Backward-compatible Software Upgrades for ADS-B and AIS To Support ECDSA-Secured Protocols

Ahsan Saleem, Hannu Turtiainen, Andrei Costin and Timo Hämäläinen
Faculty of Information Technology, University of Jyväskylä, Jyväskylä, 40014 Finland

ahsan.m.saleem@jyu.fi
hannu.ht.turtiainen@jyu.fi
andrei.costin@jyu.fi
timo.t.hamalainen@jyu.fi

Abstract: During the past few decades, the aviation, maritime, aerospace, and search-and-rescue domains have witnessed tremendous improvement thanks to technological, digitalization and Internet of Things (IoT) advances such as Automatic Dependent Surveillance–Broadcast (ADS-B) (e.g., Aviation IoT, Airports IoT) and Automatic Identification System (AIS) (e.g., Maritime IoT). All these are high-profile examples of new digital communication protocols combined with IoT devices that make efficient use of wide-area earth and space radio communications to provide real-time, truly globally interoperable, and optimised services required by these domains. However, the protocols and technologies mentioned above, both from an architectural and implementation point of view, exhibit fundamental cybersecurity weaknesses (both at protocol and IoT device level). These weaknesses make them an easy target for potential attackers. The two fundamental flaws of these protocols are the lack of digital signatures (i.e., integrity and authenticity) and the lack of encryption (i.e., confidentiality and privacy). The risks associated with these, and other weaknesses have been over the last decade repeatedly demonstrated with ease by ethical cybersecurity researchers. In this paper, we design, propose, and discuss a single generic PKI-enabled message integrity and authenticity scheme that works seamlessly for any of the ADS-B, and AIS, with the possibility of easy extension and integration into other protocols (e.g., ACARS). Our scheme can be added as backward-compatible software upgrades (e.g., third-party library) to existing systems without requiring expensive architectural redesign, upgrades, and retrofitting. Our present work is aimed to serve as a bootstrap to securing such insecure protocols without completely replacing or redesigning the systems. It also aims to provide a discussion background of advantages and limitations of such backward-compatible securing methods.

Keywords: Cybersecurity, Protocol Upgrades, Message Authentication, ADS-B, 1090ES, AIS.

1. Introduction

In aviation, aircrafts periodically broadcast their aviation data using a surveillance technique known as Automatic Dependent Surveillance-Broadcast (ADS-B). Air Traffic Control (ATC) and other airplanes receive this data, providing them with situational awareness. Currently, there are insufficient security measures to ensure the privacy, availability, and integrity of transmitting data between aircraft and air traffic controllers (Kožović et al., 2023) (Manesh and Kaabouch, 2017) (Strohmeier et al., 2013) (Wu et al., 2020). Consequently, an attacker may insert fake data or stop actual data from being correctly delivered because no authentication mechanisms are used at the data connection layer (Costin and Francillon, 2012) (Khandker et al., 2021) (Khandker et al., 2022a) (Mäurer et al., 2022). Various security schemes have been proposed to secure ADS-B transmission messages, including symmetric cryptographic-based (Chen, 2012) (Kacem et al., 2015), identity-based signature algorithms (Thumbur et al., 2019) (Yi et al., 2022), time-efficient stream loss-tolerant authentication (TESLA) protocol (Yang et al., 2018) (Sciancalepore and Di Pietro, 2019), anonymous authentication schemes (Asari et al., 2021) (Jegadeesan et al., 2021) and blockchain-based schemes (Wu et al., 2023) (Habibi Markani et al., 2023).

In the maritime domain, vessel traffic services rely on the Automated Identification System (AIS) for automatic ship tracking. AIS is an open standard and due to unauthenticated and unencrypted nature make it vulnerable to threats such as spoofing, hijacking, and availability disruption (Balduzzi et al., 2014) (Hall et al., 2015) (Khandker et al., 2022b) (Tran et al., 2021). To secure AIS, several security schemes have been proposed, including anonymous authentication schemes (Goudosis and Katsikas, 2022) (Jegadeesan et al., 2021), TESLA protocol-based scheme (Sciancalepore et al., 2021) and blockchain based schemes (Duan et al., 2022) (Freire et al., 2022).

In this study, we proposed authentication and integrity schemes for ADS-B (aviation) and AIS (maritime) systems. Despite the different domains, the architecture, technologies, and protocols of the ADS-B and AIS systems exhibit noteworthy similarities. Security threats and the proposed cybersecurity solutions are similar. Therefore, we propose a scheme that addresses the security concerns of both protocols to secure in our study. There are core motivations for our work. First and foremost, the bulk of the existing proposed solutions are either theoretical (Costin and Francillon, 2012) (Chen, 2012b) or require complete/major system redesign and

replacement in the case of practically demonstrated solutions (Thumbur et al., 2019) (Yang et al., 2014) (Goudossis and Katsikas, 2019) (e.g. introduction of new sub-protocols). Second, even for practically feasible solutions (Yang et al., 2018) (Sciancalepore et al., 2021) (Wimpenny et al., 2022), the proposed solutions are not uniform across multiple technologies and/or customised for each technology stack (that is, ADS-B-only, AIS-only). This makes such solutions harder to maintain in the long run, brings more fragmentation to technology stacks, and increases the verification efforts of each individually customised approach. To address these limitations, we propose backward-compatible software only solution to provide stronger security to ADS-B and AIS protocols, which can easily be integrated with the existing systems and protocols.

Our main contributions with this work are as follows:

1. We propose backward-compatible and software-only message authentication and integrity approach for existing insecure protocols in aviation (ADS-B).
2. We also propose a backward-compatible and software-only message authentication and integrity scheme for maritime (AIS).
3. We provide a security analysis of the proposed scheme, which shows that the proposed scheme is secured under a defined security model.

2. Related Work

This section summarises the security and authentication-enhancing schemes previously proposed for ADS-B and AIS. Chen et al. (2012) proposed an ADS-B message confidentiality and authentication scheme based on block ciphers. Yang et al. (2015) proposed an ADS-B authentication batch verification scheme based on identity-based signature. Pan et al. (2012) proposed an elliptic curve cipher (ECC) and X.509 certificate-based authentication scheme for ADS-B. Thumbur et al. (2019) proposed an identity based authentication batch verification scheme for ADS-B. Yang et al. (2018) proposed confidentiality and integrity scheme for ADS-B transmission messages. Wu et al. (2019) proposed a certificate-less short signature-based authentication and integrity scheme for ADS-B. Asari et al. (2021) presented hierarchical authentication and integrity scheme of ADS-B data based on a certificate-less public key cryptographic technique. Yang et al. (2014) proposed an identity signature based authentication and integrity scheme for ADS-B. Prakash et al. (2019) proposed an authentication scheme for ADS-B based on message authentication code (MAC). Recently blockchain-based security schemes for ADS-B are proposed in (Wu et al., 2023) (Habibi Markani et al., 2023).

Sciancalepore et al. (2021) proposed an authentication scheme for AIS broadcast messages. Goudossis et al. (2019) proposed an authentication and integrity scheme for AIS, and in their follow-up work (Goudosis and Katsikas, 2020) addressed the implementation aspects of (Goudossis et al., 2019). Goudosis et al. (2022) proposed secure automatic identification system (SecAIS) that provides the authentication, confidentiality, and anonymisation of AIS messages. Wimpenny et al. (2022) proposed an elliptic curve based data integrity and authentication scheme for AIS. Su et al. (2017) proposed a digital certificate-based identity authentication scheme to ensure authentication and integrity of AIS data. Jegadeesan et al. (2021) proposed AIS anonymous authentication scheme. The blockchain-based authentication and integrity schemes for AIS are proposed in (Duan et al., 2022) (Freire et al., 2022).

2.1 Comparison with Existing Works

Our present work is the best compared with the following existing works. In the ADS-B field, the work (Yang et al., 2018) is closest to our approach. However, this scheme is based on the TESLA protocol for authentication, which cannot be practically used in real-time authentication scenarios owing to the core idea of a delayed authentication mechanism due to symmetric key generation and distribution challenges. While our proposed approach is a public key cryptographic algorithm-based scheme which is real-time, backward-compatible, practical authentication scheme. In the AIS field, the schemes proposed by (Sciancalepore et al., 2021) (Wimpenny et al., 2022) are closest to our approach. These schemes are either inherently delayed authentication mechanisms or use separate VHF data-exchange system (VDES) side channels to carry digital signatures, which require the installation of new VDES hardware on the transmitter and receiver sides. However, our AIS proposed approach is real-time and practical and retains backward compatibility by carrying a signature payload in a “New type” of message in follow-up AIS communication. Moreover, our foremost differentiator, compared with the closest related work, is that our scheme provides a generic approach that adds cryptographically strong message authenticity and integrity to all protocols (e.g. ADS-B and AIS) in a single implementation.

3. Preliminaries, Models and Goals

This section provides background knowledge and defines our systems models of ADS-B and AIS, as well as the security goals of the proposed scheme.

3.1 ADS-B Model and Message Format

The proposed ADS-B model is illustrated in Figure 1. ADS-B comprises two distinct communication subsystems: ADS-B OUT and ADS-B IN. In the proposed ADS-B model, an aircraft continuously transmits information regarding its altitude, velocity, and position through ADS-B OUT and ADS-B IN enables aircraft to receive nearby ADS-B messages transmitted by other aircraft or Air Traffic Control (ATC). The aircraft receives primary information from a navigation satellite, which is subsequently transmitted to another aircraft and the ATC through the ADS-B OUT. The receiver aircraft receives this information using an ADS-B IN and then processes and displays it in the aircraft's cockpit.

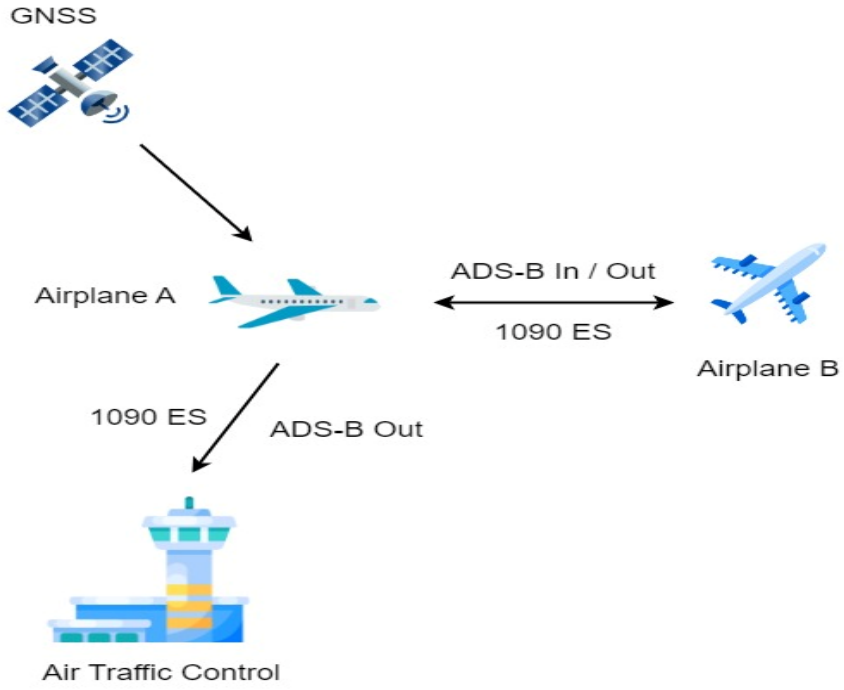

Figure 1: General ADS-B Model (simplified)

The ADS-B 112-bit message format, which consists of five fields, is illustrated in Figure 2.

5-bits	3-bits	24-bits	56-bits	24-bits
DF	CF	ICAO	ADS-B Data	Parity Bits

Figure 2: Long ADS-B 1090ES Message Format (112 bits)

3.2 AIS Model and Message Format

The proposed AIS model is shown in Figure 3, where vessels and the AIS control center exchange navigation information, such as identification and position data, using a Global Navigation Satellite System (GNSS). This allows for various uses, such as identifying ships, tracking them from a distance, changing routes, and preventing and investigating accidents.

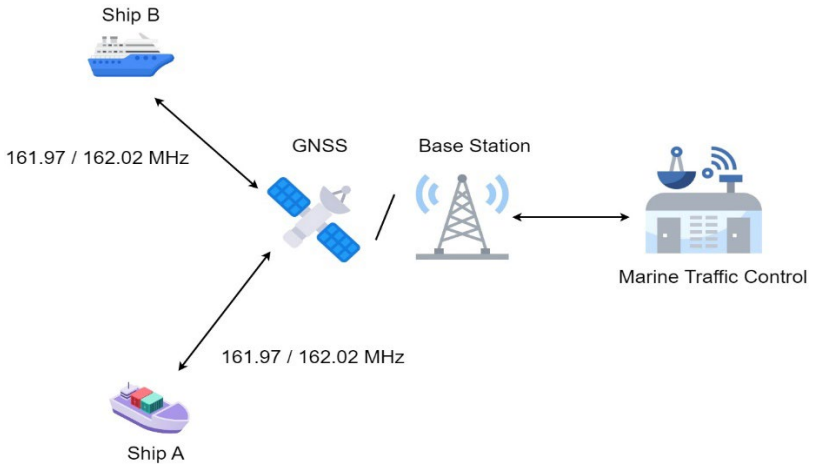

Figure 3: General AIS Model (simplified)

In AIS, channel A communication uses a frequency of 161.975 MHz, whereas channel B uses 162.025 MHz. AIS message has an overall size of 256 bits (International Telecommunication Union, 2014),and its format is shown in Figure 4.

8-bits	24-bits	8-bits	168-bits	16-bits	8-bits	24-bits
Ramp Up	Preamble	Start Flag	AIS Data	FCS	End Flag	Buffer

Figure 4: AIS Message Format (256 bits)

3.3 Threat Model and Security Goals

In adversary model, we assume that an adversary can intercept and modify the contents of the existing messages and may try to inject fake messages into the transmission channel following the ADS-B/AIS message format. In the absence of security measures, an adversary can intercept, retransmit, or delay transmitting messages, resulting in replay attacks. These attacker capabilities are realistic, as demonstrated by several studies (Costin and Francillon, 2012) (Khandker et al., 2021) (Khandker et al., 2022b) (Khandker et al., 2022a). These vulnerabilities enable eavesdropping, message injection, message modification, and replay attacks to occur. Moreover, the availability of low-cost software-defined radio (SDR) enables adversaries to launch these types of attacks.

In our proposed schemes, we aim to achieve the following security goals.

1. Message Authentication: Message authentication means that incoming data on the receiver side are from an authentic source and the receiver can verify the message origin. Our proposed schemes ensure source authentication of the messages and ensure that the messages originate from the authenticated transmitter or source.
2. Message Integrity: Message integrity of the received message means that no one has tampered with the transmitting messages, and any modification should be detected at the receiver side. Our proposed schemes ensure the integrity of the transmitted messages and can detect and filter out tampered messages.
3. Resistance to False Data Injection Attack: An attacker may try to insert false data into a legitimate message. Any false data injected by an attacker should be easily detected on the receiver side when our scheme is employed.
4. Prevention of Replay Attack: Replay attack means that an adversary maliciously intercepts and delays or retransmits messages to the receiver. The receiver must be able to detect and filter replay messages. The proposed schemes can efficiently detect and discard replay messages.
5. Strong Cryptographic Guarantees: For stronger security, we use ECDSA 256-bit key signature algorithm over the SHA-256 hash of the message. This provides strong future-proof guarantees while simultaneously minimising the digital signature output at the same time.

An attacker model in which adversaries become mobile is called a mobile attacker or a mobile adversary model (Shang, 2023). We did not consider this type of attack in our threat model, which is an interesting extension of our work, and we consider for future exploration. Additionally, other types of attacks, such as denial of service and jamming attacks, are possible against ADS-B and AIS; however, these attacks are outside the scope of this study.

3.4 Non-Security Goals

In addition to the security goals of our proposed scheme, we define the non-security goals of our schemes.

1. Backward Compatibility: This means that our schemes are software-only solutions and require no modification to existing protocols and hardware.
2. Single Generic Approach: The proposed schemes are software-only solutions, and we envision that our solution can work as a third-party library for upgraded systems. This will enable a single and generic code base that is easy to deploy and audit.
3. Minimum Communication Cost: For minimum communication cost, we consider a 512-bit length ECDSA signature algorithm in our scheme.

4. Proposed Solution

In this section, we describe ADS-B and AIS authentication scheme. The notations used in the proposed scheme are listed in Table 1.

Table 1: List of Notations

Symbol	Definition
G	Generator
k	Random number
R	Random point
$privKey$	Private key
$pubKey$	Public key
T_s	Timestamp
h	Hash digest
σ	Signature
df_m	DF (ADS-B) message
ais_m	AIS message

4.1 ADS-B Authentication

This section provides source authentication and message integrity for the ADS-B messages. The proposed scheme consists of two algorithms: *ADS-B Signature Generation and Encapsulation*, and *ADS-B Signature Verification and De-encapsulation*. For authentication and message integrity, we use the ECDSA signature scheme. To maintain backward compatibility and openness of the ADS-B message, transmitter transmit a signed message of an ADS-B message (e.g. DF11 or DF17, which are the most common ADS-B messages in general) encapsulated within an ADS-B DF24 ELM message that follows-up. In this way, the transmitter continues to transmit ADS-B normally and transmits the respective signed message in a follow-up message using the DF24 ELM message. The message field of the ADS-B DF24 ELM is of 80-bits, and a full signature cannot be accommodated within a single packet. Therefore, to accommodate the digital signature data, we used a built-in message-chaining mechanism available in the ADS-B DF24 ELM, which can chain up to 16 segments related to the same ADS-B DF24 communication.

The complete ADS-B authentication mechanism on the transmitter and receiver sides is illustrated in Figure 5. Given that the signature, timestamp, and ICAO take 600 bits, in practice, 8-chained DF24 ELM messages are required to transmit a digital signature of one standard ADS-B message.

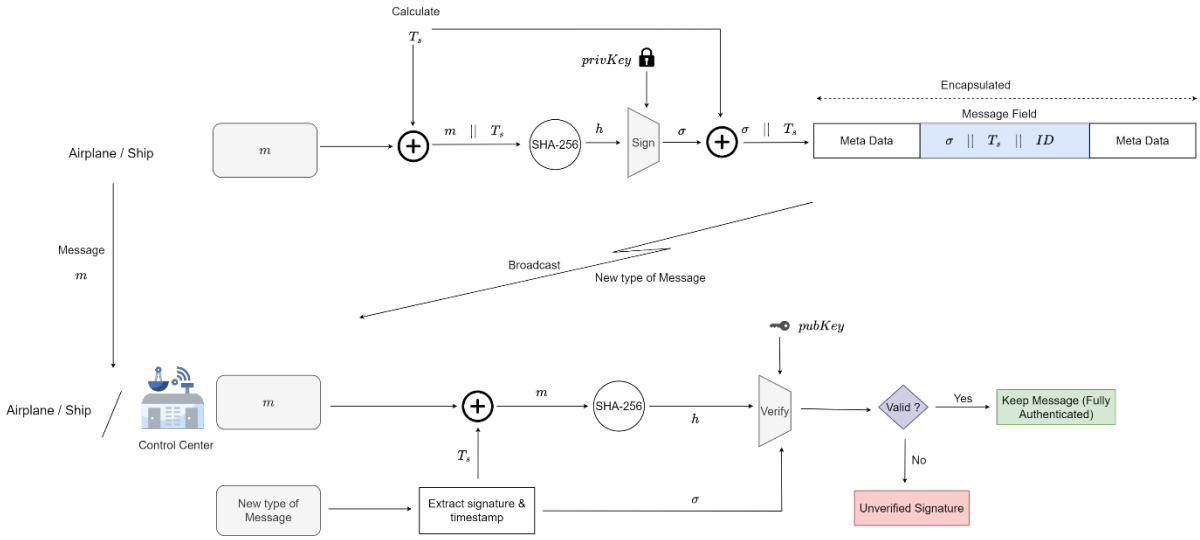

Figure 5: Our proposed Message authenticity and integrity scheme

4.1.1 ADS-B Signature Generation and Encapsulation

For ADS-B message signature generation and encapsulation of signed messages in the DF24 ELM message, transmitter used Algorithm 1. In the first step, it calculates timestamp T_s. Then the transmitter computes the hash digest $h = hash(df_m \vee T_s)$ of the full raw ADS-B 56bit or 112bit message (e.g., DF11 or DF17) concatenated with T_s using the hash algorithm $SHA - 256$. In next step, computes the signature σ of the hashed value h using $privKey$. To prevent a replay attack, timestamp T_s is concatenated with a signed message. The message field of the DF24 ELM is of 80-bits. Therefore, the chaining mechanism of DF24 is used to encapsulate the signed-message in the DF24 ELM and forward the "New type" of the ADS-B message to ATC.

Algorithm 1: ADS-B Signature Generation and Encapsulation

1: **procedure**

2: **Input:** ADS-B message df_m , $SHA - 256$, $privKey$

3: **Output:** Signature $\sigma = \{r, s\}$, Encapsulated DF24 ELM

4: Compute timestamp T_s

5: Calculate $h = hash(df_m \vee T_s)$ using $SHA - 256$

6: Computes signature proof $\sigma = (privKey, h)$

7: Concatenate signature with ID and timestamp $\sigma \vee T_s \vee ICAO$

8: Chaining signed message into 80-bits of the available payload of DF24 ELM

9: Transmit encapsulated DF24 ELM to ATC (or ADS-B IN aircraft/device)

10: **end procedure**

4.1.2 ADS-B Signature Verification and De-Encapsulation

ATC receives the encapsulated DF24 ELM from the sender and authenticates the message using Algorithm 2. The first step de-encapsulates the DF24 ELM message and obtains $\sigma \vee T_s$ from the message field. ATC computes the hash digest as $hash(df_m \vee T_s)$ using the received timestamp and already received message (e.g., DF11, DF17, or any other ADS-B DF message for that purpose). Finally, the receiver verifies the signature using $pubKey$ of the sender and successful verification shows that the message originated from an authenticated source, and no one has tampered with the received message. The timestamp binding with the signature prevents replay attacks.

Algorithm 2: ADS-B Signature Verification and De-encapsulation

1: **procedure**
2: **Input:** Encapsulated DF24 ELM, ADS-B message df_m , $SHA-256$, $pubKey$
3: **Output:** Authenticated data
4: De-encapsulate DF24 ELM message and get Signed message $\sigma \vee T_s \vee ICAO$
5: Calculate $h = hash(df_m \vee T_s)$ using $SHA-256$
6: Signature validation using Public Key $(pubKey, h, \sigma)$
7: **if** Signature is validated **then**
8: Keep received message (Fully Authenticated)
9: **else**
10: Possibly tampered/replayed, therefore UNVERIFIABLE
11: **end if**
12: **end procedure**

4.2 AIS Authentication

This section describes the proposed authentication and integrity scheme for AIS messages. The proposed AIS authentication scheme consists of two algorithms: *AIS Signature Generation and Encapsulation*, and the other is *Signature Verification and De-encapsulation*. AIS messages have overall size of 256-bit and containing 168-bit of the message field. In proposed scheme, we use an Elliptic Curve-based Digital Signature for source authentication and data integrity of the AIS message. The message field of an AIS message is 168 bits. Therefore, signed messages cannot be accommodated in this field. To overcome this problem, we use AIS Message Type 8 in our scheme for 4-consecutive slots. For the openness of the AIS protocol, we encapsulate signed messages into an existing protocol message, to which we apply a special interpretation. This process is illustrated in Figure 5. First, there is an AIS message, and then there is a follow-on message with a digital signature inside Message Type 8.

This procedure retains the backward compatibility and openness of the AIS. This enables the transmitter to continuously transmit AIS messages normally and send signed messages to the receiver in follow-up messages. Given that the signature takes 512 bits with a timestamp of 64 bits, it requires 4-chained AIS Message Type 8 messages to transmit a digital signature of one standard AIS message.

4.2.1 AIS Signature Generation and Encapsulation

In the proposed AIS authentication scheme, Algorithm 3 is AIS Signature Generation and Encapsulation, which signs the AIS message and encapsulates it into AIS Message Type 8. The transmitter first calculates timestamp T_s and computes the hash digest $hash(ais_m \vee T_s)$ of the AIS message concatenated with timestamp T_s using the hash algorithm $SHA-256$. Then, the transmitter computes the signature proof σ using the $privKey$. To prevent a replay attack and to link the AIS message with the correct signed message on the receiver side, concatenate the timestamp T_s with the signature σ and finally encapsulate the signed message into AIS Message Type 8, and send this as a "New type" of AIS message to the AIS receiver(s).

Algorithm 3: AIS Signature Generation and Encapsulation

1: **procedure**
2: **Input:** AIS message ais_m , $SHA-256$
3: **Output:** Signature $\sigma = \{r, s\}$, Encapsulated AIS Message
4: Compute timestamp T_s
5: Calculate $h = hash(ais_m \vee T_s)$ using $SHA-256$
6: Computes signature proof $\sigma = (privKey, h)$

7: Concatenate signature with ID and timestamp $\sigma \vee T_s$

8: Chaining signed message into 168-bits of the available payload of Message Type 8

9: Transmit encapsulated AIS messages to MTC or other Ship

10: **end procedure**

4.2.2 AIS Signature Verification and De-Encapsulation

The AIS receiver receives the encapsulated AIS message from the transmitter, and Algorithm 4 de-encapsulates and authenticates the received AIS message. The first step de-encapsulates the AIS message and obtains the signed message concatenated with the timestamp $\sigma \vee T_s$. To link an already received AIS message with the received signed message and prevent a replay attack, it computes hash digest $hash(ais_m \vee T_s)$ using the received timestamp and with already received AIS message. The receiver then performs signature validation using $pubKey$ of the transmitter and signature verification ensures that the incoming data are from an authenticated source, and no one has tampered with the AIS message.

Algorithm 4: AIS Signature Verification and De-encapsulation

1: **procedure**

2: **Input:** Encapsulated AIS Message, AIS message ais_m , $SHA-256, pubKey$

3: **Output:** Authenticated data

4: De-encapsulate AIS message and get Signed message $\sigma \vee T_s$

5: Calculate $h = hash(ais_m \vee T_s)$ using $SHA-256$

6: Signature validation using Public Key $(pubKey, h, \sigma)$

7: **if** Signature is validated **then**

8: Keep received message (Fully Authenticated)

9: **else**

10: Possibly tampered/replayed, therefore UNVERIFIABLE

11: **end if**

12: **end procedure**

Many of the proposed ADS-B and AIS message authentication and integrity schemes require modifications to existing protocols and transponders, resulting in a loss of compatibility for real-world deployment. However, our proposed ADS-B and AIS schemes are backward-compatible and retain the openness of protocols, thus requiring no hardware or protocol changes.

4.3 Assumptions, Constraints, Recommendations

In this subsection, we enumerate the assumptions, constraints, and recommendations of the proposed schemes.

1. PKI and Key Management are out of Scope: In proposed schemes, we assume that PKI services are already established and readily available. Second, key management (i.e. generation, distribution, expiration, revocation, and reissue) is available with the upgraded system.
2. Cryptographic Computations: The systems upgraded with our solutions are supposed to have cryptographic computation capabilities (i.e., signature generation, signature verification) for both the transmitter and the receiver. Therefore, an upgraded system may have cryptographic modules to perform cryptographic computations.
3. Transmission Errors: We assume that our proposed schemes are not completely resistant to transmission errors introduced by the transmission medium or adversaries. We assume that the error detection and recovery capabilities of the underlying protocols are sufficient to avoid transmission errors; therefore, normal and signed messages are recoverable on the receiver side.

5. Security Modelling and Analysis

In this section, we theoretically evaluate the security strength of the proposed scheme under our defined threat model.

Theorem 1. The legitimate receiver can detect data modification by external attacker.

Proof. The transmitter computes the digital signature σ of its transmitting data using the private key $privKey$, and sends it to the receiver. The receiver validates the signature by using the $pubKey$ of the transmitter and successful validation ensures no one has tampered with the message. The proposed scheme is secured against data modification attacks.

Theorem 2. Prevention of ghost-injection attacks.

Proof. The sender computes a digital signature σ on its data using the private key $privKey$, attaches the current timestamp T_s, and transmits it to receiver. The receiver then validates the signature using the $pubKey$ of the sender. The successful validation of the received message ensures that message is from authenticated source and thus prevents the ghost-injection attacks.

Theorem 3. Prevention of replay attacks.

Proof. The transmitter calculates current timestamp T_s, attaches it to the signature, and transmit it to receiver. The receiver obtains timestamp T_s from signed message and computes $hash(m \vee T_s)$ and then perform signature validation using the $pubKey$ of the transmitter. The signature binding of the timestamp T_s prevents the replay attack hence proposed scheme prevents the replay attack (Smith, 2023; Warner, 2022).

6. Conclusion

In this paper, we proposed a backward-compatible and lightweight message authenticity and integrity scheme for ADS-B and AIS based on state-of-the-art ECDSA standards. The proposed scheme retains the backward-compatibility and openness nature of ADS-B and AIS by transmitting signed messages in follow-up “New type” of messages that non-upgraded systems can safely discard. Moreover, we provide a lightweight security analysis to demonstrate that our proposed scheme is secure under our threat model and can prevent the aforementioned types of attacks.

We first implemented, tested, and evaluated the scheme for a similar protocol COSPAS-SARSAT in our accepted paper at peer-reviewed NDSS SpaceSec24 (Saleem et al., 2024), and we aim to implement and comparative-evaluate our proposed scheme as immediate future work.

Acknowledgements

Hannu Turtiainen thanks the Finnish Cultural Foundation / Suomen Kulttuurirahasto (www.skr.fi) for supporting his Ph.D. dissertation work and research (grant decision no. 00231412). The authors acknowledge the use of royalty-free icons in Figures 1, 3 and 5 courtesy of https://www.flaticon.com/ (icons by: DinosoftLabs, Wendy-G, juicy_fish, Freepik, Flat Icons, surang, Freepik, Peter Lakenbrink).

References

Asari, A., Alagheband, M.R., Bayat, M., Asaar, M.R., 2021. A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems. Comput. Netw. 185, 107599.

Balduzzi, M., Pasta, A., Wilhoit, K., 2014. A security evaluation of AIS automated identification system, in: Proceedings of the 30th Annual Computer Security Applications Conference. pp. 436–445.

Chen, T.-C., 2012a. An authenticated encryption scheme for automatic dependent surveillance-broadcast data link, in: CSQRWC 2012. IEEE, pp. 127–131.

Chen, T.-C., 2012b. An authenticated encryption scheme for automatic dependent surveillance-broadcast data link, in: CSQRWC 2012. IEEE, pp. 127–131.

Costin, A., Francillon, A., 2012. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices.

Duan, Y., Huang, J., Lei, J., Kong, L., Lv, Y., Lin, Z., Chen, G., Khan, M.K., 2022. AISChain: Blockchain-based AIS data platform with dynamic bloom filter tree. IEEE Trans. Intell. Transp. Syst. 24, 2332–2343.

Freire, W.P., Melo Jr, W.S., do Nascimento, V.D., Nascimento, P.R., de Sá, A.O., 2022. Towards a secure and scalable maritime monitoring system using blockchain and low-cost IoT technology. Sensors 22, 4895.

Goudosis, A., Katsikas, S., 2022. Secure Automatic Identification System (SecAIS): Proof-of-Concept Implementation. J. Mar. Sci. Eng. 10, 805.

Goudosis, A., Katsikas, S., 2020. Secure ais with identity-based authentication and encryption. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 14, 287–298.

Goudossis, A., Katsikas, S.K., 2019. Towards a secure automatic identification system (AIS). J. Mar. Sci. Technol. 24, 410–423.

Habibi Markani, J., Amrhar, A., Gagné, J.-M., Landry, R.J., 2023. Security establishment in ADS-B by format-preserving encryption and blockchain schemes. Appl. Sci. 13, 3105.

Hall, J., Lee, J., Benin, J., Armstrong, C., Owen, H., 2015. IEEE 1609 influenced automatic identification system (AIS), in: 2015 IEEE 81st Vehicular Technology Conference (VTC Spring). IEEE, pp. 1–5.

International Telecommunication Union, 2014. Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band. Recommendation M.1371.

Jegadeesan, S., Obaidat, M.S., Vijayakumar, P., Azees, M., 2021. SEAT: secure and energy efficient anonymous authentication with trajectory privacy-preserving scheme for marine traffic management. IEEE Trans. Green Commun. Netw. 6, 815–824.

Kacem, T., Wijesekera, D., Costa, P., 2015. Integrity and authenticity of ADS-B broadcasts, in: 2015 IEEE Aerospace Conference. IEEE, pp. 1–8.

Khandker, S., Turtiainen, H., Costin, A., Hämäläinen, T., 2022a. On the (In) Security of 1090ES and UAT978 Mobile Cockpit Information Systems–An Attacker Perspective on the Availability of ADS-B Safety-and Mission-Critical Systems. IEEE Access 10, 37718–37730.

Khandker, S., Turtiainen, H., Costin, A., Hämäläinen, T., 2022b. Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience. IEEE Access 10, 29493–29505.

Khandker, S., Turtiainen, H., Costin, A., Hämäläinen, T., 2021. Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures. IEEE Trans. Aerosp. Electron. Syst. 58, 2702–2719.

Kožović, D.V., \DJur\djević, D.Ž., Dinulović, M.R., Milić, S., Rašuo, B.P., 2023. Air traffic modernization and control: ADS-B system implementation update 2022: A review. FME Trans. 51, 117–130.

Manesh, M.R., Kaabouch, N., 2017. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. Int. J. Crit. Infrastruct. Prot. 19, 16–31.

Mäurer, N., Guggemos, T., Ewert, T., Gräupl, T., Schmitt, C., Grundner-Culemann, S., 2022. Security in digital aeronautical communications a comprehensive gap analysis. Int. J. Crit. Infrastruct. Prot. 38, 100549.

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

Prakash, P., Abdelhadi, A., Pan, M., 2019. Secure authentication of ADS-B aircraft communications using retroactive key publication. ArXiv Prepr. ArXiv190704909.

Saleem, A., Costin, A., Turtiainen, H., Hämäläinen, T., 2024. Towards message authentication and integrity for COSPAS-SARSAT 406 MHz distress beacons using lightweight ECDSA digital signatures, in: Workshop on Security of Space and Satellite Systems (SpaceSec) 2024, NDSS.

Sciancalepore, S., Di Pietro, R., 2019. SOS: Standard-compliant and packet loss tolerant security framework for ADS-B communications. IEEE Trans. Dependable Secure Comput. 18, 1681–1698.

Sciancalepore, S., Tedeschi, P., Aziz, A., Di Pietro, R., 2021. Auth-AIS: secure, flexible, and backward-compatible authentication of vessels AIS broadcasts. IEEE Trans. Dependable Secure Comput. 19, 2709–2726.

Shang, Y., 2023. Resilient vector consensus over random dynamic networks under mobile malicious attacks. Comput. J. bxad043.

Smith, G.P., 2023. Python Docs: Secure hashes and message digests.

Strohmeier, M., Lenders, V., Martinovic, I., 2013. Security of ADS- B: State of the Art and Beyond. DCS.

Su, P., Sun, N., Zhu, L., Li, Y., Bi, R., Li, M., Zhang, Z., 2017. A privacy-preserving and vessel authentication scheme using automatic identification system, in: Proceedings of the Fifth ACM International Workshop on Security in Cloud Computing. pp. 83–90.

Thumbur, G., Gayathri, N., Reddy, P.V., Rahman, M.Z.U., others, 2019a. Efficient pairing-free identity-based ADS-B authentication scheme with batch verification. IEEE Trans. Aerosp. Electron. Syst. 55, 2473–2486.

Thumbur, G., Gayathri, N., Reddy, P.V., Rahman, M.Z.U., others, 2019b. Efficient pairing-free identity-based ADS-B authentication scheme with batch verification. IEEE Trans. Aerosp. Electron. Syst. 55, 2473–2486.

Tran, K., Keene, S., Fretheim, E., Tsikerdekis, M., 2021. Marine network protocols and security risks. J. Cybersecurity Priv. 1, 239–251.

Warner, B., 2022. Pure-Python ECDSA and ECDH.

Wimpenny, G., Šafář, J., Grant, A., Bransby, M., 2022. Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. J. Navig. 75, 333–345.

Wu, Z., Guo, A., Yue, M., Liu, L., 2019. An ADS-B message authentication method based on certificateless short signature. IEEE Trans. Aerosp. Electron. Syst. 56, 1742–1753.

Wu, Z., Shang, T., Guo, A., 2020. Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey. IEEE Access 8, 122147–122167.

Wu, Z., Shang, T., Yue, M., Liu, L., 2023. ADS-Bchain: A Blockchain-based Trusted Service Scheme for Automatic Dependent Surveillance-Broadcast. IEEE Trans. Aerosp. Electron. Syst.

Yang, A., Tan, X., Baek, J., Wong, D.S., 2015. A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification. IEEE Trans. Serv. Comput. 10, 165–175.

Yang, H., Huang, R., Wang, X., Deng, J., Chen, R., 2014. EBAA: An efficient broadcast authentication scheme for ADS-B communication based on IBS-MR. Chin. J. Aeronaut. 27, 688–696.

Yang, H., Zhou, Q., Yao, M., Lu, R., Li, H., Zhang, X., 2018. A practical and compatible cryptographic solution to ADS-B security. IEEE Internet Things J. 6, 3322–3334.

Yi, P., Li, J., Zhang, Y., Chen, Y., 2022. Efficient hierarchical signature scheme with batch verification function suitable for ADS-B system. IEEE Trans. Aerosp. Electron. Syst. 59, 1292–1299.

Biography

Ahsan Saleem received his M.Sc. in Information Security in 2020 from COMSATS University Islamabad, Pakistan. He is currently doing his Ph.D. in Software and Communication Engineering at the University of Jyväskylä, Finland. His research interest is Information Security, Applied Cryptography and Wireless protocols Security.

Hannu Turtiainen received the M.Sc. degree in cybersecurity from the University of Jyväskylä, Jyväskylä, in 2020, where he is currently pursuing the Ph.D. degree in software and communication technology. His research topic is Machine Learning and Artificial Intelligence in the Cybersecurity and Digital Privacy field.

Andrei Costin received the Ph.D. degree from EURECOM/Telecom ParisTech, Sophia Antipolis, France in 2015. He is currently a Senior Lecturer/Assistant Professor of Cybersecurity with the University of Jyväskylä, Finland. He has been publishing and presenting at more than 45 top international cybersecurity venues, both academic and industrial.

Prof. Timo Hämäläinen has over 25 years of research and teaching experience related to computer networks. He has led tens of externally funded network management-related projects. He has more than 200 internationally peer-reviewed publications and supervised 36 Ph.D. theses. His research interests include wireless/wired network resource management (IoT, SDN, NFV) and network security.