Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 760834, 13 pages
http://dx.doi.org/10.1155/2013/760834

Research Article

On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas

Hong-Ning Dai,[1] Qiu Wang,[1] Dong Li,[1] and Raymond Chi-Wing Wong[2]

[1] *Faculty of Information Technology, Macau University of Science and Technology, Avenida Wai Long, Taipa, Macau*
[2] *Department of Computer Science and Engineering, The Hong Kong University of Science and Technology,
Clear Water Bay, Kowloon, Hong Kong*

Correspondence should be addressed to Hong-Ning Dai; hndai@ieee.org

Received 2 March 2013; Revised 29 June 2013; Accepted 29 June 2013

Academic Editor: S. Khan

The eavesdropping attack is a serious security threat to a wireless sensor network (WSN) since the eavesdropping attack is a prerequisite for other attacks. Conventional WSNs consist of wireless nodes equipped with omnidirectional antennas, which broadcast radio signals in all directions and are consequently prone to the eavesdropping attacks. Different from omnidirectional antennas, directional antennas radiate radio signals on desired directions and potentially reduce the possibility of the eavesdropping attacks. In this paper, we propose a model to analyze the eavesdropping probability in both single-hop WSNs and multihop WSNs with omnidirectional antennas and directional antennas. We verify the correctness of our analytical model by conducting extensive simulations. We have found that using directional antennas in either single-hop WSNs or multihop WSNs can significantly reduce the eavesdropping probability. The reason of the improved security of WSNs with directional antennas lies in (i) *the smaller exposure region* of a directional antenna and (ii) *the fewer hops* to route a packet due to the longer transmission range of a directional antenna. Our results have also shown that the security improvement factor heavily depends on the node density, the antenna beamwidth, and the signal path loss factor.

1. Introduction

Recently, wireless sensor networks (WSNs) have received enormous interests from both industry and academia [1]. WSNs have been used in environmental monitoring, health care, surveillance security, farming, and so forth. Many studies assume that sensor nodes are deployed in random from an airplane. Those scatted sensor nodes self-organize to form an ad hoc network, in which data packets are transmitted through multihops from the source node to the destination node.

In WSNs, any wireless node residing in the *transmission* range of the transmitter can potentially decode the signal when both the transmitter and the receiver are unaware of the *reconnaissance* [2]. The reconnaissance, also named the *eavesdropping* activity, has attracted considerable attentions recently since many adversary attacks often follow the eavesdropping activity, for example, hear-and-fire attacks [3]. Specifically, there are two types of eavesdropping attacks in WSNs [4]: (i) *Passive Eavesdropping*, in which the *malicious* nodes detect the information by listening to the message transmission in the broadcasting wireless medium; (ii) *Active Eavesdropping*, where the malicious nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly nodes. The study on the passive eavesdropping attacks is often more important than that on the active eavesdropping attacks since the malicious nodes must have the knowledge of the friendly nodes via conducting passive eavesdropping activities before they can actively attack the friendly nodes. Thus, we only consider the passive eavesdropping attacks in this paper.

Conventional WSNs typically consist of nodes equipped with omnidirectional 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 omnidirectionally inevitably leads to *high interference* and a *short transmission range*. Both these two factors severely limit the network performance of WSNs equipped with omnidirectional antennas. We call such networks as wireless omnidirectional sensor networks (*WONs*).

Compared with omnidirectional antennas, directional antennas can concentrate most of radio signals on desired directions. In other undesired directions, there are no radio signals or the weakened signals. Therefore, using directional antennas in WSNs can potentially reduce the interference [5]. Besides, the transmission range can be significantly extended compared with omnidirectional antennas. We call such networks as directional-antennas wireless sensor networks (*DAWNs*).

1.1. Contributions. In this paper, we only concentrate on the *passive eavesdropping attack* in *WONs* and *DAWNs*. We have found that using directional antennas in WSNs can significantly improve the network security in terms of reducing the *eavesdropping probability* in both single-hop networks and multihop networks. Our contributions are summarized as follows.

The first contribution of this paper is to formally establish the eavesdropping model in WSNs with consideration of omnidirectional antennas and directional antennas. In particular, we propose *the exposure region* to determine whether an adversary node can eavesdrop the transmission or not. We also define the eavesdropping condition, the single-hop eavesdropping probability, and the multihop eavesdropping probability.

Secondly, we analyze the eavesdropping attacks in both single-hop networks and multihop networks with both omnidirectional antennas and directional antennas. We have found that a *DAWN* has a much lower eavesdropping probability than a *WON* in either single-hop networks or multihop networks. The security improvement of directional antennas owes to the *smaller exposure region* and the *fewer hops to route a packet*.

Last, we conduct extensive simulations to verify the correctness of our analytical models. We show that the simulation results exactly agree with our analytical model in both single-hop *WONs* and single-hop *DAWNs*. We also show that both the simulation results and the analytical results in multihop networks keep the same trend in the eavesdropping probability although there exist quite small gaps between them. We have found the reasons behind this effect and pointed out the future direction.

The remainder of the paper is organized as follows. Section 2 presents the models and the definitions. In Section 3, we analyze the eavesdropping attack in single-hop networks. Section 4 presents the analytical results of the eavesdropping attach in multihop networks. We then discuss the simulation results in Section 5. Section 6 reviews the related work. Finally, we conclude the paper in Section 7.

2. Models and Notations

We adopt the notations shown in (Notation) throughout the paper. Sections 2.1 and 2.2 present the directional antenna model and the transmission model, respectively. In Section 2.3, we propose an eavesdropping model to analyze the eavesdropping attacks.

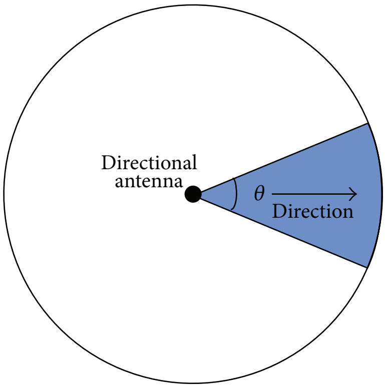


Figure 1: The antenna model.

2.1. Antenna Model. In this paper, we consider a directional antenna model that was used in previous studies [6–11]. This model can simplify our analysis. The reasons why we choose the model are summarized as follows. Firstly, even in a more realistic model, the sidelobes and backlobes are so small that they can be ignored. For example, in a more realistic model (the cone-sphere model) [12] in which the sidelobes and backlobes are counted, the gain of the main lobe is more than 100 times of the gain of the sidelobes. Secondly, smart antennas often have null capability that can almost eliminate the sidelobes and backlobes.

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 Figure 1. The gain outside the beamwidth is assumed to be zero. More specifically, we have

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

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

2.2. Channel Model. We next describe the channel model. We denote the transmission power of node i by P_i and represent the channel gain from node i to node j as γ_{ij}. We also assume that all nodes use the same transmission power P_t, that is, $P_i = P_t$. 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

$$\mathrm{SINR} \geq \beta, \tag{3}$$

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.

Note that there are only one transmitter and one receiver in a single-hop network and all other nodes are *adversary* nodes, which are passive eavesdroppers and will not transmit actively. In a multihop network (see Section 4), there are N *good* nodes and M passive *adversary* nodes, which will not transmit actively. Besides, we also assume that only one of all the N good nodes can transmit at a time. Based on these assumptions on a single-hop network and a multihop network, we can concentrate our analysis on the eavesdropping attacks and ignore the interference from other nodes. Therefore, we have $\sum_{k \neq i} P_k \cdot \gamma_{kj} = 0$. We then have

$$\mathrm{SINR} = \frac{P_t \cdot \gamma_{ij}}{\eta} \geq \beta. \tag{4}$$

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

$$\gamma_{ij} = C \cdot G_t \cdot G_r \cdot \frac{1}{d_{ij}^{\alpha}}, \tag{5}$$

where d_{ij} denotes the distance between node i and node j, $C = (\lambda/4\pi)^2$ (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 ($2 \leq \alpha \leq 4$) [13].

Note that the channel model also holds for both the normal transmission and the eavesdropping attack. When the channel model is used for the normal transmission, G_t and G_r in (5) are the antenna gain of a transmitter and the antenna gain of a receiver, respectively, where a transmitter and a receiver are also denoted as *Good* nodes. When the channel model is used for the eavesdropping attack, G_t and G_r in (5) are the antenna gain of a transmitter and the antenna gain of an adversary node, respectively, where an adversary node is also denoted as a *malicious* or *bad* node.

2.3. Eavesdropping Model. We next formally propose our eavesdropping model. First, we map *WONs* and *DAWNs* to the following two cases, which are summarized in Table 1.

Table 1: Directional case and omnidirectional case.

	Omnidirectional (I)	Directional (II)
Transmitter	Omni	Directional
Receiver	Omni	Omni
Adversary	Omni	Omni

In Case I (Omnidirectional), the transmitters, the receivers, and the adversary nodes use omnidirectional antennas (Omni for short). The Omnidirectional case corresponds to a *WON*. In Case II (Directional), the transmitters use directional antennas while the receivers and adversary nodes use omnidirectional antennas. The Directional case corresponds to a *DAWN*. Note that the adversary nodes are equipped with omnidirectional antennas in both Cases I and II. This is because, due to the directionality of a directional antenna, the adversary nodes have no knowledge about the position of the transmitter. They have to listen *omnidirectionally* in order to eavesdrop the messages. Similarly, we also consider that the receivers use omnidirectional antennas so that they can find the transmitters easily.

Second, we analyze the channel model for the eavesdropping attacks. 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 (4). After combining Inequality (4) and (5), we have

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

We denote the right-hand side (RHS) of (6) as

$$R_{\max} = \left(\frac{C \cdot P_t \cdot G_t \cdot G_r}{\beta \cdot \eta} \right)^{1/\alpha} \tag{7}$$

which is the maximum radius within which an adversary node can correctly eavesdrop the information from the transmitter.

We then define the *exposure* region as follows.

Definition 1 (exposure region). The exposure region of a transmitter is an area that any adversary nodes within this area can potentially eavesdrop the transmission from the transmitter.

It is obvious that the area of the exposure region is determined by the geometric shape of the exposure region and the maximum radius $R_{\max}$, which is defined in (7). Note that in Case I (Omnidirectional), a transmitter has a *circular* exposure region with radius $R_{\max} = R_o$, which can be calculated by

$$R_o = \left(\frac{C \cdot P_t \cdot G_o^2}{\beta \cdot \eta} \right)^{1/\alpha}, \tag{8}$$

where G_o^2 means that both the transmitter and the adversary node are using omnidirectional antennas.

In Case II (Directional), a transmitter has an exposure region of a *sector* with angle θ and radius $R_{\max} = R_d$, which is given by

$$R_d = \left(\frac{C \cdot P_t \cdot G_d \cdot G_o}{\beta \cdot \eta} \right)^{1/\alpha}, \tag{9}$$

where G_d means that the transmitter is using a directional antenna and G_o means that the adversary node is using omnidirectional antenna.

Note that both the receiver and the adversary nodes have the same minimum SINR (i.e., β) to decode the information to the transmitter. Figures 2 and 3 illustrate the exposure

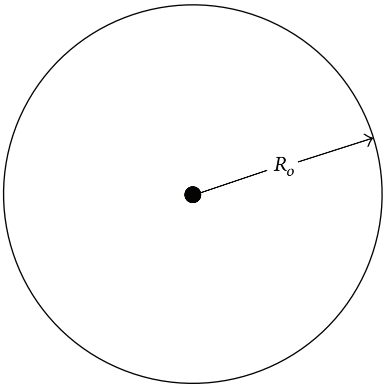


Figure 2: The exposure region of an omnidirectional antenna.

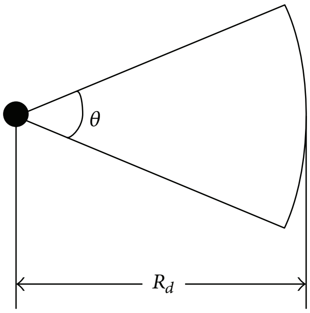


Figure 3: The exposure region of a directional antenna.

regions of a directional antenna and an omnidirectional antenna, respectively.

We then define the *eavesdropping condition* as follows.

Definition 2 (eavesdropping condition). An adversary node can successfully eavesdrop the information from the transmitter *if and only if the adversary node falls into the exposure region of the transmitter*.

To evaluate the seriousness of eavesdropping attacks, we define the *eavesdropping* probability $p(\mathrm{e})$ of a WSN in single-hop networks and multihop networks, respectively.

Definition 3 (single-hop eavesdropping probability). The eavesdropping probability $p(\mathrm{e})$ equals the probability that at least one adversary node falls into the exposure region of the transmitter.

Definition 4 (multihop eavesdropping probability). The eavesdropping probability of a multihop transmission is the probability that at least one-hop transmission is eavesdropped.

It is obvious that $0 \leq p(\mathrm{e}) \leq 1$. In order to compare the eavesdropping attacks at two different types of WSNs, namely, WSN_A and WSN_B, we define the security improvement factor as follows.

Definition 5 (security improvement factor). The security improvement factor $I_{A/B}$ of WSN_A over WSN_B is the ratio of the eavesdropping probability of WSN_A to the eavesdropping probability of WSN_B, that is, $I_{A/B} = p_A(\mathrm{e})/p_B(\mathrm{e})$, where $p_A(\mathrm{e})$ denotes the eavesdropping probability of WSN_A and $p_B(\mathrm{e})$ denotes the eavesdropping probability of WSN_B.

When $I_{A/B} > 1$, it implies that WSN_B has the lower eavesdropping probability than WSN_A, that is, WSN_B is more secure than WSN_A. Similarly, $I_{A/B} < 1$ means that WSN_A is more secure than WSN_B. When $I_{A/B} = 1$, WSN_A has the eavesdropping security equal to that of WSN_B. Note that the definition of Security Improvement Factor applies for both single-hop networks and multihop networks.

Finally, we describe the node distribution. In this paper, we consider that both the adversary nodes and the good nodes are distributed in a two-dimensional plane. We use a Poisson point process to model the distribution of the nodes [14]. In particular, the probability $p(i)$ of finding i nodes in an area of S is given by

$$p(i) = f(i, S) = \frac{(\rho S)^i}{i!} e^{-\rho S}, \tag{10}$$

where $f(i, S)$ is the probability mass function and ρ is the node density.

3. Security Analysis on Single-Hop Networks

In this section, we analyze the eavesdropping probabilities of Omnidirectional case and Directional case in single-hop networks, in which all packets are transmitted through only one hop.

3.1. Eavesdropping Probability of WSNs. Generally, the eavesdropping probability of a single-hop WSN can be obtained by the following lemma.

Lemma 6. *The eavesdropping probability can be calculated by*

$$p(\mathrm{e}) = 1 - e^{-\rho \cdot S}. \tag{11}$$

Proof. From the definition of the eavesdropping probability, that is, Definition 3, we have

$$\begin{aligned} p(\mathrm{e}) &= p(i \geq 1) \\ &= 1 - p(i < 1) = 1 - p(i = 0), \end{aligned} \tag{12}$$

where i denotes the number of adversary nodes falling into the exposure region of a transmitter. □

Since the distribution of adversary nodes follows Poisson point process as defined in (10), we then have

$$p(\mathrm{e}) = 1 - e^{-\rho \cdot S}. \tag{13}$$

As shown in Lemma 6, to determine the eavesdropping probability, we need to calculate the area of the exposure region S first. We then calculate the exposure region S under the Omnidirectional case (*WONs*) and the Directional case (*DAWNs*), respectively.

In Omnidirectional case, the transmitter, the receiver, and the adversary nodes are equipped with omnidirectional antennas. The exposure region of an omnidirectional antenna is a circle with radius R_o, as shown in Figure 2. The area of the exposure region can be calculated by

$$S_o = \pi \cdot R_o^2, \tag{14}$$

where R_o can be obtained by (8).

In Directional case, the transmitter is equipped with a directional antenna while eavesdroppers are equipped with omnidirectional antennas. The exposure region of a directional antenna is a sector with radius R_d and angle θ, as shown in Figure 3. The area of the exposure region can be calculated by

$$S_d = \frac{\theta}{2\pi} \cdot \pi \cdot R_d^2, \tag{15}$$

where R_d can be obtained by (9).

After replacing S in (11) by S_o (defined in (14)) and S_d (defined in (15)), respectively, we obtain the eavesdropping probability of the Omnidirectional case and the eavesdropping probability of the Directional case, which are given as the following lemma.

Lemma 7. *The eavesdropping probability of the Omnidirectional case, denoted by P_o, can be calculated by*

$$p_o(e) = 1 - e^{-\rho \cdot S_o}. \tag{16}$$

The eavesdropping probability of the Directional case, denoted by P_d, can be calculated by

$$p_d(e) = 1 - e^{-\rho \cdot S_d}. \tag{17}$$

3.2. Comparison between WONs and DAWNs under 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 Omnidirectional case, as follows:

$$N_o = \rho \cdot S_o = \rho \cdot \pi \cdot R_o^2. \tag{18}$$

We then have the following theorem to compare a *WON* with a *DAWN* in terms of the security improvement factor.

Theorem 8. *The security improvement factor of a WON over a DAWN is equal to*

$$I_{o/d} = \frac{1 - e^{-N_o}}{1 - e^{-N_o \cdot (\theta/2\pi)^{1-(2/\alpha)}}}. \tag{19}$$

Proof. From the definition of security improvement factor, that is, Definition 5, we have

$$I_{o/d} = \frac{p_o(e)}{p_d(e)}, \tag{20}$$

where $p_o(e)$ and $p_d(e)$ denote the eavesdropping probabilities of a *WON* and a *DAWN*, respectively.

Replacing $p_o(e)$ and $p_d(e)$ in (20) by RHS of (16) and RHS of (17), respectively, we have

$$\begin{aligned} I_{o/d} &= \frac{p_o(e)}{p_d(e)} \\ &= \frac{1 - e^{-\rho \cdot \pi \cdot R_o^2}}{1 - e^{-\rho \cdot \pi \cdot R_d^2 \cdot (\theta/2\pi)}} \\ &= \frac{1 - e^{-N_o}}{1 - e^{-N_o \cdot (\theta/2\pi)^{1-(2/\alpha)}}}. \end{aligned} \tag{21}$$

□

We then analyze the security improvement factor of a *WON* over a *DAWN*. In particular, we have the following.

Corollary 9. *DAWNs have the eavesdropping probability no higher than that of WONs under the same network settings. More precisely, one has the following.*

(i) *When the pass loss factor $\alpha = 2$, $I_{o/d} = 1$, no matter what θ and N_o are, it implies that a DAWN has the same eavesdropping probability as a WON.*

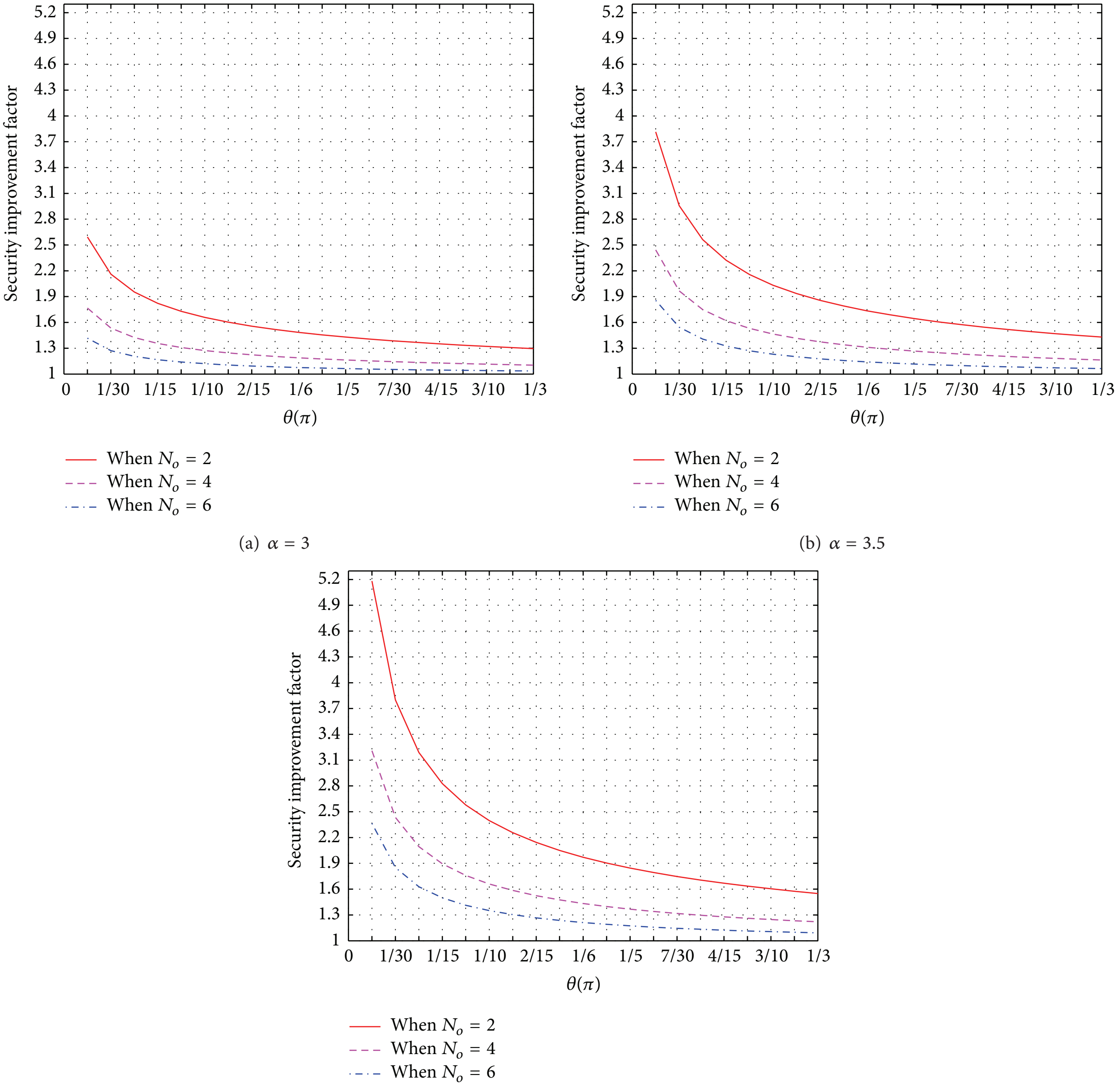
(ii) *When the pass loss factor $\alpha > 2$, $I_{o/d} > 1$, it implies that a DAWN has higher eavesdropping probability than a WON.*

We then calculate the security improvement factor $I_{o/d}$ with varied beamwidth θ, node density N_o, and path loss factor α. Figure 4 illustrates the security improvement factor of single-hop transmissions.

It is shown in Figures 4(a), 4(b), and 4(c) that the security improvement factor $I_{o/d}$ is always greater than 1 when $\alpha > 2$. In other words, using directional antennas in such environments can always reduce the eavesdropping probability and improve the network security. Figure 4 also shows that the security improvement factor $I_{o/d}$ increases when the path loss factor α increases. Therefore, using directional antennas in higher path-loss environments may improve the network security further.

Besides, it is also shown in Figure 4 that with the increased node density N_o, the security improvement factor $I_{o/d}$ decreases. This is because more adversary nodes fall into the exposure region with the increased node density. Therefore, from the adversary point of view, the best way to improve the success rate of eavesdropping attacks is to distribute more adversary nodes in the whole network.

Moreover, Figure 4 also shows that the security improvement factor $I_{o/d}$ increases with the decreased antenna beamwidth θ. In other words, the narrower antenna beamwidth leads to the higher security improvement. For example, in Figure 4(c), $I_{o/d} = 2.83$ when $\alpha = 4$, $N_o = 2$, and $\theta = \pi/15$ (i.e., 12°). Thus, in a network distributed with dense adversary nodes, we should use narrow-beam antennas to avoid eavesdropping.



(a) $\alpha = 3$

(b) $\alpha = 3.5$

(c) $\alpha = 4$

Figure 4: Security improvement factor of single-hop transmissions.

4. Security Analysis on Multihop Networks

In this section, we extend our analysis from single-hop networks to multihop networks. We first derive the eavesdropping probability of multihop transmissions. Then, we analyze the security improvement factor of *WONs* over *DAWNs* under multihop networks.

4.1. Routing Path in Multihop Networks. To analyze the eavesdropping probability of multihop transmissions, we construct a simple routing scheme that chooses a route with the shortest distance to forward data packets. We first introduce the Source-Destination (S-D) Line model [3, 15].

In the S-D Line model, we divide the unit-area plane into a lot of equal-sized square cells as shown in Figure 5. Each of them has an identical area of $a(n)$. The size of the cell, $a(n)$ should be greater enough to ensure that there is at least one node in each cell. It is the necessary condition to ensure that the network is connected.

In this S-D Line model, we directly draw a line to connect a source node S and its destination node D. Then, node S will send data packets to its destination D by multihop forwarding those packets along the cells lying on its S-D line. Figure 5 shows an example of S-D lines, where the green line indicates a S-D Line. In the case of *WONs*, the packets are forwarded along the *adjacent* cells lying on the S-D line. For example,

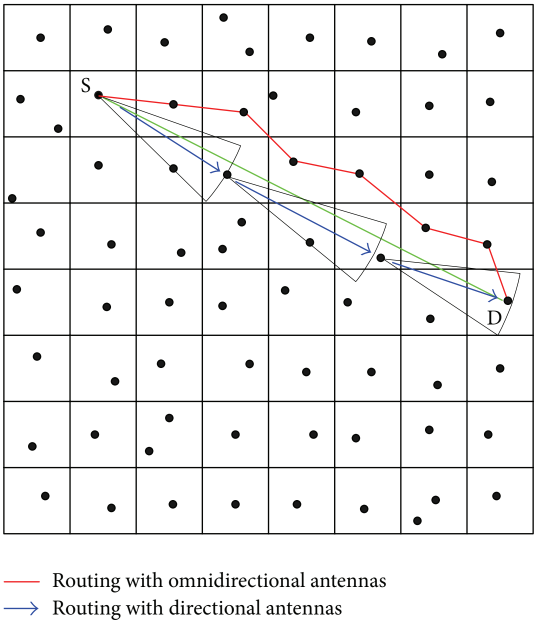

S
D
Routing with omnidirectional antennas
Routing with directional antennas

Figure 5: The S-D Line model.

the red line as shown in Figure 5 denotes the routing path from S to D in a *WON*. However, the cells lying on the S-D line in a *DAWN* are not necessary to be adjacent since a directional antenna has a longer transmission range than an omnidirectional antenna. As shown in Figure 5, only 3 hops are needed from S to D, compared with the omnidirectional antenna case, which requires 7 hops from S to D. Therefore, using directional antennas can potentially reduce the number of hops.

We then calculate the number of hops required to route a packet from S to D. Since calculating the exact number of hops is difficult, we are only concerned about the number of hops H from S to D. In the S-D line model, the number of hops depends on both the length of the S-D line l and the transmission range of each hop, which is R_o in a *WON* and is R_d in a *DAWN*.

We next calculate the number of hops H_o of a *WON*, which is bounded by

$$H_o = \left[\frac{l}{R_o} \right], \tag{22}$$

where $[\cdot]$ denotes the near integer function and R_o is the maximum transmission range of an omnidirectional antenna, which can be calculated from (8).

Similarly, the number of hops H_d of a *DAWN* is bounded by

$$H_d = \left[\frac{l}{R_d} \right], \tag{23}$$

where R_d is the maximum transmission range of a directional antenna, which can be calculated from (9).

4.2. Eavesdropping Probability of Multihop Networks. In general, the eavesdropping probability of a multihop WSN (either *WON* or *DAWN*) can be obtained by the following lemma.

Lemma 10. *The eavesdropping probability of multihop networks can be calculated by*

$$p_m(\mathrm{e}) = 1 - (1 - p(\mathrm{e}))^H, \tag{24}$$

where H is the number of hops and $p(\mathrm{e})$ is the eavesdropping probability of a single-hop transmission, which can be calculated by Lemma 6.

Proof. From the definition of the eavesdropping probability of multihop networks, that is, Definition 4, we have

$$p_m(\mathrm{e}) = 1 - (1 - p(\mathrm{e}))^H. \tag{25}$$

Note that we assume that each hop has the same eavesdropping probability. □

For a *WON*, since $p(\mathrm{e}) = p_o(\mathrm{e})$, which can be calculated from (16) and the number of hops $H = H_o$, which can be calculated from (22). Therefore, we have the eavesdropping probability of a *WON* denoted by p_{mo}

$$p_{mo}(\mathrm{e}) = 1 - (1 - p_o(\mathrm{e}))^{H_o}. \tag{26}$$

For a *DAWN*, since $p(\mathrm{e}) = p_d(\mathrm{e})$, which can be calculated from (17) and the number of hops $H = H_d$, which can be calculated from (23), we have the eavesdropping probability of a *DAWN* denoted by p_{md}

$$p_{md}(\mathrm{e}) = 1 - (1 - p_d(\mathrm{e}))^{H_d}. \tag{27}$$

From (24), we have found that with the increased number of hops H, the multihop eavesdropping probability also significantly increases. Since directional antennas have a longer transmission range than omnidirectional antennas, that is, $R_d > R_o$, the number of required hops for directional antennas is smaller than that for omnidirectional antennas. Therefore, using directional antennas in multihop networks can potentially reduce the multihop eavesdropping probability, which will be verified in Section 5.

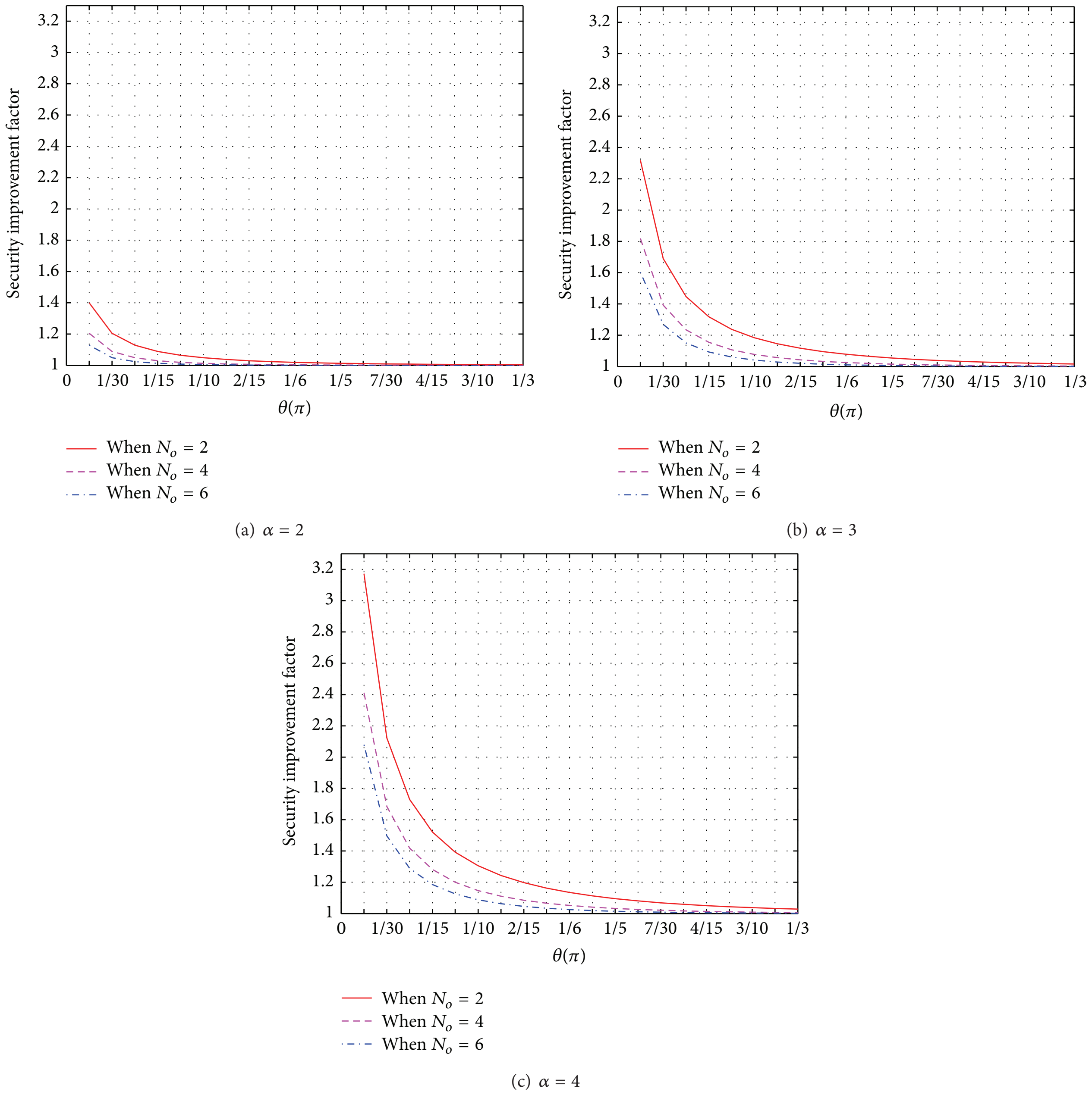
4.3. Comparison between WONs and DAWNs under Multihop Networks. We then have the following theorem to compare a *WON* with a *DAWN* in terms of the security improvement factor under multihop networks.

Theorem 11. *The security improvement factor of a WON over a DAWN under multihop networks is equal to*

$$I_{o/d}^{m} = \frac{1 - (1 - p_o(\mathrm{e}))^{H_o}}{1 - (1 - p_d(\mathrm{e}))^{H_d}}. \tag{28}$$

Proof. From the definition of security improvement factor, that is, Definition 5, we have

$$I_{o/d}^{m} = \frac{p_{mo}(\mathrm{e})}{p_{md}(\mathrm{e})}. \tag{29}$$



(a) $\alpha = 2$

(b) $\alpha = 3$

(c) $\alpha = 4$

Figure 6: The security improvement factor of multihop transmissions.

After replacing p_{mo} and p_{md} of (28) by RHS of (26) and RHS of (27), we have

$$I_{o/d}^{m} = \frac{1-\left(1-p_o\left(\mathrm{e}\right)\right)^{H_o}}{1-\left(1-p_d\left(\mathrm{e}\right)\right)^{H_d}}. \tag{30}$$

□

Note that when $H_o = 1$ and $H_d = 1$, $I_{o/d}^{m} = p_o(\mathrm{e})/p_d(\mathrm{e})$, which is equal to $I_{o/d}$, given by (19). Thus, the security improvement factor $I_{o/d}$ under the single-hop networks can be regarded as a special case of the multihop networks.

We then calculate $I_{o/d}^{m}$ with varied beamwidth θ, node density N_o, and path loss factor α. Figure 6 illustrates security improvement factor $I_{o/d}^{m}$. It is shown in Figure 6 that the security improvement factor $I_{o/d}^{m}$ decreases when the node density N_o increases (e.g., N_o increases from 2 to 6). This is because, when the node density N_o increases, more adversary nodes fall into the exposure region, which results in higher eavesdropping probability. Similar to single-hop networks, the security improvement factor of multihop transmissions $I_{o/d}^{m}$ also significantly increases with the decreased antenna beamwidth θ. In other words, the narrower antenna beamwidth θ is, the higher security improvement $I_{o/d}^{m}$ is.

Two factors contribute to the increment of the security improvement of multihop transmissions: (i) the smaller exposure region with narrower beamwidth θ leads to the less eavesdropping probability of single-hop transmissions; (ii) the narrower beamwidth θ is, the higher antenna gain is (refer to (1)), which also results in the longer transmission range R_d and consequently leads to the less eavesdropping probability of multihop transmissions $p_{md}(\mathrm{e})$.

Moreover, it is also shown in Figure 6 that there is a higher multihop security improvement factor $I_{o/d}^{m}$ in a higher path-loss environment (e.g., $\alpha = 4$) than that in a lower path-loss environment (e.g., $\alpha = 3$). Using directional antennas in such environments may bring more benefits.

In addition, different from the single-hop networks, the security improvement $I_{o/d}^{m}$ under the multihop networks is always greater than 1 even when the path loss factor $\alpha = 2$ (note that $I_{o/d} = 1$ when $\alpha = 2$ under the single-hop networks as shown in Corollary 9). This mainly owes to the reduced number of hops by using directional antennas. Our analytical results imply that multihop networks with directional antennas are generally more secure than multihop networks with omnidirectional antennas.

5. Empirical Results

In this section, we conduct extensive simulations to evaluate the correctness and the accuracy of our proposed models in single-hop networks (Section 5.1) and multihop networks (Section 5.2). In the simulations, both adversary nodes and good nodes are randomly distributed on a plane of area $l \times l\,\mathrm{m}^2$. To eliminate the border effects, we use the sub-area approach [16]. Specifically, we only compute the eavesdropping probability of the nodes within an inner square of area $l' \times l'\,\mathrm{m}^2$, where l' is sufficiently smaller than l. Besides, the simulation results are calculated by averaging over 10000 random topologies in single-hop networks and obtained by averaging over 1000 random topologies in multihop networks.

5.1. Single-Hop Networks. Figure 7 shows the eavesdropping probability versus node density when $\alpha = 3$ (Figure 7(a)) and $\alpha = 4$ (Figure 7(b)). Note that the analytical results are represented in curves (ana) and the simulation results are indicated by markers (sim) in Figure 7. Besides, each simulation result is calculated by averaging over 10000 random topologies.

As shown in Figures 7(a) and 7(b), the simulation results almost exactly match the analytical results in all cases. Besides, it is shown in Figures 7(a) and 7(b) that the eavesdropping probability increases when N_o increases. This is because, when N_o increases, the more adversary nodes fall into the exposure regions, leading to the higher eavesdropping probability (the networks become the less secure).

Moreover, we can see in Figure 7 that a *DAWN* always has the lower eavesdropping probability than a *WON* in all cases, which further confirms our earlier observations in Section 3. In other words, using directional antennas in wireless networks can potentially improve the security. In addition, when α is fixed, we can see that the eavesdropping probability decreases with the increased beamwidth θ. It implies that a narrower-beam antenna can potentially reduce the eavesdropping probability and further improve the security of transmissions.

Furthermore, we can also see that the eavesdropping probability of a *DAWN* significantly drops with the increased path loss factor α (e.g., α increases from 3 in Figure 7(a) to 4 in Figure 7(b)) while α just slightly affects the eavesdropping probability of a *WON*. It is shown in [13] that the path loss factor α is generally greater than 3 in urban outdoor environments. Therefore, using directional antennas in such environments may bring more benefits on reducing the eavesdropping probability than using omnidirectional antennas.

5.2. Multihop Networks. Tables 2 and 3 show the eavesdropping probabilities under multihop networks when $\alpha = 3$ and $\alpha = 4$, respectively. Note that we choose lower density N_o (i.e., ranging from 0.05 to 0.5) in both Tables 2 and 3. The main reason lies in the higher eavesdropping probability under multihop networks than that under single-hop networks (it is obvious that the whole transmission is eavesdropped once one-hop transmission is eavesdropped). Besides, we choose $l = 1200$ m in Table 2 and $l = 400$ m in Table 3. This is because we have to limit the number of hops when $\alpha = 4$ in order to avoid that the eavesdropping probability reaches one too fast. More specifically, when $\alpha = 4$, both R_d and R_o drop significantly, resulting in the increased number of hops (recall that H_d and H_o depend on R_d and R_o) and consequently leading to the severely increased eavesdropping probability. Furthermore, to obtain the proper routing path, which approximates that derived under the S-D Line model (Section 4), we first choose a source-destination node pair, which spans nearly the dimension of the network (i.e., $\approx l$). Then we obtain the shortest routing path based on the Dijkstra's algorithm [17]. Note that each of our simulation results is calculated by averaging over 1000 random topologies. (Note that it is extremely time consuming to obtain the multihop result for each random topology.)

Both Tables 2 and 3 show that a *WON* has much higher eavesdropping probability than a *DAWN* when $\alpha = 3$ and $\alpha = 4$. Besides, the eavesdropping probability of a *WON* goes more quickly to reach one than that of a *DAWN*. The reason behind this phenomenon lies the higher single-hop eavesdropping probability of a *WON* than that of a *DAWN*.

As shown in Tables 2 and 3, the eavesdropping probability $p_{mo}(\mathrm{e})$ of a *WON* and the eavesdropping probability $p_{md}(\mathrm{e})$ of a *DAWN* increase significantly with the increased node density. This agrees with our observation that the higher N_o is, the more adversary nodes fall into the exposure regions, which results in the higher single-hop eavesdropping probability, either $p_o(\mathrm{e})$ or $p_d(\mathrm{e})$. As a result, the multihop eavesdropping probabilities $p_{mo}(\mathrm{e})$ and $p_{md}(\mathrm{e})$ increase.

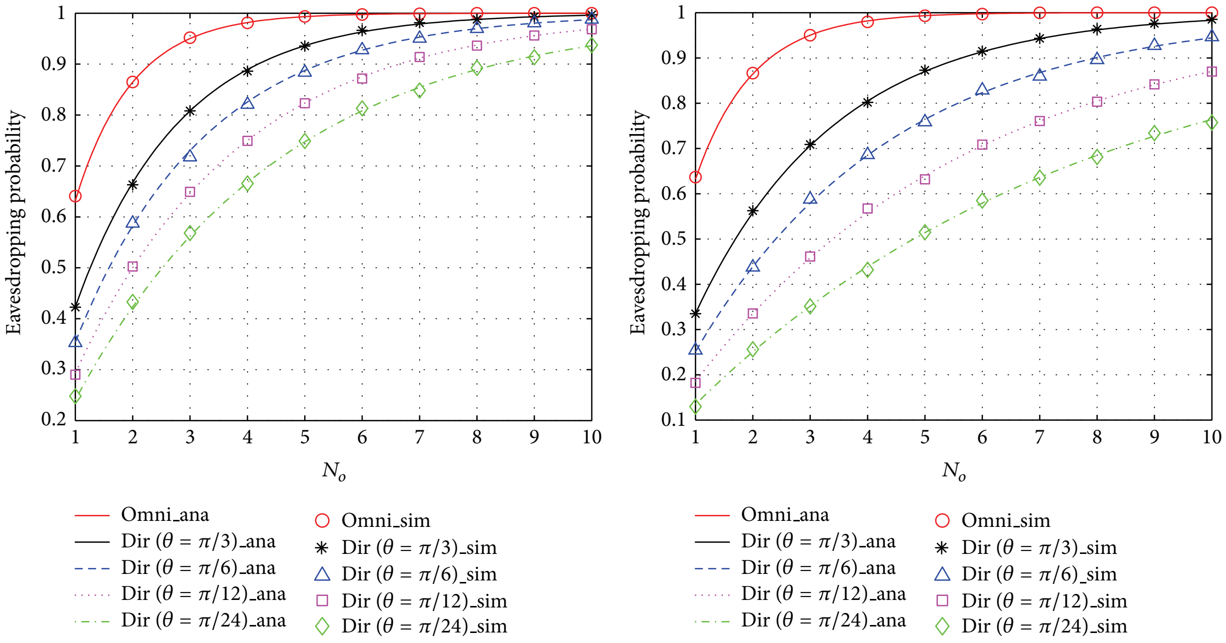
Besides, Tables 2 and 3 also show that the narrower the beamwidth θ is, the smaller the eavesdropping probability $p_{md}(\mathrm{e})$ is. For example, $p_{md}(\mathrm{e}) = 0.544$ (simulation) with beamwidth $\theta = \pi/12$ is much smaller than $p_{md}(\mathrm{e}) = 0.714$ (simulation) with beamwidth $\theta = \pi/6$ with the node density $N_o = 0.20$ and the path loss factor $\alpha = 3$. This mainly owes to the two factors described in Section 4. Moreover, it is also shown in Tables 2 and 3 that $p_{md}(\mathrm{e})$ decreases when the path loss factor α increases. Therefore, using directional antennas in such high path loss environments may gain more security improvement.

Table 2: Eavesdropping probability versus node density N_o when $\alpha = 3$.

N_o	$p_{mo}(\mathrm{e})$		$p_{md}(\mathrm{e})$ $(\theta = \pi/3)$		$p_{md}(\mathrm{e})$ $(\theta = \pi/6)$		$p_{md}(\mathrm{e})$ $(\theta = \pi/12)$	
	Analytical	Simulation	Analytical	Simulation	Analytical	Simulation	Analytical	Simulation
0.05	0.727	0.624	0.338	0.360	0.231	0.255	0.144	0.187
0.10	0.925	0.851	0.562	0.605	0.408	0.444	0.268	0.346
0.15	0.979	0.944	0.710	0.751	0.544	0.589	0.374	0.439
0.20	0.994	0.988	0.808	0.866	0.649	0.714	0.464	0.544
0.25	0.998	0.989	0.873	0.915	0.730	0.790	0.542	0.607
0.30	0.999	0.996	0.916	0.943	0.792	0.835	0.608	0.685
0.35	0.999	0.996	0.944	0.953	0.840	0.890	0.664	0.746
0.40	0.999	0.999	0.963	0.973	0.877	0.884	0.713	0.818
0.45	0.999	0.998	0.976	0.990	0.905	0.928	0.754	0.829
0.50	0.999	0.999	0.984	0.990	0.927	0.941	0.790	0.863

Table 3: Eavesdropping probability versus node density N_o when $\alpha = 4$.

N_o	$p_{mo}(\mathrm{e})$		$p_{md}(\mathrm{e})$ $(\theta = \pi/3)$		$p_{md}(\mathrm{e})$ $(\theta = \pi/6)$		$p_{md}(\mathrm{e})$ $(\theta = \pi/12)$	
	Analytical	Simulation	Analytical	Simulation	Analytical	Simulation	Analytical	Simulation
0.05	0.683	0.570	0.264	0.300	0.171	0.176	0.106	0.120
0.10	0.899	0.801	0.458	0.488	0.313	0.374	0.201	0.236
0.15	0.968	0.903	0.601	0.663	0.431	0.482	0.286	0.305
0.20	0.989	0.963	0.706	0.756	0.528	0.554	0.362	0.399
0.25	0.996	0.980	0.784	0.818	0.609	0.655	0.430	0.483
0.30	0.998	0.993	0.841	0.878	0.676	0.712	0.490	0.554
0.35	0.999	0.999	0.883	0.909	0.731	0.766	0.544	0.604
0.40	0.999	0.999	0.913	0.933	0.777	0.820	0.593	0.651
0.45	0.999	0.999	0.936	0.959	0.815	0.828	0.636	0.671
0.50	0.999	0.999	0.953	0.961	0.847	0.873	0.674	0.752



(a) $\alpha = 3$

(b) $\alpha = 4$

Figure 7: Eavesdropping probability versus node density N_o, averaged over 10000 random-generated topologies with $l = 1200$ m (curves = analytical results and markers = simulation results), where omni and dir represent *DAWNs* and *WONs*, respectively.

There exist quite small gaps between the analytical values and the simulation results as shown in Tables 2 and 3 though both of them have the same trend. More precisely, as shown in Tables 2 and 3 that the analytical values are always greater than the simulation results in a *WON* while the analytical values are always smaller than the simulation results in a *DAWN*. This effect may owe to two factors: (1) the number of hops in simulations is often greater than that in analysis; (2) there are some overlapping regions counted in each hop when we conduct simulations. It is obvious that Factor (1) will lead to the higher simulation results than the analytical values while Factor (2) will lead to the lower simulation results than the analytical values. In a *WON*, Factor (2) dominates Factor (1) since the overlapping ratio of the circular region is very high. As a result, the analytical value is always slightly greater than the simulation result. On the contrary, in a *DAWN*, Factor (1) dominates Factor (2), consequently leading to the higher simulation result than the analytical value. A more precise analytical model for multihop networks is expected to be proposed in the future while it is beyond the scope of this paper.

6. Related Work

Wireless Sensor Networks (WSNs) are prone to the malicious attacks due to the shared wireless medium, the multihop transmissions, and the decentralized control scheme [2, 18–20]. In a WSN, any wireless node residing in the *transmission* range of the transmitter can potentially decode the signal when both the transmitter and the receiver are unaware of the *reconnaissance*. Besides, it is also difficult to implement the centralized control mechanisms in WSNs. Furthermore, multihop communications are also suggested in WSNs to reduce the interference and to improve the network capacity [21]. However, the multihop communication is vulnerable to the malicious attacks.

One of the malicious attacks, namely, the *eavesdropping* attack, has attracted considerable attentions recently since many other malicious attacks often follow the eavesdropping activity. As summarized in [4, 18], there are two types of eavesdropping attacks in WSNs: passive eavesdropping and active eavesdropping. The study on the passive eavesdropping attacks is often more important than that on the active eavesdropping attacks since it is a prerequisite that the malicious nodes have the knowledge of the good nodes via conducting passive eavesdropping activities.

There are a number of studies on investigating the passive eavesdropping attack [2–4, 18]. But, most of them considered a *WON*, in which each node is equipped with an *omnidirectional* antenna, which radiates the radio signals in all directions and consequently is more prone to the eavesdropping attacks. Compared with omnidirectional antennas, directional antennas can concentrate radio signals on desired directions. In other undesired directions, there are no radio signals or weakened signals. Thus, using directional antennas in WSNs can potentially reduce the interference and consequently improve the network performance.

There are a number of studies on using directional antennas in wireless ad hoc networks. The first category of them mainly focuses on the theoretical analysis on the network performance, for example, the network capacity and the transmission delay. In particular, studies [6, 22, 23] derived the approximated network capacity of wireless networks with directional antennas, in which each node is equipped with only one directional antenna and only one channel is used. More specifically, Yi et al. [6] show that using directional antenna in arbitrary networks achieves a capacity gain of $2\pi/\sqrt{\alpha\beta}$ when both the transmitter and the receiver are equipped with directional antennas, where α and β are transmitter and receiver antenna beamwidth, respectively. Under random networks (in which n nodes are randomly placed, directional antennas of each node are randomly adjusted, and the destination of a flow is also randomly chosen), the throughput improvement factor is $4\pi^2/\alpha\beta$ when both the transmitter and the receiver are equipped with directional antennas. Other studies [10, 11] are focused on multi-channel and multi-interface networks with directional antennas, which are proved to have a higher network capacity than that single-channel networks with directional antennas. Besides, the study [24] shows that the transmission delay in wireless networks with directional antennas due to multihop transmissions can be significantly reduced due to the longer transmission range of directional antennas. The second category of studies focus on improving the network performance in Medium Access Control (MAC) layer [8, 12, 25–37]. In particular, using directional antennas in wireless networks often results in the new hidden terminal problem and the deafness problem, which were first addressed in [28]. Both the new hidden terminal problem and the deafness problem severely degrade the network performance. Therefore, a number of studies were proposed to address them [8, 30–32, 34, 35]. However, many of these solutions only solve either the new hidden terminal problem or the deafness problem but not both. Besides, many of them often have additional overheads due to sending additional control packets. For example, circular DMAC [8] needs transmitting multiple RTS frames for each data packet.

Most of the above studies focus on improving the network performance by using directional antennas. However, there is little work on the security issue by using directional antennas. The study [38] is one of the earliest studies on exploring using directional antennas in wireless networks to improve the network security. It is shown in [38] that using directional antennas can significantly reduce the average detection probability compared with using omnidirectional antennas. However, their studies only analyze single-hop multihop transmission and do not consider other benefits of directional antennas, such as the longer transmission range, which may reduce the number of hops and consequently improve the security further.

7. Conclusion

In this paper, we have explored using directional antennas in wireless sensor networks to improve the network security in terms of reducing the eavesdropping probability. In particular, we analyzed the eavesdropping probability of single-hop networks and that of multihop networks. We have found that using directional antennas in either a single-hop network or a multihop network can significantly reduce the eavesdropping probability. The security improvements of using directional antennas owe to the *smaller exposure region* and the *fewer hops* due to the longer transmission range. Besides, we also derived the security improvement factors of single-hop transmissions and multihop transmissions. We have found that both the single-hop security improvement factor and the multihop security improvement factor heavily depend on the antenna beamwidth, the node density, and the path loss factor. It is shown that using a narrow beam antenna can significantly improve the network security by reducing the eavesdropping probability.

There are some interesting topics in the eavesdropping activities of *DAWNs*. For example, most of current studies always assume that the adversary nodes are uniformly and randomly distributed in the networks. What about the eavesdropping probability if the distribution of the adversary nodes is non-uniform and deliberate? Besides, does the power control schemes will affect the eavesdropping probability of a *DAWN*?

Notations

G_t:	Antenna gain of transmitters
G_r:	Antenna gain of receivers
G_d:	Directional antenna gain
G_o:	Omnidirectional antenna gain
θ:	Antenna beamwidth, that is, the angle between the half-power points of the main lobe
γ_{ij}:	The channel gain from node i to node j
P_t:	Fixed transmission power of all nodes
SINR:	Signal-to-Interference-Plus-Noise Ratio
α:	Signal path loss factor
β:	Minimum signal to interference and noise ratio
η:	Fixed environmental noise power level
R_d:	Maximum radius of the exposure region of directional antennas
R_o:	Maximum radius of the exposure region of omnidirectional antennas
ρ:	Node density
N_o:	The average number of nodes in a circle with radius R_o (the reference node density)
$p(\mathrm{e})$:	Single-hop eavesdropping probability
$p_d(\mathrm{e})$:	Single-hop eavesdropping probability of a directional antenna
$p_o(\mathrm{e})$:	Single-hop eavesdropping probability of an omnidirectional antenna
$p_m(\mathrm{e})$:	Multihop eavesdropping probability
$p_{md}(\mathrm{e})$:	Multihop eavesdropping probability of a directional antenna
$p_{mo}(\mathrm{e})$:	Multihop eavesdropping probability of an omnidirectional antenna
$I_{A/B}$:	The security improvement factor of WSN$_A$ over WSN$_B$.

Acknowledgments

The work described in this paper was supported by Macao Science and Technology Development Fund under Grant no. 036/2011/A and Grant no. 081/2012/A3. The authors would like to thank Guodong Han and Qinglin Zhao for their valuable comments.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] F. Anjum and P. Mouchtaris, *Security for Wireless Ad Hoc Networks*, Wiley-Interscience, New York, NY, USA, 1st edition, 2007.

[3] J. C. Kao and R. Marculescu, "Eavesdropping minimization via transmission power control in Ad-Hoc wireless networks," in *Proceedings of the 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (SECON '06)*, pp. 707–714, Reston, Va, USA, September 2006.

[4] M. Anand, Z. G. Ivesy, and I. Leez, "Quantifying eavesdropping vulnerability in sensor networks," in *Proceedings of the 2nd International Workshop on Data Management for Sensor Networks (DMSN '05)*, pp. 3–9, 2005.

[5] X. Huang, J. Wang, and Y. Fang, "Achieving maximum flow in interference-aware wireless sensor networks with smart antennas," *Ad Hoc Networks*, vol. 5, no. 6, pp. 885–896, 2007.

[6] S. Yi, Y. Pei, and S. Kalyanaraman, "On the capacity improvement of Ad Hoc wireless networks using directional antennas," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03)*, pp. 108–116, 2003.

[7] L. Bao and J. J. Garcia-Luna-Aceves, "Transmission scheduling in Ad Hoc networks with directional antennas," in *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom '02)*, pp. 48–58, September 2002.

[8] T. Korakis, G. Jakllari, and L. Tassiulas, "A MAC protocol for full exploitation of directional antennas in ad-hoc wireless networks," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03)*, pp. 98–107, June 2003.

[9] Z. Zhang, "Pure directional transmission and reception algorithms in wireless Ad Hoc networks with directional antennas," in *Proceedings of the IEEE International Conference on Communications (ICC '05)*, vol. 5, pp. 3386–3390, Seoul, Republic of Korea, May 2005.

[10] 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 *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 1301–1309, Phoenix, Ariz, USA, April 2008.

[11] J. Zhang and X. Jia, "Capacity analysis of wireless mesh networks with omni or directional antennas," in *Proceedings of the IEEE INFOCOM*, pp. 2881–2885, Rio de Janeiro, Brazil, April 2009.

[12] R. Ramanathan, "On the performance of Ad Hoc networks with beamforming antennas," in *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '01)*, pp. 95–105, Long Beach, Calif, USA, 2001.

[13] T. S. Rappaport, *Wireless Communications: Principles and Practice*, Prentice Hall, Upper Saddle River, NJ, USA, 2nd edition, 2002.

[14] Y. Wang and J. J. Garcia-Luna-Aceves, "Directional collision avoidance in Ad Hoc networks," *Performance Evaluation*, vol. 58, no. 2-3, pp. 215–241, 2004.

[15] A. El Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Throughput-delay trade-off in energy constrained wireless networks," in *Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04)*, March 2004.

[16] C. Bettstetter, "On the connectivity of Ad Hoc networks," *Computer Journal*, vol. 47, no. 4, pp. 432–447, 2004.

[17] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, MIT Press, Boston, Mass, USA, 3rd edition, 2009.

[18] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 167575, 7 pages, 2013.

[19] N. A. Alrajeh, S. Khan, J. Lloret, and J. Loo, "Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 374796, 11 pages, 2013.

[20] N. Meghanathan, "A survey on the communication protocols and security in cognitive radio networks," *International Journal of Communication Networks and Information Security*, vol. 5, pp. 19–38, 2013.

[21] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, 2000.

[22] A. Spyropoulos and C. S. Raghavendra, "Capacity bounds for Ad-Hoc networks using directional antennas," in *Proceedings of the IEEE International Conference on Communications (ICC '03)*, pp. 348–352, May 2003.

[23] J. Zhang and S. C. Liew, "Capacity improvement of wireless Ad Hoc networks with directional antennae," *Mobile Computing and Communications Review*, vol. 10, no. 4, pp. 17–19, 2006.

[24] H. N. Dai, "Throughput and delay in wireless sensor networks using directional antennas," in *Proceedings of the 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '09)*, pp. 421–426, Melbourne, Australia, December 2009.

[25] Y. B. Ko, V. Shankarkumar, and N. H. Vaidya, "Medium access control protocols using directional antennas in Ad Hoc networks," in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '00)*, vol. 1, pp. 13–21, Tel Aviv, Israel, March 2000.

[26] A. Nasipuri, S. Ye, J. You, and R. E. Hiromoto, "A MAC protocol for mobile Ad Hoc networks using directional antennas," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '2000)*, vol. 3, pp. 1214–1219, Chicago, Ill, USA, September 2000.

[27] M. Takai, J. Martin, R. Bagrodia, and A. Ren, "Directional virtual carrier sensing for directional antennas in mobile Ad Hoc networks," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '02)*, pp. 183–193, Lausanne, Switzerland, June 2002.

[28] R. R. Choudhury, X. Yang, N. H. Vaidya, and R. Ramanathan, "Using directional antennas for medium access control in Ad Hoc networks," in *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom '02)*, pp. 59–70, Atlanta, Ga, USA, September 2002.

[29] Z. Huang, C. C. Shen, C. Srisathapornphat, and C. Jaikaeo, "A busy-tone based directional MAC protocol for Ad Hoc networks," in *Proceedings of the MILCOM*, vol. 2, pp. 1233–1238, October 2002.

[30] R. R. Choudhury and N. H. Vaidya, "Deafness: a MAC problem in Ad Hoc networks when using directional antennas," in *Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP '04)*, pp. 283–292, October 2004.

[31] H. Gossain, C. Cordeiro, and D. P. Agrawal, "MDA: an efficient directional MAC scheme for wireless Ad Hoc networks," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '05)*, pp. 3633–3637, St. Louis, Mo, USA, December 2005.

[32] H. Gossain, C. Cordeiro, and D. P. Agrawal, "Minimizing the effect of deafness and hidden terminal problem in wireless Ad Hoc networks using directional antennas," *Wireless Communications and Mobile Computing*, vol. 6, no. 7, pp. 917–931, 2006.

[33] M. Takata, M. Bandai, and T. Watanabe, "A receiver-initiated directional MAC protocol for handling deafness in Ad Hoc networks," in *Proceedings of the IEEE International Conference on Communications (ICC '06)*, pp. 4089–4095, Istanbul, Turkey, July 2006.

[34] J. Wang, H. Zhai, P. Li, Y. Fang, and D. Wu, "Directional medium access control for Ad Hoc networks," *Wireless Networks*, vol. 15, no. 8, pp. 1059–1073, 2009.

[35] 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 *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '07)*, pp. 4969–4973, Washington, DC, USA, November 2007.

[36] X. Liu, A. Sheth, M. Kaminsky, K. Papagiannaki, S. Seshan, and P. Steenkiste, "DIRC: increasing indoor wireless capacity using directional antennas," in *Proceedings of the ACM SIGCOMM Conference on Data Communication (SIGCOMM '09)*, pp. 171–182, August 2009.

[37] H. N. Dai, K. W. Ng, and M. Y. Wu, "On busy-tone based MAC protocol for wireless networks with directional antennas," *Wireless Personal Communications*, 2013.

[38] X. Lu, F. Wicker, P. Lio, and D. Towsley, "Security estimation model with directional antennas," in *Proceedings of the IEEE Military Communications Conference (MILCOM '08)*, pp. 1–6, San Diego, Calif, USA, November 2008.

The Scientific World Journal

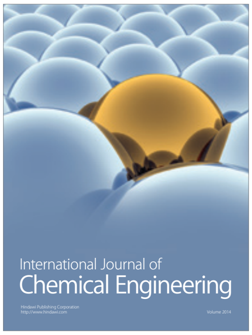
International Journal of
Rotating Machinery

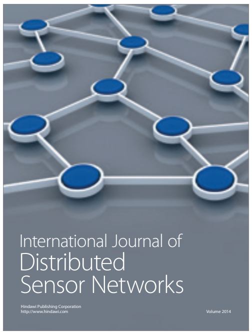
Journal of
Robotics

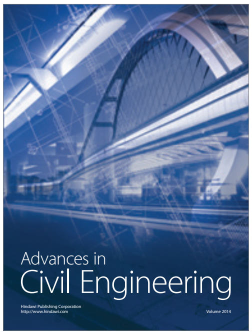
Journal of
Sensors

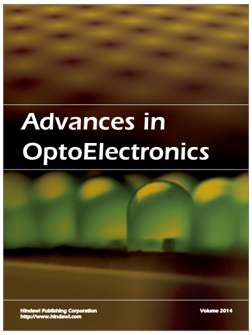
Advances in
Mechanical Engineering

Journal of
Engineering


International Journal of
Chemical Engineering

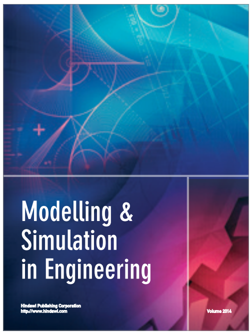

International Journal of
Distributed Sensor Networks

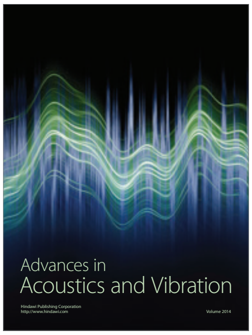

Advances in
Civil Engineering


Advances in
OptoElectronics

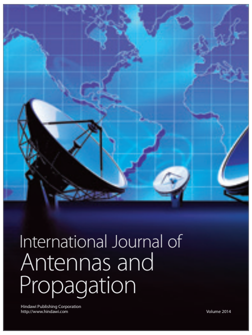
VLSI Design

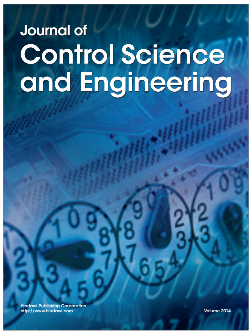
International Journal of
Navigation and Observation

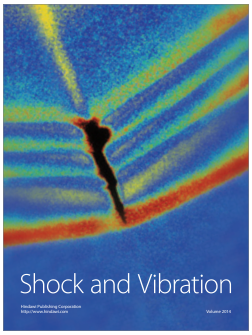

Modelling &
Simulation
in Engineering


Advances in
Acoustics and Vibration

Active and Passive
Electronic Components


International Journal of
Antennas and Propagation


Journal of
Control Science
and Engineering


Shock and Vibration

Journal of
Electrical and Computer
Engineering