Received June 29, 2018, accepted August 7, 2018, date of publication September 3, 2018, date of current version September 21, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2868225

Secure Capacity Analysis for Magnetic Inductive Coupling-Based SWIPT System

SUNGMIN HAN[1], (Student Member, IEEE), HAN-JOON KIM[1], (Student Member, IEEE), JAESEOK LEE[2], AND JI-WOONG CHOI[1,3], (Senior Member, IEEE)

[1]Daegu Gyeongbuk Institute of Science and Technology, Daegu 42988, South Korea
[2]Hanwha Systems, Yongin 17121, South Korea
[3]Brain Engineering Convergence Research Center, DGIST, Daegu 42988, South Korea

Corresponding author: Ji-Woong Choi (jwchoi@dgist.ac.kr)

This work was supported in part by the DGIST R&D Program of the Ministry of Science and ICT under Grant 18-ST-02, in part by the Institute for Information & communications Technology Promotion (IITP) through the Korean Government (MSIT) (Resilient Cyber-Physical Systems Research), under Grant 2014-0-00065, and in part by the Bio & Medical Technology Development Program of the National Research Foundation (NRF) through the Korean Government (MSIT) under Grant NRF-2017M3A9G8084463.

ABSTRACT Many researchers have provided meaningful insights for physical layer security (PLS) in various wireless communication systems. However, few works have carried out an intensive PLS analysis for magnetic inductive coupling (MIC)-based simultaneous wireless information and power transfer (SWIPT). This paper analyzes the effect of the angular position of coils on the secure capacity of a MIC-based SWIPT system in the presence of a potential malicious power receiver. Using a simple coupling model, we analyze the maximum achievable secure capacity of a MIC-based SWIPT system when the transmitter has knowledge of the coil angular positions of the receiver and the potential eavesdropper. In addition, we expand our analysis to the case where the transmitter has only limited knowledge of the coil angular positions of the receiver and the potential eavesdropper due to the angular fluctuation of the coils. Since employing the PLS technique with a traditional security algorithm can enhance security, the analysis will provide a meaningful contribution for improving MIC-based SWIPT system security.

INDEX TERMS Magnetic induction coupling (MIC), physical layer security (PLS), secure capacity, magnetic coil, near field communication (NFC).

I. INTRODUCTION

A magnetic inductive coupling (MIC)-based communication system is a short-range communication system used for rapid transmission of short message applications, such as smartphone pairing and peer-to-peer communication. Since MIC-based communication is employed in applications requiring high security, e.g., mobile banking, e-ticketing, and e-payment, the security requirement of MIC-based communication system is also increasing [1]–[4]. Due to the vulnerability of wireless channels, MIC-based communication systems suffer security threats, such as data modification or eavesdropping [1]–[5].

In addition to the MIC-based communication system, recent studies have been focused on MIC-based simultaneous wireless information and power transfer (SWIPT) systems which allow high power and information transfer [6]. Since a sufficient power transfer rate cannot be achieved with the conventional communication power level, the transmission power of SWIPT systems is much larger than that of conventional communication systems. Therefore, the amount of leakage power to the undesired node is noticeable. For SWIPT systems that use one shared channel to transfer power and information, the increased leakage power makes MIC-based SWIPT system more vulnerable to eavesdropping.

Existing studies on MIC-based communication system security mostly have analyzed its vulnerabilities and threat preventing methods at the software level by using cryptographic algorithms [7]–[11]. In [7], security risks of a near field communication (NFC) system are studied, and [8] investigates the vulnerability of the NFC authentication protocol. Based on investigation results, new pseudonym-based secure authentication protocols are proposed in [7] and [8]. References [9] and [10] propose an NFC-based secure payment system that is assisted by an external secured vault server to mitigate inherent security vulnerabilities of NFC systems. Eun *et al.* [11] improve the security performance of an authentication protocol by using conditional privacy protection methods.

Recently, physical layer security (PLS) techniques have been proposed in various wireless communication systems to improve security [12]. Unlike traditional encryption algorithms, PLS techniques achieve a highly secured system by using the physical characteristics of the transceiver and channel. PLS techniques do not depend on cryptographic algorithms, and thus are reliable in the presence of traditional security threats, that is, leakage of an encryption key. Therefore, MIC-based communication system can be more secure with both PLS and cryptographic techniques. For example, magnetic beamforming techniques can improve security by reducing signal leakage in an undesirable direction [13]. In [14] and [15], a magnetic beamforming scheme is used for long range and secured wireless power transfer. To reduce signal leakage, Kim *et al.* [16] introduce a multipole loop antenna that can cancel crosstalk between undesired coils. However, previous studies mainly focus only on improving the data rate or power transfer efficiency rather than improving security. In addition, there has been no intensive theoretical analysis, to the best knowledge of the authors, on the security performance of MIC systems exploiting PLS.

Since MIC is sensitive to the angular positions of coils, the secure capacity of MIC-based communication systems is quite dependent on the angular positions of coils. In this paper, we analyze the effect of the angular position of coils on the secure capacity of a MIC-based SWIPT system using a simple MIC model to exploit the PLS technique. To be specific, the system consists of one transmitter, one information receiver, and one power receiver, where the power receiver is potentially malicious. By receiving information and power at two receivers, respectively, SWIPT is performed. Our first analysis assumes that the angular positions of the receiver coils are fixed, and the transmitter perfectly knows the angular positions of all receiver coils. The analysis is then expanded to the case where the transmitter has only limited information about the angular positions of the receiver coils due to limited feedback or angular position fluctuation of the receiver coils. We also suggest the optimal transmitter angular position to maximize the secure capacity, which satisfies the power transfer requirement. By doing so, we provide insight into the effect of the angular position of coils on the secure capacity of a MIC-based SWIPT system, which is helpful for understanding achievable security performance of MIC-based SWIPT systems with PLS the technique.

The rest of this paper is organized as follows. In Section II, we describe the system model of a MIC-based SWIPT system with a brief introduction about MIC. Section III presents the analytical results on the secure capacity of the system model. Section IV provides our conclusion and suggestions for future works.

II. SYSTEM MODEL AND PRELIMINARIES

A. INTRODUCTION TO MIC

Before presenting our system model, we briefly introduce background knowledge of MIC, which corresponds to the basic MIC link model considered thoroughly in this work.

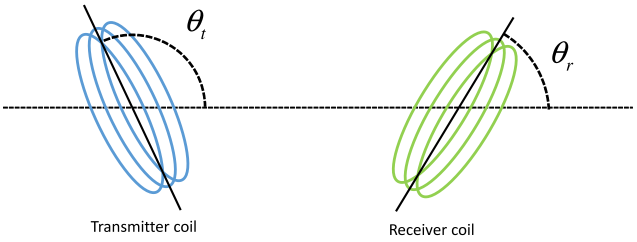


FIGURE 1. Conventional magnetic inductive coupling model.

The MIC between transmitter and receiver coils is expressed as J^2H, where J is the angular coefficient depending on the angular positions of coils, and H is the magnetic channel gain due to all other effects such as intrinsic characteristics of coils air-gap between the coils. When the transmitter and receiver coils are located as shown in Fig. 1, the angular coefficient J is

$$\begin{aligned} J &= 2\sin(\theta_t)\sin(\theta_r) + \cos(\theta_t)\cos(\theta_r) \\ &= \sqrt{4\sin^2(\theta_r) + \cos^2(\theta_r)}\cos(\theta_t - \arctan(2\tan(\theta_r))) \\ &= \sqrt{4\sin^2(\theta_t) + \cos^2(\theta_t)}\cos(\theta_r - \arctan(2\tan(\theta_t))), \end{aligned} \tag{1}$$

where θ_t and θ_r are the angular positions of both the transmitter and receiver coils, respectively [6], [17].

When θ_r is given, the maximum achievable value of J^2 by controlling θ_t is $4\sin^2(\theta_r) + \cos^2(\theta_r)$. Therefore, with given θ_r, the maximum achievable received power is

$$P_r^{\max} = H\left(4\sin^2(\theta_r) + \cos^2(\theta_r)\right)P_t, \tag{2}$$

where P_t is the transmission power. Similarly, it is worthwhile to note that, when θ_t is given, the maximum achievable received power is alternatively expressed as $H\left(4\sin^2(\theta_t) + \cos^2(\theta_t)\right)P_t$.

B. SYSTEM MODEL

Following the basic model discussed in Fig. 1, we consider a MIC-based SWIPT system model in Fig. 2 that consists of one transmitter *Alice*, and two receivers *Bob* and *Eve*. Each node has one magnetic coil. The receivers can switch to information or power exclusive receiving mode. We assume that *Bob* and *Eve* are designated to be in information and power exclusive modes, respectively. The SWIPT is conducted by the following procedure. *Alice* transmits a modulated signal that contains information to *Bob*, and *Bob* decodes the

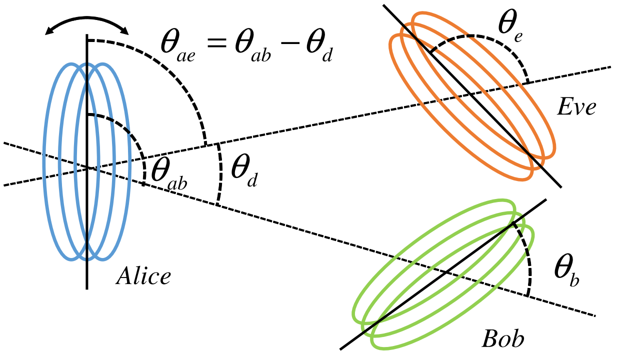


FIGURE 2. Magnetic wiretap channel model.

received signal to obtain the information. On the other hands, *Eve* rectifies the received signal[1] to store power instead of decoding. Note that this system is a simplified version of the system already proposed in [6]. To be specific, in [6], there are multiple power exclusive receivers with a single information exclusive receiver, and the transmitter has orthogonally arranged coils to support receiver coils in a three-dimensional space.

When all nodes operate according to the designated modes, i.e., *Eve* does not decode the signal, the information from *Alice* to *Bob* is secured. However, there is the potential threat of *Eve*; e.g., *Eve* intentionally switches to information exclusive mode to eavesdrop information instead of power saving, and thus the secure capacity of the system is limited by *Eve*. Minimizing the received signal power of *Eve* can improve the secure capacity. However, since *Alice* does not know whether *Eve* tries eavesdropping or not, *Alice* should serve power to *Eve*. For example, the received power of *Eve* should be larger than a given threshold.

When the transmission power of *Alice* is P_a, the received power of *Bob* and *Eve* is $P_b = J_b^2 H_b P_a$ and $P_e = J_e^2 H_e P_a$, respectively, where J_b and J_e are the angular coefficients of *Alice-Bob* and *Alice-Eve* links, respectively, H_b and H_e are the magnetic channel gains of *Alice-Bob* and *Alice-Eve* links, respectively, and θ_{ab}, θ_{ae}, θ_d, θ_b, and θ_e indicate the angular positions of the coils, as shown in Fig. 2. We assume that the angular position of *Alice*'s coil is only adjustable, e.g., θ_b and θ_e are given; J_b and J_e are then expressed as

$$\begin{aligned} J_b &= \sqrt{\frac{P_b^{\max}}{H_b P_a}} \cos\left(\theta_{ab} - \alpha_b\right), \\ J_e &= \sqrt{\frac{P_e^{\max}}{H_e P_a}} \cos\left(\theta_{ae} - \alpha_e\right) \\ &= \sqrt{\frac{P_e^{\max}}{H_e P_a}} \cos\left(\theta_{ab} - \alpha_e - \theta_d\right), \end{aligned} \tag{3}$$

where $\alpha_b = \arctan\left(2\tan\left(\theta_b\right)\right)$, $\alpha_e = \arctan\left(2\tan\left(\theta_e\right)\right)$, and

$$\begin{aligned} P_b^{\max} &= H_b P_a \left(4\sin^2\left(\theta_b\right) + \cos^2\left(\theta_b\right)\right), \\ P_e^{\max} &= H_e P_a \left(4\sin^2\left(\theta_e\right) + \cos^2\left(\theta_e\right)\right), \end{aligned} \tag{4}$$

are the maximum achievable received signal power of *Bob* and *Eve* when θ_b and θ_e are given, respectively, where the secure capacity C_s is defined as

$$\begin{aligned} C_s &\triangleq \left[\ln\left(1 + \frac{P_b}{N_0}\right) - \ln\left(1 + \frac{P_e}{N_0}\right)\right]^+ \\ &= \left[\ln\left(\frac{N_0 + P_b}{N_0 + P_e}\right)\right]^+ \\ &= \left[\ln\left(\frac{N_0 + J_b^2 H_b P_a}{N_0 + J_e^2 H_e P_a}\right)\right]^+, \end{aligned} \tag{5}$$

where $[x]^+ = \max\{x, 0\}$, and N_0 is the noise power [18]. To focus on the analysis of the effect of the angular positions of coils on the secure capacity, we assume that the magnetic channel gains of *Alice-Bob* and *Alice-Eve* links are identical; that is $H_b = H_e$.

III. SECURE CAPACITY ANALYSIS AND VERIFICATION

In this section, we investigate the secure capacity of the system under two assumed scenarios: 1) receiver coils are fixed, and *Alice* has knowledge of the angular positions of the receiver coils, 2) due to the angular fluctuation of the receiver coils or limited feedback, *Alice* has only limited information of the angular position of the receiver coils. In addition, we also provide strategies for maximizing the secure capacity.

A. FULL KNOWLEDGE OF ANGULAR POSITIONS

First, we analyze the secure capacity when fixed receiver angular position information is given to *Alice*. Since MIC between coils is quite strong compared to typical wireless channel gain, in a MIC system, the received signal strength is much larger than the noise power level, which clearly indicates that $P_b/N_0, P_e/N_0 \gg 1$. Then (5) can be approximated for a high signal to noise power ratio (SNR) environment into C_s^a as

$$\begin{aligned} C_s \approx C_s^a &= \left[\ln\left(\frac{P_b}{P_e}\right)\right]^+ \\ &= \left[\ln\left(\frac{J_b^2 H_b P_a}{J_e^2 H_e P_a}\right)\right]^+ = \left[\ln\left(\frac{J_b^2}{J_e^2}\right)\right]^+ \\ &= \left[\ln\left(\frac{P_b^{\max}\cos^2\left(\theta_{ab} - \alpha_b\right)}{P_e^{\max}\cos^2\left(\theta_{ab} - \alpha_e - \theta_d\right)}\right)\right]^+. \end{aligned} \tag{6}$$

Fig. 3 shows the approximation error $\left|C_s - C_s^a\right|/C_s$ in various SNR environments. The approximation error tends to decrease when P_b is much larger than P_e. However, the approximation error is less than 1% when P_e/N_0 is larger than 20 dB regardless of the value of P_b/P_e. Therefore, C_s^a provides analysis results with only marginal differences.

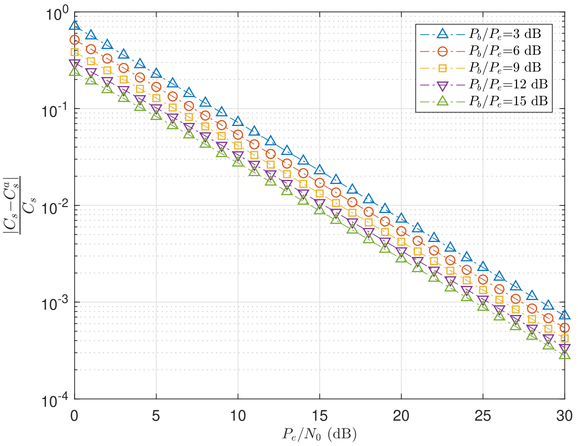


FIGURE 3. Approximation error $\left|C_s - C_s^a\right|/C_s$ in various SNR environments.

[1] This received signal does not contain information for *Eve*

Next, the strategy for maximizing the secure capacity is provided. Since *Eve* is the power receiver, P_e should be larger than its given threshold, $\tilde{P}_e$. The secure capacity maximization can be achieved by the adjusting angular position of *Alice* as

$$C_s^{a*} = \max_{\theta_{ab}} \left[\ln\left(\frac{P_b^{\max}\cos^2(\theta_{ab}-\alpha_b)}{P_e^{\max}\cos^2(\theta_{ab}-\alpha_e-\theta_d)} \right) \right]^+ , \quad \text{subject to } P_e = P_e^{\max}\cos^2(\theta_{ab}-\alpha_e-\theta_d) \geq \tilde{P}_e. \tag{7}$$

From (7), note that since P_e cannot be larger than $P_e^{\max}$, $\tilde{P}_e$ should be smaller than $P_e^{\max}$. In addition, if $P_b^{\max}$ $(\geq P_b)$ is smaller than $\tilde{P}_e$ $(\leq P_e)$, C_s^a is always 0 (see (6)). Therefore, the optimal C_s^{a*} should be obtained under the assumptions $P_e^{\max} \geq \tilde{P}_e$ and $P_b^{\max} > \tilde{P}_e$.

Recall that our objective is to maximize the secure capacity under the constraint of the received power of *Eve*. When $\theta_{ab} = (\alpha_e + \theta_d + \pi/2)$, C_s^a is diverging to infinity because P_e is minimized to 0. Since C_s^a is a simple concave function, adjusting θ_{ab} from $(\alpha_e + \theta_d + \pi/2)$ monotonically decreases C_s^a. In addition, adjusting θ_{ab} from $(\alpha_e + \theta_d + \pi/2)$ increases P_e. Therefore, the optimal θ_{ab} is the point corresponding to $P_e = \tilde{P}_e$. Since there are two values of θ_{ab} corresponding to $P_e = \tilde{P}_e$, the value that gives a C_s^a is optimal θ_{ab}. Fig. 4 shows C_s^a and P_e when $\theta_b = \pi/4$, $\theta_e = \pi/8$, $\theta_d = \pi/2$, and $\tilde{P}_e = 0.3$. In Fig. 4, when $\theta_{ab} = 0.22\pi$, C_s^a is diverging to infinity, and P_e is minimized to 0. As aforementioned, adjusting θ_{ab} from 0.22π reduces C_s^a and increases P_e. Therefore, the optimal θ_{ab} is one of the values corresponding to $P_e = \tilde{P}_e = 0.3$, which are indicated as red squares in Fig. 4. In this case, since the right point red square gives a higher C_s^a, the right one is the optimal θ_{ab}. By doing so, the optimal point is obtained as

$$\theta_{ab}^* = \mathrm{mod}\left(s^{\pm}\arccos\left(\sqrt{\frac{\tilde{P}_e}{P_e^{\max}}} \right) + \alpha_e + \theta_d, \pi \right), \tag{8}$$

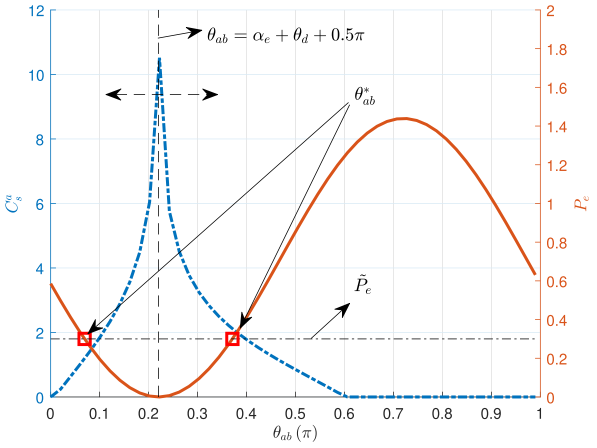


FIGURE 4. Minimum and maximum values of C_s^a and P_e, where the red squares are points of θ_{ab} corresponding with $P_e = \tilde{P}_e$, when $\theta_b = \pi/4$, $\theta_e = \pi/8$, $\theta_d = \pi/2$, and $\tilde{P}_e = 0.3$.

where $\mathrm{mod}(\cdot, \pi)$ is modulo operation by π, $s^{\pm} = \mathrm{sgn}(\mathrm{mod}(\alpha_e + \theta_d + \pi/2, \pi) - \mathrm{mod}(\alpha_b, \pi))$, and $\mathrm{sgn}(\cdot)$ is a sign function. The optimal secure capacity is obtained by substituting θ_{ab}^* to (6) as

$$\begin{aligned} C_s^{a*} &= \left[\ln\left(\frac{P_b^{\max}\cos^2(\theta_{ab}^*-\alpha_b)}{P_e^{\max}\cos^2(\theta_{ab}^*-\alpha_e-\theta_d)} \right) \right]^+ \\ &= \left[\ln\left(\frac{P_b^{\max}\cos^2\left(s^{\pm}\arccos\left(\sqrt{\frac{\tilde{P}_e}{P_e^{\max}}}\right)+\alpha_e+\theta_d-\alpha_b\right)}{\tilde{P}_e} \right) \right]^+ . \end{aligned} \tag{9}$$

Since $\cos^2(\cdot) \leq 1$, (9) cannot be larger than $C_{s,\mathrm{UB}}^{a*} = \left[\ln\left(P_b^{\max}\right) - \ln\left(\tilde{P}_e\right)\right]^+$.[2] Therefore, the upper bound of C_s^a linearly decreases when the transmitted power to *Eve* is exponentially increased. In fact, analysis of the effect of $\tilde{P}_e$ on the exact value of C_s^a is difficult because (9) cannot be simplified in general. Instead, we provide the exact effect of $\tilde{P}_e$ on C_s^a in two special cases. Since a typical case can be represented by a mixture of the following two cases, these cases provide an intuitive understanding of the relationship between $\tilde{P}_e$ and C_s^a.

1) SPECIAL CASE 1: $(\alpha_e + \theta_d - \alpha_b) = \pi/2$

By substituting $(\alpha_e + \theta_d - \alpha_b) = \pi/2$ to (6), we have

$$C_s^a = \left[\ln\left(\frac{P_b^{\max}\cos^2(\theta_{ab}-\alpha_b)}{P_e^{\max}\cos^2(\theta_{ab}-\alpha_b-\pi/2)} \right) \right]^+ . \tag{10}$$

In this case, *Alice* has the largest adjustability of the ratio between information and power transfer rate since the phase of the numerator term is different by $\pi/2$ from the phase of the denominator term. For example, when θ_{ab} is close to α_b, the magnitude of the numerator is enlarged, but the magnitude of the denominator is decreased. C_s^{a*} then becomes

$$\begin{aligned} C_s^{a*} &= \left[\ln\left(\frac{P_b^{\max}\cos^2\left(s^{\pm}\arccos\left(\sqrt{\frac{\tilde{P}_e}{P_e^{\max}}}\right)+\frac{\pi}{2}\right)}{\tilde{P}_e} \right) \right]^+ \\ &= \left[\ln\left(\frac{P_b^{\max}\left(1-\frac{\tilde{P}_e}{P_e^{\max}}\right)}{\tilde{P}_e} \right) \right]^+ \\ &= \left[\ln\left(P_b^{\max}\right) + \ln\left(\frac{P_e^{\max}-\tilde{P}_e}{P_e^{\max}\tilde{P}_e} \right) \right]^+ \\ &= \left[\ln\left(P_b^{\max}\right) - \ln\left(\tilde{P}_e\right) - \ln\left(\frac{P_e^{\max}}{P_e^{\max}-\tilde{P}_e} \right) \right]^+ . \end{aligned} \tag{11}$$

In this case, one can observe that C_s^{a*} is smaller than its general upper bound $C_{s,\mathrm{UB}}^{a*}$. That is, C_s^{a*} cannot reach the

[2] This is actually the upper bound of the optimal secure capacity.

upper bound even if *Alice* has the largest adjustability with the loss of $\ln\left(\frac{P_e^{\max}}{P_e^{\max}-\tilde{P}_e}\right)$. Note that the loss depends on the ratio between $\tilde{P}_e$ and $P_e^{\max}$. Therefore, in this case, even if *Eve* has a much more advantageous angular position than *Bob* for receiving the signal from *Alice* (i.e., $P_e^{\max} \gg P_b^{\max}$), the maximum achievable secure capacity can be close to the theoretical upper bound by limiting $\tilde{P}_e$.

Fig. 5 shows the optimal secure capacity when the condition $(\alpha_e + \theta_d - \alpha_b) = \pi/2$ is satisfied with the angular positions of the coils, as shown in Fig. 6. The detailed parameters of Fig. 5 are $P_a = 1$, $H_b = H_e = 1$, and $N_0 = 10^{-3}$. Our approximation result C_s^{a*} is accurate and identical to the result of C_s^* when N_0 is much smaller then P_a. To be specific, when $\tilde{P}_e$ is relatively smaller than $P_e^{\max}$ (i.e., $\tilde{P}_e < 0.1P_e^{\max}$), C_s^{a*} is very close to $C_{s,\mathrm{UB}}^{a*}$. Therefore, the secure capacity of the system almost reaches the theoretical upper bound $C_{s,\mathrm{UB}}^{a*}$ when *Eve* requires relatively small power P_e with the condition $(\alpha_e + \theta_d - \alpha_b) = \pi/2$.

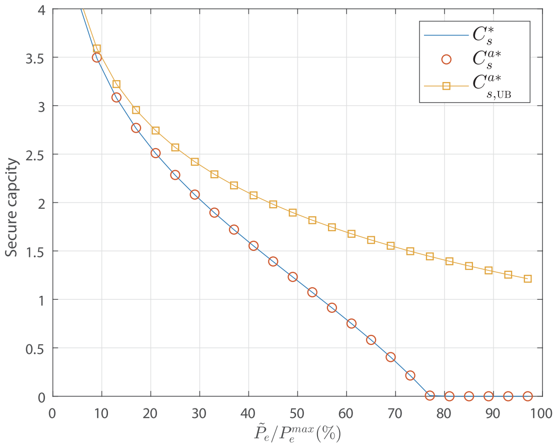


FIGURE 5. Optimal secure capacity when *Alice* has the largest adjustability, where $\alpha_e + \theta_d - \alpha_b = \pi/2$, $\theta_b = \pi/2$, $\theta_e = \pi/11$, $P_a = 1$, $H_b = H_e = 1$, and $N_0 = 10^{-3}$.

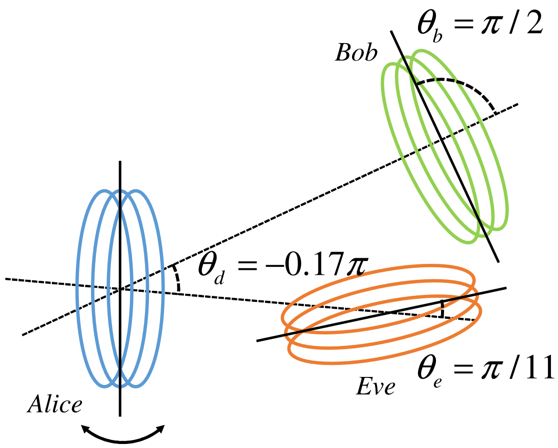


FIGURE 6. Example case of angular positions of coils when *Alice* has the largest adjustability, where $\alpha_e + \theta_d - \alpha_b = \pi/2$, $\theta_b = \pi/2$, $\theta_e = \pi/11$, $P_a = 1$, $H_b = H_e = 1$, and $N_0 = 10^{-3}$.

2) SPECIAL CASE 2: $(\alpha_e + \theta_d - \alpha_b) = 0$

By substituting $(\alpha_e + \theta_d - \alpha_b) = 0$ to (6), we have

$$C_s^a = \left[\ln\left(\frac{P_b^{\max}\cos^2(\theta_{ab}-\alpha_b)}{P_e^{\max}\cos^2(\theta_{ab}-\alpha_b)}\right)\right]^+. \tag{12}$$

In this case, *Alice* has no adjustability of the ratio between information and power transfer rate because the phase of the numerator and denominator are the same, i.e., constant C_s^{a*} irrespective of θ_{ab}. Moreover, since $(\alpha_e + \theta_d - \alpha_b) = 0$, C_s^{a*} is

$$\begin{aligned} C_s^{a*} &= \left[\ln\left(\frac{P_b^{\max}\cos^2\left(\arccos\left(\sqrt{\frac{\tilde{P}_e}{P_e^{\max}}}\right)\right)}{\tilde{P}_e}\right)\right]^+ \\ &= \left[\ln\left(\frac{P_b^{\max}\frac{\tilde{P}_e}{P_e^{\max}}}{\tilde{P}_e}\right)\right]^+ \\ &= \left[\ln\left(P_b^{\max}\right) - \ln\left(P_e^{\max}\right)\right]^+ \end{aligned} \tag{13}$$

In this case, C_s^{a*} does not depend on $\tilde{P}_e$, and thus $\tilde{P}_e$ does not affect the secure capacity. Note that in this case C_s^{a*} is still smaller than the upper bound $C_{s,\mathrm{UB}}^{a*}$ because $P_e^{\max} \geq \tilde{P}_e$.

Fig. 7 shows the secure capacity when $(\alpha_e + \theta_d - \alpha_b) = 0$ with the angular positions of the coils shown in Fig. 8. In Fig. 7, P_a, $H_b = H_e$, and N_0 are set as 1, 1, and 10^{-3}, respectively. Since the gap between C_s^{a*} and C_s^* is negligible, our approximation-based analysis is accurate in a high SNR environment with this condition. In Fig. 7, C_s^{a*} is constant because C_s^{a*} is only affected by $P_e^{\max}$. However, as $\tilde{P}_e$ increases, the upper bound $C_{s,\mathrm{UB}}^{a*}$ decreases, and $C_{s,\mathrm{UB}}^{a*}$ converges to C_s^{0*} when $\tilde{P}_e = P_e^{\max}$. This case shows that the secure capacity is much lower than its upper bound for a small $\tilde{P}_e$, but the secured transmission is steadily available regardless of $\tilde{P}_e$.

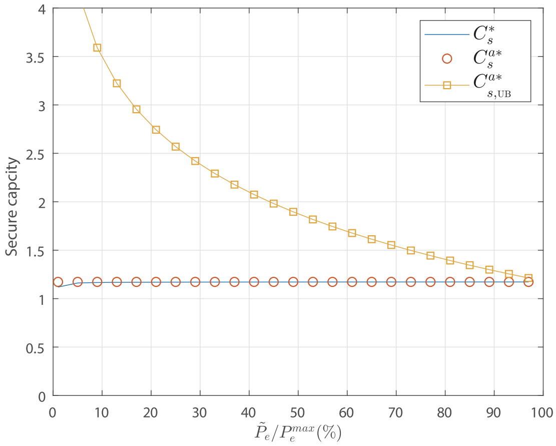


FIGURE 7. Optimal secure capacity when *Alice* has no largest adjustability, where $\alpha_e + \theta_d - \alpha_b = 0$, $\theta_b = \pi/2$, $\theta_e = \pi/11$, $P_a = 1$, $H_b = H_e = 1$, and $N_0 = 10^{-3}$.

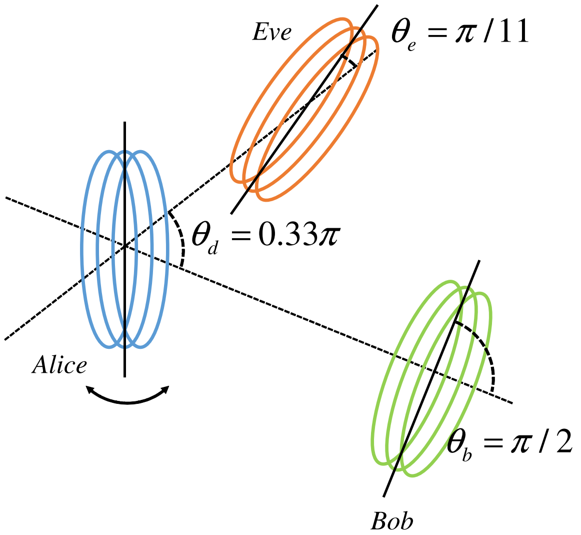


FIGURE 8. Example case of angular positions of coils when *Alice* has no adjustability, where $\alpha_e + \theta_d - \alpha_b = \pi/2$, $\theta_b = \pi/2$, $\theta_e = \pi/11$, $P_a = 1$, $H_b = H_e = 1$, and $N_0 = 10^{-3}$.

As observed in Fig. 5 and Fig. 7, the secure capacity has a completely distinct tendency for both special cases. When $(\alpha_e + \theta_d - \alpha_b) = \pi/2$, the optimal secure capacity is high and close to the upper bound for small $\tilde{P}_e$ with high sensitivity to $\tilde{P}_e$. When $(\alpha_e + \theta_d - \alpha_b) = 0$, however, the optimal secure capacity is constant with $\tilde{P}_e$ and close to the upper bound for a large $\tilde{P}_e$. Therefore, when $(\alpha_e + \theta_d - \alpha_b) = \pi/2$, $\tilde{P}_e$ should be a small value to make C_s^{a*} be close to the upper bound of the secure capacity. When $(\alpha_e + \theta_d - \alpha_b) = 0$, however, $\tilde{P}_e$ should be a large value for the better security and power transfer performance. Since $(\alpha_e + \theta_d - \alpha_b)$ is nor 0 nor $\pi/2$ in general, the optimal secure capacity has a mixed tendency between those of special case 1 and 2, e.g., different sensitivity to $\tilde{P}_e$ and θ_{ab}.

B. LIMITED KNOWLEDGE OF ANGULAR POSITIONS

The angular position of the coils cannot be fixed in a practical environment. For example, even small hand movement of the user may cause a significant fluctuation of the angular positions of the receiver coils. In such circumstances, *Alice* has only limited information about instantaneous angular positions of the receiver coils. In this subsection, we discuss the secure capacity for the case shown in Fig. 9. To be specific, we assume that *Alice* only knows θ_{ab}, θ_{ae}, Φ_b, and Φ_e, where Φ_b and Φ_e represent the maximum range of angular fluctuation of the coils of *Bob* and *Eve*, respectively.

To represent the angular fluctuation of the receiver coils, we assume that θ_b and θ_e are random variables that follow

$$\begin{aligned} \mathcal{U}_b &\sim \mathcal{U}\left(\beta_b - \Phi_b, \beta_b + \Phi_b\right), \\ \mathcal{U}_e &\sim \mathcal{U}\left(\beta_e - \Phi_e, \beta_e + \Phi_e\right), \end{aligned} \tag{14}$$

respectively, where $\beta_b = \arctan\left(2\tan\left(\theta_{ab}\right)\right)$, $\beta_e = \arctan\left(2\tan\left(\theta_{ae}\right)\right)$, and $\mathcal{U}\left(a, b\right)$ is the continuous uniform distributions of which the minimum and maximum values are a and b, respectively. When θ_{ab} is given, the angular coefficients of *Alice-Bob* and *Alice-Eve* links are alternatively expressed (see the third line of (1)) as

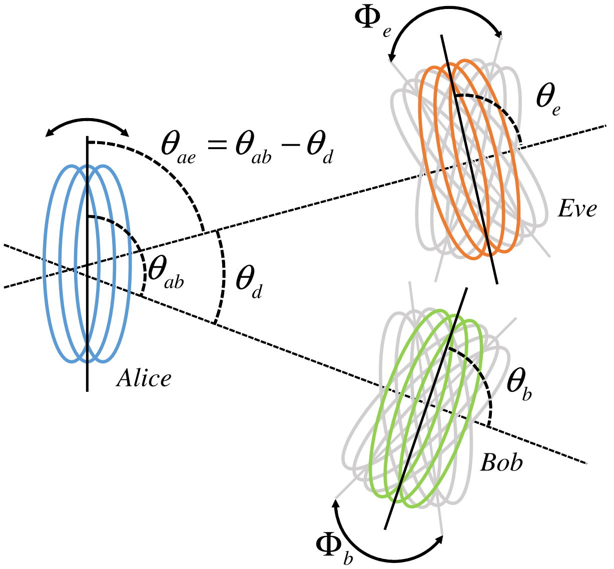


FIGURE 9. Magnetic wiretap channel model with angular fluctuation of receiver coils.

$$\begin{aligned} J_b &= \sqrt{4\sin^2(\theta_{ab}) + \cos^2(\theta_{ab})}\cos(\theta_b - \beta_b), \\ J_e &= \sqrt{4\sin^2(\theta_{ae}) + \cos^2(\theta_{ae})}\cos(\theta_e - \beta_e). \end{aligned} \tag{15}$$

Since J_b and J_e are maximized when $\theta_b = \beta_b$, $\theta_e = \beta_e$, respectively, β_b and β_e are the best angular positions for the receiving power from *Alice*. Note that the means of $\mathcal{U}_b$ and $\mathcal{U}_e$ are β_b and β_e, respectively. Therefore, the angular positions of the receiver coils are fluctuating with the center of the best angular position. In addition, smaller Φ_b and Φ_e indicate that each receiver can control its angular position exactly. When the random variable Y follows the distribution $\mathcal{U}(-y, y)$, the probability distribution function of $X = \cos^2(Y)$ is

$$f_X(x) = \frac{1}{2y\sqrt{x - x^2}}. \tag{16}$$

By using (16), the mean received power of *Eve* $E\left[P_e\right]$ is derived as

$$\begin{aligned} E\left[P_e\right] &= H_e P_a E_{J_b}\left[J_b^2\right] \\ &= \left(4\sin^2(\theta_{ae}) + \cos^2(\theta_{ae})\right) H_e P_a \\ &\quad \cdot \underset{\beta_e - \Phi_e \le \theta_e \le \beta_e + \Phi_e}{E_{\theta_e}}\left[\cos^2(\theta_e - \beta_e)\right] \\ &= \left(4\sin^2(\theta_{ae}) + \cos^2(\theta_{ae})\right) H_e P_a \\ &\quad \cdot \int_{\cos^2(\Phi_e)}^{1} \frac{x}{2\Phi_e\sqrt{x - x^2}} dx \\ &= \left(1 + 3\sin^2(\theta_{ae})\right) H_e P_a \\ &\quad \cdot \left(0.5\cos(\Phi_e)\sin(\Phi_e)\Phi_e^{-1} + 0.5\right). \end{aligned} \tag{17}$$

When the angular position of *Eve* is completely random, i.e., $\Phi_e = \pi/2$, then $E\left[P_e\right]$ is equal to $0.5\left(1+3\sin^2(\theta_{ae})\right)H_eP_a$ (see (17)).[3] In addition, since $\left(1+3\sin^2(\theta_{ae})\right) \geq 1$, $E\left[P_e\right]$ is larger than $0.5H_eP_a$ regardless of Φ_e and θ_{ab}.

Fig. 10 shows the analysis and simulation results of $E\left[P_e\right]$ in various θ_{ae} and Φ_e environments. When the angular position of *Eve* is completely random ($\Phi_e = \pi/2$), $E\left[P_e\right]$ is halved compared to the case where the angular position of *Eve* is optimally fixed ($\Phi_e = 0$). In addition, in the case of the worst environment ($\theta_{ae} = 0$, $\Phi_e = \pi/2$), $E\left[P_e\right]$ is not lower than $0.5\,(= 0.5H_eP_a)$. Fig. 11 is a contour plot of $E\left[P_e\right]$ with gradient arrows where the numbers in the plot are the values of $E\left[P_e\right]$. When θ_{ae} is not close to $\pi/2$, $E\left[P_e\right]$ is more sensitive to θ_{ae} than Φ_e. Therefore, the increment of angular fluctuation of *Eve* does not greatly decrease $E\left[P_e\right]$ except the case where the angular position of *Alice* is advantageously set to *Eve*, such that $\theta_{ae} \simeq \pi/2$.

[3] This value is identical with half of received power when there is no angular fluctuation of *Eve*.

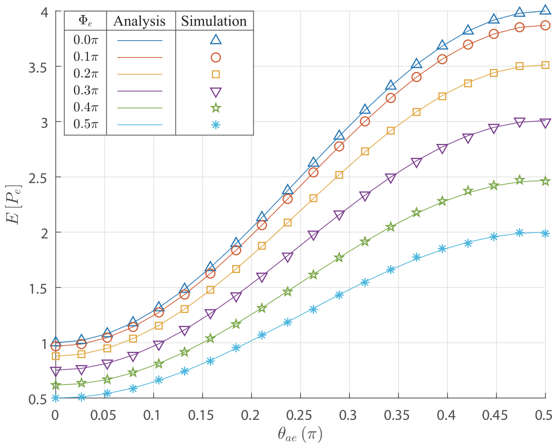


FIGURE 10. Analysis and simulation results of $E\left[P_e\right]$ when $H_e = 1$ and $P_a = 1$.

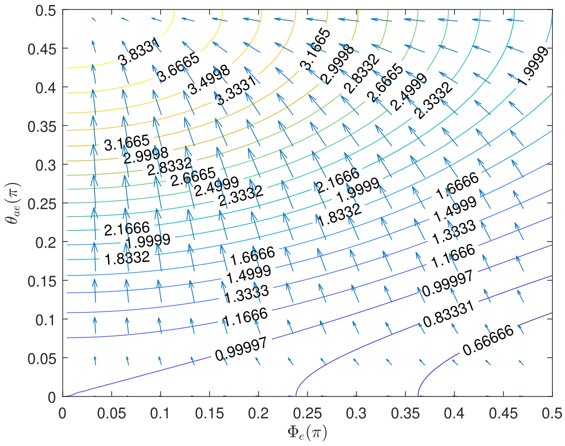


FIGURE 11. Contour plot of $E\left[P_e\right]$ with gradient arrows when $H_e = 1$ and $P_a = 1$.

Since the secure capacity is defined as (5), the mean secure capacity is

$$E\left[C_s\right] = E_{P_b,P_e}\left[\left[\ln\left(1+\frac{P_b}{N_0}\right) - \ln\left(1+\frac{P_e}{N_0}\right)\right]^+\right]. \tag{18}$$

Since the angular position of *Bob* and *Eve* are independent and $[\cdot]^+$ is a convex function, (18) is lower bounded as

$$\begin{aligned} E\left[C_s\right] &\geq \left[E_{P_b,P_e}\left[\ln\left(1+\frac{P_b}{N_0}\right) - \ln\left(1+\frac{P_e}{N_0}\right)\right]\right]^+ \\ &= \left[E_{P_b}\left[\ln\left(1+\frac{P_b}{N_0}\right)\right] - E_{P_e}\left[\ln\left(1+\frac{P_e}{N_0}\right)\right]\right]^+. \end{aligned} \tag{19}$$

The first term of the second line of (19) can be rewritten as

$$\begin{aligned} &E_{P_b}\left[\ln\left(1+\frac{P_b}{N_0}\right)\right] \\ &\quad = E_{J_b}\left[\ln\left(1+\frac{H_bP_a\lambda_{\theta_{ab}}J_b^2}{N_0}\right)\right] \\ &\quad = E_{\theta_b}\left[\ln\left(1+\frac{H_bP_a\lambda_{\theta_{ab}}\cos^2(\theta_b-\beta_b)}{N_0}\right)\right] \\ &\quad = \int_{\cos^2(\Phi_b)}^{1} \ln\left(1+\frac{H_bP_a\lambda_{\theta_{ab}}x}{N_0}\right)\frac{1}{2\Phi_b\sqrt{x-x^2}}dx \\ &\quad = -\ln\left(1+\frac{H_bP_a\lambda_{\theta_{ab}}x}{N_0}\right)\frac{\ln\left(\sqrt{x-1}+\sqrt{x}\right)}{i\Phi_b}\Bigg|_{\cos^2(\Phi_b)}^{1} \\ &\qquad + \int_{\cos^2(\Phi_b)}^{1}\frac{H_bP_a\lambda_{\theta_{ab}}}{N_0+H_bP_a\lambda_{\theta_{ab}}}\frac{\ln\left(\sqrt{x-1}+\sqrt{x}\right)}{i\Phi_b}dx, \end{aligned} \tag{20}$$

where $\lambda_{\theta_{ab}} = 1+3\sin^2\theta_{ab}$. The integration in the last line of (20) can be expressed in a complicated form with a logarithmic integral function by tedious calculation, and thus we can obtain the result of (20) without a full numerical integration or a complicated simulation. The mean secure capacity $E\left[C_s\right]$ in (19) is lower bounded as

$$\begin{aligned} &E\left[C_s\right] \\ &\quad \geq \zeta_{H_b,P_a}\left(\theta_{ab},\Phi_b\right) - \zeta_{H_e,P_a}\left(\theta_{ae},\Phi_e\right) \\ &\quad = \Bigg[-\ln\left(1+\frac{H_bP_a\lambda_{\theta_{ab}}x}{N_0}\right)\frac{\ln\left(\sqrt{x-1}+\sqrt{x}\right)}{i\Phi_b}\Bigg|_{\cos^2(\Phi_b)}^{1} \\ &\qquad + \int_{\cos^2(\Phi_b)}^{1}\frac{H_bP_a\lambda_{\theta_{ab}}}{N_0+H_bP_a\lambda_{\theta_{ab}}}\frac{\ln\left(\sqrt{x-1}+\sqrt{x}\right)}{i\Phi_b}dx \\ &\qquad + \ln\left(1+\frac{H_eP_a\lambda_{\theta_{ae}}x}{N_0}\right)\frac{\ln\left(\sqrt{x-1}+\sqrt{x}\right)}{i\Phi_e}\Bigg|_{\cos^2(\Phi_e)}^{1} \\ &\qquad - \int_{\cos^2(\Phi_{\theta_{ae}})}^{1}\frac{H_eP_a\lambda_{\theta_{ae}}}{N_0+H_eP_a\lambda_e}\frac{\ln\left(\sqrt{x-1}+\sqrt{x}\right)}{i\Phi_e}dx\Bigg]^+, \end{aligned} \tag{21}$$

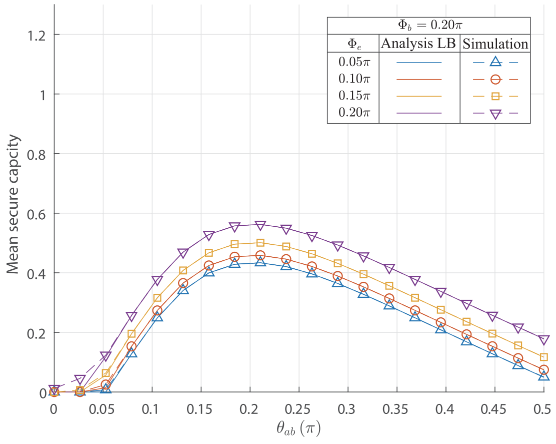


FIGURE 12. $E[C_s]$ **with analytical lower bounds when** $\theta_d = 0.10\pi$, $\Phi_b = 0.20\pi$, $P_a = 1$, $H_b = H_e = 1$, **and** $N_0 = 10^{-3}$.

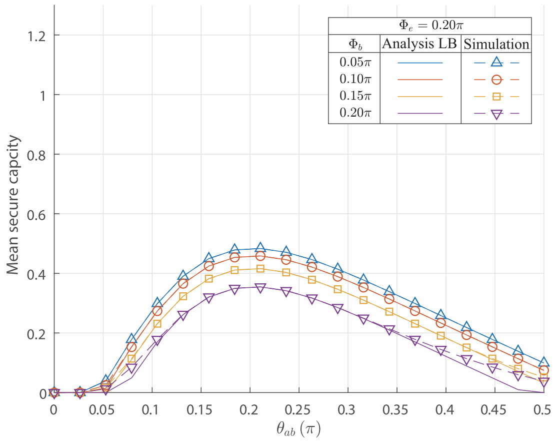


FIGURE 13. $E[C_s]$ **with analytical lower bounds when** $\theta_d = 0.10\pi$, $\Phi_e = 0.20\pi$, $P_a = 1$, $H_b = H_e = 1$, **and** $N_0 = 10^{-3}$.

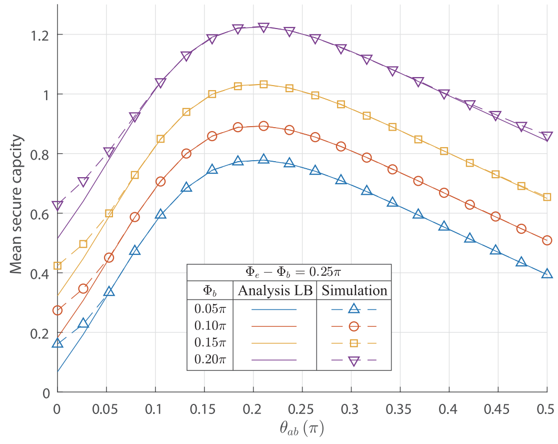


FIGURE 14. $E[C_s]$ **with analytical lower bounds when** $\theta_d = 0.10\pi$, $\Phi_e - \Phi_b = 0.25\pi$, $P_a = 1$, $H_b = H_e = 1$, **and** $N_0 = 10^{-3}$.

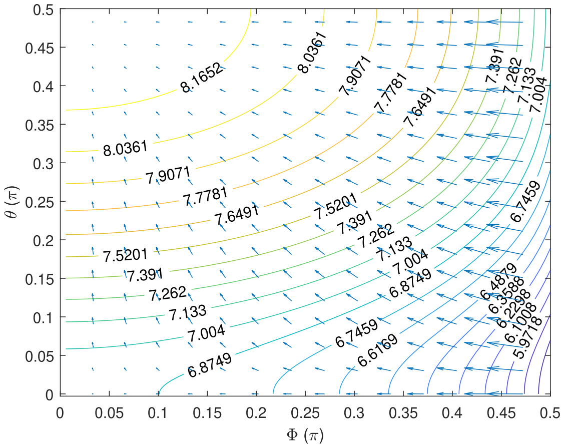


FIGURE 15. **Contour plot of** $\zeta_{H,P}(\theta,\Phi)$ **with gradient arrows when** $H = 1$, $P = 1$, **and** $N_0 = 10^{-3}$.

where

$$\zeta_{H,P}(\theta,\Phi) \triangleq -\ln\left(1+\frac{HP\lambda_\theta x}{N_0}\right)\frac{\ln\left(\sqrt{x-1}+\sqrt{x}\right)}{i\Phi}\Bigg|_{\cos^2(\Phi)}^{1} + \int_{\cos^2(\Phi)}^{1}\frac{HP\lambda_\theta}{N_0+HP\lambda_\theta}\frac{\ln\left(\sqrt{x-1}+\sqrt{x}\right)}{i\Phi}dx, \qquad (22)$$

and $\lambda_\theta = 1 + 3\sin^2\theta$.

Fig. 12 to 14 and 16 show the mean secure capacity $E[C_s]$ with analytical lower bounds. For the simulation, P_s, $H_b\ (= H_e)$, and N_0 are set as 1, 1, and 10^{-3}, respectively. In most ranges, the lower bound matches the simulation results. Even if there are some gaps between the simulation results and the lower bound, the lower bound tracks tendency of the simulation results well. Therefore, we can expect the effect of θ_{ab} on $E[C_s]$ with the lower bound, and thus the optimal θ_{ab} can be determined without intensive simulation. The effect of Φ_e and Φ_b on $E[C_s]$ is investigated in Fig. 12 to 14. As shown in Fig. 12, a larger Φ_e makes a higher $E[C_s]$. In contrast, a smaller Φ_b brings the better mean secure capacity shown in Fig. 13. That means that the angular position uncertainty of *Eve* improves the security, while the angular position uncertainty of *Bob* degrades the security. Interestingly, when $\Phi_e - \Phi_b$ is a constant, a larger angular position uncertainty of the receiver coils improves $E[C_s]$. In Fig. 14, where $\Phi_e - \Phi_b = 0.25\pi$, $E[C_s]$ is improved by about 0.4 when $\Phi_b = 0.20\pi$ compared with the case of $\Phi_b = 0.05\pi$. Since $E[C_s] \geq \left(\zeta_{H_b,P_a}(\theta_{ab},\Phi_b) - \zeta_{H_e,P_a}(\theta_{ae},\Phi_e)\right)$, the reason of the above is figured out by Fig. 15 which shows the contour plot of $\zeta_{H,P}(\theta,\Phi)$. In Fig. 15, the magnitude of the gradient becomes higher when Φ is close to 0.5π. Therefore, the value of $\left(\zeta_{H,P}(0.1\pi, 0\pi) - \zeta_{H,P}(0.1\pi, 0.1\pi)\right)$ is much smaller than $\left(\zeta_{H,P}(0.1\pi, 0.4\pi) - \zeta_{H,P}(0.1\pi, 0.5\pi)\right)$. Consequently, greater angular fluctuation of the receiver coils is better for security when $\Phi_e - \Phi_b$ is constant.

The effect of θ_d on $E[C_s]$ can be investigated by Fig. 12. Since θ_d is the angle between *Bob* and *Eve*, as shown in Fig. 9, a larger θ_d indicates larger separation between *Bob* and *Eve*. Obviously, when *Bob* and *Eve* are sufficiently separated,

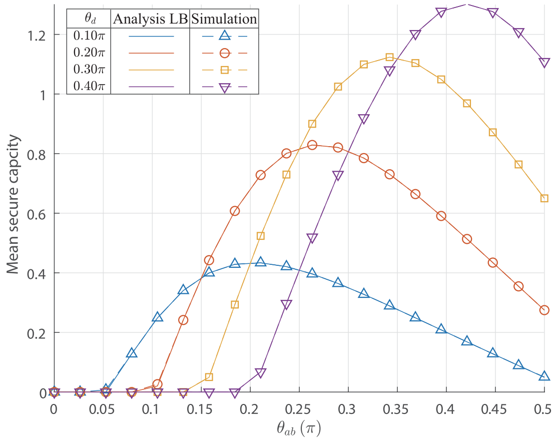


FIGURE 16. $E\,[C_s]$ **with analytical lower bounds when** $\Phi_e = 0.05\pi$, $\Phi_b = 0.05\pi$, $P_a = 1$, $H_b = H_e = 1$, **and** $N_0 = 10^{-3}$.

Alice has large adjustability of the ratio between information and power transfer rate, and thus secure capacity is improved. In addition, the value of θ_{ab} that corresponds to the peak of $E\,[C_s]$ is moved by θ_d.

IV. CONCLUSION

In this paper, we study a MIC-based SWIPT system in the aspect of PLS using the secure capacity. When the location and angular positions of information and potential eavesdropping power receivers are given, a transmitter can maximize the secure capacity by appropriately adjusting its angular position with a minimum power transfer constraint to the potential eavesdropping receiver. In addition, we provide some intuition about the secure capacity of a MIC-based SWIPT system using two special cases. Furthermore, we also derive the mean secure capacity and received power when the transmitter has limited information about the angular positions of the receivers because the angular positions of the receiver coils are fluctuating due to movements and practical errors. The secure capacity increases when the angular fluctuation of *Eve* increases, and/or the fluctuation of *Bob* decreases. For future work, our results can be extended to multi-coil environments, that is, multiple power and information receivers.

REFERENCES

[1] A. Alzahrani, A. Alqhtani, H. Elmiligi, F. Gebali, and M. S. Yasein, "NFC security analysis and vulnerabilities in healthcare applications," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process. (PACRIM)*, Aug. 2013, pp. 302–305.

[2] N. Akinyokun and V. Teague, "Security and privacy implications of NFC-enabled contactless payment systems," in *Proc. Int. Conf. Availability, Rel. Secur.*, 2017, p. 47.

[3] C. Kumar and H. Kour, "Security technique in NFC: A review," *Int. J. Mod. Comput. Sci. Appl.*, vol. 5, no. 1, pp. 39–43, 2017.

[4] C.-H. Chen and I.-C. Lin, "NFC attacks analysis and survey," in *Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, 2014, pp. 458–462.

[5] Y. Wang, C. Hahn, and K. Sutrave, "Mobile payment security, threats, and challenges," in *Proc. Int. Conf. Mobile Secure Services (MobiSecServ)*, 2016, pp. 1–5.

[6] S. Kisseleff, I. Akyildiz, and W. Gerstacker, "Magnetic induction-based simultaneous wirelss information and power transfer for single information and multiple power receivers," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1396–1410, Mar. 2017.

[7] S. M. Shariati, A. Abouzarjomehri, and M. H. Ahmadzadegan, "Investigating NFC technology from the perspective of security, analysis of attacks and existing risk," in *Proc. Int. Conf. Knowl.-Based Eng. Innov. (KBEI)*, 2015, pp. 1083–1087.

[8] J. Xu, K. Xue, Q. Yang, and P. Hong, "PSAP: Pseudonym-based secure authentication protocol for NFC applications," *IEEE Trans. Consum. Electron.*, vol. 64, no. 1, pp. 83–91, Mar. 2018.

[9] S. Ghosh, A. Majumder, J. Goswami, A. Kumar, S. P. Mohanty, and B. K. Bhattacharyya, "Swing-pay: One card meets all user payment and identity needs: A digital card module using NFC and biometric authentication for peer-to-peer payment," *IEEE Consum. Electron. Mag.*, vol. 6, no. 1, pp. 82–93, Jan. 2017.

[10] A. Majumder, J. Goswami, S. Ghosh, R. Shrivastawa, S. P. Mohanty, and B. K. Bhattacharyya, "Pay-cloak: A biometric back cover for smartphones: Facilitating secure contactless payments and identity virtualization at low cost to end users," *IEEE Consum. Electron. Mag.*, vol. 6, no. 2, pp. 78–88, Apr. 2017.

[11] H. Eun, H. Lee, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," *IEEE Trans. Consum. Electron.*, vol. 59, no. 1, pp. 153–160, Feb. 2013.

[12] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[13] H.-J. Kim, H. Hirayama, S. Kim, K. J. Han, R. Zhang, and J.-W. Choi, "Review of near-field wireless power and communication for biomedical applications," *IEEE Access*, vol. 5, no. 1, pp. 21264–21285, 2017.

[14] H. Sun, H. Lin, F. Zhu, and F. Gao, "Magnetic resonant beamforming for secured wireless power transfer," *IEEE Signal Process. Lett.*, vol. 24, no. 8, pp. 1173–1177, Aug. 2017.

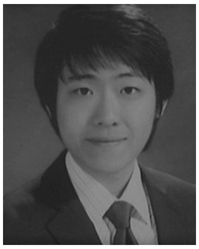
[15] K. Kim, H.-J. Kim, and J.-W. Choi, "Magnetic beamforming with non-coupling coil pattern for high efficiency and long distance wireless power transfer," in *Proc. IEEE Wireless Power Transf. Conf. (WPTC)*, May 2017, pp. 1–4.

[16] H.-J. Kim, J. Park, K.-S. Oh, J. P. Choi, J. E. Jang, and J.-W. Choi, "Near-field magnetic induction MIMO communication using heterogeneous multipole loop antenna array for higher data rate transmission," *IEEE Trans. Antennas Propag.*, vol. 64, no. 5, pp. 1952–1962, May 2016.

[17] S. Kisseleff, I. F. Akyildiz, and W. H. Gerstacker, "Throughput of the magnetic induction based wireless underground sensor networks: Key optimization techniques," *IEEE Trans. Commun.*, vol. 62, no. 12, pp. 4426–4439, Dec. 2014.

[18] J. Y. Ryu, J. Lee, and T. Q. S. Quek, "Transmission strategy against opportunistic attack for MISO secure channels," *IEEE Commun. Lett.*, vol. 20, no. 11, pp. 2304–2307, Nov. 2016.

SUNGMIN HAN (S'13) received the B.S. degree in electronics engineering from the Korea University of Technology and Education, Cheonan, in 2012. He is currently pursuing the Ph.D. degree with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, South Korea. His research areas are communication theory and communication networks.



HAN-JOON KIM (S'15) received the B.S. and M.S. degrees in information control and instrumentation engineering from Kwangwoon University, Seoul, South Korea, in 2011 and 2013, respectively. He is currently pursuing the Ph.D. degree in information and communication engineering with the Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea. His research interests include magnetic communication, wireless power transfer, and transcranial magnetic stimulation.

JAESEOK LEE received the B.S. and Ph.D. degrees in radio communication engineering from Korea University, Seoul, South Korea, in 2008 and 2015, respectively. In 2015, he was a Research Engineer with the Institute of New Media and Communications, Seoul National University, Seoul, and from 2015 and 2017, he was a Research Fellow with the Information and Communication Engineering Department, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea. He is currently a Senior Engineer with Hanwha Systems, Yongin, Gyeonggi-do, South Korea. His research interests include the sparse signal recovery, compressed sensing theory, and active electronically scanned array radar signal processing.

JI-WOONG CHOI (S'00–M'04–SM'09) received the B.S., M.S., and Ph.D. degrees from Seoul National University (SNU), Seoul, South Korea, in 1998, 2000, and 2004, respectively, all in electrical engineering. From 2004 to 2005, he was a Post-Doctoral Researcher with the Inter-University Semiconductor Research Center, SNU. From 2005 to 2007, he was a Post-Doctoral Visiting Scholar with the Department of Electrical Engineering, Stanford University, Stanford, CA, USA. He was also a Consultant with GCT Semiconductor, San Jose, CA, USA, for development of mobile TV receivers, from 2006 to 2007. From 2007 to 2010, he was with Marvell Semiconductor, Santa Clara, CA, USA, as a Staff Systems Engineer for next-generation wireless communication systems, including WiMAX and LTE. Since 2010, he has been with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea, as an Associate Professor. His research interests include wireless communication theory, signal processing, biomedical communication applications, and brain machine interface.