PAPER • **OPEN ACCESS**

Research on the security of communication addressing and reporting system of civil aircraft

To cite this article: Xu Lu 2019 *IOP Conf. Ser.: Earth Environ. Sci.* **295** 032026

Research on the security of communication addressing and reporting system of civil aircraft

Xu Lu

Liaison Engineering Department, ShangHai Aircraft Design And Research Institute, 200436, China

xulu@comac.cc

Abstract. ACARS is a digital data link system that transmits short messages by radio or satellite between aircraft and ground stations. ACARS control centre is connected with each ACARS ground station and each airline information centre through the ground communication network. Exchange data and information with airlines in both directions through code addressing. However, because ACARS messages use plaintext transmission, anyone can monitor and decode ACARS messages with a low-cost receiver and obtain details such as aircraft type, location, planned route, passenger status and aircraft operation state, etc., thus posing a major threat to flight safety. The following security problems exist in the current ACARS system.

1. Introduction

As the electronic equipment that most commercial airliners must install and ensure its normal operation, ACARS can not only realize the exchange of data and information between the two places, but also give some help to the airlines. On the ground, the ACARS system consists of a network of multiple radio transceivers that can accept or send data link messages and distribute them to different airlines on the network. With the use of ACARS, the ability of airlines to monitor and direct aircraft has greatly increased.

ACARS special VHF (very high frequency) communication frequency range is 118-136.975mhz, including channel bandwidth of 25 kHz, 760 total channels, using half duplex mode.ACARS system has two types of operation modes, namely, category A operation and category B operation. On the ground, the ACARS system consists of a network of multiple radio transceivers that can accept or send data link messages and distribute them to different airlines on the network. With the use of ACARS, the ability of airlines to monitor and direct aircraft has greatly increased.

Because of its characters transmission characteristics, ACRS messages can be monitored and processed by anyone using low-cost detection equipment to obtain details of aircraft type, location, estimated route, cargo status, and flight operations. Airlines want to protect such information to maintain competitive advantage, and the military wants military aircraft to use ACARS while maintaining the confidentiality of military missions.

2. AMS application layer

AMS uses an existing ACARS communications network and can be used with other ACARS devices in use. The AMS application layer can be divided into three sub-layers. They are safety method layer, safety mechanism sub-layer and safety service sub-layer. These three sub-layers provide a complete security frame structure from bottom to top. The security algorithm is the method of implementing the

security mechanism, and the security mechanism provides security services.

The three sub-layers play different roles in the process of AMS receiving and processing data. The three sub-layers provide a complete security architecture, which ensures the security and integrity of data transmission. The combined action of the three sub-layers ensures the fast and real-time communication advantages of ACARS. Despite the volume of traffic, the amount of information it transmits can be multiplied many times, and the airline's services can be expanded.

2.1. AMS security services

AMS provides data confidentiality, message authentication and integrity, and key to establish a total of 3 types of security services. Data integrity protects AMS messages from tampering, including insertion, replacement, and deletion of some content. Message authentication is also known as data source authentication, where the crew or aircraft information system ensures that the message is initiated by the correct entity.

The AMS key establishment security service provides communicators with the ability to establish encryption keys in a secure and authenticated manner. This key is required to support data confidentiality, data integrity, and message authentication security services.

2.2. Security regime

The encryption mechanism uses symmetric encryption, where the sender and receiver use the same key to encrypt and resolve the data, which is generated by the AMS key creation scheme at the beginning of a secure session. In a secure and authenticated manner, the key negotiation mechanism generates a pair of temporarily used Shared keys between the communicating entities, one for message authentication and the other for data encryption. The sender uses the encryption process and session-specified encryption keys to encrypt the data that needs to be protected, and the receiver uses the decryption process and session-specified encryption keys to decrypt and recover the data. The two communicating parties use their own personal keys, each other's public keys and public parameters to obtain the two corresponding keys of the session.

The message authentication code mechanism uses symmetric encryption. After the key is established, the message authentication code is used as an encryption mechanism to provide data security and message authentication security services. The message authentication code of a session is generated by the key establishment scheme at the beginning of the secure session. The sender uses the message authentication code generation method and the message authentication key specified by the session to generate the message authentication code. The receiver uses the message authentication code generation method and the discounting authentication key specified by the session to generate the local message authentication code and compare it with the received message authentication code. If the two are the same, the received message is considered to be from the established security session and has not been tampered with. The encryption mechanism uses symmetric encryption. The sending and receiving parties use the same key to encrypt and reconcile the data. The key is generated by the AMS key establishment scheme at the beginning of the secure session. The sender uses the encryption key specified by the encryption process and the session to encrypt the data that needs to be protected. The receiver uses the encryption key specified by the decryption process and the session to decrypt and restore the data.

2.3. Security algorithm

The password algorithm used in the AMS security mechanism[4] is shown in the following table 1.

Table 1. Table of cryptographic algorithms

Arithmetic	Security mechanism	category	Safety and features
Elliptic curve digital signature	A digital signature	asymmetric encryption	At the same security level, the key length is shorter than other algorithms, which is

			suitable for ACARS systems with limited resources
Hash message authentication code	Message authentication	symmetrical encryption	A cryptographic HASH function whose security depends not only on the HASH function used but also on the instantaneity
The advanced encryption standard algorithm chooses the cipher backfeed mode	Data encryption	symmetrical encryption	AES algorithm has high security, CFB mode can adapt to the change of encrypted data length, and has flexibility in use
Diffie-hellman on the elliptic curve	Key agreement	asymmetric encryption	The key agreement protocol is simple and easy to implement. The public key must be digitally signed before it is exchanged to ensure the authentication and integrity of the public key
Hash algorithm (sha-256)	Digital signature/message authentication/key negotiation	-	The hash function has the characteristics of irreversibility and nonexistence of collision, and the 256 bit hash algorithm has high security

3. Shortcomings in AMS message processing

ACRS protocol header also contains information such as aircraft tail number, and there is a hidden danger of data leakage. ACARS is not a separate system. Its normal operation requires the coordination of many systems to be achieved. The inherent characteristics of ACARS data link plaintext transmission make the security of ACARS system under great threat, and its security is directly related to the safety of aircraft flight.

The aviation communication encryption scheme integrates the advantages of symmetric and asymmetric encryption systems, and adopts such security mechanisms as digital signature, key negotiation, message authentication and encryption. The spoofing and entity camouflage attacks of ACARS data link are very important to the information security of aircraft, which needs to be solved with more rigorous methods.

Because the key generation of AES algorithm is complicated, and the decryption algorithm needs to be rewritten, which affects the speed of encryption and decryption process. The key generation and encryption algorithm of SM4 algorithm is basically the same, and it does not need to rewrite the decryption algorithm, which improves the efficiency of encryption and decryption. In summary, for ACARS systems with limited resources and bandwidth, SM4 algorithm has the advantages of low computational overhead, fast encryption speed and certain security advantages, which can make the whole system work best.

4. Conclusion

On this basis, combined with the existing problems in ACARS data chain secure communication, we build a new certificateless key isolation signature and encryption scheme. This scheme has two advantages. One is that it does not need digital management of users' public keys, which can avoid a large amount of overhead caused by the management of public key data verification in the traditional PKI mechanism. Second, it can effectively reduce the harm caused by key leakage.

Multiple encryption algorithms can ensure data confidentiality, message authentication and integrity of the security services. It is not only suitable for civil aviation, but also meets the information security needs of military aviation. There is an urgent need for airlines, national aircraft and the military to have a secure ACARS network system to ensure the safe transmission of sensitive or secret information.

Acknowledgments
Thank Shanghai aircraft Design and Research Institute for providing me a platform to understand avionics, thank my Minister Wang Bing for his help and guidance, and finally, thank the experts for their criticism and revision, so that the article can be completed smoothly.

References
[1] Aloke Roy. Secure Aircraft Communications Addressing And Reporting System[C]//Digital Avionics Systems.20th Conference.Columbia,MD,USA:IEEE,2001,7A(2):1-11. W. Strunk Jr., E.B. White,The Elements of Style,third ed.,Macmillan,New York, 1979.
[2] Gu Lize,Zheng Shihui,Yang Yixian. Modern Cryptography Course [M]. Beijing: Beijing University of Posts and Telecommunications Press, 2009.
[3] Yang Long. Research and Application of Aircraft Communication Addressing and Reporting System [D]. Shandong University, 2013.
[4] ARINC. Communications Management Unit (CMU) Mark 2. ARINC Specification 758-2, published, March 25, 2005.
[5] Tianxi. Research and Simulation of communication addressing and reporting system for large aircraft [D]. University of Electronic Science and Technology, 2013.
[6] NATO.STANAG 462,2005,Final Draft of Proposed Standards for Software STANAG4626 Part I – Architecture[S] UK: NATO,2005.
[7] Du Min, Zhang Dong. Research on Dual-state Access of Embedded Real-time Multi-partition Operating System [J]. Aviation Computing Technology, 2014, 44 (6): 89-90.
[8] ARINC. ACARS Protocols for Avionic End Systems, ARINC Specification 619-2, published, March 11, 2005.
[9] Pereira M.S.,Investigation of the three competing VHF digital data link communications technology for commercial aviation[C], Digital Avionics Systems Conference, 2002. Proceedings. The 21st,2002,1:3C7/1-3C7/8.
[10] Williams, F. The general aviation technology revolution[C], Digital Avionics Systems Conference, 1995., 14th DASC,1995,207-212.