2014

An Analytical Model on Eavesdropping Attacks in Wireless Networks

Xuran Li, *Macau University of Science and Technology*
Hong-Ning Dai, *Macau University of Science and Technology*
Qinglin Zhao, *Macau University of Science and Technology*

An Analytical Model on Eavesdropping Attacks in Wireless Networks

Xuran Li and Hong-Ning Dai and Qinglin Zhao
Faculty of Information Technology
Macau University of Science and Technology, Macau
Email: lxrget@163.com and hndai@ieee.org and qlzhao@must.edu.mo

***Abstract*—This paper concerns the eavesdropping problem from the eavesdroppers' perspective, which is new since most of previous studies only concentrate on the good nodes. We propose an analytical framework to investigate the eavesdropping attacks, taking account into various channel conditions and antenna models. Our extensive numerical results show that the probability of eavesdropping attacks heavily depends on the shadow fading effect, the path loss effect and the antenna models; particularly, they imply that using directional antennas at eavesdroppers can increase the probability of eavesdropping attacks when the path loss effect is less notable. This study is helpful for us to prevent the eavesdropping attacks effectively and economically.**

I. Introduction

The eavesdropping security [1]–[6] of wireless ad hoc networks has received extensive attentions recently since many malicious attacks often follow the eavesdropping activities [7]. However, most of the current studies have only concentrated on either mitigating the eavesdropping activities [2]–[6] or protecting the communications between the transmitters and the receivers (also named as *good* nodes) by using encryption algorithms [8]. Surprisingly, only few studies investigate the eavesdropping behaviors conducted by the malicious nodes, which are denoted by *eavesdroppers* 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, we will investigate the eavesdropping activities from the eavesdroppers' perspective in this paper. To the best of our knowledge, *there is no analytical study on the eavesdropping attacks from the eavesdroppers' perspective*.

In this paper, we investigate the eavesdropping activities of malicious nodes under realistic wireless channel environments with consideration of the shadow-fading and the path loss effects. In addition, we also consider the different antenna models mounted at eavesdroppers. The contributions of this paper are two-fold.

- First, we propose an analytical model to investigate the probability of eavesdropping attacks quantitatively with consideration of various channel conditions and different antenna models.
- Second, we have conducted extensive numerical studies on the probability of eavesdropping attacks. Specifically, we have found that the eavesdropping successful rate heavily depends on the antenna models of eavesdroppers as well as the channel conditions.

The remaining paper is organized as follows. We first present the antenna models as well as the channel models in Section II, then formulate the problem in Section III. We next show the numerical results in Section IV. Finally, the paper is concluded in Section V.

II. Models

A. Channel Models

To describe the channel model, we consider 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

$$P_e(v) = \frac{k_1 G_g(u) G_e(v) P_g(u)}{S_h (d(u,v))^{\alpha}} \tag{1}$$

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 2 to 4 [9] and S_h is a random variable, which is used to model the shadowing effect [10].

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

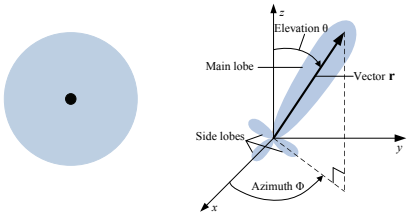
$$S_h = 10^{\omega/10} \tag{2}$$

where ω is a Gaussian random variable with zero mean and standard deviation σ usually ranging from 4 to 10 [10], [11]. There is no shadowing effect when σ = 0.

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

$$\delta(u,v) = \frac{P_g(u)}{P_e(v)} = \frac{S_h (d(u,v))^{\alpha}}{G_g(u) G_e(v)} \tag{3}$$

An eavesdropper can successfully eavesdrop a transmission if and only if the signal attenuation δ is no greater than the given threshold δ_0.



(a) Omni-directional antenna (b) Directional antenna

Fig. 1. Antenna models

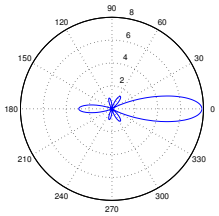


Fig. 2. Radiation pattern of UCA antenna on 2-D plane

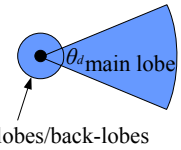


Fig. 3. Keyhole antenna

B. Antenna Models

Both good nodes and eavesdroppers are equipped with antennas, which are devices used for radiating/collecting radio signals into/from space. There are two types of antennas: *omni-directional* antennas and *directional* antennas [12]. An omni-directional antenna, which can radiate/collect radio signals uniformly to all directions in space (as shown in Fig. 1 (a)), 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 (as shown in Fig. 1 (b)).

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* in a spherical coordinate system as follows

$$G(\theta,\phi) = \eta \frac{U(\theta,\phi)}{U_o} \tag{4}$$

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 ($\phi \in (0,2\pi)$), as shown in Fig. 1 (b)), and η is the efficiency factor, which is set to be 1 since an antenna is often assumed to be lossless. We define the *radiation intensity* $U(\theta,\phi)$ as the power radiated from an antenna per unit solid angle. U_o denotes the radiation intensity of an omni-directional antenna with the same radiation power P_{rad} as a directional antenna.

We consider an idealistic *isotropic* antenna to model the antenna gain of an omni-directional antenna. 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 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

$$P_{rad} = \oiint_{\Omega} U(\theta,\phi)\, d\Omega = \int_0^{2\pi}\int_0^{\pi} U(\theta,\phi)\sin\theta d\theta d\phi \tag{5}$$

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. (5). In other words, $U_o = \frac{1}{4\pi}P_{rad}$. After replacing U_o in Eq. (4) by $\frac{1}{4\pi}P_{rad}$ and replacing P_{rad} by the integration, we have

$$G(\theta,\phi) = \frac{U(\theta,\phi)}{\frac{1}{4\pi}\int_0^{2\pi}\int_0^{\pi} U(\theta,\phi)\sin\theta d\theta d\phi} \tag{6}$$

Note that Eq. (6) can be applied for the calculation of the antenna gain of any types of directional antenna models, which will be described as follows.

One of the most commonly used directional antennas is a Uniform Circle Array (UCA) antenna, which consists of M isotropic antenna elements equally spaced on the xy-plane along a circle of radius a. 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 [13], the radiation intensity of a UCA antenna fulfills the following formula.

$$U(\theta,\phi) \propto |\mathbf{E}(\theta,\phi)|^2 \tag{7}$$

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

$$\mathbf{E}(\theta,\phi) = \sum_{m=1}^{M} I_m e^{jka[\sin\theta\cos(\phi-\phi_m)-\sin\theta_0\cos(\phi_0-\phi_m)]} \tag{8}$$

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 [11]. 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. (6) by combining Eq. (7), we then compute the gain $G(\theta,\phi)$ as follows.

$$G(\theta,\phi) = \frac{|\mathbf{E}(\theta,\phi)|^2}{\frac{1}{4\pi}\int_0^{2\pi}\int_0^{\pi}|\mathbf{E}(\theta,\phi)|^2\sin\theta d\theta d\phi} \tag{9}$$

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. 2 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 analysis. Several simplified directional antenna models are proposed to approximate

the realistic antennas [12], [14]. In this paper, we consider the *Keyhole* antenna model. As shown in Fig. 3, Keyhole antenna model consists one main-lobe with beamwidth θ_d and side/back-lobes in other directions. Following the similar calculation steps in [5], we have the antenna gain of Keyhole antenna model as follows

$$G_s = \frac{2 - G_m(1 - \cos(\frac{\theta_d}{2}))}{1 + \cos\frac{\theta_d}{2}} \tag{10}$$

where G_m and G_s are the gain of main-lobe and the gain of side-lobes and back-lobes, respectively.

C. Node Distribution

We consider a wireless ad hoc network, in which all the good nodes are equipped with omni-directional antennas and eavesdroppers are equipped with either directional antennas and omni-directional antennas for comparison purpose. All the good nodes are assumed to be randomly distributed in a 2-D 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 then have the probability mass function of the number of nodes X in an area A as follows:

$$P(X = x) = \frac{(\rho A)^x}{x!} e^{-\rho A} \tag{11}$$

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

III. Analysis on Eavesdropping Attacks

A. Effective Eavesdropping Area

As shown in Section II-A, 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., $\delta \leq \delta_0$. In other words, the probability of having no eavesdropper listening in a communication is given by

$$\begin{aligned} P(\delta > \delta_0) &= P(\frac{S_h d(u,v)^\alpha}{G_g(u)G_e(v)} > \delta_0) \\ &= P((\frac{\delta_0 G_g(u)G_e(v)}{S_h})^{\frac{1}{\alpha}} < d) \end{aligned} \tag{12}$$

We define a random variable D as

$$D = (\frac{\delta_0 G_g(u)G_e(v)}{S_h})^{\frac{1}{\alpha}} \tag{13}$$

which is referred to the *eavesdropping range* of an eavesdropper. After substituting Eq. (13) into Eq. (12), we have $P(\delta > \delta_0) = P(D < d)$, which implies that a communication can not be eavesdropped by a malicious node if it is outside its eavesdropping range D. Since D is a random variable, we denote the expected value of D by the *effective eavesdropping area*, which is given by $E[\pi D^2] = \pi E[D^2]$.

We then have

$$\begin{aligned} E[\pi D^2] &= \pi E[(\frac{\delta_0 G_g(u)G_e(v)}{S_h})^{\frac{2}{\alpha}}] \\ &= \pi(\delta_0)^{\frac{2}{\alpha}} \cdot E[S_h^{-\frac{2}{\alpha}}] \cdot E[(G_g(u)G_e(v))^{\frac{2}{\alpha}}] \end{aligned} \tag{14}$$

As shown in Eq. (14), the effective eavesdropping area consists of two components: the shadow fading component $E[S_h^{-\frac{2}{\alpha}}]$ and the antenna gain component $E[(G_g(u)G_e(v))^{\frac{2}{\alpha}}]$. In particular, the shadow fading component depends on both the shadowing effect and the path loss effect. Besides, the antenna gain component depends on the antenna gains of the eavesdropper and the good node and the path loss effect.

B. Probability of Eavesdropping Attacks

To derive the probability of eavesdropping attacks, 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 II-C), we then have the probability of no good node falling in the eavesdropping area, which is given by the following equation,

$$P(Y = 0) = e^{-\rho \cdot E[\pi D^2]} \tag{15}$$

where $E[\pi D^2]$ is given by Eq. (14).

We denote the probability of eavesdropping attacks by $P(E)$, which can be calculated as follows

$$P(E) = 1 - P(Y = 0) = 1 - e^{-\rho \cdot E[\pi D^2]} \tag{16}$$

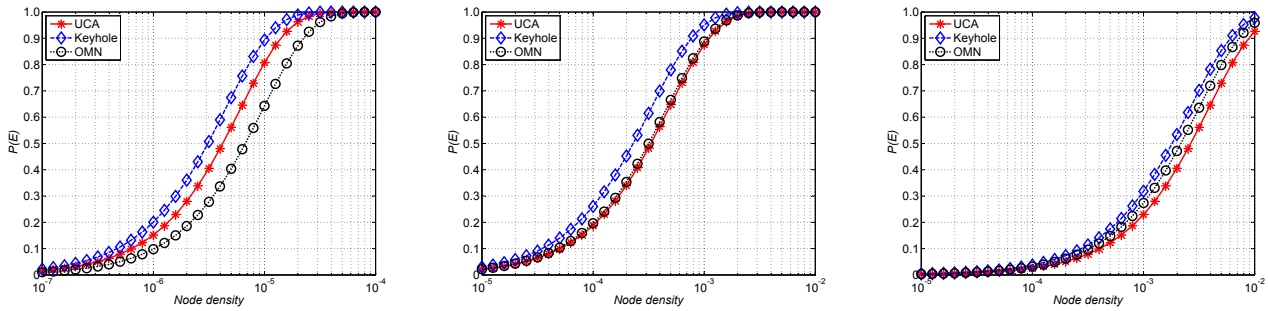
As shown in Eq. (16) and Eq. (14), the probability of eavesdropping attacks heavily depends on the path loss effect, the shadowing effect and the antenna gains. We next will conduct the numerical study on the probability of eavesdropping attacks in Section IV.

IV. Numerical Results

In this section, we present the numerical results of the probability of eavesdropping attacks. In particular, we consider the eavesdropper equipped with various antenna models, such as the omni-directional model (OMN), the keyhole model (Keyhole) and the realistic model (UCA). Note that each good node is equipped with an omni-directional antenna (OMN). Besides, both the shadow fading effect and the path loss effect are also considered in our analysis. We first give the results without shadowing effects (i.e. $\sigma = 0$) in Section IV-A. Then, we present the results with the shadow fading factor σ ranging from 6 to 10 in Section IV-B.

A. Results without Shadowing Effects

We first give the analytical results without shadowing effect (when $\sigma = 0$). Fig. 4 (a), (b) and (c) present the results with $\alpha = 2$, the results with $\alpha = 3$ and the results with $\alpha = 4$, respectively. Note that we choose the different range of the node density ρ with $\alpha = 2$ (i.e., 10^{-7} to 10^{-4}) from that with $\alpha = 3$ and $\alpha = 4$ (i.e., 10^{-5} to 10^{-2}). This is because of the higher probability of eavesdropping attacks when the path loss factor $\alpha = 2$. It implies that the good nodes are more vulnerable to eavesdropping attacks when the path loss effect is not that notable. This finding has further confirmed the previous results [5], [6]. Besides, Fig. 4



(a) $\alpha = 2$ (b) $\alpha = 3$ (c) $\alpha = 4$

Fig. 4. Probability of eavesdropping attacks $P(E)$ without shadowing effect ($\sigma = 0$) when $\alpha = 2$ (node density ρ ranging from 10^{-7} to 10^{-4}) and $\alpha = 3, 4$ (node density ρ ranging from 10^{-5} to 10^{-2}) with attenuation threshold $\delta_0 = 50$dB.

(a) also shows that both Keyhole-eavesdroppers and UCA-eavesdroppers have higher $P(E)$ than OMN-eavesdroppers when $\alpha = 2$. This may owe to the effect that a directional antenna can concentrate its receiving capability on a certain direction. As a result, a directional-eavesdropper can listen in some directions better than an OMN-eavesdropper.

Fig. 4 (b) and (c) show that Keyhole-eavesdroppers always have higher $P(E)$ than OMN-eavesdroppers and UCA-eavesdroppers. Besides, when $\alpha = 3$ (Fig. 4 (b)), the probability of eavesdropping attacks of UCA-eavesdroppers is quite close to that of OMN-eavesdroppers. For example, when the path loss factor $\alpha = 3$ and the node density $\rho = 10^{-4}$, $P(E)$ of OMN-eavesdroppers and $P(E)$ of UCA-eavesdroppers are 0.1964 and 0.1881, respectively. However, when $\alpha = 4$, OMN-eavesdroppers have higher $P(E)$ than UCA-eavesdroppers. We will explain the reasons later.

B. Results with Shadowing Effects

We then take the shadow fading effect into account. Fig. 5, Fig. 6 and Fig. 7 show the results with $\alpha = 2$, the results with $\alpha = 3$ and the results with $\alpha = 4$, respectively. For each case, we choose the shadow fading effect factor σ ranging from 6 to 10. Similar to the results without shadow fading effect, the range of the node density ρ when $\alpha = 2$ is different from that when $\alpha = 3$ and $\alpha = 4$.

We have found that the shadow fading effect has no significant impact on $P(E)$ when the shadow factor is relatively small (i.e., $\sigma \leq 6$). For example, there is no significant difference between the values of $P(E)$ with $\sigma = 0$ and the values of $P(E)$ with $\sigma = 6$. However, when the shadowing factor σ is further increased (i.e., $\sigma \leq 8$), the curves become more steep for all OMN-eavesdroppers, Keyhole-eavesdroppers and UCA-eavesdroppers. We take UCA-eavesdroppers with $\alpha = 3$ as an example. Specifically, the node density $\rho = 0.005$ with $P(E)$ reaching 1 when $\sigma = 6$ while the node density $\rho = 0.0032$ with $P(E)$ reaching 1 when $\sigma = 8$ and the node density $\rho = 0.0016$ with $P(E)$ reaching 1 when $\sigma = 10$. In other words, it requires low node density to reach the *full eavesdropping probability* (i.e., $P(E) = 1$) when the shadow fading effect is significant. This 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).

As shown in Fig. 5, Fig. 6 and Fig. 7, the probability of eavesdropping attacks always decreases with the increased path loss exponent α. This coheres with that without the shadowing effect (as shown in Fig. 4). It implies that the path loss fading effect always brings the adverse effect on the eavesdropping attacks.

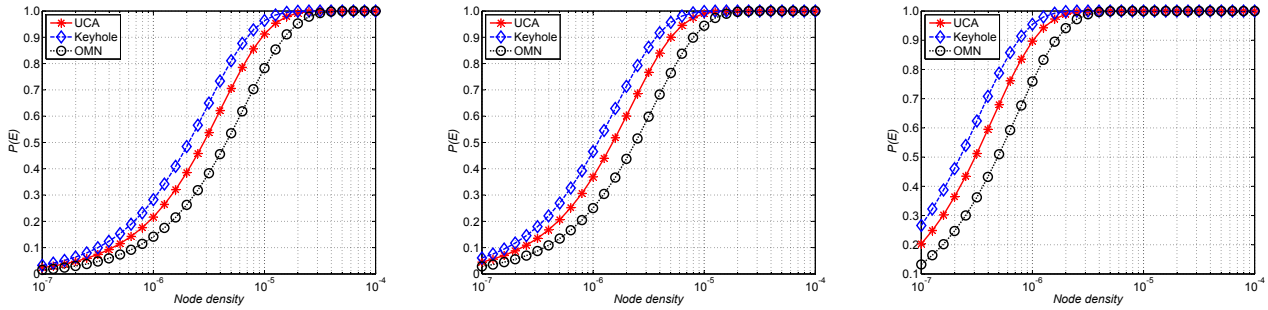
As shown in both the results with shadowing effects and the results without shadowing effects, Keyhole-eavesdroppers always have $P(E)$ than OMN-eavesdroppers and UCA-eavesdroppers. This can be explained as follows. Using directional antennas at eavesdroppers can lead to the effect that eavesdroppers 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 have even lower values of $P(E)$ than OMN-eavesdroppers when $\alpha = 4$. Compared with UCA-eavesdroppers, Keyhole-eavesdroppers are less sensitive to the "listening narrower" effect since the Keyhole model has *broader* side/back lobes.

V. Conclusion

In this paper, we analyze the probability of eavesdropping attacks in wireless networks with consideration of both channel conditions and antenna models. The numerical results show that the probability of eavesdropping attacks heavily depends on the shadowing effect, the path loss effect and the antenna models. Specifically, we have found that both Keyhole-eavesdroppers and UCA-eavesdroppers have higher probability of eavesdropping attacks than that of OMN-eavesdroppers when the path loss effect is less significant. This implies that the eavesdroppers might conduct diverse eavesdropping attacks by choosing directional or omni-directional antennas according to the path loss effect; as a result, the good nodes should take corresponding measures to prevent the attacks effectively. Besides, we have also found that the randomness brought by the shadow fading effect can lead to the increased probability of eavesdropping attacks.

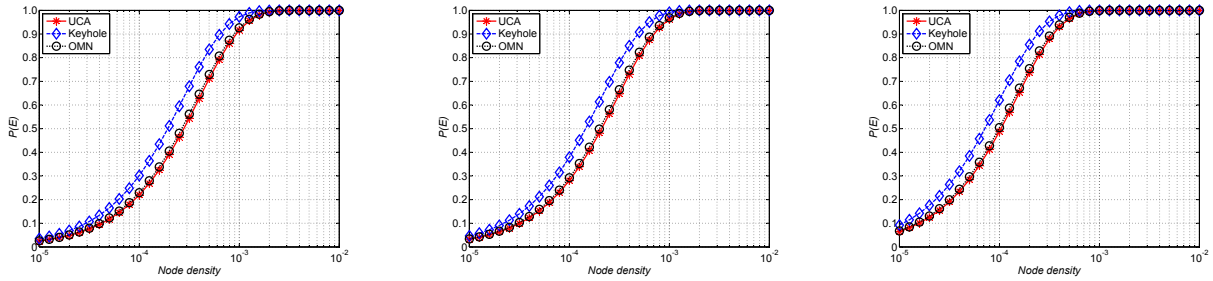
Acknowledgement

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. The authors would like to thank Gordon G.-D. Han for his excellent comments.



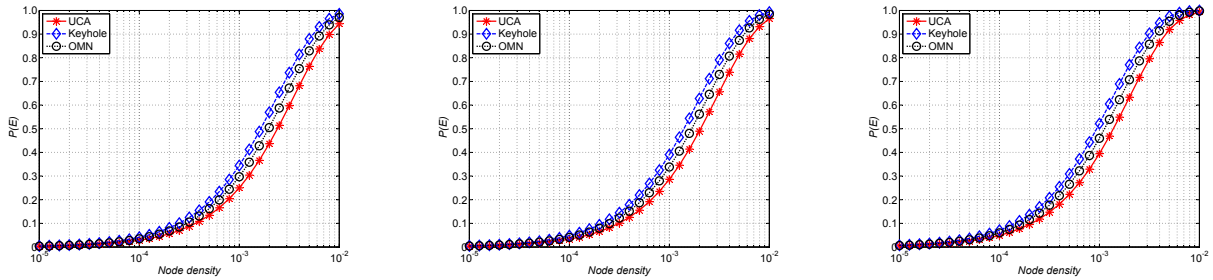
(a) $\sigma = 6$ (b) $\sigma = 8$ (c) $\sigma = 10$

Fig. 5. Probability of eavesdropping attacks $P(E)$ with shadowing effects when $\alpha = 2$ with node density ρ ranging from 10^{-7} to 10^{-4} and attenuation threshold $\delta_0 = 50$dB.



(a) $\sigma = 6$ (b) $\sigma = 8$ (c) $\sigma = 10$

Fig. 6. Probability of eavesdropping attacks $P(E)$ with shadowing effects when $\alpha = 3$ with node density ρ ranging from 10^{-5} to 10^{-2} and attenuation threshold $\delta_0 = 50$dB.



(a) $\sigma = 6$ (b) $\sigma = 8$ (c) $\sigma = 10$

Fig. 7. Probability of eavesdropping attacks $P(E)$ with shadowing effects when $\alpha = 4$ with node density ρ ranging from 10^{-5} to 10^{-2} and attenuation threshold $\delta_0 = 50$dB.

REFERENCES

[1] M. Anand, Z. G. Ivesy, and I. Leez, "Quantifying eavesdropping vulnerability in sensor networks," in *Proceedings of the 2nd International VLDB Workshop on Data Management for Sensor Networks*, 2005.

[2] J.-C. Kao and R. Marculescu, "Eavesdropping Minimization via Transmission Power Control in Ad-Hoc Wireless Networks," in *Proceedings of IEEE SECON*, 2006.

[3] X. Lu, F. Wicker, P. Lio, and D. Towsley, "Security Estimation Model with Directional Antennas," in *Proceedings of MILCOM*, 2008.

[4] H.-N. Dai, D. Li, and R. C.-W. Wong, "Exploring Security Improvement of Wireless Networks with Directional Antennas," in *Proceedings of IEEE LCN*, 2011.

[5] Q. Wang, H.-N. Dai, and Q. Zhao, "Eavesdropping Security in Wireless Ad Hoc Networks with Directional Antennas," in *Proceedings of IEEE WOCC*, 2013.

[6] H.-N. Dai, Q. Wang, D. Li, and R. C.-W. Wong, "On eavesdropping attacks in wireless sensor networks with directional antennas," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[7] F. Anjum and P. Mouchtaris, *Security for Wireless Ad Hoc Networks*, 1st ed. Wiley-Interscience, 2007.

[8] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of Generating a Secret Key Using Wireless Fading Under Active Adversary," *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1440–1451, 2012.

[9] T. S. Rappaport, *Wireless communications : principles and practice*, 2nd ed. Upper Saddle River, N.J.: Prentice Hall PTR, 2002.

[10] C. Bettstetter and C. Hartmann, "Connectivity of Wireless Multihop Networks in a Shadow Fading Environment," *Wireless Networks*, vol. 11, no. 5, pp. 571–579, 2005.

[11] X. Zhou, S. Durrani, and H. Jones, "Connectivity Analysis of Wirelss Ad Hoc Networks with Beamforming," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 9, pp. 5247 – 5257, 2009.

[12] H.-N. Dai, K.-W. Ng, M. Li, and M.-Y. Wu, "An overview of using directional antennas in wireless networks," *International Journal of Communication Systems (Wiley)*, vol. 26, no. 4, pp. 413 – 448, 2013.

[13] C. A. Balanis, *Antenna Theory : Analysis and Design*, 2nd ed. New York: John Wiley & Sons, 1997.

[14] P. Li, C. Zhang, and Y. Fang, "The Capacity of Wireless Ad Hoc Networks Using Directional Antennas," *IEEE Transactions on Mobile Computing*, vol. 10, no. 10, pp. 1374–1387, 2011.

[15] C. Bettstetter, "On the Connectivity of Ad Hoc Networks," *The Computer Journal*, vol. 47, no. 4, pp. 432 – 447, 2004.