International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-10, August 2020

On the Secrecy Outage of Wiretap Channel

Reshmitha Bethi, Sujatha Allipuram

***Abstract*: In wireless data transmission, providing security over communication channels has become a growing concern. Traditionally cryptography is used to provide secrecy. However, physical layer studies show that it allows a huge potential in providing secrecy. In this paper, secrecy outage probability is derived for Rician fading channels. A new secrecy metric Generalized Secrecy Outage Probability(GSOP) derivation is considered to overcome the limitation of traditional Outage probability for both passive and active cases of eavesdropping.**

Keywords: Active eavesdropper, fading, secrecy outage probability, wireless communication.

I. INTRODUCTION

The Information-theoretic study differentiates the main channel from the eavesdropper channel by developing comparative metrics between both channels, such as channel capacities and signal to noise ratios(SNR). It was understood that randomness is one of the main elements in the physical layer security implementations. In this paper, we shall study the effectiveness of fading in providing secure communication. Shannon's cipher system [1] was the first model considered with metrics such as entropy, mutual information, and conditional entropy. Shannon's notion of perfect secrecy depends on Eve's capacity to decode D from X where D is the original message and X is the code word obtained after encoding message with a key, K. Thus, K played a major role in his studies. When entropy of K is greater than D, perfect secrecy is achieved. Shannon's work was extended by Wyner[2] later by Csiszár and Körner[3]. They proved the existence of the channel codes which resulted in the possibility of secure and reliable transmission when we consider discrete memoryless channels. These codes are called wiretap codes.

Perfect secrecy is defined as zero mutual information; compromising this perfect secrecy condition, strong secrecy is defined as zero information leakage; Weak secrecy is when the information leakage is zero on average but not on each channel use. Their studies were extended to Gaussian wiretap channels. In [4], term secrecy capacity Cs is defined and was understood that it is the difference between the capacities of the main and wiretap channels. The limitations of Gaussian wiretap channels can be overcome by considering communication schemes exploiting feedback such as secret key agreement schemes by Maurer [5]. Thangaraj et al. [12], shown how low-density parity-check(LDPC) codes can achieve the secrecy capacity of the erasure wiretap channel in an asymptotic manner. These codes are shown to be used in providing perfect secrecy communications at rates below the secrecy capacity of other channels. Transmission and power rate allocation schemes were presented for secure communication through fading channels by Gopala et al. [7], Liang et al [8], and Li et al [9], in which an ergodic secrecy capacity of fading channels was derived. Parada and Blahut [6] established the secrecy capacity of various degraded fading channels. Barros and Rodrigues [10] provided a detailed characterization of the outage secrecy capacity of slow fading channels, and in such channels, it is shown that information-theoretic security is guaranteed by fading alone, and this is true even in the case where average Signal-to-noise ratio (SNR) of a legitimate receiver—without the need for public communication over a feedback channel. Later in [13], Rician fading channels are considered and, a closed-form expression for strictly positive secrecy capacity (SPSC) is derived.

II. SYSTEM MODEL

We consider the wireless system setup depicted in Fig.1, where a legitimate user (Alice) wants to send a message to another user (Bob). A third party (Eve) is also capable of intercepting the information. And it is also considered that Alice has channel side information of Bob but does not have CSI of Eve. Here we consider quasi-static fading channels.

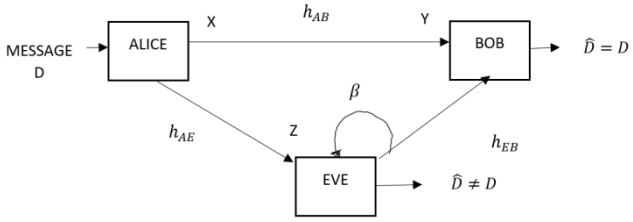

Fig.1. System model

Message D is encoded into code word X= [x(1),x(2),..x(i)…x(n)] which is transmitted through a quasi-static fading channel. Y is the output of the main channel (channel between Alice and Bob) received at Bob.

$$Y = Xh_{AB} + N_m \quad (1)$$

h_{AB} is the channel fading coefficient between Alice and Bob. N_m is the zero-mean circularly symmetric complex Gaussian noise of the main channel. The third party i.e. is Eve, is capable of eavesdropping the signal sent by Alice by observing the channel output of another independent fading channel. Z is the output of the wiretap channel (channel between Alice and Eve) received at Eve.

Revised Manuscript Received on August 30, 2020.
* Correspondence Author
Reshmitha Bethi, Department of ECE, G. Narayanamma Institute of Technology and Science, India. E-mail: reshmitha.bethi@gmail.com
Sujatha Allipuram, Department of ECE, G. Narayanamma Institute of Technology and Science, India. E-mail: allipuramsujathareddy@gmail.com

$$Z=Xh_{BE}+N_w \quad (2)$$

h_{AE} is the channel fading coefficient between Alice and Eve. N_w is the zero-mean circularly symmetric complex Gaussian noise of wiretap channel.

The input is subjected to a power constraint that is

$$\frac{1}{n}\sum_{i=1}^{n} E[|X(i)|^2] \le P_t ,$$

where P_t corresponds to average transmit signal power, E[•] is the average value. Fig.1. depicts the system model for active eavesdropper that is Eve interrupts the communication between Alice and Bob. P_j is the jamming power used by Eve. h_{AE} is the fading coefficient of the channel between Eve and Bob . When P_j =0 then that means Eve is passive i.e., not interrupting the communication. Here we now consider passive Eavesdropper case.

Secure communications over quasi-static channels are determined by instantaneous fading realization. The instantaneous signal-to-noise ratio (SNR) at Bob's receiver is thus given by

$$M= P_t|h_{AB}|^2/N_M \quad (3)$$

Likewise, the instantaneous SNR at Eve's receiver is given by

$$W= P_t|h_{AE}|^2/N_W \quad (4)$$

III. SECRECY PERFORMANCE ANALYSIS

In the following Secrecy outage probability (SOP) and Generalized secrecy outage probability(GSOP) are derived. We consider Rician fading in the main channel, then the probability density function (PDF) of M takes the following form

$$f_M(m) = a(1+k_m)\exp(-k_m)\exp[-a(1+k_m)m] \times I_0\left[2\sqrt{ak_m(1+k_m)m}\right], (m \ge 0) \quad (5)$$

Where a=1/$E[M]$, k_m is the Rician factor defined as the ratio of signal power of the dominant path to the sum of the scattered path. E[M] is the average of M.

The cumulative distribution function (CDF) of M can be expressed as

$$F_M(m) = 1 - Q_1\left(\sqrt{2k_m}, \sqrt{2a(1+k_m)m}\right) \quad (6)$$

Where $Q_1(\bullet,\bullet)$ is first-order Marcum Q function defined as

$$Q_1(\alpha,\beta) = \int_\beta^\infty x\, exp\left[-\left(\frac{x^2+\alpha^2}{2}\right)\right] I_0(\alpha x)\, dx \quad (7)$$

Where α, β are non-negative real numbers and $I_0(\bullet)$ is modified Bessel function of the first kind of order zero.

Similarly, when we consider Rician fading in the wiretap channel, then the PDF and CDF of W respectively are

$$f_W(w) = b(1+k_w)\exp(-k_w)\exp[-b(1+k_w)w] \times I_0\left[2\sqrt{bk_w(1+k_w)w}\right], (w \ge 0) \quad (8)$$

Where b=1/$E[W]$, k_w is the Rician factor of eavesdropper channel, E[W] stands for the average of W.

$$F_W(w) = 1 - Q_1\left(\sqrt{2k_w}, \sqrt{2a(1+k_w)w}\right) \quad (9)$$

according to [4] the secrecy capacity of the quasi-static fading channel is

$$C_s = \frac{1}{2}\log\left(1+\frac{|h_{AB}|^2P_t}{N_M}\right) - \frac{1}{2}\log\left(1+\frac{|h_{AE}|^2P_t}{N_W}\right) \quad (10)$$

Here the secrecy capacity for one realization of the quasi-static fading channel, from equations (3), (4) and (10), is given as

$$C_s = \begin{cases} \log(1+M) - \log(1+W), M > W \\ 0 \qquad\qquad\qquad\quad , M \le W \end{cases} \quad (11)$$

A. Secrecy Outage Probability

Secrecy outage is the probability of secrecy capacity less than some target secrecy rate and is given as

$$P_0(R_s) = P(C_s < R_s) \quad (12)$$

where R_s is the target secrecy rate.

The secrecy outage probability is given as the following

$$P_0 = 1 - P_{C_s}$$

Where, P_{C_s} is the probability of secrecy capacity

$$P_{C_s} = P(C_S > \tau)$$

Here Pr(•) is the probability function, which implies

$$P_{C_s} = P\left(log\,\frac{1+M}{1+W} > R_s\right) \quad (13)$$

$$P_{C_s} = P\left[\frac{1+M}{1+W} > \exp(R_s)\right]$$

$$= P[M > (1+W)\exp(R_s) - 1]$$

$$= \int_0^\infty f_W(w)\left[\int_{(1+W)\exp(R_s)-1}^\infty f_M(m)dm\right]dw$$

Using the property of a probability density function that is

$$F_X(x) = \int_{-\infty}^{x} f_X(x)dx$$

$$1 - F_X(x) = \int_x^\infty f_X(x)dx$$

We obtain as the following

$$P_{C_s} = \int_0^\infty f_W(w)\,(1 - F_M((1+W)\exp(R_s) - 1))dw$$

$$= b(1+k_w)\exp(-k_w) \times \int_0^\infty exp[-b(1+k_w)w] \times I_0\left[2\sqrt{bk_w(1+k_w)w}\right] \times Q_1\left(\sqrt{2k_m}, \sqrt{2a(1+k_m)[\exp(R_s)(1+w]-1}\right) dw \quad (14)$$

When the value of k_m or k_w becomes zero the Rician distribution becomes Rayleigh distribution. Different combinations obtained are as follows

1. Rayleigh/Rayleigh ($k_m = k_w$=0)
2. Rayleigh/Rician ($k_m = 0, k_w > 0$)
3. Rician/Rayleigh($k_m > 0, k_w = 0$)
4. Rician/Rician($k_m > 0, k_w > 0$)

Equation (14) can also be used to characterize the following four cases. The first case can be reduced after substituting $k_m = k_w$=0, as the following

$$P_0 = 1 - b\int_0^{\infty} exp[-bw]\exp\left(-\frac{2a(\exp R_s(1+w)-1)}{2}\right)dw$$

$$= 1 - b\int_0^{\infty} exp[-bw]\exp(a - aexp(R_s) - aexp(R_s)w)\,dw$$

$$= 1 - b\int_0^{\infty} exp[a - aexp(R_s)]\exp(-b - aexp(R_s)e)\,dw$$

$$= 1 - bexp[a - aexp(R_s)]\int_0^{\infty}\exp(-b - aexp(R_s)w)\,dw$$

$$= \frac{b+aexp(R_s)-bexp(a-aexp(R_s))}{b+aexp(R_s)} \quad (15)$$

The second case can be reduced as the following after substituting $k_m = 0, k_w > 0$

$$P_0 = 1 - b(1+k_w)\times\exp(-k_w)\int_0^{\infty} exp[-b(1+k_w)w]\times I_0\left[2\sqrt{bk_w(1+k_w)w}\right]\times Q_1\left(0,\sqrt{2a[\exp(R_s)(1+w]-1}\right)dw \quad (16)$$

The third case can be reduced as the following after substituting $k_m > 0, k_w = 0$

$$P_0 = 1 - b\exp(0)\int_0^{\infty} exp[-bw]\times I_0[0] \times Q_1\left(\sqrt{2k_m},\sqrt{2a(1+k_m)[\exp(h)(1+w]-1}\right)dw$$

$$P_0 = 1 - b\int_0^{\infty} exp[-bw]\times Q_1\left(\sqrt{2k_m},\sqrt{2a(1+k_m)[\exp(R_s)(1+w]-1}\right)dw \quad (17)$$

The fourth case ($k_m > 0, k_w > 0$) can be given as the following

$$P_0 = 1 - b(1+k_w)\exp(-k_w)\int_0^{\infty} exp[-b(1+k_w)w]\times I_0\left[2\sqrt{bk_w(1+k_w)w}\right]\times Q_1\left(\sqrt{2k_m},\sqrt{2a(1+k_m)[\exp(R_s)(1+w]-1}\right)dw \quad (18)$$

The drawback of secrecy outage probability is it doesn't consider decodability of an eavesdropper, and cannot characterize how much information was leaked when the outage occurs. Thus a new metric was considered. General Secrecy outage probability(GSOP) [16] is the new secrecy metric that establishes a link between the secrecy outage probability and the decodability of the message by the eavesdropper. Fractional equivocation (Δ) was considered in this metric. This is defined as

$$\Delta = \frac{H(D|Z)}{H(D)} \quad (19)$$

D is the message sent, Z is the message Eve received. Δ quantifies the level at which Eve is confused.

General Secrecy outage probability is defined as

$$P_{GSOP} = P(\Delta < \alpha), \quad 0 < \alpha \le 1 \quad (20)$$

Where $0<\theta\le 1$ is the minimum acceptable fractional equivocation. Classical secrecy outage probability is simply θ = 1. 1-Δ gives the ratio of information leaked to eve to the entropy of the original message.

From [16] we have

$$\Delta = \begin{cases} 1, & if\ W < 2^{R_b-R_s}-1 \\ \frac{R_b-\log_2(1+W)}{R_s}, & if\ 2^{R_b-R_s}-1 < W < 2^{R_b}-1 \\ 0, & if\ 2^{R_b}-1 < W \end{cases} \quad (21)$$

GSOP translates to P (Δ < θ) =P (1 − Δ > 1 − θ), which tells us the probability of information leak greater than value 1- θ.

B. Generalized secrecy outage probability for passive Eavesdropper

GSOP in terms of SNR of eve is given as

$$P_{GSOP}=P\left(\frac{R_b-\log_2(1+W)}{R_s} < \alpha\right)$$
$$=P(R_b - \log_2(1+W) < R_s\alpha)$$
$$=P(\log_2(1+W) > R_b - R_s\theta)$$
$$=P((1+W) > 2^{R_b-R_s\alpha})$$
$$=P(W > 2^{R_b-R_s\alpha}-1)$$
$$\text{Let } 2^{R_b-R_s\alpha}-1 = \theta$$
$$P_{GSOP}= P(W \ge \theta), \quad 0 < \theta \le 1 \quad (22)$$
$$P(W \ge \theta)=P\left(\frac{|h_{AE}|^2P_t}{N_W} \ge \theta\right)$$
$$= P\left(|h_{AE}|^2 \ge \frac{\theta N_W}{P_t}\right)$$
$$= 1 - CDF\left(\frac{\theta N_W}{P_t}\right)$$
$$\text{Let } \frac{\theta N_W}{P_t} = A$$
$$= 1 - CDF(A) \quad (23)$$

Where $|h_{AE}|^2$ is fading coefficient of wiretap channel, P_t is the transmission power.

GSOP for Rician and Rayleigh distributions as follows

For Rician distribution, the GSOP is given as

$$P_{GSOP(RI)} = 1 - \left(1 - Q_1\left(\sqrt{2k_w},\sqrt{2b(1+k_w)A}\right)\right)$$
$$=Q_1\left(\sqrt{2k_w},\sqrt{2b(1+k_w)A}\right) \quad (24)$$

For Rayleigh distribution, the GSOP is given as

$$P_{GSOP(RA)}=e^{-\frac{A}{W}} \quad (25)$$

C. Generalized secrecy outage probability for active Eavesdropper

Till now we have considered the passive Eavesdropper which means eve does not interrupt the communication between Alice and Bob. Now we will consider the active case of Eavesdropper where eve tries to disturb the communication between Alice and Bob.

The GSOP from equation(22) is given as $P_{GSOP}= P(W \ge \theta)$, for an active case

$$W = \frac{|h_{AE}|^2P_t}{N_W + \beta P_j}$$

Where $|h_{AE}|^2$ is the fading coefficient of wiretap channel, P_t is the transmission power and P_j is the jamming power.

$$P_{GSOPA}= P(W \ge \theta)$$
$$=P\left(\frac{|h_{AE}|^2P_t}{N_W+\beta P_J} \ge \theta\right)$$
$$= P\left(|h_{AE}|^2 \ge \frac{(N_W+\beta P_j)\theta}{P_t}\right)$$
$$1 - CDF\left(\frac{(N_W+\beta P_j)\theta}{P_t}\right)$$
$$\text{Let } \frac{(N_W+\beta P_j)\theta}{P_t} = B$$

$$P_{GSOPA} = 1 - CDF(B) \quad (26)$$

In Active case, GSOP for Rician and Rayleigh distributions are as follows

For Rician distribution, the GSOP is given as

$$P_{GSOPA(RI)} = 1 - \left(1 - Q_1\left(\sqrt{2k_w}, \sqrt{2b(1+k_w)B}\right)\right)$$
$$= Q_1\left(\sqrt{2k_w}, \sqrt{2b(1+k_w)B}\right) \quad (27)$$

For Rayleigh distribution the GSOP is given as

$$P_{GSOP(RA)} = e^{-\frac{B}{E(W)}} \quad (28)$$

These equations are analyzed to observe how GSOP varies depending on different conditions.

IV. RESULTS AND DISCUSSION

Here the results for different cases are plotted

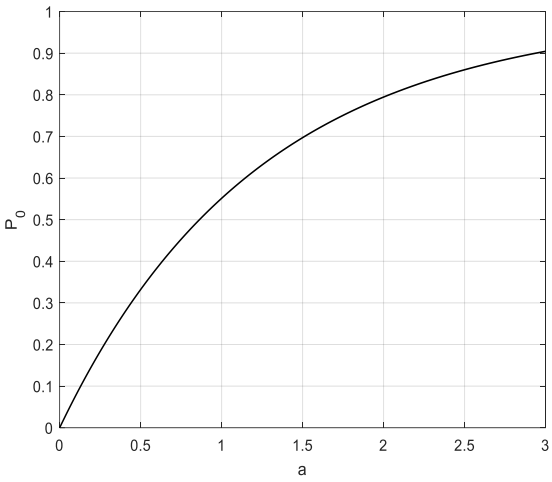

Fig.2. 1/E(M)(a) vs Secrecy outage probability, when $k_m = k_W$=0 from Equation.(15)),b=10,, R_s=0.5.

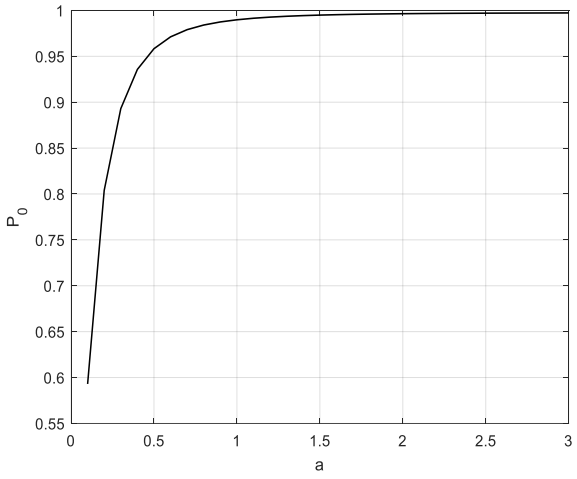

Fig.3. 1/E(M) (a) vs Secrecy outage probability when $k_m = 0, k_W > 0$ from Equation.(16),b=10, k_W =6, R_s=0.5.

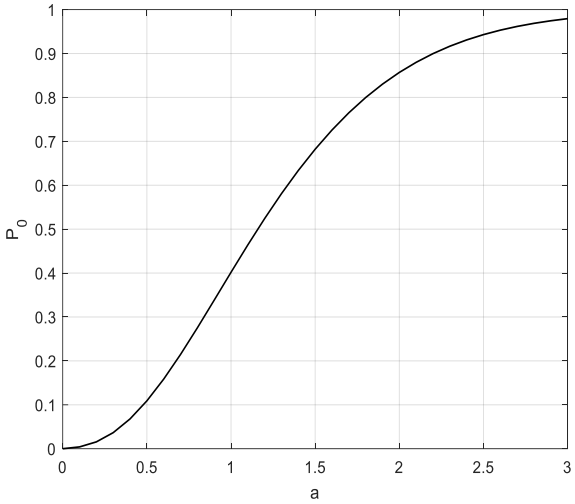

Fig.4. 1/E(M) (a) vs Secrecy outage probability, when $k_m > 0, k_W = 0$ from equation.(17) b=10, k_m =6, R_s=0.5.

From Figs.2-4 we can observe that as a i.e., 1/E(M) and Rican factor of wiretap channel (k_w) are increasing secrecy outage probability(SOP) is increasing and as k_m is increasing SOP is decreasing. In Fig.3. and Fig.4. k_m or k_w appear exclusively and show different trends. As for k_m its increase means that the direct path between Alice and Bob is possible which results in the decrease of SOP. In the case of k_w its increase the direct path between Alice and Eve thereby increasing SOP.

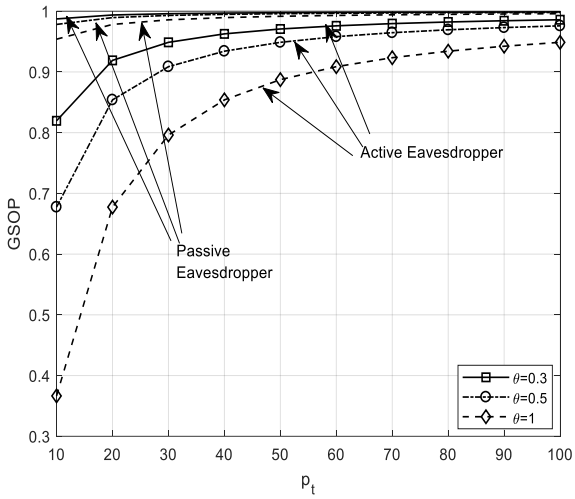

Fig.5. GSOP vs P_t for passive and active eavesdropper Ricain fading from Equations.(24) and (27) a=1, N_W=1, k_w =2, β=1, P_j=10dB.

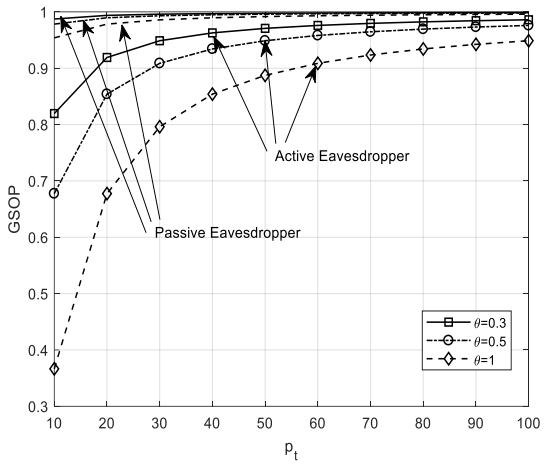

Fig.6. GSOP vs P_t for passive and active eavesdropper Rayleigh fading from Equations.(25)and (28) a=1, N_W=1,E(W)=1, β=1, P_j=10dB.

From Figs.5-6 it is observed that GSOP increases as transmitting power(P_t)increases and as θ increases GSOP decreases. θ is the highest value of SNR of Eve allowed. GSOP is the probability of SNR of Eve greater than the allowed value theta. Higher θ would reduce the range of values that outage probability could be risked to, which reduces the GSOP which we observe in Figs.5-6 SNR is proportional to P_t, so as P_t increases probability of SNR greater than theta increases thus GSOP increases in Figs.5-6. We observe this relation.

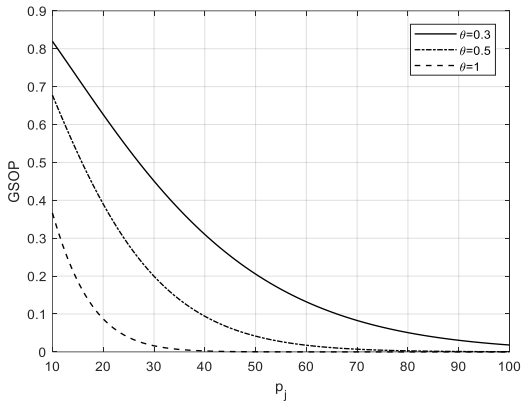

Fig.7. GSOP vs P_j for active eavesdropper Rician fading from Equation.(27) a=1, N_W=1,E(W)=1, β=1, P_t=10dB.

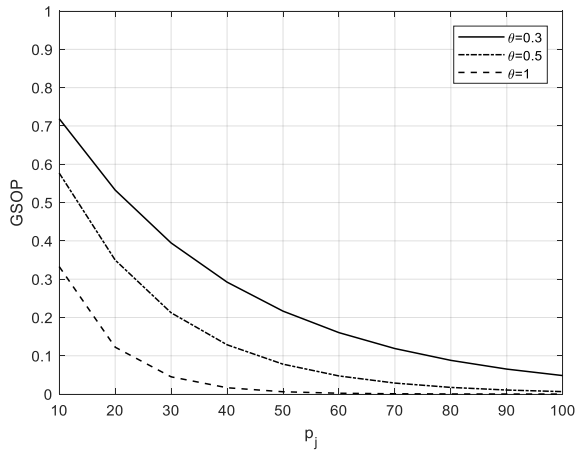

Fig.8. GSOP vs P_j for active eavesdropper Rayleigh fading from Equation.(28) a=1, N_W=1,E(W)=1, β=1, P_t=10dB.

From Figs.7-8 we can observe that as jamming power (P_j) increases GSOP is decreasing and as θ value increases GSOP is decreasing.

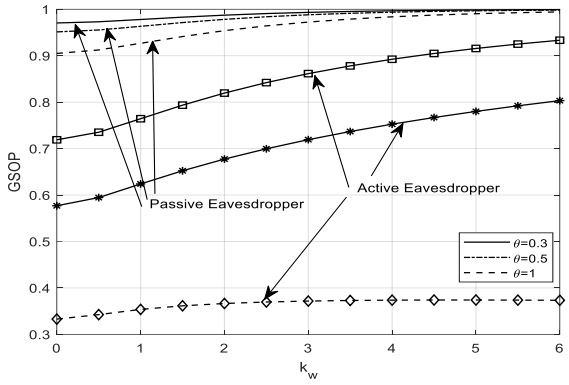

Fig.9. GSOP vs k_W for passive and active eavesdropper Rician fading from Equations.(24)and (27) a=1, N_W=1, β=1, P_t=10dB, P_j=10dB.

From Fig.9 we can observe that as Rician factor of Eve (k_w)increases GSOP is increasing and as θ value increases GSOP is decreasing.

V. CONCLUSION

We have analyzed secrecy outage probabilities of Rician fading channels and observed how outage probability is affected by different factors like average SNR and the Rician factors of the fading channels . A new secrecy metric called GSOP is derived to overcome the drawbacks of secrecy Outage probability and how the GSOP is affected depending on transmission power(P_t), jamming power(P_j) and Rician factor(k_w) is observed. It is shown that as theta value approaches one GSOP decreases and doesn't fall below 0.9 in the passive eavesdropper. Till now a passive case of the eavesdropper is considered where eve doesn't disturb the transmission between Alice and Bob. We considered the active case of eavesdropper and observed that in the active case too, as theta value increases GSOP decreases, but its value is reducing below 0.9.

This work can be extended to a case where both channels follow rician fading and also can be extended to other fading channels like Nakagami, k-μ fading. Furthermore, work can also be extended to the different system model, for example, MIMO systems communications where Alice, Bob and Eve can have multiple antennas.

REFERENCES

1. C.E. Shannon, "Communication theory of secrecy systems," Bell Syst.Tech. Journ., vol. 29, pp. 656–715, 1949.
2. A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. Journ., vol. 54, pp.1355–1387, 1975.
3. I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. IT-24, no. 3, pp. 339–348, May 1978.
4. S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," IEEE Trans. on Inform. Theory, vol. 24, no. 4, pp. 451456 July 1978.
5. U. Maurer, "Secret key agreement by public discussion from common information,"IEEETrans.Inf.Theory,vol.39,no.3,pp.733–742,May 1993.

6. P. Parada and R. Blahut, “Secrecy capacity of simo and slow fading channels,” in Proc. IEEE Int. Symp. Information Theory (ISIT 2005), Adelaide, Australia, Sep. 2005, pp. 2152–2155.
7. P. K. Gopala, L. Lai, and H. El-Gamal, “On the secrecy capacity of fading channels,” in Proc. IEEE Int. Symp. Information Theory, Nice, France, Jun. 2007, pp. 1306–1310.
8. Y. Liang, H. V. Poor, and S. Shamai (Shitz), “Secrecy capacity region of fading broadcast channels,” in Proc. IEEE Int. Symp. Information Theory, Nice, France, Jun. 2007, pp. 1291–1295.
9. Z. Li, R. Yates, and W. Trappe, “Secrecy capacity of independent parallel channels,” in Proc. 44th Annu. Allerton Conf. Communications, Control and Computing, Monticello, IL, Sep. 2006, pp. 841–848.
10. Matthieu Bloch, J.Barros, Miguel R. D. Rodrigues and Steven W.McLaughlin, ”Wireless Information-Theoretic Security,” IEEE Trans. on Inform. Theory, vol. 54, no. 6 June 2008.
11. Miguel R.D.Rodrigues, João Barros “Secrecy Capacity of Wireless Channels” , Proc. IEEE Int. Symp. Inf. Theory (ISIT), pp. 356-360, Jul. 2006.
12. Matthieu Bloch, Andrew Thangaraj, Steven W. McLaughlin, and Jean-Marc Merolla, “LDPC-based Gaussian key reconciliation,” in Proc. of the IEEE International Workshop on Information Theory, Punta del Este, Uruguay, March 2006.
13. Xian Liu “Probability of Strictly Positive Secrecy Capacity of Ricain-Rician Fading Channel,” IEEE WIRELESS COMMUNICATIONS LETTERS, vol. 2, no. 1 February 2013.
14. Jiangbo Si, Zan Li, Julian Cheng, Caijan Zhong “Sececy Performance of Multi-antenna Wiretap Channels With Diversity Combining Over Correlated Rayleigh Fading Channels, ” IEEE Trans. on Wireless Communication.
15. R. Price, “Some non-central F-distributions expressed in closed form, ”Biometrika, vol. 51, pp. 107–122, 1964
16. Biao He, Xiangyun Zhou, A. Lee Swindlehurst “On Secrecy Metrics for Physical Layer Security over Quasi-Static Fading Channels” IEEE Trans. on Wireless Communication.
17. Theodore Rappaport, Wireless Communications: Principles and Practice, 2nd Edition, Prentice Hall, 2001.
18. Andrea Goldsmith, Wireless Communications, 2004.

AUTHORS PROFILE

Reshmitha Bethi, received the B.Tech degree in Electronics and Communication Engineering from JNTUA college of Engineering, Kalikiri in 2017. Currently she is pursuing M.Tech degree in Digital Electronics and Communication Engineering at G. Narayanamma Institute of Technology and Science, Hyderabad, India.

Sujatha Reddy Allipuram, currently working as Assistant Professor in ECE department at G. Narayanamma Institute of Technology and Science.