An ADS-B based Secure Geographical Routing Protocol for Aeronautical Ad Hoc Networks

Mohamed-Slim Ben Mahmoud, Nicolas Larrieu

An ADS-B based Secure Geographical Routing Protocol for Aeronautical Ad Hoc Networks

Mohamed Slim Ben Mahmoud
and
Nicolas Larrieu
ENAC, TELECOM
F-31055, Toulouse, France
slim.ben.mahmoud@recherche.enac.fr
nicolas.larrieu@enac.fr

***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*-Network Security; Routing; AANETs**

I. Introduction to Aeronautical Ad Hoc Networks

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. Thanks to IT (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 the 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 as shown in figure 1:

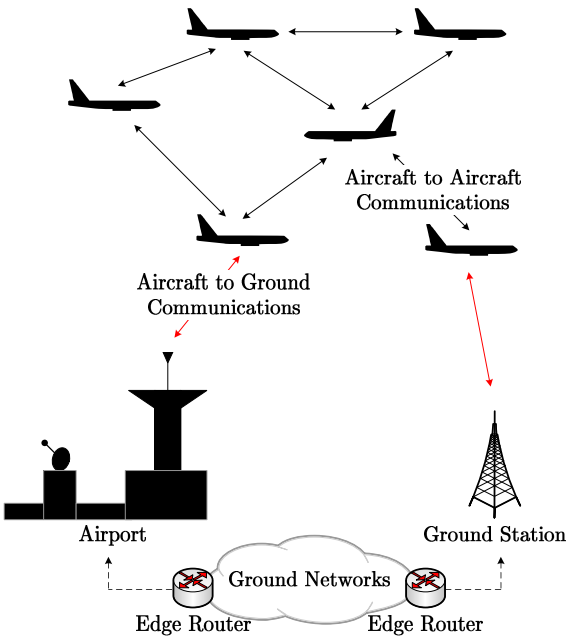

Figure 1. AANET Network Topology

Similarly to VANETs (Vehicular Ad hoc Networks), AANETs are characterized by very high mobility of nodes and limited degrees of freedom in movement patterns. These networks can be used to provide a plethora of aeronautical services such as ATS (Air Traffic Services) and AOC (Airline Operation Communication) safety services [2], Internet connection for onboard passengers, or more long-term applications such as electronic duplication of black box data.

These emerging network systems require specific routing protocols to cope with aeronautical environment constraints. For instance, in classical MANETs, nodes can move freely and randomly whereas in AANETs, aircraft move along a predetermined route according to a flight plan. Besides, usually MANETs use a flat geographic position information (2D) whereas AANETs use a 3D information to locate the aircraft. Figure 2 illustrates pre-determined NATs (North Atlantic Tracks) which are aircraft (red dotes) routes computed daily for flights between Europe and United States [1]:

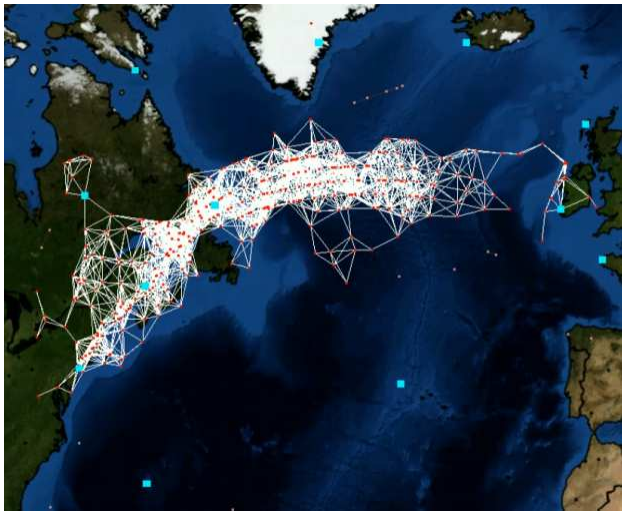

Figure 2. AANET Connectivity in Oceanic Area

These aircraft patterns can be useful in order to optimize the routing scheme performances and meet high performance requirements. For instance, Landing clearance or weather reporting are not delay-tolerant applications, meaning that on-demand routing protocols are not recommended for AANETs (on-demand routing approaches induce high latency because of the route discovery process).

II. 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 2), one may reasonably expect that future AANETs will involve aircraft belonging to different airlines.

In order to tackle the confidentiality of inter-airline 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 [5] and the ADS-B (Automatic Dependent Surveillance-Broadcast) protocol [9] used to retrieve the aircraft position. Our work is an improvement of the hybrid ADS-B/GPSR system provided by Seo et al. in [11].

This paper is organized as follows. Section III presents a brief overview of existing AANET routing protocols. Section IV discusses related work while section V provides AANETs routing security requirements to be fulfilled. Section VI presents our secure geographical routing protocol for AANETs. Section VII provides a formal verification of the protocol using the AVISPA (Automated Validation of Internet Security Protocols and Applications) tool, then simulation results are discussed. Finally, an overview of future work is given in VIII.

III. Overview of AANETs Routing Protocols

Figure 3 shows a classification of existing routing protocols in AANETs according to the network structure adopted in the protocol design. We distinguish topology-based protocols, which regroups proactive, reactive, and hybrid routing schemes, and geographic protocols which require the assistance of a GPS (Global Positioning System) to provide the node's positions. As far as modern aircraft are already equipped with reliable positioning and navigation satellite-based GPS systems, we think that this class of routing protocols is quite suitable to the AANETs context.

Besides, from a delay point of view, position aided routing protocols should provide good performances compared to topology-based protocols since there is no need to maintain routing tables or set-up route paths before sending a packet: this a noticeable advantage with regard to the strict latency performances needed for aeronautical services. From now, we consider only geographic-assisted routing protocols.

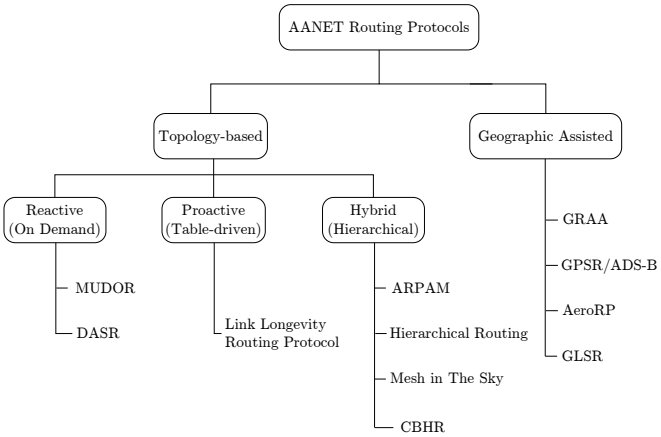

Figure 3. Classification of AANET Routing Protocols

Hyeon et al. presented the GRAA (Geographic routing Protocol for Aircraft Adhoc Networks) protocol in [3]. The GRAA routing scheme behaves differently, depending on aircraft movements. Each aircraft hold a neighbor table periodically updated in order to keep track on the moving direction of its one hop neighbor. The next hop is decided using a predictive heuristic on both the expected geographical position of the destination and the node velocity.

Peters et al. proposed the Aeronautical Routing Protocol (AeroRP) [8] for telemetry data among AANETs. The routing decision in AeroRP is based on a speed heuristic calculated for each one-hop neighbor of the node holding the packet. This decision metric is calculated by the source node for all its neighbors in order to know which one will be the sooner in the transmission range of the destination.

Medina et al. introduced the GLSR (Geographic Load Sharing Routing) [7] protocol for the airborne Internet. GLSR exploits path diversity to compensate congestion issues using the TDMA technique. GLSR reduces the link congestion by using multipaths and maximizes the speed of advance of all neighbors toward the destination. The advance is defined as the difference between two geographical distance (respectively from the neighbor and the source node) to the destination.

The integrated ADS-B/GPSR system will be discussed in section 4. In our comparative study of section VII-B, we selected GRAA and the integrated ADS-B/GPSR system as both are based on the GPSR routing algorithm. Our choice is mainly driven by the high performance of GPSR in MANETs and VANETs, its flexibility, and adaptability to the AANET environment.

IV. Related Work

As for now, AANET routing security has been barely discussed in few work. Sampigethaya et al. discussed AANET security as a major concern in future data-based aeronautical communications [10]. Emerging threats and potential vulnerabilities have been identified, then security requirements and mitigation solutions have been presented. Routing vulnerabilities have just been discussed as an issue to be mitigated in the scope of jamming and side-channel attacks: there is no further security analysis on AANET routing protocols themselves.

Iordanakis and Dilintas provided a vulnerability assessment of the ARPAM (Adhoc Routing Protocol for Aeronautical Mobile Adhoc Networks) routing protocol for AANETs in [4]. They discussed the security shortcomings resulting from the protocol design such as message tampering and selective forwarding. However, they have not provided a mitigation solution to cope with these vulnerabilities.

V. AANETs Routing Security Requirements

The AANET routing security requirements can be summarized as the following:

- *Security of geographical position information*: data integrity should not be comprised since the aircraft position is usually used to build the neighbor table and find the destination node location when a packet has to be routed. If an attacker succeeds in modifying these 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, inter-airline 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.

VI. A Secure Geographical Routing Protocol for AANETs

As mentioned in section II, our proposal is build upon a system integration of ADS-B and GPSR protocols. We first summarize the hybrid ADS-B/GPSR system before introducing the security improvements made for both protocols.

A. System Integration of ADS-B and GPSR Protocols

ADS-B is a cooperative surveillance system for ATS. any ADS-B 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. ADS-B 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. It uses two routing schemes: a greedy mode and a perimeter mode. In greedy mode, GPSR forwards a packet to the closest node in the neighbor table to the destination. If the forwarding node is itself the closest node to the destination, GPSR switches to the perimeter mode. When the forwarding node finds a neighbor that can greedily forward packets, it ends the perimeter mode and starts the greedy mode again. The information on one-hop neighbors is obtained by a beaconing scheme, while the position of the destination is obtained by a location service.

However, GPSR uses a beaconing scheme for the neighbor table and location service, which increases the control packet overhead and collision probability. The ADS-B and GPSR hybrid system provided by Seo et al. and illustrated in figure 4 totally eliminate the GPSR beaconing overhead. Indeed, instead of sending control packets to build its neighbor table, GPSR uses the state vector that is included in ADS-B messages. Such a table is updated every second for freshness matters.

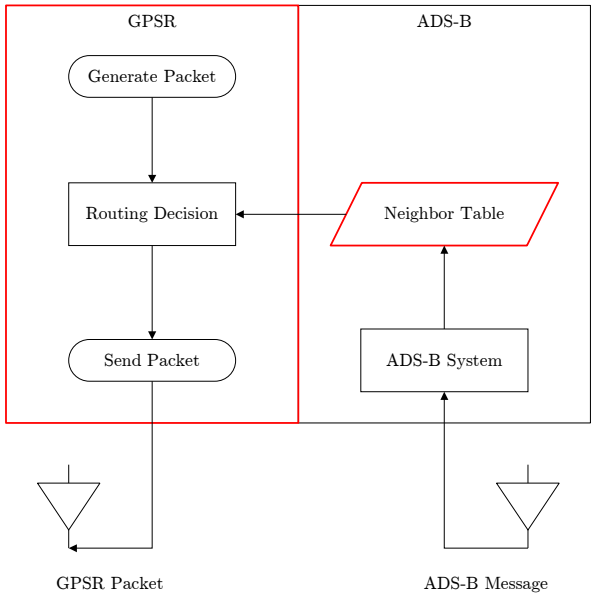

Figure 4. System integration of ADS-B and GPSR protocols

From a performance point of view, we found this system integration interesting for the aeronautical context where performance constraints are very strict. However, from a security point of view, neither ADS-B messages nor GPSR routing packets are secured. Thus, next we present two solutions: firstly, a solution to provide message integrity in ADS-B equipped aircraft; secondly, we will describe an improved GPSR secure routing protocol.

B. ADS-B data integrity

The ADS-B security has been investigated in several work. McCallie et al. provided a complete survey of ADS-B vulnerabilities in [6]. Among them, data integrity is a major concern. In our system, as ADS-B will be used to build the neighbor table, we used an hybrid hash function/cryptographic signature block to provide ADS-B message integrity. Figure 5 illustrates the proposed mechanism:

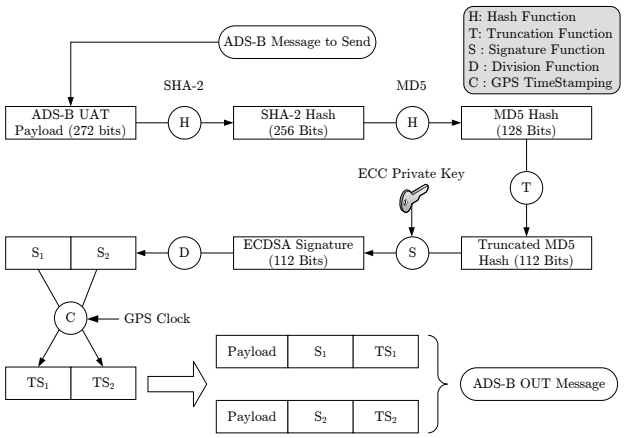

Figure 5. ADS-B Data Integrity Mechanism

We used a 272 bits length UAT (Universal Access Transceiver) ADS-B format [9]. Indeed, unlike other ADS-B systems (*e.g.* 1090ES), this UAT format provides an additional reserved field for future development and experimental use. However, the reserved field has a limited length (128 bits), then we managed to find a solution that maximize the security and in the same time, fit in the reserved field.

For this purpose, we first used two successive has functions: a 256 bits SHA-2 (Secure Hash-2) hash followed by a 128 bits MD5 (Message Digest 5) hash. For the signature mechanism, we used ECDSA (Elliptic curve digital signature algorithm) which provides a good trade-off between robustness and security overloading. As a matter of example, given a 112 bits private key length, ECDSA provides a 224 bits signature whereas RSA (Rivest Shamir Aldman) provides a 2048 bits signature. However, the hash digest length is larger than the 112 bits ECDSA input block size, meaning we need to truncate the hash before the signature.

At this point, one may expect a truncation after the first hash function (without adding a second hash), but as the truncation increases, the collision probability on the hash also increases. Thus, we managed to truncate on 16 bits from the 128 bits MD5 digest instead of 144 bits from the 256 bits SHA-2 digest. Then, we divided the signature into two separate message (S_1 and S_2), computed a timestamp for each (respectively T_1 and T_2), then send them into two successive ADS-B messages. When both packets are

received, the destination rebuilds the whole signature using the timestamps and the GPS clock, recomputes in its own the signature resulting from the payload he received, then compares both signature : if they match, the ADS-B message is authenticated and assumed secure.

C. GPSR secure routing

Figure 6 shows the improvement we made to the original GPSR protocol in order to cope with the inter-airline privacy issue:

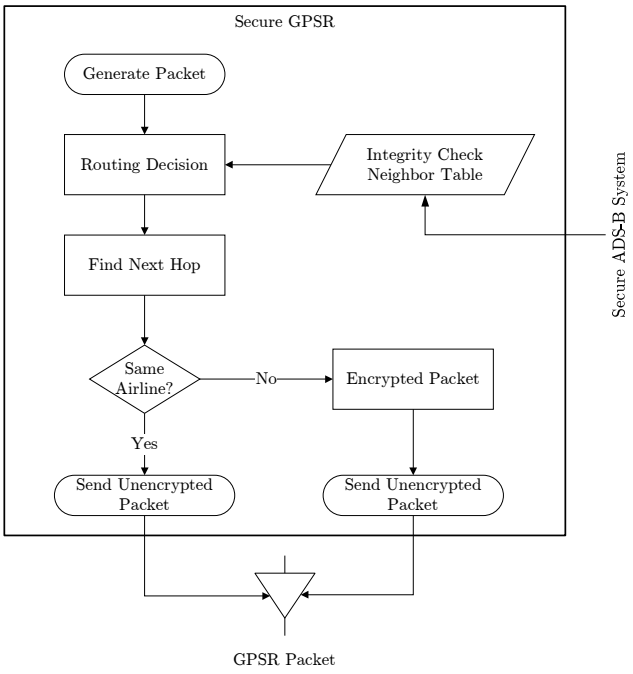

Figure 6. Secure GPSR Routing Scheme Improvement

The first step is to build the neighbor table using the ADS-B secure geographic position explained in the previous sub-section. Then, we use the same GPSR greedy/perimeter routing schemes to find the closest neighbor 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 ADS-B 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). This key distribution issue will be discussed as a future work in section VIII.

VII. Validation and Simulation

A. Formal Validation

In order to verify our proposal, the formal automatic security analyzer AVISPA has been used. The formal verification procedure has been divided into two steps: first we have specified the protocol using HLPSL (High Level Protocol Specification Language). Then, we used these protocol specifications to verify that the security requirements are met. AVISPA uses 4 different checking back-ends for the verification: the execution of the protocol specification under these back-ends exhibits safe results and thus validate our proposal.

B. Simulation Results

We used NS2 (Network Simulator 2) to evaluate our secure protocol. For the cryptographic components, we used the Cryptlib crypto tookit to generate the keys for the encryption and signature operations. Note that the NS2 CBR (Constant Bit Rate) traffic generator has been used according to AOC application requirements found in the COCR (Communications Operating concept and Requirements for the Future Radio System) [2] document. Besides, we managed to use real aircraft traffic patterns issued from the french ANSP (Aeronautical Network Service Provider) database instead of an adhoc mobility model. In the first part of the simulation, we aimed to compare our protocol to the original GPSR protocol, the original hybrid ADS-B/GPSR system, and another position-based AANET routing protocol, namely GRAA. The performance metrics used in the comparison are: the packet delivery ratio, the routing overhead (*i.e.* control routing packets), and end to end delay.

The second step of the simulation was to inspect our protocol behavior when the airline density in the AANET topology varies. Besides the three performance metrics listed above, we studied also the ratio of encrypted packets. Table I illustrates the three scenarios defined for the second part of the simulation. All the simulation results presented below are the average of 10 runs each.

Table I
Scenarios Definition

Scenario	Description
Heavy Load	Reference scenario, no changes to initial inputs
Medium Load	Aircraft belonging to the most represented airline are removed (-10% of heavy load)
Weak Load	Aircraft belonging to the less represented airlines are removed (-50 % of heavy load)

Figure 7 shows a comparison of four protocol performances according to the PDR, the routing overhead, and the end to end delay. Part (a) shows that our protocol has a higher PDR compared to GRAA and GPSR. Indeed, thanks to the use of ADS-B aircraft positions, our protocol is able to send a high ratio of data packet, whereas both

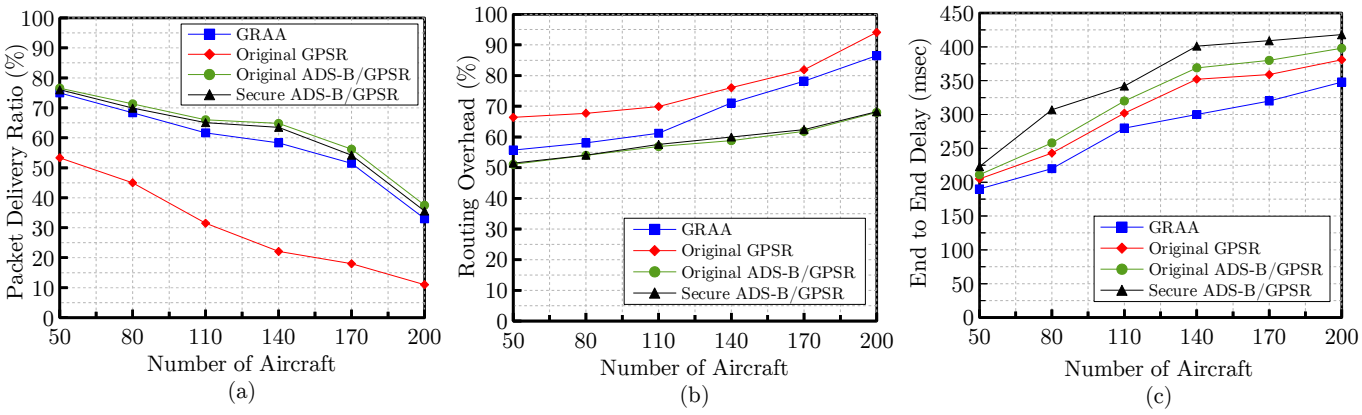

Figure 7. Performance Comparison of the Original GPSR, the Original Hybrid ADS-B/GPSR, the Secure Hybrid ADS-B/GPSR, and GRAA Protocols

GRAA and GPSR, need first to send beacon packets to build the neighbor table, then to locate the destination position. Quantitatively speaking, our proposal enhances the PDR by 3% compared to GRAA and 31% compared to GPSR.

Part (b) illustrates the evolution of control packet overhead as a function of aircraft number. Results show that both hybrid ADS-B/GPSR schemes (*i.e.* original and secure) have the lowest routing overhead ratios. Our protocol reduces the control overhead by 10% compared to GRAA and 17% compared to the original GPSR protocol. Indeed, the control packet overhead of GRAA and GPSR is caused by both the beacon messages (to construct the neighbor table) and the location service messages (to locate the position of the destination node). As for PDR, the difference with the original hybrid ADS-B/GPSR is inconspicuous as both protocols rely on ADS-B to overcome the beaconing scheme. Also, thanks to its lower overhead and higher PDR, our protocol exhibits a higher data throughput compared to GRAA and GPSR.

However, our protocol has a higher end to end delay compared to the other protocols as shown in part (c) of figure 7. Indeed, unlike GRAA, GPSR, and the hybrid ADS-B/GPSR protocols, securing data packets in our protocol implies additional processing time to encrypt or decrypt a packet by a node on the routing path. Figure 9 shows that the encrypted packet ratio increases as a function of the number of aircraft for our protocol, which is one explanation for the higher delay. Now, thinking outside the *"comparison"* box, the high delay exhibited by the secure ADS-B/GPSR protocol can be easily solved by using high processing devices for the encryption/decryption functions on-board the aircraft. Indeed, unlike *"classic"* MANET nodes where computation capabilities are usually limited, aircraft are able to carry heavy and strong computing devices.

Figure 8 illustrates the impact of airline density on the protocol performances under the scenario loads presented in table I. As we can see, except the PDR which remains slightly the same for the three scenario loads (the connectivity is not altered as far as there is always a routing path from the source to the destination node), the airline density has a more visible impact on both the routing overhead, encrypted packet ratio, and end to end delay.

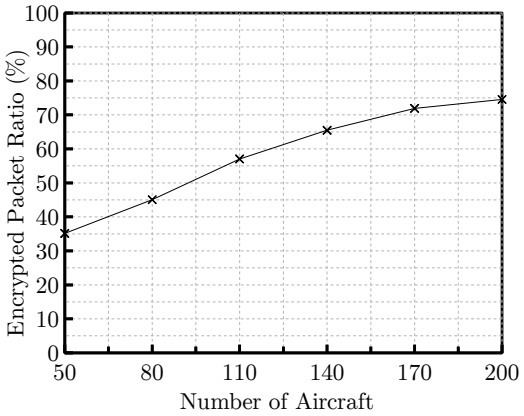

Figure 9. Percentage of Encrypted Packets (%)

The encrypted packet ratio decreases for the weak load scenario because the likelihood of having an aircraft of the same airline in the routing path increases, then the data packets are less encrypted compared to the medium and the high load scenarios (where the probability of having different airlines in the routing path increases). Besides, as discussed in the first part of the simulations, the routing overhead and the encrypted packet ratios are strongly related.

Even if the delay seems to decrease in the weak load scenario (the encryption and decryption time decrease as a function of the encrypted packet ratio), the most important observation in our sense is that it remains (for all three scenarios) always under the highest RCTP (Required

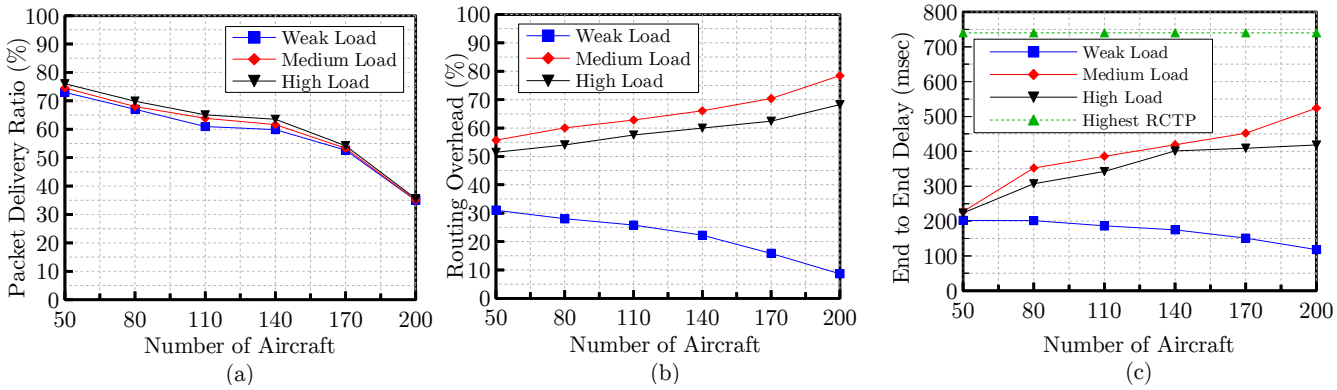

Figure 8. Performance Comparison of the Secure GPSR Protocol in Different Scenarios

Communication Technical Performances) delay constraint specified by EUROCONTROL for AOC services (and equal to 740 ms) [2]. However, we need to conduct additional simulations to find out when such a limit is reached (*i.e.* number of aircraft and airline density).

VIII. Conclusion

In this paper, we have presented the design and evaluation of an ADS-B based secure geographic routing protocol for AANETs. As we have shown, many previous routing protocols for AANETs have been provided using different routing approaches, but all of them have assumed a trusted and secure inter-aircraft environment. Instead, in designing our protocol, we considered the airline confidentiality security issue in AANETs, which will be, in our opinion, an inconvenience for the effective deployment of AANETs. We have also carefully selected the less expensive cryptographic primitives to secure both the geographic aircraft positions retrieved using the ADS-B protocol, and the packets routed using GPSR. Throughout several simulations, we have conducted a comparison study with GRAA, GPSR, and the original hybrid ADS-B/GPSR protocols, and we studied the behavior of our proposal when the airline density in the AANET topology varies.

As future work, we aim to improve the secure hybrid ADS-B/GPSR protocol using additional security features. Indeed, the secure routing protocol provided in this paper assumes that a pre-distribution key scheme is fully operational. This hypothesis gives rise to a separate, yet closely related, research field dealing with key management algorithms to support AANET secure routing protocol development. Thus, we plan to first discuss the existing key management schemes in MANETs/VANETs and their applicability to AANETs (*e.g.* distributed approach, centralized approach, based on threshold cryptography). Then we will provide a new key management scheme to support the secure routing protocol presented in this paper.

References

[1] F. Besse, A. Pirovano, and J. Radzik. Wireless adhoc network access for aeronautical communications. 2010.

[2] EUROCONTROL. Communications operating concept and requirements for the future radio system, 2002.

[3] S. Hyeon, K. Kim, and S. Yang. A new geographic routing protocol for aircraft adhoc networks. In *29th Digital Avionics Systems Conference*, 2010.

[4] M. Iordanakis and G. Dilintas. Arpam routing protocol vulnerabilities in aanets. In *2nd International Scientific Conference eRA*, September 2007.

[5] Brad Karp and H. T. Kung. Gpsr: greedy perimeter stateless routing for wireless networks. In *Proc. of the 6th annual international conference on Mobile computing and networking (MobiCom)*, 2000.

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

[7] D. Medina, F. Hoffmann, F. Rossetto, and C.-H. Rokitansky. A crosslayer geographic routing algorithm for the airborne internet. In *IEEE International Conference on Communications (ICC)*, 2010.

[8] K. Peters, A. Jabbar, E.K. Cetinkaya, and J.P.G. Sterbenz. A geographical routing protocol for highly-dynamic aeronautical networks. In *IEEE Wireless Communications and Networking Conference*, 2011.

[9] RTCA. Minimum aviation system performance standards for ads-b (do 242a). 2002.

[10] K. Sampigethaya, R. Poovendran, and Bushnell L. Security of aircraft ad hoc networks in the next-generation air transportation system. In *AIAA Aviation Technology, Integration and Operations Conference (ATIO)*, 2008.

[11] D. Seo, S. Kim, and Y. Suh. System integration of gpsr and ads-b for aeronautical ad hoc networks. In *IEEE Military Communications Conference*, 2008.