2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) | 978-1-6654-9425-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/TrustCom56396.2022.00143

A Compatible and Identity Privacy-preserving Security Protocol for ACARS

Xinwei Li*, Qianyun Zhang*, Lexi Xu†, Tao Shang*
*School of Cyber Science and Technology, Beihang University, Beijing 100191, China
†Research Institute, China United Network Communications Corporation, Beijing 100048, China
E-mail: zhangqianyun@buaa.edu.cn

***Abstract*—Aircraft Communications Addressing and Reporting System (ACARS) has been widely used in aviation datalink. However, for lack of security designs, ACARS faces increasing security threats such as eavesdropping and message injection. Although several security solutions has been proposed on aviation surveillance message, such as Automatic Dependent Surveillance-Broadcast, those on ACARS have received far less attention. To further improve the session security and privacy of civil aviation users, we put forwards a compatible protocol for ACARS datalink to protect message security as well as aircraft identity privacy. The proposed solution provides communication confidentiality, and supports data integrity and user identity verification. Meanwhile, by replacing the aircraft's identity transmitted in plaintext with a variable anonymity, the privacy of an aircraft is protected from the disclosure of aircraft identity. Moreover, our protocol is compatible with current ACARS standards, making the proposed solution easy-to-deploy and practical. Formal analysis and simulations are carried out to make sure the security of proposed protocol.**

***Index Terms*—Aircraft Communications Addressing and Reporting System (ACARS), aviation communication security, privacy protection**

I. Introduction

ACARS, a digital datalink system for transmission of short messages between aircrafts and ground stations via airband radio or satellite, has become one of the most widely-used datalink protocols in modern aviation [1]. However, the ACARS is particularly vulnerable to attacks because of the lack of security consideration when the ACARS protocol was designed [2]. Until now, in most parts of the world, ACARS message is transmitted in plaintext without any cryptographic protection. With the development of radio technology, ACARS messages can be easily parsed or generated using low-cost radio hardwares and open source programs, and attackers can monitor the commercial or private aircrafts in real time through online websites and applications [3], [4].

In the early days, the major concern of civil aviation safety is to avoid dangerous people boarding the aircraft and the attack on communication systems has not been extensively considered until the 9/11 attack [5]. Over last decades, efforts has been carried out on ground-to-air datalink security. The problem of leaking passenger privacy and the possibility of inferring commercial secrets from the flight route and passenger identities was discussed in [6]. Potential security challenges from wireless networks were reviewed and a framework for security evaluation methodology was presented in [7].

Many studies has been conducted on the cryptographic solutions to security issues on air-to-ground datalink. To overcome the cost of public key infrastructure (PKI), identity-based cryptologic methods are introduced to aviation datalink security. Identity-based signatures (IBS) in [8]–[10] and identity-based encryptions (IBE) in [11] are proposed to achieve the authentication and confidentiality of aircraft Automatic Dependent Surveillance-Broadcast messages. However, such schemes require prior knowledge of the identifies of all communication participants, indicating that the identity privacy cannot be protected. Considering the fixed bit length of aviation communication data packets, format preserving encryption (FPE) is adapted for aviation datalink privacy protection in [12], [13]. Based on the loose time synchronization between the sender and receiver, Time Efficient Stream Loss-tolerate Authentication (TESLA) has the prospect of being applied to broadcast ground-to-air datalinks [13]. A standard-compliant and loss tolerant security ADS-B communication framework called Securing Open Skies (SOS) was proposed in [14]

In addition, non-cryptography methods are gradually introduced into the ground to air datalink security. To solve the problem of location forgery of ADS-B, H. Yang proposed an accurate and efficient aircraft location verification (AEALV) for ADS-B to quickly identify the legitimacy of the aircraft by verifying the claimed location of the aircraft to verify the location information [15]. ADS-B message can be authenticated by specific emitter identification in [16]. A physical unclonable function (PUF) mutual authentication key exchange (PMAKE) scheme based on challenge response was preliminary evaluated suitable for L-band digital aeronautical communication system [17].

In the early 2000s, some initial attempts to protect the privacy and authentication of ACARS began to emerge. These works described architectures to protect the confidentiality and authentication of ACARS message. Communication, Navigation and Surveillance/Air Traffic Management (CNS/ATM) and Security ACARS are early protocols for ACARS security [18], [19]. To take advantage of the benefits of both asymmetric and symmetric schemes, hybrid scheme was adapted to solve the security concerns on confidentiality, authentication and integrity [20]. The first relatively complete work to secure

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61901020; in part by the CAAC Safety Capacity Building Fund under Grant 25400002021102001; and in part by the Young Elite Scientists Sponsorship Program by CAST under Grant 2021QNRC001.

2324-9013/22/$31.00 ©2022 IEEE
DOI 10.1109/TrustCom56396.2022.00143

communication systems on ACARS came from the U.S. Air Force. It developed ACARS Message Security (AMS), a security version of ACARS ensuring confidentiality and authenticity in ARINC 823 standard in 2007 [21]. Although AMS provides strong confidentiality and authentication mechanism, it hasn't been widely used in civil aviation. One possible reason is adopting AMS in civil aviation may cause a dramatic traffic increment beyond the datalink capacity [5].

However, the aforementioned solutions on aviation datalink did not provide protection on confidentiality, authentication, integrity and identity privacy at the same time, and few studies have been carried out on ACARS datalink. In this paper, we proposed a compatible cryptographic solution to ACARS datalink security concerns. The proposed protocol provides protections on the confidentiality, authentication and integrity of messages, as well as the identity privacy of flights. Meanwhile, variable anonymized identities prevent attackers from inferring aircraft identities from collecting data over long periods of time. The security of this protocol has been demonstrated. The formal analysis of the proposed protocol has been done using BAN logic, and evaluated the security using AVISPA.

II. Security Model

ACARS message frame format is shown in Table I according to the current ARINC 618 standard [1]. The message plaintext is stored in the Text field. Flight ID represents the flight number of an aircraft , showing the aircrafts' flying routes for passengers. The Aircraft Registration Number (ARN) indicates aircraft's unique identity in the air traffic control department. Since the fields of Flight ID and Text are adjacent, for convenience, we refer to the Flight ID and the Text collectively as Text in the subsequent descriptions.

TABLE I
ACARS message frame format in ARINC 618 [1]

Field Name	SOH	Mode	ARN	TAK	Label	DBI	STX
Length	1	1	7	1	2	1	1
Example	<SOH>	2	..B1120	<NAK>	5Z	3	<STX>
Field Name	**MSN**	**FlightID**	**Text**	**Siffix**	**BCS**	**BCS Suffix**	
Length	4	6	0-210	1	2	1	
Example	M01A	CA5276	HELLO	<ETX>		<DEL>	

As mentioned in Section I, due to the lack of security considerations in current ACARS protocol, the sensitive information in ARN and Text field might be leaked to attackers, and the attackers can also generate forged ACARS messages to interfere with the aircraft and ground station. We abstract a threat model from the ACARS scenario as Fig. 1. The model can capture two different types of attacks: passive attack and active attack.

Passive Attack: Eavesdropping and aircraft reconnaissance attacks are categorized as passive attacks. ACARS adapted in civil aviation systems sends plaintext information over an unencrypted wireless channel with a public-available character encoding protocol. Aviation privacy was defined in [22] as existence, intention, status, and passenger/cargoinformation. A

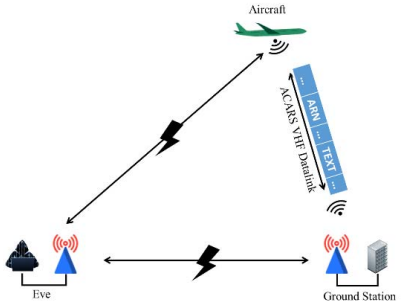

Fig. 1. Security Model of ACARS.

third-party attacker can easily receive and parse the message using RF receivers. So eavesdropping is the most immediate weakness of ACARS. The intruders directly obtain reports from aircrafts and instructions from ground stations through eavesdropping, causing disclosure of passenger privacy. Moreover, intruders can even deduce political and business secrets simply by learning that a certain plane is in a certain place without message text.

Active attacks: Message injection, message modification and reply attack are common active attacks. Due to the absence of authentication schemes in ACARS, attackers can construct legitimate fake messages and inject fake messages into existing air traffic communications [23]. Attackers send packets that have already been received by the destination host for the purpose of spoofing the system, and this replay attack can also cause the air traffic control departments and pilots to misjudge the airspace situation.

III. Protocol Design

A. Design Goals

To defense against aforementioned threats, this work focuses on providing confidentiality, integrity, and authentication to ACARS messages, and at the same time, persevering aircraft identity privacy.

Confidentiality means that message text can be prevented from disclosing to unauthorized users and entities. The plaintext can only be acquired by authorized flights and ground stations. Integrity ensures that the received ACARS message is not modified or lost during transmission. In our proposed scheme, integrity protection is realized through message authentication code (MAC) and digital signature mechanism. In ACARS, authentication guarantees that the message comes from legal flights or ground stations. Identity privacy means that the real identity of aircraft shouldn't be inferred by attackers. To achieve the identity privacy, ARN field in ACARS message is encrypted. Our solution must be compatible with existing ACARS systems in order to have the potential for large-scale applications.

B. Protocol Description

In order to balance the security and the efficiency, we adapt symmetric keys in sessions to encrypt message texts and gen-

erate MACs to protect the authentication and confidentiality of messages. To achieve the secure delivery of symmetric session keys, we constructed a session establishment protocol for ground stations and aircraft with asymmetric crypto and time stamps. To manage the public keys and certificates, a public key infrastructure (PKI) is used in the protocol relying on the trust of users to those certificate authority (CA). In aviation datalink, approved users include aircraft, controllers and airline operation departments, and a user is only possible to gain others' public keys when it is associated with a valid certificate.

Symbols and functions used in the protocol are defined in Table II. The proposed ACARS ground-to-air datalink anonymous secure session protocol would be described in two stages: session establishment and downlink/uplink transmission . Ground stations and the aircrafts request each other's public key through the PKI in advance. The first time an aircraft enters the coverage of a ground station, the conversation would be established. When the session has been successfully established, they would communicate securely according to the downlink/uplink transmission protocol. Detailed descriptions about the proposed protocol are as follows.

TABLE II
SYMBOL DEFINITION

Symbols	Definitions
k_d	Symmetric key generated by the aircraft and passed to the ground station during session establishment
pk_F, pk_G	Public key of flights and ground stations
sk_F, sk_G	Private key of flights and ground stations
$ARN()$	Aircraft Registration Number, the unique identifier of aircraft
$AID()$	The anonymous identity of the aircraft
$HASH()$	Hash function
$SIG()$	Digital signature algorithm
$VER()$	Signature verification algorithm
$ENC(text, pk)$ $DEC(text, sk)$	Asymmetric encryption/decryption algorithm with public key pk or private key sk
$ENC(text, k_d, iv)$ $DEC(text, k_d, iv)$	Symmetric encryption/decryption algorithm with key k_d and initial vetor iv

1) Session Establish Protocol: The first time the aircraft enters the airspace covered by the ground station, the aircraft needs to exchange keys and parameters required for the session with the ground station to ensure the transmission of subsequent uplink or downlink messages. Session establishment is the key of achieving ACARS session security.

Step 1: Ground station informs the aircrafts in the airspace of its identity. According to the provisions of the ARINC 618 standard [1], the ground station broadcasts its identity at regular intervals. After receiving the signal, the passing aircrafts begin to establish a session with the ground station. We use F and G to represent the flight and the ground station, respectively. This progress can be represented as `Message 1:`

$$G \rightarrow F : ID_G \tag{1}$$

Step 2: The aircraft initiates a request for session establishment, delivering keys and other parameters to the ground station. a) The aircraft confirms the identity of the airspace ground station by ID_G, and find its pk_G from the certificate database. b) The aircraft generates an initial vector iv_0 and session key k_d, and at the same time records the timestamp t of the moment. c) During the session establishment stage, the anonymous identity of the aircraft is calculated using a public key cryptographic algorithm as $AID = ENC(ARN, k_d)$. d) The aircraft then generates a signature with its private key $\Gamma_1 = SIG(iv_0||k_d||t||ARN, sk_F)$. e) The aircraft encrypt symmetric key, parameters and the signature with the aircraft's public key by $C_1 = ENC(iv_0||k_d||t||\Gamma_1, pk_G)$. f) Original ARN field is replaced by the anonymous identity (AID) generated before. C_1 is also filled into the Text field for sending. This process can be represented as `Message 2:`

$$F \rightarrow G : \{\{k_d, t, ARN\}k_F^{-1}, k_d, t\}_{k_G}, \{ARN\}_{k_d} \tag{2}$$

Step 3: The ground station processes the request from the aircraft to obtain session key and the aircraft's identities. If the validation is passed, the ground station responds to the aircraft's request. a) After receiving a message from flight, the ground station first decrypt C_1 with its private key sk_G to obtain the session key k_d, the initial vector iv_0, the timestamp t, and the signature ARN: $iv_0||k_d||t||\Gamma_1 = DEC(C_1, sk_G)$. b) Take the AID from the ARN field and decrypt the flight's ARN plaintext $ARN = DEC(AID, k_d)$. c) The ground station obtains the public key of the flight pk_F from the certificate database through ARN, and verifies the message signature $VER(iv_0||k_d||t||ARN, \Gamma_1, pk_F)$. d) If successfully verified, with the current time t_1, the ground station verifies the freshness of the timestamp t by checking whether the delay between t and t_1 is within a reasonable range $t_1 - t < T_0$. If the verification fails, the ground station discards this message and waits for a new one. e) If the freshness verification passes, the ground station generates a signature from t, ARN, iv_0 and k_d by calculating $\Gamma_2 = SIG(t||ARN||iv_0||k_d, sk_G)$. The signature value Γ_2 is put into the Text field, and the ARN field is replaced by AID. Then, the ground station sends it back to the aircraft. This process can be represented as `Message 3:`

$$F \rightarrow G : \{t, ARN, k_d\}_{k_G^{-1}} \tag{3}$$

f) The ground station predicts N anonymous identities to be used by the aircraft during the session through calculating $AID_i = ENC(iv_{0i}, k_d, ARN)$, in which initial vectors are calculated by $iv_{0i} = iv_0 + i, 1 \leq i \leq N$. the process of generating an anonymous identity is shown in Fig. 2.

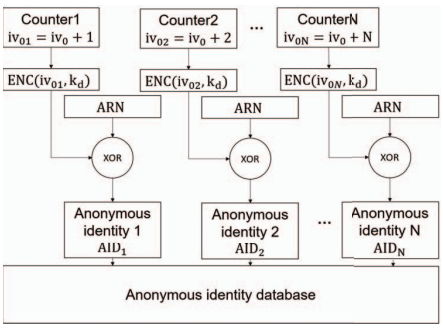

Fig. 2. Generating the anonymous identity database of the aircraft through symmetric cryptography.

Step 4: a) The aircraft fetches the signature Γ_2 from the message sent back by the ground station, and then verify the message signature pair $VER(t||ARN||iv_0||k_d, \Gamma_2, pk_G)$. A positive verification result indicates that the ground station is ready for a conversation with the flight. b) The flight calculates the N anonymous identities to be used during the session by $AID_i = ENC(ARN, k_d, iv_{0i})$, where $iv_{0i} = iv_0 + i, 1 \leq i \leq N$.

Fig. 3 shows the session establishment protocol scheme.

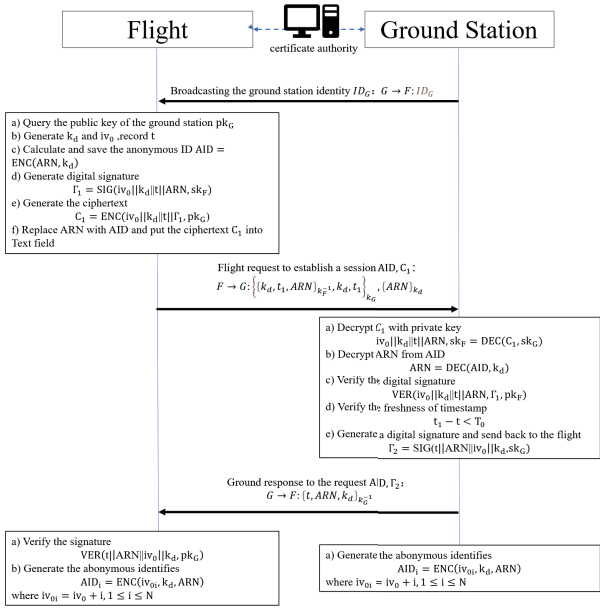

Fig. 3. Schematic diagram of the session establishment protocol.

2) Transmission protocol: After the session has been successfully established, both the ground station and the aircraft obtain or generate the initial vector, session key, anonymous identity database and other parameters required for the session. Taking downlink as an example, this section describes message transmission of the ACARS anonymous secure session protocol on the basis of the original ACARS protocol.

Step 1: In the downlink messages, flight sends an ACARS message to the ground station. a) The flight generates the message plaintext M_1 and the message sequence number MSN_1 according to the ARINC 618 standard, and then calculates the hash value $H_1 = HASH(M_1||MSN_1)$. b) According to the sequence number MSN_1 transmitted in plaintext, the initial vector of this message is calculated as $iv_i = HASH(iv_0||MSN_1)$. c) Then, the flight generates ciphertext $C_1 = ENC(M_1||H_1, k_d, iv_i)$. d) The flight randomly selects an anonymous identity AID_i from the anonymous identity database to replace the original ARN, and then fills the ciphertext C_1 into the Text field and transmits the message. This process can be represented as `Message 4`:

$$F \rightarrow G : \{M_1, hash(M_1||MSN_1)\}_{k_d}, ARN_{k_d} \quad (4)$$

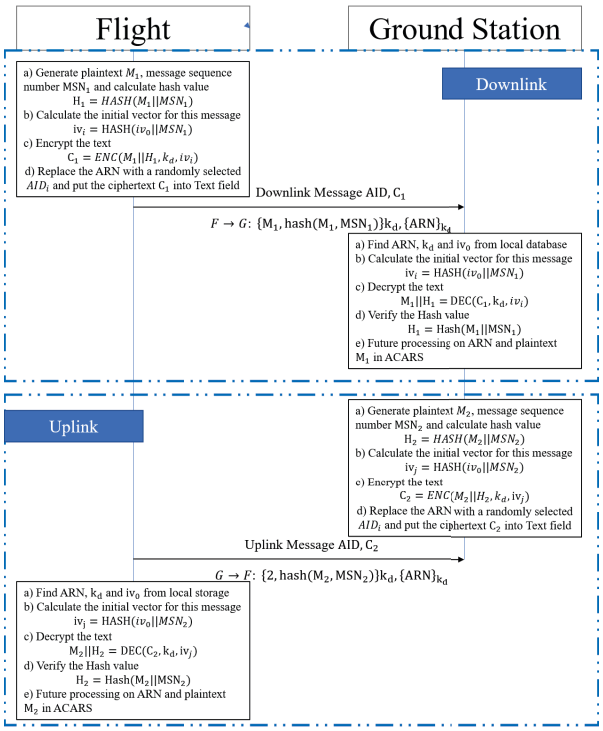

Fig. 4. Schematic diagram of the session transmission protocol.

Step 2: a) When the ground station receives a downlink message, the ground station performs the following procedures. The anonymous identity AID in ARN field should be checked firstly to recognize whether this flight has finished the session establishment protocol. Normally, the ground station can find the AID from the pre-calculated anonymous identity database, and query the original ARN as well as the initial vector iv_0 and key k_d of the flight from local storage. b) Ground station then calculates the initial vector of this message $iv_i = HASH(iv_0||MSN_1)$. The MSN_1 in plain text can be read directly from message. c) Ground station decrypts the cyphertext $M_1||H_1 = DEC(C_1, k_d, iv_i)$. d) After decryption, the ground station verifies the hash value $H_2 = Hash(M_1, ||MSN_1)$. e) If the hash function is verified successfully, the ground station sends the original ARN and the plaintext to the next level of ACARS system for future processing.

The uplink transmission procedure is similar to the downlink. The transmission protocol is shown in Fig. 4.

IV. Security Analysis and Performance Evaluation

In this section, formal analysis of the protocols has been carried out. The proposed session establishment protocol with the desired authentication and secrecy goals is verified using formal analysis based on Burrows, Abadi, and Needham

(BAN) Logic [24], and the whole protocol is simulated in Automated Validation of Internet Security Protocols and Applications (AVISPA).

A. Formal Analysis with BAN Logic

Notations in BAN logic is defined in Table III. We idealize

TABLE III
SYMBOL DEFINITIONS IN BAN LOGIC

Notation	Definition
$P \overset{k}{\leftrightarrow} G$	P and Q have a shared key
$\overset{k_P}{\rightarrow} P$	the public key of P
$P \mid \equiv MSG$	P believes the message MSG
$P \mid \sim MSG$	P once said the message MSG
$P \Rightarrow MSG$	P controls the message MSG
$P \lhd MSG$	P received the message MSG
$\#(MSG)$	the message MSG is fresh
$\{MSG\}_k$	MSG is encrypted by the shared key k
$\{MSG\}_{pk}$	MSG is encrypted by the public key pk
$\{MSG\}_{pk^{-1}}$	MSG is signed by the private key pk^{-1}

the proposed session establishment protocol as (2) and (3).

Goals of BAN logical analyses include both primary and secondary beliefs. In the protocol, due to parameters $F \overset{k_d}{\leftrightarrow} G$ and ARN are generated by F, proofs on the expressions $F \mid \equiv F \overset{k_d}{\leftrightarrow} G$ and $F \mid \equiv ARN$ are not necessary. Goals to be proven in the protocol are listed in Table IV.

TABLE IV
ANALYSIS GOALS OF THE PROPOSED PROTOCOL

Goals	Expression
GOAL1	$G \mid \equiv F \overset{k_d}{\leftrightarrow} G$
GOAL2	$G \mid \equiv ARN$
GOAL3	$F \mid \equiv G \mid \equiv F \overset{k_d}{\leftrightarrow} G$
GOAL4	$F \mid \equiv G \mid \equiv ARN$
GOAL5	$G \mid \equiv F \mid \equiv F \overset{k_d}{\leftrightarrow} G$
GOAL6	$G \mid \equiv F \mid \equiv ARN$

According to the proposed protocol, we have the following initial assumptions as demonstrated in Table V.

TABLE V
INITIAL ASSUMPTIONS IN THE PROPOSED PROTOCOL

Assumptions	Expression
Assump.1	$G \mid \equiv \overset{k_F}{\rightarrow} F$
Assump.2	$F \mid \equiv \overset{k_G}{\rightarrow} G$
Assump.3	$F \Rightarrow F \overset{k_d}{\leftrightarrow}$
Assump.4	$F \Rightarrow ARN$
Assump.5	$G \mid \equiv F \Rightarrow F \overset{k_d}{\leftrightarrow} G$
Assump.6	$G \mid \equiv F \Rightarrow ARN$
Assump.7	$F \mid \equiv \#(t)$
Assump.8	$G \mid \equiv \#(t)$

From (2), according to the BAN inference rule

$$\frac{G \mid \equiv \overset{k_G}{\rightarrow} G, G \lhd \{\{k_d, t, ARN\} k_F^{-1}, k_d, t\}_{k_G}}{G \lhd \{k_d, t, ARN\} k_F^{-1}, k_d, t} \tag{5}$$

$$\frac{G \mid \equiv \overset{k_F}{\rightarrow} F, G \lhd \{k_d, t, ARN\} k_F^{-1}}{G \mid \equiv F \mid \sim k_d, t, ARN} \tag{6}$$

From **Assump.7**, we can see

$$\frac{G \mid \equiv \#(t)}{G \mid \equiv \#(k_d, t, ARN)} \tag{7}$$

According to (6) and (7)

$$\frac{G \mid \equiv \#(k_d, t, ARN), G \mid \equiv F \mid \sim k_d, t, ARN}{G \mid \equiv F \mid \equiv k_d, t, ARN} \tag{8}$$

From which we can derive $G \mid \equiv F \mid \equiv \{k_d, ARN\}$. This indicates that **GOAL5** and **GOAL6** are satisfied. k_d is the shared secret between F and G, thus k_d can be written as $F \overset{k_d}{\leftrightarrow} G$. From the initial assumption **Assump.5** and **Assump.6**,

$$\frac{G \mid \equiv \{F \Rightarrow F \overset{k_d}{\leftrightarrow} G, ARN\}, G \mid \equiv F \mid \equiv \{k_d, ARN\}}{G \mid \equiv F \overset{k_d}{\leftrightarrow} G, ARN} \tag{9}$$

GOAL1 and **GOAL2** are achieved.

From (3), **Assump.1** and **Assump.7**, we have

$$\frac{F \rightarrow G : \{t, ARN, k_d\}_{k_G^{-1}}, F \mid \equiv \overset{k_G}{\rightarrow} G}{F \mid \equiv G \mid \sim t, ARN, k_d} \tag{10}$$

$$\frac{F \mid \equiv \#(t)}{F \mid \equiv \#(t, ARN, k_d)} \tag{11}$$

$$\frac{F \mid \equiv G \mid \sim \{t, ARN, k_d\}, F \mid \equiv \#(t, ARN, k_d)}{F \mid \equiv G \mid \equiv t, ARN, k_d} \tag{12}$$

With $\frac{F \mid \equiv G \mid \equiv t, ARN, k_d}{F \mid \equiv G \mid \equiv ARN, k_d}$, **GOAL3** and **GOAL4** are satisfied. The formal analysis with BAN logic on the session establishment protocol achieves all beliefs on the flight identity and the session key. Therefore, the security of the session establishment has been guaranteed.

B. Simulation in AVISPA

In this subsection, AVISPA, a security simulation tool providing various attacks [25], is adapted to evaluate the security level of the proposed aviation session establishment and transmission protocols. The secrecy and authentication of the session secret key k_d and flight identity privacy ARN are realized in session establishment process . The secrecy and authentication of the transmitted message text msg and the flight identity privacy ARN are achieved.

C. Performance evaluation

In this subsection, we compare the proposed security scheme with existing approaches. Their performance on aviation datalinks are summarized in Table VI.

TABLE VI
SYMBOL DEFINITIONS IN BAN LOGIC

	Confidentiality	Authentication	Integrity	Identity Privacy
[8]	✓		✓	
[10]		✓	✓	
[13]		✓	✓	✓
[19]	✓			
[20]	✓	✓	✓	
[21]	✓	✓	✓	
[26]		✓	✓	
Proposed	✓	✓	✓	✓

As seen from the table, the proposed protocol completely guarantees the confidentiality, integrity and authentication of ACARS messages, as well as aircrafts identity privacy. Data

integrity is provided by the hash operation adapted with symmetric ciphers, which gives an unique solution for a specific input. Each aircraft shares a unique key with the ground station by asymmetric ciphers and hence different session keys guarantee the authentication of the message source. For the identity privacy, it is preserved by the anonymous identity database. For each session, aircrafts or ground stations randomly select anonymous identities from the database to replace the original ARNs, which creatively prevents the risk of aircraft identity privacy breach. Moreover, compared with the method in [21], variable anonymous identity avoids attackers from analyzing the aircraft through statistical characteristics. Meanwhile, the message sequence number prevents the possibility of reply attack.

V. Conclusion

Aiming to improve the aviation communication security, we designed an ACARS datalink anonymous secure session protocol including Session establishment and downlink/uplink transmission. Session establishment protocol guarantees a secure delivery of session key and parameters through asymmetric passwords, and the downlink/uplink protocol encrypts session messages with symmetric passwords combining MACs and digital signatures. Thus, confidentiality, integrity and authentication of the ACARS datalink are comprehensively guaranteed. Besides, the randomly selected anonymous identity protects the identity privacy and avoid attackers from targeting an aircraft through long-term eavesdropping. Security of the proposed protocol has been proven by both formal analysis and simulations. In addition, to ensure the compatibility of the proposed protocol, the encrypted ACARS message frame format is maintained the same as ACARS standard, and therefore supporting practical deployment of the security solution.

References

[1] Aeronautical Radio Inc. (ARINC). 618-7: Air/Ground Character-Oriented Protocol Specication. Technical Standard. 2013.

[2] M. Smith, D. Moser, M. Strohmeier, V. Lenders and I. Martinovic, “Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS,” in Proceedings of International Conference on Financial Cryptography and Data Security, Malta, Apr. 2017, pp. 105-122.

[3] FlightAware. Global Flight Tracking, 2017. URL https: //uk.flightaware.com/commercial/global. Retrieved on 2022-05-03.

[4] Flightradar24 AB. Flightradar24, 2017. URL https://www. flightradar24.com. Retrieved on 2022-05-03.

[5] C. Bresteau, S. Guigui, P. Berthier and J. M. Fernandez, “On the security of aeronautical datalink communications: Problems and solutions,” in Proceedings of Integrated Communications, Navigation, Surveillance Conference (ICNS), Herndon, VA, USA, Apr. 2018, pp. 1A4-1-1A4-13.

[6] M. Smith, D. Moser, M. Strohmeier, V. Lenders, I. Martinovic, “Undermining privacy in the aircraft communications addressingand reporting system (ACARS),” in Proceedings of Privacy Enhancing Technologies, Barcrlona, Spain, Jun. 2018, pp. 105–122.

[7] K. Sampigethaya, R. Poovendran and L. Bushnell, “Secure Operation, Control, and Maintenance of Future E-Enabled Airplanes,” in Proceedings of the IEEE, vol. 96, no. 12, pp. 1992-2007, Dec. 2008.

[8] J. Baek, Y. Byon, E. Hableel and M. Al-Qutayri, “An Authentication Framework for Automatic Dependent Surveillance-Broadcast Based on Online/Offline Identity-Based Signature”, in Proceedings of Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Compiegne, France, Oct. 2013, pp. 358-363.

[9] 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. 686–688, Mar. 2014.

[10] A. Yang, X. Tan, J. Baek, and D. S. Wong, “A New ADS-B Authentication Framework Based on Efficient Hierarchical Identity-based Signature with Batch Verification,” *IEEE Trans. Services Comput.*, vol. 10, no. 2, pp. 165–175, Mar./Apr. 2017.

[11] J. Baek, E. Hableel, Y. Byon, D. S. Wong, K. Jang and H. Yeo, “How to Protect ADS-B: Confidentiality Framework and Efficient Realization Based on Staged Identity-Based Encryption,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 690-700, Mar. 2017.

[12] C. Finke, J. Butts, R. Mills, and M. Grimaila, “Enhancing the security of aircraft surveillance in the next generation air traffic control system,” *Int. J. Crit. Infrastruct. Protection*, vol. 6, no. 1, pp. 3–11, Mar. 2013.

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

[14] S. Sciancalepore and R. Di Pietro, ”SOS: Standard-Compliant and Packet Loss Tolerant Security Framework for ADS-B Communications,” in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 4, pp. 1681-1698, 1 July-Aug. 2021.

[15] H. Yang, Q. Zhou, D. Liu, H. Li and X. Shen, ”AEALV: Accurate and Efficient Aircraft Location Verification for ADS-B,” in *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 4, pp. 1399-1411, Dec. 2021.

[16] N. Jiang, S. Qi, F. Luo, W. Jun and W. Wang, ”ADS-B Message Authentication Using Features of Signal in Transition Regions,” 2019 IEEE International Conference on Signal, Information and Data Processing (ICSIDP), 2019, pp. 1-5.

[17] N. Mäurer, T. Gräupl, C. Schmitt and G. D. Rodosek, ”PMAKE: Physical Unclonable Function-based Mutual Authentication Key Exchange Scheme for Digital Aeronautical Communications,” 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021, pp. 206-214.

[18] McParland, Thomas, 2001, CIVS/ATM Package-II Standards and Recommended Practices (SAMs), Sub- Volume VIII - ATN Security Services, Draft, Tokyo, Japan, ICAO.

[19] A. Roy, “Secure aircraft communications addressing and reporting system (ACARS),” in Proceedings of 20th Digital Avionics Systems Conference, Daytona Beach, FL, USA, Oct. 2001, vol. 2, pp. 7A2/1-7A2/11.

[20] C. Risley, J. McMath and B. Payne, “Experimental encryption of aircraft communications addressing and reporting system (ACARS) aeronautical operational control (AOC) messages,” in Proceedings of 20th Digital Avionics Systems Conference, Daytona Beach, FL, USA, vol. 2, Oct. 2001, pp. 7D4/1-7D4/8.

[21] Aeronautical Radio Inc. (ARINC). Datalink Security, Part1 - ACARS Message Security. Technical Standard 823P1, 2007.

[22] M. Smith, M. Strohmeier, V. Lenders and I. Martinovic, ”On the security and privacy of ACARS,” 2016 Integrated Communications Navigation and Surveillance (ICNS), 2016, pp. 1-27.

[23] M. Schäfer, V. Lenders, and I. Martinovic, “Experimental analysis of attacks on next generation air traffic communication,” in Proceedings of Applied Cryptography and Network Security. Banff, AB, Canada, Feb. 2013, pp. 253-271.

[24] M. Burrows, M. Abadi, and R. Needham, “A logic of authentication,” *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[25] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron, “The AVISPA tool for the automated validation of internet security protocols and applications,” in Proceedings of International Conference on Computer Aided Verification, Scotland, U.K., Jul. 2005, pp. 281–285.

[26] Z. Wu, A. Guo, M. Yue and L. Liu, “An ADS-B Message Authentication Method Based on Certificateless Short Signature,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 3, pp. 1742-1753, Jun. 2020.