IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)
Article number 9716665, 2021, Pages 7–11

Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio

TajDini, M.[a], Sokolov, V.[a], Skladannyi, P.[a]

[a]Borys Grinchenko Kyiv University, Kyiv, Ukraine

Abstract

This paper discusses the aviation Automatic Dependent Surveillance-Broadcast Vulnerabilities such as Sniffing and Spoofing over it with the help of Software Defined Radio (SDR) by looking at data frame structure and no encryption on this kind of message, we were able to capture 1090 MHz and 978 MHz signals and decoding them and gather all necessary information from it. Then we tried to have visual information by using VirtualRadar and online aviation databases. So we successfully could regenerate and encode messages with our data input and resend them at the same frequency as we captured 1090 MHz. That led us to a spoofing attack, which we could confirm by receiving our own generated messages. And in the end, we had an idea to use Long Short-Term Memory (LSTM) neural network to detect such spoofing attacks. © 2021 UkrMiCo 2021.

Author keywords

ADS-B; Mode S; SDR; sniffing; software-defined radio; spoofing

About this paper

https://ieeexplore.ieee.org/document/9716665

Online ISBN: 978-166542652-7
DOI: 10.1109/UkrMiCo52950.2021.9716665
EID: 2-s2.0-85126958490

First Online: 24 February 2022
Original language: English
Publisher: IEEE Inc.