for the leakage of broadcasters' private keys can be achieved in the proposed scheme.

Finally, we present the comparison of the functionalities in **Table 2**, where a checkmark "√" signals that a functionality is present.

Table 2. Functionalities Comparison

Functionality	Pan et al. [11]	Chen [12]	Ours
ADS-B Authentication	√	√	√
Without Certificate		√	√
Without Encryption	√		√
Without Random Oracle			√
Batch Verification			√
Key Evolution			√

6. Performance Evaluation

In this section, we evaluate the performance of the proposed scheme in terms of computation cost and communication overhead.

As shown in **Fig. 1,** ADS-B broadcast messages from an aircraft are received either by the ground stations or by other aircrafts. Generally, the ground stations have powerful processing capacity and large storage capability, but aircrafts have just limited computation power and little storage space due to the limitation of the avionics size. Hence, the computation cost of the authentication is very important for the aircrafts with limited resources. As a result, in the following, the evaluation of the performance is focused on the aircrafts.

6.1 Computation Time of Our Scheme

Regarding the computation cost, we focused on the running time simulation for each phase of our scheme. Firstly, experiments were conducted on ARMv7 rev2 microprocessor with adjustable frequencies from 200MHz to 1440MHz and memory with 240M RAM to study the running time. Then, we used MIRACL cryptographic library (version 5.6.1) to implement these operations, where for AES-128 security, *R*-ate pairing on Barreto-Naehrig curve (embedding degree k=12) with 1-2-4-12 tower of extensions is used [22-23]. The performances of these operations are summarized in **Table 3** where we denote the average running time of *System Initialization*, *Broadcaster Registration*, *Message Broadcast*, *Signature Verification*, and *Private Key Evolution* by T_{Init}, T_{Reg}, T_{Sig}, T_{Vrf} and T_{Evol}, respectively. As shown in **Table 3**, for the typical setting, each phase operation of the proposed scheme is very efficient. Hence, our scheme is well suitable for the avionics devices with limited resources in practice.

Table 3. Computation Time of Our Scheme

CPU Frequency	T_{Init} (ms)	T_{Reg}(ms)	T_{Sig}(ms)	T_{Vrf}(ms)	T_{Evol}(ms)
200 MHz	654.2526	44.5630	89.1269	613.2895	48.1207
400 MHz	306.1514	21.5168	43.0336	291.6227	23.9273
800 MHz	149.2435	10.0965	20.1931	143.4164	11.4224
1,000 MHz	119.8140	7.9800	15.9600	121.8339	8.2105
1,440 MHz	84.9613	6.3856	12.7712	80.4850	6.6139

Remark 5. In an ATM system, the operations could be performed by powerful computer. However, in an aircraft, due to the limitation of the avionics size, the operations could be performed by an ARM based computer with limited resources.

6.2 Comparison of Verification Delay

Here, we denote a pairing operation, an elliptic curve scalar multiplication in G_1, and a map-to-point hash function $H: \{0,1\}^* \rightarrow G_1$ by Pa, M and H, respectively. Other operations are negligible, compared with the ones mentioned above. Note that in our scheme, the running time of $H_1: \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and $H_2: \{0,1\}^* \times G_T \rightarrow \mathbb{Z}_q^*$ could be negligible, compared to the running time of Pa, M and H.

Next, we compare the proposed scheme with YCK in [10] in terms of the verification delay. We also include ECDSA in the comparison as a criterion [24], which is the signature algorithm adopted in [11]. **Table 4** shows the combination of the dominant operations of the three schemes in terms of verifying a single signature and n signatures, respectively. From the batch verification in Eq. (9), we observe that the computation cost to verify n distinct signatures is $2Pa+nM$. According to [10], with YCK, the computation cost spent on verifying n signatures is equal to $(n+1)Pa+nM+nH$; while with the ECDSA, verifying distinct n signatures requires $2nM$. Since ECDSA is not identity-based, additional operations are needed to verify the public key's certificate. Thus, the overall message verification cost for ECDSA should be doubled.

Table 4. Comparison of Verification Delay

Scheme	Verify a single signature	Verify n signatures ($n > 1$)
Ours	$1Pa+1M$	$2Pa+nM$
YCK **[10]**	$1Pa+1M+1H$	$(n+1)Pa+nM+nH$
ECDSA **[24]**	$4M$	$4nM$

The verification delay of a recipient against the number of the received messages is plotted in **Fig. 5**. In this experiment, the recipient side programs have been implemented as **Table 3** in a 1440-MHz ARM processor. The running time for Pa, M and H are 72.1901 ms, 6.3856 ms and 8.2388 ms, respectively. As shown in **Fig. 5**, we can observe that the verification delay by using YCK is always the largest no matter how many messages are received by a recipient. Another interesting result is that when the number of received messages is smaller than 8, the ECDSA scheme achieves the smallest message verification latency; however, when the number of messages is greater than 8, our scheme yields much less verification latency. **Fig. 5** also shows that within a 300-ms interval, the maximum number of signatures that can be verified by the recipient is equal to 3, 15, and 29 when the YCK, ECDSA, and our scheme are adopted, respectively. Obviously, our scheme can verify the largest number of signatures with the same resources than the others.

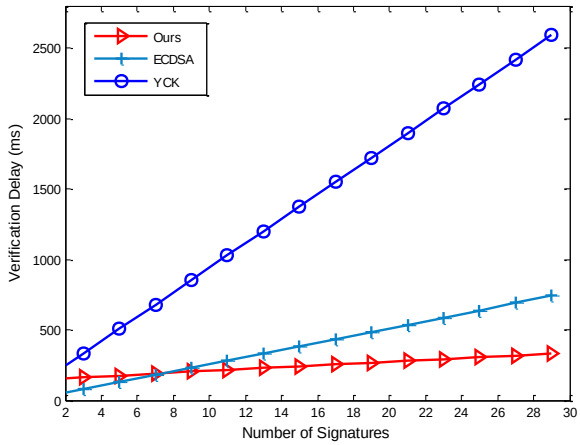


Fig. 5. Comparison of Verification Delay

6.3 Comparison of Communication Overhead

Then we compare the transmission overhead in ours and ECDSA which is adopted in [11]. For convenience, we consider the secure level of 1024-bit RSA signature as a criterion. Here, the transmission overhead includes a signature and a certificate (if necessary) appended to the original message, while the message itself is not counted.

In our scheme, the length of a signature is 1120 bits (140 bytes). This is because the total length of the signature in our scheme is $|G_1| + |G_T|$. And if the security level with 1024-bit RSA is required, then $|G_1| = 160$ and $|G_T| = 960$ by adopting 160-bit MNT curve [20]. The length for ECDSA is only 42 bytes. However, when we use ECDSA, a certificate must be transmitted along with a signature. If we use the certificate presented in IEEE 1609.2 Standard [24], which has 125 bytes in length, the total transmission overhead of ECDSA is 167 (42+125) bytes. **Fig. 6** plots the communication overhead with the number of messages. As shown, the total length in our scheme is smaller than that in ECDSA. Therefore, it is more suitable for low-bandwidth ADS-B data link communications.

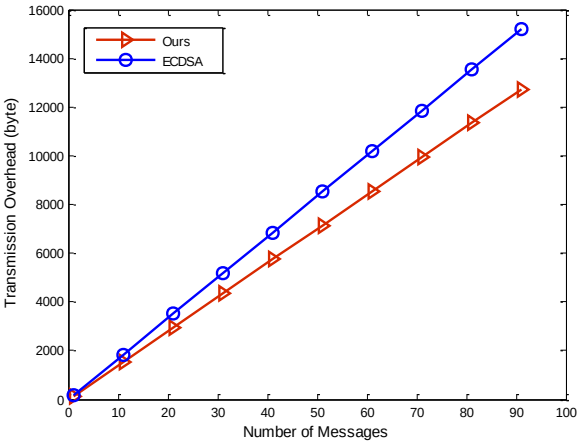


Fig. 6. Comparison of Communication Overhead

7. Conclusion

In this paper, we proposed an efficient broadcast authentication scheme with batch verification for ADS-B messages by modifying the Kurosawa-Heng IBS scheme. The security analysis demonstrates that our scheme can achieve integrity and authenticity of ADS-B messages, batch verification, and resilience to key leakage. The performance evaluation shows that the scheme is computationally efficient for the typical avionics devices with limited resources, and it has low communication overhead well suitable for low-bandwidth ADS-B data link. In the future work, we will explore other challenging security issues in ADS-B data link communications, such as the privacy concerns of the civil aviation aircraft and so on. In addition, we will design the simulation system to test the authentication for ADS-B communication.

References

[1] Federal Aviation Administration, "Automatic Dependent Surveillance Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service; OMB approval of information collection, 14 CFR Part 91," *Federal Register*, vol. 75, no. 154, August 11, 2011. http://www.faa.gov/airports/resources/advisory_circulars/index.cfm/go/document.current/documentNumber/150_5220-26

[2] J. Krozel, I. I. Dominick Andrisani, M. A. Ayoubi, T. Hoshizaki and C. Schwalm, "Aircraft ADS-B Data Integrity Check," in *Proc. of AIAA Aircraft Tech., Integration, and Operations Conf.*, Chicago, 2004. http://www.metronaviation.com/documents/publications/old/Aircraft_ADS-B_Data_Integrity_Check.pdf

[3] E. Valovage and D. Hall, "Enhanced ADS-B research," in *Proc. of IEEE Aerospace Conf.*, Big Sky, 2006. Article (CrossRef Link)

[4] A. Perrig, R. Canetti, J. D. Tygar and D. Song, "The TESLA broadcast authentication protocol," *CryptoBytes*, vol. 5, no.2, pp. 2-13, 2002. http://www.citeulike.org/user/mkhabbazian/article/1305474

[5] K. Sampigethaya and R. Pooverndran, "Privacy of future air traffic management broadcasts," in *Proc. of IEEE Digital Avionics Syst. Conf.*, pp. 6.A.1-1-6.A.1-11, October 2009. Article (CrossRef Link)

[6] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, "Future e-enabled aircraft communications and security: the next 20 years and beyond," in *Proc. of the IEEE*, vol. 99, no. 11, pp. 2040-2055, November 2011. Article (CrossRef Link)

[7] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Proc. of Crypto'84*, pp. 47-53, 1985. Article (CrossRef Link)

[8] F. X. Standaert, T. G. Malkin, and M. Yung. "A unified framework for the analysis of side-channel key recovery attacks," in *Proc. of Eurocrypt'09*. pp. 443-461, 2009. Article (CrossRef Link)

[9] K. Kurosawa and S. H. Heng, "Identity-based identification without random oracles," in *Proc. of ICCSA 2005*, pp. 603-613, 2005. Article (CrossRef Link)

[10] H. Yoon, J. H. Cheon and Y. Kim, "Batch verifications with ID-based signatures," in *Proc. of ICISC 2004*, pp.223-248, 2005. Article (CrossRef Link)

[11] W. Pan, Z. Feng and Y. Wang, "ADS-B Data Authentication Based on ECC and X. 509 Certificate," *Journal of Electronic Science and Technology*, vol. 10, no. 1, pp. 51-55, 2012. http://www.intl-jest.com/archives/2012/1/10/51-5564461.pdf

[12] T. Chen, "An authenticated encryption scheme for automatic dependent surveillance-broadcast data link," in *Proc. of Cross Strait Quad-Regional Radio Science and Wireless Technology Conference 2012*, pp. 127-131, 2012. Article (CrossRef Link)

[13] J. Cha and J. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," in *Proc. of*

PKC 2003, pp. 18-30, 2003. Article (CrossRef Link)
[14] P. S. Barreto, B. Libert, N. McCullagh and J. J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. of Asiacrypt'05*, pp. 515-532, 2005. Article (CrossRef Link)
[15] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. of Crypto'86*, pp. 186-94, 1986. Article (CrossRef Link)
[16] RTCA DO-282, "Minimum Operational Performance Standards for Universal Access Transceiver (UAT) automatic dependent surveillance – broadcast," 2002. http://infostore.saiglobal.com/store/Details.aspx?productID=1387876
[17] RTCA DO-260A, "Minimum Operational Performance Standard for 1090 MHz Extended Squitter ADS-B and TIS-B," 2002. http://infostore.saiglobal.com/store/Details.aspx?ProductID=1387875
[18] Federal Aviation Administration, *Aeronautical Information Manual*, Washington: Government Printing Office, 2012. http://www.faa.gov/air_traffic/publications/ATpubs/AIM/index.htm
[19] D. McCallie, J. Butts and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78-87, 2011. http://www.sciencedirect.com/science/article/pii/S1874548211000229
[20] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Proc. of Eurocrypt' 04*, pp. 56-73, 2004. Article (CrossRef Link)
[21] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. of Crypto'01*, pp. 213-229, 2001. Article (CrossRef Link)
[22] "MIRACL Crypto." https://certivox.com/solutions /miracl-crypto-sdk/
[23] E. Lee, H. Lee, C. Park, "Efficient and generalized pairing computation on abelian varieties," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1793-1803, 2009. Article (CrossRef Link)
[24] IEEE Standard 1609.2, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," 2006. http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=11000

Haomiao Yang, received his M.S. and Ph.D. degrees in Computer Applied Technology from University of Electronic Science and Technology of China (UESTC) in 2004 and 2008 respectively. He is an associate professor in Network Security Technology Laboratory in UESTC. Currently, he is doing post-doctoral research in the Research Center of Information Cross-over Security, Kyungil University, Republic of Korea. His research interests include cryptography, cloud security, and the cyber-security for aviation communications.

Hyunsung Kim received his M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2011 with the Department of Computer Engineering, Kyungil University. Currently, he is an associate professor at the Department of Cyber Security, Kyungil University, Republic of Korea. His current research interests are cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.

Hongwei Li received his M.S. degree in Computer Application from Southwest Jiaotong University (SWJTU) and Ph.D. degree in Computer Software and Theory from University of Electronic Science and Technology of China (UESTC) in 2004 and 2008 respectively. From 2011 to 2012, he worked as a Postdoctoral Fellow at University of Waterloo, Canada. Currently, he is an associate professor at the School of Computer Science and Engineering, UESTC, China. His research interests include cryptography, and the secure smart grid.

Eunjun Yoon received his M.S. degree in computer engineering from Kyungil University in 2002 and the Ph.D. degree in computer science from Kyungpook National University in 2006, Republic of Korea. From 2007 to 2008, he was a full-time lecturer at Faculty of Computer Information, Daegu Polytechnic College, Republic of Korea. He is currently an assistant professor the Department of Cyber Security, Kyungil University, Republic of Korea. His current research interests are cryptography, authentication technologies, smart card security, network security, mobile communications security, and steganography.

Xiaofen Wang, received her M.S. and Ph.D. degrees in Cryptography from Xidian University in 2006 and 2009 respectively. She is an instructor in Network Security Technology Laboratory in UESTC. Her research interests include pairing-based cryptography, authentication and key agreement protocols, signature schemes and privacy preserving protocols.

Xuefeng Ding received his M.S. degree in information security from Sichuan University in 2011. He is currently a teacher in Information Management Center of Sichuan University. His research interests include cryptography, broadcast authentication technologies, mobile communications security, and the cyber-security for aviation communications.