IEEE 18th IEEE International Conference on Computer Science and Information Technologies (CSIT)
Article number 195025, 2023, Pages 1–5

Jump-Stay Jamming Attack on Wi-Fi Systems

Sokolov, V.[a], Skladannyi, P.[a], Platonenko, A.[a]

[a] Borys Grinchenko Kyiv University, Kyiv, Ukraine

Abstract

The growth of wireless technologies and the proliferation of smart devices increase the attack surface. As wireless networks become more widespread and critical in various sectors, the risk of jamming attacks increases. With an increase in the switching interval between frequencies, the average availability time increases, but periodically the connection with the access point is completely lost. When the switching time is commensurate with the time of the experiment, the values of the average speed cease to be indicative. The paper shows that it can be seen that jamming with a single noise generator on more pilots leads to an increase in the intervals, which reduces the effect of jamming. For each system, we should choose the optimal ratio between the number of frequencies for jamming and the number of transmitters. According to the results of the experiment, it can be seen that it is possible to concentrate energy only in limited parts of the spectrum, which makes it possible to effectively suppress the operation of Wi-Fi networks. To effectively counter this type of attack, dynamic frequency hopping of the pilot sub-carriers should be used according to a predetermined algorithm.

Author keywords

ADF435x; interference; jamming; SDR; software-defined radio; Wi-Fi

About this paper

https://ieeexplore.ieee.org/document/10324031

Online ISBN: 979-835036046-2
DOI: 10.1109/CSIT61576.2023.10324031
EID: 2-s2.0-85179844674

First Online: 27 November 2023
Original language: English
Publisher: IEEE Inc.