Eavesdropping Attacks in Wireless Ad Hoc Networks under a Shadow Fading Environment

Xuran Li and Hong-Ning Dai and Qinglin Zhao and Qiu Wang

Faculty of Information Technology, Macau University of Science and Technology, Macau SAR
lxrget@163.com, hndai@ieee.org, qlzhao@must.edu.mo, qiu_wang@foxmail.com

Abstract. This paper concerns the eavesdropping attacks in wireless ad hoc networks under a shadow fading environment. Most of previous studies have only concentrated on protecting the confidential communications at both the transmitters and the receivers and little attention has been paid on investigating the eavesdropping behaviors done by the malicious nodes. We therefore investigate the eavesdropping success rate of eavesdroppers equipped with various antenna models under various channels conditions, such as the path loss effect and the shadow fading effect. In particular, we formulate the eavesdropping attack problem with consideration of both simplistic directional antenna models and realistic antenna models. We then conduct extensive simulations to evaluate the eavesdropping success rate with different eavesdroppers. Our simulation results show that the eavesdropping success rate heavily depends on both the antenna models and the channel conditions.

1 Introduction

Eavesdropping intrusion is a typical passive attack in wireless networks, which is constitutive of Internet of Vehicles (IOVs). Encryption is the most commonly used technique to protect the confidential communications, which is shown to work effectively in wireless LAN (e.g., WEP [1], WPA and WPA2 [2]). However, it may not be feasible to apply the conventional ciphers (encryption algorithms) to wireless ad hoc networks (WAHNs) due to the following inherent constraints of WAHNs [3]: (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 the centralized manner.

The current countermeasures to eavesdropping attacks in WAHNs mainly include (i) designing light-weight encryption algorithms to encrypt the communications between the transmitter and the receiver [4–6] and (ii) mitigating eavesdropping possibility by using power control schemes and using directional antennas [7–11]. But, most of the current studies have been concentrated on protecting the confidential communications at both the transmitters and the receivers, which are denoted as the good nodes. Surprisingly, only little attention has been paid to investigating the eavesdropping behaviors conducted by the malicious nodes (also named as eavesdroppers throughout the whole paper). To
probe the eavesdropping behaviors is important since we can provide the better protection on the communications if we know the activities of eavesdroppers better. For example, we only need to encrypt the communications in the area that is vulnerable to eavesdroppers so that we can significantly save the security cost of WAHNs. Therefore, the goal of this paper is to investigate the eavesdropping activities at the malicious nodes.

To the best of our knowledge, this paper is one of the first attempts in investigating the eavesdropping attacks from the eavesdroppers’ aspects. In particular, we study the eavesdropping success rate in typical WAHNs, in which good nodes are mounted with conventional omni-directional antennas while malicious nodes are mounted with either directional antennas or omni-directional antennas. In short, we call the malicious nodes with omni-directional antennas as OMN-eavesdroppers and call the malicious nodes with directional antennas as DIR-eavesdroppers. More specifically, we also consider three directional antenna models for DIR-eavesdroppers, i.e., the keyhole model, the sector model and the realistic model. To simplify our presentation, we call the eavesdropper with the keyhole model, the eavesdropper with the sector model and the eavesdropper with the realistic antenna model as Keyhole-eavesdropper, Sector-eavesdropper, and Realistic-eavesdropper, respectively. In addition, we also consider realistic wireless channel environments with considering both the shadow-fading and the path loss effects together. We then conduct empirical studies with considering the above factors together. Our major research findings are summarized as follows.

1. We found that the eavesdropping success rate of eavesdroppers heavily depends the antenna models of eavesdroppers. In particular, Keyhole-eavesdroppers usually have the highest eavesdropping success rate among all the eavesdroppers. Sector-eavesdroppers perform better when the path-loss effect is less remarkable (e.g., the path loss exponent is 3) and they perform poorer when the path-loss effect is more remarkable e.g., the path loss exponent is 4). However, Realistic-eavesdroppers always perform worse than other eavesdroppers.

2. We found that the eavesdropping success rate also heavily depends on various the channel conditions. Generally, the eavesdropping success rate is higher when the path-loss effect is less remarkable and it’s lower when the path-loss effect is more remarkable. Besides, the shadowing effect can not be ignored in analyzing the eavesdropping success rate. Specifically, when the shadowing effect is somewhat more remarkable, eavesdroppers have the higher eavesdropping success rate than those when the shadowing effect is somewhat less remarkable.

3. We provide insights from our simulations results. In particular, we found that the simplistic antenna models, such as the keyhole model and the sector model are over-optimistic on estimating the eavesdropping success rate while the realistic antenna model is too complicated. In addition, an analytical model with other channel conditions shall be proposed to investigate the eavesdropping possibility.
The remaining paper is organized as follows. We first give the system model as well as antenna models in Section 2. Section 3 then presents the problem formulation. We next give the simulation results in Section 4. Finally, the paper is concluded in Section 5.

2 System Model

2.1 Spatial 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 $\rho$, which can accurately model a uniform distribution of nodes when the network area approaches infinity [12]. We then have the probability mass function of the number of nodes $X$ in an area $A$ as follows:

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

where $\rho A$ is the expected number of nodes in area $A$.

2.2 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 in a spherical coordinate system as follows [13],

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

where $\theta$ is the elevation angle from z-axis ($\theta \in (0, \pi)$), $\phi$ is the azimuth angle from the x-axis in the xy-plane ($\phi \in (0, 2\pi)$), and $\eta$ 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.
Isotropic Antenna We consider 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, we need to conduct simulation experiments on a 2-D plane. Thus, we project the 3-D antenna gain to the $xy$-plane. Fig. 1 (a) shows the radiation pattern of an isotropic antenna.

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 Fig. 1 (b).

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

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

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

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

Fig. 1. Antenna models
Note that Eq. (4) is applied for the calculation of the antenna gain of any types of directional antenna models, which will be described as follows.

**Uniform Circle Array (UCA) Antenna** 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 $a$, as shown in Fig. 2. In this structure, $r$ is the distance between the antenna and the observation position, $\Delta$ is the distance between two neighboring elements, which is usually chosen as $\lambda/2$ and $\lambda$ is the wavelength of electromagnetic wave radiated from elements. As shown in [13], the radiation intensity of a UCA antenna fulfills the following formula.

\[ U(\theta, \phi) \propto |E(\theta, \phi)|^2 \quad (5) \]

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

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

where $j$ is the imaginary unit for which $j^2 = -1$, $k = 2\pi/\lambda$, $\lambda$ is the wavelength of the propagating signal, $\phi_m = 2\pi m/M$ is the angular position of $m$th element on $xy$-plane, $I_m$ is the amplitude excitation of the $m$th element, which is set to be 1, similar to [14]. 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.

\[ G(\theta, \phi) = \frac{|E(\theta, \phi)|^2}{\frac{1}{4\pi} \int_0^{2\pi} \int_0^\pi |E(\theta, \phi)|^2 \sin \theta d\theta d\phi} \quad (7) \]

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 $\phi = \pi/2$ (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.
2.3 Simplified Directional Antenna Models

The realistic directional antenna models (e.g., UCA and ULA antennas) are too complicated to be used in analytical studies. Thus, several simplified directional antenna models are proposed to approximate the realistic directional antennas. In particular, there are two typical simplified directional antenna models described as follows.

- **Keyhole Antenna Model** [15, 16] consists one main-lobe with beamwidth $\theta_d$ and side/back-lobes to other directions, as shown in Fig. 4 (a).
- **Sector Antenna Model** [17, 18] consists only one main-lobe with beamwidth $\theta_d$ after ignoring back/side-lobes, as shown in Fig. 4 (b).

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.

$$P_{rad} = P_s + P_m$$

(8)

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

$$P_m = \int_0^{\theta_d} \int_0^{2\pi} G_m U_0 \sin \theta \, d\theta d\phi$$

(9)

$$P_s = \int_0^{\theta_d} \int_0^{\pi} G_s U_0 \sin \theta \, d\theta d\phi - \int_0^{\theta_d/2} \int_0^{2\pi} G_s U_0 \sin \theta \, d\theta d\phi$$

(10)

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

We then have

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

(11)

As shown in Eq. (11), $G_s$ is a function of the antenna gain of the main-lobe $G_m$ and the beamwidth $\theta_d$. When $G_s = 0$, this keyhole model becomes a sector model. In practice, we choose the half-power beamwidth of a realistic antenna as $\theta_d$ for the keyhole model and the sector model.
2.4 Wireless Channel Models

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

$$P_e(v) = \frac{k_1 G_g(u) G_e(v) P_g(u)}{S_h(d(u, v))^\alpha} \tag{12}$$

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, $\alpha$ is the path loss factor usually ranging from 3 to 4 [19] 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

$$S_h = 10^{\omega/10} \tag{13}$$

where $\omega$ is a Gaussian random variable with zero mean and standard deviation usually ranging from 4 to 12 [14]. 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 $P_e(v)$. We then define the power attenuation $\delta(u, v)$ between $u$ and $v$ as follows by normalizing Eq. (12) (i.e., $k_1 = 1$)

$$\delta(u, v) = \frac{P_g(u)}{P_e(v)} = \frac{S_h(d(u, v))^\alpha}{G_g(u) G_e(v)} \tag{14}$$

This can be expressed in terms of dB as

$$\delta(u, v) = \alpha 10 \log\left(\frac{d(u, v)}{1m}\right) + 10 \log(G_g(u) \cdot G_e(v)) + 10 \log(S_h) \tag{15}$$

We define $\delta_1(u, v) = \alpha 10 \log\left(\frac{d(u, v)}{1m}\right)$dB as the geometric component, $\delta_2(u, v) = 10 \log(G_g(u) \cdot G_e(v))$ as the antenna gain component, $\delta_3(u, v) = 10 \log(S_h)$ as the shadow fading component. In particular, the geometric component $\delta_1(u, v)$ only depends on the path loss exponent $\alpha$ 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 $\delta$ is no greater than the given threshold $\delta_0$.

3 Eavesdropping Attacks in Wireless Ad Hoc Networks

In this paper, we investigate the passive eavesdropping activity in wireless networks. In particular, we consider random network topologies consisting of $N_g$ link pairs. In addition to transmitters and receivers, there are $N_e$ eavesdropper...
uniformly distributed at random in the same area. There is a fact that only transmitters can potentially be eavesdropped by eavesdroppers since only they are sending messages. Thus, we will only consider transmitters and eavesdroppers in the following analysis.

As shown in the eavesdropping model defined in Section 2.4, when the received power at an eavesdropper is greater than a given threshold, it can potentially decode the information from the transmitter, i.e., it can successfully eavesdrop the information from the transmitter. We are interested in the question - what is the possibility of messages being eavesdropped? Specifically, how many eavesdroppers will successfully eavesdrop the messages? Furthermore, what factors affect this eavesdropping possibility?

To answer these questions, we employ the success rate of eavesdropping attack to measure the eavesdropping possibility, which is in short denoted as the eavesdropping success rate. In particular, we conduct a simulation-based study over a large number of random topologies in order to obtain an empirical value for the eavesdropping success rate. To be more specific, we define the eavesdropping success rate $R(s)$ as follows

$$R(s) = \frac{\# \text{ successful eavesdroppers}}{\# \text{ eavesdroppers}}$$

where $\#$ represents “number of”. It is shown in Eq. (16) that the eavesdropping success rate is equal to the percentage of the number of eavesdroppers that successfully eavesdrop messages over the total number of eavesdroppers. The higher $R(s)$ means the higher eavesdropping possibility of the network.

4 Simulation Results

We conduct extensive simulations to investigate the eavesdropping success rate with eavesdroppers equipped with various antenna models, such as the isotropic model (OMN), the keyhole model, the sector model, the realistic antenna (UCA model). Note that every good node is equipped with an isotropic antenna (OMN). Our simulations were conducted in an area of $l \times l$ with minimizing the impacts of the border effects [12] by properly setting a larger outbox. Note that $l$ is chosen as 3200 m. The number of malicious nodes is fixed to be 50 while the number of good nodes is ranged from 200 to 3200. Note that we consider the pathloss exponent $\alpha$ ranging from $\alpha = 3$ to $\alpha = 4$, the shadow fading factor (the stand deviation) $\sigma$ 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 3,000 random topologies.

4.1 Results without Shadowing Effects

We first conduct the simulations to compare the eavesdropping success rate $R(s)$ of OMN-eavesdropper, Keyhole-eavesdropper, Sector-eavesdropper, and
Realistic-eavesdropper under the same network settings. In this set of experiments, we do not consider the shadowing effects. We present the results in Fig. 5, where the path loss factor $\alpha$ ranges from 3 to 4.

It is shown in Fig. 5 (a) and Fig. 5 (b) that when the path loss factor $\alpha$ is increased from 3 to 4, the eavesdropping success rate of all the eavesdroppers decreases. This mainly owes to the increased path loss effect when $\alpha$ is increased from 3 to 4, which results in the lower eavesdropping possibility of eavesdroppers. Besides, it is also shown in Fig. 5 (a) and Fig. 5 (b) that in both cases, Keyhole-eavesdroppers always have the highest eavesdropping success rate among all the eavesdroppers, such as OMN-eavesdroppers, Sector-eavesdroppers, and Realistic-eavesdroppers. Moreover, Sector-eavesdroppers have nearly the same eavesdropping success rate as OMN-eavesdroppers and Realistic-eavesdroppers have the slightly lower eavesdropping success rate than OMN-eavesdroppers. The possible reason behind the results mainly lies in the effect that there is no side/back-lobes in a sector antenna model (as shown in Fig. 4) while both the keyhole model and the realistic model have. When the path loss effect becomes more remarkable, it is more difficult for Sector-eavesdroppers to tap in the communications of good nodes since they can only listen in certain directions. Compared with Sector-eavesdroppers, Keyhole-eavesdropper and realistic eavesdropper can also receive the signals from other directions (in which the side/back-lobes locate) even if those signals are quite weak.

4.2 Results with Shadowing Effects

We then conduct the simulations to compare the eavesdropping success rate $R(s)$ of OMN-eavesdropper, Keyhole-eavesdropper, Sector-eavesdropper, and Realistic-eavesdropper with consideration of shadowing effects. We vary the shadowing effect factor (the standard deviation $\sigma$) from 6 to 10. We present the results in Fig. 6 and Fig. 7 where the path loss factor $\alpha$ ranges from 3 to 4.

It is shown in Fig. 6 that the eavesdropping success rate $R(s)$ of OMN-eavesdroppers, Keyhole-eavesdroppers, Sector-eavesdroppers, and Realistic-eavesdroppers significantly increases when the shadowing effect factor $\sigma$ increases (from 6, 8 to
Fig. 6. Eavesdropping success rate $R(s)$ with shadowing effects when $\alpha = 3$ with $N_e = 50$ eavesdroppers uniformly distributed nodes on $l \times l$ area threshold attenuation $\delta_0 = 50$dB.

10 corresponding to Fig. 6 (a), Fig. 6 (b) and Fig. 6 (c)). The reason behind the results may owe to the randomness induced by shadowing effects, which sometimes contribute to improvement of the network connectivity as shown in [20]. Meanwhile, Fig. 6 also shows that Sector-eavesdroppers with shadowing effects perform better than those without shadowing effects (see Fig. 5). One of the possible reasons may lie in the non-regular shape of the eavesdropping area when the shadowing effects are considered in which Sector-eavesdroppers perform the best.

Fig. 7 shows the simulation results with shadowing effects when $\alpha = 4$. When the shadowing effect factor $\sigma$ increases from 6, 8 to 10 corresponding to Fig. 7 (a), Fig. 7 (b) and Fig. 7 (c), the eavesdropping success rate $R(s)$ of OMN-eavesdroppers, Keyhole-eavesdroppers, Sector-eavesdroppers, and Realistic-eavesdroppers slightly increases. For example, $R(s)$ of Keyhole-eavesdroppers when $N_e = 3200$ is 0.3087 with $\sigma = 8$ as shown in Fig. 7 (b) in contrast to $R(s) = 0.3476$ with $\sigma = 10$ as shown in Fig. 7 (c). The main reason is the the path loss effect dominates the eavesdropping possibility when the path loss component $\alpha$ is large.

Besides, we also found that all the eavesdroppers perform differently when the path loss exponent is 3 as shown in Fig. 7 and the path loss exponent is
Fig. 7. Eavesdropping success rate $R(s)$ with shadowing effects when $\alpha = 4$ with $N_e = 50$ eavesdroppers uniformly distributed nodes on $l \times l$ area threshold attenuation $\delta_0 = 50\text{dB}$.

4 as shown in Fig. 6, respectively. In particular, we found that the eavesdropping success rate of Sector-eavesdroppers is always lower than that of other eavesdroppers when $\alpha = 4$. In other words, Sector-eavesdroppers perform much worse when the path loss effect is significantly increased. Meanwhile, at this time, OMN-eavesdroppers have the relatively higher eavesdropping success rate compared with the case when the path loss effect is less remarkable ($\alpha=3$). The reason behind the above results can be explained as follows. When the path loss effect is less remarkable (e.g., $\alpha=3$) and the shadowing effect is in force, the directional antennas have the advantage in eavesdropping attacks compared with omni-directional antennas since they can listen better in some directions. However, when the path loss effect is more remarkable, the eavesdropping area of all the eavesdroppers is shrinking, which leads to the lower eavesdropping success rate. Compared with Sector-eavesdroppers that are susceptible to the changing shape of the eavesdropping area, the shrunken eavesdropping area of OMN-eavesdroppers is not that significant. Therefore, compared with directional antennas, omni-directional antennas seems less sensitive to the varying environments.
4.3 Discussions

As shown in the simulation results when either shadowing effects are considered or not, Realistic-eavesdroppers always perform worse than Keyhole-eavesdroppers, Sector-eavesdroppers and OMN-eavesdroppers. These results are counter-intuitive since using directional antennas at either transmitters or receivers can usually improve Signal-to-Interference-Noise-Ratio (SINR), implying that DIR-eavesdroppers can listen better than OMN-eavesdroppers. The reason behind these results can be explained as follows:

1. Due to the side-lobes and back-lobes of realistic antennas (as shown in Fig. 1 (b)), which can not be ignored, the listening capability of Realistic-eavesdroppers is lessened compared with simplistic directional antenna models, such as keyhole model and sector model. As a result, Realistic-eavesdroppers have less chance to tap in the communications of good nodes.

2. The simplistic directional antenna models, such as keyhole model and sector model are over-optimistic to estimate the eavesdropping success rate since they somewhat exaggerate the listen capability of directional antennas. For example, Keyhole-eavesdroppers can listen further and broader than Realistic-eavesdroppers.

According to the above point 2, we argue that the simplistic antenna models are still quite useful since realistic antennas are too complicated to be used in analyzing the performance of wireless networks with directional antennas. One of possible future works is to propose a less complicated but more realistic antenna model to be employed to the analytical studies.

Moreover, so far we have found that there are few analytical models on investigating eavesdropping attacks, in which most of environmental factors such as the shadowing effect, the path loss effect and the multi-path effect have been considered together. To quantitatively investigate the impacts of multiple the channel conditions together is another interesting open topic in the future.

5 Conclusion

In this paper, we investigate the eavesdropping attacks in wireless ad hoc networks from an eavesdropper’s aspect. Specifically, we consider various channel conditions such as the path loss effect and the shadowing effect. Besides, we also assume that eavesdroppers are equipped with omni-directional antennas, realistic directional antennas, the keyhole antenna model and the sector antenna model. Our simulation results show that the eavesdropping success rate heavily depends on the channel conditions and the antenna models.

Acknowledgment

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 constructive comments.
References


