Impact of Mobility on Physical Layer Security over Wireless Fading Channels

Jie Tang, Monireh Dabaghchian, Kai Zeng, Hong Wen

***Abstract*—Wireless physical layer security has attracted great attention in recent years. Although mobility is an intrinsic property of wireless networks, most of the existing works only consider static scenarios and the impact of mobility on wireless physical layer security is not well understood. To fill this gap, in this paper, we investigate physical layer security in the scenario with a random mobile receiver under Rayleigh fading channel. We consider a common scenario where a base station (BS) or access point (AP) communicates to a random mobile receiver with a passive eavesdropper in a circular region. The secrecy performance under three typical random mobility models are studied: random waypoint model (RWP), random direction model (RD), and border move model (BM). We investigate the secrecy characteristics of mobile user under steady state running and provide a general analytical framework for computing the ergodic secrecy capacity (ESC). We derive tractable closed-form expressions of positive secrecy capacity probability (PSCP) and secrecy outage probability (SOP) for RWP and RD mobility users, respectively. By comparing secrecy performance of mobility with static case, we find that RWP mobile user can achieve much better secrecy performance than the others. We then investigate the secrecy performance of RWP mobile user with pause time. Furthermore, two types of secrecy improvement strategies for random mobile users are proposed. In the first strategy, a transmit subcell for RWP users is bounded. We allow the transmitter to communicate with the mobile user only when he is moving within the subcell. In the other strategy, the transmitter is turned on only when the evaluated secrecy performance reaches to a required level. We strike a good tradeoff between secrecy improvement and transmit outage probability. Extensive simulation results validate our theoretical analysis. Finally, we extend our framework to other realistic scenarios, including nodes moving in other shapes of areas, and multiple non-cooperative and cooperative eavesdroppers.**

***Index Terms*—Physical layer security, mobility, random mobility models, secrecy capacity, secrecy outage probability.**

I. Introduction

Wireless physical layer security is a promising technique to directly leverage the unique properties of the wireless medium or radio to enhance the wireless network security [1–4]. It can be applied to various wireless networks, such as WiFi, cellular, sensor and vehicular networks [5, 6]. During the past decades, physical layer security has been widely investigated since Wyner proposed the wiretap channel model [7]. For Rayleigh fading wiretap channel, the secrecy outage probability (SOP) was defined and the ergodic secrecy capacity [8] [9] was considered to describe the average secrecy capacity when the eavesdropper's channel state information (CSI) is unknown to legitimate users. Recently, there has been a growing interest in studying the impact of large scale path loss and small scale channel fading on physical layer secrecy [10–15]. The challenge in taking the path loss factor into consideration for the physical layer secrecy lies in that the location of the passive eavesdropper is unknown to legitimate users. The stochastic geometry theory [16] is used as an effective mathematical tool to model the random location and the number of nodes (i.e., legitimate and eavesdropping nodes) in the networks [10–15].

Most existing works only study the physical layer secrecy under static scenarios. The distance between the transmitter and receivers is assumed to be fixed and time-invariant[8, 10–15]. However, in many scenarios of wireless networks, the users can be mobile, e.g., cellular users walking on the street or riding on a bus, or students walking on a campus while connecting with campus WiFi networks. In this paper, to fill this gap, we investigate the impact of mobility on physical layer security. We consider a random mobile user with a passive eavesdropper in a circular region. In this mobile scenario, the secrecy capacity will be fluctuating inevitably with the change of node's locations. For a random mobile receiver, we investigate the secrecy characteristics under steady state running, and consider both large scale path loss and small-scale fading factors.

We summarize our main contributions as follows:

- We investigate the physical layer security with mobile users under three typical random mobility models (RWP, RD, and BM). We derive the closed-form expressions of positive secrecy capacity probability (PSCP) and secrecy outage probability (SOP) for RWP and RD mobile users in steady state running, under Rayleigh fading channel. For RWP mobile user, we derive two concise tractable closed form expressions of PSCP and SOP. Further results are derived from the RWP spatial node distance probability density distribution function (SPDF) of E. Hyytia (HC) [17] and C. Bettstetter (CB) [18].
- We provide a general analytical framework to compute the ergodic secrecy capacity (ESC) for the random mobile receivers. Based on the framework, we compare the secrecy performances of the three mobility models with classic mean static (MS) node distribution [13].
- We analyze the secrecy performance for RWP mobile receiver with running pause time. Furthermore, we pro-

Jie Tang is with University of Electronic Science and Technology of China. He is also a visiting researcher at George Mason University, Fairfax, U.S.A (e-mail: cs.tan@163.com).

Monireh Dabaghchian and Kai Zeng are with George Mason University, Fairfax, U.S.A. Kai Zeng ✉ is the corresponding author (e-mail: mdabaghc@masonlive.gmu.edu; kzeng2@gmu.edu;).

Hong Wen is with University of Electronic Science and Technology of China (e-mail: sunlike@uestc.edu.cn).

Manuscript received July 29, 2017; revised November 22, 2017 and May 14, 2018; accepted August 14, 2018

pose two types of secrecy improvement strategies for random mobile users. In the first strategy, we define a transmit subcell for the random mobile user and allow the transmitter to communicate with the mobile user only when he is moving within the subcell. In the second strategy, the transmitter only sends secret information when the evaluated secrecy performance reaches to a required level. We investigate the transmit outage probability for the mobile user and compare the secrecy improvement introduced by both strategies.

- Finally, we discuss the future trends and extend our framework to other realistic scenarios, including nodes moving in other shape areas, and multiple non-cooperative and cooperative eavesdroppers.

Through our study, we have the following findings:

- By comparing the secrecy performance of three types of mobility users with mean static (MS) scenario [13], our simulation and numerical results verify that the RWP mobile user can achieve significantly better secrecy performance than the others. Furthermore, the secrecy performance of the RD mobile user is very close to the MS scenario. The BM mobile user has the worst secrecy performance. The path loss exponent and the ratio of transmit power to region radius are the key factors to affect the secrecy performance.
- By investigating the case of RWP mobile user with pause time, we find that pause time degrades the secrecy performance. The RWP user who keeps moving without pause can achieve higher secrecy performance than the user with pause time. When the pause time becomes larger, the secrecy performance approaches to the cases of RD and MS scenarios.
- Both of our proposed secrecy improvement strategies can effectively improve secrecy performance of RWP users with low complexity. For an appropriate subcell radius in the first strategy, the RWP user can achieve lower transmit outage probability than the RD user.

The rest of this paper is organized as follows. The related works are discussed in Section II. The system model and problem formulation are proposed in Section III. Section IV analyzes secrecy for random mobile receivers under fading channels and investigates the secrecy of mobile users with running pause time. The simulation results are presented to validate our theoretical analysis. In Section V, two types of secrecy improvement strategies are proposed. We extend the model to the cases of users moving in other shapes of areas, and multiple non-cooperative and cooperative eavesdropping nodes in Section VI. Section VII concludes the work.

II. Related Works

Physical layer security has attracted great attentions in research during the past decades. The wiretap channel under various scenarios has been studied, such as the Gaussian wiretap channels [19], Rayleigh fading channels [8], [20], and the multi-antenna systems [21–24]. A series of physical layer secrecy transmission strategies have been proposed [9], [21], [22], [25], [26].

Recently, there has been a growing interest to comprehensively consider the large scale path loss factor with small scale fading for physical layer security [10–15]. In [27], the authors modeled the geographic distribution of the legitimate transmitter and eavesdropping nodes as two independent Poisson point processes (PPP) to investigate the quality of service (Qos) and SOP for large-scale decentralized wireless networks. [27] utilized a guard zone to stop eavesdroppers from approaching the legitimate nodes, which can improve secrecy performance. Work [11] assumed that the eavesdroppers are uniformly distributed over a ring centered at the base station (BS) and legitimate users' locations are fixed and known to the BS. The authors in [11] presented the closed form expression for SOP when the BS knows the statistical CSI of both legitimate users and eavesdroppers. Work [12] investigated the ergodic secrecy capacity by assuming that both the legitimate and eavesdropping nodes are randomly deployed according to two independent PPP distributions. The protected zones in [12] surrounded by the transmitter and the legitimate nodes were investigated to enhance the secrecy. [10] investigated the secrecy transmission from the BS to the closest PPP distributed legitimate users, under PPP distributed colluding eavesdroppers. The closed-form expressions for SOP at the ith closest legitimate users in Rayleigh fading channel are derived in [10]. Work [13] considered a uniformly distributed user in a circular region and an eavesdropper with fixed distance from the BS. For the downlink and uplink connectivity, [13] investigated the average secrecy capacity under different radius of secrecy guard zone by simulation. However, [13] did not provide exact SOP closed-form expression or any analytical analysis.

For multi-antenna systems, by taking the location and path loss effect of the nodes into consideration, [14] investigated the best antenna placement for eavesdroppers by assuming the uniformly distributed eavesdropper over a ring centered at the BS. The legitimate receiver in [14] is known and with a fixed distance from the transmitter. [15] studied a multi-antenna system in the presence of Poisson distributed eavesdroppers. All of these works consider only static nodes.

For the networks with random mobile nodes, [28] derived the probability density distribution function (PDF) of the received power under the RWP [29] and RD mobility [30] models. The authors derived the mathematical expressions for path loss exponent of 4 in terms of confluent hypergeometric function. In [31], the authors derived the outage probability and average bit error rate (BER) for RWP mobile nodes under the Nakagami-m fading channel. However, all these works only studied received signal quality in random mobile networks [28], [31]. The impact of mobility on physical layer security has not been well studied.

III. System Model and Problem Formulation

A. System Model

The model is illustrated in Fig. 1. We consider three single antenna ends in a circular area with radius R. Alice is the BS or AP located in the center of the circle, communicating with the legitimate user Bob. A passive eavesdropper Eve is located

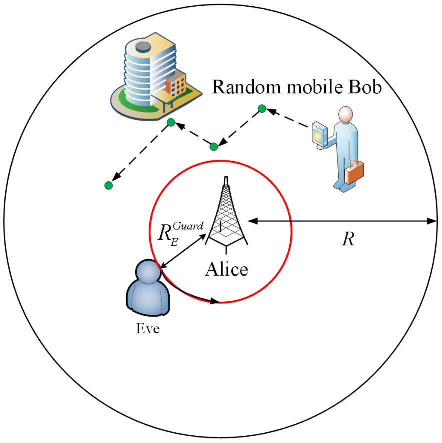


Figure 1: Physical layer security with random mobile receiver Bob

somewhere in the circular region. The legitimate users (Alice and Bob) do not know the exact location of Eve. During the communication period, Bob moves randomly in the circular area. The mobile track of Bob is random and the distance between Bob and Alice is time-varying. We study the secrecy of the mobile receiver under three typical random mobility models [17], [29], [30], which are illustrated below.

RWP mobile Bob: First, Bob randomly chooses a point D_0 in the circular region. Then, he randomly chooses a coordinate D_1 (D_1 is uniformly distributed in the circular area) as his next destination point and moves to it with a constant speed v_1. The speed can be randomly (uniformly) chosen from $[v_{min}, v_{max}]$. After Bob arrives at the destination point D_1, then he may choose to stop for a random pause time $t_{p,1}$ at this point. Also, $t_{p,i}$ $(i = 1, 2, 3...)$ is randomly chosen from $[t_{p,min}$,$t_{p,max}]$. Then, he chooses a new destination D_2 and moves to it with a new speed v_2, and continues this process. The RWP mobility model is a very good model for real world mobile users in a specific region.

RD mobile Bob: Bob randomly starts in D_0 point in the circular region. Then, he randomly chooses a direction θ_1 $(0 \leq \theta_1 \leq 2\pi)$ and moves with a constant speed v_1 $(v_{min} \leq v_1 \leq v_{max})$ for a random period of time t_1 $(t_{min} \leq t_1 \leq t_{max})$. He may pause for a random time $t_{p,i}$ $(t_{p,min} \leq t_{p,i} \leq t_{p,max})$. Then, he chooses a new direction θ_2 and moves to it with a new speed v_2 under a new travel time t_2, and continues this process. Obviously, the RD Bob may dash on the border of the region. Many works have studied the rebound effect on the region border and here we assume Bob rebounds with a new direction $\theta_i = \theta_i + \pi/2 \mod 2\pi$ at the border [30].

Border Move (BM) mobile Bob: The BM mobility model is the special case of RWP model [17]. Unlike the RWP Bob, the BM mobile Bob always chooses a destination on the border of the region, and moves to it.

Eavesdropping model: Assuming that Alice employs a secrecy guard zone with radius R_E^{Guard} [12] to guarantee Eve's distance $r_E \geq R_E^{Guard}$ to her. This guard zone can be realized in practice when the antenna of the BS is mounted on a big tower or roof of a building, where an attacker cannot easily get close to it.

Firstly, we consider the typical downlink connectivity, when Alice transmits secrecy data to Bob. Assuming Eve knows Alice's location and the secrecy guard zone R_E^{Guard}. In the worst case, Eve can always eavesdrop at the boundary of the guard zone where the distance between Eve and BS is $r_E = R_E^{Guard}$ (Eve can be static or move around the guard zone). This model is illustrated in Fig. 1. Considering the uplink connection, where Bob transmits secrecy data to Alice. Here we assume Bob can also have a secrecy guard zone with radius R_E^{Guard} to prevent Eve from approaching too close to him. The eavesdropping signal quality for Eve from Bob is related to his distance from Bob. In the worst case scenario, we assume Eve can always follow Bob with distance $r_E = R_E^{Guard}$. Based on this observation, the uplink and downlink connections are considered symmetric. Without loss of generality, we only analyze the downlink connectivity in the rest of this paper.

B. Physical Layer Secrecy and Mathematical Formulation

Assume Eve is eavesdropping with a distance of r_E to Alice. At a time instant, when Bob is with a distance of d_{AB} to Alice ($0 < r_E, d_{AB} \leq R$ according to our model). The received signal at Bob and Eve can be presented as:

$$y_{Bob} = \frac{\sqrt{P_T}}{d_{AB}^{a/2}} h_{AB} s + n_B, \qquad y_{Eve} = \frac{\sqrt{P_T}}{r_E^{a/2}} h_{AE} s + n_E, \qquad (1)$$

where a is the path loss coefficient. It may vary from 2 to 6 which is determined by the propagation environment [32]. P_T is the transmit power, s denotes the transmit symbol and here let $|s|^2 = 1$. n_B and n_E are independent zero-mean unit-variance complex Gaussian noise at Bob and Eve, respectively. h_{AB} and h_{AE} are time-varying complex fading coefficients of channels from Alice to Bob and Alice to Eve, respectively. In the real world scenario, a mobile user may suffer a complex fading which is highly related to his propagation environment, such as Nakagami-m fading, Rayleigh-lognormal fading, etc. [32]. In this paper, we assume h_{AB} and h_{AE} follows Rayleigh fading with a circularly symmetric complex Gaussian random variable (RV) of zero-mean and unit-variance. Other fading scenarios can be analysed by using the same analytical framework.

Let r and w denote the instantaneous received SNR at Bob and Eve, respectively:

$$r = \frac{P_T\,|h_{AB}|^2}{d_{AB}^a \sigma_B^2}, \qquad w = \frac{P_T\,|h_{AE}|^2}{r_E^a \sigma_E^2}. \qquad (2)$$

Without loss of generality, let σ_B^2 and σ_E^2 be equal to 1, then the average receive SNR of Bob and Eve can be denoted as:

$$\tilde{r} = \frac{P_T}{d_{AB}^a} \qquad \tilde{w} = \frac{P_T}{r_E^a}, \qquad (3)$$

Considering the locations of Bob and Eve, the instant secrecy capacity under Rayleigh fading channel [8] can be represented by

$$C_S = [\log(1 + r(d_{AB})) - \log(1 + w(r_E))]^+, \qquad (4)$$

where $[x]^+ = \max(0, x)$.

We now introduce three secrecy metrics studied in this paper. *1) The Positive Secrecy Capacity Probability (PSCP)*:

the probability of existence of a non-zero secrecy capacity (PSCP) can be written as [8]:

$$P(C_S > 0) = P\left(r(d_{AB}) > w(r_E)\right). \tag{5}$$

2) The Secrecy Outage Probability (SOP): the probability of instances when secrecy capacity is less than the target secrecy rate $R_S (R_S > 0)$:

$$P^{out}(R_S) = P(C_S < R_S) = P\left\{\left[\log\left(\frac{1 + r(d_{AB})}{1 + w(r_E)}\right)\right]^+ < R_S\right\}. \tag{6}$$

3) Ergodic Secrecy Capacity: the average secrecy capacity which can be written as

$$C_S^E = E_{r,w,d_{AB}}\left\{C_S\left[r(d_{AB}), w(r_E)\right]^+\right\}, \tag{7}$$

where $E_{x_1,x_2,..,x_n}\{\cdot\}$ is the mean value operator for RV $x_1, x_2, .., x_n$.

As is known, according to Jake's model [32] for mobile communication, a faster moving speed leads to a higher time-varying rate of the channel. Thus the mobile Bob may suffer fast fading, which is highly related to his moving speed and prorogation environment. For slow flat fading when Bob is moving at a relatively low speed, the PSCP and SOP can properly reflect the system's secrecy performance and provide a metric to the secure strategy designs [21, 23]. As for fast fading, the ergodic secrecy capacity in Eq.(7) can utilize a lower bound of the average achievable secrecy rate [8, 33].

For classic physical layer secrecy with static nodes [11-15], the distances d_{AB} and r_E remain constant during the communication. However, in our work, Bob keeps moving randomly and the d_{AB} is time-varying. A more detailed analysis of the random mobile receiver is provided in the next section.

IV. Secrecy Analysis for Mobile User

In this section, we investigate the SOP and ESC performance for RWP, RD and BM random mobile user, respectively. Firstly, we focus on the scenario where Bob keeps moving without any pauses ($t_p = 0$). Then in Section IV-E, we analyze the pause time effects on secrecy performance of mobile users.

A. Secrecy Analysis for RWP Mobile User

For mobile Bob, d_{AB} is time varying. For simplicity of derivation, we convert the real distance to the normalized distance as

$$\bar{d}_{AB} = \frac{d_{AB}}{R},\ \bar{r}_E = \frac{r_E}{R}, \quad 0 < \bar{d}_{AB}, \bar{r}_E \le 1. \tag{8}$$

Obviously, $\bar{d}_{AB}$ and $\bar{r}_E$ depict the scale distances between the nodes and the area center corresponding to the real distances.

For random mobility users running into steady state, the spatial node distance probability density distribution function (SPDF), $f(d)$, illustrates the probability density of a mobile user appearing in a spatial position with distance d from the central point. When $t_p = 0$, for RWP mobility receivers, a well known approximate SPDF is given by C.Bettstetter [18] (we denote it as CB in this work). E. Hyytia [17] (we denote it as HC in this work) derived an accurate closed-form expression of the SPDF for RWP mobile users in an unit circle. With radius $R = 1$, the expression $f_{CB}(d)$ and $f_{HC}(d)$ are given by:

$$f_{CB}(d) = 4d - 4d^3, \ (0 < d \le 1). \tag{9a}$$

$$f_{HC}(d) = \frac{12}{73}(27d - 35d^3 + 8d^5), \ (0 < d \le 1). \tag{9b}$$

The SPDF expressions of Eq. (9) have been verified to be very close to the simulation results of the real movement process [18, 28]. For the simplicity of representation, we make the following substitutions:

$$m := \bar{d}_{AB}^a = \frac{d_{AB}^a}{R^a}, \quad k := \bar{r}_E^a = \frac{r_E^a}{R^a}, \quad (0 < m, k \le 1). \tag{10}$$

Then, the SPDF of a path loss with order a (i.e., PDF of $m = d_{AB}^a$) will be as follows:

$$f_m(m) = f_d(\bar{d}_{AB}^a) = f_d(m^{\frac{1}{a}})\left|\frac{\partial(m^{\frac{1}{a}})}{\partial m}\right|. \tag{11}$$

From Eq. (9) and Eq. (11), we get SPDFs of CB and HC with m variable as:

$$f_{CB}(m) = \frac{4}{a}\left(m^{\frac{2}{a}-1} - m^{\frac{4}{a}-1}\right), \tag{12a}$$

$$f_{HC}(m) = \frac{12}{73a}(27m^{\frac{2}{a}-1} - 35m^{\frac{4}{a}-1} + 8m^{\frac{6}{a}-1}), \tag{12b}$$

The value of path loss exponent a usually meets $2 \le a \le 6$, which is determined by the propagation environment [32]. The exponent $a = 2$ works well in some small indoor area prorogation environment. The exponent $a = 4$ works well on the generalized outdoor propagation model with a certain spread distance [32]. Here we firstly derive the closed expressions of PSCP and SOP under $a = 2$, 4, respectively. Then we extend our results to arbitrary values of path loss exponents.

1) The Positive Secrecy Capacity Probability $P(C_S > 0)$:

When Eve and Bob are located with real distances r_E and d_{AB} from Alice, the scale conditional probability $P(C_S > 0|m)$ can be derived from [8] as:

$$\begin{aligned} P(C_S > 0|d_{AB}) &= \frac{\tilde{r}}{\tilde{r} + \tilde{w}} = \frac{1}{1 + d_{AB}^a / r_E^a} \\ &= \frac{1}{1 + \bar{d}_{AB}^a / \bar{r}_E^a} = \frac{1}{1 + m/k}, \end{aligned} \tag{13}$$

Therefore, from Eq. (13), the scale conditional probability $P(C_S > 0|m)$ can be written as:

$$P(C_S > 0|m) = \frac{1}{1 + m/k}, \quad 0 < m, k \le 1. \tag{14}$$

For random mobile receiver Bob, the m itself is a random variable. Therefore, in steady state, $P(C_S > 0)$ for RWP mobile Bob can be written as

$$P(C_S > 0) = \int_0^1 P(C_S > 0|m) f(m) dm. \tag{15}$$

Then from Eq. (14) and Eq. (15), we can derive the closed-form expression for $P(C_S > 0)$ based on the SPDFs of CB and HC, respectively.

Proposition 1: *Based on CB's SPDF, the closed-form expression of $P_{CB}(C_S > 0)$ under $a = 2$ can be represented as:*

$$P^{a=2}_{CB}(C_S > 0) = 2k\left[k\ln(1+\frac{1}{k}) + \ln(1+\frac{1}{k}) - 1\right], \quad (16)$$

Proof. By substituting $a = 2$ in Eq. (12), the $P_{CB}(C_S > 0)$ can be derived as:

$$\begin{aligned} P_{CB}(C_S > 0) &= \int_0^1 P(C_S > 0|m) f_{CB}(m) dm|_{a=2} \\ &= \int_0^1 \frac{2(1-m)}{1+\frac{m}{k}} dm \\ &= 2\left[\int_0^1 \frac{1}{1+\frac{m}{k}} dm - \int_0^1 \frac{m}{1+\frac{m}{k}} dm\right]. \end{aligned} \quad (17)$$

By changing variable $m/k = t$ in calculus, the integral terms in Eq.(17) can be derived with integral TABLE [34], which given the results in proposition 1. □

Similarly, we can derive the closed from expression of $P^{a=2}_{HC}(C_S > 0)$ based on HC's SPDF.

Proposition 2: *The closed-form expression of $P^{a=2}_{HC}(C_S > 0)$ under the path loss factor $a = 2$ and $0 \le k \le 1$ can be presented in Eq. (18) as:*

$$\begin{aligned} P^{a=2}_{HC}(C_S > 0) =& \frac{6}{73}\left[8k^3\ln(1+\frac{1}{k}) + 35k^2\ln(1+\frac{1}{k}) + \right. \\ & \left. 27k\ln(1+\frac{1}{k})) - 8k^2 - 31k\right]. \end{aligned} \quad (18)$$

Proof. By substituting $a = 2$ into Eq. (12), the $P_{HC}(C_S > 0)$ can be derived as:

$$\begin{aligned} P^{a=2}_{HC}(C_S > 0) &= \int_0^1 P(C_S > 0|m) f_{HC}(m) dm|_{a=2} \\ &= \frac{6}{73}\int_0^1 \frac{1}{1+\frac{m}{k}}(27 - 35m + 8m^2) dm. \end{aligned} \quad (19)$$

By changing variable in calculus and integration by parts, the integral terms in Eq.(19) can be derived with integral TABLE [34]. The results in proposition 2 are obtained. □

Discussion: From propositions 1 and 2, the closed form expression of $P(C_S > 0)$ for RWP mobile Bob can be represented as a simple element function of k. As we know, from Eq. (10), the parameter $k = \bar{r}_E^a$ is the normalized distance between Alice and Eve. Therefore, the PSCP is only related to the normalized eavesdropping distance $\bar{r}_E$ in the real region. If we normalize the real secrecy guard zone radius as $R_E^{min} = R_E^{Guard}/R$ $(0 < R_E^{min} \le 1)$, then for any given guard radius $\bar{r}_E = R_E^{min}$, the system can easily evaluate the PSCP value by substituting $k = \bar{r}_E^a$ in Propositions 1 and 2. Otherwise, if the secrecy requirement γ is given which should meet $P(C_S > 0) \ge \gamma$, Alice can also easily evaluate the minimum required secrecy guard radius R_E^{min} to satisfy the secrecy requirement $P(C_S > 0) \ge \gamma$.

Furthermore, as we can see, the closed-form expression of CB in Proposition 1 is simpler than the HC result in Proposition 2. From Eq. (16), we can see the $P^{a=2}_{CB}(C_S > 0)$ is an increasing function of k, implying that the larger secrecy guard radius can provide high secrecy. When $k \to 0$, $\lim_{k\to 0} P^{a=2}_{CB}(C_S > 0) = 0$, which corresponds to the situation that Eve is eavesdropping with a distance $r_E \to 0$ to Alice, so the value of $P(C_S > 0)$ becomes zero. Otherwise, by substituting $k = 1$ into Eq. (16), we can get $P^{a=2}_{CB}(C_S > 0) = 4\ln(2) - 2 \approx 0.77258$, which represents the case when Eve can only eavesdrop at the circular area boundary. Similarly, for the pass loss factor $a = 4$, we derive $P^{a=4}_{CB}(C_S > 0)$ and $P^{a=4}_{HC}(C_S > 0)$ as follows.

Proposition 3: *For path loss factor $a = 4$, the closed-form expression of $P^{a=4}_{CB}(C_S > 0)$ is given by:*

$$P^{a=4}_{CB}(C_S > 0) = 2\sqrt{k}\arctan\sqrt{k} - k\ln(1+\frac{1}{k}). \quad (20)$$

Proposition 4: *For path loss factor $a = 4$, the closed-form expression of $P^{a=4}_{HC}(C_S > 0)$ is given by Eq. (21).*

$$\begin{aligned} P^{a=4}_{HC}(C_S > 0) =& \frac{3}{73}\left[\arctan k^{-\frac{1}{2}}(54k^{\frac{1}{2}} - 16k^{-\frac{3}{2}}) - \right. \\ & \left. 35kln(1+\frac{1}{k}) + 16k\right]. \end{aligned} \quad (21)$$

The closed form expressions in Propositions 3 and 4 for path loss $a = 4$ are also composite by simple element functions. From Eq. (20), when $k \to 0$, $\lim_{k\to 0} P^{a=4}_{CB}(C_S > 0) = 0$, which represents the case that Eve is eavesdropping with a distance $r_E \to 0$ to Alice. By substituting $k = 1$ into Eq. (20), we get $P^{a=4}_{CB}(C_S > 0) \approx 0.9258$. The closed-form expressions derived from HC SPDF are somewhat more complex than corresponding CB results. However, they are more accurate and we illustrate them further in Section IV-F2 and IV-F3.

2) The secrecy outage probability $P^{out}(R_S)$:

When Eve and Bob are located with real distances r_E and d_{AB} from Alice, the corresponding scale conditional SOP $P^{out}(R_S|m)$ can be derived from (9) in [8] as:

$$P^{out}(R_S|d_{AB}) = P(C_S < R_S|d_{AB}) = 1 - \frac{e^{d_{AB}^a(\frac{1-2^{R_S}}{P_T})}}{1 + 2^{R_S}(\frac{d_{AB}^a}{r_E^a})}. \quad (22)$$

Therefore, the scale conditional SOP $P^{out}(R_S|m)$ for $R_S > 0$ can be written as:

$$P^{out}(R_S|m) = 1 - \frac{e^{\frac{R^a(1-2^{R_S})}{P_T}m}}{1 + \frac{2^{R_S}}{k}m}. \quad (23)$$

Thus, for the random mobile Bob, $P^{out}(R_S)$ can be written as:

$$P^{out}(R_S) = \int_0^1 P^{out}(R_S|m) f(m) dm, \quad (24)$$

where R_S is the desired secrecy rate and P_T is transmit power. For simplification of mathematical representation, we define

$$b = \frac{2^{R_S}}{k}, \quad \lambda = \frac{R^a(1-2^{R_S})}{P_T}. \quad (25)$$

Proposition 5: *The closed-form expression of $P^{CB}_{out}(R_S)$ $(R_S > 0)$ based on CB SPDF under path loss factor $a = 2$ is given by:*

$$P^{out}_{CB}(R_S) = 1 - 2(1+\frac{1}{b})f + \frac{2(e^{\lambda} - 1)}{b\lambda}, \quad a = 2, \quad (26)$$

where $f = \exp(-\frac{\lambda}{b})\left[Ei(\frac{\lambda(1+b)}{b}) - Ei(\frac{\lambda}{b})\right]$, and $Ei(x) = \int_{-\infty}^{x} exp(u)/u \ du$ is the exponent integral function.

Proof. By substituting $a = 2$ in Eq. (12), we get

$$\begin{aligned} P_{CB}^{out}(R_S) &= \int_0^1 P^{out}(R_S|m) f_{CB}(m) dm|_{a=2} \\ &= 1 - 2\int_0^1 \frac{e^{\lambda m}}{1+bm} dm + 2\int_0^1 \frac{m e^{\lambda m}}{1+bm} dm. \end{aligned} \tag{27}$$

The first integral in the last line of Eq. (27) can be derived from Eq. (3.351 ETII217) in [34] as:

$$\int_0^1 \frac{e^{\lambda m}}{1+bm} dm = \exp(-\frac{\lambda}{b})\left[Ei(\frac{\lambda(1+b)}{b}) - Ei(\frac{\lambda}{b})\right]. \tag{28}$$

Based on Eq. (28), by integrating by parts, the second integral in the last line of Eq.(27) can derived as a expression of b, λ, f:

$$\int_0^1 \frac{m e^{\lambda m}}{1+bm} dm = \frac{e^{\lambda} - 1}{b\lambda} - \frac{1}{b} f. \tag{29}$$

Substituting Eqs. (28), (29) to (27), the result in *Proposition 5* is achieved. □

Similarly, we can derive the expression of SOP for path loss a = 2 based on HC's SPDF below.

Proposition 6: *The closed form expression of $P_{out}^{HC}(R_S)$ for HC under path loss factor $a = 2$ can be given by Eqs. (30) and (31) at the bottom of this page.*

Discussion: From the results in Proposition 5 and 6, the SOP value is related to k, a, P_T, R_S, and the real region radius R. However, for given R_S and secrecy guard radius R_E^{min}, the power to radius ratio with exponent a, as $\Delta = P_T/R^a$ becomes the key factor determining the SOP performance. We will illustrate its impact on SOP further through simulation in Section IV-F4. Similarly, we can derive the SOP for path loss factor $a = 4$ below.

Property 1: For path loss $a = 4$, the expression of $P_{CB}^{out}(R_S)$ based on CB's SPDF can be given as:

$$P_{CB}^{out}(R_S) \approx 1 + f - \frac{2e^{\lambda\epsilon^2} arctan\sqrt{b}}{\sqrt{b}}, \ \epsilon \in (0,1), \ a = 4. \tag{32}$$

Proof. The expression of $P^{out}(R_S)$ for CB can be derived as:

$$\begin{aligned} P_{CB}^{out}(R_S) &= \int_0^1 P^{out}(R_S|m) f_{CB}(m) dm|_{a=4} \\ &= 1 - \int_0^1 \frac{e^{\lambda m}}{1+bm}(m^{-\frac{1}{2}} - 1) dm \\ &= 1 + f - \int_0^1 \frac{e^{\lambda m}}{(1+bm)\sqrt{m}} dm. \end{aligned} \tag{33}$$

The integral in the above equation is not theoretically tractable. Instead, we provide an approximate expression here based on the mean value theorem for integrals [35]. Let $\sqrt{m} = t$, we can write the right hand of integral term in the last equation as

$$\int_0^1 \frac{e^{\lambda m}}{(1+bm)\sqrt{m}} dm = \int_0^1 \frac{2e^{\lambda t^2}}{1+bt^2} dt = \int_0^1 f(t)g(t)dt, \tag{34}$$

where $f(t) = 2e^{\lambda t^2}$, $g(t) = \frac{1}{1+bt^2}$. Functions $f(t)$ and $g(t)$ are continuous functions in region $(0,1)$ and $g(t) > 0$. According to mean integral theorem [35], there at least exists a value $\epsilon \in (0,1)$, which meet $\int_0^1 f(t)g(t)dt = f(\epsilon)\int_0^1 g(t)dt$. Thus, we get

$$\begin{aligned} \int_0^1 \frac{e^{\lambda m}}{(1+bm)\sqrt{m}} dm &= 2e^{\lambda\epsilon^2} \int_0^1 \frac{1}{1+bt^2} dt \\ &= \frac{2e^{\lambda\epsilon^2} arctan(\sqrt{b})}{\sqrt{b}}, \epsilon \in (0,1). \end{aligned} \tag{35}$$

Taking Eq. (35) to Eq. (33), Property 1 is proofed. □

By using the numerical computation tools, we can easily search an appropriate value for ϵ to approach the integral results. Similarly, we can derive the SOP expression for path loss a = 4 based on SPDF of HC below.

Property 2: *For path loss $a = 4$ under SPDF of HC, the expression of $P_{HC}^{out}(R_S)$ can be given as follows:*

$$\begin{aligned} P_{HC}^{out}(R_S) \approx & 1 + \frac{105}{73} f - \frac{162}{73} \frac{arctan(\sqrt{b}) e^{\lambda\epsilon_1^2}}{\sqrt{b}} - \\ & \frac{48}{73} e^{\lambda\epsilon_2}(\frac{1}{b} - \frac{\arctan\sqrt{b}}{b\sqrt{b}}), \ \epsilon_1, \epsilon_2, \in (0,1). \end{aligned} \tag{36}$$

The tractable SOP closed-form expressions of the mobile user are very useful, which can provide references to SOP constrained secrecy strategy design [23] for RWP mobile users in the future.

B. Secrecy Analysis for RD and BM Users

In this subsection, we analyze the SOP and PSCP for RD and BM Bobs. Here we use mean static (MS) receiver scenario [13] for a comparison. The MS represents the scenario where Bob is a static node and appears in the region, uniformly.

1) SOP for RD and MS users: For MS user in an unit radius circular region, the probability density function under polar coordinate can be presented as: $(\bar{d}_{AB}, \theta) = 1/\pi$, where $0 < \bar{d}_{AB} \leq 1, 0 \leq \theta \leq 2\pi$. For RD mobile receiver, the work [30] has proved that the steady state SPDF approaches to the uniform distribution. Thus, for steady state, the RD random mobile user has the same SPDF with the MS static user. By using the polar coordinate integral, the steady state SPDF for both the RD mobile Bob and the MS static Bob can be written

$$P_{HC}^{out}(R_S) = 1 - \frac{162}{73} f - \frac{210}{73b} f + \frac{210}{73}\left(\frac{e^{\lambda} - 1}{b\lambda}\right) - \frac{48e^{-\frac{\lambda}{b}}}{73b^3}(Ef + Ff - Gf), \quad a = 2 \tag{30}$$

$$Ef = \frac{b(b-\lambda)}{\lambda^2} e^{\frac{\lambda}{b}} - \frac{b\left[b - \lambda(b+1)\right] e^{\frac{\lambda(b+1)}{b}}}{\lambda^2}, \quad Ff = Ei(\frac{\lambda(1+b)}{b}) - Ei(\frac{\lambda}{b}), \quad Gf = \frac{2b}{\lambda}\left[e^{\frac{(1+b)\lambda}{b}} - e^{\frac{\lambda}{b}}\right] \tag{31}$$

as $f_{RD}(d) = f_{MS}(d) = \frac{1}{\pi}\int_0^{2\pi} d\, d\theta = 2d$. Similarly, for the SPDF with path loss component m, we have

$$f_{RD}(m) = f_{MS}(m) = \frac{2}{a}m^{\frac{2}{a}-1}. \tag{37}$$

From Eqs. (15), (24), (37), we obtain

$$P_{RD}(C_S > 0) = P_{MS}(C_S > 0),\ P_{RD}^{out}(R_S) = P_{MS}^{out}(R_S). \tag{38}$$

We can see that RD mobile user has the same SOP performance as MS static user. Then, by taking $a = 2$ in Eq. (37), we have

$$P_{RD}^{a=2}(C_S > 0) = \int_0^1 \frac{1}{1+\frac{m}{k}}dm = k\ln(1+\frac{1}{k}). \tag{39}$$

Similarly, by taking $a = 4$ in Eq. (37), we can get

$$P_{RD}^{a=4}(C_S > 0) = \int_0^1 \frac{m^{-\frac{1}{2}}}{2(1+\frac{m}{k})}dm = \sqrt{k}\arctan\sqrt{\frac{1}{k}}. \tag{40}$$

We can derive the closed form of $P_{RD}^{out}(R_S)$ for $R_S > 0$. By taking $a = 2$ in Eq. (37), we have

$$P_{RD}^{out}(R_S) = 1 - \int_0^1 \frac{e^{\lambda m}}{1+bm}dm = 1 - f, \quad a = 2. \tag{41}$$

Based on *Property 1*, for $a = 4$, we can get the approximate SOP expression as:

$$P_{RD}^{out}(R_S) = 1 - \frac{1}{2}\int_0^1 \frac{e^{\lambda m}}{\sqrt{m}(1+bm)}dm \approx 1 - \frac{e^{\lambda\varepsilon_3^2}\arctan\sqrt{b}}{\sqrt{b}}, \tag{42}$$

where $\varepsilon_3 \in (0, 1)$.

2) Border mobile user: The Border mobile (BM) model is also called RWPB [17]. It is the special case of RWP where Bob always chooses the waypoint on the perimeter of the region. The BM Bob always keeps moving across the region until he arrives at the circular boundary. According to [17], the steady state SPDF of BM can be presented as:

$$f_{BM}(d) = \frac{F_{BM}'(d)}{2\pi d} \tag{43}$$

where $F_{BM}(d) = \int_0^{\phi_0}\sqrt{d^2 - \sin^2\phi}d\phi$ and $\phi_0 = \arcsin d$. The integral term of $F_{BM}(d)$ is the second ellipse integral [34]. Based on Eq. (43), we can get the numerical evaluation of the SOP. Also, we will show that BM receiver has the worst secrecy performance compared to other mobile receivers in the Section IV-F2 and IV-F3.

C. SOP of Arbitrary Path Loss Coefficients

In this subsection, we extend the SOP expressions to arbitrary values of path loss coefficient a, which may vary from 2 to 6 in practice [32]. Let $v = \frac{2}{a}$, where $\frac{2}{6} \leq v \leq 1$. From Eqs. (12) and (37), the SPDF expressions of CB, HC, RD can be presented in a general form as:

$$f_{(CB,HC,RD)}(m) = \sum_{i=1}^{L} Dv(A_i m^{B_i v-1}). \tag{44}$$

For example, for SPDF of RD user $f_{RD}(m)$, where $L, D, A_i, B_i = 1$. For RWP user's SPDFs $f_{CB}(m)$ and $f_{HC}(m)$, where $L = 2, 3$,$D = 2, \frac{6}{73}, A_i = [1, -1], [27, -35, 8]$ and $B_i = [1, 2], [1, 2, 3]$, respectively. From Eq. (15), we can get the PSCP expression with m, v variables as:

$$\begin{aligned} P_a(C_S > 0) &= \int_0^1 \frac{1}{1+\frac{m}{k}}\sum_{i=1}^{L} Dv(A_i m^{B_i v-1})dm \\ &= \sum_{i=1}^{L} DA_i v\Phi(k, v, B_i), \end{aligned} \tag{45}$$

where $\Phi(k, v, B_i) = \int_0^1 \frac{t^{B_i v-1}}{1+(t/k)}dt$ is a definite integral with parameters (v, k, B_i), which can be evaluated through mathematic software. Similarly, the SOP can be written as

$$P_a^{out}(R_S) = 1 - \sum_{i=1}^{L} DA_i v\Phi_{out}(k, v, B_i), \tag{46}$$

where $\Phi_{out}(k, v, B_i) = \int_0^1 \frac{e^{\lambda t}t^{B_i v-1}}{1+bt}dt$. For different R_S requirement, the parameter $b = 2^{R_S}/k$ can be larger than 1. Thus the definite integral $\Phi_{out}(k, v, B_i)$ cannot be presented in closed-form expression with confluent hypergeometric series. However, for given parameters (k, v, B_i), it can be evaluated through mathematic software.

D. The Ergodic Secrecy Capacity of Mobile Bob

In this subsection, we discuss the ergodic secrecy capacity for random mobile receivers. According to [8], when given the real positions of Bob and Eve, the secrecy capacity can be derived as:

$$\begin{aligned} C_S(d_{AB}) &= \int_0^\infty\int_0^\infty [C_S(d_{AB}|r, w)]^+ f(r)f(w)drdw \\ &= F(\frac{P_T}{d_{AB}^a}) - F(\frac{P_T}{d_{AB}^a + r_E^a}), \end{aligned} \tag{47}$$

where $f(r)$ and $f(w)$ are the instantaneous SNR PDF of Bob and Eve, respectively. As it is known for Rayleigh channel, $f(r)$ and $f(w)$ follow the exponential distribution. From [8], $F(x)$ can be written as $F(x) = \int_0^\infty \frac{1}{x}\log_2(1+u)\exp(-\frac{u}{x})du$. Therefore, we can get the average ergodic capacity for the random mobile receiver as

$$C_S^E = \int_0^1 \left[F(\frac{P_T}{mR^a}) - F(\frac{P_T}{(m+k)R^a})\right] f(m)dm, \tag{48}$$

where $f(m)$ denotes the user's SPDF with variable m (i.e. RWP, RD in Eqs. (12), (37)). By combining the SPDF expressions, we can get the numerical calculation results of the C_S^E in Eq. (48) by using mathematical tools. From Eq. (48), C_S^E relates to factor Δ and k. We will evaluate their impacts on the secrecy capacities through simulation in Section IV-F4.

E. The RWP Pause Time Impact on Secrecy Performance

In this subsection, we investigate the secrecy effect of the pause time $t_p \neq 0$ for the mobile user. The pause time is an important parameter for real secrecy consideration since it is more realistic that Bob can "take a rest" when he arrives at the destination before he starts a new movement period. When $t_p \neq 0$, we can write the SPDF of the random mobile Bob as two independent static and mobility components [29] as:

$$f(d) = p_{pause}f_p(d) + (1 - p_{pause})f_m(d), \tag{49}$$

where $0 < d \leq 1$ presents the normalized distance from the BS. $f_p(d)$ is the distribution of Bob's pause points before a new movement and the mobility component $f_m(d)$ accounts for the part that Bob is actually moving. As for RWP user, the waypoint is chosen uniformly from the region, so $f_p(d) = f_{MS}(d) = 2d$. p_{pause} is the probability of pause. Let $p_{move} = 1 - p_{pause}$, from Eq. (49), we can write $P^{out}(R_S)$ for $t_p > 0$ as:

$$\begin{aligned} P^{out}(R_S) = & p_{pause} \int_0^1 P^{out}(R_S|d) f_p(d)\, dd + \\ & p_{move} \int_0^1 P^{out}(R_S|d) f_m(d)\, dd. \end{aligned} \tag{50}$$

From Eq. (50), for random mobile Bob with $t_p > 0$, we get:

$$P^{out}(R_S) = p_{pause} P^{out}_{MS}(R_S) + p_{move} P^{out}_{M}(R_S), \tag{51}$$

where $P^{out}_{MS}(R_S)$ is the SOP of pause components and $P^{out}_{M}(R_S)$ presents the mobile components.

Property 3: *For SOP $P^{out}(R_S)$ of RWP Bob with $t_p > 0$, we have:*

$$P^{out}_{RWP,t_p>0}(R_S) = p_{pause} P^{out}_{MS}(R_S) + p_{move} P^{out}_{RWP,t_p=0}(R_S), \tag{52}$$

where $P^{out}_{RWP,t_p=0}(R_S)$ denotes the SOP when $t_p = 0$.

Proof. For RWP Bob, the pause component of SOP is the same as $P^{out}_{MS}(R_S)$ in Eq. (38). The mobility part component ($t_p \neq 0$) of SOP for RWP user is $P^{out}_{RWP,M}(R_S) = P^{out}_{RWP,t_p=0}(R_S)$ that has been discussed in the previous section. From Eq. (51), we obtain *Property 3*. □

From *Property 3*, the node pause probability p_{pause} becomes very crucial. For RWP mobile user, p_{pauser} can be presented as [29]:

$$p_{pause} = \frac{E(T_p)}{E(T_p) + E(T_m)} = \frac{1}{1 + \frac{E(T_m)}{E(T_p)}}, \tag{53}$$

where $E(T_p)$ is the average pause time and $E(T_m)$ is the average moving time. Based on Eq. (53), p_{pause} is determined by the proportion of the average moving time to average pause time. From Eq. (52) and (53), when $E(T_p) \to \infty$, $p_{pause} \to 1$ and $p_{move} \to 0$, the scenario becomes equivalent to MS and RD scenarios. Otherwise, when $E(T_p) \to 0$, the $p_{pause} \to 0$ and $p_{move} \to 1$, the scenario becomes equivalent to the mobile situation with $t_p = 0$. We can see that the pause time has a negative impact on secrecy and it achieves higher secrecy as the RWP mobile user keeps moving without any pause time ($t_p = 0$).

F. Simulation and Numerical Results

In this subsection, we illustrate secrecy properties of the random mobile user by numerical and simulation results. We sample on Bob's moving paths to simulate his random mobility process [17]. From Fig. 2 to Fig. 7, unless otherwise specified, the mobile parameters are set as $P_T = 1$, pause time $t_p = 0$, moving speed $v = 0.1R$, and the sample distance is determined to be $0.1v$. For RD Bob, each movement epoch time is $t_i = 1$.

1) Sampling points of RWP, BM and RD Bobs under steady state:

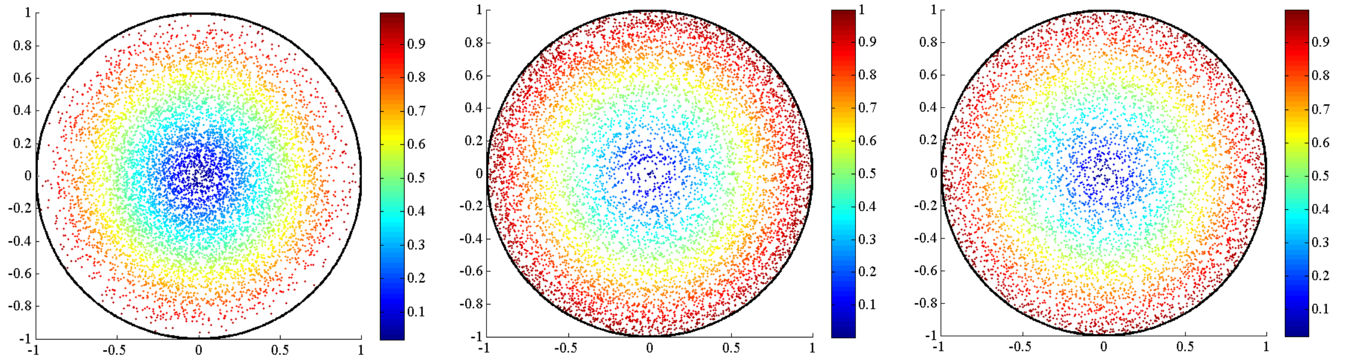
In Fig. 2, we show the sampling points of RWP, BM and RD mobile receivers in the circular region with radius $R = 1$, respectively. Alice locates in the origin with coordinates $(0, 0)$ and keeps transmitting signal to the random mobile Bob during the running period. When Bob is running into steady state, we draw the last 10^4 sampling points for RWP, BD and RD receiver, respectively.

From Fig. 2 (a), we can find that the RWP receiver Bob's sampling points are very sparse in the boundary region (the red printing points). Almost no point appears in the circular boundary. The point density becomes more and more intensive towards the center of the circular region (the blue printing points). On the contrary, in Fig. 2 (b), the border move (BM) receiver Bob's sampling points are very dense in the boundary region (the red printing point), but become more and more sparse towards the central region (the blue printing points). The RD receiver Bob in Fig. 2 (c) has more uniform density coverage in the whole circular region, compared to RWP and BM Bobs. The phenomenons shown in Fig. 2 indicate that the RWP Bob has higher probability to be close to Alice. This characteristic benefits the secrecy, since a closer distance yields a higher SNR. On the contrary, the BM user has lower probability to be close to Alice, which results in lower SNR and lower secrecy.

2) Analytical and simulation results of PSCP and SOP:

Figure 3 to 7 compare the simulation results with our analytical results and study the secrecy for RWP, RD, MS and BM random mobile receivers. In Fig. 3-7, unless otherwise specified, the x-axis denotes the normalized secrecy guard radius $R^{min}_E = R^{Guard}_E / R$ versus from (0,1). The channel coefficients h_{AB}, h_E are assumed to follow Rayleigh fading with a circularly symmetric complex Gaussian RV of zero-mean and unit-variance. We obtain 3×10^5 sample points for statistic results. For $P^{out}(R_S)$ in Fig. 3 and Fig. 4, we set the desired secrecy rate $R_S = 0.1$. The approximate parameters for SOP are set as $\varepsilon = \varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 0.5$. The label "sim" denotes the simulation results and "ana" denotes the theoretic results.

Figure 3 and 4 verifies our analytical expressions of PSCP and SOP under path loss factors $a = 2$ and 4, respectively. In Fig. 3 and Fig. 4, all of the analytical results are very close to the simulation results, which validate our theoretic analysis. For RWP user, the theoretic results based on HC's SPDF (red circular marked) are closer to the simulation results (the black line) than the CB's results (black circular marked). All of the users' secrecy performance improves as the guard radius R^{min}_E becomes larger. In Fig. 3 and Fig. 4, we can see that RWP user clearly has higher secrecy performance than RD (blue dash line) and BM receivers (blue solid line), which verifies our theoretical analysis and predictions. As can be seen in Fig. 3 and Fig. 4, for most of the guard radius values R^{min}_E, the RWP user can achieve higher PSCP and SOP performance about 10% to 20% compared to RD user. Besides, the secrecy performance of RD mobile receiver is very close to MS static receiver. The secrecy performance of BM receiver is slightly worse than RD receiver.

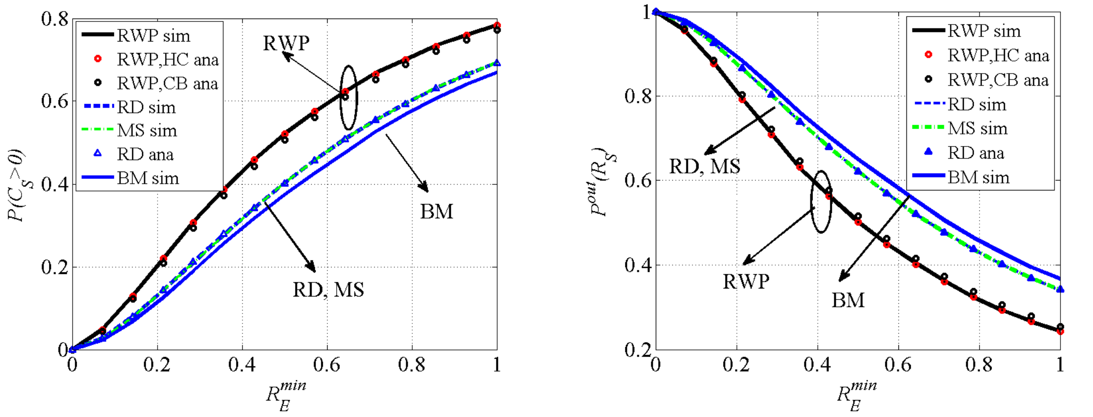


(a) RWP

(b) BM

(c) RD

Figure 2: The sampling points of RWP, BM and RD mobile receivers with circular region of radius $R = 1$ in (a), (b) and (c), respectively. The BS Alice locates in the origin of coordinates $(0, 0)$ keeps transmitting information to mobile receiver Bob. When Bob is running into steady state, Fig.2 plots 10^4 sample points for RWP, BD and RD receivers, respectively.



(a) PSCP

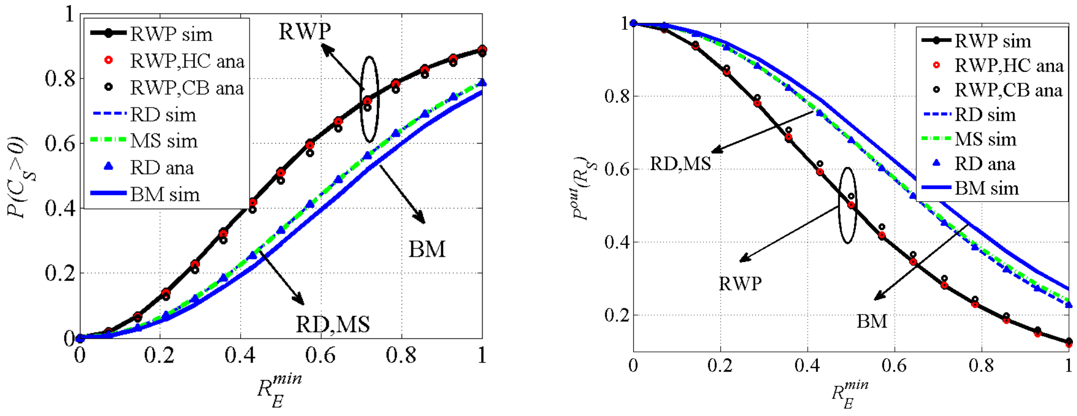
(b) SOP

Figure 3: The simulation and analytical results of $P(C_S > 0)$ and $P^{out}(R_S)$ for pass loss $a = 2$ versus the normalized radius $0 < R_E^{min} \leq 1$.

3) Analytical and simulation results of secrecy capacity : Figure 5 shows the results of ergodic secrecy capacity C_S^E under path loss $a = 2, 4$, respectively. From Fig. 5, we can see that all of the analytical results are close to simulation results. The secrecy capacity C_S^E increases as guard zone radius becomes larger. Above all, the RWP Bob clearly achieves higher secrecy capacity than other users and the advantage is increasing when the guard zone radius R_E^{min} is larger. For example, in Fig. 5 (b), with the guard zone radius $R_E^{min} = 0.6$, the RWP Bob has a C_S^E more than 2 bps compared to RD Bob is 1 bps. For guard zone radius $R_E^{min} = 1$, the RWP user's C_S^E is close to 3.5 bps compared to RD Bob is about 2 bps. Furthermore, the secrecy capacity of RD mobile receiver is very close to the MS static receiver (rose dot line). The BM receiver has the lowest secrecy capacity. The phenomenon in Fig. 5 verifies our analytical results and indicates that the RWP mobile user can achieve the highest secrecy capacity.

4) The impact of circular radius R and path loss a: Figure 6 evaluates the impact of different power to region radius ratio Δ on secrecy for RWP Bob. The path loss set as $a = 2$ and the power to radius ratio with exponent is set as $\Delta = P_T/R^a = 1, 0.25, 0.04, 0.01$, respectively. From Fig. 6 (a), the SOP of $\Delta = 1$ (black solid line) is much lower than $\Delta = 0.01$ (triangular marked green line). Furthermore, in Fig. 6 (b), C_S^E is sharply decreasing with smaller Δ. The reason behind it is that for given R_E^{min} with a smaller Δ, if Alice utilizes the same transmit power P_T in a larger R circular region, Bob will randomly move in a larger circular region, then his received SNR will be much more lower which degrades secrecy performance sharply. Otherwise, if Bob moves in the circular with same R, but Alice utilizes much smaller P_T, Bob's received SNR will also decreases dramatically which degrades secrecy performance.

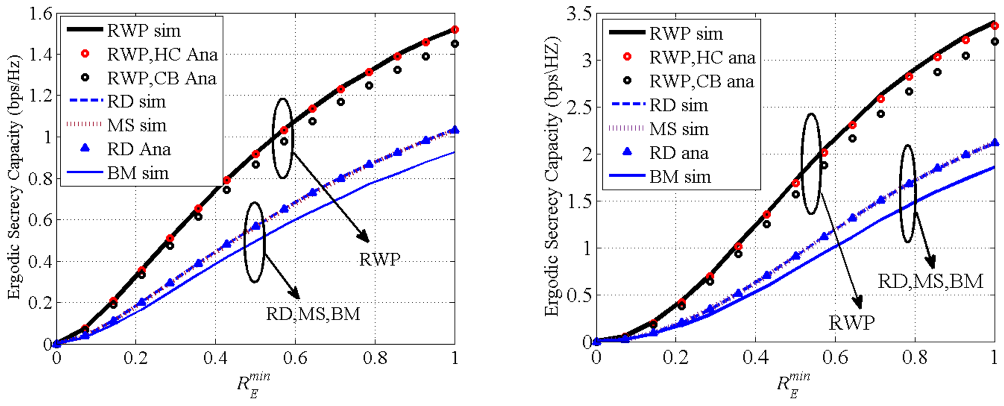
Figure 7 evaluates the SOP and ESC under different path loss coefficients $a = 2, 3, 4$ for RWP Bob under the same region radius $R = 10$ and $P_T = 1$. In the Fig. 7 (a), it shows that SOP performance is significantly increasing with higher path loss factor a. The SOP with smaller path loss propagation $a = 2$ is lower than $a = 4$. Figure 7 (b) shows for guard radius $R_E^{min} > 0.2$, the lower path loss factor $a = 2$ (blue solid line) clearly provides higher secrecy capacity C_S^E. It is also shown in the figure that when Eve can keep close to Alice with guard radius $R_E^{min} \leq 0.2$, the higher path loss factor $a = 4$ (green dash line) achieves slightly higher C_S^E than smaller factor $a = 2$. It can be explained that when Eve is located relatively close to Alice, the smaller path loss $a = 2$ makes Eve achieve higher received SNR. It makes more negative



(a) PSCP

(b) SOP

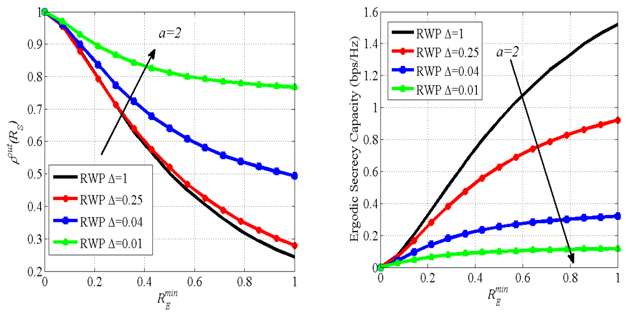
Figure 4: The simulation and analytical results of $P(C_S > 0)$ and $P^{out}(R_S)$ for pass loss $a = 4$ versus the normalized radius $0 < R_E^{min} \leq 1$.



(a) $a = 2$

(b) $a = 4$

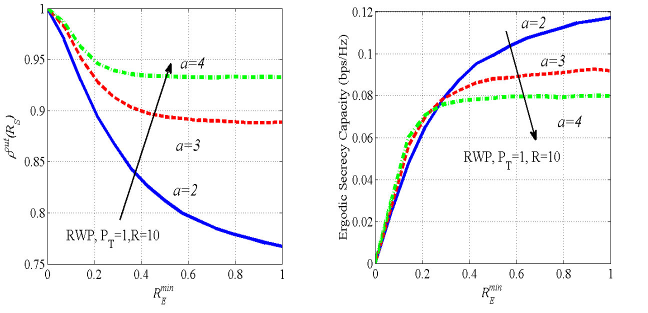
Figure 5: The simulation and analytical results of ESC C_S^E for pass loss $a = 2, 4$ versus the normalized guard radius $0 < R_E^{min} \leq 1$.



(a) SOP

(b) C_S^E

Figure 6: The SOP and ergodic secrecy capacity C_S^E of RWP Bob with different $\Delta = 1, 0.25, 0.04, 0.01$ versus the normalized guard radius $0 < R_E^{min} \leq 1$. The pass loss $a = 2$.



(a) SOP

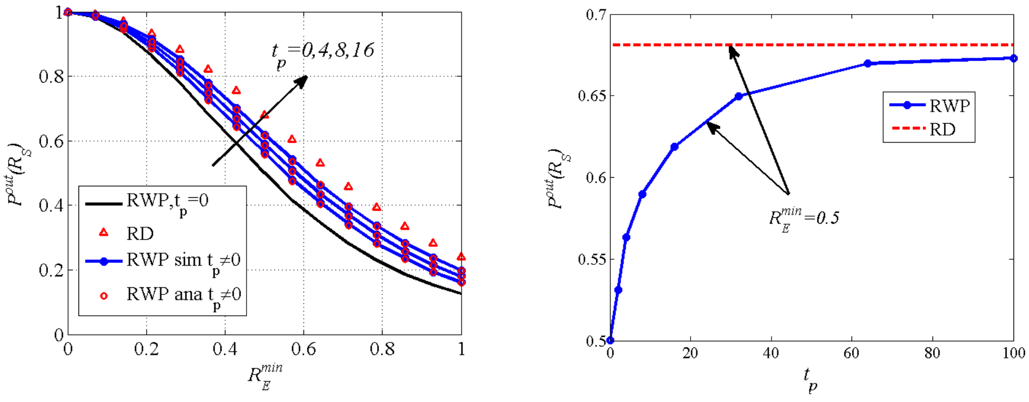
(b) C_S^E

Figure 7: The SOP and ergodic secrecy capacity C_S^E of RWP Bob under different pass loss $a = 2, 3, 4$ versus the normalized guard radius $0 < R_E^{min} \leq 1$. The circular radius $R = 10$ and transmit power $P_T = 1$.

effects on ergodic secrecy capacity. However, with guard zone radius R_E^{min} increased, Eve's received SNR becomes lower. At the same time, the smaller path loss progation environment makes mobile Bob's receiver SNR much higher, which makes more contribution to the secrecy capacity.

5) The impact of pause time on SOP:

Figure 8 shows the pause time impact on the SOP under path loss coefficient $a = 4$. In Fig. 8 (a), the pause time at each destination point is set as $t_p = 0, 4, 8, 16$, respectively. The other parameters are kept all the same as the simulations in Fig. 4. From Fig. 8 (a), we can see the SOP of Bob with pause time t_p is higher than the mobile Bob without pause time (black solid line). The value of SOP becomes higher with the increase of pause time t_p and it approaches more and more close to RD user (red triangle mark). For Bob with pause time t_p, the simulation results (blue line) are consistent with



(a)

(b)

Figure 8: The pause time impact on SOP. (a) shows the SOP simulation and numerical results under different pause time $t_p = 0, 4, 8, 16$ versus $0 < R_E^{min} \le 1$. (b) shows the SOP asymptotic effects of $t_p \rightarrow 100$ for RWP Bob when R_E^{min} is fixed as 0.5 .

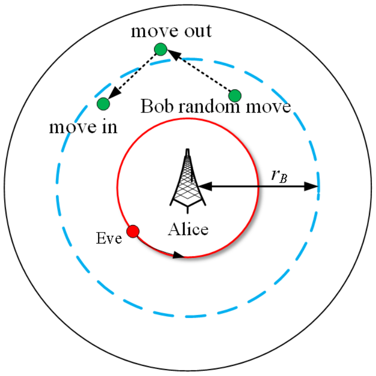


Figure 9: Secrecy improvement strategy based on the transmit subcell (inner region of blue dotted circular) with radius r_B. If Bob moves outside the subcell, Alice suspends the communication. If Bob moves into the subcell, Alice continues the communication.

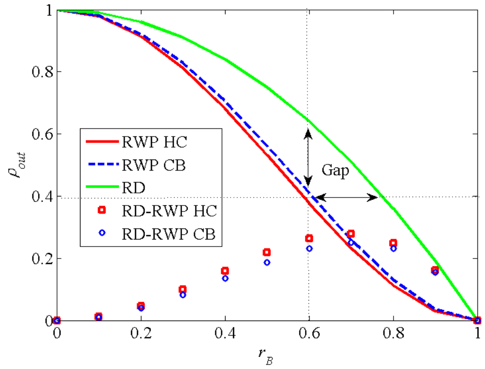


Figure 10: The transmit outage probability ρ_{out} for RWP and RD receiver versus $0 < r_B \le 1$.

analytical results (red circular mark). Figure 8 (b) illustrates the SOP variation tendency when $t_p \rightarrow 100$. The guard zone R_E^{min} in Fig. 8 (b) is fixed to be 0.5. The phenomenon shown in Fig. 8 is fully consistent with our analysis of the pause time impact in section IV-E and verifies the RWP Bob without pause time will have higher secrecy performance.

V. Secrecy Improvement Strategies for Random Mobile Users

In this section, we investigate two practical secrecy improvement strategies for mobile users.

A. Secrecy Improvement Strategy 1

From the previous analysis, when the mobile user is running in the boundary region of the cell that are far from Alice, he may have a high probability to suffer a weak instant secrecy performance. Intuitively, we can bound a subcell transmit circular region with a radius r_B. During the communication, if Alice finds Bob move outside the transmission subcell where ($d_{AB} > r_B$), she suspends transmiting secret information to Bob. If Bob moves into the subcell ($d_{AB} \le r_B$), Alice continues to transmit. The strategy is illustrated in Fig. 9.

Clearly, the smaller r_B gets, the higher will be the instant secrecy. However, the probability that Bob moves out of this subcell is also increased, which leads to a higher transmit outage probability ρ_{out}, which is defined as $\rho_{out} = \int_{r_B}^{1} f(d)\, dd$ here, where the $f(d)$ is SPDF of Bob. For high security demanding scenario, sometimes we would rather sacrifice a few communication quality (i.e. tolerate a transmit outage probability $\rho_{out} \le \xi$) to ensure the security performance. For a given threshold $\rho_{out} = \xi$, we aim to find the minimum required subcell radius $\min(r_B) = R_B$ that provides the highest secrecy. For a given transmit subcell radius r_B, we can obtain ρ_{out}^{HC} for RWP Bob as

$$\rho_{out}^{HC} = \int_{r_B}^{1} \frac{12}{73}(27d - 35d^3 + 8d^5)\, dd = \frac{(r_B^2 - 1)^2(73 - 16r_B^2)}{73}. \tag{54}$$

From Eq. (9), we can get the expression of ρ_{out}^{CB} for RWP user based on CB's SPDF as $\rho_{out}^{CB} = \int_{r_B}^{1}(4d - 4d^3)\, dd = (r_B^2 - 1)^2$. Similarly, we can get the RD user's transmit outage probability ρ_{out}^{RD} as $\rho_{out}^{RD} = \int_{r_B}^{1}(2d)\, dd = 1 - r_B^2$.

Property 4: *For a given transmit subcell radius r_B, the transmit outage ρ_{out} for RWP and RD mobile users satisfy:*

$$\rho_{out}^{RD} > \rho_{out}^{CB} > \rho_{out}^{HC}, \quad 0 < r_B \le 1 \tag{55}$$

Proof. In Eq. (54), let $h = \frac{73-16r_B^2}{73}$, $0 < r_B \le 1$. Obviously $57/73 \le h \le 1$, then we get $\rho_{out}^{HC} = h\rho_{out}^{CB} \le \rho_{out}^{CB}$. Thus we get $\rho_{out}^{RD} - \rho_{out}^{CB} = r_B^2(1 - r_B^2) \ge 0$, which proves *Property 4*. □

Table I: Minimum required subcell radius R_B for RWP and RD users under different ρ_{out}

ρ_{out}	0.05	0.1	0.2	0.3	0.4	0.5
R_B^{RWP}	0.8690	0.8113	0.7243	0.6518	0.5851	0.5205
R_B^{RD}	0.9747	0.9487	0.8944	0.8367	0.7746	0.7071

Figure 10 shows the theoretic value of ρ_{out}^{RD}, $\rho_{out}^{HC}, \rho_{out}^{RC}$ versus $0 < r_B \leq 1$. From Fig. 10, for a given transmit subcell r_B, ρ_{out}^{RD} is much higher that ρ_{out}^{HC}. For example, when $r_B = 0.8$, $\rho_{out}^{RWP} \approx 0.1$ but $\rho_{out}^{RD} \approx 0.35$. Also, for a given transmit outage $\rho_{out} = \xi$, the minimum needed subcell radius r_B^{min} can be obtained through inverse function calculation. From Fig.10, for a given ρ_{out}, we can see the minimum needed subcell radius $R_B^{RWP} < R_B^{RD}$, which implies the RWP user is likely to get more secrecy improvement under the same ρ_{out} compared to RD user. Table I lists R_B for RWP and RD user under $\rho_{out} \leq 0.5$ for comparison.

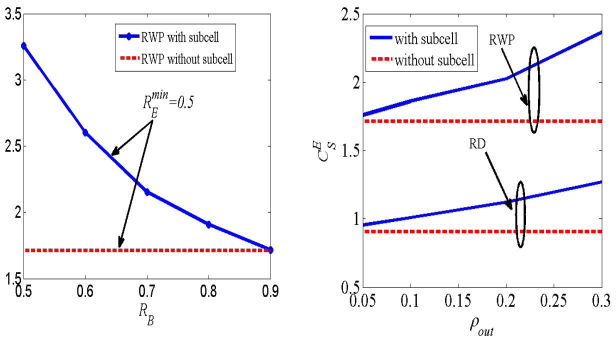
B. Secrecy Improvement Strategy 2

The secrecy improvement strategy 1 sacrifices all the communications out of the transmit subcell, which may cause discomfort to the mobile users. Here we provide the secrecy improvement strategy 2. Consider for mobile users, the strategy should be realized with low complexity, because the channel is time varying and the secrecy improvement performance will be sensitive to the processing delay. In the real world communication, assume Bob periodically feeds back his instantaneous SNR r to Alice within a very short time t_Δ, thus the instantaneous SNR r during t_Δ can be seen as constant. For time-varying fading channels, r can be estimated by the methods of [36]. However, without loss of generality, we have normalized the background noise powers of Bob and Eve in the first line under Eq. (2). Thus r, w can be directly reflected by the received signal strength (RSS) [32] of Bob and Eve, respectively. Bob can feedback r to Alice through a secured channel or not, because the information of r makes no contribution to Eve's eavesdropping. Then Alice can transmit secret information only when the instantaneous secrecy capacity reaches to a required level R_S^T, e.g. $C_S^T = log(1+r) - C_E^T(R_E^{min}) \geq R_S^T$, where $C_E^T(R_E^{min})$ denotes the instantaneous channel capacity of Eve eavesdropping at the guard zone boundary with radius R_E^{min}. In practice, $C_E^T(R_E^{min})$ can not be known by Alice and Bob. However, if Alice has known the channel statistic distribution, she can evaluate Eve's average channel capacity $C_E(R_E^{min})$ [8] as an approximation. Thus Alice can transmit secret information only when $r \geq \tau$, where $\tau = 2^{C_E(R_E^{min})+R_S^T} - 1$.

Obviously, for fixed R_E^{min}, the user will get more secrecy capacity improvement when threshold τ becomes larger. However, for mobile Bob, the larger τ will cause higher transmit outage probability where $\rho_{out} = P(r \leq \tau)$. For secrecy improvement strategy 2, the ρ_{out} for RWP and RD mobile users under arbitrary R and a can be calculated by Eq. (8) in [31]. For Raleigh fading channel with path loss $a = 4$, we can utilize results in [28] to calculate ρ_{out} for RWP and RD Bob as:

Table II: Maximum achievable τ^{RWP}, τ^{RD} for RWP and RD users under different ρ_{out}

ρ_{out}	0.05	0.1	0.2	0.3	0.4	0.5
τ^{RWP}	0.35	0.80	1.80	3.40	5.50	9.5
τ^{RD}	0.16	0.33	0.74	1.28	2.00	3.1



(a)

(b)

Figure 11: Secrecy capacity improvement compared with no subcell scenario under fixed guard radius $R_E^{min} = 0.5$. (a) shows C_S^E improvement for RWP versus minimum transmit subcell radius R_B from 0.5 to 0.9. (b) shows C_S^E improvement for RWP and RD users under given ρ_{out} from 0.05 to 0.3.

$$\rho_{out}^{RWP} = \frac{3}{73}\int_0^\tau \left[\frac{54}{3}\ {}_1F_1(\frac{3}{2},\frac{5}{2},-r) - \frac{35}{2}\ {}_1F_1(2,3,-r) + \frac{16}{5}\ {}_1F_1(\frac{5}{2},\frac{7}{2},-r)\right] dr, \tag{56a}$$

$$\rho_{out}^{RD} = \int_0^\tau \frac{1}{3}\ {}_1F_1(\frac{3}{2},\frac{5}{2},-r) dr. \tag{56b}$$

where ${}_1F_1(\cdot)$ is the confluent hypergeometric function [34]. Since r is real and positive, we can write [28]

$$ {}_1F_1(a, 1+a, -r) = e_1^{-r} F_1(1, 1+a, r) \tag{57}$$

From Eqs. (56) and (57), we can get

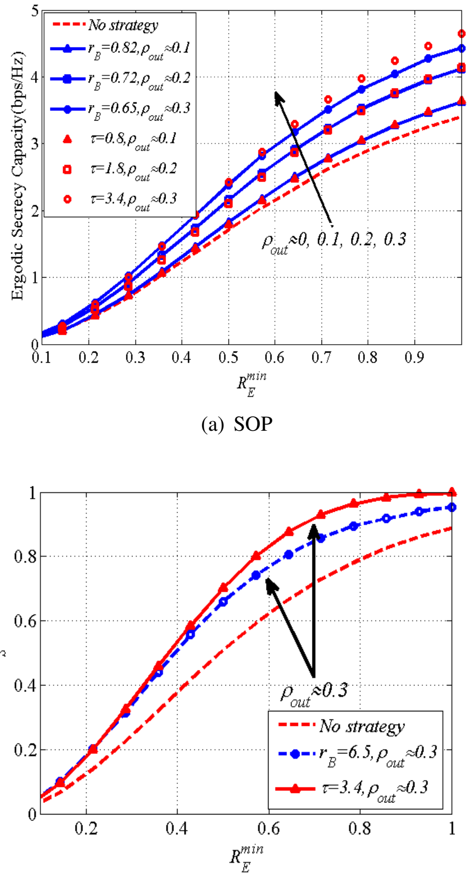
$$\rho_{out}^{RWP} = \frac{3}{73}\sum_{k=0}^{\infty}\left[\frac{\frac{54}{3}(1)_k}{(k!)(\frac{5}{2})_k} - \frac{\frac{35}{2}(1)_k}{(k!)(3)_k} + \frac{\frac{16}{5}(1)_k}{(k!)(\frac{7}{2})_k}\right]\Gamma(k+1,\tau) \tag{58a}$$

$$\rho_{out}^{RD} = \frac{1}{3}\sum_{k=0}^{\infty}\frac{(1)_k}{(k!)(\frac{5}{2})_k}\Gamma(k+1,\tau) \tag{58b}$$

where $\Gamma(k+1,\tau) = \int_0^\tau t^k e^{-t} dt$ is a lower incomplete gamma function [34]. $(a)_k = a(a+1)(a+2)...(a+k-1)$ is rising factorial/Pochhammer symbol. For a given ρ_{out}, the approximately maximum achievable τ^{RWP}, τ^{RD} for RWP and RD Bob can also be calculated by Eq. (58). In Table II, we list τ^{RWP}, τ^{RD} under ρ_{out} from 0.05 to 0.5. As shown in Table II, for the given ρ_{out}, the threshold τ^{RWP} can be larger than τ^{RD}, which indicates that RWP users can get more secrecy improvement than RD users.

C. Simulation and Numerical Results

Figure 11 shows the secrecy improvement of the subcell strategy 1. The guard radius is fixed as $R_E^{min} = 0.5$. The Fig. 11 (a) plots the RWP users secrecy capacity improvement



(a) SOP

(b) C_S^E

Figure 12: (a) compares secrecy capacity improvement of Strategy 1, 2 for RWP Bob with no secrecy improvement strategy scenario, versus the normalized guard radius $0 < R_E^{min} \leq 1$. The requirement of transmit outage sets as $\rho_{out} \approx 0.1, 0.2, 0.3$. Strategy 1 sets transmit subcell radius $r_B = 0.82, 0.72, 0.65$ and Strategy 2 sets threshold $\tau = 0.8, 1.8, 3.4$, respectively. (b) compares the PSCP improvement for Strategy 1 and 2 under $\rho_{out} \approx 0.3$.

compared to no transmit subcell situation, versus the transmit subcell radius R_B from 0.5 to 0.9. Figure 11 (b) compares the C_S^E improvement for RWP and RD mobile Bob under given transmit outage probability ρ_{out} from 0.05 to 0.3. Here for the given transmit outage probability ρ_{out}, the minimum required subcell radius R_B is calculated for RWP and RD users, respectively. Then the corresponding R_B is employed into simulations to compare with no subcell scenarios. From Fig. 11 (b), we can see that higher outage probability ρ_{out} will result in more secrecy capacity improvement. Meanwhile, we can see when ρ_{out} goes from 0.05 to 0.3, the RWP Bob can achieve higher secrecy capacity improvement than RD user.

Figure 12 (a) compares secrecy capacity improvement strategies 1 and 2 (denoted by Strategy 1, 2 in the following paper) for RWP Bob to the scenario without secrecy improvement strategy, versus the normalized guard radius $0 < R_E^{min} \leq 1$. The requirement of transmit outage is set as $\rho_{out} \approx 0.1, 0.2, 0.3$. Strategy 1 sets transmit subcell radius $r_B = 0.82, 0.72, 0.65$ and Strategy 2 sets $\tau = 0.8, 1.8, 3.4$, respectively. The other parameters are all the same with the simulations in Fig. 4. Fig. 12 (a) shows Strategy 1 and 2 can both effectively increase the average secrecy capacity. The user's secrecy capacity improves when the subcell radius r_B becomes smaller or τ becomes larger. However, the smaller subcell or larger τ also causes higher transmit outage probability. A tradeoff between secrecy and transmit outage should be considered in the real application. Figure 12 (b) compares the PSCP improvement of Strategy 1 and 2 under $\rho_{out} \approx 0.3$. It shows that Strategy 1, 2 can both clearly improve the PSCP performance. Strategy 2 can achieve relatively higher performance than Strategy 1 under $\rho_{out} \approx 0.3$. It is illustrated by Fig. 13. Figure 13 compares the $P(C_S > 0)$ sample points of RWP user for Strategy 1 and 2 under $\rho_{out} \approx 0.3$. The guard zone radius (red circle) is sets as $R_E^{min} = 0.5$ and transmit subcell (green dot circle) of Strategy 1 is $r_B = 0.65$. Figure 13 (a), (b) simulated 10^4 sample points for Strategy 1 and 2, respectively. As shown in Fig. 13, for Strategy 1, all the $P(C_S > 0)$ points are constrained in the transmit subcell, because the communication is turned off outside the subcell. But for Strategy 2, Bob can still get some $P(C_S > 0)$ points outside the transmit subcell, which achieves higher PSCP performance.

VI. Future trends discuss

In this section, we extend the proposed model to other realistic scenarios, including users moving in other shapes of areas, and multiple non-cooperative and cooperative eavesdroppers.

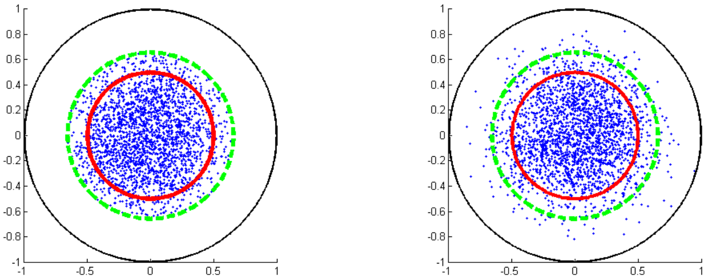
A. Users Move in Other Shapes of Areas

The proposed model can also be extended to Bob moves in other shapes of regions. For square region where length and width are $2x_m, 2y_m$, respectively, the RWP two-dimension approximate location PDF $f(x, y)$ with coordinate $0 \leq x \leq 2x_m, 0 \leq y \leq 2y_m$ [18] can be written as $f(x, y) \approx f(x)f(y) = \frac{9}{16x_m^3 y_m^3}(x^2 - x_m^2)(y^2 - y_m^2)$. For Alice located in square center, we can move the square center to coordinate $(0, 0)$ by substituting $x_0 = x - x_m$ and $y_0 = y - y_m$. By calculating the probability density function with random variable $d = \sqrt{x_0^2 + y_0^2}$, we can get SPDF expression $f(d)$ for square region. Based on $f(d)$, the secrecy performance can be analyzed by the similar methods in Section IV. For more complex shapes such as regular hexagon and triangle [17], the secrecy performance can be derived with the similar methods. Due to page limitation of this paper, we do not elaborately derive the SOP closed form expression for user moving in other shapes of areas, it can be left for the future work.

B. Multiple Non-cooperative Eavesdroppers

In this subsection, we extend the proposed model to multiple non-cooperative eavesdroppers scenario. Consider when there are N_E non-cooperative eavesdroppers in the region and each of them processes the received signal independently. Similarly, the worst-case situation is that all the eavesdroppers keep around the guard zone border $\bar{r}_E = R_E^{min}$. Based on [20], for a given distance $m = \bar{d}_{AB}^a$, we can get conditional PSCP $P_{N_E}(C_S > 0|m)$ under N_E multiple non-cooperative Eves as:

$$P_{N_E}(C_S > 0|m) = \prod_{i=1}^{N_E} \frac{i}{i + \frac{m}{k}}. \quad (59)$$



(a) (b)

Figure 13: The RWP Bob's $P(C_S > 0)$ sample points for Strategy 1 and 2 under $\rho_{out} \approx 0.3$. The red circle denotes guard zone ($R_E^{min} = 0.5$) and green dot circle denotes transmit subcell for strategy 1 with $r_B = 0.65$. (a), (b) simulated 10^4 points for Strategy 1 and 2, respectively.

For random mobile Bob, the $P_{N_E}(C_S > 0)$ can be written as

$$\begin{aligned} P_{N_E}(C_S > 0) &= \int_0^1 P_{N_E}(C_S > 0|m) f(m) dm \\ &= \int_0^1 \prod_{i=1}^{N_E} \frac{i}{i + \frac{m}{k}} f(m) dm, \end{aligned} \tag{60}$$

where $f(m)$ denotes the SPDF of the mobile user with normalized variable m (refer to Eqs. (12), (37)). Similarly, based on [20], the conditional SOP $P_{N_E}^{out}(R_S|m)$ under N_E multiple non-cooperative Eves can be written as

$$P_{N_E}^{out}(R_S|m) = 1 - e^{\lambda m} \prod_{i=1}^{N_E} \frac{i}{i + bm}, \tag{61}$$

where λ, b can refer to Eq. (25). Thus, for random mobile Bob, $P_{N_E}^{out}(R_S)$ can be written as

$$\begin{aligned} P_{N_E}^{out}(R_S) &= \int_0^1 P_{N_E}^{out}(R_S|m) f(m) dm \\ &= 1 - \int_0^1 e^{\lambda m} \prod_{i=1}^{N_E} \frac{i}{i + bm} f(m) dm. \end{aligned} \tag{62}$$

Achieving the closed form of SOP for RWP random mobility user under multiple Eves is not mathematically tractable. However, we can get the numerical results through Monte Carlo simulation.

C. Multiple Cooperative Eavesdroppers

The proposed model can also be extended to multiple cooperative eavesdroppers scenario. Consider the worst-case situation for legitimate users in downlink communication where all the N_E cooperative eavesdroppers are eavesdropping at the boundary of the guard zone with $\bar{r}_E = R_E^{min}$. Assume the N_E colluded eavesdroppers know each other's channel coefficients and perform MRC combine (maximum ratio combine) to get the largest united receive SNR [37]. Based on Eqs. (10) and (13) in [37], for a given distance $m = \bar{d}_{AB}^a$, the conditional PSCP and SOP under Reyleigh fading channel can be written as:

$$P_{N_E}(C_S > 0|m) = (1 + \frac{m}{k})^{-N_E}, \tag{63a}$$

$$P_{N_E}^{out}(R_S|m) = 1 - \frac{e^{\lambda m}}{(1 + bm)^{N_E}} \tag{63b}$$

where λ, b can refer to Eq. (25). Thus for random mobile Bob, we can derive PSCP and SOP as

$$P_{N_E}(C_S > 0) = \int_0^1 (1 + \frac{m}{k})^{-N_E} f(m) dm, \tag{64a}$$

$$P_{N_E}^{out}(R_S) = \int_0^1 \left[1 - \frac{e^{\lambda m}}{(1 + bm)^{N_E}} \right] f(m) dm \tag{64b}$$

where $f(m)$ denotes SPDF of the mobile user with normalized variable m (refer to Eqs. (12), (37)). Due to page limitation of this paper, we do not elaborately derive the closed-form SOP expressions under multiple cooperative eavesdroppers, it can be left for the future work. However, based on Eq. (64), we can get the numerical results through Monte Carlo simulation. Obviously, the more clouded eavesdroppers will decrease the mobile user's secrecy performance. However, the legitimate users can utilize multiple antennas and artificial noise (AN) [23] to enhance secrecy, which will be studied in the future researches.

VII. Conclusions

In this work, we studied the impact of random mobility on physical layer security. We investigated the secrecy capacity under a random mobile receiver with a passive eavesdropper in a circular region. We considered secrecy under three typical random mobility models (RWP, RD, and BM) and provided a general analytical framework to analyze the ergodic secrecy capacity. We derived closed-form expressions of PSCP and SOP for RWP and RD users, respectively. By comparing the secrecy performance of the mobile users with MS static user, we verified that the RWP users can achieve significant higher secrecy performance compared to the others. We further investigated the secrecy for RWP users with pause time and provided two types of practical secrecy improvement strategies for mobile users. Finally, we extended our model to the cases of nodes moving in other shapes of areas, and multiple non-cooperative and cooperative eavesdroppers.

References

[1] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[2] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks,"

IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 44–58, Jan. 2013.

[3] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Commun. Mag*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[4] L. Hu, H. Wen, B. Wu, F. Pan, R. F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219–228, Feb 2018.

[5] R. Jin, X. Du, K. Zeng, L. Huang, L. Xiao, and J. Xu, "Delay analysis of physical-layer key generation in dynamic roadside-to-vehicle networks," *IEEE Trans. Veh. Technol*, vol. 66, no. 3, pp. 2526–2535, Mar. 2017.

[6] X. Du and H. h. Chen, "Security in wireless sensor networks," *IEEE Wireless Commun.*, vol. 15, no. 4, pp. 60–66, Aug. 2008.

[7] A. D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[9] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Letter*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[10] J. Bai, X. Tao, J. Xu, and Q. Cui, "The secrecy outage probability for the ith closest legitimate user in stochastic networks," *IEEE Commun. Letter*, vol. 18, no. 7, pp. 1230–1233, Jul. 2014.

[11] D. S. Karas, A. A. Boulogeorgos, and G. K. Karagiannidis, "Physical layer security with uncertainty on the location of the eavesdropper," *IEEE Wireless. Commun. Letter*, vol. 5, no. 5, pp. 540–543, Oct. 2016.

[12] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Veh. Technol*, vol. 65, no. 8, pp. 6146–6158, Aug. 2016.

[13] X. X. L. Tao, Z. Yan and Z. Shidong, "Mean physical-layer secrecy capacity in mobile communication systems," *Journal of Tsinghua University*, vol. 55, no. 11, pp. 1241–1245, 2015.

[14] J. Wang, J. Lee, and T. Q. S. Quek, "Best antenna placement for eavesdroppers: Distributed or co-located?" *IEEE Commun. Letter*, vol. 20, no. 9, pp. 1820–1823, Sept. 2016.

[15] T. X. Zheng, H. M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lette*, vol. 18, no. 8, pp. 1299–1302, Aug. 2014.

[16] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, Jun. 2013.

[17] E. Hyytia, P. Lassila, and J. Virtamo, "Spatial node distribution of the random waypoint mobility model with applications," *IEEE Trans. Mobile Comput.*, vol. 5, no. 6, pp. 680–694, Jun. 2006.

[18] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 2, no. 3, pp. 257–269, Jul. 2003.

[19] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[20] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *2007 IEEE ISIT*, Jun. 2007, pp. 1301–1305.

[21] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," *IEEE Commun. Letter*, vol. 21, no. 3, pp. 524–527, Mar. 2017.

[22] J. Tang, H. Wen, L. Hu, H. Song, G. Zhang, F. Pan, and H. Liang, "Associating MIMO beamforming with security codes to achieve unconditional communication security," *IET Communications*, vol. 10, no. 12, pp. 1522–1531, 2016.

[23] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," in *2016 IEEE ICC*, May 2016, pp. 1–5.

[24] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive base station cooperation for physical layer security in two-cell wireless networks," *IEEE Access*, vol. 4, pp. 5607–5623, 2016.

[25] H. Wen, J. Tang, J. Wu, and H. Song, "A cross-layer secure communication model based on discrete fractional fourier fransform (DFRFT)," *IEEE Trans. Emerg. Top. Comput.*, vol. 3, no. 1, pp. 119–126, Mar. 2015.

[26] J. Tang, H. H. Song, F. Pan, H. Wen, B. Wu, Y. Jiang, X. Guo, and Z. Chen, "A MIMO cross-layer precoding security communication system," in *2014 IEEE CNS*, Oct. 2014, pp. 500–501.

[27] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[28] K. Govindan, K. Zeng, and P. Mohapatra, "Probability density of the received power in mobile networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3613–3619, Nov. 2011.

[29] C. Bettstetter, H. Hartenstein, and X. P. Costa, "Stochastic properties of the random waypoint mobility model," *Wireless Networks*, vol. 10, no. 5, pp. 555–567, 2004.

[30] P. Nain, D. Towsley, B. Liu, and Z. Liu, "Properties of random direction models," in *IEEE INFOCOM*, vol. 3, Mar. 2005, pp. 1897–1907 vol. 3.

[31] V. A. Aalo, C. Mukasa, and G. P. Efthymoglou, "Effect of mobility on the outage and ber performances of digital transmissions over Nakagami-m fading channels," *IEEE Trans. Veh. Technol*, vol. 65, no. 4, pp. 2715–2721, Apr. 2016.

[32] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[33] S. C. Lin and C. L. Lin, "On secrecy capacity of fast fading mimome wiretap channels with statistical csit," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3293–3306, Jun. 2014.

[34] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[35] F. B. Hildebrand, *Advanced calculus for applications*. Prentice-Hall Englewood Cliffs, NJ, 1962, vol. 63.

[36] A. Wiesel, J. Goldberg, and H. Messer-Yaron, "SNR estimation in time-varying fading channels," *IEEE Trans. Wireless Commun.*, vol. 54, no. 5, pp. 841–848, May 2006.

[37] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and $varepsilon$-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sept 2011.

PLACE
PHOTO
HERE

Jie Tang was born in Chengdu, P.R.China. He achieved Ph.D. degree from Communication and information system at University of Electronic Science and Technology of China (UESTC), P.R.China. He is also a visiting scholar in George Mason University, Fairfax, U.S.A. His current main interests lie in wireless communication security and cyber security.

PLACE
PHOTO
HERE

Monireh Dabaghchian received the B.S. and M.S. degrees both in Electrical Engineering-Communications from University of Tabriz, Tabriz, Iran in 2006 and 2009, respectively. She is currently a Ph.D. student in the Electrical and Computer Engineering Department at George Mason University, Fairfax, VA, USA. Her research interests are broadly in theoretical machine learning, online learning algorithms, Multi-armed-bandit, statistical learning, information theory and their applications in security and privacy of wireless communication and spectrum sharing networks.

PLACE
PHOTO
HERE

Kai Zeng is an associate professor in the Department of Electrical and Computer Engineering at George Mason University. He received his Ph.D. degree in electrical and computer engineering from Worcester Polytechnic Institute (WPI) in 2008. He was a postdoctoral scholar in the Department of Computer Science at University of California, Davis (UCD) from 2008 to 2011. He worked in the Department of Computer and Information Science at the University of Michigan — Dearborn as an assistant professor from 2011 to 2014. He was a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) award in 2012. He won the Excellence in Postdoctoral Research Award at UCD in 2011 and Sigma Xi Outstanding Ph.D. Dissertation Award at WPI in 2008. He is an Editor of IEEE Transactions on Wireless Communications. His current research interests are in cyber-physical system security and privacy, physical layer security, network forensics, and cognitive radio networks.

PLACE
PHOTO
HERE

Hong Wen was born in Chengdu, P. R. China. She received her Ph.D. degree in Communication and Computer Engineering Dept. at the Southwest Jiaotong University (Chengdu, P. R. China) in 2004. Then she worked as an professor in the University of Electronic Science and Technology of China (UESTC), P. R. China. From January 2008 to August 2009, she was a visiting scholar and postdoctoral fellow in the ECE Dept. at University of Waterloo. Her current main interests lie in wireless communication systems security.