Computer Networks 55 (2011) 2259–2270

Contents lists available at ScienceDirect

Computer Networks

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

Fight jamming with jamming – A game theoretic analysis of jamming attack in wireless networks and defense strategy

Lin Chen [a,*], Jean Leneutre [b]

[a] Laboratoire de Recherche en Informatique (LRI), CNRS, University of Paris-Sud XI and INRIA, 91405 Orsay, France
[b] Department of Computer Science and Networking, TELECOM ParisTech – LTCI CNRS 5141, 46 Rue Barrault, Paris 75013, France

ARTICLE INFO

Article history:
Received 22 June 2010
Received in revised form 7 March 2011
Accepted 13 March 2011
Available online 23 March 2011
Responsible Editor: P. Dowd

Keywords:
Jamming
Security game
Wireless network
Game theory

ABSTRACT

In wireless networks, jamming is an easily mountable attack with detrimental effects on the victim network. Existing defense strategies mainly consist of retreating from the jammer or rerouting traffic around the jammed area. In this paper, we tackle the problem from a different angle. Motivated by the high energy-consuming nature of jamming, we propose our defense strategy to defeat the jammer by draining its energy as fast as possible. To gain an in-depth insight on jamming and to evaluate the proposed defense strategy, we model the interaction between the jammer and the victim network as a non-cooperative game which is proven to admit two equilibria. We demonstrate analytically that the proposed defense strategy can eliminate the undesirable equilibrium from the network's perspective and increase the jammer's energy consumption at the remaining equilibrium without degrading the performance of the victim network. We also investigate the game dynamics by developing the update mechanism for the players to adjust their strategies based on only observable channel information. Numerical study is then conducted to evaluate the performance of the proposed strategy. Results demonstrate its effectiveness in defeating jamming, especially when the jammer is aggressive.

1. Introduction

1.1. Background and motivation

It is widely recognized that the broadcast nature of the shared wireless medium makes wireless networks extremely vulnerable to various attacks ranging from the passive eavesdropping to the sophisticated manipulation of routing information, among which an easily mountable one with detrimental effects on the victim network is jamming, a malicious attack whose objective is to disrupt the communication of the victim network by intentionally causing interference or collision at the receiver side. Usually launched at the PHY and MAC layers, jamming requires no special hardware and can virtually paralyze any wireless networks. [14] provides a taxonomy of different types of jamming in wireless networks. The detrimental degradation on throughput caused by the jamming attack in IEEE 802.11 WLANs is demonstrated in [2], in which the authors show that even the memoryless jamming attack can reduce the network throughput by up to 90%.

Besides traditional spread spectrum techniques at the physical layer (cf. [3,4]), the defense strategies in existing literature mainly consist of retreating from the jammer after detecting jamming or rerouting traffic around the jammed area. In [1], Xu et al. propose two strategies to evade jamming. The first strategy, channel surfing, is a form of spectral evasion that involves legitimate wireless devices changing the channel that they are operating on. The second strategy, spatial retreats, is a form of spatial evasion where legitimate devices move away from the jammer. In [5], Wood et al. present a distributed protocol

* Corresponding author. Tel.: +33 169153940.
E-mail addresses: Lin.Chen@lri.fr (L. Chen), Jean.leneutre@telecom-paristech.fr (J. Leneutre).

1389-1286/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2011.03.006

to map the jammed region so that the network can avoid routing traffic through it. The solution proposed by Cagalj et al. [6] uses different wormholes (wired wormholes, frequency-hopping pairs, and uncoordinated channel hopping) that lead out of the jammed region to report the alarm to the network operator. In [7], Wood et al. investigate how to deliberately avoid jamming in IEEE 802.15.4-based wireless networks. A recently proposed strategy consists of constructing a low-rate timing channel in the physical layer in spite of the presence of the jammer [11]. In [12], Awerbuch et al. propose a jamming-resistant MAC protocol for single-hop wireless networks with provable robustness against adversarial jammers. The authors of [20] and [21] study the effect of adversarial jamming in 802.11 networks.

Despite the different techniques used in existing solutions, they usually require frequency hopping capability or sufficient node mobility to avoid confronting the jammer. Such requirements might be too expensive to implement or even impractical in some scenarios, e.g., single-channel WLANs. Moreover, their effectiveness may be significantly reduced if the jammer is strategic, e.g., mapping the jammed area becomes more difficult if the jammer keeps moving in an unpredictable fashion.

1.2. Paper overview

In this paper, we tackle the problem of defeating jamming from a different angle. Our work is motivated by the observation that although a jamming packet of a few bits suffices to disrupt a transmitted packet, as argued in [8], yet continuously transmitting the jamming packets is energy-consuming and may quickly drain the energy of the jammer with limited battery supply. In other words, a jammer with limited energy resource can never succeed jamming the victim network for any extended period of time. This is especially the case where the jammer is restricted to a configuration similar to that of ordinary network nodes with limited energy resource such as laptops, e.g., an attacker with a mobile device aiming at jamming the WiFi-based hotspots in an airport. Given the above argument, an alternative defense strategy against jamming besides passively retreating, especially when it is impossible to move away from the jammer, is to actively fight the jammer face-to-face by draining its energy as fast as possible.

Following the above line of defense, we proceed our analysis as follows. Firstly, we formulate jamming as an optimization problem for the jammer whose goal is to block the communication of the victim network as long time as possible under its energy constraint. To this end, it controls the probability of transmitting jamming packets to strike a balance between keeping a high jamming probability and limiting the energy consumption. On the network side, each node adapts its channel access probability to maximize its utility under the jamming attack. We model the interaction between the jammer and the network as a non-cooperative game G. We show that G has two Nash equilibria (NE) and at one of them, the jammer can paralyze the network with little energy consumption. To avoid this inefficient NE for the network, we propose our defense strategy by introducing the anti-jammer, a special node dedicated to draining the jammer's energy. To achieve its goal, the anti-jammer configures the probability of transmitting bait packets to attract the jammer to transmit. We then formulate the new jamming game G' with the anti-jammer and show that G' admits a unique NE where if the anti-jammer chooses its strategy wisely, the network utility remains the same as that in G, but the jammer's energy consumption increases significantly. Next, we extend our efforts to investigate the dynamics of G' by developing an update mechanism in which the anti-jammer and network nodes adjust their transmission strategies based on only observable channel information.

1.3. Related work on game theoretical analysis on jamming

Recently, applying game theory [18] in different areas of wireless communication has attracted considerable research attention. Concerning jamming, Mallik et al. [13] model the problem of a victim node and a jammer transmitting to a common receiver in an on–off mode as a two-person zero-sum noncooperative dynamic game. Structures of steady-state solutions to the game are then investigated. Sagduyu et al. [15] model the denyof-service (DoS) attacks as stochastic games among non-cooperative selfish nodes that randomly transmit packets to a common receiver and malicious nodes with the dual objectives of blocking the packet transmissions of the other selfish nodes as well as optimizing their individual performance. The NEs are analyzed and the network performance is compared with the cooperative equilibrium. In [16], Li et al. formulate the jamming attack as optimization problem as well as max–min problem and derive the optimal attacking strategy for the jammer to maximize the duration before being detected and the optimal defense strategy for the defender to alleviate the attack damage. Altman et al. study the jamming game in wireless networks with transmission cost [9] and with partially available information [10].

1.4. Summary of contribution and paper organization

Compared with existing work, the focus of our work is not only to alleviate the damage caused by the jammer, but also to fight the jammer actively by draining its energy as quickly as possible. The main contributions of our work can be summarized as follows:

- *Game theoretic framework:* we establish a game theoretic model between the victim network and the energy-limited jammer and derive the NE.
- *Active defense strategy:* we propose an active defense strategy against jamming and demonstrate its benefits via both mathematical analysis and numerical experiment.
- *Distributed strategy update mechanism:* we derive a distributed update mechanism in which the anti-jammer and network nodes adjust their strategies based on observable channel information.