A DATA AUTHENTICATION SOLUTION OF ADS-B SYSTEM BASED ON X.509 CERTIFICATE

FENG Ziliang*, PAN Weijun*/[1] , WANG Yang***
*** Institute of Image and Graphics, Sichuan Univ.**
**** Air Traffic Management College, Civil Aviation Flight Univ. of China**

Keywords: *ADS-B, Data Authentication, ECC, X.509*

Abstract

A solution of data authentication of ADS-B systems based on the ECC and X.509 certificate is proposed in this paper. It can avoid key distribution problems combined with the symmetric key algorithm and prevent the ADS-B data spoofing thoroughly. Experimental test results showed that the solution is valid and appropriate in ADS-B UAT mode.

1 General Introduction

A major characteristic of Automatic Dependent Surveillance - Broadcast (ADS-B) technology is to broadcast the sender's location data periodically. It leads to several severe security problems respectively, such as data spoofing which has not been solved perfectly. A solution to the problem of data authentication of ADS-B systems based on the ECC and X.509 certificate is proposed in this paper, which may avoid the key distribution problems combined with the symmetric key algorithm, preventing ADS-B data spoofing thoroughly.

2 A Proposed Solution of ADS-B Data Authentication

There are two possible approaches to attacking ADS-B systems by data spoofing. One is to manipulate reasonable ADS-B data, which is valid in format and to send it in time. Another is recording legal ADS-B signals or data in advance and to resend them at some specified time, which is also named data replay attack. The aims of both are intended to disorder the display of ground and airborne ADS-B equipment, or to confuse the command of the air traffic controller. ADS-B data spoofing is a severe potential threaten to the safety of air traffic[1] and considered as the most serious obstacle for the popularization of ADS-B.

The potential and possible approaches against ADS-B data spoofing may be cryptography techniques. However, there are several difficulties that should be overcome although modern cryptography techniques have been proved very safe and are used very widely. The most important problem is how to choose appropriate cryptography techniques.

In a symmetrical cryptography system, the key of sender and receiver must be symmetrical or be the same[2]. The obvious difficulty of using in ADS-B is the distribution and management of the symmetrical keys, because the ADS-B system is not a well-connected network and the keys cannot be well distributed in real time, which limits the use of symmetrical cryptography.

In a public keys cryptography system, there are two keys that are named private key and public key respectively. The public key could be published so that it could be distributed in advance. So it is suitable for the ADS-B system. However, the encrypted data size is too big for using public key cryptography with enough encryption strength. For example, the typical or minimum RSA key size should be 1024 bits or more, this means that if using RSA cryptography is used to encrypt an ADS-B data block (typical payload size is 274 bits in UAT or Universal Access Transceiver), the consequential data size is at least 1024 bits. Therefore the encryption leads to greater expansion compared with the original data size. Furthermore, the greater the encryption strength, the bigger the consequential data size.

[1] Communication Author

Simply using encryption technologies to against ADS-B data spoofing should not be applicable, because the broadcasting position data could not be decoded correctly by the public, and this would also violate the original intention of the ADS-B system design. Data authentication technology, sometimes called Data Signature Algorithm (DSA), is a data signature and verification technology, which does not involve changing the original data itself but adds an additional stamping data to guarantee that the data is created by its original hosts.

ECC (Elliptic Curve Cipher) has been proved as an excellent public key cryptography with small key size compared with RSA based and examples showed that the encryption strength of ECC with 128 bits key size is similar to the strength of RSA with 1024 bits key size. The ECDSA (Elliptic Curve Data Signature Algorithm) is a data signature algorithm derived from ECC and DSA, and it has been standardized in FIPS 186-3b by NIST[3]. Although the signature data length of ECDSA is twice that of its key, the smaller key size makes it more suitable for ADS-B data authentication.

To accommodate the encryption data or signature data, the data block format, include ADS-B IN data and ADS-B OUT data format, should be changed no matter which cryptography is used.

The main points of the proposed ADS-B data authentication solution are described as follow. The timestamp data of GPS will be added to check the data reply attack. The original ADS-B out payload and the timestamp data should be signed by ECDSA algorithm with the ECC private key. The signature data will be encapsulated in a new data type of ADS-B out, which will be defined to accommodate new signature data. The new data will be sent together with original payload data through the ADS-B communication channel.

The GPS data and signature data in received ADS-B data will be separated from the original payload. The received GPS timestamp could be compared with current time to check the replay attacks, and the signature data could be verified by the ECDSA verification algorithm with the public key in the X.509 certificate, which can be verified by the hierarchy model of X.509 management mechanism.

The most significant difference between the proposed solution and others is the use of the X.509 certificate with the ECC public key and the extra GPS timestamp. It makes the ADS-B data authentication solution become practical because of the smaller amount of signature data and the measure of anti-replay attacks.

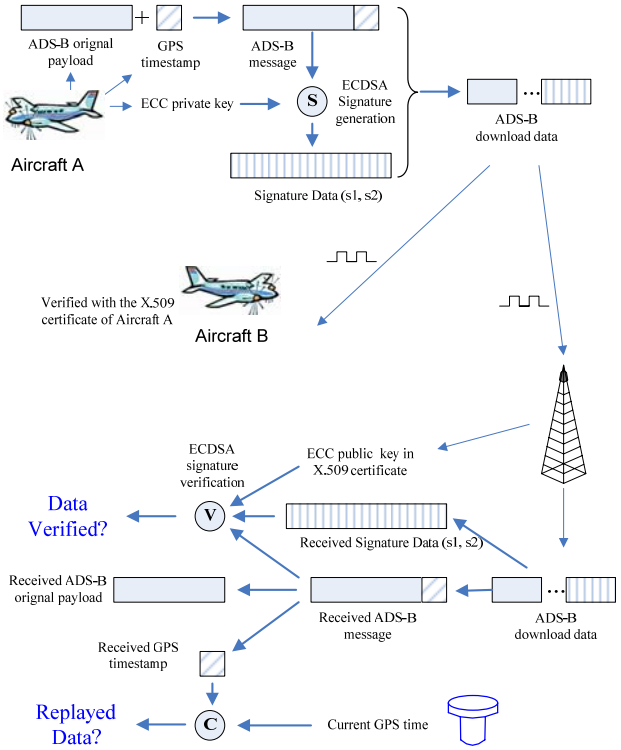

Fig.1. Proposed Solution of ADS-B Data Authentication

The proposed solution is shown in fig.1. Where letter S, V, C in circle denote the signature process, the verification process and the comparison process.

3 The Analysis of the Key Technology

Three important problems will be discussed in this paper. They are the analysis of authentication data size and the digital signature algorithm, the modification of the data format of ADS-B out, the management and the usage of the X.509 certificate.

3.1 Authentication Data Size and the Digital Signature Algorithm

The available ADS-B out data space is small and limited in various ADS-B realization technologies[4][5]. A small of signature data is required; meanwhile, it could result in a reduction in the security of the signature.

Considering the typical data block size of payload in UAT, there are only 272 bits of data space left, and with the 32 bits HDR data space, there is only 240 bits data space that can be used.

To accommodate the GPS data stamp, the elliptic curves over a 112 bit prime field could be selected (such as curve named secp112r1) of which the input data size will be 112 bits at most and the signature data size will be 224 bits. The ECDSA signature output data include two parts, s1 and s2 respectively (in openssl[6] nominated r and s respectively). If other elliptical curves with a higher order are selected, the signature data size will be increased correspondently.

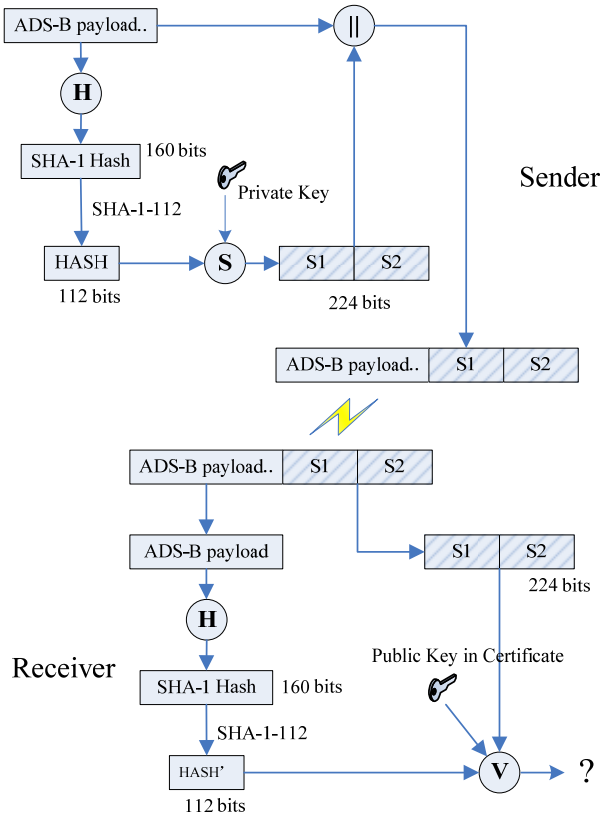

Fig.2. Hash Truncation and Data Signature Algorithm Process

In the data signature process, a hash value should be calculated before calculating the ECDSA signature, and the hash function may be chosen to be SHA-1 with the output data block size 160 bits, which is larger than 112, the maximal input size of the selected signature process. This means that the hash value must be truncated before the signature process to fit the ECDSA input block size. The data truncation process will not affect the subsequent signature or verification process, because they are truncated before encryption and it is symmetrical in both signature and verification ends, which is minimally different from the traditional process. The negative effect of the truncation process may be tiny because the discarded data is small even though the process may reduce the security of the signature and it should be ignored completely. The process is illustrated in Fig.2, where letter H in the circle denotes the process of SHA-1 process.

3.2 The Analysis of ADS-B OUT Data Format

The GPS timestamp data will be included in the final ADS-B OUT data except signature data and it is useful in avoiding the replay attacks. The 32 bits timestamp can be selected. And it adds the signature data size by 224bits, the new data size is 256 bits, which is larger than the volume size of 240 bits according UAT MOPS (RTCA DO-282)[4] for an ADS-B out message payload excluding the 32 bits HDR field for all type. A compromise timestamp sending solution is used to split the timestamp data into two parts (named T1 and T2) and to send 16 bits once. It means the replay attacks check frequency will be halved.

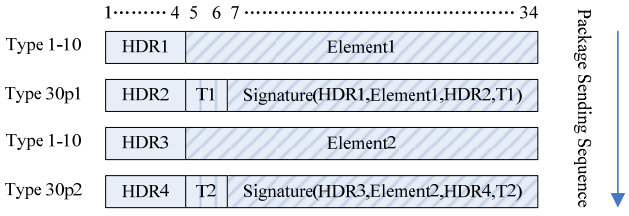

Fig.3. UAT data composition of new type 30

A new type 30 is defined to accommodate the GPS timestamp and signature data. It will be

sent following any other original ADS-B data types. This means that the communication volume after adding the signature data will be twice the original volume. The encapsulated data format and package sending sequence is illustrated in Fig.3. The input data of ECDSA signature generation include 3 parts, the last whole payload package (HDR1 and element1), the header or the new payload package (HDR2), and the current GPS timestamp (T1 or T2).

In 1090ES, besides the occupation of the aircraft location and other necessary information, only 56 bits of ME field may be used[5]. It is not enough for the above signature data and timestamp, so 4 DF24 (COMM-D) packages may be combined and there are 320 bits payload for the total that could be used to accommodate the signature data and timestamp. The new DF24 package will be sent following DF17. This means that the communication volume will be 5 times as the original volume.

3.3 Management and Using of Certificate

The ADS-B aircraft certificate is a special file issued by the CA (Certificate Authority), which should be distributed in public because there is a public key contained in certificate and it can be used to verify the signature of ADS-B out data.

A certificate can be considered as the identity of an aircraft because it can be verified by the upper certificate authority in the X.509 hierarchy model. Accordingly the root CAs should be crossed certified with each other so that the aircraft ADS-B certificate in other areas can also be verified through the X.509 hierarchy mechanism. When an ADS-B message should be verified, for example, when a ground station or an aircraft B need to verify the received ADS-B message from the local aircraft A, it has only to perform verification process by using the public key of A; when this is a need to verify the message from an unknown aircraft Z, the hierarchy model or certificate chains should be used to verify the public key of Z step by step, illustrated in Fig.4 as:

CAAC<<FAA>>FAA<<AA>>AA<<Z>>

When the public key of Z can be verified, it can be used to verify the message from aircraft Z.

To verify a message of ADS-B, certificates of all levels are very necessary. But it is impractical to store all the certificates of aircrafts in the world for every verifier, especially for the airborne verifier. A practical certificate exchange and distribution mechanism may be the combination certificate exchange scheme with a static certificate database and dynamic certificates.

The establishment of a static certificate database is essential for the ADS-B ground station. It means that a the special ground service network of the ADS-B certificate database, which is helpful in the establishment of certificate chains, the query of a certificate, the revocation of certificates, should be established first, and this is practical and easy. The certificates for one flight are limited. For an airborne receiver, the certificates used during one flight can be estimated and downloaded from the certificate network before take off.

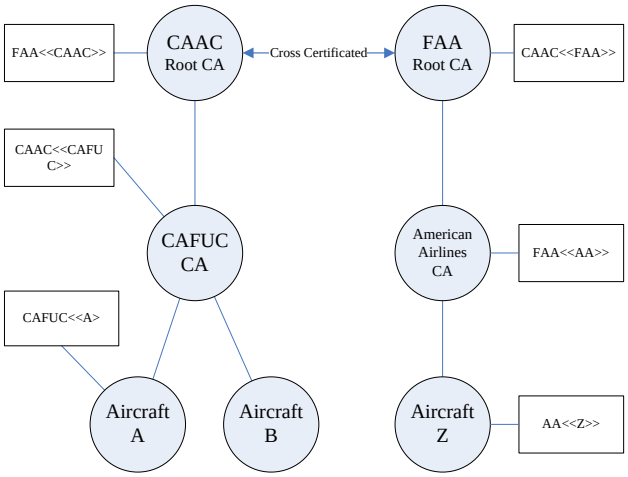

Fig.4. Certificate Chains and Hierarchy Model

The dynamic certificates exchange scheme, which includes certificate or certificate chain request broadcasting and uploading function, is to remedy the insufficiency of the certificate, especially in temporary change of flight plan or in a long distance flight. For example, if aircraft A need to verify another aircraft B without its certificate, it could broadcast the certificate request message of B, and the ground station, nearby aircraft, or aircraft B could respond. If the new certificate could not be verified by A because of the lack of certificate chains, it could

broadcast the request for certificate chains also. After a request is responded, all the aircraft or ground stations in this area will receive the certificate or chains, and all of them could verify it.

This scheme will concern the modification of upload and download data format of ADS-B. Although there are 423 bytes application data space that could be used in the UAT ground uplink message payload[4], which is suitable for the upload of temporary certificate and chains. The data format of certificate request and reply need to be redefined.

4 Laboratory Test

The laboratory test is illustrated in Fig.4. There are 3 computers, which are used to denote 2 airborne ADS-B devices (computer A and B) and 1 ground station (computer C), and the clock of all computers was set to the same before test. 3 serial communication lines are used to connect 3 computers to simulate the air-ground and air-air communication and the baud rate were set to 9600 bps.

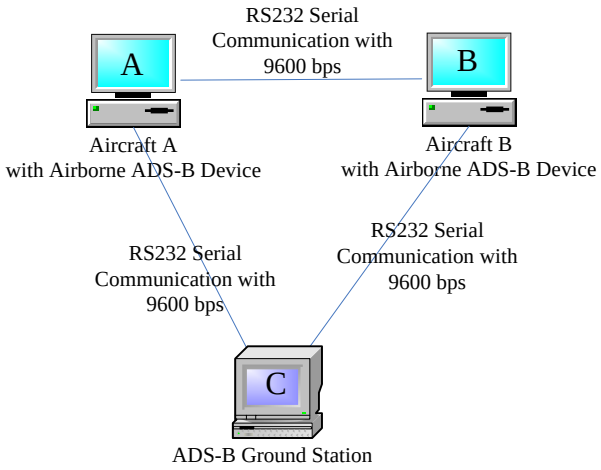

Fig.4. Scheme of Laboratory Experimental Test

There is one software is running in A and B with the function of creating a simulated flight track of aircraft per second, sending encapsulated UAT position package (type 1) and a new package (type 30) per second, receiving the ADS-B package of another aircraft, displaying dynamic information of nearby aircraft.

Two software run in computer C, one is the certificate management software with the function of creating the certificate of root CA or aircraft, distributing certificate; another one is the flight dynamic display software with the function of verifying the received ADS-B message, displaying aircraft dynamics information in the air especially including the verification status of ADS-B data. As illustrated in Fig.5, if an aircraft passes the verification process the message “verified” in green will displayed in the third line of its tag, if it does not pass, the message will be “SP data!” or “RP Data!” in red; if it does not include a verification message, the message will be “No Sig” in gray.

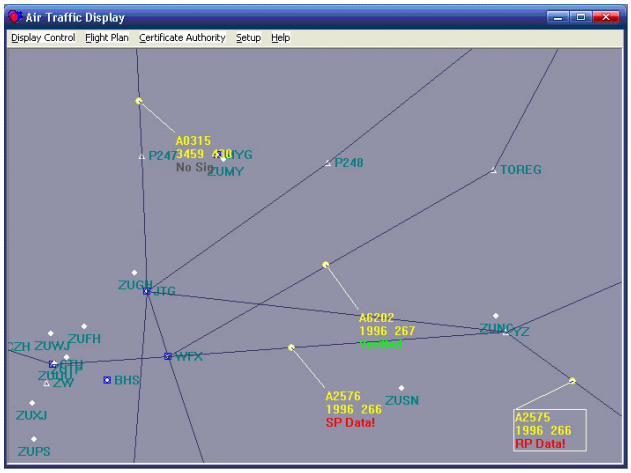

Fig.5. Display of ADS-B verification

The laboratory experimental testing results showed that the proposed solution is valid and suitable for the verification of ADS-B out data of UAT.

5 Summary

An ADS-B data authentication solution based on the ECC certificate and the X.509 certificate is proposed. The extra signature data and timestamp was appended in the ADS-B out message to verify the original message and to check replay attacks. A suggestion of data format modification of the UAT ADS-B, a combination mechanism of static and dynamic certificate exchange was proposed. Laboratory experimental test results showed that the

solution is valid and suitable for the verification of ADS-B out data of UAT.

Acknowledgements

This work is supported by CAAC Research Fund (No: MHRD2009203), the National Nature Science Foundation of China (No: 60736046) and Civil Aviation Flight Technology and Flight Safety Base Fund.

References

[1] Darryl H Phillips. *ADS-B Terrorist's Dream, Security's Nightmare - Will ADS-B Increase Safety and Security for Aviation.* http://www.airsport-corp.com/adsb2.htm, 2000

[2] Behrouz A. Forouzan. *Cryptography and Network Security*. McGraw-Hill companies, Inc. 2008

[3] FIPS PUB 186-3. *Digital Signature Standard (DSS).* U.S. Department of Commerce, National Institute of Standards and Technology, 2009

[4] RTCA. *Minimum Operating Performance Standard for Universal Access Transceiver (UAT) Automatic Dependent Surveillance Broadcast*, RTCA DO-282A, July 29, 2004

[5] RTCA. *Minimum Operational Performance Standard for 1090 MHz Extended Squitter ADS-B and TIS-B*, RTCA DO-260A, April 10, 2003

[6] Nils Larsch. *OpenSSL Document for ECDSA.* http://www.openssl.org/docs/crypto/ecdsa.html. 2010

Copyright Statement