Exploring Security Improvement of Wireless Networks with Directional Antennas

Hong-Ning Dai and Dong Li
Macau University of Science and Technology, Macau
hndai@ieee.org, dli@ieee.org

Raymond Chi-Wing Wong
Hong Kong University of Science and Technology, Hong Kong
raywong@cse.ust.hk

***Abstract*—There are a number of studies on using directional antennas in wireless networks. Many of them concentrate on analyzing the theoretical capacity improvement by using directional antennas. Other studies focus on designing proper Medium Access Control (MAC) protocols to improve the practical network throughput. There are few works on the security improvement using directional antennas. In this paper, we explore the benefits of directional antennas in security improvements on both single-hop and multi-hop wireless networks. In particular, we found that using directional antennas in wireless networks can significantly reduce the eavesdropping probabilities of both single-hop transmissions as well as multi-hop transmissions and consequently improve the network security.**

I. Introduction

Wireless networks typically consist of nodes equipped with omni-directional antennas which broadcast radio signals uniformly in all directions. Only a portion of these signals can reach the destinations and most of them are lost. This property of radiating signals omni-directionally inevitably leads to *high interference* and a *short transmission range*. Both these two factors severely limit the network performance of wireless networks equipped with omni-directional antennas. We call such networks as wireless omni-directional networks (*WONs*).

Compared with omni-directional antennas, directional antennas can concentrate most of radio signals on desired directions. In other undesired directions, there are no radio signals or weakened signals. Therefore, using directional antennas in wireless networks can potentially reduce the interference. Besides, the transmission range can be significantly extended compared with omni-directional antennas. We call such networks as directional-antennas wireless networks (*DAWNs*).

Most of the recent studies on DAWNs are concerned with the performance improvement of DAWNs. In particular, there are a number of theoretical studies on the scalability of DAWNs in terms of the network capacity [1], [2] and the network delay [3]. Besides, other studies focus on the designing issues of DAWNs, especially on Medium Access Control (MAC) layer, e.g., [4]–[10].

However, there are few studies on the security issue of DAWNs, especially for the *eavesdropping attack*. In particular, there are two types of eavesdropping attacks in wireless networks [11]: (i) *Passive Eavesdropping*, in which the *adversary* nodes detect the information by listening to the message transmission in the broadcasting medium of wireless networks; (ii) *Active Eavesdropping*, in which the adversary nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly nodes.

In this paper, we only focus on the *passive eavesdropping attack*. We found that using directional antennas in wireless networks can significantly improve the network security in terms of reducing the *eavesdropping probability* in both single-hop networks and multi-hop networks. Our contributions are shown as follows.

- We formally establish the eavesdropping model in wireless networks. In particular, we propose *the exposure region* to determine whether an adversary node can eavesdrop the transmission or not.
- We analyze the eavesdropping attack in single-hop networks. In particular, we derive the eavesdropping probabilities of a single-hop WON and a single-hop DAWN. Moreover, we found that a DAWN has a much lower eavesdropping probability than a WON since it has a smaller exposure region.
- We conduct a study on the eavesdropping attack in multi-hop networks. Specifically, we found that using directional antennas in multi-hop wireless networks can significantly reduce the multi-hop eavesdropping probability than using omni-directional antennas.

The remainder of the paper is organized as follows. Section II presents the models and the definitions. In Section III, we analyze the eavesdropping attack in single-hop networks. Section IV presents the analytical results of the eavesdropping attach in multi-hop networks. We conclude the paper in Section V.

II. Models and Notations

In this paper, we consider a directional antenna model that was used in previous studies [1], [9], [12]. In particular, we assume that a directional antenna gain G_d is within a specific angle θ, where θ is the beamwidth of the antenna, as shown in Fig. 1. The gain outside the beamwidth is assumed to be zero. More specifically, we have

$$G_d = \begin{cases} \frac{2\pi}{\theta} & \text{within } \theta \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

The antenna gain of an omni-directional antenna can be regarded as a special case in our model when the beamwidth $\theta = 2\pi$. Then, we have $G_o = 1$. Note that a directional antenna generally has a beamwidth $\theta < \pi$. Therefore, we have

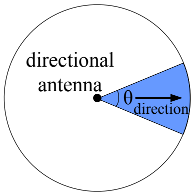


Fig. 1. The Antenna Model

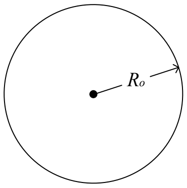


Fig. 2. The omni-directional exposure region

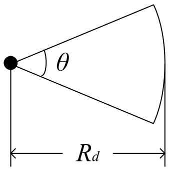


Fig. 3. The directional exposure region

$G_d > G_o$. Moreover, the narrower the beamwidth of an antenna is, the higher antenna gain it has.

A. Transmission Model

We denote P_t the common transmission power for every node in the network and γ_{ij} the channel gain from node i to node j. Thus, the received power at node j is $P_t \cdot \gamma_{ij}$. The signal-to-interference-plus-noise ratio at node j denoted by $SINR$ is defined to be

$$\frac{P_t \cdot \gamma_{ij}}{\eta + \sum_{k \neq i} P_k \cdot \gamma_{kj}} \tag{2}$$

The transmission from node i can be successfully received by node j if and only if $SINR \geq \beta$ where β is the minimum signal to interference and noise ratio and η is the environmental noise power level, which is assumed to be the same for all nodes.

There are only one transmitter and one receiver in a single-hop network and all others nodes are passive *adversary* nodes, which will not transmit actively. In a multi-hop network, there are N *good* nodes and M passive *adversary* nodes, which will not transmit actively. Besides, only one of all the N good nodes can transmit at a time. Thus, we ignore the interference from other nodes. Then we have $\sum_{k \neq i} P_k \cdot \gamma_{kj} = 0$.

$$SINR = \frac{P_t \cdot \gamma_{ij}}{\eta} \geq \beta \tag{3}$$

In this paper, we only consider the large-scale path loss in the channel model [13]. Thus, the channel gain is given by

$$\gamma_{ij} = C \cdot G_t \cdot G_r \cdot \frac{1}{d_{ij}^{\alpha}} \tag{4}$$

where d_{ij} denotes the distance between node i and node j, $C = (\frac{\lambda}{4\pi})^2$ (λ is the wavelength of the signal), G_t and G_r are the antenna gains for the transmitter and the receiver, respectively, and α is the path loss factor ($3 \leq \alpha \leq 4$) [13].

B. Eavesdropping Model

In this paper, we consider two cases: (I) Omni-directional case and (II) Directional case, as shown in Table I.

We use a Poisson point process to model the distribution of both the adversary nodes and the good nodes [14]. In particular, the probability $p(i)$ of finding i nodes in an area of S is given by:

$$p(i) = f(i, S) = \frac{(\rho S)^i}{i!} e^{-\rho S} \tag{5}$$

TABLE I
DIRECTIONAL CASE AND OMNI-DIRECTIONAL CASE

	Omni-directional (I)	**Directional (II)**
Transmitter	Omni	Directional
Receiver	Omni	Omni
Adversary	Omni	Omni

where ρ is the node density.

If an adversary node can correctly decode the information from the transmitter, the SINR at the adversary node must satisfy the condition given in Inequality 3. Combining Inequality 3 and Eq. 4, we have

$$d_{ij} \leq (\frac{C \cdot P_t \cdot G_t \cdot G_r}{\beta \cdot \eta})^{\frac{1}{\alpha}} \tag{6}$$

We denote the right hand side of Eq. 6 as R_{max} which is the maximum radius within which an adversary node can correctly eavesdrop the information from the transmitter.

Definition 1: (Eavesdrop Condition). An adversary node can successfully eavesdrop the information from the transmitter *if and only if the adversary node is within the exposure region of the transmitter.*

Definition 2: (Exposure Region). The *exposure region* of a transmitter is an area that any adversary nodes within this area can eavesdrop the transmission from the transmitter.

In particular, in the omni-directional case, a transmitter has an exposure region of a *circle* with radius R_o, as shown in Fig. 2, which can be calculated by

$$R_o = (\frac{C \cdot P_t \cdot G_o \cdot G_o}{\beta \cdot \eta})^{\frac{1}{\alpha}} \tag{7}$$

In the directional case, a transmitter has an exposure region of a *sector* with angle θ and radius R_d, as shown in Fig. 3, which is given by

$$R_d = (\frac{C \cdot P_t \cdot G_d \cdot G_o}{\beta \cdot \eta})^{\frac{1}{\alpha}} \tag{8}$$

Definition 3: (Eavesdropping Probability). The eavesdropping probability $p(\mathrm{e})$ equals the probability that *at least* one adversary node falls into the exposure region S of the transmitter.

Combining the definition of the eavesdropping probability and Eq. 5, we have

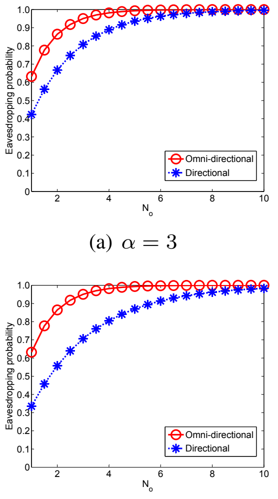
$$p(\mathrm{e}) = p(i \geq 1) = 1 - e^{-\rho \cdot S} \tag{9}$$

Therefore, the eavesdropping probability depends on the *node density* ρ and the *area of the exposure region* S. The higher the node density is, the higher eavesdropping probability is. Besides, the larger area of the exposure region also leads to a higher eavesdropping probability.

III. SECURITY ANALYSIS ON SINGLE-HOP NETWORKS

To simplify the analysis, we define the *reference node density* N_o, which is the average number of nodes within an exposure region of the Omni-directional case, as follows

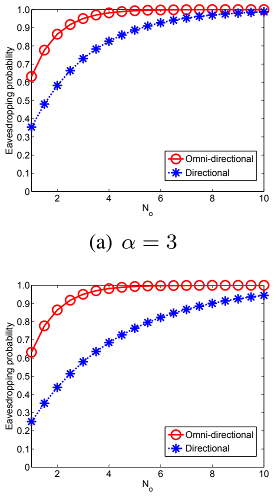
$$N_o = \rho \cdot S_o = \rho \cdot \pi \cdot R_o^2 \tag{10}$$



(a) $\alpha = 3$

(b) $\alpha = 4$

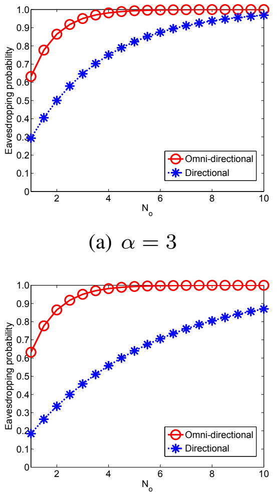
Fig. 4. $p(\mathrm{e})$ with $\theta = \frac{\pi}{3}$



(a) $\alpha = 3$

(b) $\alpha = 4$

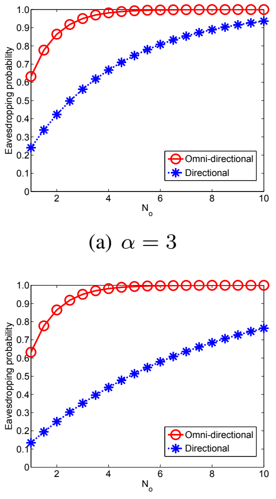
Fig. 5. $p(\mathrm{e})$ with $\theta = \frac{\pi}{6}$



(a) $\alpha = 3$

(b) $\alpha = 4$

Fig. 6. $p(\mathrm{e})$ with $\theta = \frac{\pi}{12}$



(a) $\alpha = 3$

(b) $\alpha = 4$

Fig. 7. $p(\mathrm{e})$ with $\theta = \frac{\pi}{24}$

The average node within an exposure region of the Directional case (i.e., a sector with radius R_d and angle θ)

$$N_d = \rho \cdot S_d = N_o \cdot (\frac{\theta}{2\pi})^{1-\frac{2}{\alpha}} \tag{11}$$

From Eq. 11, when $\alpha > 2$ and $\theta < 2\pi$, we always have $S_d < S_o$ and $N_d < N_o$.

We then calculate the eavesdropping probability of a WON, $p_o(\mathrm{e})$, and the eavesdropping probability of a DAWN, $p_d(\mathrm{e})$. It is shown in Fig. 4, 5, 6 and 7 that both the eavesdropping probabilities $p_o(\mathrm{e})$ and $p_d(\mathrm{e})$ increase when N_o increases. This is because, when N_o increases, the more adversary nodes fall into the exposure regions and lead to the higher eavesdropping probability and the less secure.

Besides, it is also shown in Fig. 4, 5, 6 and 7 that at any cases, the eavesdropping probability $p_d(\mathrm{e})$ of a DAWN is always less than that of a WON. This is because a directional antenna has a smaller exposure region than an omni-directional antenna. Thus, using directional antennas in wireless networks can potentially reduce the eavesdropping probability and improve the security.

Moreover, we also found that $p_d(\mathrm{e})$ decreases with the increased path loss factor α (increasing from 3 to 4). It is shown in [13] that the path loss factor α is generally ≥ 3 in urban outdoor environments. Therefore, using directional antennas in such environments may bring more benefits on reducing the eavesdropping probability.

It is also shown in Fig. 4, 5, 6 and 7 that the narrower the antenna beamwidth θ is, the lower eavesdropping probability of a DAWN $p_d(\mathrm{e})$ is. Therefore, using a narrower-beam antenna can potentially reduce the eavesdropping probability and further improve the security of transmissions.

IV. Security Analysis on Multi-hop Networks

A. Linear Networks

Fig. 8 illustrates a linear network consisting of a source node S, a destination node D and n routing nodes, which are all good nodes. Except them, all other nodes around them are adversary nodes. We are concerned about the minimum number of hops H, which is required to route a packet from S to D. In fact, $H = \lceil \frac{l}{d} \rceil$. In particular, we have the minimum number of hops of a WON, $H_o = \lceil \frac{l}{R_o} \rceil$ and the minimum number of hops of a DAWN, $H_d = \lceil \frac{l}{R_d} \rceil$.

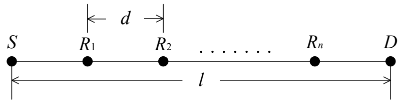


Fig. 8. The Linear Network

Note that the maximum possible length of the routing path l is determined by the node density and the number of nodes in the networks. We assume that the number of adversary nodes M is far greater than the number of good nodes N (including source node S and destination node D as well as the routing nodes), i.e., $M >> N$. In fact, l is bounded by $\sqrt{\frac{M}{\rho}}$, where ρ is the node density.

Definition 4: Eavesdropping Probability for Multi-hop. The eavesdropping probability of a multi-hop transmission is the probability that *at least* one-hop transmission is eavesdropped.

The eavesdropping probability of a multi-hop transmission can be calculated by

$$p_m(\mathrm{e}) = 1 - (1 - p(\mathrm{e}))^H \tag{12}$$

For a WON, $p(\mathrm{e}) = p_o(\mathrm{e})$. Therefore, we have

$$p_{mo}(\mathrm{e}) = 1 - (1 - p_o(\mathrm{e}))^{H_o} \tag{13}$$

For a DAWN, $p(\mathrm{e}) = p_d(\mathrm{e})$ and we have

$$p_{md}(\mathrm{e}) = 1 - (1 - p_d(\mathrm{e}))^{H_d} \tag{14}$$

B. Analytical Results

To illustrate the eavesdropping probability of multi-hop transmissions with varied N_o, θ and α, we calculate the values of

N_o	p_{mo}(e)	p_{md}(e)
1	0.9817	0.6053
2	0.9975	0.7315
3	0.9975	0.8002
4	0.9996	0.8443
5	0.9999	0.8749
6	0.9999	0.8975

(a) $\alpha = 3$

N_o	p_{mo}(e)	p_{md}(e)
1	0.9502	0.4800
2	0.9817	0.6033
3	0.9975	0.6778
4	0.9997	0.7296
5	0.9999	0.7682
6	0.9999	0.7984

(b) $\alpha = 4$

TABLE II
THE MULTI-HOP EAVESDROPPING PROBABILITY WHEN $\theta = \frac{\pi}{3}$

N_o	p_{mo}(e)	p_{md}(e)
1	0.9817	0.4433
2	0.9975	0.5632
3	0.9975	0.6374
4	0.9996	0.6901
5	0.9999	0.7301
6	0.9999	0.7618

(a) $\alpha = 3$

N_o	p_{mo}(e)	p_{md}(e)
1	0.9502	0.3221
2	0.9817	0.4229
3	0.9975	0.4900
4	0.9997	0.5404
5	0.9999	0.5808
6	0.9999	0.6142

(b) $\alpha = 4$

TABLE III
THE MULTI-HOP EAVESDROPPING PROBABILITY WHEN $\theta = \frac{\pi}{6}$

N_o	p_{mo}(e)	p_{md}(e)
1	0.9817	0.3086
2	0.9975	0.4066
3	0.9975	0.4722
4	0.9996	0.5219
5	0.9999	0.5618
6	0.9999	0.5950

(a) $\alpha = 3$

N_o	p_{mo}(e)	p_{md}(e)
1	0.9502	0.2064
2	0.9817	0.2789
3	0.9975	0.3299
4	0.9997	0.3702
5	0.9999	0.4036
6	0.9999	0.4323

(b) $\alpha = 4$

TABLE IV
THE MULTI-HOP EAVESDROPPING PROBABILITY WHEN $\theta = \frac{\pi}{12}$

N_o	p_{mo}(e)	p_{md}(e)
1	0.9817	0.2074
2	0.9975	0.2802
3	0.9975	0.3314
4	0.9996	0.3718
5	0.9999	0.4053
6	0.9999	0.4341

(a) $\alpha = 3$

N_o	p_{mo}(e)	p_{md}(e)
1	0.9502	0.1284
2	0.9817	0.1767
3	0.9975	0.2119
4	0.9997	0.2404
5	0.9999	0.2646
6	0.9999	0.2859

(b) $\alpha = 4$

TABLE V
THE MULTI-HOP EAVESDROPPING PROBABILITY WHEN $\theta = \frac{\pi}{24}$

p_{mo}(e) and p_{md}(e), respectively, and list them in Tables II, III, IV and V.

It is shown in Tables II, III, IV and V that with the increased node density N_o, both p_{mo}(e) and p_{md}(e) also significantly increase. But we always have $p_{md}(\mathrm{e}) < p_{mo}(\mathrm{e})$. This is because directional antennas can significantly reduce the eavesdropping probability of multi-hop transmissions. This security improvement owe to two benefits: (i) the narrow beamwidth leads to the lower eavesdropping probability; (ii) the longer transmission range of a directional antenna leads to the fewer hops and consequently results in less eavesdropping probability of multi-hop transmissions.

Besides, Tables II, III, IV and V also show that the narrower the beamwidth θ is, the smaller the eavesdropping probability p_{md}(e) is. For example, $p_{md}(\mathrm{e}) = 0.4323$ with beamwidth $\theta = \frac{\pi}{12}$ is much smaller than $p_{md}(\mathrm{e}) = 0.6142$ with beamwidth $\theta = \frac{\pi}{6}$ under the same network setting, i.e., the node density $N_o = 6$ and the path loss factor $\alpha = 4$.

Moreover, it is also shown in Table II, III, IV and V that p_{md}(e) decreases when the path loss factor α increases. Therefore, using directional antennas in such high path loss environments may gain more security improvement.

V. CONCLUSION

In this paper, we explored using directional antennas in wireless networks to improve the network security in terms of reducing the eavesdropping probability. In particular, we analyzed the eavesdropping probability of single-hop transmissions and that of multi-hop transmissions, respectively. We found that using directional antennas in either a single-hop network or a multi-hop network can significantly reduce the eavesdropping probability. The security improvements owe to the *smaller exposure region* and the *fewer hops* due to the longer transmission range. It is shown that using a narrow beam antenna can significantly improve the network security.

REFERENCES

[1] S. Yi, Y. Pei, and S. Kalyanaraman, "On the capacity improvement of ad hoc wireless networks using directional antennas," in *Proc. of MobiHoc*, 2003.

[2] J. Zhang and S. C. Liew, "Capacity improvement of wireless ad hoc networks with directional antennae," *Mobile Computing and Communications Review*, vol. 10, pp. 17 – 19, 2006.

[3] H.-N. Dai, "Throughput and delay in wireless sensor networks using directional antennas," in *Proceedings of the Fifth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2009.

[4] Y. B. Ko, V. Shankarkumar, and N. H. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks," in *Proc. INFOCOM'2000*, Tel Aviv, Israel, 2000, pp. 13 – 21.

[5] A. Nasipuri, S. Ye, and R. E. Hiromoto, "A MAC protocol for mobile ad hoc networks using directional antennas," in *Proc. WCNC*, 2000.

[6] R. Ramanathan, "On the performance of ad hoc networks with beamforming antennas," in *Proc. of MobiHoc*, 2001.

[7] M. Takai, J. Martin, R. Bagrodia, and A. Ren, "Directional virtual carrier sensing for directional antennas in mobile ad hoc networks," in *Proc. MobiHoc'2002*, Lausanne, Switzerland, 2002, pp. 183 – 193.

[8] R. R. Choudhury, X. Yang, N. H. Vaidya, and R. Ramanathan, "Using directional antennas for medium access control in ad hoc networks," in *Proc. of ACM MobiCom*, 2002.

[9] T. Korakis, G. Jakllari, and L. Tassiulas, "A MAC protocol for full exploitation of directional antennas in ad-hoc wireless networks," in *Proc. MobiHoc'2003*, Annapolis, Maryland, USA, 2003, pp. 98 – 107.

[10] H.-N. Dai, K.-W. Ng, and M.-Y. Wu, "A Busy-Tone based MAC Scheme for Wireless Ad Hoc Networks using Directional Antennas," in *Proc. of IEEE GLOBECOM*, 2007.

[11] 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.

[12] H.-N. Dai, K.-W. Ng, R. C.-W. Wong, and M.-Y. Wu, "On the Capacity of Multi-Channel Wireless Networks Using Directional Antennas," in *Proc. of IEEE INFOCOM*, 2008.

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

[14] Y. Wang and J. J. Garcia-Luna-Aceves, "Directional collision avoidance in ad hoc networks," *Performance Evaluation Journal (Elsevier)*, vol. 58, pp. 215–241, 2004.