International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 3 (March'2016)

A THREE LEVEL HIERARCHICAL SIGNATURE ON ADS-B SUPPORTING BATCH VERIFICATION

Shilpa Mary Philips,
B.Tech Student,
Department of Information Technology,
Velammal Institute of Technology,Chennai,India.

N.Raja Rajeswari,
B.Tech Student,
Department of Information Technology,
Velammal Institute of Technology,Chennai,India.

B.Hema,
Assistant Professor,
Department of Information Technology,
Velammal Institute of Technology,Chennai,India.

Abstract: Recently, a new technique will replace conventional radar systems and be deployed as part of the next generation air transportation systems. Unlike in traditional radar systems where aircraft only respond to interrogations by ground stations. In the ADS-B system, aircraft continuously obtain their positions based on some satellite positioning techniques (e.g., GPS) and periodically broadcast their positions as well as some other information such as the current velocity to ground stations and other aircraft. Recently, flight tracker Web sites based on the mashup of ADS-B data have gained popularity, providing Web users with a visual overview of air-traffic around the world. Each aircraft equipped with an ADS-B device keeps broadcasting plaintext messages to other aircraft and the ground station controllers once or twice per second. The lack of security measures in ADS-B systems makes it susceptible to different attacks. Among the various security issues, we investigate the integrity and authenticity of ADS-B messages. In this project we demonstrate that attacks range from passive attacks (evasdropping) to active attacks(message jamming ,replying of injection) .This prompts the idea to bring RSA algorithm and HMAC to generate signature in which we can overcome and predict the attack and can ensure the integrity of message.

Keywords: RSA,Three level Identity based signature, Integrity, HMAC,Mashup.

I.INTRODUCTION

Conventional ATC techniques are based on radar systems which include primary surveillance radars (PSR) and secondary surveillance radars (SSR). PSRs are independent and non-cooperative. Namely, PSRs transmit high-frequency signals, receive the echoes reflected from the aircraft and then can determine the position of the aircraft, without requiring the aircraft's participation. On the other hand, SSRs cooperate with and interrogate the aircraft to get responses which are generated by the onboard systems equipped in the aircraft. The responses may contain information of the aircraft such as identification codes, height, and altitude. However, traditional PSR and SSR systems suffer from some disadvantages such as low precision and high cost.

II.PROBLEM DEFINITION

- An active attacker can modify or inject messages which could result in some destructive attacks such as Ghost Aircraft Injection attack and Virtual Trajectory Modification attack.
- An active attacker who has full control over the wireless communication channel can inject, modify and delete ADS-B messages.
- PSRs and SSRs are independent, non-cooperative and much expensive.
- The responses may contain high sensible information of the aircraft such as identification codes, height, and altitude. Hence the communication should be very sensible.
- Traditional PSR and SSR systems suffer from some disadvantages such as low precision and high cost.

III. PROPOSED SYSTEM

In our proposed ADS-B system has "smart objects" that can create a graphical representation of aircraft on the Web. In this a plane object created through mashup of ADS-B data displays the basic ADS-B attributes such as call sign, registration, altitude, speed and position. Providing ADS-B data with authenticity, which is a main theme of this paper, is also important for the related Web services to maintain high level of reliability. ADS-B data are broadcast through wireless channel (radio frequency data-link) without any cryptographic mechanisms implemented. Besides the ground controllers and aircraft, anyone who holds a single low-cost ADS-B receiver can obtain the ADS-B data. We mainly deal with data integrity and source integrity. Data integrity ensures that the ADS-B data has not been modified upon arriving at the receivers. In this paper, we propose to apply hierarchical identity-based signature (HIBS) to ADS-B authentication and in fact a three-level HIBS is sufficient. The top level PKG could be an authoritative organization such as the ICAO, the FAA or

EUROCONTROL. The second level consists of different airlines around the world and the aircraft stand in the third level. In addition, at any time the aircraft or the ground ADS-B receivers will receive a large number of signatures from different surrounding aircrafts which may belong to different airlines and it needs an efficient scheme to verify these signatures as soon as possible. We use batch verification to mitigate this concern. Batch verification is classified into three types, while we deal with the most intractable but desirable one, i.e. type 3. Type 3 batch verification allows multiple signatures on multiple messages generated by multiple signers to be verified at the same time batch verification can be classified into full batch verification and partial batch verification.

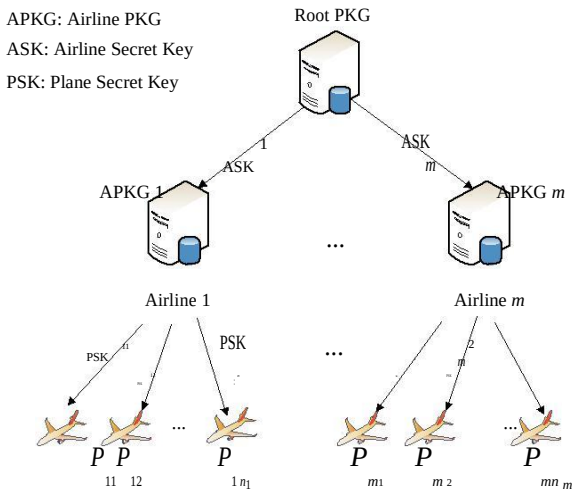
In this new framework, we employ a three level HIBS mechanism. The top level PKG generates private keys for the second-level PKGs (the airlines). Each airline is responsible for generating private signing keys for its affiliated aircraft. Each aircraft signs its messages with corresponding signing key and broadcasts the messages together with the signatures. And the signatures are verified in the ground station verifier (the airport).

IV.MODULES

- Web technology and smart objects,
- Virtual airport nodes and air craft nodes,
- Effective controlling and communications between Airports and crafts,
- Batch verification and control changes and identification of injected data .

V.KEYWORDS:

APKG: Airline PKG
ASK: Airline Secret Key
PSK: Plane Secret Key
SKIDA: Airlines secret key
SKIDF: Aircraft secret key



(a) Setup and Extract Phase

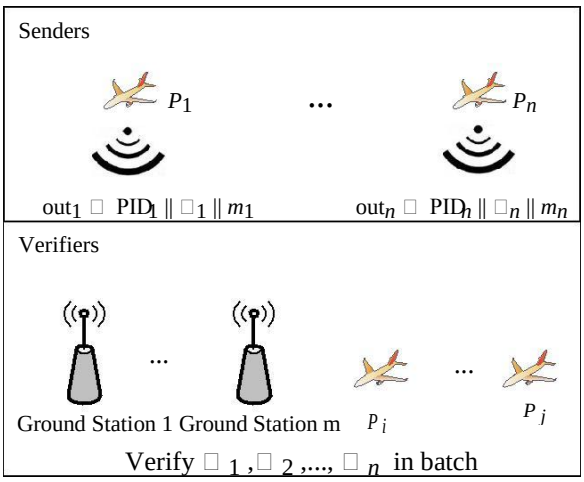


Figure 1. The Proposed ADS-B Authentication Frame-work.

VI.WEB TECHNOLOGY AND SMART OBJECT:

Creating website to visually predict and plot our registered airports and aircrafts. The authorized elements from the root PKG (Airport authority of India) only can plot on Google map in our website. Using the highly secured networking socket communication can create the registered and authorized elements could appear on the map. The secured network application communicates through the authorized internet protocols among them. The root level main authority monitors the every occurrence of elements in the server of the website and verify with the Setup phase algorithm when the element get generated. The authorized element only gets the signatures and keys generated from the authority of root level PKG.

On input of a security parameter, the Setup algorithm allows the top PKG to generate the master secret key and the master public key. The root level PKG keeps the master key pair (msk, mpk) that will be used to generate secret keys for low-level nodes.

VII.VIRTUAL AIRPORT AND AIRCRAFT NODES:

On input of the master secret key, and an airline identity IDA, the Extract A algorithm generates a secret key skIDA for IDA. The Level-1 nodes are airlines each with an identity like IDA. The second level PKGs which can generate the secret signing keys for the bottom level nodes.

Airport nodes are created to controls and communicate with the aircraft nodes. And craft nodes show the important details

like range, location, destination, craft number and the source airport of the crafts themselves. Generation of the keys and ids are based on the input of top level PKG (Authority) to the low level PKG (Airlines and aircrafts) using RSA algorithm and HMAC algorithm. Due to this attackers cannot predict the keys and signatures of the nodes.

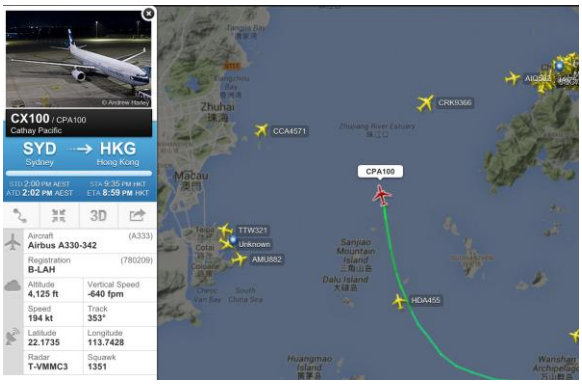


Figure 2: A Mashup Displaying ADS-B data of a plane around Hong Kong peovided by flightrada24.

VIII. EFFECTIVE COMMUNICATIONS AND CONTROLS BETWEEN AIRPORT AND AIRCRAFT:

On input of the secret key skIDA for the Level-2 nodes are the aircraft each with an identity like IDF .The airline identity IDA and an aircraft identity IDF, the Extract F algorithm generates a secret key skIDF for IDF belonging to IDA. The messages and information's are high sensible and secured. So it could be highly integrated and secured. On the input of skIDF to the registered crafts are controlled and communicated by the source airports among the matched keys and signatures. And matched airports only can communicate with the aircrafts and controlled them automatically from belonged station. Information's from the airport to aircrafts and crafts to station communications can be controlled by ground station belongs to the aircrafts. After reached the destination, above entire rolls are handled by the destination port.

IX. BATCH VERIFICATION AND CONTROL CHANGE AND IDENTIFICATION OF INJECTED DATA:

On input of the secret key skIDF and a message m, the Sign algorithm generates a signature of m. On input of a signature on a messages m with respect to airline identity IDA and aircraft identity IDF, the Verify algorithm outputs either 0 or 1, where 1 represents that the signature is valid.

In existing system each crafts are verified individually but proposed systems implements the batch verification schemes to verify the bulky requests from the crafts. We give a formal security proof for the proposed extended scheme that supports full batch verification. Verifications are based on the skIDF, skIDA, signature and keys from root level PKG's. After the verification in destination port the entire controls are handle by the destination port which is alternately changes afterwards the verification in somewhere airports.

X. ENHANCEMENT:

- ✓ In the experiment, we run each scheme ten times to get an average value. We measure the running time of generating and verifying n signatures where n could be from 1 to 1000 increment by 100.
- ✓ Both our basic scheme and extended scheme are about five times faster than verifying n signatures independently.
- ✓ No matter how many signatures are verified in batch at one time, we always need only two more parings in the basic scheme than that in the full scheme. There is some more multiplication operations needed in the basic scheme, but these operations are much less time-consuming than the pairing operations and thus have little influence on the computational time.
- ✓ Visually we use the google map to verify the secure data integrity and transmission between airport and aircraft.

XI. ALGORITHM USED:

Name : RSA ALGORITHM.
Cryptography type: Asymmetric Encryption/Decryption.
Name : H-MAC ALGORITHM.
Signature type : 32 –bit signature.

XII. ADVANTAGES:

- ✓ Automatic Dependent Surveillance-Broadcast (ADS-B) has become a crucial part of next generation air traffic surveillance technology and will be mandatorily deployed for most of the airspaces worldwide.
- ✓ The number of aircraft has been increasing tremendously over the last decade. So need to verify bulk number of aircrafts using Batch verification.
- ✓ We give a formal security proof for the extended scheme. Experiment results show that our schemes with batch verification are tremendously more efficient in batch verifying n signatures than verifying n signatures independently.
- ✓ With this accurate information, the ground controllers or other surrounding aircraft can monitor and track the location and path of an aircraft, which provides aircraft and the ground controllers a common situational awareness. This improves pilots' decision-

making ability dramatically and makes air traffic management much easier.

XIII. CONCLUSION:

In this paper, we proposed a new ADS-B authentication framework based on three-level hierarchical identity-based signature (HIBS) with batch verification, which can significantly reduce the verification cost. Basing on the framework, we demonstrated two concrete schemes. The basic scheme supports only partial batch verification while the extended scheme provides full batch verification but requiring existing techniques to ensure the integrity of some public values. We gave a formal proof for the security of our extended scheme. The experiment results show that our proposed cheme is much more efficient than traditional ones.

XIV. REFERENCES:

[1] http://www.flightradar24.com
[2] Baek, J., Byon, Y.J., Hableel, E., Al-Qutayri, M.: An authen-tication framework for automatic dependent surveillance-broadcast based on online/offline identity-based signature. In: 8th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2013. pp. 358–363. IEEE (2013)
[3] Baek, J., Byon, Y.J., Hableel, E., Al-Qutayri, M.: Making air traffic surveillance more reliable: a new authentication framework for automatic dependent surveillance-broadcast (ads-b) based on online/offline identity-based signature. Security and Communication Networks (2014)
[4] Bellare, M., Garay, J.A., Rabin, T.: Fast batch verification for modular exponentiation and digital signatures. In: Advances in Cryptology - EUROCRYPT 1998. LNCS, vol. 1403, pp. 236– 250. Springer (1998)
[5] Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. Journal of Cryptology 17(4), 297–319 (2004)
[6] Camenisch, J., Hohenberger, S., Pedersen, M.Ø.: Batch verification of short signatures. In: Advances in Cryptology - EUROCRYPT 2007. LNCS, vol. 4515, pp. 246–263. Springer (2007)
[7] Costin, A., Francillon, A.: Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. Black Hat USA (2012)
[8] Feng, Z., Pan, W., Wang, Y.: A data authentication solution of ADS-B system based on x.509 certificate. In: 27th International Congress of the Aeronautical Sciences, ICAS 2010 (2010)
[9] Ferrara, A.L., Green, M., Hohenberger, S., Pedersen, M.Ø.: Practical short signature batch verification. In: Topics in Cryptology - CT-RSA 2009. LNCS, vol. 5473, pp. 309–324. Springer (2009)
[10] Fiat, A.: Batch rsa. In: Advances in Cryptology - CRYPTO'89. LNCS, vol. 435, pp. 175–185. Springer (1989)
[11] Gentry, C., Silverberg, A.: Hierarchical id-based cryptography. In: Advances in Cryptology - ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer (2002)
[12] Krozel, J., Andrisani, D., Ayoubi, M.A., Hoshizaki, T., Schwalm, C.: Aircraft ADS-B data integrity check. In: 4th Aviation Technology, Integration and Operations Forum. pp. 1–11 (2004)
[13] Mantilla-Gaviria, I., Leonardi, M., Galati, G., Balbastre-Tejedor, J.: Localization algorithms for multilateration (mlat) systems in airport surface surveillance. Signal, Image and Video Processing pp. 1–10 (2014), http://dx.doi.org/10.1007/ s11760-013-0608-1
[14] Mattern, F., Floerkemeier, C.: From active data management to event-based systems and more. chap. From the Internet of Computers to the Internet of Things, pp. 242–259. Springer-Verlag, Berlin, Heidelberg (2010), http://dl.acm.org/citation. cfm?id=1985625.1985645
[15] McCallie, D., Butts, J., Mills, R.: Security analysis of the ADS-B implementation in the next generation air transportation sys-tem. International Journal of Critical Infrastructure Protection 4(2), 78–87 (2011)
[16] Purton, L., Abbass, H., Alam, S.: Identification of ADS-B system vulnerabilities and threats. In: Australian Transport Research Forum. pp. 1–16 (2010)
[17] Sampigethaya, K., Poovendran, R.: Visualization & assessment of ADS-B security for green ATM. In: 29th Digital Avionics Systems Conference, DASC 2010. pp. 3.A.3–1 – 3.A.3–16. IEEE (2010)