Computers and Electrical Engineering 36 (2010) 367–382

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks

Sudip Misra [a], Sanjay K. Dhurandher [b,*], Avanish Rayankula [b], Deepansh Agrawal [b]

[a] School of Information Technology, Indian Institute of Technology, Kharagpur, West Bengal, India
[b] CAITFS, Division of Information Technology, Netaji Subhas Institute of Technology, University of Delhi, New Delhi, India

ARTICLE INFO

Article history:
Available online 12 May 2009

Keywords:
Jamming
Security attacks
Channel surfing
Defence
Denial of Service
NS-2

ABSTRACT

The advent of wireless networks has brought a new set of security issues with it. One of the most feared of these is the jamming-based attacks. In this paper, we propose a pre-emptive detection strategy using honeynodes and a response mechanism based on the existing Channel Surfing Algorithm [Xu W, Trappe W, Zhang Y, Wood T. Channel surfing and spatial retreats: defenses against wireless denial of service. ACM Wireless Security 2004;80–9] to protect wireless nodes from a jammer. Honeynodes generate dummy communication at a frequency close to the actual frequency of operation, and pre-emptively alert authentic nodes of imminent attacks, so that the authentic nodes can jump to another frequency even before a jammer starts scanning that frequency. The next frequency is selected using a novel approach which uses a hybrid of reactive and proactive channel selection procedures. We have simulated the proposed approach using NS-2. The experimental results further prove a marked improvement in the performance of the proposed system over the Channel Surfing Algorithm in terms of the packet delivery ratio, the jammed duration, control message overhead and the number of channel re-configurations.

1. Introduction

The medium of communication shared by everyone in wireless networks introduces an interesting way of attacking wireless services: Jamming [1,12]. Jamming refers to blocking of a communication channel with the intent of preventing the flow of any information. Such an attack is a subclass of the Denial-of-Service (DoS) attacks [13,14,19], and is one of the most feared forms of attacks in wireless networks. This is because, with the existing network architecture, there is very little that can be done to overcome a jamming attack. Mitigation and prevention of jamming attacks is a topic in which lot of research is being undertaken currently. A detailed review of related existing literature will be presented in the subsequent sections.

Wireless networks are broadly classified into two categories: wireless infrastructure-based networks (e.g., WLANs and cellular networks) and infrastructure-less networks (e.g., ad hoc networks).

Wireless infrastructure-based networks consist of two major network components: base-stations (or access points) and mobile nodes. Mobiles nodes are connected to one another through a base-station, which, in turn, are, typically, connected through a wired distribution system. Fig. 1 shows a sample wireless infrastructure-based network with two base-stations and three wireless nodes. Every wireless node can be associated with only one base-station at a given time. On the other hand, a wireless ad hoc network is a decentralized wireless network. These networks are unlike managed wireless networks,

* Corresponding author.
E-mail address: dhurandher@rediffmail.com (S.K. Dhurandher)

0045-7906/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2009.03.013

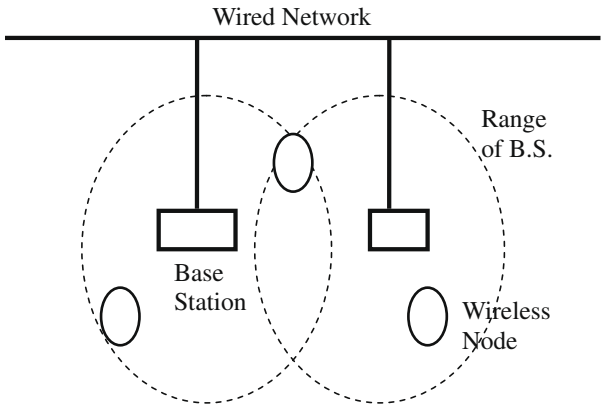

Fig. 1. A wireless infrastructure-based network.

in which an access point manages communication among other nodes. In this work, we restricted to jamming attacks in wireless infrastructure-based networks only.

The objective of this work is to propose an efficient algorithm to mitigate jamming attacks in wireless infrastructure-based networks. We intend to provide an efficient solution that can be easily incorporated in the existing network architecture, to achieve better robustness than the widely used Channel Surfing Algorithm [4] by using honeynodes along with dynamic channel prediction in wireless infrastructure networks.

Jamming-based DoS attack focuses on preventing networked nodes from communicating. The nodes could be both wired or wireless. The attacks are carried out with the help of a "jammer". A jammer is an entity that purposefully tries to interfere with the physical transmission and reception of communications. Fig. 2 shows a sample network of nodes under the influence of a jamming attack.

In the given scenario, the shaded node shown is a jammer, which disrupts communication in the normal network by jamming the darkened nodes. Since the darkened nodes are under the influence of a jammer, their communication with the remaining network collapses.

There are two classifications of jamming attacks [1]:

- Physical layer jamming.
- By ignoring MAC layer rules.

Physical layer jamming involves constant jamming of the medium of communication (in wireless networks this medium would be air) in order to incapacitate the nodes under its influence from participating in any further network activity. Attacks can also be instigated by not following the underlying MAC layer protocol properly. Jammers can make use of the vulnerabilities in the 802.11, 802.11b or 802.11g protocols [8,19] in WLANs.

Generally one of the following four methods is used for jamming [2]:

1. *Constant*: This kind of jammer continuously sends random bits of data on to a channel.

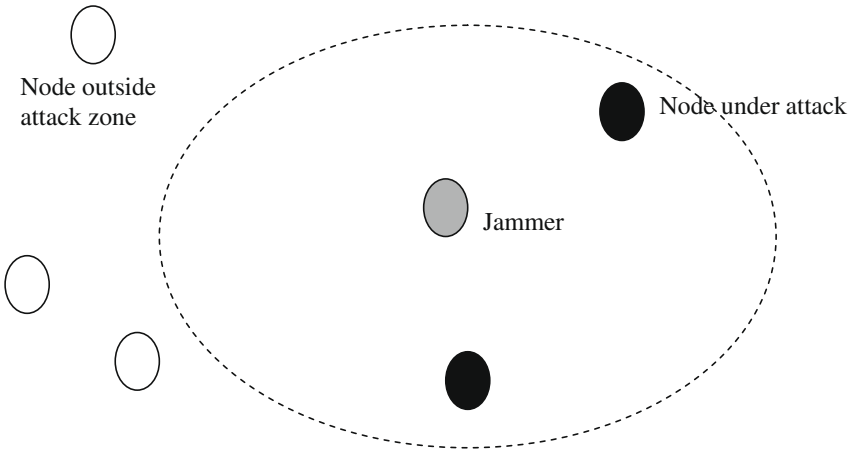

Fig. 2. A sample network of nodes under the influence of a jamming attack.