ISSN: 0976-3104
SPECIAL ISSUE: Emerging Technologies in Networking and Security (ETNS)
Rose et al.

ARTICLE OPEN ACCESS

# EFFICIENT AND SECURE DATA TRANSMISSION IN AIR-CRAFTS

**Anto Rose, T. Praveen, Karthick, Marudhu Pandiyan***

*Department of Computer Science and Engineering, Vel Tech High Tech Dr.RangarajanDr.Sakunthala Engineering College, Avadi, Chennai, INDIA*

## ABSTRACT

***Aims:****Android is the majority popular platform for mobile devices. It facilitates distribution of data and services between applications using a affluent inter-app communication system. While access to resources can be restricted by the Android permission system, enforcing permissions is not satisfactory to prevent security violations, as permissions may be mismanaged, purposely or accidentally. Materials and methods:Security is the major issue in aircrafts . So in this paper we present some new security schemes for securing the data communication in aircrafts. We used a new technique that is used to replace conventional radar. For tracking the Aircrafts we are using ADS-B system. It is used for finding the current position of the aircrafts. It uses satellites for updating the current location of the aircrafts. The ADS-B system communicates with the satellite and continuously broadcast their position and other information such as the current velocity of the aircrafts and the movement of other nearby aircrafts. Results:If we communicate the aircrafts without the ADS-B it will create many problems like any active attacker can modify our confidential data. There are several kinds of aircraft attacks are available such as Ghost Aircraft Injection and Virtual Trajectory Modification attack. An active attacker can inject, modify and delete the messages. For avoiding all these things and for providing security we are using ADS-B authentication systems.* ***Conclusion:****It mainly focusing on data integrity. It uses cryptographic concepts for data encryption and Decryption. And also the signature matching and verification is used for security purposes.*

**Published on:** 08th– August-2016

KEY WORDS

*Authentication; ADS-B system; Integritry; Tracking; Batch Verification.*

***Corresponding author: Email:** drsowmyab1@gmail.com**Tel:** +91- 8884546649;

## INTRODUCTION

Now a days the usage of aircrafts has been increasing day by day. According to the statistics in Europe the number of registered aircrafts is around 26500 per day. Most of the persons are preferring to travel by air. Because of this Traffic and security problem arisen. The Airways traffic control is mainly based on the radars. For controlling the traffic in airways it uses two types of radars Primary Surveillance Radar(PSR) and Secondary Surveillance Radar(SSR). The Primary Surveillance Radar are fully independent and also it is non- cooperative [10]. The Primary Surveillance Radar is used for transmitting the signals with very high frequency and also it receives the echoes which is reflecting from other aircrafts. By the use of this echo from other aircrafts it will identify the position of the aircrafts. Without the usage or the participation of the particular aircraft we can find the location of aircrafts.

The Secondary Surveillance Radar(SSR) gathers information from the aircrafts all the aircrafts uses the onboard system which is in built in all kinds of aircrafts. Based on the onboard we can transmit our message is delivered to the Secondary Surveillance Radar. The information contains many useful information about the radars like the identification code of the particular aircraft, at what height it is flying and the altitude of the aircrafts.

Both the Primary Surveillance Radar and the Secondary Surveillance Radar has some disadvantages both are high cost and difficult to manage.

And also both the radars are not providing high security. The features of these two radars will not sets for Military based application. It does not maintains integrity, availability and confidentiality. Because of these drawbacks[2] we cannot use Primary Surveillance Radar and Secondary Surveillance Radar. The new technique is used for replacing the drawbacks which is available in the Primary Surveillance Radar and the Secondary Surveillance Radar. The Automatic Surveillance Broadcast System is used [5]. It replaces the Primary Surveillance Radar and Secondary Surveillance Radar . Most of the countries like Australia and Canada is using Automatic Surveillance Broadcast System. It is standardized by the Federal Aviation Administration. In the traditional radar system the

THE IIOAB JOURNAL
ISSN: 0976-3104

aircrafts only respond to the ground station. The Automatic Surveillance Broadcast System does not used Radars. It uses only the satellite [4] based on this it communicates to the ground station. Mainly it is based on the GPS. Based on the GPs it continuously broadcast their position to other aircrafts and also it broadcast the velocity and the height.

By the use of these information from the ground the ground controller can control and find out the current location of the aircraft [3] [8]. Because of this the pilot can take decision in an efficient manner and also it helps to control the traffic. The ADS-B system plays vital role in air ways traffic control and also in communication system. The mashup technology is to be used in the ADS-B system. The ADS-B combined with the mashup.

The ground controller can track or monitor the status of the aircrafts in their website. The ADS-B system broadcast their message through wireless channel . It transmits their message without the use of any cryptographic technique. The ground controller and the aircraft uses only the single low cost ADS-B receiver. The Active attacker can attack the data from the ADS-B system. So the ADS-B[9] system uses data integrity concept. In Data Integrity the data cannot be modified by anyone and also it uses source integrity.
Both the data integrity and the source integrity gives more security to the ADS-B system based data transmission. The source integrity is also otherwise known as authenticity. In source integrity while sending the message to the receiver before sending the message [13] itself it should get permission from the receiver. If the receiver or the ground controller has given permission then only it will start sending message. The batch verification is the additional security scheme which is to be used in the [12] aircrafts. It uses signatures if multiple signature is receiving the ground station the Batch verification scheme verifies all the signatures. The batch verification does not allow the partial verification of signature.

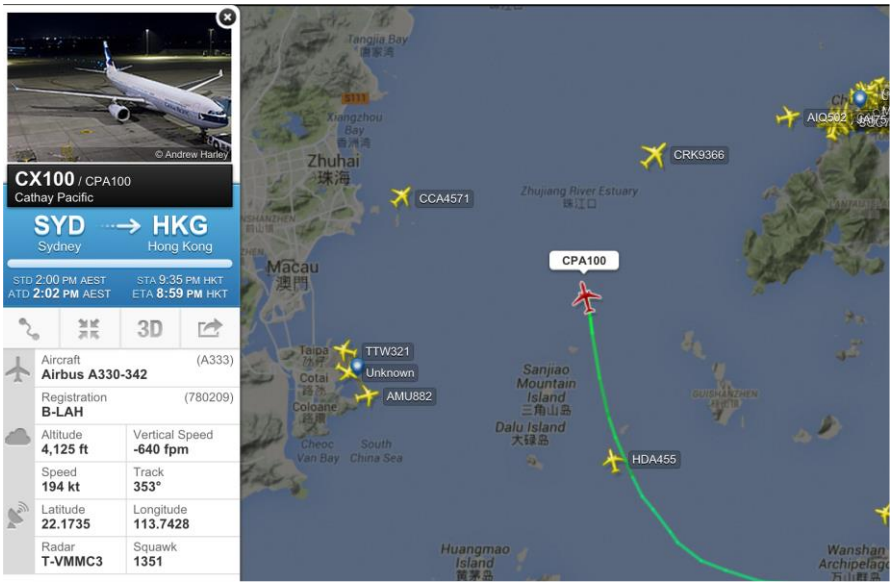


**Fig: 1.ADS- B Mashup**

The ADS-B is viewed from the ground by using some smart objects which gives the neat graphical representation on the web page of the ground controller.

**Contributions**

1. In this paper we proposed and used the efficient authentication method that is ADS-B authentication System.
2.Used Batch Verification Scheme in this each and the every airline has the responsibility to generate the private keys.
3. It uses two types of verification scheme one is partial verification scheme and the another one is batch Verification

THE IIOAB JOURNAL
ISSN: 0976-3104



## RELATED WORK

In this Security is the main issue so we used some integrity concepts for authentication. The Symmetric key encryption technique is used for encrypting or sharing the same key between the sender and the receiver. But it is very difficult to deploy the key values.

The Digital Signature is the good Method for Batch Verification and also it provides more authenticity than the Symmetric Key Encryption.

### *Tracking aircrafts*

The aircrafts can be tracked based on the ADS-B system. The ADS-B system uses GPS. It does not uses Radar. The Radar communication is not that much effective when comparing with the GPS Communication. It receives the signals from the other or nearby aircrafts based on that we can track the location of the aircrafts and also we can track the Velocity of the aircrafts. [4] [8]
The aircraft tracking is very difficult because of the traffic. Now a days all are using the airways to travel so the traffic is more. Because of this much traffic the security becomes one of the major issues in aircrafts.


**Fig: 2.Tracking Aircrafts**.

The ADS-S uses a special tool by the use of that tool the aircrafts are to be monitored in their web site.

### *Use of GPS in ADS-B*

The Radars are very costly and also it does not provides efficient and effective communication. The Gps is very easy to transmit the signal. The Aircrafts uses GPS for communicating to the ground station. The GPS periodically broadcast the signal.

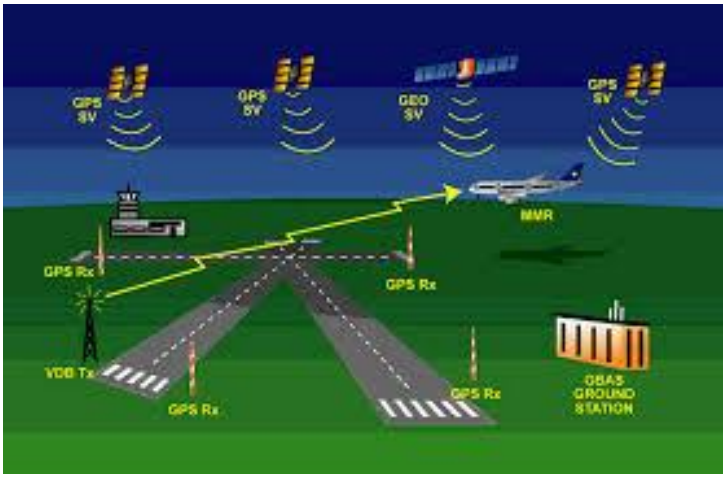


**Fig: 3. Aircraftsuses GPS for Data Transmission**

By the use of GPS the current location and the Velocity of the aircrafts can be tracked easily. Because of this the pilot can track the aircrafts and the decision making an we can control the traffic easily.

THE IIOAB JOURNAL
ISSN: 0976-3104

The GPS is very cheap comparing with the Radars.

## DEFINITIONS

### *Mathematical definition*

Let R and S are to be too cyclic graphs of prime order P. Let M be a generator of R. Then the bilinear map is to be represented by R x R →S.

1. Bilinearity: a,b = Z.
2. Non- degeneracy: If G is a generator of the graph G then the value of the G is not equals 1.
3. Computable: It uses some efficient algorithm to execute. The algorithm is e (u,v).

### *Hierarchical based signature*

There are three levels of Hierarchical identity Based signature. It is a tree based structure .In Hierarchial based signature the Level-0 is the root of the tree. In this all the signatures which are all storing in the database forms a tree based structure.

The airlines are the second levels of the hierarchical data structure. The ADS-B scheme uses Batch verification. $ID_i$, $Root^{A.}$ which is used for generating secret keys. The value $RT_i$belongs the secret key which is to be used in the $Root^{A.}$

## SECURITY MODELS

It uses three phases they are setup phase, Query phase and output phase. In setup phase it sends the query to the LEVEL -1 identity. $T^{*.}$ The value of C is used to generate the keys.

In the Query Phase the Query for the aircrafts $IG_c$ is to be generated.

In the output phase the message M are to be verified by using the signature.

1) Verify(M, IDA X M IDF x z) = 1;
2) A Extract A Query on IDA.
3) A Extract F Query on (IDA, IDF).
4) Signing Query on (IDA, IDF, M)

## CONTROLLING TRAFFIC

The usage of the aircrafts is increasing day by day so in aircrafts the security and the traffic control is the major issue.
For Controlling the traffics it uses the ADS-B authenticates System. It uses the GPS and sends or broadcast the signal to the ground station.

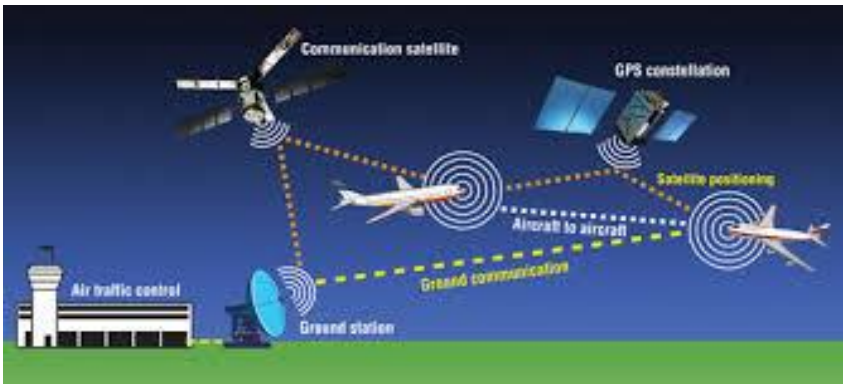


**Fig: 4. Traffic Control in Aircrafts**

The above image describes the traffic control system. Based on the GPS it tracks the signal coming from the Aircrafts and the Velocity of the aircraft. All the aircrafts contains onboard based on the onboard it transmits the signal to the ground station.

The Ground Station Controller uses mash up and they monitors all the movement of the aircrafts from the ground station if any traffic occurs they will sends message to the pilot. The pilot immediately changes the direction of the aircraft and also it tracks the velocity by uses all these we can track the flight easily.

The ADS-B system is used for tracking the aircrafts. Earlier the radars are use but it does not track the signal properly and also it is very difficult to maintain and also it is very costly. When comparing the ADS-B system with the Radar the Radars causes many aircraft accidents because it does signal properly and also it is very difficult to maintain and also it is very costly.

THE IIOAB JOURNAL
ISSN: 0976-3104



## PERFORMANCE

The usage of the ADS-B system reduce the traffic control and also it helps the ground station to track the aircrafts and also it guides the pilot to change the location if any problems occurs. In addition it uses batch Verification which is used for the security purpose and also it uses the partial verification of the signatures. It uses hierarchical tree based for storing the signature in the database

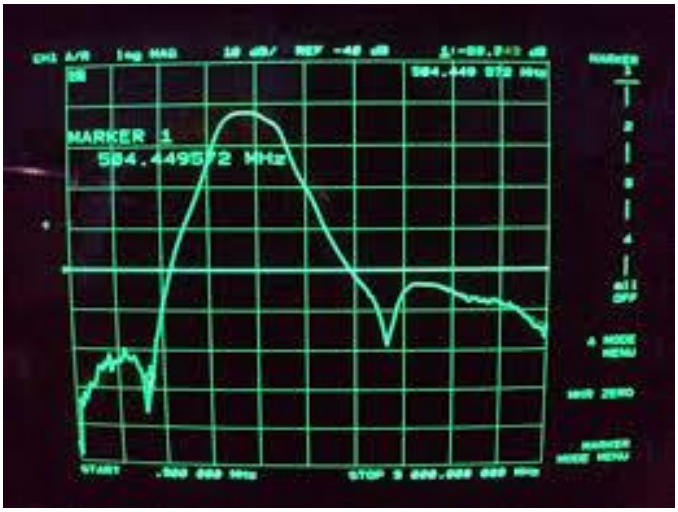


**Fig: 5. Performance Measure Of ADS-B System.**

……..

The above graphical diagram represents the performance of the ADS-B system compares with the radar. It Shows the performance comparison of ADS-B and the Performance of Radar comparing with the radar communication the ADS-B is much more better. Now a days most of the developed countries are using this system only. Because of high cost and the less performance automatically the usage of the radar is decreasing and also it does not provide that much security.

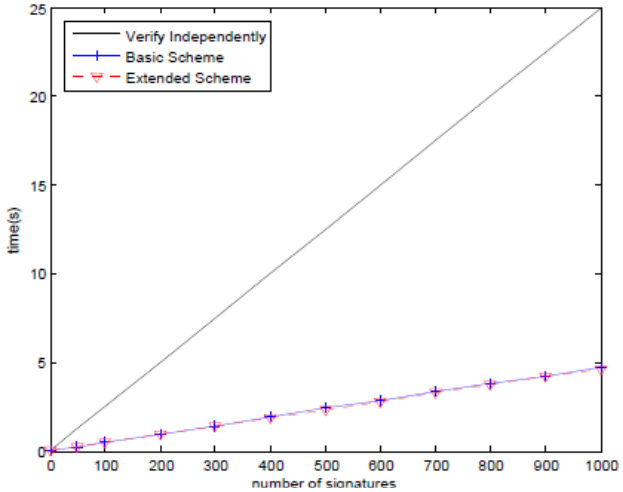


**Fig: 6. Performance Measure Of Batch Verification**

……..

The Batch Verification Scheme uses Signatures for the authentication Purpose. Before transmitting the singnal to the aircraft both the sender and the receiver.

## DISCUSSION

The ADS-B authentication scheme and the batch verification scheme is used for the security purpose. It uses Source integrity and destination integrity. Both the sender and the receiver has to verify the signature so it provides more security than other system.

THE IIOAB JOURNAL
ISSN: 0976-3104

## CONCLUSION

In this paper we propose the new and efficient scheme for the authentication scheme ADS-B and also it uses the three levels of the hierarchical structure for Batch verification it is used to reduce the verification cost. Based on the ADS-B system we can track the aircraft and also we can control the traffic. By the use of the Batch Verification we can verify the signature so that the security is high comparing with the previous one. The ADS-B uses GPS so the cost is low and also it uses source integrity and signature verification. Comparing with previous one this scheme is more effective and efficient.

## CONFLICT OF INTEREST

None declared.

## ACKNOWLEDGEMENT

None

## FINANCIAL DISCLOSURE

No financial support was received for this work.

## REFERENCES

[1] Sampigethaya K, Poovendra R. [2010]Visualization &assessmentof ADS-B security for green ATM. In: 29th Digital Avionics Systems Conference, DASC 2010. pp. 3.A.3–1 – 3.A.3–16. *IEEE*

[2] Sch¨afer M, Lender V, Martinovic I. [2013]Experimental analysis of attacks on next generation air traffic communication. In: Proceedings of 11th International Conference on Applied Cryptography and Network Security, ACNS 2013. LNCS, 7954: 253–271. Springer

[3] Krozel J, Andrisani D, Ayoubi MA, Hoshizaki T, Schwalm C.[2004] Aircraft ADS-B data integrity check. In: 4th Aviation Technology, *Integration and Operations Forum*,1–11

[4] Baek J, Byon YJ, Hableel E., Al-Qutayri M.[ 2014]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

[5] Yoon, H., Cheon, JH, Kim, Y Batch .[ (2004)]verifications with id-based signatures. In: 7th International Conference on Information Security and Cryptology, ICISC 2004. *LNCS*, 3506: 233–248 Springer

[6] McCallie D, Butts J, Mills R.[ 2011] Security analysis of the ADS-B implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection*, 4(2):78–87

[7] Purton, L., Abbass, H., Alam, S.[ 2010] Identification of ADS-B system vulnerabilities and threats. In: Australian Transport Research Forum. 1–16

[8] Samuelson K, Valovage E, Hall D.[ 2006]Enhanced ADS-B research. In: *IEEE Aerospace Conference*, 1–7. *IEEE*

[9] Sch¨afer M, Lenders V, Martinovic I.[2013] Experimental analysis of attacks on next generation air traffic communication. In: Proceedings of 11th International Conference on Applied Cryptography and Network Security, *ACNS* 2013. *LNCS*, 7954: 253–271

[10] Strohmeier, M., Lenders, V., Martinovic, I.: Security of ADS-B:State of the art and beyond. CoRR abs/1307.3664 (2013)

[11] Strohmeier, M., Lenders, V., Martinovic, I.: Lightweight location verification in air traffic surveillance networks. In: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security. pp. 49–60. CPSS '15, ACM, New York, NY, USA (2015), http://doi.acm.org/10.1145/2732198.2732202

[12] ] Strohmeier M, Sch¨afer M, Lenders V, Martinovic I..[2014] Realities and challenges of nextgen air traffic management: The case of ADS-B. *IEEE Communications Magazine* 52(5):111–118)

[13] Wesson KD, Humphreys TE, Evans BL.[2004] Can cryptography secure next generation air traffic surveillance? *IEEE Security & Privacy Magazine*

[14] Yoon H, Cheon JH, Kim Y.[2004] Batch verifications with id-based signatures. In: 7th International Conference on Information Security and Cryptology, *ICISC* 2004. *LNCS*, 3506: 233–248