School of Engineering and Applied Science (SEAS), Ahmedabad University

B.Tech(ICT) Semester V: Wireless Communication (CSP 311)

- Group No : 15
- Group Members:
  Shyam Patel (AU1741030)
  Ratnam Parikh (AU1741036)
  Dhairya Dudhatra(AU1741058)
  Jinesh Patel (AU1741076)
  Nisarg Shah (AU1741087)
- Project Title:

  1) Impact of Mobility on Physical Layer Security over Wireless Fading Channels

  2) Include the new title based on your contributions.

1 Introduction

1.1 Background

Write three detailed paragraphs as instructed below.

- First paragraph includes the general discussion of topic.
- A steadily growing component of modern communication systems nowadays is based on wireless technologies that make use of smaller and more mobile and portable electronic devices.The issues of privacy and security in wireless communication networks have taken on an increasingly important role as these networks continue to flourish worldwide. Traditionally, security is viewed as an independent feature with little or no relation to the remaining data communication tasks and, therefore, state- of-the-art encryption algorithms are insensitive to the physical nature of the wireless medium. For a Typical Eavesdropper Scenario. To meet this challenge, system designers have traditionally borrowed cryptography techniques and implemented at the upper layers of the Networks protocol stack. The computational resource-intensive-needy nature of cryptography-based security algorithms however does not scale well when employed in devices which are continuously growing smaller and smaller in size and have reduced and lower power constraints. Lighter weight security implementations are needed for this new generation of smaller devices, especially as the development of Internet of Things devices continues at an ever-increasing rate. Physical Layer Security is a collection of different security techniques that seek to

exploit the random nature of wireless channels to either obscure the information being exchanged over the channel and/or provide a mechanism to generate private keys that can then be used to facilitate encrypted communications Thus need to provide a light-weight security strategy for these systems has become a more important problem. While the underlying techniques of PLS(Physical Layer Security) have been known for some time, the potential secrecy benefits of them need further investigation.The need to deliver secure communications utilizing wireless systems is an increasingly complex challenge given both the broadcast nature of the wireless medium and the rapid advancements in technology available to potential eavesdroppers.

- Second paragraph includes the general related work (must include 10-15 related references e.g [1]) During the past decades, physical layer security has been widely investigated since Wyner proposed the wiretap channel model [1]. For Rayleigh fading wiretap channel, the secrecy outage probability (SOP) was defined and the ergodic secrecy capacity [2] [3] 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 [4-9]. The challenge in taking the path loss factor in consideration for the physical layer secrecy lies in that the location of the passive eavesdropper is unknown to legitimate users. The stochastic geometry theory [10] 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 [4-9].

- Third paragraph includes more closely related work including your base article (must include 3-4 closely related references) For the networks with random mobile nodes, [28] derived the probability density distribution function (PDF) of the received power under the Random Way point Model [29] and Random Direction RD mobility [30] models. The authors derived the mathematical expressions for path loss exponent of 4 in terms of confluent hyper geometric 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.

1.2 Motivation

Most existing work study physical layer secrecy with static Eavesdropper or mobile/static legitimate User and Proper Knowledge of CSI**(Channel State Information)** or Perfect CSI at Receiver side.The distance of Eve to Base station was assumed to be fixed and Time-invariant.Though in many scenarios of Wireless network Eve can be mobile e.g., People sharing ride with you in cab,bus or People normally walking along the street.So Mobility of Eavesdropper is the case which needs to studied.

1.3 Contributions

- Justify contribution-1 in detail
- Justify contribution-2 in detail
- Justify contribution-3 in detail

2 Performance Analysis of Base Article

- List of symbols and their description

Symbol	**Description**
$P(C_s > 0)$	Positive Secrecy Capacity Probability (PSCP)
$P^{out}(R_s)$	Secrecy Outage Probability (SOP)
$f(d)$	Spatial node distance Probability Density distribution Function (SPDF)
P	
M	

- **System Model/Network Model** : Insert the image of system model used in your base article and/or in your new work and clearly describe the channel, the transmitted signal (e.g BPSK,QAM etc.,) and the nature of noise.

  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 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 starts from 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. $t_{p,1}$ (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 : First, Bob randomly starts from point D_0 in the circular region. Then, he randomly chooses a direction θ_1 ($0 \geq \theta_1 \geq 2\pi$) and moves with a constant speed v_1 ($v_{min} \geq v_1 \geq v_{max}$) for a random period of time t_1 ($t_{min} \geq t_1 \geq t_{max}$). He may pause for a random time $t_p, i(tp, mintp, itp, max).Then, hechoosesanewdirection2andmovestoitwithanewspeedv2underanewtraveltimet2, and$

$\theta_i + \pi/2 \bmod 2\pi$ 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: Assume that Alice employs a secrecy guard zone with radius R E Guar d [12] to guarantee Eve's distance r E R E Guar d 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. We assume Eve knows Alice's location and the secrecy guard zone R E Guar d . 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 Guar d (Eve can be static or move around the guard zone). This model is illustrated in Fig. 1. Next, consider 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 Guar d to prevent Eve from approaching too close to him. The eavesdropping signal quality for Eve from Bob is related to her 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.

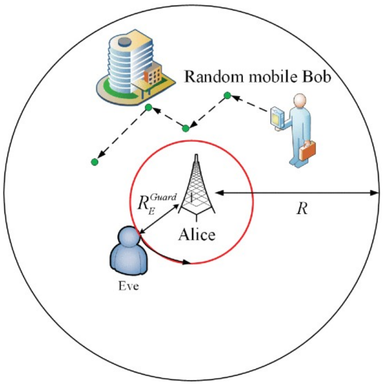
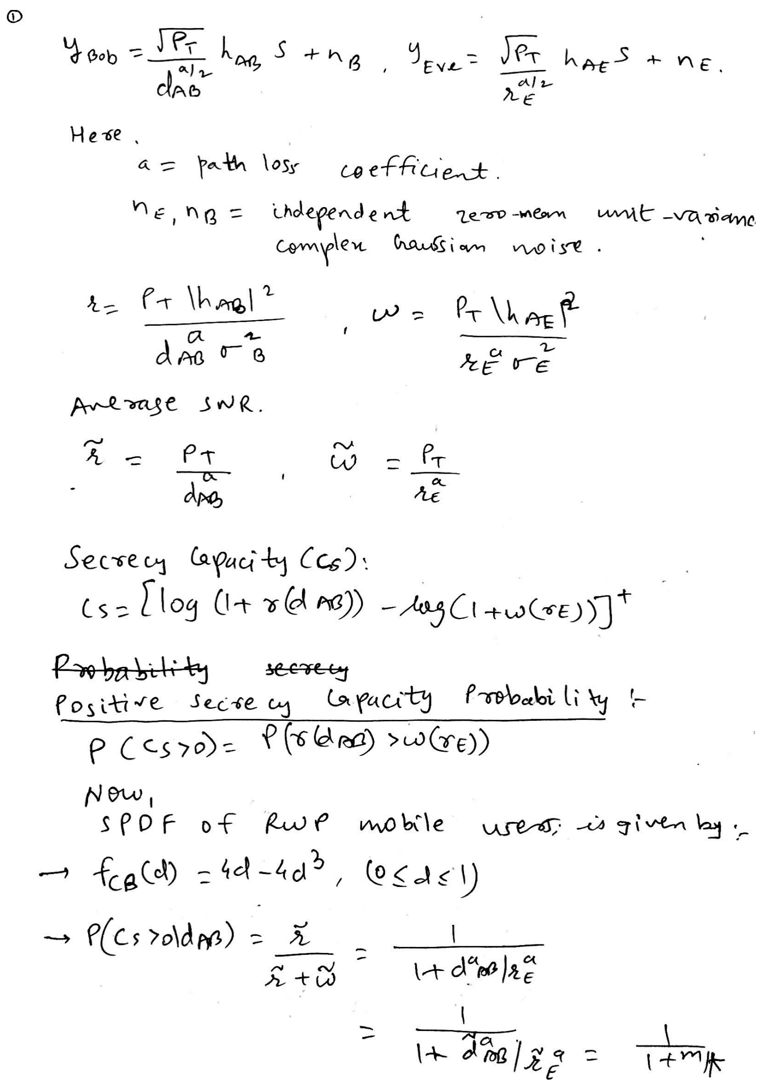


Figure 1:

- Detailed derivation of performance metric-I
- Detailed derivation of performance metric-II (add if base article contains more performance metric)

3 Performance Analysis of New contributions

- System Model
- Detailed derivation of performance metric-I
- Detailed derivation of performance metric-II (add if your have more performance metric)



①

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

Here,

a = path loss coefficient.

n_E, n_B = independent zero-mean unit-variance complex Gaussian noise.

$$\gamma = \frac{P_T |h_{AB}|^2}{d_{AB}^{a} \sigma_B^2} , \quad \omega = \frac{P_T |h_{AE}|^2}{r_E^{a} \sigma_E^2}$$

Average SNR.

$$\tilde{\gamma} = \frac{P_T}{d_{AB}^{a}} , \quad \tilde{\omega} = \frac{P_T}{r_E^{a}}$$

Secrecy Capacity (C_S):

$$C_S = [\log (1+ \gamma(d_{AB})) - \log(1+\omega(r_E))]^+$$

~~Probability~~ ~~secrecy~~

Positive secrecy Capacity Probability :-

$$P(C_S > 0) = P(\gamma(d_{AB}) > \omega(r_E))$$

Now,

SPDF of RWP mobile users, is given by :-

$$\rightarrow f_{CB}(d) = 4d - 4d^3 , \quad (0 \leq d \leq 1)$$

$$\rightarrow P(C_S > 0 | d_{AB}) = \frac{\tilde{\gamma}}{\tilde{\gamma} + \tilde{\omega}} = \frac{1}{1 + d_{AB}^{a} / r_E^{a}}$$

$$= \frac{1}{1 + \tilde{d}_{AB}^{a} / \tilde{r}_E^{a}} = \frac{1}{1+m}$$

Figure 2:

4 Numerical Results

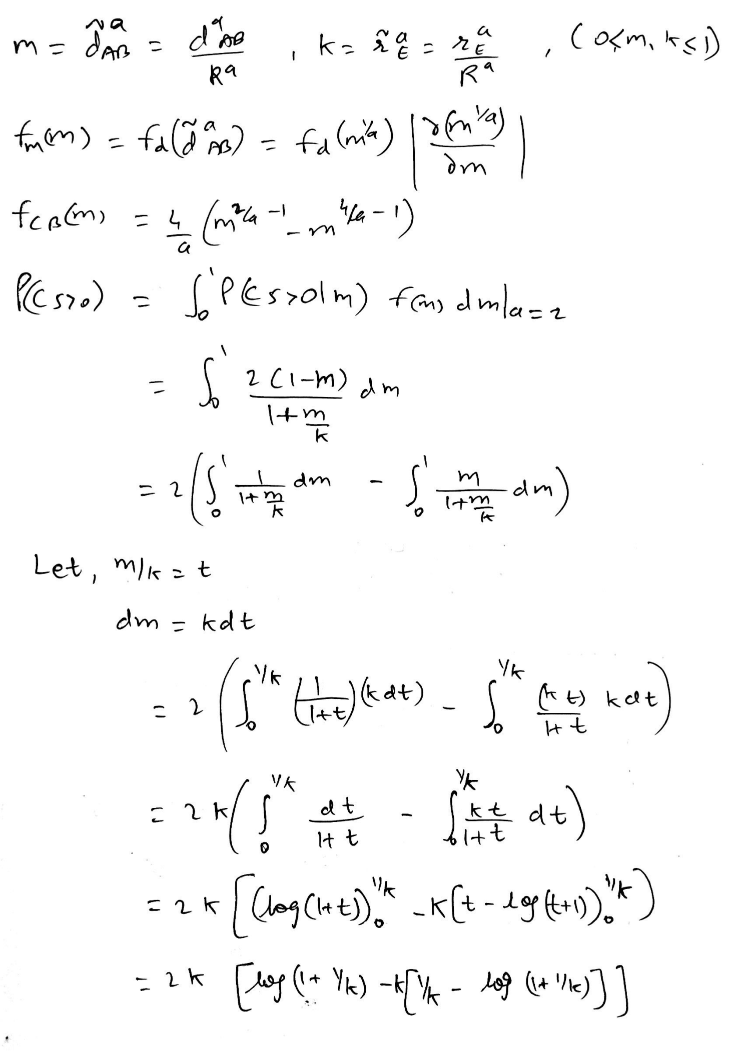
4.1 Simulation Framework

This paragraph must include the values of all controlling parameters set in you simulations, no. of montecarlo iterations, etc.

4.2 Reproduced Figures

- Reproduced Figure-1

  Insert two figures side by side in a same row. The left figure is first figure of your base article (You can crop this). Name this as Figure 1B (Base stands for base article). And the right figure should include the corresponding reproduced figure that you have generated (along with legends). Name this as Figure 1R (R stands for reproduce figure)



$$m = \tilde{d}_{AB}^{a} = \frac{d_{AB}^{a}}{R^{a}} \quad , \quad k = \tilde{r}_{E}^{a} = \frac{r_{E}^{a}}{R^{a}} \quad , \quad (0 < m, k \leq 1)$$

$$f_m(m) = f_d(\tilde{d}_{AB}^{a}) = f_d(m^{1/a}) \left| \frac{\partial (m^{1/a})}{\partial m} \right|$$

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

$$P(C_S > 0) = \int_0^1 P(C_S > 0 \mid m)\, f(m)\, dm \Big|_{a=2}$$

$$= \int_0^1 \frac{2(1-m)}{1+\frac{m}{k}}\, dm$$

$$= 2\left(\int_0^1 \frac{1}{1+\frac{m}{k}}\, dm - \int_0^1 \frac{m}{1+\frac{m}{k}}\, dm\right)$$

Let, $m/k = t$

$$dm = k\,dt$$

$$= 2\left(\int_0^{1/k} \left(\frac{1}{1+t}\right)(k\,dt) - \int_0^{1/k} \frac{(k\,t)}{1+t}\, k\,dt\right)$$

$$= 2k\left(\int_0^{1/k} \frac{dt}{1+t} - \int_0^{1/k} \frac{k\,t}{1+t}\, dt\right)$$

$$= 2k\left[\left(\log(1+t)\right)_0^{1/k} - k\left[t - \log(t+1)\right)_0^{1/k}\right)$$

$$= 2k\left[\log(1+1/k) - k\left[1/k - \log(1+1/k)\right]\right]$$

Figure 3:

Describe the figure in detail(for e.g Figure 1B and 1R shows the plot of P_d versus P_f) for diferent controloing parameters(eg. sample size) and derive the inference.

- Reproduced Figure-2

  Follow in the similar way as instructed above. Name the figures as Figure 2R and 2B.

  Describe the figure in detail and derive the inference.

4.3 New Results

- New Result-1

  Insert the the new results and explain in detail as instructed above.

- New Result-2

Insert the the new results and explain in detail as instructed above.

- New Result-3

  Insert the the new results and explain in detail as instructed above.

5 Conclusions

- Derive conclusion-1 from the new work. This should be in sync with the motivation of tour work and the project definition/Title
- Derive conclusion-2 from the new work. This should be in sync with the motivation of tour work and the project definition/Title

6 Contribution of team members

6.1 Technical contribution of all team members

Enlist the technical contribution of members in the table. Redefine the tasks (e.g Task-1 as simualtion of fig.1 and so on)

Tasks	**Shyam Patel**	**Ratnam Parikh**	**Dhairya Dudhatra**	**Jinesh Patel**	**Nisarg Shah**
Task-1					
Task-2					
Task-3					

6.2 Non-Technical contribution of all team members

Enlist the non-technical contribution of members in the table. Redine the tasks (e.g Task-1 as report writing etc.)

Tasks	**Shyam Patel**	**Ratnam Parikh**	**Dhairya Dudhatra**	**Jinesh Patel**	**Nisarg Shah**
Task-1					
Task-2					
Task-3					

7 Submission checklist

This section provides the submission checklist for smooth and efficient submission process. (This is for your reference and please remove this while writing your report).

- Hardcopy of this project Report
- Hard copy of base article
- Hard copy of **turnitin report** (It should be less than 15 percent after excluding the bibliography)
- Hard copy of analysis (handwritten)
- Softcopy of above four documents in pan-drive/hard drive.
- Folder of matlab codes (with proper naming)
- Folder of new and reproduced results in .fig and .jpg format
- .pdf Scanned copy of analysis (handwritten)
- latex (.tex) file of the project report.

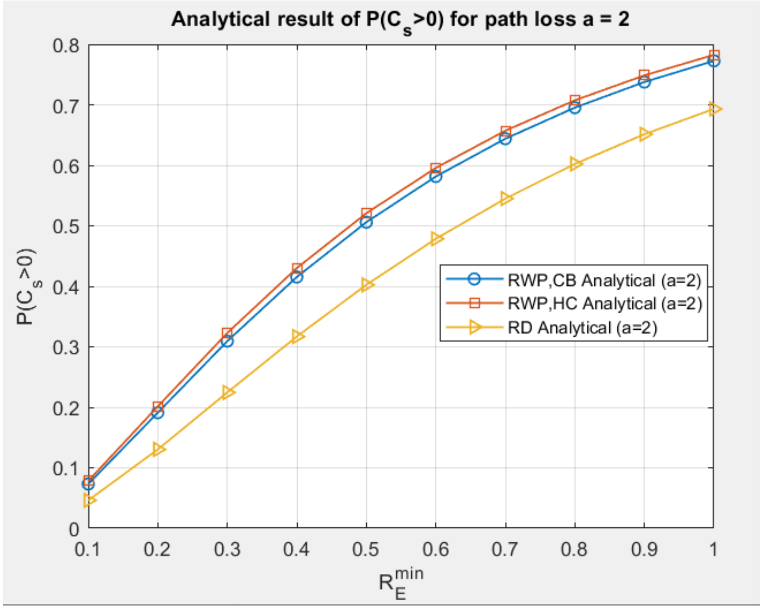


Figure 4:

References

[1] M. Sun, C. Zhao, S. Yan, and B. Li, “A novel spectrum sensing for cognitive radio networks with noise uncertainty,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4424–4429, 2017.

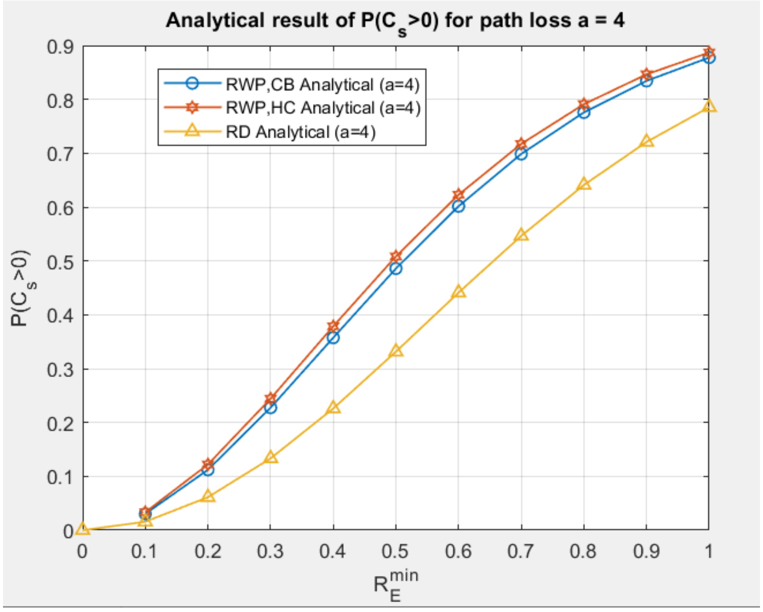


Figure 5:

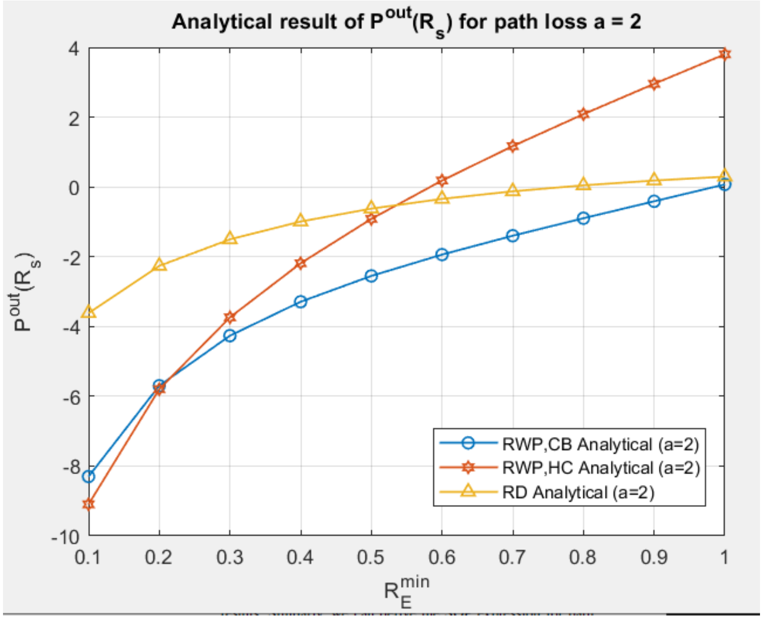


Figure 6:

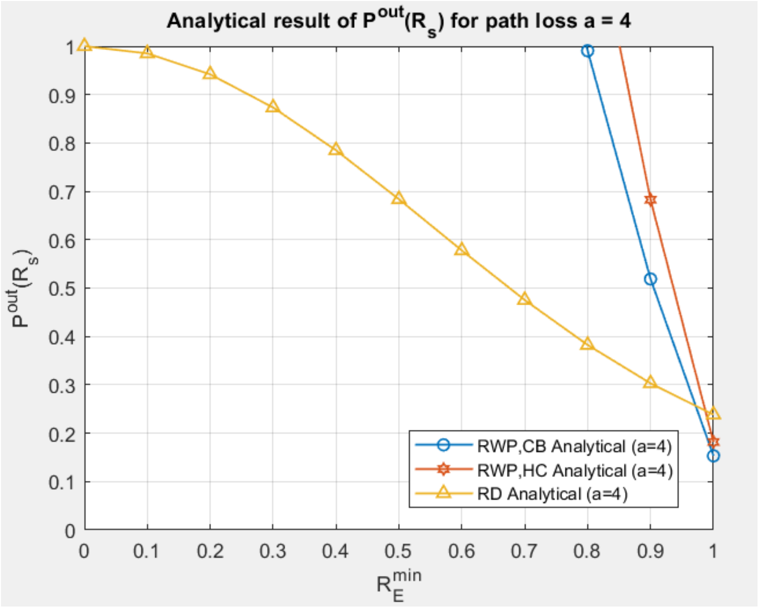

Analytical result of $P^{out}(R_s)$ for path loss a = 4
$P^{out}(R_s)$
R_E^{min}
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
RWP,CB Analytical (a=4)
RWP,HC Analytical (a=4)
RD Analytical (a=4)

Figure 7: