International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-170 PAGE NO: 1037-1042
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

SECURE ROUTING PROTOCOL FOR AERONAUTICAL AD HOC NETWORKS

S.RAMYA,
M.phil Scholar, Department of Computer Science,
Sri Vasavi College [SFW], Bharathiar University, Erode-638 316, India.
E-mail id: ramyagays@gmail.com, Ph: 8883304702

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, and 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.

1. 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.

Thanks to IT (Information Technology) progresses made in last decades, avionics 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

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-170 PAGE NO: 1037-1042
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

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. 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.

2. 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 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.

In aeronautical communications, three different service domains are typically distinguished: Air Traffic Control (ATC), Airline Operational Communications (AOC), and Aeronautical Passenger Communications (APC). ATC services are related to the safe and secure operation of flight, and comprise the communication between the cockpit crew and the air traffic controllers on the ground. A typical example for ATC services are flight clearances instructing a pilot to take a new heading. AOC services enable air lines to operate their fleets more efficiently by exchanging business related information such as catering information or the status of connecting flights, between the cockpit cabin crew and the airline operations center on the ground, but are generally not safety related. Finally, APC services are intended for the entertainment of passengers during

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-170 PAGE NO: 1037-1042
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

the flight. In this work, we will focus on APC services only.

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 ADS-B (Automatic Dependent Surveillance-Broadcast) protocol used to retrieve the aircraft position. Our work is an improvement of the hybrid ADS-B/GPSR system. This paper is organized as follows. Presents a brief overview of existing AANET routing protocol, Security Protocols and Applications tool, then simulation results are discussed.

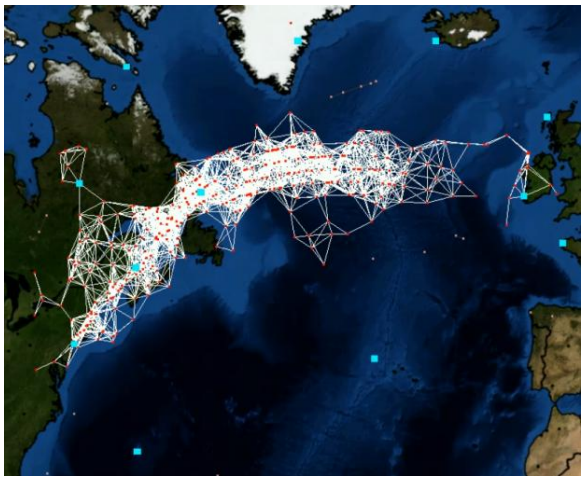

Fig.1. AANET Connectivity in Oceanic Area

3. 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 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: 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.

4. A SECURE GEOGRAPHICAL ROUTING PROTOCOL

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, and aircraft identifier) to other aircraft. ADS-B is the future data- based

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-170 PAGE NO: 1037-1042
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

surveillance system; it provides more accurate and rich information than the traditional radar technology used today. GPSR is a well known geographic routing protocol

B. ADS-B data integrity

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

C. GPSR secure routing

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. 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 banded 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).

5. 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 executions of the protocol specification under these back-ends exhibits safe results and thus validate our proposal.

D. Simulation Results

We used NS2 (Network Simulator 2) to evaluate our secure protocol. For the cryptographic components, we used the Cryptic crypto took it 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) 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 ADSB/GPSR system, and another position-based AANET routing protocol, namely GRAA.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-170 PAGE NO: 1037-1042
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

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.

6. 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.

7. FUTURE WORK

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.

To achieve security goals for Mobile Ad hoc Networks (MANET) has gained significant attention in recent year, MANETs are dynamic in nature. Any nodes can join and leave the network at any time.

8. 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.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-170 PAGE NO: 1037-1042
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

[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.