Authentication and integrity for ADS-B

Executive summary

Huge modernisation programs such as SESAR in Europe and NextGen in the U.S. have the ambitious goal to increase the safety, capacity, and efficiency of air traffic management (ATM) while at the same time decrease its ecological footprint and overall cost. A key component of these efforts is the transition from ground-based air traffic surveillance to a more accurate and more cost-efficient cooperative and dependent system, the Automatic Dependent Surveillance-Broadcast (ADS-B). Transponders equipped with ADS-B periodically broadcast surveillance information such as location, velocity, and identity over a digital data link. While this new approach has many advantages, its simplicity and the associated digitalisation come at a high price. Surveillance information is no longer provided by trusted ground infrastructure but by remote devices that are beyond control of the end user (e.g. air navigation service provider). Combined with the widespread availability of cheap yet powerful tools such as software-defined radios, this shift of trust poses a serious security threat as fake surveillance information can be injected into the ATM system over this wireless interface rather easily.

In order to fix the security problems of ADS-B in a sustainable way, authentication and data integrity must become an integral part of future versions of the protocol. This goal, however, constitutes a major challenge since the data link characteristics and the strong need for legacy compatibility render most cryptographic solutions unusable. ATM stakeholders and technology providers have jointly conducted several projects within the SESAR JU work package 15 with the goal to increase the capacity and security of the ADS-B data link. Project 15.04.06 in particular tested the feasibility of an additional legacy-compatible phase shift keying (PSK)-based ADS-B overlay. Such an overlay would increase the data volume that can be transferred in a single ADS-B transmission while preserving backwards compatibility. It could be used to add security-relevant information to ADS-B transmissions to provide authentication and integrity services. The SESAR JU project 15.04.06 demonstrated that such an overlay is indeed feasible and since then, the phase overlay has become a part of the ongoing standardisation efforts for the next ADS-B version that is likely to be published in the coming months. However, the performance in a realistic environment and the specific design of an authentication and integrity service based on such an overlay remain open questions. In fact, these two questions are strongly interdependent since existing broadcast authentication schemes need to be adapted based on the characteristics of the underlying data link.

This project aimed at answering these questions by first investigating the performance of the ADS-B phase overlay under real-world 1090 MHz radio frequency conditions and then using these insights to design a realistic ADS-B authentication and integrity protocol. More specifically, we integrated SeRo Systems' PSK-enabled ADS-B receiver GRX1090 into the testbed used by DISCO Lab in 2012 to evaluate attacks on ADS-B under realistic conditions. Using this testbed, we studied the bit error rate (BER) of different phase overlay configurations in a realistic radio environment and analysed the expected net data rate under the assumption that typical error correction codes such Reed-Solomon codes are used.

Based on the insights gained throughout these experiments, we devised a modified version of the Time Efficient Stream Loss-tolerant Authentication (TESLA) protocol that was originally proposed by Perrig et al. in 2002. We modified the original protocol with respect to trade-offs that account specifically for the missing (loose) time synchronisation required by TESLA, the comparably low number of bits that can be accommodated in the new phase overlay, the computational load at the receiver which may track high numbers of aircraft simultaneously, and a simplified key management scheme.

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287.