A Practical and Compatible Cryptographic Solution to ADS-B Security

Haomiao Yang, *Member, IEEE*, Qixian Zhou, Mingxuan Yao, Rongxing Lu, *Senior Member, IEEE*, Hongwei Li, *Member, IEEE*, and Xiaosong Zhang

***Abstract*—As the heart of next-generation air transportation systems, the automatic dependent surveillance-broadcast (ADS-B) is becoming a substitute for the radar, because it can enhance flight safety by requiring aircraft to regularly broadcast their precise geographic positions. Despite its promise, the lack of security mechanisms, e.g., not providing data encryption and message authentication, is a significant barrier to realistically deploy this new technology. While many methods have been proposed for ADS-B security, they can deal with either privacy or integrity unilaterally, and also need to change current ADS-B standards. In this paper, we present a new cryptographic solution to ADS-B security by first carefully exploiting some cryptographic primitives, and then adapting them to the air traffic-monitoring scenario. In contrast to previous approaches, our proposed solution is not only of high compatibility with existing protocols of ADS-B, but also lightweight for congested data links and resource-constraint avionics. Furthermore, it can also tolerate package loss and disorder that frequently occur in ADS-B wireless broadcast networks, making the proposed solution easy-to-deploy and practical. Security analysis shows that our proposal simultaneously achieves the confidentiality and authenticity of ADS-B messages. In addition, performance evaluation also demonstrates the efficiency of communication and computation for the proposal by using flight data of *OpenSky*–a sensor network that covers Central Europe aiming at gathering ADS-B flight data. Finally, the deployment in a real airport environment also proves the effectiveness of our solution.**

***Index Terms*—Air traffic control, automatic dependent surveillance-broadcast (ADS-B) communication, compatibility, privacy, security.**

I. Introduction

WITH the speeding-up of aviation modernization, automatic dependent surveillance-broadcast (ADS-B), as core of next-generation air transportation systems, has been rapidly replacing the antiquated secondary surveillance radar (SSR), and featured in requiring aircraft to broadcast periodically their geographic positions and velocities obtained from modern satellite-based navigation systems [2].

As the traditional SSR is deployed on the ground, it can merely detect aircraft within limited ranges. Consequently, there exist quite a little cases of aircraft disappearance at sea, e.g., Malaysia Airlines Flight 370 [3], due to the aircraft beyond the radar coverage. Different from the traditional SSR, the modern ADS-B surveillance technology, acquiring precise geographical locations from the global satellite-navigation-based system, is capable of extending surveillance range and enhancing situational awareness, thus it can considerably improve the flight safety. According to [4] and [5], ADS-B has been mandated in airspaces of U.S. and Europe by 2020.

Despite its promise, this critical aviation technology, surprisingly, did not take the security into account when being designed, rendering the ADS-B system vulnerable to a large number of attacks, because ADS-B messages are all clearly sent over wireless broadcast channels. For example, a mobile APP *Plane Finder AR* can provide real-time flight information for any given aircraft, including heading, call-sign, and so on. The hacker Haines, at Black Hat 2012 [6], also illustrated the easiness of inserting false airplanes into the surveillance monitor, with only an inexpensive ADS-B transmitter.

Many cryptographic approaches have recently been proposed to tackle some known attacks on ADS-B [7]–[10]. However, traditional cryptographic technologies cannot be trivially and directly utilized to ensure ADS-B security. Although ADS-B data may be encrypted to resist passive eavesdropping attacks [8], simply encrypting the entire ADS-B message is regarded conflicting with open nature of ADS-B broadcast. For instance, concerning flight safety and operational requirements, the federal aviation administration (FAA) claims the necessity of clear ADS-B data [11]. Consequently, it is a challenging problem for implementing the confidentiality of ADS-B messages without compromising flight safety.

Manuscript received August 21, 2018; revised October 18, 2018; accepted November 11, 2018. Date of publication November 21, 2018; date of current version May 8, 2019. The work of H. Li was supported in part by the National Key Research and Development Program of China under Grants 2017YFB0802300 and 2017YFB0802000, and the National Natural Science Foundation of China under Grants 61772121, 61728102, and 61472065. The work of H. Yang was supported in part by the National Key Research and Development Program of China (2017YFB0802003), National Natural Science Foundation of China (U1633114) and Sichuan Science and Technology Program (2018GZ0202). The work of R. Lu was supported in part by NSERC Discovery Grants (04009), NBIF Start-Up Grant (Rif 2017-012), HMF2017 YS-04, and LMCRF-S-2018-03. This is an extension version of a conference paper included in the Proceedings of IEEE GLOBECOM 2017 [1]. *(Corresponding author: Hongwei Li.)*

H. Yang, Q. Zhou, H. Li, and X. Zhang are with the School of Computer Science and Engineering and Center for Cyber Security, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: haomyang@uestc.edu.cn; qxzhou1010@qq.com; hongweili@uestc.edu.cn; johnsonzxs@uestc.edu.cn).

M. Yao is with the College of Computing, Georgia Institute of Technology, Atlanta, GA 30318 USA (e-mail: myao42@gatech.edu).

R. Lu is with the Faculty of Computer Science, Canadian Institute of Cybersecurity, University of New Brunswick, Fredericton, NB E3B 5A3, Canada (e-mail: rlu1@unb.ca).

Digital Object Identifier 10.1109/JIOT.2018.2882633

On the other side, in order to defend against active injection attacks, asymmetric algorithms (such as digital signatures [12]) have been exploited to guarantee the integrity of ADS-B messages. Nevertheless, it may result in heavy communication and computation burden. Apart from that, previous solutions to ADS-B security can only unilaterally achieve either confidentiality or integrity. Moreover, they all require changing existing protocols and transponders of ADS-B, breaking the compatibility to bring about obstructions of real-world deployments. It is worth noting that key management is notoriously difficult for air traffic surveillance networks, i.e., existing schemes of key exchange (e.g., [13]–[15]) are not appropriate for deployment in large-scale, distributed, and dynamic environments of ADS-B. With respect to processing capability, avionics are usually resource-constrained, and ADS-B communication channels, whether ES 1090 [16] or UAT [17], are both congested with low bandwidth. Therefore, the state-of-the-art cryptographic countermeasures are insufficient, and it is extremely desirable for an effective and practical cryptographic alternative to ADS-B security, considering realistic requirements of the privacy, authenticity, performance, and compatibility in air traffic monitoring and control.

In this paper, aiming at above challenges, we propose a cryptographic solution to ADS-B security with the practicability and high compatibility, ensuring both confidentiality and integrity without having to change existing protocols, and upgrade legacy transmitters on ADS-B. Therefore, our proposal is suitable for large-scale and low-cost deployments. The primary idea is to break linkages between aircraft's identities and the associated geographic positions to ensure the privacy, make full utilization of reserved fields in the ADS-B format to perform broadcast authentication, and tolerate greatly the package loss and disorder simultaneously. Specifically, we first explore in depth cryptographic primitives of the timed efficient stream loss-tolerant authentication protocol (TESLA) [18] and the format-preserving encryption (FPE) [19], and then adapt them to ADS-B environments. This paper extends our previous work related to ADS-B security [1] by achieving adaptive TESLA and solving disorder problems. In specific, our contributions in this paper are given as below.

1) We present a lightweight and practical cryptographic solution to secure ADS-B communication problems that can protect ADS-B systems from both active and passive attacks. The proposal is capable of guaranteeing high compatibility by adapting specific cryptographic primitives to accommodate ADS-B message format.
2) We analyze formally the security of our schemes, comprehensively achieving the confidentiality and authenticity.
3) We perform the performance evaluation of our approaches, by conducting simulations in embedded devices and desktop computers, respectively, on the basis of real fight data from *OpenSky*, a large-scale sensor network for the purpose of gathering massive ADS-B messages [20].
4) We implement a deployment for our solution in a real airport environment, where the authentication process takes only 0.081 s under realistic air traffic conditions. In addition, even if the encryption option is turned on, the console of surveillance can still display the same fight trajectories, demonstrating the feasibility of our solution in a realistic ADS-B scenario.

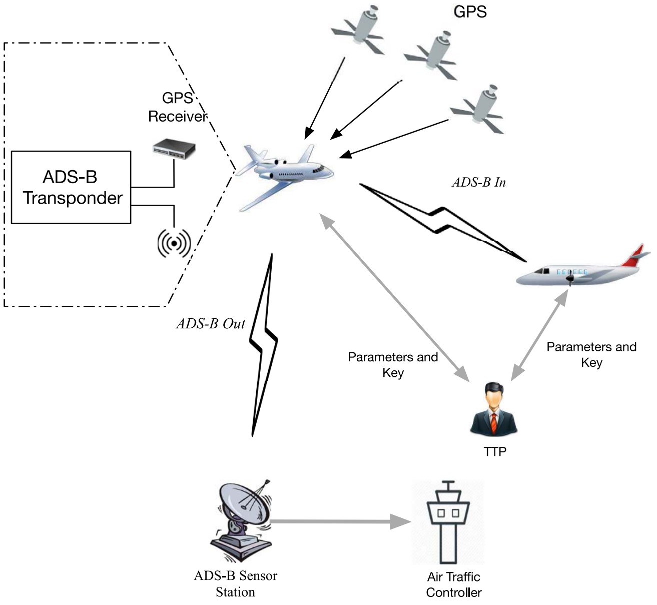


Fig. 1. System model under consideration.

The remainder of this paper is organized in the following way. We state the secure ADS-B communication problem first, including the system model, threat model, and design goals in Section II. Then, we give preliminaries in Section III. In Section IV, we elaborate specific processes when applying the proposed solution in ADS-B systems. In Section V, we accomplish extended discussions to enhance ADS-B security. We further assess security and performance for our schemes in Sections VI and VII, respectively. In Section VIII, we deploy our solution in the real-world airport to verify effectiveness. In Section IX, related works are presented. Finally, we conclude this paper in Section X.

II. Problem Statement

In this section, we formalize the system model, present a realistic threat model by identifying various kinds of attacks, and define our design goals.

A. System Model

It is well known that as the heart of next-generation air traffic monitoring and control technologies, ADS-B consists primarily of two types of data links, UAT [17] or ES 1090 [16]. In this paper, we mainly concentrate on ES 1090 containing 112-bit data frames, which is pervasively available in most airspaces. Nevertheless, our approach is also conveniently adapted to UAT scenarios.

As illustrated in Fig. 1, our system model is abstracted from key components of general ADS-B systems [21], [22], where aircraft determine their own positional information obtained from the global navigation satellite system such as GPS. After that, transponders continuously broadcast ADS-B messages,

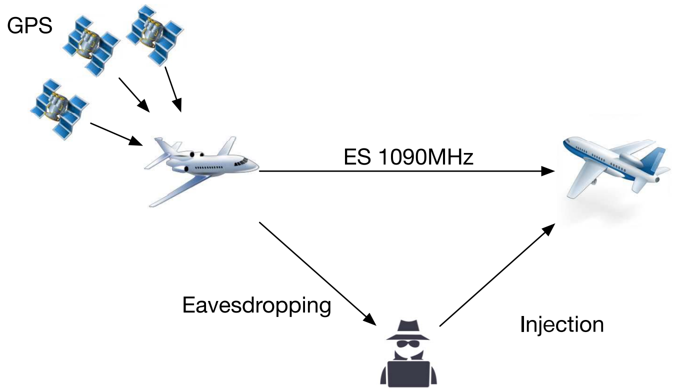


Fig. 2. Threat model considering a sophisticated attacker.

including position, velocity, intent, etc., to the surrounding via *ADS-B out*–an airborne communication subsystem. If equipped with ADS-B receivers, nearby aircraft and ground stations can receive messages by *ADS-B in*–a corresponding communication subsystem, to improve situational awareness. Note that the air traffic controller (ATCO) connecting to ground sensor stations will play a vital role of surveillance by displaying aircraft on the monitor upon received position claims. Due to the connectivity of civil aviation Intranet networks, we can assume that the security of on-ground communications is guaranteed.

The trusted third party (TTP) needs to be incorporated into the system model, serving as the authority of key management. Indeed, ATCO may act as TTP to fulfill the functionality of key generation and distribution. In that way, we also assume that there exist secure channels between TTP and aircraft to transmit keys and public parameters. In fact, the secure channel may be implemented by using the protocol of controller-pilot data link communication (CPDLC), offering ground-air data communication [8].

It is worth noting that our model focus on security issues of ADS-B for general aviation aircraft, not for scheduled-based commercial airliners that are run on public and regulated routes.

B. Threat Model

As aforementioned, the negligence of security primitives in designing ADS-B protocols, imposes a serious threat to air traffic security, since ADS-B broadcast messages are all transmitted over unencrypted wireless networks, and message authentication mechanisms are not provided yet. In this section, we develop a pertinent threat model as illustrated in Fig. 2 that can capture two distinct types of realistic attacks, passive eavesdropping attacks called *aircraft reconnaissance* and active injection attacks called *aircraft ghost injection* [7], launched by a sophisticated attacker.

1) *Aircraft Reconnaissance:* To improve flight safety and enhance international interoperability, clear data links are strongly recommended by FAA, in order to keep critical surveillance data, such as positional information of aircraft, openly accessible. However, this also renders ADS-B systems susceptible to security breaches stemming from a lack of confidentiality. For example, only if equipped with an inexpensive ADS-B receiver, any adversaries can intercept broadcasts and eavesdrop messages by tuning to corresponding frequencies. In that way, the valuable information, e.g., aircraft's positions, can be linkable to their identities, resulting in the privacy leakage.
2) *Aircraft Ghost Injection:* An adversary can falsify flight data in full compliance with the ADS-B message format, and then broadcast them via off-the-shelf and low-cost ADS-B transmitters, generating so-called *ghost aircraft injection* attacks. For the absence of mechanisms of authenticity and integrity in the ADS-B protocol, the airplane receiving fake messages may turn to avoid collision with nonexistent airplanes. Also, false message injections can cause severely interference with air traffic control, by introducing a large number of ghost airplanes on ATCO displays, thereby crippling potential operational capacity. Additionally, the injected bit-flipping signals on physical channels likely lead to the disappearance of existing aircraft on the monitoring screen [7].

Besides these two threats of *aircraft reconnaissance* and *aircraft ghost injection* involved in the above model, there also exist other threats, e.g., the attacks of flood denial on ground sensors or aircraft. As we mainly focus on protecting the confidentiality and integrity of ADS-B messages, they are out of scope of this paper, and will be further studied in our future work.

C. Design Goals

With reference to the above models, our design goal is to provide a holistic cryptographic solution to ADS-B security with high compatibility and practicability that can effectively defend against *aircraft reconnaissance* as well as *aircraft ghost injection* attacks. In particular, the following security and efficiency requirements are desirable.

1) *Privacy:* Any unauthorized entity should not setup connections between aircraft's digital identifiers and their valuable information such as highly accurate locations. Especially concerning private airplanes owned by companies or individuals, their location trajectories are much likely related to visiting places of business or personal interest. Thus, the identity anonymity should be also achieved to protect the privacy of general aviation aircraft.
2) *Authenticity and Integrity:* Any received ADS-B data should be validated to prevent malicious message injections that may deceive air traffic surveillance and collision avoidance systems.
3) *Robustness to Packet Loss and Disorder:* Considering that the ADS-B mandatory roll-out may bring about, with a great possibility, the rising of channel utilization in next few decades, the loss and disorder of ADS-B packets may increase significantly on the physical layer. Therefore, our techniques should be capable of tolerating packet loss and disorder effectively.

TABLE I
NOTATIONS

Notation	Meaning
λ	Security parameter
$\lvert \cdot \rvert$	Bit length
$\|$	Concatenation operator
T	FFX Tweak
K_F	FFX Key
$FFX.Encrypt_K^T(\cdot)$	FFX Encryption
K_i	*i-th* key in *Keychain*
P_i	*i-th* packet
$F(\cdot)$	One-way function
$F^{'}(\cdot)$	Truncating function
$\Gamma_i = \mathcal{H}(K_i, D_i)$	Generation of authenticating code
pid	Encrypted ICAO

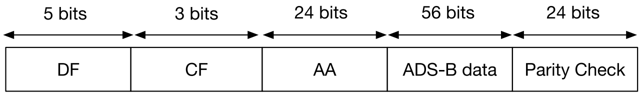
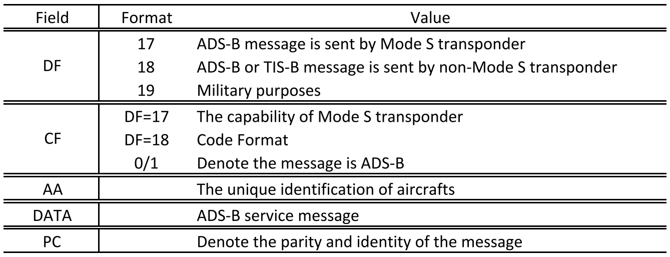


Fig. 3. Format of ADS-B message.

TABLE II
MEANING OF MESSAGE FIELDS



Field	Format	Value
DF	17	ADS-B message is sent by Mode S transponder
	18	ADS-B or TIS-B message is sent by non-Mode S transponder
	19	Military purposes
CF	DF=17	The capability of Mode S transponder
	DF=18	Code Format
	0/1	Denote the message is ADS-B
AA		The unique identification of aircrafts
DATA		ADS-B service message
PC		Denote the parity and identity of the message

4) *Efficiency:* Our solution should be lightweight in terms of communication overhead and computation cost, with regard to low-bandwidth data links and resource-limited avionics, to relax expensive system requirements.
5) *Compatibility:* To deploy in real systems, our solution should guarantee high compatibility, without having to change current ADS-B protocols, which is of particular importance due to the long certification and adoption cycle of upgrading existing aviation technologies.

III. PRELIMINARIES

In this section, we recall FFX and TESLA, which will serve as building blocks of our proposal. Before that, some notations are listed in Table I.

A. ADS-B Message Format

As illustrated in Fig. 3, the data link standard of ES 1090 [16], formats the ADS-B message with 112 bits in length, and the message consists of the following five fields: 1) downlink format (DF); 2) code format (CF); 3) ICAO aircraft address (AA); 4) ADS-B data (Data); and 5) parity check (PC), and the meaning of each field is shown in Table II.

TABLE III
TC OF *Data* FIELD

TC	Meaning
1-4	Aircraft identification
5-8	Surface position
9-18	Airborne position (Baro Alt)
19	Airborne velocities
20-22	Airborne position (GNSS Height)
23	Test message
24	Surface system status
25-27	Reserved
28	Extended squitter AC status
29	Target state and status (V.2)
30	Reserved
31	Aircraft operation status

Note that the AA field carries the aircraft unique identifier, known as the international civil aviation organization (ICAO) address of 24 bits, which generally needs to consider the privacy issue. Also, only the 56-bit data field may be employed to transmit data, and the type code (TC) segment of five bits, at the beginning of the data field, are shown in Table III. ADS-B messages with reserved fields, e.g., TC $= 25$ do not be processed by existing transponders, while others are accordingly parsed as the aircraft identification, position, velocity, etc. It is also noteworthy that our authentication method can utilize these reserved fields to send the verification codes, thereby not requiring changes of the existing ADS-B message format.

B. FFX

The FPE [19], as a symmetric cipher, can remain the same format between plaintexts and ciphertexts which are both taken over the same character set Chars $= \{0, 1, 2, \ldots, \text{radix} - 1\}$. In particular, FFX represents a typical FPE algorithm that has been accepted by NIST recently [23]. FFX specially employs the Feistel network, where the *X* suggests multiple parameter choices containing the round function, the number of Feistel network rounds, the degree of imbalance, etc. For more details, please refer to [23].

Compared to the encryption algorithms with the fixed message block size, such as AES, FFX has a special advantage in the ADS-B setting, i.e., it can encipher messages with arbitrary length (e.g., the 112-bit ADS-B message). Consequently, we can exploit FFX to encrypt the AA field in the ADS-B message, not requiring the additional padding for the fixed block length.

C. TESLA

As is known to all, TESLA [18], as a lightweight broadcast authentication protocol, is widely available in wireless communications. The core idea in TESLA, is to make use of the *Keychain*, a sequence of keys acquired by continuously utilizing one-way hash function. In TESLA, to achieve authenticity and integrity of the messages, the broadcaster first employs reversely the keys in *Keychain* to produce encrypted message

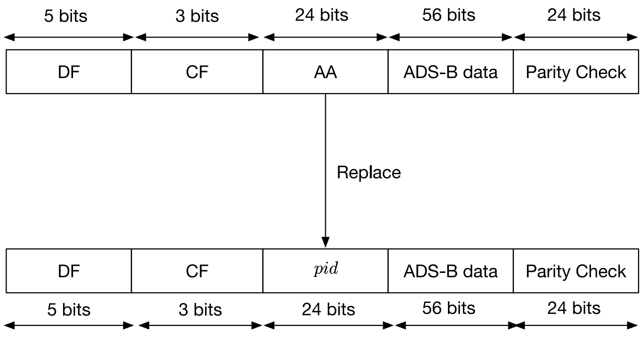


Fig. 4. Encryption and replacement of AA field.

authentication codes (MACs), sent along with the emitted messages. After an amount of messages, the broadcaster publishes used keys of generating MACs, allowing the receiver to verify previously buffered messages for delay. What is more, the receiver may derive formerly used keys through hash operations for multiple derivations due to the continuity of *Keychain*. It is worth noting that due to the broadcast nature of ADS-B communications, we can adapt TESLA to the air traffic surveillance scenario, so as to guarantee the authenticity and integrity of ADS-B data.

IV. Our Proposed Solution

As demonstrated in the above threat model, we mainly focus on discussing two types of potential threats, namely *aircraft reconnaissance* and *aircraft ghost injection*, to ADS-B systems. In this section, we present our solution to resist these malicious attacks as follows. Before we describe our solution in detail, we first present the rationale of our solution.

A. Rationale of Our Solution

1) Resistance to Aircraft Reconnaissance: To defend against passive attacks, we shall only encrypt the AA field in the ADS-B message, which demonstrates three advantages as follows. First, the unique ICAO filled in the AA field is intended for the aircraft identification, and the encryption of ICAO is able to prevent an adversary from pinning a specified aircraft. Second, traditional block ciphers require standard block sizes, while the 24-bit ICAO does not conform to the prescribed block size. Herein, we specify FFX as the underlying encryption primitive as it can support arbitrary length of plaintexts, and remain the same format between the ICAO and its corresponding ciphertext. Therefore, it can be compatible with the existing ADS-B protocol. Third, encrypting totally the ADS-B message does not obey the open accessibility of positional data. Consequently, our strategy to encrypt only the AA field, does not affect the functionality of air traffic surveillance. As shown in Fig. 4, the encryption is sketchy described as such procedure that TTP first runs the FFX encryption, and then the aircraft replaces its ICAO with the associated ciphertext pid. We will elaborate details of incorporating this encryption approach in our solution in Section IV-B.

It is noteworthy that Sampigethaya *et al.* [24] have presented an identity privacy-preserving method of the random silent period for general aviation aircraft. This method can enhance spatial and temporal uncertainty, by updating digital identifiers of aircraft but no transmitting them in a random silent period, to confuse the target aircraft with surrounding aircraft. However, the privacy level is dependent on the size of the anonymity set of neighboring aircraft. Consequently, the privacy level would decline with the decrease of the number of surrounding aircraft. Therefore, the method may not be suitable if the airspace is not busy.

2) Resistance to Aircraft Ghost Injection: To prevent active attacks from malicious injection adversaries, on one hand, we can appropriately adapt TESLA to ADS-B systems, and utilize the keyed-hash MAC, to protect the authenticity and integrity of ADS-B messages. Furthermore, the adaption of TESLA can also achieve the resilience of packet loss, which commonly occurs on ADS-B data links, as there is no mechanism of collision avoidance and retransmission for ADS-B packets. As indicated in [22], the mean error rate of ADS-B packets is up to 33%. On the other hand, we can employ the reserved ADS-B fields to accommodate the keys and MACs, transmitted along with messages needed to be authenticated. As a result, legacy transmitters can also correctly parse received ADS-B packets, and our approach can be compatible with current ADS-B standards. The generation and verification procedures of ADS-B packets are illustrated in Figs. 5 and 6, respectively, and the detailed process will be later described in Section IV-B.

It is also worth noticing that there are other potential approaches to ensure the integrity of ADS-B position data, such as the k-nearest neighbors [25] and the multilateration [20], in which the main idea is to double check the authenticity of location claims made by aircraft and other ADS-B participants. Therefore, it is different from the verification of the broadcast sources and messages by cryptographic MACs.

B. Description of Our Solution

On the basis of above security measures, we will present the whole framework of our solution to demonstrate how to achieve privacy and integrity comprehensively, simultaneously not requiring modifications to the ADS-B protocol. Concretely, our solution includes the following four algorithms: 1) ParamGen(Θ); 2) KeyChainGen(F); 3) Encrypt(E); and 4) Authenticate($\mathcal{H}$).

1) *$\Theta(\lambda)$:* TTP publishes the necessary parameters (e.g., T, K_F, n) for ADS-B systems on the input of the security level λ.
2) *$F(K_n)$:* TTP invokes recursively the one-way function $F(\cdot)$ to compute *Keychain* as $F^{v}(K_n) = F(F^{v-1}(K_n))$, where *Keychain* $= (K_0, K_1, \ldots, K_n)$. In our proposal, F may be instantiated as SHA1 which means $\{|K_i| = 160|0 \leq i \leq n\}$.
3) *$E(ICAO, K_F, T)$:* TTP runs the FFX encryption algorithm by taking in ICAO of the aircraft, the key K_F and the tweak T, and then outputs pid, the ciphertext related to ICAO, to the aircraft.
4) *$\mathcal{H}(K_i, D_i)$:* The aircraft produces the encrypted MAC Γ_i for D_i through the keyed-hash function $\mathcal{H}$ with the

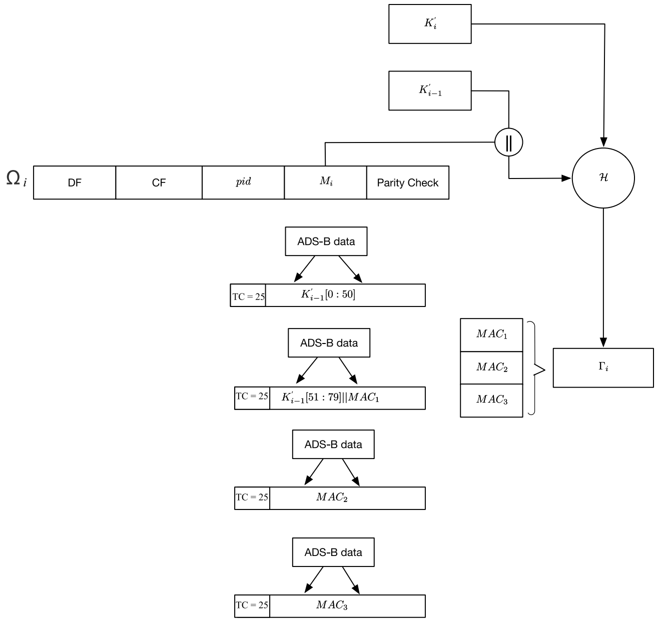


Fig. 5. Packet format and generation procedure.

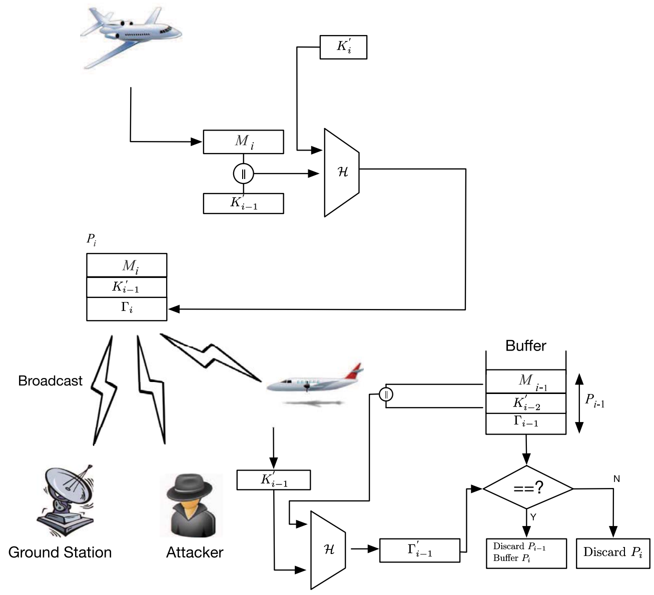


Fig. 6. Packet verification procedure.

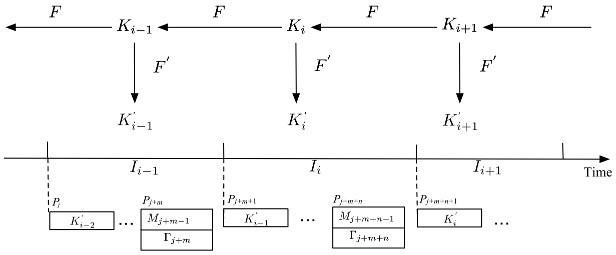


Fig. 7. Implementation of adaptive-TESLA.

key K_i. In this proposal, $\mathcal{H}$ may be implemented using HMAC-SHA1-96 which implies $\{|\Gamma_i| = 96 | 1 \leq i \leq n\}$.

Note that, in order to lower the communicational overhead, we exploit the truncation function $F'(K_i)$ to shorten the key from $\{|K_i| = 160 | 0 \leq i \leq n\}$ to $\{|K_i'| = 80 | 0 \leq i \leq n\}$.

Furthermore, the framework of our solution can be divided into two phases, *Initialization* and *Online Authentication*, which are detailed below.

1) Initialization: First of all, the aircraft with the intended use of ADS-B is required to accomplish registration in TTP, in which the associated ICAO is submitted by the aircraft to TTP via a secure channel. In general, the secure channel may be built on the communication subsystem of CPDLC. After receiving the ICAO, TTP processes the request of registration in the following way.

Step 1: On the input of the security level λ, TTP invokes first $\Theta(\lambda)$ to obtain T, and $K_F \in \{0,1\}^{160}$ for the aircraft.

Step 2: TTP runs the FFX encrypting algorithm as $\text{pid} = E(\text{ICAO}, K_F, T)$.

Step 3: TTP picks a random K_n in the set of $\{0,1\}^{160}$ and then calls repeatedly the one-way function $F(\cdot)$ until the entire *Keychain* is attained where *Keychain* $= (K_0, K_1, \ldots, K_n)$.

Step 4: TTP returns the tuple $\sigma_1 = (\text{pid}, \text{Keychain})$ to the aircraft via the secure channel and publishes the tuple $\sigma_2 = (\text{pid}, K_0)$ to the public.

2) Online Authentication: As shown in Fig. 4, the unique ICAO has been substituted with the pid retrieved from TTP. As is known, M_i indicates the ADS-B Data intended to be transmitted in the original message. Furthermore, as Fig. 6 illustrates, M_i is concatenated with K_{i-1}' which is the truncating result of $F'(K_{i-1})$, forming $D_i = \langle M_i || K_{i-1}' \rangle$. Then, the aircraft calculates the keyed-hash MAC as $\Gamma_i = \mathcal{H}(K_i', D_i)$.

For the simplicity of description, we abstract the format of ith ADS-B message as $\Omega_i = \langle \text{Head} || \text{pid} || \text{Data}_i || \text{PC}_i \rangle$ where $\text{Head} = \langle \text{DF} || \text{CF} \rangle$, $\text{Data}_i = \langle M_i || K_{i-1}' || \Gamma_i \rangle$, and PC_i is the CRC of the message to detect transmission errors.

In an ADS-B message, as is known, excluding the TC segment from the Data field, the remaining has merely the space of 51 bits to transmit data, while Data_i with $\Gamma_i \in \{0,1\}^{96}$ and $K_i' \in \{0,1\}^{80}$, is too long to be accommodated in this limited space. As a result, the packet P_i needs to be split into five consecutive messages. Thereinto, the first message is almost the same as the original one, with the data field still specified as M_i, except that ICAO is replaced by pid. Then, in the subsequent four messages, the data fields are filled with $\langle K_{i-1}' || \Gamma_i \rangle$ orderly, with TC assigned the value of 25 which denotes the reservation field. As demonstrated in Fig. 7, the specific process of transmission is detailed in the following.

Step 1: The sender replaces the ICAO using the pseudonym pid with the same length and alphabet.

Step 2: The sender withdraws the keys K_{i-1} and K_i from the *Keychain*, and applies the truncation function as $K_{i-1}' = F'(K_{i-1})$ and $K_i' = F'(K_i)$, respectively.

Step 3: The sender calculates and constructs P_i as $\langle \text{Head} || AA_i || \text{Data}_i || \text{PC}_i \rangle$, in which $\text{Data}_i = \langle M_i || K_{i-1}' || \Gamma_i \rangle$ with $\Gamma_i = \mathcal{H}(K_i', \langle M_i || K_{i-1}' \rangle)$. Considering that the available space of Data is very limited, the sender orderly fills the Data field with

$\langle K'_{i-1}||\Gamma_i\rangle$ that needs to use four ADS-B messages all with TC $= 25$.

Step 4: The sender broadcasts P_i via *ADS-B out*.

Upon receiving P_i, the receiver first checks whether P_i is consistent in the ADS-B message format, e.g., the length of each field and the CRC code of the entire message. If yes, then the receiver buffers P_i, otherwise discards it directly. Based on the idea of delayed authentication, the receiver cannot immediately verify P_i owing to the unawareness of K'_i which is used to produce the authentication code Γ_i, until receiving P_{i+1} that contains K'_i. The specific process of verification is as follows.

Step 1: The receiver first extracts $D_i = \langle M_i||K'_{i-1}\rangle$ and K'_i from P_i and P_{i+1}, respectively, calculates $F'(F(K'_i))$, and then compares it with K'_{i-1} in D_i. If they are equal, the procedure goes to the next step. Otherwise, the receiver simply discards P_{i+1} without any other processing.

Step 2: The receiver evaluates $\Gamma'_i = \mathcal{H}(K'_i, D_i)$.

Step 3: The receiver withdraws Γ_i from the buffered P_i, and checks if $\Gamma'_i \overset{?}{=} \Gamma_i$.

Step 4: If the above equation holds, P_i is first popped off, and P_{i+1} is then pushed into the buffer. Otherwise, P_{i+1} is directly thrown away.

3) Tolerating Packet Loss: Considering the case of packet loss that the receiver receives P_{i+m} while packets between P_i and P_{i+m} have been lost, the authenticating process of the buffered P_i is stated below.

Step 1: The receiver retrieves $D_i = \langle M_i||K'_{i-1}\rangle$ and K'_{i+m-1} from P_i and P_{i+m}, respectively, evaluates recursively $F'(F^m(K'_{i+m-1}))$, and compares it with K'_{i-1} in D_i. If equal, then the receiver proceeds with the following steps, otherwise directly discards P_{i+m}.

Step 2: The receiver derives $K'_i = F'(F^{m-1}(K'_{i+m-1}))$ first, and then calculates $\Gamma'_i = \mathcal{H}(K'_i, D_i)$.

Step 3: The receiver withdraws Γ_i from P_i, and checks if $\Gamma'_i \overset{?}{=} \Gamma_i$.

Step 4: If they are equal, P_i is first popped off, and P_{i+m} is then stored in the buffer. Otherwise, the receiver drops P_{i+m} as corrupted.

Note that some exceptional cases of packet loss need to be highlighted. In specific, when applying TESLA in the complicated ADS-B environment with interferences, it is likely for the receiver to receive just the first message in P_i, and the last four ones in P_{i+1}, while the last four messages in P_i and the first one in P_{i+1} are all lost. The reconstruction may be in such way that the first message in P_i and the last four ones in P_{i+1} are combined, forming a new packet because of the time continuity in these five messages. Nevertheless, the warning information on the incorrectness of the reconstructed packet is informed due to the failure of authenticating P_{i-1}. As a result, the receiver abandons the five mismatched messages, and expects arrivals of next packets.

V. Extended Discussion

In this section, we will have some extended discussion on how to make our solution more suitable for the deployment in realistic ADS-B systems. In particular, two issues, disorders and the adaptive-TESLA, will be discussed as below.

A. Disorder

In our proposal, the ADS-B transponder, via the wireless channel, broadcasts a sequence of packets $P_1, P_2, \ldots, P_n$ in order. In each packet, the original ADS-B message is first sent, immediately followed by the subsequent four ones with the reserved field of TC $= 25$, indicating the transmission of the key and MAC. Under normal circumstances, these messages can be received still in the emission order. However, as environmental factors, e.g., electromagnetic interferences, climatic changes, multipath effects, etc., might influence the propagation velocity of ADS-B signals, it is possible that the arrivals of messages are out-of-order. In this part, we will address the disorder problem in the practical real-world aviation setting. Furthermore, we will consider the following two kinds of disorders.

1) *Inner-Packet Disorder:* The total five ADS-B messages in a packet may be received in a wrong order.
2) *Interpacket Disorder:* The packets sent earlier, may be later received.

To handle the disorder problem, we demonstrate the timestamp means, which is based on the arrival time of physical ADS-B signals. When applying this approach, the aircraft needs to contain the timestamp, acquired via GPS, in the ADS-B message. For *inner-packet disorder*, it is simple to restore ADS-B messages to their correct order directly by the timestamp. In light of *interpacket disorder*, the method may be relatively complicated, considering that the timestamp can determine the orientation of derivating the keys in *Keychain*, which are used to authenticate packets. In specific, if the case of *Interpacket disorder* arises, when the receiver has received and buffered P_{i-1}, P_{i+1} may arrive earlier than P_i. Consequently, the authentication of P_{i-1} needs twice derivations of the keys, from K'_i in P_{i+1} to K'_{i-2} in P_{i-1} by $K'_{i-2} = F'(F^2(K'_i))$. Hence, after the authentication of P_{i-1} by using P_{i+1}, the receiver cannot anymore utilize already buffered P_{i+1} to authenticate later arrived P_i due to the one-way feature of the *Keychain*. As a result, the receiver directly disposes the disorderly P_i as corrupted.

B. Adaptive-TESLA

As afore described, we exploit the one-way *Keychain* with the retroactive key issuing, to achieve the delayed authentication of ADS-B messages. With regard to the notoriously jammed data link of ES 1090, every $K_i \in \{0, 1\}^{160}$ in *Keychain* has been truncated into $K'_i \in \{0, 1\}^{80}$, in order to reduce communication overhead. Nevertheless, for authenticating a message M_i, an associated key K'_{i-1} needs to be, every time, transmitted along with M_i. Therefore, for sending only a message with the payload of 51 bits, we are required to cost extra 176 bits, if specifying HMAC-SHA1-96 as the keyed hash function. As a result, this way needs to occupy the additional bandwidth of four messages, excluding the original one of carrying M_i.

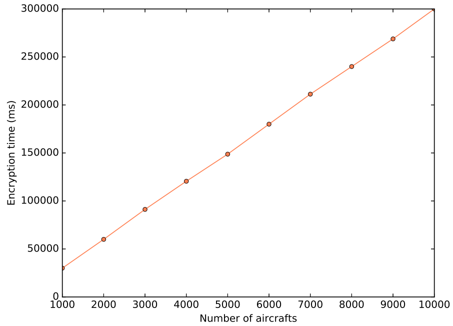


Fig. 8. Encryption time on ATCO.

The benefit of this one-off using different keys for each packet, is the guarantee of verification speed and resistance of memory-based DoS attacks [7], as the receiver is supposed to buffer only one packet used to verify the next arrivals. Nevertheless, the disadvantage is also apparent since every time the corresponding key needs to be sent along with every message, which results in the dramatically increased communication cost with the number of transmitted messages. In order to mitigate such overhead, we ingeniously design the adaption version of TESLA, called *Adaptive-TESLA*. It requires loose time synchronization, which can be easily implemented through satellite-based navigation systems such as GPS. Consequently, the sender is not yet required to deliver each packet accompanied with the different key per time. As only if in one time period, the same key can be employed to generate distinctive MACs for successively emitted messages, the traffic burden is considerably eased.

To be specific, according to the specification of ES 1090, TC $= 25, 26, 27, 30$ all stand for the reserved fields. Therefore, in *Adaptive-TESLA*, we may choose TC $= 25$ and TC $= 26$ to distinguish the packet with the MAC from the one with the key. As shown in Fig. 8, the sender publishes K'_{i-1} at the beginning of the time interval I_i, and the K'_{i-1} is filled in the Data field, with TC $= 26$ denoting the reserved field for the key delivery. Then, subsequently emitted packets, only including MACs with TC $= 25$, will not contain K'_{i-1} anymore in this time period I_i, thus saving significantly the bandwidth.

However, we have to pay extra cost for Adaptive TESLA. On one hand, as above mentioned, the loose time synchronization is required for ADS-B participants to ensure that the generated MACs and the corresponding verification key are in the same period. On the other hand, it is necessary to consider the proper time interval of updating keys to achieve the tradeoff between the updating cost and the key security.

VI. Security Analysis

In this section, we analyze the security of our solution, focusing on the privacy of aircraft's digital identifiers, and the authenticity and integrity of transmitted ADS-B messages.

A. Privacy

In current ADS-B communications, the straightforward and obvious security vulnerability is that, the attacker intercepts the wireless broadcasts of ADS-B on the unencrypted data links, only with some inexpensive off-the-shelf hardware. In that case, the attacker is able to eavesdrop and collect a large enough number of clear ADS-B messages. Furthermore, by mining the large-scale flight data, the attacker may establish the correlation between the aircraft's ICAO and its corresponding locations, thereby imperiling the privacy, e.g., business interests or personal preferences. On the other side, the openness of ADS-B systems should be also remained, by making aircraft positional data publicly available. To achieve both the privacy and openness, we employ FFX to encipher only the aircraft unique digital identifier of ICAO, instead of encrypting the whole ADS-B message. As a result, such correlation can be cut off, and the aircraft's identity cannot be linkable to its precise geographic information.

Therefore, this means that the privacy of our solution can be built on the FFX security. As is known, the ciphertext has the same format with the plaintext in FFX. Nevertheless, the similar patterns in the plaintext have been diffused in the ciphertext with sufficient entropy, thus preventing possible cryptanalysis, e.g., known plaintext attacks. Indeed, as stated in [23], FFX has been proved with the semantic security against adaptive chosen-ciphertext attacks, assuming that the underlying round function such as AES, is a good pseudo-random function (PRF). Consequently, our proposal can provide strong confidentiality protections, not compromising aircraft data in the ADS-B environment.

B. Authenticity and Integrity

In the attacks of *aircraft ghost injection*, a sophisticated adversary intends to forge or modify ADS-B data. However, it is infeasible to create correct MACs for ADS-B messages when the keys in *Keychain* are agnostic to the adversary. Furthermore, even if obtaining one key, the adversary can only make use of this key to produce MAC only once, since one-way *Keychain* is not adversely derivable, thus informally verifying the active-attack-resistance of our solution. Subsequently, we will formally prove the authenticity and integrity for disseminated ADS-B packets based on the following assumption.

Assumption 1: There does not exist any probabilistic-polynomial-time (PPT) algorithm that is able to distinguish between a PRF and an ideal random function. Furthermore, the HMAC function $\mathcal{H}$ is secure with collision-resistance [26]. Additionally, There exist hash functions with the property of target collision-resistance (TCR); namely, given a fixed message x and a hash function $F(\cdot)$, it should be computationally infeasible to find a value $x' \neq x$ such that $F(x') = F(x)$ [27].

Theorem 1: According to Assumption 1, the proposed approach can guarantee the authenticity and integrity of ADS-B data packets.

Proof: Here, we only give a sketchy proof framework on the basis of [28, Th. A.1]. First of all, we assume that $\mathcal{H}$ is secure with collision-resistance, and $F(\cdot)$ is a hash function with TCR property. In that case, the authenticity and integrity of our proposal can be reduced to the indistinguishability between a PRF and an ideal random function. ■

TABLE IV
FURTHER SECURITY COMPARISON

Security functionality	ECDSA [12]	TESLA [18]	FFX [23]	Ours
Privacy			√	√
Integrity	√	√		√
Compatibility			√	√

First, suppose that a PPT adversary $\mathcal{A}$ is capable of defeating the authenticity and integrity of our authentication method; that is, $\mathcal{A}$ transmits a message m to a receiver $\mathcal{R}$, such that although a sender $\mathcal{S}$ does not deliver m, $\mathcal{R}$ still agrees to take m, and ensures that m is authentic and comes from $\mathcal{S}$, with non-negligible advantage. Then, there is a PPT adversary $\mathcal{B}$ which utilizes $\mathcal{A}$, with non-negligible probability, to crack the above indistinguishability.

For this purpose, $\mathcal{B}$ first provides $\mathcal{A}$ with a simulated network environment since $\mathcal{B}$ can control all data communications. Next, $\mathcal{B}$ invokes $\mathcal{A}$ in the similar way as illustrated in [28]. For example, $\mathcal{B}$ also needs to choose a random integer $l \in \{1, \ldots, n\}$, where n is the maximum number of emitted ADS-B packets. It is worth noting that by the simulation, $\mathcal{B}$ intends $\mathcal{A}$ to break the authenticity and integrity; that is to say, $\mathcal{A}$ can falsify the lth packet P_l through interactions with $\mathcal{B}$.

As aforementioned, $\mathcal{B}$'goal is to distinguish a PRF from an ideal random function, thereby being offered the capability of accessing an oracle $G(\cdot)$ in the interactive game. So, when $\mathcal{A}$ issues an adaptively chosen query m to $\mathcal{B}$, $\mathcal{B}$ forwards it to the oracle $G(\cdot)$, and $\mathcal{A}$ is then answered with $G(m)$. Note that $G(m)$ is either a random number with the uniform distribution in $\{0, 1\}^*$, or a pseudo-random value PRF(m). After performing queries, $\mathcal{B}$ is required to tell whether $G(\cdot)$ is a true random function or a PRF. If correct, $\mathcal{B}$ succeeds in the game. Subsequently, we will give an argument that $\mathcal{B}$ will win the game if $\mathcal{A}$ can forge ADS-B packets with non-negligible advantage.

If $G(\cdot)$ is of true randomness, $\mathcal{A}$ can make a success forgery in the ADS-B data dissemination, only with negligible advantage. Nevertheless, as assumed above, if packets are authenticated by using a PRF, there is non-negligible probability ϵ for $\mathcal{A}$ to falsify P_l. Consequently, $\mathcal{B}$ succeeds in the game with the advantage of at least ϵ/l, which is also non-negligible. Furthermore, it is also infeasible for $\mathcal{A}$ to hand a false initial packet P_1 to $\mathcal{R}$ according to the above assumption. In addition, if $\mathcal{A}$ can deceive $\mathcal{R}$ into accepting a spoofing packet P_l, this means that a collision with $F(P'_l) = F(P_l)$ may be found, which also disobeys our assumption. Finally, we conclude from these contradictions that our method is able to protect the authenticity and integrity of ADS-B data packets.

C. Further Security Comparison

As Table IV illustrates, we perform the comparison of the security functionality with existing approaches.

1) *ECDSA* [12], based on the elliptic curve cipher (ECC), is employed to guarantee the integrity of ADS-B messages. However, this technique needs to add ECC signatures to the end of associated messages, which may lead to the expensive cost for modifying ADS-B protocols or upgrading legacy devices. Meanwhile, in [12], all fields of the ADS-B message are still required to be broadcast in plain text, violating the privacy.
2) *TESLA* [18] protects the integrity rather than the privacy for ADS-B messages. At the meantime, it requires, in the similar way, that the corresponding MAC is appended to the message, thereby equally failing the compatibility.
3) *FFX* [23] is able to provide ADS-B systems both with privacy and compatibility due to the characteristics of FPE. However, it does not afford the protection of integrity, which may raise security breaches, e.g., corruption of flight data or injection of ghost aircraft. As opposed to previous methods, our techniques can simultaneously achieve the privacy, integrity, and compatibility.

VII. PERFORMANCE EVALUATION

To quantify the effectiveness of our approaches in real-world ADS-B environments, in this section, we will evaluate the performance of our solution. As described in Section IV-B, our processing is divided into two phases: 1) *initialization* containing the generation of *Keychain* and pid and 2) *online authentication* involving the verification of ADS-B messages. Therefore, the performance evaluation should be accordingly carried out for the two phases. Moreover, this evaluation will be performed with respect to two types of aviation participants, the aircraft and the ATCO. The former is equipped with resource-restricted avionics, which can be simulated by the smart phone with the ARM-v7 processor running the Android 5.0.1 system. The latter is provided with powerful computers which can be emulated through the server with the E5-2620@2.40GHz processor running the Ubuntu 14.04 system. It is noteworthy that this simulation is conducted by using real ADS-B data from the *OpenSky* sensor network [20].

A. Performance on Encryption

In the phase of *Initialization*, the ATCO accomplishes the FFX encryption of the aircraft's real identity ICAO to acquire the corresponding pseudonym pid, and then replaces the original clear ICAO with the generated ciphertext pid. In comparison with the FFX encryption time, the time for replacement may be ignored. In addition, the time of producing *Keychain* is also negligible, as the operations of one-way hash are fairly fast. Consequently, the time overhead in *Initialization* costs mainly in the FFX encryption, and we will estimate the encryption time with the number of aircraft as below.

For the number of aircraft varies significantly in light of distinctive airspaces, to accurately reflect the time cost of FFX in real-world ADS-B systems, we measure the encryption time on ATCO every 1000 aircraft from 1000 to 10 000. The experimental results are collected as shown in Fig. 9, indicating that the encryption time is roughly linear with the number of aircraft. Furthermore, to intuitionally demonstrate the efficiency of ADS-B encryption, we calculate the average time for one aircraft, and the resulting time is approximately 30 ms. As a

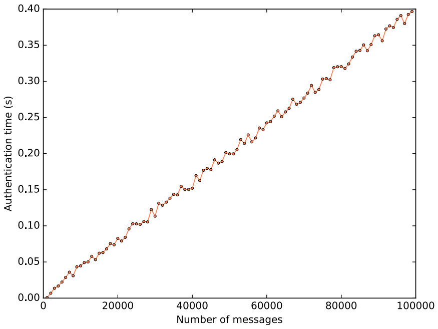


Fig. 9. Authentication time on ATCO.

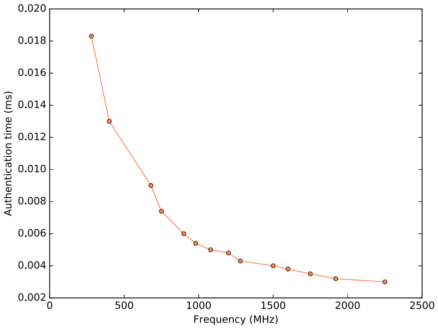


Fig. 10. Authentication time on aircraft.

consequence, in *Initialization*, the encryption is deemed to be considerably efficient, and thus ATCO is capable of simultaneously coping with registrations for a great quantity of participants, suitable for a large-scale ADS-B network.

B. Authentication on ATCO

As suggested in our solution, the aircraft is required to continuously transmit ADS-B broadcast messages, followed by associated MACs, to nodes within close proximity. These surrounding nodes include ground stations connected to the ATCO, as well as other *en route* aircraft. In that case, all listening receivers need to verify received ADS-B messages to prevent possible injection or manipulation attacks. Accordingly, the performance of authenticating a large number of messages is essential to be evaluated, so as to assess the availability when applying our approaches to the large-scale air traffic network. Nevertheless, participants are likely to own distinctive processing capabilities. For instance, the aircraft are generally equipped with resource-limited embedded avionics, but the ATCO may be provided with high-performance servers. Thus, this evaluation need to consider receivers' respective computational power. In this part, we will first analyze the performance of authentication on ATCO.

We implement the simulation of authentication on ATCO, and collect a huge amount of data on consumed time to point Fig. 10, which shows the time cost with respect to buffered messages of up to 10^5. As seen in Fig. 10, the time cost of verification approximates to the linearity with the number of messages, attaining the mean time of about 0.004 ms for authenticating one message. Consequently, our authentication scheme can offer comparably lightweight integrity protections by efficiently detecting injected false ADS-B messages. Therefore, it can achieve the scalability for the ever-rising air traffic and aircraft density in most airspaces.

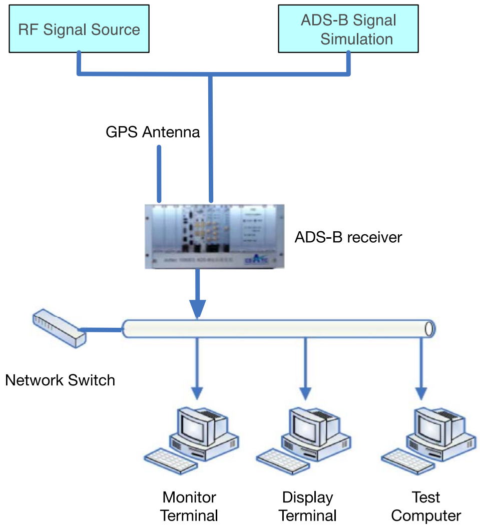


Fig. 11. Test environment.

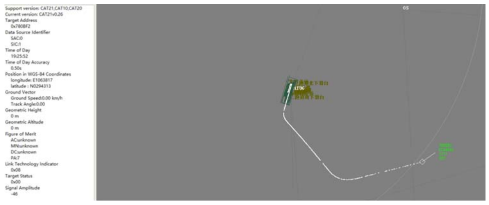
C. Authentication on Aircraft

The aircraft are equally required to verify received flight data to defend against the fake message injection, e.g., inserting ghost airplanes on the cockpit display. It is worth noting that concerning capability-constrained avionics, we will focus on the performance simulation of being able to reflect different handling capacities for various types of on-board devices.

Based on above discussion, we make use of Java and NDK C++ to reconstruct the authentication program, and then install it in the smart phone with the ARM-v7 embedded processor. Furthermore, by acquiring the root privilege of the android system, we can adjust, by running APPs like *SetCPU*, the processor frequencies on behalf of levels of calculating power. As demonstrated in Fig. 11, the frequencies are set to fourteen values from 2265 MHz down to 300 MHz, and the authentication becomes more inefficient with frequency drop. Nevertheless, even for the lowest frequency of 300 MHz, the time consumed only costs 0.018 ms for verifying one ADS-B message. As a result, our method is sufficiently lightweight, and the overhead of authenticating time may put the great stress on neither the ATCO nor the aircraft. Therefore, it can relax the requirement of computational resources, suitable for a variety of widely available avionics.

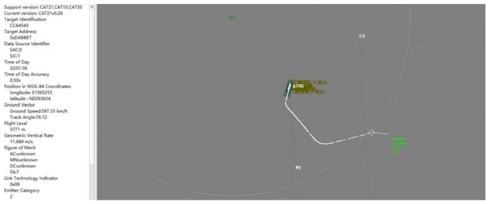
VIII. Compatibility Analysis

An imperative goal of our solution is to assure the compatibility in the real air traffic surveillance environment. Hence, in the section, we will exhibit the experiment results on the compatibility by the real airport deployment. Before that, we will first give a summary analysis about the reason of achieving the compatibility as below.



```
Support version: CAT21,CAT10,CAT20
Current version: CAT21v0.26
Target Address
    0x780BF2
Data Source Identifier
    SAC:0
    SIC:1
Time of Day
    19:25:52
Time of Day Accuracy
    0.50s
Position in WGS-84 Coordinates
    longitude: E1063817
    latitude : N0294313
Ground Vector
    Ground Speed:0.00 km/h
    Track Angle:0.00
Geometric Height
    0 m
Geometric Altitude
    0 m
Figure of Merit
    AC:unknown
    MN:unknown
    DC:unknown
    PA:7
Link Technology Indicator
    0x08
Target Status
    0x00
Signal Amplitude
    -46
```

Fig. 12. Original trajectory.



```
Support version: CAT21,CAT10,CAT20
Current version: CAT21v0.26
Target Identification
    CCA4543
Target Address
    0xDABBE7
Data Source Identifier
    SAC:0
    SIC:1
Time of Day
    22:01:36
Time of Day Accuracy
    0.50s
Position in WGS-84 Coordinates
    longitude: E1065255
    latitude : N0293634
Ground Vector
    Ground Speed:597.33 km/h
    Track Angle:76.12
Flight Level
    3771 m
Geometric Vertical Rate
    11.684 m/s
Figure of Merit
    AC:unknown
    MN:unknown
    DC:unknown
    PA:7
Link Technology Indicator
    0x08
Emitter Category
    2
```

Fig. 13. Trajectory after processing.

1) *FFX:* Compared to traditional encryption algorithms, FFX can ensure the same format, e.g., the length and character repertory, between the aircraft's real digital identifier ICAO and its pseudonym pid, without altering the message format. Additionally, using conventional block ciphers such as AES, also needs the extra padding for the fixed block size, thereby ulteriorly stressing the already congested ES 1090 channel.
2) *TESLA:* Our authentication approaches are built on TESLA, further by filling the key and MAC in the reserved data fields with TC = 25 and TC = 26, respectively, which can be in accordance with current ADS-B standards. Consequently, when receiving our authenticating messages, existing transponders do not drop them as corrupted, but parse them as reserved, and then hand them in to high-level applications for the subsequent handling, thus not requiring to upgrade the legacy hardware.

In order to assess the compatibility in a realistic air traffic surveillance scenario, our solution has been deployed in the Chongqing Jiangbei International Airport. The test environment is illustrated in Fig. 11 as follows.

1) The ADS-B transmitter reassembles real ADS-B messages retrieved from this airport, to make them adapted to our scheme, and then broadcasts them again on the ES 1090 data link.
2) The ADS-B receiver first observes if these reassembled data can be received, and then parses them according to associated ADS-B protocols.
3) ATCO checks whether the parsed data conform to the ADS-B standard format. If no, then these data are discarded, otherwise displayed onto monitoring screens.

The experiments involve processing the encrypted message and keyed-hash MAC by using the off-the-shelf hardware, and the results are shown in Figs. 12 and 13. Note that the original ICAO is set to be "780BF2," while the resulting pid is assigned to be "DABBE7" after FFX encryption. As a result, our encryption method can keep the AA field format unchanged, and thus the transponder cannot effectively distinguish. At the meantime, in light of the identical air traffic data, two flight trajectories are calculated with MAC and without MAC respectively, and then displayed on ATCO monitoring screens. The same of two tracks demonstrates that the existing ADS-B devices do not drop our produced ADS-B data as corrupted. Therefore, our authentication approach can be also compatible with existing protocols and transponders of ADS-B.

To further analyze the performance of our solution in the real-world ADS-B setting, we conduct authentication experiments in the above-mentioned airport. As is known, especially during a rush hour, this airport is significantly busy with approximate 200 airplanes of takeoff and landing. The result shows that for up to 4500 messages, the total time of authentication only cost 81 ms, with the transponder working frequency of 300 MHz. As a consequence, under realistic air traffic conditions, with high density of aircraft, our solution can decrease neither security nor performance on the heavily utilized ES 1090 data link. Therefore, it is very suitable for the large-scale and low-cost ADS-B deployments.

IX. Related Works

To secure the ADS-B communication, cryptographic countermeasures may be explored to protect the authenticity and integrity of air traffic data. Sampigethaya *et al.* [9], [29] first investigated security measures that exploited the symmetric-key encryption or digital signatures to authenticate ADS-B messages.

Following this research line, an authenticated encryption scheme for ADS-B data links was subsequently suggested by employing symmetric block ciphers [30]. Nevertheless, it is strongly acknowledged that managing and distributing the symmetric keys are not easy in large-scale and dynamic networks, especially for not well-connected wireless broadcast channels of ADS-B. Recently, Wesson *et al.* [11] discussed inherent disadvantages of the symmetric-key techniques in the ADS-B setting, and thus vigorously recommended the integrity protections of utilizing the public key cryptography. Therefore, myriad ADS-B authentication approaches based on the public-key infrastructure (PKI), were proposed in succession [31]–[34]. As an example, Pan *et al.* [12] created ECDSA signatures for ADS-B messages, which were then verified by others participants by using X.509 certificates. However, the certificate-based signatures cannot be well applied to low-bandwidth ADS-B networks, since it is costly to transmit and verify certificates in terms of communication and computation overheads.

To more efficiently perform authentication, the identity-based signature (IBS) is also considered as an alternative. In IBS, the public keys are directly extracted from users' identities such as e-mail address, telephone number, and so on. As a consequence, the PKI is not yet essential, thereby measurably reducing the operation and maintenance costs for PKI [35]. However, the IBS-based verifications [36], [37], still need to attach IBS signatures behind emitted messages, with having to modify existing ADS-B protocols. Therefore, it may equally cause the problem of incompatibility, which obstructs deploying ADS-B in practical real-world aviation scenarios.

Moreover, it is well known that TESLA is thought of as a lightweight authentication protocol, which is widely applied to wireless broadcast communications. However, the trivial use of TESLA seems not to be a good way, owing to some special requirements of ADS-B. For instance, TESLA could not work well when emergent messages are required to be authenticated in real time, because of its core idea on the delayed authentication. Hence, we need to explore in depth the utilization of TESLA in the ADS-B communication environment. In addition, there are potential approaches to protect data security. For example, the truth discovery technique [38], [39] can be also used to guarantee the authenticity and integrity of ADS-B messages.

On the other hand, as for the confidentiality of ADS-B messages, the encryption in an asymmetric mode, still has the high demand for PKI, which similarly challenges the realistic deployment. There were also sophisticated symmetric cryptographic methods [31], [40], [41], presented to ensure the privacy of aircraft identity by enciphering the entire ADS-B message. However, the encrypted positional data cannot any more be publicly accessible to those participants without keys, possibly affecting the flight safety. This does not yet conform to the anticipated openness intend of ADS-B. In addition, traditional block ciphers, e.g., AES, need the extra padding to fit the fixed block size, thereby considerably extending the message length. As a result, they also increase the burden on the already jammed ES 1090 channel.

Therefore, to enhance the security of ADS-B, it is imperative to present a practical and highly compatible cryptographic solution to comprehensively protect the confidentiality and integrity of ADS-B messages.

X. Conclusion

In this paper, we have addressed security issues for the real ADS-B system, and presented a complete cryptographic solution to comprehensively ensure the privacy and integrity of ADS-B messages. Meanwhile, the use of the FFX encryption and reserved ADS-B messages can guarantee the compatibility of our solution with existing ADS-B protocols. Extensive experiments based on real flight data demonstrate the high performance of the proposed approaches, suitable for the deployment in practical real-world aviation system. In our future work, other challenging security concerns will be further explored, e.g., privacy-preserving location estimation in air traffic surveillance networks.

References

[1] H. Yang, M. Yao, Z. Xu, and B. Liu, "LHCSAS: A lightweight and highly-compatible solution for ADS-B security," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–7.

[2] *Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B)*, RTCA, Washington, DC, USA, Oct. 2002.

[3] P. P. Pan and K. Semple. (Mar. 2014). *A Routine Flight, Till Both Routine and Flight Vanish*. [Online]. Available: https://www.nytimes.com/2014/03/23/world/asia/a-routine-flight-till-both-routine-and-flight-vanish.html

[4] *Automatic Dependent Surveillance–Broadcast*, FAA, Washington, DC, USA, Oct. 2016.

[5] *Cascade News 9—Update on Developments*, EUROCONTROL, Brussels, Belgium, Oct. 2010.

[6] D. Storm. (Aug. 2012). *Curious Hackers Inject Ghost Airplanes Into Radar, Track Celebrities' Flights*. [Online]. Available: http://www.computerworld.com/article/2472455/cybercrime-hacking/curious-hackers-inject-ghost-airplanes-into-radar.html

[7] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1066–1087, 2nd Quart., 2015.

[8] C. Finke, J. Butts, and R. Mills, "ADS-B encryption: Confidentiality in the friendly skies," in *Proc. 8th Annu. Cyber Security Inf. Intell. Res. Workshop*, 2013, pp. 1–9.

[9] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, "Future e-enabled aircraft communications and security: The next 20 years and beyond," *Proc. IEEE*, vol. 99, no. 11, pp. 2040–2055, Nov. 2011.

[10] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in Internet of Things with privacy preserving: Challenges, solutions and opportunities," *IEEE Netw.*, vol. 32, no. 6, pp. 144–151, Nov. 2018, doi: 10.1109/MNET.2018.1700374.

[11] K. D. Wesson, T. E. Humphreys, and B. L. Evans. *Can Cryptography Secure Next Generation Air Traffic Surveillance?*. [Online]. Available: https://radionavlab.ae.utexas.edu/images/stories/files/papers/adsb_for_submission.pdf

[12] W. Pan, Z. Feng, and Y. Wang, "ADS-B data authentication based on ECC and X. 509 certificate," *J. Electron. Sci. Technol.*, vol. 10, no. 1, pp. 51–55, 2012.

[13] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 870–885, Apr. 2019, doi: 10.1109/TIFS.2018.2868162.

[14] H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, "Personalized search over encrypted data with efficient and secure updates in mobile clouds," *IEEE Trans. Emerg. Topics Comput.*, vol. 6, no. 1, pp. 97–109, Jan./Mar. 2018.

[15] M. M. E. A. Mahmoud, J. Mišić, K. Akkaya, and X. Shen, "Investigating public-key certificate revocation in smart grid," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 490–503, Dec. 2015.

[16] *Minimum Operational Performance Standard for 1090 MHz Extended Squitter ADS-B and TIS-B*, document RTCA DO-260, RTCA Inc., Washington, DC, USA, 2009.

[17] *Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance—Broadcast*, document RTCA DO-282, RTCA Inc., Washington, DC, USA, 2009.

[18] A. Perrig, D. Song, R. Canetti, J. Tygar, and B. Briscoe, "Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction," IETF, Fremont, CA, USA, Rep. RFC 4082, 2005.

[19] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers, "Format-preserving encryption," in *Proc. Int. Workshop Sel. Areas Cryptography*, 2009, pp. 295–312.

[20] M. Strohmeier, I. Martinovic, M. Fuchs, M. Schäfer, and V. Lenders, "OpenSky: A swiss army knife for air traffic security research," in *Proc. IEEE/AIAA 34th Digit. Avionics Syst. Conf. (DASC)*, 2015, pp. 401–413.

[21] D. Mccallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *Int. J. Crit. Infrastruct. Protect.*, vol. 4, no. 2, pp. 78–87, 2011.

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

[23] M. Bellare, P. Rogaway, and T. Spies, *The FFX Mode of Operation for Format-Preserving Encryption*," NIST, Gaithersburg, MD, USA, vol. 20, 2010.

[24] K. Sampigethaya, R. Poovendran, and C. S. Taylor, "Privacy of general aviation aircraft in the NextGen," in *Proc. Digit. Avionics Syst. Conf.*, 2012, pp. 1–15.

[25] M. Strohmeier, V. Lenders, and I. Martinovic, "Lightweight location verification in air traffic surveillance networks," in *Proc. ACM Workshop Cyber Phys. Syst. Security*, 2015, pp. 49–60.

[26] M. Bellare, "New proofs for NMAC and HMAC: Security without collision-resistance," in *Proc. Int. Conf. Adv. Cryptol.*, 2006, pp. 602–619.

[27] M. Bellare and P. Rogaway, "Collision-resistant hashing: Towards making UOWHFs practical," in *Proc. Adv. Cryptol. (CRYPTO)*, 1997, pp. 470–484.

[28] A. Perrig, C. Ran, J. D. Tygar, and D. Song, “Efficient authentication and signing of multicast streams over lossy channels,” in *Proc. IEEE Security Privacy*, 2000, pp. 56–73.

[29] K. Sampigethaya and R. Poovendran, “Privacy of future air traffic management broadcasts,” in *Proc. IEEE/AIAA 28th Digit. Avionics Syst. Conf.*, Oct. 2009, pp. 6.A.1-1–6.A.1-11.

[30] T.-C. Chen, “An authenticated encryption scheme for automatic dependent surveillance-broadcast data link,” in *Proc. Cross Strait Quad Regional Radio Sci. Wireless Technol. Conf.*, 2012, pp. 127–131.

[31] E. Valovage, “Enhanced ADS-B research,” in *Proc. IEEE/AIAA 25th Digit. Avionics Syst. Conf.*, 2006, pp. 1–7.

[32] R. Robinson *et al.*, “Impact of public key enabled applications on the operation and maintenance of commercial airplanes,” in *Proc. 7th AIAA ATIO Conf. 2nd CEIAT Int. Conf. Innov. Integr. Aero Sci. 17th LTA Syst. Tech. Conf. Followed 2nd TEOS Forum*, 2007, p. 7769.

[33] M. J. Viggiano, E. M. Valovage, K. B. Samuelson, and D. L. Hall, “Secure ADS-B authentication system and method,” U.S. Patent 7/730/307, Jun. 1, 2010.

[34] Z. Feng, W. Pan, and Y. Wang, “A data authentication solution of ADS-B system based on X.509 certificate,” in *Proc. 27th Int. Congr. Aeronaut. Sci. (ICAS)*, 2010, pp. 1–6.

[35] A. Shamir, *Identity-Based Cryptosystems and Signature Schemes*. Berlin, Germany: Springer, 1984.

[36] H. Yang *et al.*, “An efficient broadcast authentication scheme with batch verification for ADS-B messages,” *KSII Trans. Internet Inf. Syst.*, vol. 7, no. 10, pp. 2544–2560, 2013.

[37] 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.

[38] Y. Zheng, H. Duan, and C. Wang, “Learning the truth privately and confidently: Encrypted confidence-aware truth discovery in mobile crowdsensing,” *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 10, pp. 2475–2489, Oct. 2018.

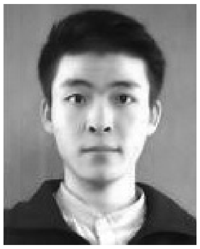
[39] Y. Zheng, H. Duan, X. Yuan, and C. Wang, “Privacy-aware and efficient mobile crowdsensing with truth discovery,” *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2017.2753245.

[40] S. Zhang *et al.*, “Verifiable outsourcing computation for matrix multiplication with improved efficiency and applicability,” *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2867113.

[41] H. Li *et al.*, “Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data,” *IEEE Trans. Cloud Comput.*, to be published, doi: 10.1109/TCC.2017.2769645.

Haomiao Yang (M’13) received the M.S. and Ph.D. degrees in computer applied technology from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2004 and 2008, respectively.

He was a Post-Doctoral Fellow with the Research Center of Information Cross Over Security, Kyungil University, Gyeongsan, South Korea, from 2012 to 2013. He is currently an Associate Professor with the School of Computer Science and Engineering and Center for Cyber Security, UESTC. His current research interests include cryptography, cloud security, and cyber security for aviation communication.



Qixian Zhou received the B.S. degree in biomedical engineering from Southwest Medical University, Luzhou, China. He is currently pursuing the M.S. degree in computer science at the University of Electronic Science and Technology of China, Chengdu, China.

His current research interests include big data security and artificial intelligence security.

Mingxuan Yao received the B.S. degree in information security from the University of Electronic Science and Technology of China, Chengdu, China. He is currently pursuing the M.S. degree at the Department of Computer Science, Georgia Institute of Technology, Atlanta, GA, USA.

His current research interests include CTF platform and applied cryptography, including ADS-B NextGen surveillance.

Rongxing Lu (S’99–M’11–SM’15) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2012.

He was a Post-Doctoral Fellow with the University of Waterloo from 2012 to 2013. He was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2013 to 2016. He has been an Assistant Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Fredericton, NB, Canada, since 2016. He has been published extensively. His current research interests include applied cryptography, privacy enhancing technologies, and IoT-big data security and privacy.

Dr. Lu was a recipient of the most prestigious Governor General’s Gold Medal, the 8th IEEE Communications Society (ComSoc) Asia–Pacific Outstanding Young Researcher Award in 2013, eight Best (Student) Paper Awards from some reputable journals and conferences, and the 2016–2017 Excellence in Teaching Award from FCS, UNB. He currently serves as the Vice-Chair (Publication) of IEEE ComSoc Communications and Information Security Technical Committee. He is currently a Senior Member of the IEEE Communications Society.

Hongwei Li (M’12) received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2008.

He is a Professor with the University of Electronic Science and Technology of China. He was a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, from 2011 to 2012. His current research interests include network security, applied cryptography, and trusted computing.

Dr. Li serves as an Associate Editor for IEEE INTERNET OF THINGS JOURNAL, and *Peer-to-Peer Networking and Applications* and as the Guest Editor for *Peer to-Peer Networking and Applications* “Special Issue on Security and Privacy of P2P Networks in Emerging Smart City.”

Xiaosong Zhang received the M.S. and Ph.D. degrees in computer science from the University of Electronic Science and Technology of China, Chengdu, China, in 1999 and 2011, respectively.

He is currently a Professor with the College of Computer Science and Engineering and the Center for Cyber Security, University of Electronic Science and Technology of China. His current research interests include cryptograph, software reliability, software vulnerability discovering, software test case generation, and reverse engineering.