Ad Hoc Networks 11 (2013) 926–943

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

An optimization framework for monitoring multi-channel multi-radio wireless mesh networks ☆

Dong-Hoon Shin [a,*], Saurabh Bagchi [b]

[a] School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85287, United States
[b] School of Electrical and Computer Engineering, Purdue University, 465 Northwestern Avenue, West Lafayette, IN 47907, United States

ARTICLE INFO

Article history:
Received 4 May 2011
Received in revised form 26 June 2012
Accepted 31 October 2012
Available online 16 November 2012

Keywords:
Wireless mesh networks
Multi-channel multi-radio wireless networks
Security monitoring
Approximation algorithm
LP rounding

ABSTRACT

This paper studies an optimal monitoring problem for behavior-based detection in multi-channel multi-radio wireless mesh networks. In behavior-based detection, nodes overhear communications in their neighborhood to determine if the behaviors of their neighbors are legitimate. The objective of this work is to maximize the number of nodes being monitored by judiciously choosing a set of monitoring nodes and also channels for the chosen monitoring nodes. This problem is NP-hard, growing exponentially with the number of monitoring nodes. We develop three approximation algorithms, each of which achieves at least a constant factor of the optimum. Furthermore, one of our algorithms achieves the *best* possible approximation ratio among all polynomial-time algorithms, unless $P = NP$. We conduct simulations in random networks and scale-free networks to evaluate the coverage and the execution time of the three algorithms.

1. Introduction

Wireless mesh networks (WMNs) are finding increasing usage in municipalities. Many cities (e.g., New Orleans, San Mateo, and Chaska) have already deployed WMNs for public service and safety personnel, and other cities, such as Philadelphia, Houston, and San Francisco, have planned city-wide WMN deployments for providing public broadband Internet access [6]. In WMNs, mobile devices connect to mesh routers, which are typically stationary devices, and mesh routers forward packets en route to the internet-conneted gateways.

WMNs are vulnerable to a wide range of security attacks that are more severe and easier to launch in these networks than in their wireline counterparts. An adversary can physically capture mesh routers and tamper with them. This is because mesh routers are often deployed in insecure locations (e.g., rooftops or streetlights), or even in a hostile environment (e.g., a battlefield). Also, they are typically low-cost devices, which lack strong hardware security protection [18]. Once mesh routers are compromised, the adversary can launch a variety of attacks with them exploiting the cooperative nature of WMNs among mesh routers. For example, the adversary can disrupt the network services by letting compromised mesh routers disobey the network protocols, such as the back-off rule for accessing channel at the MAC layer [15] and the packet-relaying duty at the Network layer.

An approach used to detect such attacks is *behavior-based detection*. In this, nodes overhear communications in their neighborhood via the open nature of wireless medium, and determine if the behaviors of their neighbors are legitimate. For instance, to detect the MAC-layer misbehavior, a node can verify if the back-off times of its

☆ This material is partially based upon work supported by the National Science Foundation under Grant No. CNS-831999 and CNS-0829588. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. The work by Dong-Hoon Shin reflected in this paper was done when he was a Ph.D. student at Purdue University.

* Corresponding author.
E-mail addresses: donghoon.shin.2@asu.edu (D.-H. Shin), sbagchi@purdue.edu (S. Bagchi).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2012.10.004

neighbors follow a legitimate pattern. Upon detection, a remediation action can be taken, such as isolation of the misbehaving node by neighboring nodes. A strategy proposed in the literature [19,23–25] to perform the behavior-based detection is to have *specialized monitoring nodes* deployed throughout the network. This takes the place of the more appealing architecture of every node participating in monitoring, because the latter is susceptible to framing of legitimate nodes due to erroneous reports by malicious nodes. Also, the quorum-based solution [13] only works well under relatively high network densities, which are unlikely in most WMN deployments.

Recently, the issue of use of multiple channels and also multiple radios in WMNs has been studied extensively (e.g., [3,10,14,16,17]). It has been shown that equipping nodes with multiple radios tuned to different non-overlapping channels can significantly increase the capacity of WMNs. An important issue that arises to defend these networks using behavior-based detection is how to strategically place a given number of monitoring nodes in the network and also which channels to tune their radios to, such that as large a fraction of normal nodes (i.e., the nodes that are not participating in monitoring) as possible are covered. One could have considered that, instead of tuning the radios of monitoring nodes to a fixed channel, we allow monitoring nodes to scan multiple channels by sensing multiple frequencies over time. However, the delay of switching the radio channel is non-negligible,[1] and hence with this approach, monitoring nodes would waste their time switching channels.

Alternatively and also equivalently to the first problem formulation, one might be interested in a problem where, given a number of monitoring nodes deployed in the network, which monitoring nodes should be activated on which channels, in order to maximize the number of normal nodes covered. The latter problem is motivated by a desire to keep the resource consumption due to monitoring nodes at a low level. This is because the security analysis for behavior-based detection is computationally expensive and energy-intensive. Note that the former problem can be mapped to the latter. To elaborate on this, assume that the network is arranged as a grid with a given number, say k, of monitoring nodes available for placement on any of m possible grid points. The former problem then becomes the following problem: how to choose k grid points on which to place the monitoring nodes and also the channels to which the radios of the monitoring nodes should be tuned, in order to attain the maximum coverage.

In this paper, we first show that the maximum coverage problem in multi-channel networks, termed MCMC, is NP-hard with the computational cost growing exponentially with the number of monitoring radios in the network. We then present three approximation algorithms to solve MCMC. The first is a greedy algorithm, referred to as *GReedy Algorithm for MCMC* (GR-MCMC), and attains an approximation ratio of $\frac{1}{2}$. Here, the *approximation ratio* is defined as the minimum among all ratios of the number of normal nodes covered by an algorithm to the optimum, where the minimum is taken over all possible network instances. It is known that that the best possible approximation ratio achievable by any polynomial-time algorithm is $1-\frac{1}{e}\approx 0.632$ (unless $P=NP$) [11]. Since the greedy algorithm cannot achieve the best approximation ratio, we explore further. The other two algorithms are based on Linear Program (LP) rounding technique (refer to Section 5). One called *Probabilistic Rounding Algorithm* (PRA) is a randomized algorithm, and achieves an *expected* approximation ratio of $1-\frac{1}{e}$. Here, the expectation is taken over internal random coins of the algorithm. The other called *Deterministic Rounding Algorithm* (DRA) attains the best approximation ratio $1-\frac{1}{e}$ in a *deterministic* manner, i.e., each time it runs, *regardless of the network topology and the channel assignment of normal nodes*. We conduct simulations in two kinds of networks—random networks and scale-free networks—and evaluate how the three algorithms—GR-MCMC, PRA, DRA—fare in these networks, in terms of detection coverage and execution time of the algorithms. A comparison of the three proposed algorithms is shown in Table 1.

The rest of the paper is organized as follows. Section 2 describes the problem formulation. Section 3 discusses applications of the proposed algorithm, and prior works related to this paper. Section 4 shows NP hardness of our problem, and presents GR-MCMC. Section 5 introduces the LP rounding technique, and presents an overview of two LP rounding-based algorithms that we develop. The two LP rounding-based algorithms, PRA and DRA, are presented in Sections 6 and 7, respectively. Section 8 presents complexity analysis of the proposed algorithms. Section 9 presents performance evaluations of the proposed algorithms through simulation. Finally, Section 10 discusses conclusions and future works.

2. Problem formulation

We are given a set of n normal nodes $u_1, \ldots, u_n$. Node u_i has a_i radios called *normal radios*. We define $U=\{u_1^1,\ldots,u_1^{a_1},\ldots,u_n^1,\ldots,u_n^{a_n}\}$, where u_i^j denotes the radio j of normal node u_i. This set U defines the set of normal radios to be verified by monitoring nodes. Each normal radio is tuned to a specific wireless channel. Each normal radio u_i^j has a non-negative weight w_{ij}. These weights of normal radios can be used to capture various application-specific objectives of monitoring. For example, one can use the weights to capture transmission rates of normal radios, which can be estimated from historical data. In this scenario, we would assign higher weights to the nodes that transmit larger volumes of data, thereby biasing our algorithm to monitor such nodes more. Or, one can assign a weight to each normal node instead of each normal radio,

Table 1
Performance comparison of our three proposed algorithms in this paper.

	GR-MCMC	PRA	DRA
Approximation ratio	$\frac{1}{2}$	$1-\frac{1}{e}$ (in expectation)	$1-\frac{1}{e}$
Complexity	GR-MCMC < PRA < DRA		

[1] Current estimate for switching delay between channels in the same frequency band with commodity IEEE 802.11 hardware is in the range of a few hundred microseconds [1] to a few milliseconds [7].