Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 26 – 33

Procedia
Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies
(ANT 2016)

Detection of Jamming Attacks in Mobile Ad Hoc Networks using Statistical Process Control

Mohammed-Alamine El Houssaini[a,]*, Abdessadek Aaroud[a], Ali El Hore[a], Jalel Ben-Othman[b]

[a] *Department of Computer Science, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco*
[b] *Department of Computer Science, Galilee Institute, Paris 13 University,* Paris, France

Abstract

A mobile ad hoc network is a group of mobile hosts that depends on wireless network interfaces with no use of fixed infrastructure or centralized administration. The main equipments of a mobile station are wireless transmitters/receivers. In this respect, the network can be seen as random chart because of the nodes ‘movement. The change of network topology relies on time when nodes move or adjust their transmission and reception parameters. The design of these networks is characterized by its vulnerability to denial of service attacks (DOS).Thus, it is very challenging. In this paper, the focus lies on a special kind of denial of service attacks called Jamming. Indeed, stations in a mobile ad hoc network share a wireless medium. Therefore, a radio signal can be jammed or interfered, which leads to the corruption and loss of the message .In this study , we suggest a new method of detection of that predictable attack by the application of the statistical process control (SPC). The SPC can be the key element of the detection of jamming attack, applied on the packet drop ratio (PDR) which refers as the number of dropped packets to the total of packets sent. The assimilation of this metric shows the nonconforming fraction. As we evaluated the performance, we substantiate that the control chart for fraction nonconforming based on the PDR detects the jamming attack in a real time by a visual graph.

Keywords: Mobile ad hoc network; IEEE 802.11; Jamming attack; Statistical process control.

* Corresponding author.
E-mail address: elhoussaini.m@ucd.ac.ma

doi:10.1016/j.procs.2016.04.095

1. Introduction

Jamming attack can deliberately lead to the stoppage or disruption of wireless communication. Interferences at the transmissions are due to jamming attack. It may appear on purpose by network load or in form of attack. A jammer can easily fulfilled by listening to the shared medium and transmitting in the same bandwidth as network, with no need of particular hardware.

The wireless medium causes various security threats to wireless networks[12]. Any station equipped with a transceiver can spy on going transmissions, inject fake messages, or block the transmission of legitimate ones. One of the essential keys for damaging the network performance is by jamming wireless transmissions. In the straightforward form of jamming, the scamper distorts transmitted messages due to interferences in the network's operational frequencies, and in closeness to the targeted receivers. As jamming attacks lower the performance of wireless networks, some effective methods are needed to detect their existence .Among techniques used in wireless medium, we have steady, tricky, reactive, smart, and random jammers.

Various metrics are used in the literature to describe jamming attacks [5]:

- Packet delivery ratio refers to the ratio overall number of packets correctly received to the total number of packets received.
- Packet sent ratio, which is measured at the transmitter side, is the total number of acknowledgments packets received to the total number of packets transmitted.
- Carrier sensing time can be seen as the time when a station has to wait for the channel to get inactive to start its transmission.
- Signal strength is meant the power that is clearly seen on the receiver end.

In our study, the focus will be on another metric for the jamming attack as we will highlight through the simulation results. This metric is called the packet drop ratio (PDR). This latter refers the number of dropped packets to the total of packets sent.

This paper is divided into six sections: The next section is about a concise summary of previous work done on jamming detection and classification in wireless networks. The third section provides an analysis on the impact of the jamming attacks. The fourth section explains our proposed model for the detection of the jamming attacks. The forth section, the authors evaluate the performance of their approach using NS2 simulator. The last section sheds light on conclusions and perspective.

2. Related work

In the nature of the wireless medium in ad hoc network, attackers can easily monitor communications between wireless devices and launch simple denial of service attack against wireless networks by jamming or interfering communication. In this respect, via conventional security mechanisms, such attacks in the physical layer cannot be detected. There are various attack strategies that a jammer can perform so as to overlap with other wireless communications. The authors in[5] classify the types of jammers as follow:

- Constant Jammer can be seen as the continuous emission of a radio signal that performs random bits.
- Deceptive Jammer refers to the fact that it does not transmit random bits instead of transmitting semi-valid packets unlike the continuous jammers. That is, the packet header is valid but the payload is useless.
- Random Jammer means the Alternation between two modes namely sleeping and jamming the channel. The first one jams for a random period of time (it can behave either like a constant jammer or a deceptive jammer), the second one (the sleeping mode) turns its transmitters off for another random period of time.
- Reactive Jammer‘s aim is not to waste resources by the fact of jamming when it senses the act of transmission. The key focus is on the receiver, trying to input as much noise as possible in the packet to modify many bits relying on less amount of power needed to modify enough bits so that when a checksum is performed over that packet at the receiver it will be grouped as not legitimate and therefore rejected.

Several approaches have been proposed in the literature for the detection of the jamming attack in wireless networks:

A new detection scheme for the jamming attack was suggested by the authors in[9]; the packet delivery ratio and signal strength were chosen as the jamming attack metrics for their system. The scheme utilizes a multimodal consistency check for jamming detection. Each node compares the value (packet delivery ratio, signal strength) with