International Journal of Intelligent Computing and Technology
IJICT
ISSN: 2457-0249 (Online)
Website: https://ijict.com 2018 (June)−Vol.2, Iss.1 Page: 25−29

# An ADSB Security Implemented for Data communication Using Ad-Hoc Network

V Suresh Kumar[1] & R Govindaraju[2]

[1,2]Assistant Professor, Department of Computer Science, Sasurie College of Arts and Science, Vijayamangalam, Tamilnadu, India

Suresh091289@gmail.com, r.govindaraju89@gmail.com

Article History: Received: March 2018; Published: June 2018

## ABSTRACT

Data communications are currently considered as a key enabler in the modernization of the aviation industry. Current aircraft are becoming equipped with advanced data communication capabilities, whereas the aviation stakeholders are seeking for new communication solutions to face the increasing air traffic load. Thus, we can expect to see large scale aeronautical ad hoc networks which could be used to meet those needs in the near future. This paper discusses the security issues to be addressed in routing protocols defined in the scope of aeronautical ad hoc networks. Existing routing approaches are briefly discussed, then a secure geographical routing protocol for future aircraft ad hoc networks is proposed. Finally the protocol is formally verified and its performances are discussed.

**KEYWORDS: Big Data, Health Care Systems, Electronic Health Records**

## INTRODUCTION

Currently, the aviation industry is about to evolve and great amendments are being discussed in order to define the ATM (Air Traffic Management) of the future. Indeed, the aviation stakeholders emphasized the emergency to address disabling issues such as air traffic growth or radio voice frequency congestion. Besides, airline companies are willing to improve their customer services to attract more passengers and remain competitive in the airline business market. CNS (Communication, Navigation, and Surveillance) technologies are particularly concerned as they represent the pillars of the operational tools used daily by the aviation actors (e.g. air traffic controllers, pilots, airline operators).

In order to fulfill such a purpose, CNS technologies are definitely shifting the paradigm of digital data for the future aviation. Information Technology progresses made in last decades, avionic systems and air ground networks are increasingly relying on software and data. The "connected aircraft" is certainly the key enabler of future aviation transportation systems. It expands the sphere of software and data to all the aircraft components and operations such as advanced embedded avionics in the cockpit, or high data-based communication capabilities between aircraft and ground stations.

For the time being, AANETs (Aeronautical Ad hoc Networks) is a top research topic in area. Their feasibility on both continental and transatlantic aeronautical areas has already been demonstrated in many studies [1]. AANETs represent a particularly challenging class of MANETs (Mobile Ad hoc Networks) where an aircraft acts as a self aware node and communicates with other aircraft and ground entities.

## AANETS ROUTING SECURITY ISSUES

There are several contributions throughout the literature in the scope of routing protocols for AANETs. These work have mainly focused on key routing operations (e.g. route establishment and maintenance) and QoS (Quality of Service) performances (e.g. minimize routing overhead and delays) with the same aim to provide an efficient and reliable routing scheme for AANETs. Nevertheless, all these solutions have been designed without security considerations in mind which leaves them defenseless against typical MANET attacks such as selective forwarding, byzantine or sinkhole attacks. In order to make one step forward from a theoretical to an operational AANET, airlines need to be convinced by the security of this kind of infrastructure. Indeed, the main challenge is to guarantee the confidentiality of airline data (e.g. kerosene consumption policy) when AOC packets are transmitted hop-by-hop to the destination.

Besides, in order to maximize the aircraft connectivity (white edges in figure 1), one may reasonably expect that future AANETs will involve aircraft belonging to different airlines. In order to tackle the confidentiality of interairline communications in future AANETs, a secure routing protocol can be an interesting idea to investigate. From a routing scheme point of view, security must preserve the reliability and accuracy of routing processes within a malicious environment: the route discovery step should guarantee valid route paths whereas the data forwarding process should prevent malicious/selfish nodes of dropping or modifying a packet. Extending these requirements, a routing protocol designed for AANETs has to secure the aircraft geographic position as well as the airline data packet when transmitted from one node to another. We will come back to these specific requirements in section V.

In order to meet these requirements and accommodate the lack of security in existing AANET routing protocols so far, we propose in this paper a secure geographical routing protocol based on the GPSR (Greedy Perimeter Stateless Routing) protocol and the ADSB (Automatic Dependent Surveillance Broadcast) protocol used to retrieve the aircraft position. Our work is an improvement of the hybrid ADSB/GPSR system provided. It presents a brief overview of existing AANET routing protocols. Security Protocols and Applications) tool, then simulation results are discussed.

## AANETS ROUTING SECURITY REQUIREMENTS

Security of geographical position information: data integrity should not be comprised since the aircraft position is usually used to build the neighbour table and find the destination node location when a packet has to be routed. If an attacker succeeds in modifying this information, he could cause data packets to be sent to wrong destination or simply re-routes all the traffic to a sink.

Airline data confidentiality: as discussed in section II, interairline communication is a prerequisite in AANETs. A trade-off between aircraft connectivity and airline data security has to be found. Data forwarding along the discovered route should be secured against non-authorized AOC information access. If each aircraft holds the right cryptographic key in the network, airline data confidentiality will be ensured. The secure geographical routing protocol presented in the next section takes into account the security requirements mentioned above, it also minimize the routing overhead due to some control and beacon messages used in other geographic routing protocols.

## ADSB AND GPSR PROTOCOLS

ADSB is a cooperative surveillance system for ATS. Any ADSB equipped aircraft is able to periodically broadcast its own state vector containing important flight related information (e.g. 3D position, velocity, aircraft identifier) to other aircraft. ADSB is the future data- based surveillance system, it provides more accurate and rich information than the traditional radar technology used today. GPSR is a well-known geographic routing protocol

### Data integrity

The ADSB security has been investigated in several work. McClain et al. provided a complete survey of ADSB vulnerabilities. Among them, data integrity is major concern. In our system, as ADSB will be used to build the neighbour table, we used a hybrid hash function cryptographic signature block to provide ADSB message integrity.

### GPSR secure routing

The first step is to build the neighbour table using the ADSB secure geographic position explained in the previous sub-section. Then, we use the same GPSR greedy/perimeter routing schemes to find the closest neighbour node to the destination. However, as explained in section I, we need here to compute a 3D Euclidean distance. Before sending the packet, the source node encrypts the payload data if and only if the destination node belongs to a different airline. This is done using the ICAO (International Civil Aviation Organization) identifier binded in the ADSB messages for each aircraft. Intermediate nodes on the routing path will be able to decrypt the message only if they belong to the same airline. Then, for each airline company, we use a pair of public/private keys. Such a key's pair can be either embedded before aircraft take-off or dynamically distributed using a PKI (Public Key Infrastructure).

## SIMULATION

Network Simulator 2 has been used to evaluate secure protocol. For generate the keys for the encryption and signature operations cryptic crypto algorithm used. Aeronautical Network Service Provider (ANSP) used to manage real time traffic. Automatic Dependent Surveillance-Broadcast protocol used to retrieve the aircraft position. Performance metrics used for comparing the original GPSR protocol and ANSB routing protocol are packet delivery ratio, the routing overhead (i.e. control routing packets), and end to end delay.

## CONCLUSION

In this paper, we have presented the design and evaluation of an ADSB based secure geographic routing protocol for AANETs. Many routing protocols for AANETs have been provided using different routing approaches, but all of them have assumed a trusted and secure inter aircraft environment. Confidentiality issue in AANET has been considered and deployed in this paper. Various simulation studies were conducted using different protocols such as GRAA, GPRS and ADSB protocols and understands that airline density varies when topology varies.

## References

1. F. Besse, A. Pirovano, and J. Radzik (2010), Wireless adhoc network access for aeronautical communications.
2. EUROCONTROL, Communications operating concept and requirements for the future radio system, 2002.
3. S. Hyeon, K. Kim, and S. Yang (2010), A new geographic routing protocol for aircraft adhoc networks. In 29th Digital Avionics Systems Conference
4. M. Iordanakis and G. Dilintas (2007), Arpam routing protocol vulnerabilities in aanets. In 2nd International Scientific Conference eRA, September 2007.

**How to cite this article:**

**V Suresh Kumar & R Govindaraju, “An ADSB Security Implemented for Data communication Using Ad-Hoc Network”, IJICT, Vol.2, Iss.1, 25-29, 2018**