Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

pervasive and mobile computing

Fast track article

Performance analysis of CR-honeynet to prevent jamming attack through stochastic modeling[☆]

Suman Bhunia[a,*], Shamik Sengupta[a], Felisa Vázquez-Abad[b]

[a] Department of Computer Science and Engineering, University of Nevada, Reno, 89557, USA

[b] Department of Computer Science, Hunter College, City University of New York, 10065, USA

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Cognitive radio
Jamming attack
Honeynet
Stochastic model
Queuing theory
Queue with vacation

ABSTRACT

Cognitive Radio Network (CRN) has to stall its packet transmission periodically to sense the spectrum for Primary User's (PU's) transmission. The limited and dynamically available spectrum and fixed periodic schedule of transmission interruption makes it harder to model the performance of a CRNs. Again, an open and dynamic spectrum access model brings forth a serious challenge of sustenance among the CRN and makes them more susceptible to jamming-based denial of service (DoS) attacks. Inspired by honeypot in the network security, we propose a honeynet based defense mechanism called CR-honeynet. CR-honeynet aims to avoid attacks on legitimate communications by dedicating a Secondary User (SU) as a honeynode, to deter the attacker from attacking legitimate SUs and attack the honeynode instead. Dedicating an SU as honeynode, on account of its permanent idleness, is wasteful of an entire node as a resource. We seek to resolve the dilemma by dynamically selecting the honeynode for each transmission period. The contribution of the current paper is two-fold. Initially, we develop the first comprehensive queuing model for CRNs, which pose unique modeling challenges, due to their fixed periodic sensing and transmission cycles. In the second step, we introduce a series of strategies for honeynode selection to combat these attacks while keeping the CRN's performance optimal for different traffic scenarios. We build a simulation of a CRN under jamming attack and analyze its performance with different honeynode selection strategies. We find that the predictions, of our mathematical model, track closely with the results of our simulation experiments.

1. Introduction

The conventional static spectrum allocation policy has resulted in suboptimal use of spectrum resource, leading to over-utilization in some bands and under-utilization in others [1]. As a solution, dynamic spectrum access-based Cognitive Radio (CR) has been proposed. CR allows secondary users (SUs) to use an idle licensed spectrum while the proprietary primary user (PU) is not transmitting. The IEEE 802.22 [2] which is an emerging standard for CR-based wireless regional area networks (WRANs), aims at a vacant licensed TV spectrum to be used by SU without causing interference to PU. Infrastructure-based cognitive radio networks (CRNs) consist of two major components: a central controller (such as base station or access point) and mobile SUs. The central controller supervises the communication and makes the spectrum allocation decisions. A sample CRN is presented in Fig. 1.

[☆] This research was supported by National Science Foundation CAREER grant CNS #1346600.

[*] Corresponding author.

E-mail addresses: sumanbhunia@gmail.com (S. Bhunia), felisav@hunter.cuny.edu (F. Vázquez-Abad).
URL: http://www.cse.unr.edu/~shamik (S. Sengupta).

http://dx.doi.org/10.1016/j.pmcj.2015.04.004
1574-1192/© 2015 Elsevier B.V. All rights reserved.

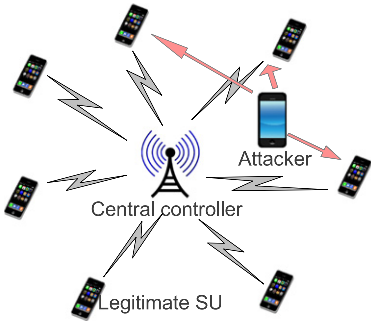

Fig. 1. A sample CRN with an attacker.

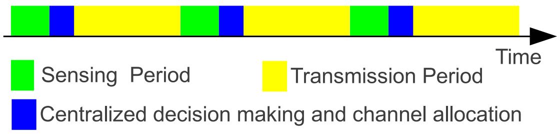

Fig. 2. Time domain representation of cognitive cycle.

The dynamic nature of the available spectrum makes CRNs vulnerable to several spectrum etiquette attacks. The IEEE 802.22 standard does not specifically address the SU–SU interaction or SU protection, although it proactively specifies the PU protection. The "open" philosophy of the CR paradigm makes such networks susceptible to attacks by smart malicious users that could even render the legitimate CR spectrum-less [1,3,4]. Due to software reconfigurability, CRs can even be manipulated to disrupt other CRNs or legacy wireless networks with even greater impact than traditional hardware radios. The jamming-based Denial of Service (DoS) [1] attack is achieved by transmitting energy on the channel where a legitimate SU is communicating. An attacker can scan through channels, identify ongoing legitimate SU communication and then transmit a jamming signal on that particular channel causing heavy interference to the SU, which in effect, can block the legitimate SU's transmission completely.

A number of defense mechanisms against such attacks have been attempted [5–10]. Most of these techniques have considered that the attacker is naive and does not evolve. Inspired by "honeypot" in cybercrime, we propose *CR-honeynet*, which passively learns the attacker's strategy of assault and then dedicates an SU as an active decoy to lure the attacker to hit the decoy node. In this way, the assailant gets false satisfaction of attack, while legitimate SUs bypass attacks. In our earlier paper [11], we introduced the learning mechanism of CR-Honeynet. However the effectiveness of CR-Honeynet in CRN has to be studied before a CRN can deploy CR-Honeynet mechanism. The goal of this paper is to investigate whether allocating resources for CR-honeynet can be beneficial for improving system performance.

To protect PU incumbent services, DSA strictly enforces SUs to periodically pause its transmission and sense for PU activity. SUs scan the wireless environment for free channels in the *sensing period* and transmit packets during *transmission period*. This cognitive cycle is depicted in Fig. 2. The centralized controller allocates different channels to each SU. Several practical challenges need to be co-opted and addressed before allocating resource for honeynet in CRNs. Although dedicating an SU as honeynode potentially makes the CRN robust, it is not a "free ride" as it degrades the effective system throughput. Critical question is how would the honeynode be chosen then? Who will be responsible ("honeynode" selection) for auxiliary communications and monitoring in honeynode? To answer the above questions, we must first understand the complexity of the CRN's traffic behavior under DSA scenario. Consider a scenario wherein a user is conducting a number of simultaneous transmissions — for example, videoconferencing, and many more. All these applications generate packets randomly and independent of other applications. The complex nature of data traffic makes it difficult to analyze the Quality of Service (QoS). CRNs, meanwhile, exhibit a unique behavior pattern that remains yet to be investigated by any mathematical model. For example, the periodic sensing by SUs forces interruption on transmission, affecting end-to-end QoS by imposing delay and jitter on packet transmission. Thus, a major goal of this work is to model a CRN's service using stochastic analysis and use our model to estimate baseline performance indicators. Then we propose state dependent honeynode selection policies for different traffic models to enhance the CRN's performance.

The rest of the paper proceeds as follows: In Section 2, we discuss the motivation for our work, i.e., DoS attacks and honeynet limitations. Section 3 presents a mathematical model to estimate CRN performance using a queue with fixed periodic server vacation. Section 4 presents several honeynode selection policies. In Section 5, we build a comprehensive simulator to study the performance of the proposed model, describe a utility model to determine when a honeynet can be used and when not, measure the fairness of all honeynode selection strategies and finally present the benefits of an optimal honeynode selection strategy that provides the best performance with fairness. Finally, Section 6 concludes the paper.

Please cite this article in press as: S. Bhunia, et al., Performance analysis of CR-honeynet to prevent jamming attack through stochastic modeling, Pervasive and Mobile Computing (2015), http://dx.doi.org/10.1016/j.pmcj.2015.04.004