Journal of Computational Science 11 (2015) 196–204

Contents lists available at ScienceDirect

Journal of Computational Science

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

On modeling eavesdropping attacks in wireless networks

Xuran Li [a], Jianlong Xu [b], Hong-Ning Dai [a,*], Qinglin Zhao [a], Chak Fong Cheang [a], Qiu Wang [c]

[a] Faculty of Information Technology, Macau University of Science and Technology, Avenida Wai Long, Taipa, Macau
[b] Shenzhen Research Institute, The Chinese University of Hong Kong, Shenzhen, China
[c] Meizu Telecom Equipment Co. Ltd., Zhuhai, China

ARTICLE INFO

Article history:
Received 30 September 2014
Received in revised form 24 October 2014
Accepted 31 October 2014
Available online 11 November 2014

Keywords:
Modeling
Security
Eavesdropping
Wireless networks

ABSTRACT

This paper concerns the eavesdropping attacks from the eavesdroppers' perspective, which is new since most of current studies consider the problem from the good nodes' perspective. In this paper, we originally propose an analytical framework to quantify the effective area and the probability of the eavesdropping attacks. This framework enables us to theoretically evaluate the impact of node density, antenna model, and wireless channel model on the eavesdropping attacks. We verify via extensive simulations that the proposed analytical framework is very accurate. Our results show that the probability of eavesdropping attacks significantly vary, depending on the wireless environments (such as shadow fading effect, node density, and antenna types). This study lays the foundation toward preventing the eavesdropping attacks in more effective and more economical ways.

1. Introduction

Eavesdropping attacks are one of typical *passive* attacks in wireless ad hoc networks (*AHNets*), which is constitutive of Internet of Vehicles (IOVs) [1]. The eavesdropping security of *AHNets* has received extensive attentions [2–7] since many malicious attacks often follow the eavesdropping activities [8]. However, most of the current studies have only concentrated on either *mitigating* the eavesdropping activities [3–7] or *protecting* the communications between the transmitters and the receivers (also named as *good* nodes) by using *encryption* algorithms [9]. Surprisingly, only few studies investigate the eavesdropping behaviors conducted by the malicious nodes. We call these malicious nodes *eavesdroppers* interchangeably throughout the whole paper. Probing the eavesdropping behaviors is crucial since we can better protect the confidential communications if we have a better knowledge on the eavesdropping activities. For example, we only need to encrypt the communications in the area or the direction that is vulnerable to eavesdropping attacks so that the security cost can be greatly saved. Therefore, the goal of this paper is to investigate the eavesdropping activities from the eavesdroppers' perspective, which is novel so far as we know.

The primary research contributions of this paper can be summarized as follows.

- We establish a novel analytical framework to analyze the eavesdropping attacks in *AHNets* under realistic wireless environments with considerations of various antenna models and channel conditions.
- We propose a novel antenna model to approximate realistic directional antennas (called *Approx-real* model). We also conduct analytical study by comparing *Approx-real* with the conventional directional model (named *keyhole* model).
- We propose an analytical model to investigate the eavesdropping *probability* of eavesdroppers under various channel conditions, such as shadowing effects and path loss effects.
- Our extensive simulation results agree with the analytical results, implying that our proposed framework can accurately model the eavesdropping probabilities in *AHNets*.

The remaining paper is organized as follows. Section 2 summarizes the related studies to this paper. We then give the antenna models as well as the channel models in Section 3. Section 4 then presents the problem formulation. We next show the simulation results in Section 5. Finally, the paper is concluded in Section 6.

2. Related works

Wireless ad hoc networks *AHNets* typically have two essential properties[10]: (1) an *AHNet* is a *self-organizing* network without

* Corresponding author. Tel.: +853 88972154.
E-mail addresses: lxrget@163.com (X. Li), jlxu@cuhkri.org.cn (J. Xu), hndai@ieee.org (H.-N. Dai), qlzhao@must.edu.mo (Q. Zhao), cfcheang@must.edu.mo (C.F. Cheang), qiu_wang@foxmail.com (Q. Wang).

http://dx.doi.org/10.1016/j.jocs.2014.10.006
1877-7503/

any central administration or infrastructure support; (2) in an *AHNet*, if two nodes are not within the transmission range of each other, other nodes are needed to relay the information in a *multi-hop* manner.

Eavesdropping attack is a typical passive attack in *AHNets*. The eavesdropping security [2–7] of *AHNets* has received extensive attentions recently since many malicious attacks often follow the eavesdropping activities [8]. However, most of the current studies have only concentrated on either mitigating the eavesdropping activities [3–7] or protecting the communications between the transmitters and the receivers by using encryption algorithms [9]. Although encryption is shown to be effective in wireless local area networks (WLAN) (e.g., WEP [11], WPA and WPA2 [12]), it may not be proper to be used in AHNets due to the following inherent constraints of AHNets [8]: (a) the inferior computational capability of wireless nodes, (b) the limited battery power of wireless nodes, (c) the difficulty of managing the distributed wireless nodes in a centralized manner.

The current countermeasures to eavesdropping attacks in *AHNets* mainly include: (i) designing light-weight encryption algorithms to encrypt the communications between the transmitter and the receiver [13,14,9] and (ii) mitigating eavesdropping possibility by using power control schemes or using directional antennas [3–6]. Surprisingly, only few studies investigate the eavesdropping behaviors conducted by the malicious nodes. However, it is important to investigate the behaviors of eavesdroppers since we can offer a better protection on the confidential communications if we know which direction is more vulnerable to eavesdropping attacks. However, so far as we know, there are few analytical studies on the eavesdropping attacks from the eavesdroppers' perspective.

3. Models

This section presents the models used in this paper. Below, Section 3.1 gives the network model. Section 3.2 then presents the antenna models. Section 3.3 gives the wireless channel model.

3.1. Node distribution

In this paper, both the transmitters and the receivers are denoted by *good* nodes. The eavesdroppers are also named as *malicious* nodes interchangeably throughout the whole paper. All the good nodes are assumed to be randomly distributed in a 2-D network area A according to a homogeneous Poisson point process with density ρ, which can accurately model a uniform distribution of nodes when the network area approaches infinity [15]. We denote by a random variable X the number of nodes in an area A. We then have the probability mass function on X given as follows:

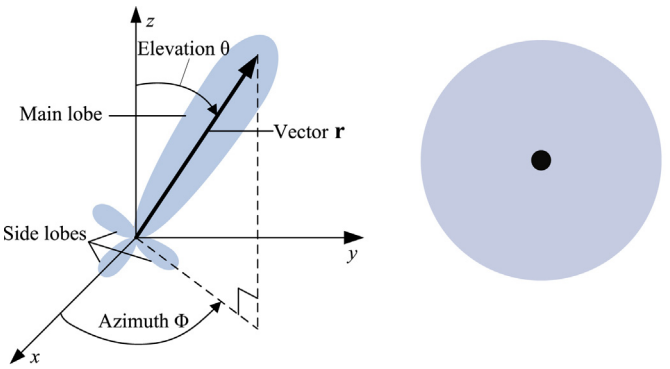
$$P(X = x) = \frac{(\rho A)^x}{x!} e^{-\rho A} \tag{1}$$

where ρA is the expected number of nodes in area A.

3.2. Antenna models

An antenna is a device that is used for radiating/collecting radio signals into/from space. An omni-directional antenna, which can radiate/collect radio signals uniformly to all directions in space, is typically used in conventional wireless ad hoc networks. Different from an omni-directional antenna, a directional antenna can concentrate transmitting or receiving capability to some desired directions so that it has better performance than an omni-directional antenna.

To model the transmitting or receiving capability of an antenna, we often use the *antenna gain*, which is the directivity of an antenna in 3-D space. The antenna gain of an antenna can be expressed in



(a) Directional antenna (b) Isotropic antenna

Fig. 1. Antenna models.

radiation pattern [16] in a spherical coordinate system as shown in Fig. 1(a), which is defined as follows.

$$G(\theta, \phi) = \eta \frac{U(\theta, \phi)}{U_o} \tag{2}$$

where θ is the elevation angle from z-axis ($\theta \in (0, \pi)$), ϕ is the azimuth angle from the x-axis in the xy-plane ($\phi \in (0, 2\pi)$), and η is the efficiency factor, which is set to be 1 since an antenna is often assumed to be lossless. In Eq. (2), $U(\theta, \phi)$ is the *radiation intensity*, which is defined as the power radiated from an antenna per unit solid angle, and U_o denotes the radiation intensity of an omni-directional antenna with the same radiation power P_{rad} as a directional antenna.

We next describe various existing antenna models used in this paper.

3.2.1. Isotropic antenna

We use an *isotropic* antenna to model the antenna gain of an omni-directional antenna. Hence, an omni-directional antenna is denoted by an isotropic antenna interchangeably throughout the paper. Since an isotropic antenna radiates the radio power uniformly in all directions in 3-D space, it is obvious that an isotropic antenna has gain $G_o = 1$ since $U(\theta, \phi) = U_o$. In this paper, since we need to conduct simulation experiments on a 2-D plane, we project the 3-D antenna gain to the xy-plane. Fig. 1(b) shows the radiation pattern of an isotropic antenna on a 2-D plane.

3.2.2. Directional antenna model

Different from an isotropic antenna, a directional antenna can radiate or receive radio signals more effectively in some directions than in others. A directional antenna consists of the *main-beam* with the largest *radiation intensity* and the *side-lobes* and *back-lobes* with the smaller radiation intensity, as shown in Figure 1(a).

In order to compute the antenna gain of a directional antenna, we firstly compute the radiation power P_{rad} of an antenna, which is given by

$$P_{rad} = \oiint_{\Omega} U(\theta, \phi)\, d\Omega = \int_0^{2\pi} \int_0^{\pi} U(\theta, \phi) \sin\theta d\theta d\phi \tag{3}$$

where Ω is the *steradian* used to measure the solid angle subtended by a particular spherical surface S and the element of solid angle $d\Omega$ of a sphere is $d\Omega = \sin\theta d\theta d\phi$.

Since an isotropic antenna radiates power in all directions with a constant radiation intensity U_o, we have $P_{rad} = 4\pi U_o$ after integrating on Eq. (3). In other words, $U_o = (1/4\pi)P_{rad}$. After replacing