Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 4313475, 10 pages
http://dx.doi.org/10.1155/2016/4313475

Hindawi

Research Article

An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things

Xuran Li,[1] Hao Wang,[2] Hong-Ning Dai,[1] Yuanyuan Wang,[1] and Qinglin Zhao[1]

[1]*Faculty of Information Technology, Macau University of Science and Technology, Avenida Wai Long, Room A208, Taipa, Macau*
[2]*Big Data Lab, Faculty of Engineering and Natural Sciences, Norwegian University of Science & Technology, Postboks 1517, 6025 Ålesund, Norway*

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

Received 28 July 2015; Accepted 7 December 2015

Academic Editor: Jong-Hyouk Lee

The security of Internet of Things (IoT) has received extensive attention recently. This paper presents a novel analytical model to investigate the eavesdropping attacks in Wireless Net of Things (WNoT). Our model considers various channel conditions, including the *path loss*, the *shadow fading effect*, and *Rayleigh fading effect*. Besides, we also consider the eavesdroppers in WNoT equipped with either omnidirectional antennas or directional antennas. Extensive simulation results show that our model is accurate and effective to model the eavesdropping attacks in WNoT. Besides, our results also indicate that the probability of eavesdropping attacks heavily depends on the shadow fading effect, the path loss effect, Rayleigh fading effect, and the antenna models. In particular, we find that the shadow fading effect is beneficial to the eavesdropping attacks while both the path loss effect and Rayleigh fading effect are detrimental. Besides, using directional antennas at eavesdroppers can also increase the eavesdropping probability. Our results offer some useful implications on designing antieavesdropping schemes in WNoT.

1. Introduction

As one of the most promising information and communication technologies (ICT), IoT has received extensive attentions from both academia and industry recently. The basic idea of IoT is to integrate "smart" objects, the *things* into the Internet with provision of various services to users [1, 2]. The typical killer applications of IoT include the logistic management with RFID technology [3], environmental monitoring with wireless sensor networks [4], smart homes [5], e-health [6], smart grids [7], Maritime Industry [8], and so forth. There are a number of diverse smart objects ranging from small Radiofrequency Identification (RFID) tags to sensors, actuators, mobile phones, smart appliances, smart meters, and so forth. Due to the device heterogeneity, various wireless communication technologies (such as ISO/IEC 18000 [3], IEEE 802.15.4 [9], and Bluetooth [10]) are also exploited to interconnect the smart devices to form a Wireless Net of Things (WNoT). Note that the conventional wired communication technologies (Ethernets, fiber-optic communication, etc.) are also mandatory to connect the WNoT with the rest of the Internet.

Security is one of the fundamental issues in IoT since it is the prerequisite for most IoT applications [11–14]. There raise a number of security threats in IoT, especially in WNoT, where the conventional security countermeasures used in wired networks may not work well in WNoT due to the following inherent constraints of WNoT: (i) the wireless medium is open for any nodes [15]; (ii) it is extremely difficult to deploy centralized control mechanisms in such distributed WNoT [2, 16, 17]. Eavesdropping attack, as one of typical security threats in wireless communication systems, has attracted considerable attention recently [18–24] since many adversary attacks often follow the eavesdropping activity, for example, the man-in-the-middle attack [25] and the hear-and-fire attack [19].

Figure 1 shows a typical example of eavesdropping attacks in a warehouse environment, where each product is attached with an RFID tag, which can passively communicate with

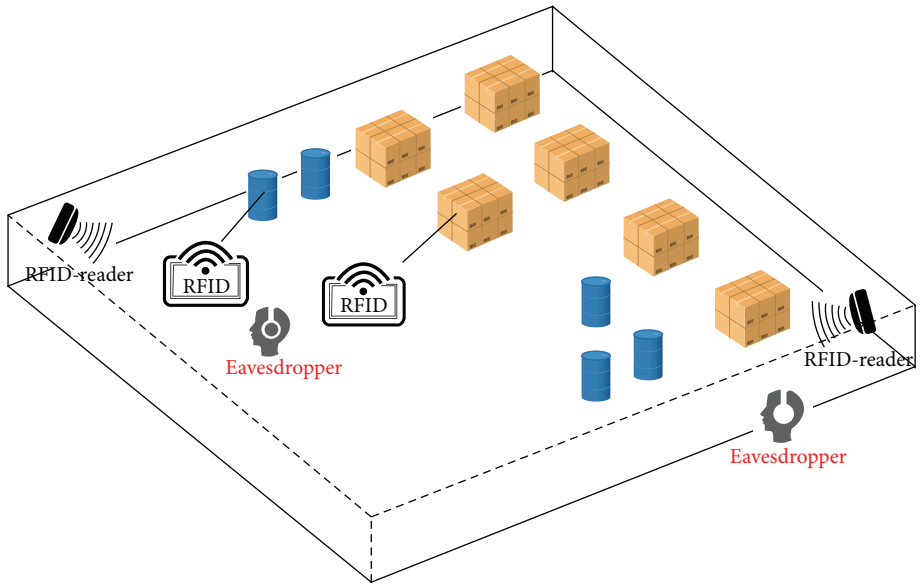

Figure 1: An example of eavesdropping activities in WNoT, where there are several eavesdroppers who are wiretapping the confidential ongoing communications between RFID tags and RFID-readers.

RFID-readers. In this environment, the confidential communications between RFID-readers and RFID tags can be easily wiretapped by eavesdroppers since it is difficult to apply antieavesdropping countermeasures (e.g., encryptions) in this scenario due to the limited computational capability and the energy-constraint of RFID tags. Note that we consider the far-field wireless communications in this scenario [26].

1.1. Related Works. Most of current studies have been concentrated on protecting the confidential communications of smart objects in WNoT, which are also named as *good* nodes in this paper. Encryption is one of the most commonly used techniques to protect the confidential communications in wireless personal area networks [11], wireless local area networks (e.g., WEP [27], WPA, and WPA2 [28]), wireless cellular networks (e.g., Cellular Message Encryption Algorithm [29]), and encryption algorithms for wireless sensor networks [30]. However, it is infeasible to apply cryptography-based techniques in WNoT due to the following reasons: (a) the inferior computational capability of smart objects [2], (b) the limited battery power of smart objects (e.g., the passive RFIDs can only harvest the energy from the readers) [1, 31], and (c) the difficulty of managing the widely distributed smart objects in centralized manner, which is the necessity for the encryption algorithms [11, 32, 33].

An alternate approach is either to design light-weighted encryption schemes [34] or to generate noise to limit the amount of information that can be extracted by an *eavesdropper* [35, 36]. However, one of the most important premises of the above schemes is that we shall have enough knowledge of the channel condition of eavesdroppers as indicated in [37–42], which nevertheless has received little attention. Besides, the wireless channel in WNoT fluctuates from time to time and is affected by various fading effects including the path loss, the shadowing effect, and the multipath effect [43]. Furthermore, most of current studies in WNoT only consider the nodes equipped with omnidirectional antennas, which radiate/receive RF signals in all directions (i.e., a less efficient way to propagate RF signals). As shown in some of the most recent studies [44, 45], directional antennas can be used at readers. Compared with omnidirectional antennas, directional antennas can concentrate the transmissions to some desired directions so that the performance can be further improved.

However, little attention has been paid to *investigating the eavesdropping behaviors conducted by the eavesdroppers in WNoT*, which is nevertheless important for us to offer better protection on the confidential communications since we can design antieavesdropping schemes with clearer targets if we have a better knowledge on the eavesdroppers, although we conducted a preliminary study on the eavesdropping probability of wireless ad hoc networks in [46]. But this paper is significantly different from our previous work [46] in the following aspects: (1) we are concerned with the eavesdropping activities in WNoT in this paper while the previous paper investigated the eavesdropping attacks in wireless ad hoc networks; (2) we propose a novel analytical model on the eavesdropping probability in this paper, where the channel randomness (including Rayleigh fading effect and the shadowing effects) is considered while the previous paper only considered a simplified geometric model; (3) we conduct extensive simulations to verify the accuracy of our proposed model in this paper while the previous paper only presented the numerical results.

1.2. Contributions. The aforementioned issues motivate us to conduct an investigation on the eavesdropping attacks in WNoT. In this paper, we analyze the eavesdropping activities

Table 1: Summary of effects on eavesdropping attacks.

Factors	Effects on eavesdropping attacks
Directional antenna	Positive
Shadow fading	Positive
Path loss	Negative
Rayleigh fading	Negative

conducted by eavesdroppers with consideration of various channel conditions and different types of antennas. *To the best of our knowledge, this is the first study on analyzing the eavesdropping attacks in WNoT from the viewpoints of eavesdroppers*. Our major research contributions in this paper can be summarized as follows:

(i) We formally establish an analytical framework to investigate the probability of eavesdropping attacks in WNoT with consideration of channel randomness. In particular, we consider the path loss effect, the shadow fading effect, and Rayleigh fading effect in our model. Besides, we also take both omnidirectional antennas and directional antennas into account of our analytical framework.

(ii) Extensive simulations show that the simulation results match the analytical results, indicating that our analytical model is accurate and effective. Our results also show that both the path loss effect and Rayleigh fading effect are *detrimental* to the probability of eavesdropping attacks while the shadow fading effect is beneficial to the eavesdropping attacks in WNoT. Besides, our results also indicate that using directional antennas at eavesdroppers can significantly improve the probability of eavesdropping attacks. We summarize our major findings in Table 1.

(iii) Our results can provide many useful implications on designing antieavesdropping schemes in WNoT. This is because we can provide the better protection on the confidential communications if we have the better knowledge about the eavesdroppers as implied in the previous studies [37–42]. For example, we can design light-weight encryption algorithms by exploiting the known channel features [47, 48]. Besides, we only need to encrypt the communications in the area or the direction that is vulnerable to eavesdropping attacks so that the security cost due to the computational complexity can be greatly saved.

The rest of this paper is organized as follows. Section 2 presents the models used in this paper. We then give the analysis on the eavesdropping attacks in Section 3. The impacts of channel randomness with consideration of the shadow fading effect and Rayleigh fading effect are discussed in Section 4. Finally, we conclude the paper in Section 5.

2. Models

In this section, we present the models used in this paper. (See Notations and Symbols section.)

2.1. Node Distribution. In this paper, we assume that all the smart objects (or nodes) are randomly distributed in a 2D area $\mathscr{A}$ according to a homogeneous Poisson point process with density ρ. We denote the number of nodes in an area $\mathscr{A}$ by a random variable N. Then, the probability mass function of N is given as follows:

$$f_N(n) = \frac{(\rho\mathscr{A})^n}{n!} e^{-\rho\mathscr{A}}, \tag{1}$$

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

2.2. Channel Model. We assume that all nodes use the common transmission power $\mathscr{P}_t$ similar to [49]. The channel gain from a node i to an eavesdropper j at a distance r is denoted by $\gamma_{ij}(r)$. Thus, the received power at the eavesdropper is $\mathscr{P}_t \cdot \gamma_{ij}(r)$. The signal-to-interference-plus-noise ratio (SINR) at the eavesdropper denoted by Λ is defined to be

$$\Lambda = \frac{\mathscr{P}_t \cdot \gamma_{ij}(r)}{\eta + \sum_{k\neq i}^{N} \mathscr{P}_t \cdot \gamma_{kj}(r)}, \tag{2}$$

where η is the power of the white noise and N denoted the number of good nodes.

The transmission from node i can be successfully eavesdropped by an eavesdropper if and only if

$$\Lambda \geq \beta, \tag{3}$$

where β is the minimum signal to interference and noise ratio.

In our analysis of eavesdropping activities, we ignore the impact of interference due to the following reasons. First, the passive eavesdroppers in WNoT do not transmit actively and therefore contribute nothing to the interference. Second, the interference is proved to converge when efficient MAC schemes are exploited and the traffic is low in a large-scale network [50, 51]. Thus, our analytical results in this paper can be regarded as the upper bound of the eavesdropping probability. We then have

$$\Lambda = \frac{\mathscr{P}_t \cdot \gamma_{ij}(r)}{\eta} \geq \beta. \tag{4}$$

2.3. Antennas. There are different types of antennas used in wireless communication systems: *omnidirectional* antennas (named *Omni* in short) and *directional antennas* (named *Dir* in short). Most of conventional smart objects are typically equipped with omnidirectional antennas, which radiate/collect radio signals into/from all directions equally. Different from an omnidirectional antenna, a directional antenna can concentrate transmitting or receiving capability on some desired directions consequently leading to the improved network performance. To model the transmitting or receiving capability of an antenna, we denote the *antenna gain* by G. It is obvious that an omnidirectional antenna has a constant antenna gain; that is, $G_o = 1$ in all directions.

We next give the antenna gain of a directional antenna. Since it is difficult to model a realistic directional antenna with precise values of antenna gain in each direction [52], we

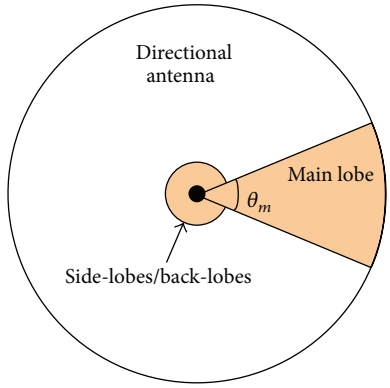

Figure 2: Directional antenna model.

use an approximate antenna model, which was first proposed in [53]. This model is also named as *Keyhole* due to the geometrical analogy to the archaic keyhole in 2D plane, as shown in Figure 2. In this model, the sector with angle θ_m represents the main *lobe* of the antenna, which has the maximum gain denoted by G_m (where θ_m is also called the antenna *beamwidth*), and the circular part represents the side-lobes and back-lobes with lower antenna gain denoted by G_s. In particular, when G_m and θ_m are given [53, 54], we can calculate G_s as follows:

$$G_s = \frac{2 - G_m\left(1 - \cos\left(\theta_m/2\right)\right)}{1 + \cos\left(\theta_m/2\right)}. \tag{5}$$

3. Analysis on Eavesdropping Attacks

This section presents our analytical framework to model the eavesdropping activities in WNoT. In particular, we first analyze *effective eavesdropping area* in Section 3.1 which is then used to derive the *probability of eavesdropping attacks* in Section 3.2. Section 3.3 presents the empirical results.

3.1. Deterministic Path Loss Model. We first consider that the channel gain is mainly determined by the large-scale path loss effect [43]. Thus, the channel gain is given by

$$\gamma_{ij}(r) = C \cdot G_g \cdot G_e \cdot \frac{1}{r^\alpha}, \tag{6}$$

where C is a constant, r is the distance between the good node and the eavesdropper, G_g and G_e are the antenna gains for the good node and the eavesdropper, respectively, and α is the path loss exponent ranging from 2 to 4 [43].

As shown in Section 2.2, an eavesdropper can successfully wiretap a transmission if and only if its $\Lambda \geq \beta$. In other words, the probability of no transmission eavesdropped is given by $P(\Lambda < \beta)$. Substituting (6) into inequality (4) and rearranging $P(\Lambda < \beta)$, we have

$$\begin{aligned} P\left(\Lambda < \beta\right) &= P\left(\frac{\mathscr{P}_t \cdot C \cdot G_g \cdot G_e}{\eta \cdot r^\alpha} < \beta\right) \\ &= P\left(r > \left(\frac{\mathscr{P}_t \cdot C \cdot G_g \cdot G_e}{\eta \cdot \beta}\right)^{1/\alpha}\right). \end{aligned} \tag{7}$$

We then define a random variable R as

$$R = \left(\frac{\mathscr{P}_t \cdot C \cdot G_g \cdot G_e}{\eta \cdot \beta}\right)^{1/\alpha}, \tag{8}$$

which is referred to the *eavesdropping range* of an eavesdropper. After substituting (8) into inequality (7), we have $P(\Lambda < \beta) = P(r > R)$, which implies that a transmission cannot be eavesdropped by an eavesdropper if and only if the transmitter falls outside the eavesdropping range R of the eavesdropper.

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

$$E\left[\pi R^2\right] = \pi E\left[\left(\frac{C \cdot \mathscr{P}_t \cdot G_g \cdot G_e}{\eta \cdot \beta}\right)^{2/\alpha}\right]. \tag{9}$$

3.2. Probability of Eavesdropping Attacks. We model the successful chance of eavesdropping attacks by the *probability of eavesdropping attacks*, denoted by $P(E)$. To derive $P(E)$, we need to analyze the probability of no good node being eavesdropped first. We denote the number of good nodes falling in the eavesdropping area by a random variable Y. Since good nodes are randomly distributed according to a homogeneous Poisson point process (as shown in Section 2.1), we then have the probability of no good node falling in the eavesdropping area, which is given by the following equation:

$$P(Y = 0) = e^{-\rho \cdot E[\pi R^2]}. \tag{10}$$

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

$$P(E) = 1 - P(Y = 0) = 1 - e^{-\rho \cdot E[\pi R^2]}. \tag{11}$$

After substituting $E[\pi R^2]$ in (11) by Right-Hand Side (RHS) of (9), we have

$$P(E) = 1 - \exp\left(-\rho \cdot \pi E\left[\left(\frac{C \cdot \mathscr{P}_t \cdot G_g \cdot G_e}{\eta \cdot \beta}\right)^{2/\alpha}\right]\right). \tag{12}$$

The physical meaning of $P(E)$ is the probability that an eavesdropper can successfully eavesdrop at least one transmission in WNoT. Besides, as shown in (12), the probability of eavesdropping attacks heavily depends on the path loss effect. Note that this model can be extended to a more general case with consideration of the shadow fading effect and the Rayleigh fading effect, which will be analyzed in Section 4.

3.3. Empirical Results. We conduct extensive simulations to verify the effectiveness and the accuracy of our proposed model. In our simulations, the probability of eavesdropping attacks in a WNoT is calculated by

$$P'(E) = \frac{\Psi}{\Omega}, \tag{13}$$

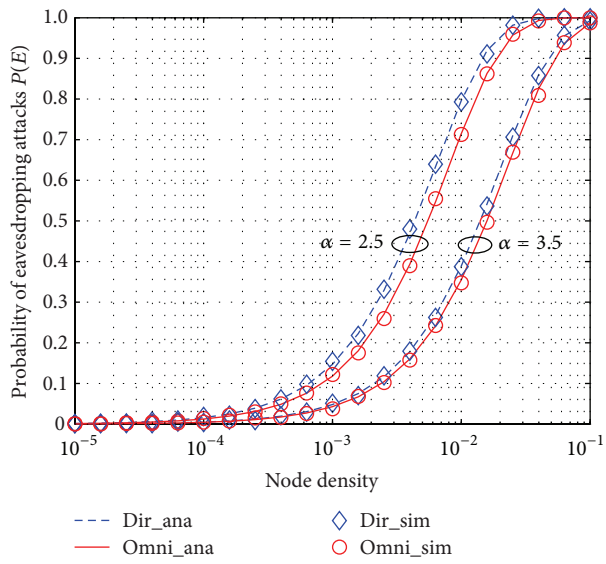

FIGURE 3: Probability of eavesdropping attacks $P(E)$ with path loss effect only when $\alpha = 2.5, 3.5$ and SINR threshold $\beta = 10$ dB.

where Ω and Ψ denote the number of total WNoT topologies and the number of WNoT topologies that have been eavesdropped, respectively. We say that a WNoT topology is eavesdropped when any smart object (node) in this topology is eavesdropped. Note that we denote the simulation results by $P'(E)$ in order to differentiate it from the analytical value $P(E)$. To minimize the impacts of the border effects, we conduct the simulations within an $l \times l$ area with the exclusion of the nodes falling in the outer box $l' \times l'$, where l' shall be significantly larger than l [55]. Note that l is chosen as 3000 m in our simulations. We fix the number of eavesdroppers and choose the node density ρ for the good nodes ranging from 10^{-5} to 10^{-1}. The other system parameters are selected as follows: $C = 10$, $\mathscr{P}_t = 1$ mWatt, $\eta = 0.01$ mWatt, and $\beta = 10$ dB. We consider eavesdroppers equipped with either omnidirectional antenna (Omni) or directional antenna (Dir) while the good nodes are equipped with omnidirectional antennas only.

Figure 3 shows both the analytical results and the simulation results of the probability of eavesdropping attacks with the path loss effect only. The curves and the markers represent the analytical results and simulation results, respectively. It is shown in Figure 3 that the simulation results have a good agreement with the analytical results, implying that our model is quite accurate.

As shown in Figure 3, we also find that the probability of eavesdropping attacks decreases with the increased path loss exponent α, implying that the path loss effect has the negative impact on eavesdropping attacks. Besides, we also find that using directional antennas at eavesdroppers can increase the probability of eavesdropping attacks although this effect is not that significant when the path loss effect is increased (e.g., $\alpha = 3.5$).

4. Impacts of Channel Randomness on Eavesdropping Attacks

In this section, we extend our analytical model in Section 3 to more general cases in consideration of two different effects of channel randomness: (1) shadow fading effect and (2) Rayleigh fading effect, which will be presented in Sections 4.1 and 4.2, respectively. We then give the empirical results in Section 4.3.

In order to model the two random effects, we introduce the *packet eavesdropping probability* denoted by $P_{E|\Lambda}(y)$, which is defined as the probability that a packet is successfully eavesdropped by an eavesdropper when the average signal-to-interference-noise ratio $\overline{\Lambda} = y$.

We then extend the analysis of eavesdropping range in Section 3.1 with consideration of the packet eavesdropping probability $P_{E|\Lambda}(y)$. We first consider the case that the packet eavesdropping probability $P_{E|\Lambda}(y)$ tends to approach a step function if good long code is used [56]. In particular, we have the cumulative distribution function (CDF) of eavesdropping range R, which is defined as follows:

$$F_R(r) = P[\Lambda(r) < \beta] = F_R\left(\frac{\eta \cdot \beta}{\mathscr{P}_t \cdot G_g \cdot G_e}\right). \quad (14)$$

In a more general case when $P_{E|\Lambda}(y)$ is not a step function, the cumulative distribution function is

$$F_R(r) = 1 - \int_0^{+\infty} f_R\left(\frac{\eta \cdot x}{\mathscr{P}_t \cdot G_g \cdot G_e} \mid r\right) P_{E|\Lambda}(x)\, dx, \quad (15)$$

where f_R is the probability density function (PDF) of R.

4.1. Shadow Fading Effect. Following the similar approach [51], we can derive the probability density function of R with consideration of the shadow fading effect as follows:

$$f_R(x) = \frac{1}{\sqrt{2\pi}\sigma x} \cdot \exp\left(-\frac{1}{2}\left(\frac{\ln x - \ln\left(C \cdot r^{-\alpha}\right)}{\sigma}\right)^2\right), \quad (16)$$

where r is the distance between a good node and an eavesdropper and σ is the standard deviation of the Gaussian distribution describing the shadow fading effect.

We then have the second moment of random variable R given as follows:

$$E\left[R^2\right] = \int_0^{+\infty} 2r\left[1 - F_l\left(\frac{\eta \cdot \beta}{\mathscr{P}_t \cdot A_G}\right)\right] dr. \quad (17)$$

After substituting $[1 - F_l(\eta\beta/\mathscr{P}_t A_G)]$ in (17) with RHS of (15) and RHS of (16) (note that $P_{E|\Lambda}(a) = 1$), we finally have

$$E\left[R^2\right] = \int_0^{+\infty} 2r \int_{\eta\beta/\mathscr{P}_t A_G}^{+\infty} \frac{1}{\sqrt{2\pi}\sigma a} \cdot e^{-(1/2)((\ln a - \ln(C \cdot r^{-\alpha}))/\sigma)^2} da\, dr, \quad (18)$$

where $A_G = E[(G_g G_e)^{2/\alpha}]$, which is defined as the *effective antenna gain factor*. It is obvious that the effective antenna gain factor depends on both the antenna gains and the path loss effect.

Let $x = (\ln a - \ln Cr^{-\alpha})/\sigma = \ln(ar^{\alpha}/C)/\sigma$; we then have

$$E\left[R^2\right] = \int_0^{+\infty} 2r \int_{\ln(\eta\beta r^{-\alpha}/\mathscr{P}_t A_G C)/\sigma}^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-x^2/2} \mathrm{d}x\, \mathrm{d}r. \quad (19)$$

Since the integrals converge absolutely, applying Fubini's theorem [57], we next get

$$E\left[R^2\right] = \left(\frac{\mathscr{P}_t A_G C}{\eta\beta}\right)^{2/\alpha} \exp\left(\left(\frac{\sqrt{2}\sigma}{\alpha}\right)^2\right). \quad (20)$$

Finally, we have the probability of eavesdropping attacks, which is given as the following equation:

$$P(E) = 1 - \exp\left(-\rho\pi\left(\frac{\mathscr{P}_t A_G C}{\eta\beta}\right)^{2/\alpha} \exp\left(\frac{\sqrt{2}\sigma}{\alpha}\right)^2\right). \quad (21)$$

The probability of eavesdropping attacks in (21) is more general than that in (12). This is because (21) becomes (12) when σ becomes 0, implying that there is no shadow fading effect and SINR is completely determined by the path loss effect.

4.2. Rayleigh Fading Effect. Rayleigh fading effect is a stochastic model for wireless propagation when there are a large number of statistically independent reflected and scattered paths from the transmitters to the receivers (or the eavesdroppers).

In the following procedure, we consider the channel condition with superimposed shadow fading and Rayleigh fading effects. We then derive the second moment of random variable R. Since (17) still holds, we have

$$\begin{aligned} E\left[R^2\right] &= \int_0^{+\infty} 2r \left[1 - F_l\left(\frac{\eta\cdot\beta}{\mathscr{P}_t\cdot A_G}\right)\right] \mathrm{d}r \\ &= \int_0^{+\infty} 2r \int_0^{+\infty} f_R\left(\frac{\eta\cdot x}{\mathscr{P}_t\cdot G_g\cdot G_e} \mid r\right) \\ &\quad \cdot P_{E|\Lambda}(x)\, \mathrm{d}x\, \mathrm{d}r, \end{aligned} \quad (22)$$

where $f_R((\eta x/\mathscr{P}_t G_g G_e) \mid r)$, which can be calculated by (16).

We next derive $P_{E|\Lambda}(x)$. Since the instantaneous SINR is exponentially distributed with mean $\Lambda = y$ [51], with the given average SINR value $\overline{\Lambda}$ and the given SINR threshold β, the packet eavesdropping probability $P_{E|\Lambda}(y)$ can be calculated by

$$\begin{aligned} P_{E|\Lambda}(y) &= \int_\beta^{+\infty} f_\Lambda(y)\, \mathrm{d}x = \int_\beta^{+\infty} \frac{1}{y}\cdot e^{-x/y} \mathrm{d}x \\ &= e^{-\beta/y}. \end{aligned} \quad (23)$$

After substituting the corresponding parts in (22) by (16) and (23), we finally have the effective eavesdropping range as follows:

$$\begin{aligned} E\left[R^2\right] &= \int_0^{+\infty} \int_0^{+\infty} e^{-(\eta\cdot\beta)/(x\cdot\mathscr{P}_t\cdot A_G)} \cdot 2r \frac{1}{\sqrt{2\pi}\sigma x} \\ &\quad \cdot e^{-(1/2)((\ln x - \ln(C\cdot r^{-\alpha}))/\sigma)^2} \mathrm{d}r\, \mathrm{d}x \\ &= \int_{-\infty}^{+\infty} \int_0^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-x^2/2} \cdot 2r \\ &\quad \cdot e^{-(\eta\cdot\beta\cdot r^{\alpha}\cdot e^{-\sigma x})/(C\cdot\mathscr{P}_t\cdot A_G)} \mathrm{d}r\, \mathrm{d}x, \end{aligned} \quad (24)$$

where $A_G = E[(G_g G_e)^{2/\alpha}]$ is the effective antenna gain factor.

The integral in (24) can be calculated by the following equation [58]:

$$\begin{aligned} &\int_0^{+\infty} 2r \cdot e^{-(\eta\cdot\beta\cdot r^{\alpha}\cdot e^{-\sigma x})/(C\cdot\mathscr{P}_t\cdot A_G)} \mathrm{d}r \\ &\quad = \frac{2}{\alpha}\Gamma\left(\frac{2}{\alpha}\right) \cdot \left(\frac{\eta\cdot\beta\cdot e^{-\sigma x}}{C\cdot\mathscr{P}_t\cdot A_G}\right)^{-2/\alpha}, \end{aligned} \quad (25)$$

where $\Gamma(\cdot)$ represents the general Gamma function.

Substituting (25) into (24) and applying it to (11), we finally have

$$P(E) = 1 - e^{-\rho\pi(2/\alpha)\Gamma(2/\alpha)\cdot((\eta\cdot\beta)/(C\cdot\mathscr{P}_t\cdot A_G))^{-2/\alpha}\cdot e^{(\sqrt{2}\sigma/\alpha)^2}}. \quad (26)$$

4.3. Empirical Results. We have conducted extensive simulations to evaluate the accuracy of our extended model. In order to compare the new results with those under the case without shadowing effects in Section 3.3, we choose the same system parameters as those in Section 3.3. Note that in order to eliminate the impacts of the border effect, the border area of the simulation area shall be slightly increased. Similarly, we also consider eavesdroppers equipped with either omnidirectional antennas or directional antennas.

Figure 4 shows the empirical results of the probability of eavesdropping attacks with shadow fading effects, where the shadow fading deviation $\sigma = 3$. Note that the curves and the markers represent the analytical results and simulation results, respectively. Figure 3 also indicates that the simulation results match the analytical results, implying the accuracy of our model.

As shown in Figure 4, we find that the probability of eavesdropping attacks is affected by both the path loss effect and the shadow fading effect. In particular, $P(E)$ decreases with the increased path loss exponent α, implying that the path loss effect is *detrimental*. In other words, the path loss effect will decrease the probability of eavesdropping attacks, which agrees with the previous results without the shadowing effect (see Figure 3). On the contrary, the shadow fading effect is *beneficial*. More specifically, if we compare Figure 4 with Figure 3, we can find that $P(E)$ increases with the increased values of the shadow fading deviation σ (e.g., σ is increased from 0 to 3). This effect is remarkable when the path loss effect is less notable (e.g., $\alpha = 2.5$). However, $P(E)$ does not increase

Table 2: Comparison between the results under the channel with shadow fading effect only and the results under the channel with superimposed shadowing and Rayleigh fading effects when $\alpha = 3$, $\sigma = 3$, and SINR threshold $\beta = 10$ dB.

Node density	Shadow fading effect only (Figure 4)		Superimposed shadow fading and Rayleigh fading effects (Figure 5)	
ρ	Omni	Dir	Omni	Dir
1×10^{-5}	0.0050	***0.0059***	0.0045 (−10.00%)	***0.0053 (−10.17%)***
1×10^{-4}	0.0489	***0.0572***	0.0443 (−9.41%)	***0.0518 (−9.44%)***
1×10^{-3}	0.3945	***0.4453***	0.3642 (−7.68%)	***0.4126 (−7.34%)***
1×10^{-2}	0.9934	***0.9972***	0.9892 (−4.20%)	***0.9951 (−2.10%)***

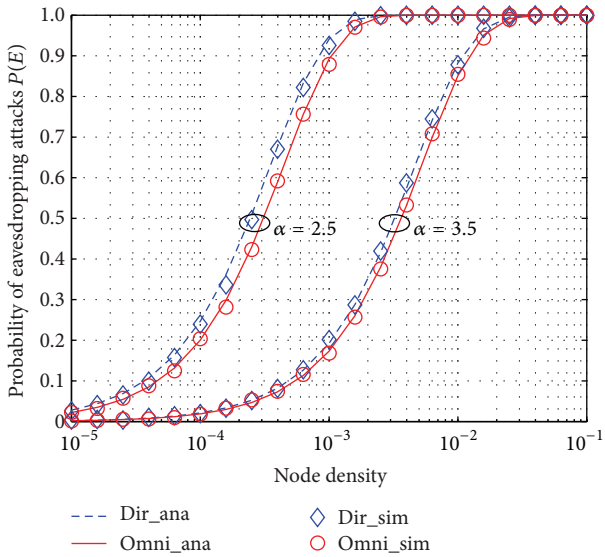

Figure 4: Probability of eavesdropping attacks $P(E)$ with shadowing effect ($\sigma = 3$) only when $\alpha = 2.5, 3.5$ and SINR threshold $\beta = 10$ dB.

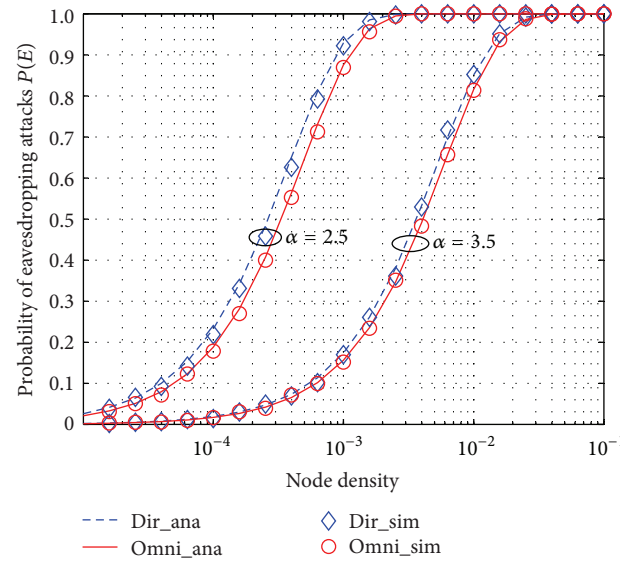

Figure 5: Probability of eavesdropping attacks $P(E)$ with superimposed shadowing effect and Rayleigh fading effect when $\sigma = 3$ and SINR threshold $\beta = 10$ dB.

significantly with the increased values of σ when $\alpha = 3.5$. Furthermore, we also find that using directional antennas at eavesdroppers can increase the probability of eavesdropping attacks with consideration of the shadowing effect.

We then investigate the probability of eavesdropping attacks under the channel with the superimposed shadow fading and Rayleigh fading effects. Figure 5 shows the results with the presence of both shadow fading and Rayleigh fading effects, where the shadow fading deviation $\sigma = 3$. As shown in Figure 5, we find that the probability of eavesdropping attacks is affected by both the shadow fading effect and the Rayleigh fading effect. Moreover, Figure 5 also indicates that Rayleigh fading effect has a *negative* impact on the probability of eavesdropping attacks even though it is not that noticeable compared with the path loss effect.

To illustrate the detrimental effect of Rayleigh fading effect, we conduct comparative study on the numerical results of the probability of eavesdropping attacks $P(E)$. In particular, Table 2 illustrates the comparison between the results of $P(E)$ under the channel with shadow fading effect only and the results under the channel with the superimposed shadow fading effect and Rayleigh fading effect when $\alpha = 3$ and $\sigma = 3$ corresponding to Figures 4 and 5, respectively. To make it clearer, we italicize the results with directional antennas in Table 2. It is shown in Table 2 that Rayleigh fading effect will decrease the probability of eavesdropping attacks compared with the results under the channel with the shadow fading effect only. For example, Rayleigh fading effect leads to the decrement of nearly 10% in terms of the probability of eavesdropping attacks when the node density $\rho = 10^{-5}$. Besides, Table 2 also indicates that using directional antennas at eavesdroppers can increase the probability of eavesdropping attacks, which is similar to the previous findings.

We also give the results under the scenario of eavesdropping attacks with Rayleigh fading effect only. Figure 6 shows the empirical results of the probability of eavesdropping attacks under the channel with Rayleigh fading effect only, where $\sigma = 0$ indicating no shadow fading effect. Similar to the previous results, we also denote the analytical results by the curves and the simulation results by the markers, as shown in Figure 6. It is shown in Figure 6 that the simulation results have a good agreement with the analytical results, implying that our analytical model is quite accurate.

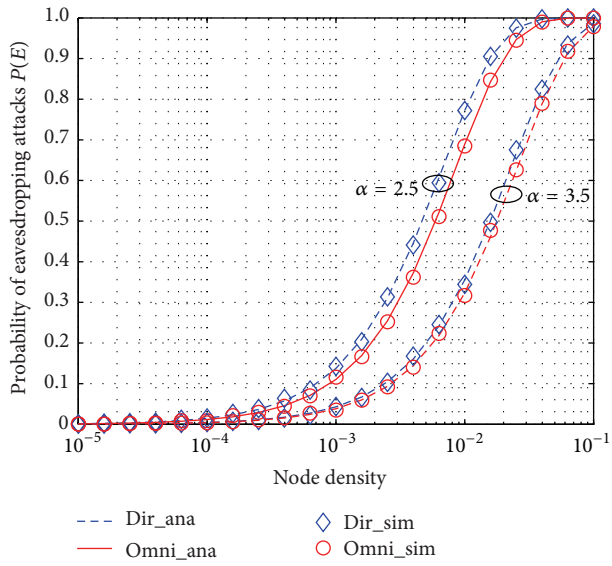

FIGURE 6: Probability of eavesdropping attacks $P(E)$ with Rayleigh fading effect only (without shadowing effect) where SINR threshold $\beta = 10$ dB and $\sigma = 0$.

As shown in Figure 6, we can see that the probability of eavesdropping attacks also depends on both the path loss effect and Rayleigh fading effect. In particular, $P(E)$ drops significantly when the path loss effect becomes more notable (e.g., $\alpha = 3.5$), as shown in Figure 6. Besides, under the wireless channel with Rayleigh fading effect, $P(E)$ in Figure 6 is even lower than that without Rayleigh fading effect in Figure 3, implying that Rayleigh fading effect is also detrimental to the eavesdropping attacks. The reason may owe to the counteracting effect of the multipath scattering signals under the channel with Rayleigh fading effect [43].

4.4. Discussions and Implications of Our Results. Our simulation results imply that using directional antennas at eavesdroppers in WNoT can significantly increase the probability of eavesdropping. Thus, directional antennas are *beneficial* to eavesdroppers. The improvement mainly owes to the effect that a directional antenna can accumulate the receiving capability of desired directions. However, we can not ignore another effect that a directional antenna can also narrow the angle of the receiving directions. More specifically, with the increased path loss (i.e., the larger α), the second effect can even counteract the first effect. Take Figure 6 as an example. The gap between the results of omnidirectional eavesdroppers and the results of directional eavesdroppers with $\alpha = 2.5$ is significantly bigger than that with $\alpha = 3.5$.

Secondly, as shown in our results, both the path loss effect and Rayleigh fading are always detrimental to the eavesdropping probability while shadowing effect and directional antennas are beneficial to the eavesdropping probability. Our findings are useful to help to design more effective antieavesdropping schemes in WNoT. This is because we need the knowledge of eavesdroppers (such as the channel characteristics) so that we can design the light-weight encryption algorithms as indicated in the previous studies [37–42]. Besides, we only need to take antieavesdropping measures in the area or the direction that is vulnerable to eavesdropping attacks so that the security cost due to the computational complexity can be greatly saved. For example, we can generate the noise only in the direction of eavesdroppers when the eavesdroppers are equipped with directional antennas while there is no noise in other directions. This new scheme may have a better performance than the existing one [35].

5. Conclusion

In this paper, we propose an analytical model to investigate the eavesdropping probability in Wireless Net of Things (WNoT) with consideration of channel randomness including the path loss effect, the shadow fading effect, and Rayleigh fading effect. After conducting extensive simulations, we show that our model is quite accurate. Besides, we have also shown that the eavesdropping probability heavily depends on the path loss effect, the shadow fading effect, and Rayleigh fading effect. More specifically, we find that the eavesdropping probability increases when the shadow fading factor σ increases and decreases when the path loss effect increases, implying that the path loss effect is detrimental to the eavesdropping attacks while the shadow fading is beneficial to the eavesdropping attacks. Moreover, similar to the path loss effect, Rayleigh fading is also destructive to the eavesdropping attacks. Furthermore, our results also indicate that using directional antennas at eavesdroppers can significantly improve the probability of eavesdropping attacks.

Notation and Symbols

$\mathcal{A}$: 2D area that nodes are randomly distributed
ρ: Density of the homogeneous Poisson point process
$\mathcal{P}_t$: Transmission power of nodes
r: Distance between the good node and the eavesdropper
$\gamma_{ij}(r)$: Channel gain from a good node i to an eavesdropper j at a distance r
Λ: SINR at an eavesdropper
β: Threshold value of SINR for eavesdropping a node successfully
η: Power of the white noise
N: Number of good nodes
α: Path loss exponent
G_m, G_s: Antenna gain of main lobe, antenna gain of side-lobe
θ_m: Main lobe beam-width of the keyhole antenna
G_g, G_e: Antenna gain of good node, antenna gain of eavesdropper
$P(E)$: Probability of eavesdropping attacks
l: Side length of topology area
R: Eavesdropping range of an eavesdropper

Ω: Number of total WNoT topologies
Ψ: Number of WNoT topologies that have been eavesdropped
$\overline{\Lambda}$: Average SINR value
$P_{E|\Lambda}(y)$: Packet eavesdropping probability when the average SINR is y
σ: Standard deviation of the Gaussian distribution describing the shadow fading effect
A_G: Effective antenna gain factor.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The work described in this paper was partially supported by Macao Science and Technology Development Fund under Grant no. 096/2013/A3 and Grant no. 104/2014/A3 and supported by Innovation Norway through the project "GCE BLUE Maritime Big Data." The authors would like to thank Gordon K.-T. Hon for his helpful comments that greatly improve the quality of this paper.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[3] ISO/IEC 18000, 2013, http://en.wikipedia.org/wiki/ISO/IEC_18000.

[4] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[5] C. Dixon, R. Mahajan, S. Agarwal et al., "An operating system for the home," in *Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation (NSDI '12)*, p. 25, USENIX Association, San Jose, Calif, USA, April 2012.

[6] K. Habib, A. Torjusen, and W. Leister, "Security analysis of a patient monitoring system for the Internet of Things in eHealth," in *Proceedings of the International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED '15)*, Lisbon, Portugal, February 2015.

[7] Z. Fan, P. Kulkarni, S. Gormus et al., "Smart grid communications: overview of research challenges, solutions, and standardization activities," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 21–38, 2013.

[8] H. Wang, O. Osen, G. Li, W. Li, H.-N. Dai, and W. Zeng, "Big data and industrial internet of things for the maritime industry in Northwestern Norway," in *Proceedings of the IEEE Region 10 Conference (TENCON '15)*, Macau, China, November 2015.

[9] IEEE 802.15.4, 2011, http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf.

[10] Bluetooth Core Specification 4.2, 2014, http://www.bluetooth.org/.

[11] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[12] A. Grau, *How to Build a Safer Internet of Things*, IEEE Spectrum, 2015.

[13] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[14] G. Strazdins and H. Wang, "Open security and privacy challenges for the internet of things," in *Proceedings of the 10th International Conference on Information, Communications and Signal Processing (ICICS '15)*, 2015.

[15] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 624–632, 2014.

[16] 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.

[17] N. Meghanathan, "A survey on the communication protocols and security in cognitive radio networks," *International Journal of Communication Networks and Information Security*, vol. 5, no. 1, pp. 19–38, 2013.

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

[19] 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)*, vol. 2, pp. 707–714, IEEE, Reston, Va, USA, September 2006.

[20] H.-N. Dai, D. Li, and R. C.-W. Wong, "Exploring security improvement of wireless networks with directional antennas," in *Proceedings of the IEEE 36th Conference on Local Computer Networks (LCN '11)*, pp. 191–194, Bonn, Germany, October 2011.

[21] 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, IEEE, San Diego, Calif, USA, November 2008.

[22] Q. Wang, H.-N. Dai, and Q. Zhao, "Eavesdropping security in wireless Ad Hoc networks with directional antennas," in *Proceedings of the 22nd Wireless and Optical Communications Conference (WOCC '13)*, pp. 687–692, May 2013.

[23] H.-N. Dai, Q. Wang, D. Li, and R. C.-W. Wong, "On eavesdropping attacks in wireless sensor networks with directional antennas," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 760834, 13 pages, 2013.

[24] E. Alsaadi and A. Tubaishat, "Internet of things: features, challenges, and vulnerabilities," *International Journal of Advanced Computer Science and Information Technology*, vol. 4, no. 1, pp. 1–13, 2015.

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

[26] R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006.

[27] IEEE 802.11a-1999, http://standards.ieee.org/getieee802/download/802.11a-1999.pdf.

[28] IEEE 802.11i-2004, http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

[29] D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the cellular message encryption algorithm," in *Advances in Cryptology—CRYPTO '97*, vol. 1294 of *Lecture Notes in Computer Science*, pp. 526–537, Springer, Berlin, Germany, 1997.

[30] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[31] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd Annual Design Automation Conference (DAC '15)*, San Francisco, Calif, USA, June 2015.

[32] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the internet of things: a standardization perspective," *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 265–275, 2014.

[33] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.

[34] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 401–410, Denver, Colo, USA, November 2007.

[35] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, and J. Reverdy, "RFID noisy reader how to prevent from eavesdropping on the communication?" in *Cryptographic Hardware and Embedded Systems—CHES 2007*, vol. 4727 of *Lecture Notes in Computer Science*, pp. 334–345, Springer, Berlin, Germany, 2007.

[36] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[37] G. P. Hancke, "Practical eavesdropping and skimming attacks on high-frequency RFID tokens," *Journal of Computer Security*, vol. 19, no. 2, pp. 259–288, 2011.

[38] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[39] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output gaussian broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4215–4227, 2010.

[40] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: secrecy degrees of freedom," *IEEE Transactions on Information Theory*, vol. 59, no. 8, pp. 4733–4745, 2013.

[41] I. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, 2003.

[42] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, 2015.

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

[44] A. Sawadi, *An RFID directional antenna for location positioning [Ph.D. dissertation]*, University of Windsor, 2012.

[45] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*, Newnes, 2nd edition, 2012.

[46] X. Li, H.-N. Dai, and Q. Zhao, "An analytical model on eavesdropping attacks in wireless networks," in *Proceedings of the IEEE International Conference on Communication Systems (ICCS '14)*, pp. 538–542, IEEE, Macau, China, November 2014.

[47] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the ACM 14th Annual International Conference on Mobile Computing and Networking (MobiCom '08)*, pp. 128–139, ACM, San Francisco, Calif, USA, September 2008.

[48] F. Huo and G. Gong, "A new efficient physical layer OFDM encryption scheme," in *Proceedings of the 33rd IEEE Conference on Computer Communications (INFOCOM '14)*, pp. 1024–1032, Toronto, Canada, May 2014.

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

[50] M. Franceschetti, O. Dousse, D. N. Tse, and P. Thiran, "Closing the gap in the capacity of wireless networks via percolation theory," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1009–1018, 2007.

[51] D. Miorandi, E. Altman, and G. Alfano, "The impact of channel randomness on coverage and connectivity of ad hoc and sensor networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 3, pp. 1062–1072, 2008.

[52] C. A. Balanis, *Antenna Theory: Analysis and Design*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1997.

[53] 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 & Computing (MobiHoc '01)*, pp. 95–105, ACM, Long Beach, Calif, USA, October 2001.

[54] Q. Wang, H.-N. Dai, and Q. Zhao, "Connectivity of wireless Ad Hoc networks: impacts of antenna models," in *Proceedings of the 14th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT '13)*, pp. 298–303, Taipei, Taiwan, December 2013.

[55] C. Bettstetter, "On the connectivity of ad hoc networks," *The Computer Journal*, vol. 47, no. 4, pp. 432–447, 2004.

[56] M. Zorzi and S. Pupolin, "Outage probability in multiple access packet radio networks in the presence of fading," *IEEE Transactions on Vehicular Technology*, vol. 43, no. 3, pp. 604–610, 2002.

[57] J. Borwein, D. Bailey, and R. Girgensohn, *Experimentation in Mathematics: Computational Paths to Discovery*, Wellesley, 2004.

[58] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, New York, NY, USA, 7th edition, 2007.