Abstract

Although air traffic is continuously increasing on a global scale, the next generation of management in this field is successfully handling this expansion and improving the safety of billions of future passengers. In this paper, Automatic Dependent Surveillance-Broadcast (ADS-B) was examined, which is a primary system, unlike traditional radar. This technology allows aircraft to automatically broadcast their intentions and location; however, it faces certain threats from which it requires some manner of protection. This paper discussed some techniques to encrypt and protect ADS-B messages. Staged Identity-Based Encryption (SIBE) was the most suitable means of solving the issues, providing, as it does, a sufficient level of security for ADS-B messages. In addition, the technique has attractive characteristics, such as confidentiality, efficiency, and a high enough degree of flexibility for effective key management and frequent encryption. This last attribute distinguishes the approach and renders it more popular than its peers.
1. THALES AIR SYSTEMS. air traffic management A guide to global surveillance, Parc tertiaire Silic ,

Index Terms

Computer Science  Security
Keywords

ADS-B, identity-based encryption, Staged Identity-Based Encryption (SIBE), encryption technique