Abstract

Wireless networks overcame the limitations of the traditional approaches in the implementation of the wired networks. The number of nodes can be easily extended and provided with the services of the networks. Amenities of the private networks are risked by the invaders and their activities to disclose the confidential contents. These invaders established a standard mode of attacking by jamming the services upon described functions. The jammers would key in attack packets to the networks claiming to be a reasonable request to block the services of the intended users. Ultimately, the network would continue answering the meaningless queries of the attackers thereby avoiding or making the users to wait indefinitely. Increase in the attacks would degrade the services and standards of the wireless networks. Denial of Service (DoS) attacks involve mechanisms to flood the medium of data transfer with futile packets, or to alter the contents of the significant information of the packets. Denial of Service attacks have extended their area of attacks to pretense their identity and revises the contents of the message packets to pose a threat to the networks. Mechanisms that have been proposed to detect and mitigate the effects of those jammers are examined in this study.
- V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in IEEE INFOCOM, Mini-Conf., 2007.

Index Terms
Keywords

Jamming  detection mechanisms  wireless networks  network security