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

1 Introduction

1.1 Background

- 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.

- 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].

- For the networks with random mobile nodes, [11] derived the probability density distribution function (PDF) of the received power under the Random Way point Model [12] and Random Direction RD mobility [13] models. The authors derived the mathematical expressions for path loss exponent of 4 in terms of confluent hyper geometric function. In [14], 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 [11], [14]. 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

  The project is related to the effect of mobility on physical layer security. Here, in the base article the effect of mobility of legitimate user is taken into consideration. For new analysis we have also tried to bring in the effect of mobility of eavesdropper. The SPDF of the mobile eavesdropper is now taken into consideration. The SPDF is taken to be the same as that of mobile user which is specific for the Random Mobility Model(RWP) used in base article and our new analysis as the base system model.

2 Performance Analysis of Base Article

- List of symbols and their description

Symbol	Description
$P(C_s > 0)$	Positive Secrecy Capacity Probability (PSCP)
$P_{R_s}^{out}$	Secrecy Outage Probability (SOP)
$f(d)$	Spatial node distance Probability Density distribution Function (SPDF)
R_E^{Guard}	Secrecy guard zone
P_T	Transmit Power
a	path loss co-efficient
$\bar{d}_{AB}$ and $\bar{r}_E$	Normalized distances
R_s	desired Secrecy Rate
$\epsilon, \epsilon 1, \epsilon 2, \epsilon 3$	Parameters for SOP
R_s	the power to radius ratio with exponent

- **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 [15], [12], [13], 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 $t_{p,i}$ ($t_{p,min}$ $\geq t_{p,i} \geq t_{p,max}$). 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 $\theta_i = \theta_i + \pi/2 \bmod 2\pi$ at the border [30].

Eavesdropping model: Assume that Alice employs a secrecy guard zone with radius R_E^{Guard} [12] to guarantee Eve's distance $r_E \leq R_E^{Guard}$ 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 down-link connectivity, when Alice transmits secrecy data to Bob. We assume 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. Next, consider the up-link 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 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 up-link and down-link connections are considered symmetric. Without loss of generality, we only analyze the down-link connectivity in the rest of this paper.

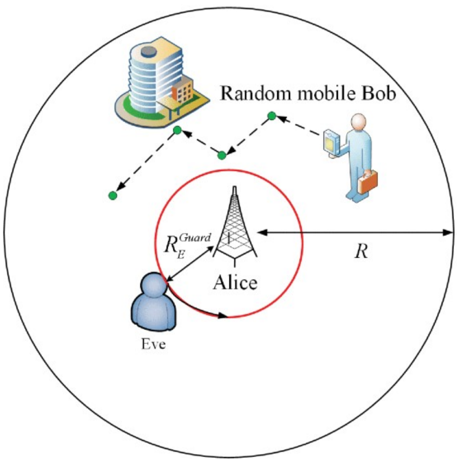

Figure 1:

- Detailed derivation of performance metric-I

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-varianc 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 :-

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

$\rightarrow$ $$P(C_s > 0 | d_{AB}) = \frac{\tilde{\gamma}}{\tilde{\gamma} + \tilde{\omega}} = \frac{1}{1 + d_{AB}^{a} / r_E^{a}} = \frac{1}{1 + \tilde{d}_{AB}^{a} / \tilde{r}_E^{a}} = \frac{1}{1+m}$$

Figure 2:

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

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

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

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

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

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

Let, $m/k = t$

$$dm = k\,dt$$

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

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

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

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

Figure 3:

$$= 2k\left[k\ln\left(1+\frac{1}{k}\right) + \ln(1+1/k) - 1\right]$$

2) Secrecy outage probability $p^{out}(R_s)$:-

$$p^{out}(R_s|d_{AB}) = P(C_s < R_s|d_{AB}) = 1 - \frac{e^{d^a_{AB}\left(\frac{1-2^{R_s}}{\rho_T}\right)}}{1+2^{R_s}\left(\frac{d^a_{AB}}{R_E^a}\right)}$$

Now, we need to scale the SOP for 'm'.

$$\therefore\ p^{out}(R_s|m) = 1 - \frac{e^{\frac{R^a(1-2^{R_s})m}{\rho_T}}}{1+\frac{2^{R_s}}{k}m}$$

For Random mobile Bob.

$$p^{out}(R_s) = \int_0^1 p^{out}(R_s|m)\, f(m)\, dm$$

$$= \int_0^1 p^{out}(R_s|m)\, f_{CB}(m)\, dm \quad k=2.$$

$$= 1 - 2\int_0^1 \frac{e^{\lambda m}}{1+bm}\, dm + 2\int_0^1 \frac{m e^{\lambda m}}{1+bm}\, dm$$

Here, $\lambda = \frac{R^a(1-2^{R_s})}{\rho_T}$, $b = \frac{2^{R_s}}{k}$.

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

$$\rightarrow \int_0^1 \frac{m e^{\lambda m}}{1+bm}\, dm = \frac{e^{\lambda}-1}{b\lambda} - \frac{f}{b}$$

substitute these in final equation

Figure 4:

$$p^{out}_{CB}(R_s) = 1 - 2\left(1+\frac{1}{b}\right)f + 2\frac{(e^{\lambda}-1)}{b\lambda}, \quad a=2.$$

$$= 1 - 2\left(1+\frac{1}{\frac{2^{R_s}}{k}}\right)\exp\left(-\frac{\lambda}{b}\right)\left[Ei\left(\lambda\left(\frac{1+b}{b}\right)\right) - Ei\left(\frac{\lambda}{b}\right)\right]$$

$$+ 2\,\frac{\left(e^{R^a(1-2^{R_s})/\rho_T} - 1\right)}{\left(\frac{2^{R_s}}{k}\right)\left(\frac{R^a(1-2^{R_s})}{\rho_T}\right)}$$

Figure 5:

3 Performance Analysis of New contributions

- System Model :- RWP Model **Mobile Bob** and **Mobile Eve**
- Detailed derivation of performance metric-I

New Analysis :-

→ In new analysis we consider Eve to be also mobile in RWP model.

→ For mobile user Bob in RWP model SPDF is given by, $f_B(d) = 4d - 4d^3$, $0 < d \le 1$

→ Now for a mobile Eve the SPDF will also remain same as it is following same model.

$\therefore f_E(d) = 4r - 4r^3$, $0 < r_e \le 1$

↳ distance of eve from legitimate transmitter.

Now, for calculation of PSCP

$$P(C_s > 0 \mid d_{AB}, r_E) \to P(C_s > 0 \mid m, k) = \frac{1}{1 + m/k}, \quad 0 < m, k \le 1$$

$$P(C_s > 0) = \int_{r_{Emin}}^{1} \int_{0}^{1} P(C_s > 0 \mid m, k) f(m, k) \, dm \, dk$$

$$= \int_{r_{Emin}}^{1} \int_{0}^{1} \left(\frac{1}{1 + m/k} \right) 2(1-m) \cdot 2(1-k) \, dm \, dk$$

$$= \int_{r_{Emin}}^{1} 2k\left(k \ln(1 + 1/k) + \ln(1 + 1/k) - 1\right) 2(1-k) \, dk$$

$$= \frac{-(r_{Emin})\left(r_{Emin}\left(2\left((r_{Emin}^2 - 2) \ln \frac{|r_{Emin}+1|}{|r_{Emin}|} - r_{Emin}\right) + 3\right) - 2\right) + 2\ln(|r_{Emin}+1|)}{2}$$

Figure 6: New Analysis-1

Second Approach:

$$h = \frac{g_x}{\sqrt{1+d_x^{a}}}$$

$g_x \rightarrow$ rayleigh channel

$d_x^{a} \rightarrow$ distribution of distance

We can get the received SNR PDF.

$$CDF = \int_0^1 \int_0^{yz} \left(x e^{-x^2/2}\right)\left(4y - 4y^3\right) dx\, dy$$

$$= \frac{8 - 8e^{-z^2/2} - 4z^2 + z^4}{z^4}$$

Now to obtain PDF, we differentiate CDF.

$$= \frac{d}{dz}\left(\frac{8 - 8e^{-z^2/2} - 4z^2 + z^4}{z^4}\right)$$

$$PDF = \frac{-8z + 8e^{-z^2/2} z + 4z^3}{z^4} - \frac{4\left(8 - 8e^{-z^2/2} - 4z^2 + z^4\right)}{z^5}$$

Now, we can estimate this with Average outage probability.

$$OP = \int_{\gamma th}^{\infty} PDF\, dz$$

$$= \int_{\gamma th}^{\infty}\left(\frac{-8z + 8e^{-z^2/2} z + 4z^3}{z^4}\right) - 4\left(\frac{8 - 8e^{-z^2/2} - 4z^2 + z^4}{z^5}\right) dz$$

$$= \frac{4\left(-2 + 2e^{-x^2/2} + x^2\right)}{x^4}$$

Figure 7: New Analysis-2

→ Considering PDF: $f_D(d) = \frac{d}{4ab}\left[\pi + 2\arcsin\left(\frac{2(d^2-(b-h)^2)}{d^2} - 1\right)\right]$

$$h = \frac{g_\alpha}{\sqrt{1+d_{\cancel{x}}^{\alpha}}}$$

g_α → Rayleigh

d^α → Distribution of Distance

$$\text{CDF} = \int_0^\infty \int_0^{Y_2} \left(x e^{-x^2/2}\right) \frac{d}{4ab}\left[\pi + 2\arcsin\left(\frac{2(d^2-(b-h)^2)}{d^2} - 1\right)\right]$$

$$= \frac{1}{4ab}\int_0^\infty \int_0^{y_2} \left(x e^{-x^2/2}\right)dx \left(y\left[\pi + 2\arcsin\left(\frac{2(y^2-(b-h)^2)}{y^2} - 1\right)\right] dy\right)$$

= Can not converged from 0 to ∞

→ Some integrals ~~were~~ did not converge and we tried to use Table of Integrals.

→ But PDF $f_D(d)$ is for impact of mobility in Linear Path. And so this PDF was not useful for this derivation.

Figure 8: New Analysis-3

4 Numerical Results

4.1 Reproduced Figures

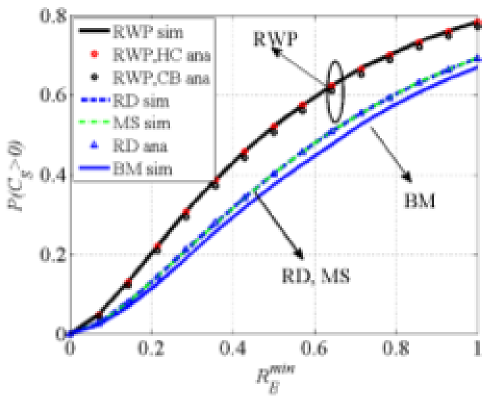

Figure 9: Base Article figure

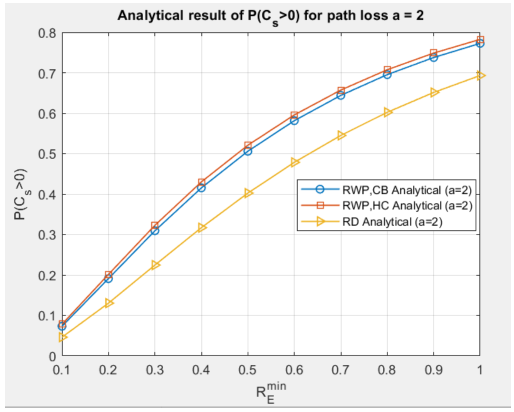

Figure 10: Reproduced figure

•

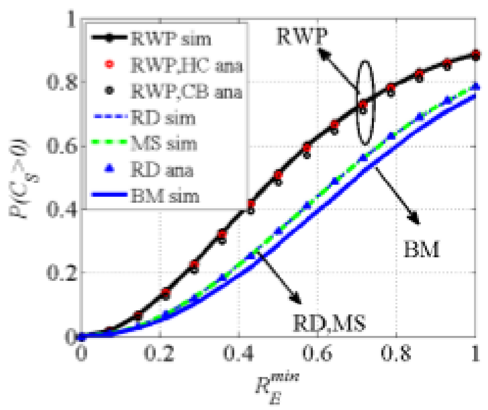

Figure 11: Base Article figure

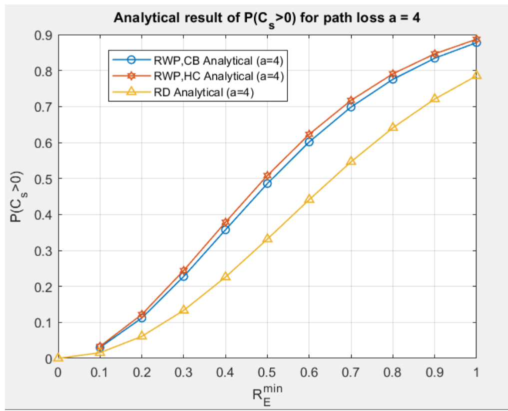

Figure 12: Reproduced figure

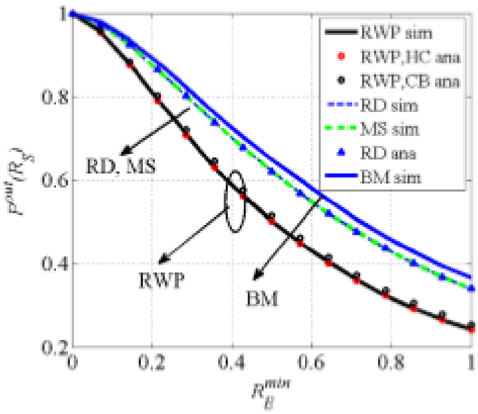

Figure 13: Base Article figure

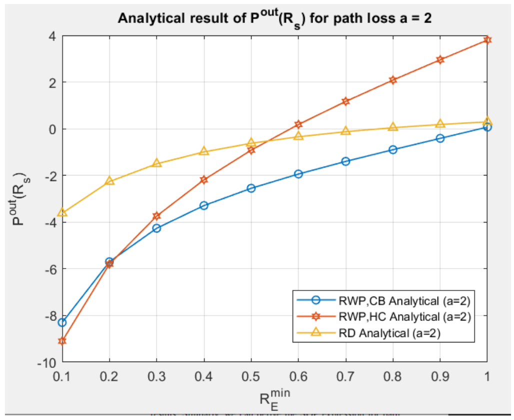

Figure 14: Reproduced figure

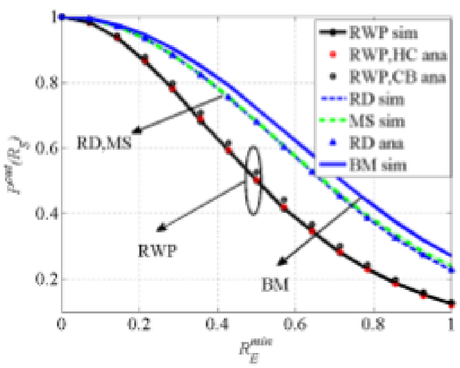

Figure 15: Base Article figure

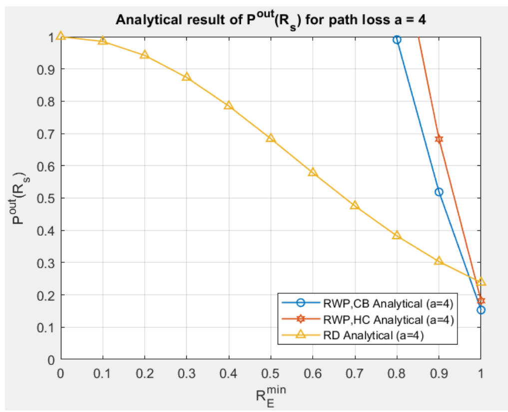

Figure 16: Reproduced figure

4.2 New Results

- New Result

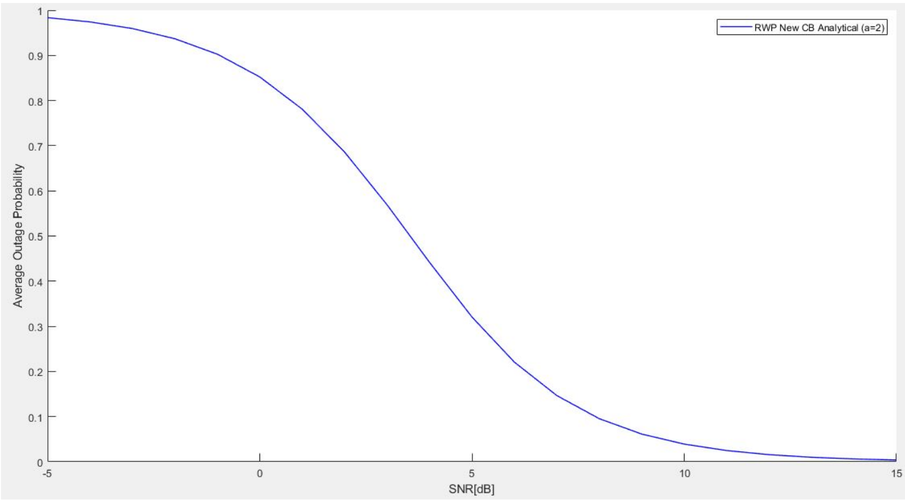

Figure 17: New Analysis

5 Conclusions

- In the existing article, only Bob was moving and Eavesdropper was static. But as soon as the mobility of Eavesdropper was considered the Positive Secrecy Capacity Probability on user's side gets better. Also impact of mobility will be seen on Secrecy outage probability. Secrecy Rate of user will be increased.

6 Contribution of team members

6.1 Technical contribution of all team members

Tasks	**Shyam Patel**	**Ratnam Parikh**	**Dhairya Dudhatra**	**Jinesh Patel**	**Nisarg Shah**
Existing Derivation		Y			Y
Analytical	Y		Y	Y	
Simulation	Y		Y	Y	
New Derivation		Y			Y
New Analytical	Y		Y	Y	

6.2 Non-Technical contribution of all team members

Tasks	**Shyam Patel**	**Ratnam Parikh**	**Dhairya Dudhatra**	**Jinesh Patel**	**Nisarg Shah**
Report	Y	Y	Y	Y	Y
Paper Reading	Y	Y	Y	Y	Y
Brain Storming	Y	Y	Y	Y	Y

7 References

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

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

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

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

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

[15] 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.