ADS-B Data Authentication Based on ECC and X.509 Certificate

Wei-Jun Pan, Zi-Liang Feng, and Yang Wang

Abstract—An automatic dependent surveillance-broadcast (ADS-B) system has serious security problems, and the data can be spoofed during broadcasting precise position information of aircraft. A solution of the ADS-B system data authentication based on the elliptic curve cipher (ECC) and X.509 certificate is proposed. It can avoid the key distribution problem by using the symmetric key algorithm and prevent the ADS-B data from being spoofed thoroughly. Experimental test results show that the solution is valid and appropriate in ADS-B universal access transceiver (UAT) mode.

Index Terms—Automatic dependent surveillance-broadcast, data authentication, elliptic curve cipher, X.509.

1. Introduction

A major function of automatic dependent surveillance-broadcast (ADS-B) technology is to broadcast the satellite-based aircraft identification, position, and speed periodically. ADS-B has been implemented in many countries and it is the backbone of the next generation air transportation system (NextGen) in United States. However, it is suffered from several severe security problems[1], such as data spoofing which has not been solved perfectly. A digital signature scheme based on elliptic curve cipher (ECC) is characterized of security and efficiency[2],[3] by referring to identification which is implemented by using certificate verifying supported by X.509 and digital signing[4]. A method of image encryption based on bivariate polynomials is proposed for improving encryption efficiency[5]. In this paper, based on the ECC and X.509 certificate, a solution to the problem of data authentication of ADS-B systems is proposed, which may avoid the key distribution problems by using the symmetric key algorithm, and prevent ADS-B data from being spoofed thoroughly.

Manuscript received November 7, 2011; January 11, 2012. This work was supported by the National Natural Science Foundation of China under Grant No. 61179072 and the Civil Aviation Science Foundation of China.

W.-J. Pan, Z.-L. Feng, and Y. Wang are with the College of Computer Science, Sichuan University, Chengdu 610065, China (e-mail: panatc@sina.com; fengziliang@scu.edu.cn; wangyang@scu.edu.cn).

W.-J. Pan is also with the College of Aviation Management, the Civil Aviation Flight University of China, Guanghan 618307, China.

Digital Object Identifier: 10.3969/j.issn.1674-862X.2012.01.009

2. Proposed Solution of ADS-B Data Authentication

There are two possible approaches to attacking ADS-B systems by data spoofing. One is manipulating reasonable ADS-B data, which is valid in format and sending in time. The other is recording legal ADS-B signals or data in advance and resending them at some specified time, which is also named data replay attack. The aims of them 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 it is 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. Although modern cryptography techniques have been proved very safe and are used very widely, there are several difficulties that should be overcome. The most important problem is how to choose appropriate cryptography techniques.

In a symmetrical cryptography system, the keys of the sender and receiver must be symmetrical or be the same[6]. The obvious difficulty of using an ADS-B system is the distribution and management of the symmetrical keys, because the ADS-B system is not a well-connected network and the keys can not 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 to use public key cryptography of enough encryption strength. For example, the typical or minimum RSA (an algorithm for public-key cryptography, RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman) key size should be 1024 bits or more, this means that if RSA cryptography is used to encrypt an ADS-B data block (typical payload size is 274 bits in universal access transceiver (UAT)), the consequential data size is at least 1024 bits. Therefore, the encryption leads to great expansion compared with the original data size. Furthermore, the greater the encryption strength, the bigger the consequential data size is.

Simply using encryption technologies to prevent
ADS-B data spoofing should not be applicable, because the broadcasting position data perhaps could not be decoded correctly by the public, and this would also violate the original intention of the ADS-B system design. The 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 has been proved as an excellent public key cryptography with a small key size compared with RSA and examples show that the encryption strength of ECC with the key size of 128 bits is similar to the strength of RSA with the key size of 1024 bits. The elliptic curve data signature algorithm (ECDSA) is a data signature algorithm derived from ECC and DSA, and it has been standardized in Federal Information Processing Standard (FIPS) 186-3 by National Institute of Standards and Technology (NIST)[19]. Although the signature data length of ECDSA is twice of 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 formats, 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 follows. The timestamp data of global position system (GPS) will be added to check the data reply attack. The original ADS-B out payload and the timestamp data should be signed by the 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 the 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 will be compared with current time to check the replay attacks, and the signature data will 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 practical due to the smaller amount of signature data and the measure of anti-replay attacks.

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

3. Analysis of Key Technology

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

3.1 Authentication Data Size and DSA

The available ADS-B out data space is small and limited in various ADS-B realization technologies[8],[9]. A small size 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 bit of data space left, and with the 32 bit header (HDR) data space, there is only 240 bit 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 the curve named secp112r1), for which the input data size will be 112 bit at most and the signature data size will be 224 bit. The ECDSA signature output data include two parts, s1 and s2, respectively (in OpenSSL, which is an open source implementation of the SSL and TLS protocols[10], nominated r and s, respectively). If other elliptical curves with a higher order are selected, the signature data size will be increased correspondently.

![Fig. 1. Proposed solution of ADS-B data authentication.](image)
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 of 160 bit which is larger than 112 bit that is 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 the verification process, because they are truncated before encryption and symmetrical in both signature and verification ends, which are 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, it can be ignored completely. The process is illustrated in Fig. 2, where the letter H in the circle denotes the process of SHA-1.

### 3.2 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 bit timestamp can be selected. It adds the signature data size by 224 bit and the new data size is 256 bit, which is larger than the volume size of 240 bit according to [8] for an ADS-B out message payload excluding the 32 bit HDR field for all types. A compromise timestamp sending solution is used to split the timestamp data into two parts (named T1 and T2) and to send 16 bit once. It means the replay attacks check frequency will be halved.

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 two times over that of the original one. The encapsulated data format and package sending sequence is illustrated in Fig. 3. The input data of ECDSA signature generation includes 3 parts, the final whole payload package (HDR1 and element1), the header or the new payload package (HDR2), and the current GPS timestamp (T1 or T2).

Two link solutions are used as the physical layer for relaying the ADS-B position reports, one is UAT, and the other one is 1090 MHz mode S extended squitter (1090ES), besides the occupation of the aircraft location and other necessary information, only 56 bit of message (ME) field may be used\(^6\). It is not enough for the above signature data and timestamp, so 4 DF24 (downlink format field 24, named COMM-D) packages may be combined and there is total 320 bit payload 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 of the size of the original.

### 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 crosswise 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 needs to verify the received ADS-B message from the local aircraft A, it has only to perform the verification process by using the public key of A. When it is needed 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

\[
\text{CAAC}<<\text{FAA}>>\text{FAA}<<\text{AA}>>\text{AA}<<\text{Z}}>
\]

where \(<<>>\) means * certificates \(*\). And as shown in Fig. 4, FAA means Federal Aviation Administration of United States, CAAC means Civil Aviation Administration of China, CAFUC means Civil Aviation Flight University of China, and AA means American Airlines, Z means aircraft 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 the distribution mechanism may be a combination certificate exchange scheme with a static certificate database and dynamic certificates.

The establishment of a static certificate database is essential for an ADS-B ground station. It means that a special ground service network of the ADS-B certificate database, which is helpful in the establishment of certificate chains, the query of a certificate, and 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 taking off.

The dynamic certificates exchange scheme, which includes certificates or certificate chain request broadcasting, and an uploading function, is to remedy the insufficiency of the certificate, especially in the temporary change of a flight plan or in a long distance flight. For example, if aircraft A needs 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 will 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 formats of ADS-B. Although there is 423 bytes application data space that could be used in the UAT ground uplink message payload\[8\], 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. 5. There are 3 computers, which are used to denote two airborne ADS-B devices (computer E and D) and one ground station (computer F), and the clock of all computers is set to the same before the test. Three serial communication lines are used to connect three computers to simulate the air-ground and air-air communications and the baud rate are set to be 9600 bps.

There is a software running in E and D with the function of creating a simulated flight track of a 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, and displaying dynamic information of nearby aircrafts.

![Fig. 4. Certificate chains and hierarchy model.](image)

![Fig. 5. Scheme of laboratory experimental test.](image)

![Fig. 6. Display of ADS-B verification.](image)
Two software run in computer F. One is the certificate management software with the function of creating the certificate of a root CA or an aircraft and distributing certificates. The other is the flight dynamic display software with the function of verifying the received ADS-B message and displaying aircraft dynamics information in the air especially including the verification status of ADS-B data. As illustrated in Fig. 6, if an aircraft passes the verification process, the message “verified” will be displayed in the third line of its tag; if it does not pass, the message will be “SP data!” or “RP Data!”; if it does not include a verification message, the message will be “No Sig”.

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

5. Conclusions

An ADS-B data authentication solution based on the ECC certificate and the X.509 certificate is proposed. The extra signature data and timestamp is 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 and a combination mechanism of static and dynamic certificate exchange are proposed. It is demonstrated that the solution is effective and appropriate for the verification of ADS-B out data of UAT by the laboratory experimental test results.

References


Wei-Jun Pan was born in Hubei Province, China, in 1968. He received the M.S. degree in aviation management from RMIT University, Australia. He works with CAFUC as a researcher and he is pursuing the Ph.D. degree with Sichuan University in computer science. His research interests include air traffic control theory and applications, and computer image process.

Zi-Liang Feng was born in Sichuan Province, China, in 1970. He received the Ph.D. degree from the Department of Mathematics, Sichuan University, in 2001. He works as a professor with Sichuan University. His research interests include air traffic control systems and image process.

Yang Wang was born in Sichuan Province, China, in 1982. She received the M.S. degree from Sichuan University in 2007. She works with Sichuan University. Her research interests include real-time systems and image process.