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 xxx

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/© 2014 Elsevier B.V. All rights reserved.

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:

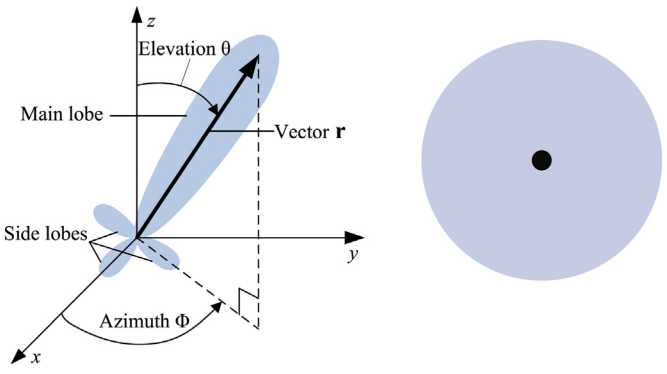
$$P(X=x)=\frac{(\rho A)^x}{x!}e^{-\rho A} \tag{1}$$

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



(a) Directional antenna (b) Isotropic antenna

Fig. 1. Antenna models.

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

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

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

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

Please cite this article in press as: X. Li, et al., On modeling eavesdropping attacks in wireless networks, J. Comput. Sci. (2014), http://dx.doi.org/10.1016/j.jocs.2014.10.006

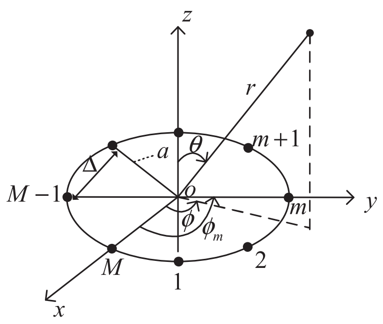


Fig. 2. Structure of UCA antenna.

U_o in Eq. (2) by $(1/4\pi)P_{rad}$ and replacing P_{rad} by the integration of Eq. (3), we have

$$G(\theta,\phi)=\frac{U(\theta,\phi)}{(1/4\pi)\int_0^{2\pi}\int_0^{\pi}U\left(\theta,\phi\right)\sin\theta d\theta d\phi} \tag{4}$$

Note that Eq. (4) is applied for the calculation of the antenna gain of any types of directional antenna models, which are described as follows.

3.2.3. Uniform circular array (UCA) antenna

One of the most commonly used directional antennas is a Uniform Circular Array (UCA) antenna, which consists of M isotropic antenna elements equally spaced on the xy-plane along a circle of radius a, as shown in Fig. 2. In this structure, r is the distance between the antenna and the observation position, Δ is the distance between two neighboring elements, which is usually chosen as $\lambda/2$ and λ is the wavelength of electromagnetic wave radiated from elements. As shown in Ref. [16], the radiation intensity of a UCA antenna fulfills the following formula.

$$U\left(\theta,\phi\right)\propto\left|E\left(\theta,\phi\right)\right|^2 \tag{5}$$

where $E(\theta, \phi)$ denotes the electric field strength at a given direction (θ, ϕ), which can be obtained by

$$E(\theta,\phi)=\sum_{m=1}^{M}I_m e^{jka[\sin\theta\cos(\phi-\phi_m)-\sin\theta_0\cos(\phi_0-\phi_m)]} \tag{6}$$

where j is the imaginary unit for which $j^2=-1$, $k=2\pi/\lambda$, λ is the wavelength of the propagating signal, $\phi_m=2\pi m/M$ is the angular position of mth element on xy-plane, I_m is the amplitude excitation of the mth element, which is set to be 1, similar to Ref. [17]. We let $\theta_0=\pi/2$ (i.e., the xy-plane) and $\phi_0\in[0, 2\pi]$ is the azimuth angle of the desired main beam.

After replacing $U(\theta, \phi)$ in Eq. (4) by combining Eq. (5), we then compute the gain $G(\theta, \phi)$ as follows.

$$G\left(\theta,\phi\right)=\frac{\left|E\left(\theta,\phi\right)\right|^2}{(1/4\pi)\int_0^{2\pi}\int_0^{\pi}\left|E\left(\theta,\phi\right)\right|^2\sin\theta d\theta d\phi} \tag{7}$$

We next obtain the radiation pattern of the UCA antenna on 2-D plane by projecting the UCA gain in 3-D space to a 2-D plane by setting $\theta=\pi/2$ (in xy-plane). Fig. 3 shows the gain patterns of a UCA antenna with $M=8$ elements when $\phi_0=0$ in a 2-D plane.

The realistic directional antenna models (e.g., UCA antennas) are too complicated to be used in simulations. Thus, several simplified directional antenna models are proposed to approximate the realistic directional antennas. In particular, we first give a conventional *Keyhole* antenna model and then present a novel directional antenna model (*Approx-real*), which was first proposed in our previous study [18].

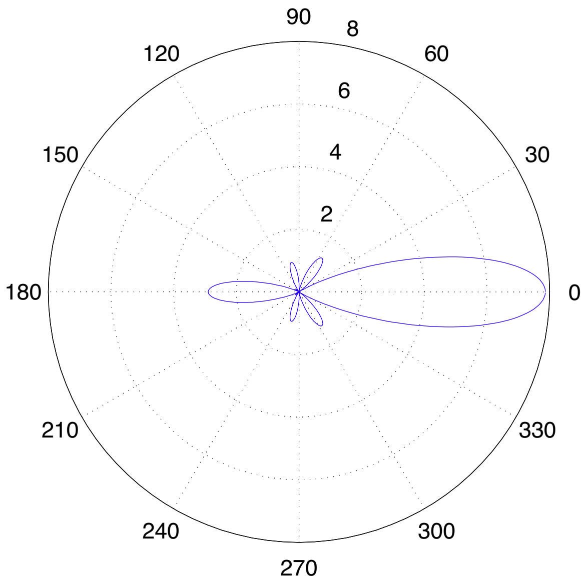


Fig. 3. Radiation pattern of UCA antenna on 2-D plane.

3.2.4. Keyhole antenna model

In keyhole antenna model [19,20], the main-beam of the directional antenna is modeled as a sector with angle θ_d (i.e., the beamwidth) and side/back-lobes are approximated as a circle around an antenna as shown in Fig. 4(a).

We first derive the antenna gain of the Keyhole model in 3-D space, as shown in Fig. 4(a). The radiation power P_{rad} consists of the main-lobe part denoted by P_m and the side/back-lobe part denoted by P_s, fulfilling the following equation.

$$P_{rad}=P_s+P_m \tag{8}$$

where $P_{rad}=4\pi U_0$, P_m and P_s can be calculated by the following integral equations, respectively.

$$P_m=\int_0^{2\pi}\int_0^{(\theta_d/2)}G_m U_0\sin\theta d\theta d\phi \tag{9}$$

$$P_s=\int_0^{2\pi}\int_0^{\pi}G_s U_0\sin\theta d\theta d\phi-\int_0^{2\pi}\int_0^{(\theta_d/2)}G_s U_0\sin\theta d\theta d\phi \tag{10}$$

where G_m and G_s are the gains of main-lobe and side-lobe respectively.

We then have

$$G_s=\frac{2-G_m(1-\cos(\theta_d/2))}{1+\cos(\theta_d/2)} \tag{11}$$

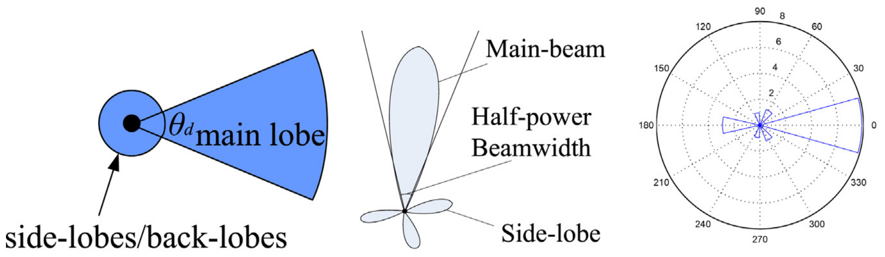
As shown in Eq. (11), G_s is a function of the antenna gain of the main-lobe G_m and the beamwidth θ_d. In practice, we choose the half-power beamwidth of a realistic antenna as θ_d for the Keyhole model, as shown in Fig. 4(a).

3.2.5. Approx-real antenna model

The conventional directional antenna models, such as the keyhole model are too simple to accurately depict an antenna. Therefore, we propose a novel antenna model that can approximates realistic directional antennas without increasing the computational complexity significantly.

Observing that the radiation pattern of a realistic directional antenna consists of multiple lobes (main-lobes and side/backlobes) as shown in Fig. 3, we approximate each lobe as a sector, which leads to our Approx-real antenna model.

Please cite this article in press as: X. Li, et al., On modeling eavesdropping attacks in wireless networks, J. Comput. Sci. (2014), http://dx.doi.org/10.1016/j.jocs.2014.10.006



(a) Keyhole antenna (b) Half-power beamwidth of realistic antenna (c) Approx antenna

Fig. 4. Directional antenna models.

Approx-real model. The antenna gain $G(\theta)$ at a certain direction can be calculated by

$$G(\theta)=\begin{cases} G_{\max}(i) & \text{within the half-power beamwidth of lobe } i \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

where $G_{\max}(i)$ denotes the maximal antenna gain of lobe i and the half-power beamwidth is the subtend angle of the directions when the radiation power falls the half of the maximal radiation power of lobe i. Notice the lobe i can be either the main-lobe or the side/back-lobes. Fig. 4(c) shows the corresponding Approx-Real model to an UCA antenna with $M = 8$ (the radiation pattern in shown in Fig. 3).

3.3. Wireless channel models

We consider an *AHNet*, in which all the good nodes are equipped with isotropic antennas and malicious nodes are equipped with either directional antennas and isotropic antennas for comparison purpose.

We assume that a good node u transmits with power $P_g(u)$. The received power at an eavesdropper v with a distance $d(u, v)$ from the good node u is denoted by $P_e(v)$, which can be calculated by

$$P_e(v) = \frac{k_1 G_g(u) G_e(v) P_g(u)}{S_h (d(u, v))^{\alpha}} \tag{13}$$

where k_1 is a constant, $G_g(u)$ and $G_e(v)$ denote the antenna gain of the good node u and the antenna gain of the malicious node v, respectively, α is the path loss factor usually ranging from 3 to 4 [21] and S_h is a random variable, which is used to model the shadowing effect.

Specifically, S_h follows a lognormal distribution, which is given by

$$S_h = 10^{\omega/10} \tag{14}$$

where ω is a Gaussian random variable with zero mean and standard deviation usually ranging from 4 to 12 [17]. There is no shadowing effect when $\sigma = 0$.

In practice, we usually compute the *power attenuation* between two nodes u and v instead of computing the received power $P_e(v)$ [15,17]. We then define the power attenuation $\delta(u, v)$ between u and v as follows by normalizing Eq. (13) (i.e., $k_1 = 1$)

$$\delta(u, v) = \frac{P_g(u)}{P_e(v)} = \frac{S_h (d(u, v))^{\alpha}}{G_g(u) G_e(v)} \tag{15}$$

This can be expressed in terms of dB as

$$\delta(u, v) = \alpha 10 \log(\frac{d(u, v)}{1\text{m}}) + 10 \log(G_g(u) \cdot G_e(v)) + 10 \log(S_h) \tag{16}$$

We define $\delta_1(u, v) = \alpha 10 \log(d(u, v)/1\text{m})\text{dB}$ as the *geometric component*, $\delta_2(u, v) = 10 \log(G_g(u) \cdot G_e(v))$ as the *antenna gain component* and $\delta_3(u, v) = 10 \log(S_h)$ as the *shadow fading component*. In particular, the geometric component $\delta_1(u, v)$ only depends on the path loss exponent α and the distance d(u,v) between u and v, which is deterministic. The antenna gain component $\delta_2(u, v)$ depends on the antenna gains of the good node and the eavesdropper, which is also deterministic when the direction of the directional antenna is fixed. The shadow fading component $\delta_3(u, v)$ is yet stochastic.

An eavesdropper can successfully eavesdrop a transmission if and only if the power attenuation δ is no greater than the given threshold δ_0. In the next section, we will formulate the eavesdropping attacks and analyze the impacts of the above components on the eavesdropping successful chance of eavesdroppers.

4. Analysis on eavesdropping attacks

This section presents our analytical framework to model the eavesdropping activities in *AHNets*. In particular, we first analyze *effective eavesdropping area* in Section 4.1, which is then used to derive the *probability of eavesdropping attacks* in Section 4.2.

4.1. Effective eavesdropping area

As shown in Section 3.3, an eavesdropper can successfully listen in a communication if and only if the signal attenuation δ is no greater than the given threshold δ_0, i.e., $\delta \le \delta_0$. In other words, the probability of having no eavesdropper listening in a communication is given by

$$P(\delta > \delta_0) = P\left(\frac{S_h d(u, v)^{\alpha}}{G_g(u) G_e(v)} > \delta_0\right) = P\left(\left(\frac{\delta_0 G_g(u) G_e(v)}{S_h}\right)^{1/\alpha} < d\right) \tag{17}$$

We define a random variable D as

$$D = \left(\frac{\delta_0 G_g(u) G_e(v)}{S_h}\right)^{1/\alpha} \tag{18}$$

which is referred to the *eavesdropping range* of an eavesdropper. After substituting Eq. (18) into Eq. (17), we have $P(\delta > \delta_0) = P(D < d)$, which implies that a transmission can be eavesdropped by a malicious node if and only if the transmitter falls in the eavesdropping range D of the malicious node.

We then consider the *effective eavesdropping area* of the malicious node, which is defined as $E[\pi D^2] = \pi E[D^2]$, where $E[D^2]$ is the second moment of the eavesdropping range D. The effective eavesdropping area is a *critical* region that only when the good node falls in this region, its transmission can be eavesdropped by eavesdroppers. We then have

Please cite this article in press as: X. Li, et al., On modeling eavesdropping attacks in wireless networks, J. Comput. Sci. (2014), http://dx.doi.org/10.1016/j.jocs.2014.10.006

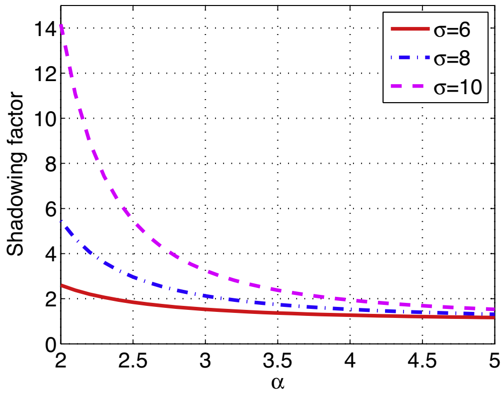


Fig. 5. Shadow fading component VS. the path loss exponent α with different values of σ.

$$E[\pi D^2] = \pi E\left[\left(\frac{\delta_0 G_g(u) G_e(v)}{S_h}\right)^{2/\alpha}\right]$$
$$= \pi(\delta_0)^{2/\alpha}\cdot E[S_h^{-2/\alpha}]\cdot E[(G_g(u)G_e(v))^{2/\alpha}] \qquad (19)$$

As shown in Eq. (19), $\pi(\delta_0)^{2/\alpha}$ is deterministic and it only depends on the path loss exponent α. Thus, the effective eavesdropping area mainly depends on two components: the *shadow fading component* $E[S_h^{-2/\alpha}]$ and the *antenna gain component* $E[(G_g(u)G_e(v))^{2/\alpha}]$. In particular, the shadow fading component depends on both the shadowing effect and the path loss effect. On the other hand, the antenna gain component depends on the antenna gains of the eavesdropper and the good node as well as the path loss effect.

Next, we analyze the impacts of thee above two components.

4.1.1. Shadow fading component

In the following, we present the results on the shadow fading component. In particular, we have the following theory.

Theorem 1. *The impact of shadow fading component on the effective eavesdropping area is given by*

$$E[S_h^{-2/\alpha}] = \exp\left\{\frac{((\ln 10/5\alpha)\sigma)^2}{2}\right\} \qquad (20)$$

Proof. We present the detailed proof in Appendix A. □

Theorem 1 shows that the impact of shadow fading component depends on both the path loss factor α and the lognormal standard deviation σ. Besides, it is also shown in Theorem 1 that the shadow fading component is always non-negative, implying that the shadow fading effect always leads to the non-decrement of the effective eavesdropping area. Fig. 5 shows that the shadow fading component versus the path loss factor α under different values of the shadowing lognormal standard deviation σ. More specifically, as shown in Fig. 5, the shadow fading component is always greater than 1 (when $\sigma \neq 0$), which confirms our observation that the shadowing effect results in the increment of the effective eavesdropping area. Furthermore, Fig. 5 also shows that the shadow fading component is increased with the increment of the variance σ. The increment of shadow fading component mainly owes to the randomness of the shadow fading effect. When the randomness of the shadow fading effect is increased (i.e., the higher fading variance σ), the shadow fading component $E[S_h{}^{1/\alpha}]$ is also increased, implying that a malicious node located further away can eavesdrop the transmission. However, it must be noticed that this phenomenon only holds when the path loss factor α is fixed. When the path loss factor α is increased, the shadow fading component $E[S_h{}^{1/\alpha}]$ significantly decreases as shown in Fig. 5 implying that the path loss factor has the negative effect on the eavesdropping successful chance.

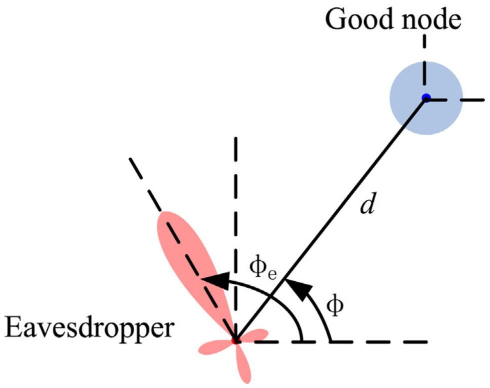


Fig. 6. Relative positions of a good node and an eavesdropper.

4.1.2. Antenna gain component

We next analyze the antenna gain component.

Since eavesdroppers have no prior-knowledge of the location information of good nodes, we assume that each eavesdropper randomly chooses a main beam direction to *listen*. More specifically, Fig. 6 shows a scenario on the calculation of the antenna gain component, where we denote by ϕ_e the main beam direction of an eavesdropper. We then denote by ϕ the direction of the eavesdropper from the good node (as shown in Fig. 6). It is obvious that ϕ_e and ϕ are uniformly distributed within $[0, 2\pi)$. The calculation of the antenna gain component is then given as follows

$$E[(G_gG_e)^{2/\alpha}] = \frac{1}{(2\pi)^2}\cdot\int_0^{2\pi}\int_0^{2\pi}(G_e(\phi,\phi_e)G_g(\pi+\phi))^{2/\alpha}d\phi_e d\phi \qquad (21)$$

Note that we always have $G_g(\pi+\phi)=1$ since each good node is equipped with an isotropic antenna with gain $G_o=1$. However, we cannot obtain a closed-form expression for Eq. (21) with realistic antennas (e.g. UCA antennas). Nevertheless, we can still obtain the numerical results of Eq. (21) since the path loss exponent α is ranged from 2 to 4 and the number of antenna elements M is usually less than 10.

We then give the discrete values of antenna gain component as shown in Table 1, where the percentage denotes the increment or the decrement compared with that of isotropic antenna. It is shown in Table 1 that when the path loss exponent α is small (e.g., $\alpha=2$), the antenna gain component of all the directional antenna models is always positive, implying that using directional antennas at malicious nodes can potentially increase the eavesdropping chance. However, with the increment of α, the benefits become less notable. More specifically, the antenna gain component decreases with the increment of α. For example, when $\alpha \geq 3$, the antenna gain component becomes even negative for realistic antenna model, implying

Table 1
Antenna gain component (compared with isotropic antenna).

α	Keyhole	Real (UCA)	Approx-real
2	1.4791 (+47.42%)	1.2674 (+26.32%)	1.2481 (+24.40%)
2.5	1.2714 (+26.72%)	1.0695 (+6.60%)	0.9631 (−4.01%)
3	1.1784 (+17.45%)	0.9789 (−2.43%)	0.8226 (−18.01%)
3.5	1.1284 (+12.47%)	0.9320 (−7.11%)	0.7408 (−26.16%)
4	1.0983 (+9.47%)	0.9061 (−9.69%)	0.6881 (−31.42%)

that using directional antennas at eavesdroppers can potentially reduce the eavesdropping chance. Furthermore, Table 1 also shows that Keyhole model may overestimate the impacts of the antenna gain component since the antenna gain component of Keyhole model always has the positive percentage of increment compared with isotropic antenna. However, Approx-real model may underestimate the impacts of the antenna gain component since it has the negative percentage of increment. The simulation results in Section 5 will further confirm these observations.

4.2. *Probability of eavesdropping attacks*

We model the successful chance of eavesdropping attacks by the *probability of eavesdropping attacks*, denoted by $P(E)$. To derive $P(E)$, we need to analyze the probability of no good node being eavesdropped first. We denote the number of good nodes in the eavesdropping area by a random variable Y. Since good nodes are randomly distributed according to a homogeneous Poisson point process (as shown in Section 3.1), we then have the probability of no good node falling in the eavesdropping area, which is given by the following equation,

$$P(Y=0)=e^{-\rho\cdot E[\pi D^2]} \tag{22}$$

where $E[\pi D^2]$ is given by Eq. (19).

We then can calculate $P(E)$ as follows

$$P(E)=1-P(Y=0)=1-e^{-\rho\cdot E[\pi D^2]} \tag{23}$$

The physical meaning of $P(E)$ is the probability that an eavesdropper can successfully eavesdrop at least one transmission in a network. Besides, as shown in Eqs. (23) and (19), the probability of eavesdropping attacks heavily depends on the shadow fading component and the antenna gain component.

5. Simulation results

In this section, we evaluate the analytical framework proposed in Section 4 by conducting extensive simulations. In particular, we consider the eavesdropper equipped with various antenna models, such as the omni-directional model (Omni), the Keyhole model (Keyhole), the Approx-real model(Approx) and the realistic model (UCA). To simplify our analysis, we call the eavesdroppers with omni-directional antennas as Omni-eavesdroppers, the eavesdroppers with Keyhole model as Keyhole-eavesdroppers, the eavesdroppers with Approx-real model as Approx-eavesdroppers and the eavesdroppers with UCA model as UCA-eavesdroppers. Note that each good node is equipped with an omni-directional antenna (Omni).

In our simulations, the probability of eavesdropping attacks is calculated as follows:

$$P_s(E)=\frac{\#\text{ topologies eavesdropped}}{\#\text{ topologies}} \tag{24}$$

where # represents "number of" and we denote the simulation results by $P_s(E)$ in order to differentiate it from the analytical value $P(E)$. Note that the simulation expression $P_s(E)$ is in accord with $P(E)$. This is because when any good nodes in a network topology are eavesdropped, the whole network is regarded as being eavesdropped, which is consistent with the definition of the eavesdropping probability.

Our simulations were conducted in an area of $l\times l$ with minimizing the impacts of the border effects by properly setting a larger outbox [15]. Note that l is chosen as 3000 m. We fix the number of malicious nodes and we choose the node density ρ for the good nodes ranging from 10^{-7} to 10^{-2}. Note that we consider the pathloss exponent α ranging from $\alpha=2.5$ to $\alpha=3.5$, the shadow fading factor (the stand deviation) σ ranging from 6 to 10 and the fixed threshold attenuation $\delta_0=50$ dB. Note that each point in the curves is the averaged value over 10,000 random topologies.

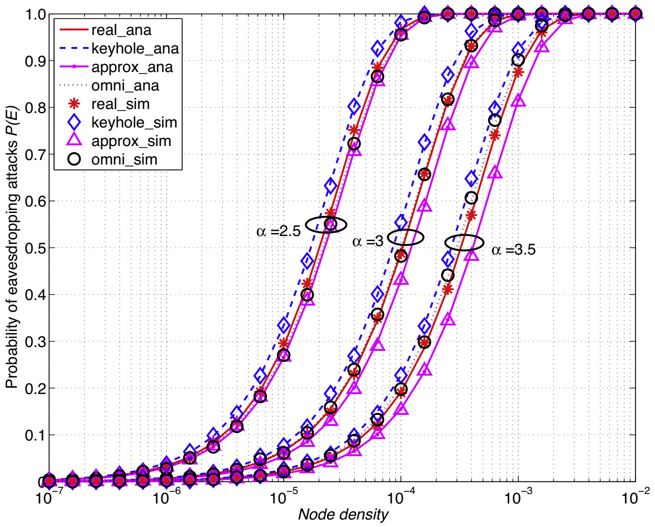


Fig. 7. Probability of eavesdropping attacks $P(E)$ without shadowing effect ($\sigma=0$) when and $\alpha=2.5, 3, 3.5$ (node density ρ ranging from 10^{-7} to 10^{-2}) with attenuation threshold $\delta_0=50$ dB.

We first give the results without the shadowing effect in Section 5.1. Then, we present the results with the shadow fading effect in Section 5.2.

5.1. *Results without shadowing effects*

Fig. 7 presents the results without shadowing effect (when $\sigma=0$), where the analytical results shown in curves are calculated in Eq. (23) and the simulation results are shown by markers. We can see that the simulation results agree with the analytical results in Section 4, implying that our analytical model can accurately model the successful rate of eavesdropping attacks.

It is also shown in Fig. 7 that the probability of eavesdropping attacks is increased when the path loss factor decreases. For example, all the eavesdroppers have higher values of $P(E)$ when $\alpha=2.5$ than those when $\alpha=3.5$. These results have further confirmed with our previous observations in Section 4. More specifically, Fig. 7 also shows that UCA-eavesdroppers have the higher values of $P(E)$ than Omni-eavesdroppers when $\alpha=2.5$. This may owes to the effect that a directional antenna can concentrate its receiving capability on a certain direction. As a result, an eavesdropper equipped with directional antennas can listen in some directions better than an Omni-eavesdropper. However, it is not true that using directional antennas at eavesdroppers can always increase the successful chance of eavesdropping attacks. In fact, when the path loss effect is increased (e.g., $\alpha=3.5$), the $P(E)$ of UCA-eavesdroppers is even slightly lower than that of Omni-eavesdroppers.

Fig. 7 also compares the results with two simplistic antenna models, i.e., Keyhole model and Approx-real model. In particular, Keyhole-eavesdroppers always have the higher values of $P(E)$ than other eavesdroppers and Approx-eavesdroppers always have the lower values of $P(E)$ than other eavesdroppers. This can be explained by the analysis in Section 4.1 that the Keyhole model overestimates the antenna gain effect and the Approx-real model underestimates the antenna gain effect.

5.2. *Results with shadowing effects*

We then take the shadow fading effect into account. Figs. 8–10 show the results with $\sigma=6$, the results with $\sigma=8$ and the results

Please cite this article in press as: X. Li, et al., On modeling eavesdropping attacks in wireless networks, J. Comput. Sci. (2014), http://dx.doi.org/10.1016/j.jocs.2014.10.006

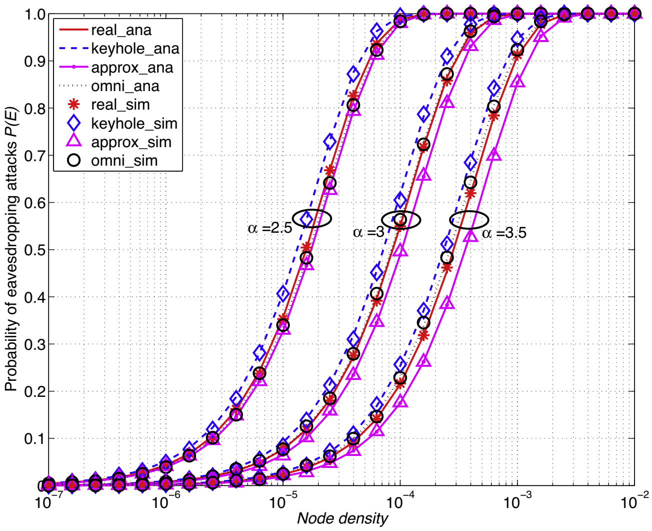


Fig. 8. Probability of eavesdropping attacks $P(E)$ with shadowing effect ($\sigma = 6$) when and $\alpha = 2.5$, 3, 3.5 (node density ρ ranging from 10^{-7} to 10^{-2}) with attenuation threshold δ_0 = 50 dB.

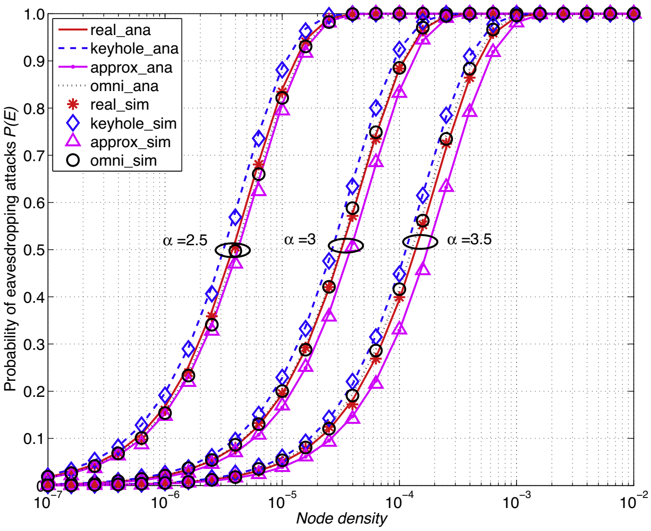


Fig. 10. Probability of eavesdropping attacks $P(E)$ with shadowing effect ($\sigma = 10$) when and $\alpha = 2.5, 3, 3.5$ (node density ρ ranging from 10^{-7} to 10^{-2}) with attenuation threshold δ_0 = 50 dB.

with $\sigma = 10$, respectively. We can see that the simulation results agree with the analytical results, implying that our analytical model can accurately model the successful rate of eavesdropping attacks even under the shadow fading environment.

We also found that the shadow fading effect has no significant impact on $P(E)$ when the shadow fading effect is relatively small. For example, there is no significant difference between the values of $P(E)$ with $\sigma = 0$ and the values of $P(E)$ with $\sigma = 6$ (as shown in Figs. 7 and 8). However, when the shadow fading effect becomes more notable ($\sigma > 6$), all the eavesdroppers have steeper curves than those with $\sigma = 6$ (as shown in Figs. 9 and 10). In particular, we take UCA-eavesdroppers when $\alpha = 3$ as an example. If we draw horizontal lines at the point with $P(E) = 1$ in Figs. 8–10, respectively, we can find that the node density $\rho = 0.001$ in Fig. 8 and $\rho = 0.0006$ in Fig. 9 and $\rho = 0.0004$ in Fig. 10. In other words, it requires lower node density to reach the *full eavesdropping probability* (i.e., $P(E) = 1$) when the shadow fading effect increases. This effect may owe to the increased effective eavesdropping area $E[\pi D^2]$ due to the randomness of the shadow fading effect (when σ is higher). This agrees with our observations in Section 4.1.

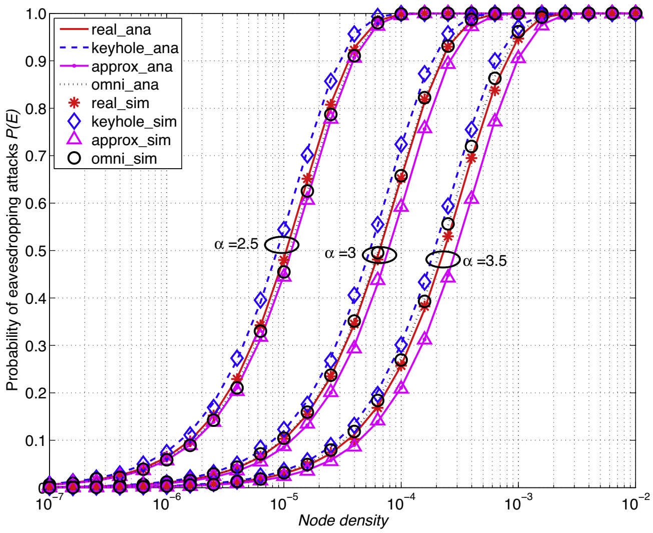


Fig. 9. Probability of eavesdropping attacks $P(E)$ with shadowing effect ($\sigma = 8$) when and $\alpha = 2.5$, 3, 3.5 (node density ρ ranging from 10^{-7} to 10^{-2}) with attenuation threshold δ_0 = 50 dB.

As shown in Figs. 8–10, the probability of eavesdropping attacks always decreases with the increased path loss exponent α. This coheres with the results without the shadowing effect (as shown in Fig. 7). It implies that the path loss effect always brings the adverse effect on the eavesdropping attacks.

Similar to the results without shadow fading effects, Keyhole-eavesdroppers always have the higher values of $P(E)$ than Omni-eavesdroppers and UCA-eavesdroppers. This can be explained as follows. Using directional antennas at eavesdroppers can lead to the effect that eavesdroppers can "*listen further*" and the effect that they may "*listen narrower*" since a directional antenna can concentrate its receiving capability on a certain direction. The "*listening narrower*" effect sometimes cancels out the benefit of the "*listening further*" effect. For example, UCA-eavesdroppers even have the lower values of $P(E)$ than Omni-eavesdroppers when $\alpha = 3.5$. Compared with UCA-eavesdroppers and Approx-eavesdroppers, Keyhole-eavesdroppers are less sensitive to the "*listening narrower*" effect since the Keyhole antenna model has *broader* side/back lobes than the UCA model and the Approx-real model. Furthermore, Omni-eavesdroppers in all the above scenarios seem less sensitive to the varying environments (both the shadow fading effect and the path loss effect).

5.3. Discussions

As shown in the above results, we found that eavesdroppers with realistic directional antennas sometimes perform even worse than Omni-eavesdroppers when the path loss effect is increased (i.e., $\alpha \geq 3$). This is counter-intuitive since many previous studies [2–7] show that using directional antennas at either transmitters or receivers can usually improve Signal-to-Interference-Noise-Ratio (SINR), implying that using directional antennas at eavesdroppers can potentially increase the successful chance of eavesdropping attacks. The reasons behind these results can be explained as follows:

1. Realistic directional antennas have the side-lobes and back-lobes (as shown in Fig. 1(a)), which have weaken the antenna gain of the main beam. As a result, eavesdroppers with realistic antennas have less chance to tap in the communications of good nodes.
2. The Keyhole model *overestimates* the probability of eavesdropping attacks since it somehow *exaggerates* the listening capability of directional antennas with relatively higher antenna gain of the main beam and the broader side-lobes and back-lobes. However, Approx-real model *underestimates* the probability of eavesdropping attacks due to the narrower side-lobes and back-lobes.

According to the above point 2, we argue that the simplistic antenna models (the Keyhole model and Approx-real model) are still quite useful since realistic antennas are too complicated to be used in analyzing the performance of wireless networks with directional antennas.

6. Conclusion

In this paper, we propose an analytical framework to model the eavesdropping attacks in wireless networks with consideration of both channel conditions and antenna models. Both the analytical results and simulation results agree with each other, which implies that our proposed analytical models can accurately approximate the eavesdropping activities of eavesdroppers. Besides, our results also show that when the path loss effect is less significant, using directional antennas at eavesdroppers can somehow increase the probability of eavesdropping attacks. However, our results also imply that using directional antennas at eavesdroppers can sometimes reduce the probability of eavesdropping attacks when the path loss effect becomes more notable. Furthermore, we also found that the randomness brought by the shadow fading effect can lead to the increased probability of eavesdropping attacks. The study in this paper has laid the foundation stone toward preventing the eavesdropping attacks in the future.

Acknowledgements

The work described in this paper was supported by Macao Science and Technology Development Fund under Grant No. 036/2011/A, Grant No. 081/2012/A3 and Grant No. 096/2013/A3 and supported by the National Natural Science Foundation of China with Grant No. 61472338. The authors would like to thank Gordon G.-D. Han for his excellent comments.

Appendix A.

Proof of Theorem 1. To prove the above theorem, we borrow the following result proved in Ref. [22]:

If a random variable $Z = \ln Y$ *has a normal distribution with mean* μ_Z *and standard deviation* σ_Z*, then the mean of the random variable* Y *is given by* $E[Y] = \exp\left\{\mu_Z + \frac{\sigma_Z{}^2}{2}\right\}$.

After taking the natural logarithm of S_h in Eq. (14), we have

$$\ln S_h{}^{1/\alpha} = \ln(10^{\omega/10\alpha}) = \frac{\omega}{10\alpha}\ln 10 \quad (25)$$

where ω is a Gaussian random variable with zero mean and standard deviation σ. From the above given result, the expected value of S_h is given by the following equation

$$E[S_h{}^{1/\alpha}] = \exp\left\{\frac{((\ln 10/10\alpha)\sigma)^2}{2}\right\} \quad (26)$$

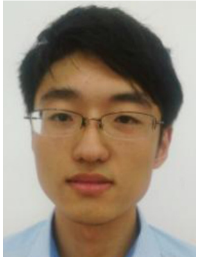
Similarly, the expected value of $S_h^{-\frac{2}{\alpha}}$ is given by

$$E\left[S_h^{-\frac{2}{\alpha}}\right] = \exp\left\{\frac{((\ln 10/5\alpha)\sigma)^2}{2}\right\} \quad (27)$$

□

References

[1] S. Wang, C. Fan, C.-H. Hsu, Q. Sun, F. Yang, A vertical handoff method via self-selection decision tree for internet of vehicles, IEEE Syst. J. (99) (2014) 1–10.
[2] M. Anand, Z.G. Ivesy, I. Leez, Quantifying eavesdropping vulnerability in sensor networks, in: Proceedings of the 2nd International VLDB Workshop on Data Management for Sensor Networks, 2005.
[3] J.-C. Kao, R. Marculescu, Eavesdropping minimization via transmission power control in ad-hoc wireless networks, in: Proceedings of IEEE SECON, 2006.
[4] X. Lu, F. Wicker, P. Lio, D. Towsley, Security estimation model with directional antennas, in: Proceedings of MILCOM, 2008.
[5] H.-N. Dai, D. Li, R.C.-W. Wong, Exploring security improvement of wireless networks with directional antennas, in: Proceedings of IEEE LCN, 2011.
[6] Q. Wang, H.-N. Dai, Q. Zhao, Eavesdropping security in wireless ad hoc networks with directional antennas, in: Proceedings of IEEE WOCC, 2013.
[7] H.-N. Dai, Q. Wang, D. Li, R.C.-W. Wong, On eavesdropping attacks in wireless sensor networks with directional antennas, Int. J. Distrib. Sensor Netw. (2013).
[8] F. Anjum, P. Mouchtaris, Security for Wireless Ad Hoc Networks, 1st ed., Wiley-Interscience, 2007.
[9] M. Zafer, D. Agrawal, M. Srivatsa, Limitations of generating a secret key using wireless fading under active adversary, IEEE/ACM Trans. Netw. 20 (5) (2012) 1440–1451.
[10] C.S.R. Murthy, B.S. Manoj, Ad hoc Wireless Networks: Architectures and Protocols, Prentice Hall, PTR, 2004.
[11] IEEE 802.11a-1999. http://standards.ieee.org/getieee802/download/802.11a-1999.pdf
[12] IEEE 802.11i-2004. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf
[13] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, Radio-telepathy: extracting a secret key from an unauthenticated wireless channel, in: Proceedings of ACM MobiCom, 2008.
[14] K. Zeng, D. Wu, A. Chan, P. Mohapatra, Exploiting multiple-antenna diversity for shared secret key generation in wireless networks, in: Proceedings of IEEE INFOCOM, 2010.
[15] C. Bettstetter, On the connectivity of ad hoc networks, Comput. J. 47 (4) (2004) 432–447.
[16] C.A. Balanis, Antenna Theory: Analysis and Design, 2nd ed., John Wiley & Sons, New York, 1997.
[17] X. Zhou, S. Durrani, H. Jones, Connectivity analysis of wirelss ad hoc networks with beamforming, IEEE Trans. Vehic. Technol. 58 (9) (2009) 5247–5257.
[18] Q. Wang, H.-N. Dai, Q. Zhao, Connectivity of wireless ad hoc networks: impacts of antenna models, in: Proceedings of the 14th International Conference on Parallel and Distributed Computing, Applications and Technologies, Taipei, Taiwan, 2013.
[19] M. Kiese, C. Hartmann, R. Vilzmann, Optimality bounds of the connectivity of adhoc networks with beamforming antennas, in: IEEE GLOBECOM 2009, 2009.
[20] P. Li, C. Zhang, Y. Fang, The capacity of wireless ad hoc networks using directional antennas, IEEE Trans. Mob. Comput. 10 (10) (2011) 1374–1387.
[21] T.S. Rappaport, Wireless Communications: Principles and Practice, 2nd ed., Prentice Hall, PTR, Upper Saddle River, NJ, 2002.
[22] D.D. Wackerly, W. Mendenhall, R.L. Scheaffer, Mathematical Statistics With Applications, Cengage Learning, 2007.

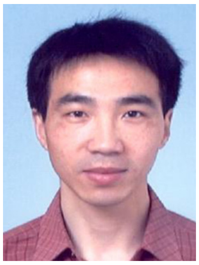


Xuran Li is an M.Sc. student in Faculty of Information and Technology of Macau University of Science and Technology, where he is now pursuing her M.Sc. in Communications Engineering. He received his B.Sc. in Communications Engineering from Century College of Beijing University of Posts and Telecommunications in 2013.

Please cite this article in press as: X. Li, et al., On modeling eavesdropping attacks in wireless networks, J. Comput. Sci. (2014), http://dx.doi.org/10.1016/j.jocs.2014.10.006

Jianlong Xu received the Ph.D. degree from South China University of Technology in 2013. He is a postdoctoral fellow at Shenzhen Research Institute, the Chinese University of Hong Kong. He is also a member of ACM. His research interests include service computing, Internet of things, and distributed computing.

Hong-Ning Dai now is with Faculty of Information Technology at Macau University of Science and Technology as an assistant professor. He obtained the Ph.D. degree in Computer Science and Engineering from the Chinese University of Hong Kong in 2008. He also received the B.E. and M.E. degrees in Computer Science and Engineering from South China University of Technology. His current research interests include wireless networks, wireless sensor networks, mobile computing and distributed systems.



Qinglin Zhao received the Ph.D. degree from the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China, in 2005. From October 2006 to August 2009, he worked as a postdoctoral researcher in the Department of Electronic and Computer Engineering, the Hong Kong University of Science and Technology (HKUST), HKSAR. Since September 2009, he has been with the Faculty of Information Technology, Macau University of Science and Technology, Avenida Wei Long, Taipa, Macau, China. His research interests include wireless and mobile networks, mobility management, and performance analysis.

Chak Fong Cheang received the B.S. degree in Automation from Tsinghua University (China), the M.S. degree in Control Science and Engineering and the Ph.D. degree in Computer Science and Technology all from Tsinghua University (China) in 1999, 2002, 2013, respectively. His research interests include computer networks.

Qiu Wang now is a software engineer in Meizu Telecom Equipment Co. Ltd., Zhuhai, China. She received her M.Sc. in Communications Engineering from Faculty of Information Technology, Macau University of Science and Technology, in 2014. Her current research interests include wireless communications and wireless networks.