International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 01, ISSN No. 2455-2143, Pages 268-272
Published Online May 2023 in IJEAST (http://www.ijeast.com)

PERFORMANCE ANALYSIS OF A POINT-TO-POINT SYSTEM UNDER ACTIVE ATTACK

Soumya Rani Kalvakota
Department of ECE
G. Narayanamma Institute of Technology and Science,
Hyderabad, Telangana, India

Sujatha Reddy Allipuram
Assistant Professor
Department of ECE
G. Narayanamma Institute of Technology and Science,
Hyderabad, Telangana, India

Abstract—**In wireless communications, security issues have become difficult due to unchangeable and unpredictable nature of the wireless medium. There are many traditional cryptographic techniques which were used previously. The physical layer security used for ensuring secure wireless communications apart from the cryptographic techniques, which is achieved after proper understanding of the nature wireless channels. Classical information theoretic secrecy is one of the metrics followed, in which, we assume that there is no(zero) leaked information at the eavesdropper which means the information decoding probability at the eavesdropper is '0'. But, practically achieving classical information theoretic secrecy is not possible.**
So, this project deals with partial secrecy. The partial secrecy of a system is measured in terms of equivocation, which gives the information of the level at which the eavesdropper (active) is confused. It means that in partial secrecy, there is information leakage but the eavesdropper cannot exactly decode the original message. The new secrecy metrics used GSOP (generalized secrecy outage probability), AFE (average fractional equivocation) and AILR (average information leakage rate) altogether provides more comprehensive and in-depth understanding of the secrecy performance over the fading channels.

Keywords—**Classical information theoretic secrecy, secrecy outage probability.**

I. INTRODUCTION

In wireless communications, providing security to the data is very difficult because of many factors affecting it. In a wireless medium, apart from abstractions in the medium, there is also threat to the data by unauthorized user (eavesdropper) who try to extract the data. Considering all the factors, providing security to the data in a wireless environment is crucial but is a difficult issue which determines the performance of a system.

In general, the secrecy performance is known by calculating secrecy outage probability (SOP). But it has two limitations:

1) It cannot give the information exactly about the eavesdropper's decidability.
2) It cannot exactly estimate the amount of leaked information to the eavesdropper.
3) In a worst case (main channel capacity is less than eve channel capacity), SOP is unable to give any information about how much information leaked to Eve.

The three new metrics used overcome the drawbacks of secrecy outage probability which are:

1) Generalized Secrecy Outage probability (GSOP) which considers some amount of information leakage at Eve and the information leaked is measured by equivocation.
2) Asymptotic Lower Bound on error probability-based secrecy metric (or) average fractional equivocation (AFE) at the eavesdropper gives the error information at Eve.
3) Average Information Leakage Rate (AILR) tells us how much the information is extracted at the eavesdropper.

By adopting the new secrecy metrics, we can establish optimal design parameters that lead to improved secrecy performance of the system.

II. SYSTEM MODEL

This paper considers a quasi-static Rayleigh fading wire-tap channel where the transmitter (Alice) wants to send important information to receiver (Bob) through the channel where the unauthorized person (Eve) is also present.

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 01, ISSN No. 2455-2143, Pages 268-272
Published Online May 2023 in IJEAST (http://www.ijeast.com)

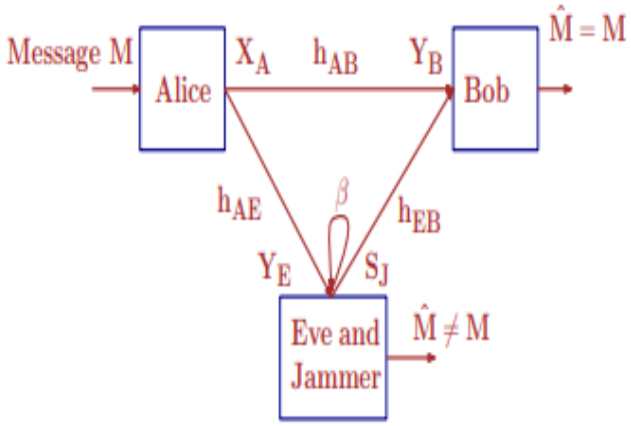

Fig.1 Active attack with eavesdropping and jamming

- It is assumed that Alice, Bob and Eve have a single antenna each it means one transmitter and one receiver.
- It is assumed that Alice does not have the CSI of Bob and Eve but knows the statistics of their channels.
- Bob also sends a one-bit feedback to Alice for ON-OFF transmission.
- The input-output equations for this model are as follows,

$$Y_B = h_{AB}X + h_{EB}S_J + N_b \quad (1)$$

$$Y_E = h_{AE}X + \sqrt{\beta}S_J + N_e \quad (2)$$

- The instantaneous channel capacities of Bob and Eve are,

$$C_b = \log_2(1 + \gamma_b) \quad (3)$$

$$C_e = \log_2(1 + \gamma_e) \quad (4)$$

- The instantaneous received signal to noise ratio (SNR's) at the intended receiver and the un-authorized person have the exponential distributions as,

$$f_{\gamma_b}(\gamma_b) = \frac{1}{\bar{\gamma}_b} * \exp\left(\frac{-\gamma_b}{\bar{\gamma}_b}\right) \quad (5)$$

$$f_{\gamma_e}(\gamma_e) = \frac{1}{\bar{\gamma}_e} * \exp\left(\frac{-\gamma_e}{\bar{\gamma}_e}\right) \quad (6)$$

- We consider the codeword transmission rate as,

$$R_b = \frac{H(X^n)}{n} \quad (7)$$

- We consider the information transmission rate as,

$$R_s = \frac{H(M)}{n} \quad (8)$$

- These two rates are fixed over time.

III.SECRECY PERFORMANCE ANALYSIS

Theorem 1. The GSOP of this system model considered is given by,

$$GSOP = e^{\frac{-(2^{(R_b-\theta R_s)}-1)(1+\beta P_J)}{\bar{z}P_t}} \quad (9)$$

Proof: The equation for GSOP is mathematically given by,

$$GSOP = P(\Delta < \Theta) \quad (10)$$

Where Δ=fractional equivocation$=\frac{R_b - C_e}{R_s}$ (11)

We have from (4) C_e value substituting them in (10), we get,

$$GSOP = P\left(\frac{R_b - \log_2(1+\gamma_e)}{R_s} < \theta\right)$$

After simplification, we get,

$$GSOP = P\left(\gamma_e < \left(2^{(R_b - \theta R_s)} - 1\right)\right)$$

But, $\gamma_e = \frac{zP_t}{(1+\beta P_J)}$

Substituting γ_e value, after simplication, we get,

$$GSOP = e^{-\left(\frac{\left(\left(2^{(R_b-\theta R_s)}-1\right)(1+\beta P_J)\right)}{\bar{z}P_t}\right.} \quad (12)$$

Theorem 2. The AFE equation for this system is given by,

$$AFE = 1 - e^{\frac{-(1+\beta P_j)n}{P_t}}\left(1 - \frac{R_b}{R_s}\right) - \frac{R_b}{R_s}e^{\frac{-(1+\beta P_j)p}{P_t}} + \frac{1}{R_s \ln(2)}\left(e^{\frac{(1+\beta P_j)}{P_t}} E_i\left(\frac{(1+\beta P_j)(1+p)}{P_t}\right) + e^{\frac{-(1+\beta P_j)p}{P_t}} \ln(1+p)\right) - \frac{1}{R_s \ln(2)}\left(e^{\frac{(1+\beta P_j)}{P_t}} E_i\left(\frac{(1+\beta P_j)(1+n)}{P_t}\right) + e^{\frac{-(1+\beta P_j)n}{P_t}} ln(1+n)\right) \quad (13)$$

Proof: We have the equation for AFE as,

$$AFE = \bar{\Delta} = E\{\Delta\} \quad (14)$$

$$AFE = \bar{\Delta} = \int_0^{\left(2^{(R_b-R_s)}-1\right)} f_{\gamma_e}(\gamma_e)\, d\gamma_e + \int_{\left(2^{(R_b-R_s)}-1\right)}^{\left(2^{(R_b)}-1\right)} \frac{R_b - log_2(1+\gamma_e)}{R_s} f_{\gamma_e}(\gamma_e) d\gamma_e \quad (15)$$

But from (6), we have, $f_{\gamma_e}(\gamma_e) = \frac{1}{\bar{\gamma}_e} * exp\left(\frac{-\gamma_e}{\bar{\gamma}_e}\right)$

Substitute in (15), after simplification, we get,

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 01, ISSN No. 2455-2143, Pages 268-272
Published Online May 2023 in IJEAST (http://www.ijeast.com)

$$AFE = 1 - e^{\frac{-(1+\beta P_j)n}{P_t}}\left(1-\frac{R_b}{R_s}\right) - \frac{R_b}{R_s}e^{\frac{-(1+\beta P_j)p}{P_t}} + \frac{1}{R_s\, ln(2)}\left(e^{\frac{(1+\beta P_j)}{P_t}} E_i\left(\frac{(1+\beta P_j)(1+p)}{P_t}\right) + e^{\frac{-(1+\beta P_j)p}{P_t}} ln(1+p)\right) - \frac{1}{R_s\, ln(2)}\left(e^{\frac{(1+\beta P_j)}{P_t}} E_i\left(\frac{(1+\beta P_j)(1+n)}{P_t}\right) + e^{\frac{-(1+\beta P_j)n}{P_t}} ln(1+n)\right)$$

Theorem 3. The AILR equation for this system model considered is given by,

$$\text{AILR}=e^{\frac{-(1+\beta P_j)n}{P_t}}\left(1-\frac{R_b}{R_s}\right)+\frac{R_b}{R_s}e^{\frac{-(1+\beta P_j)p}{P_t}} - \frac{1}{R_s\, ln(2)}\left(e^{\frac{(1+\beta P_j)}{P_t}} E_i\left(\frac{(1+\beta P_j)(1+p)}{P_t}\right) + e^{\frac{-(1+\beta P_j)p}{P_t}} ln(1+p)\right) + \frac{1}{R_s\, ln(2)}\left(e^{\frac{(1+\beta P_j)}{P_t}} E_i\left(\frac{(1+\beta P_j)(1+n)}{P_t}\right) + e^{\frac{-(1+\beta P_j)n}{P_t}} ln(1+n)\right) * R_s \quad (16)$$

Proof: The equation for AILR is given by,

$$\text{AILR} = (1-\bar{\Delta}) * R_s \quad (17)$$

Where, $\bar{\Delta}$=AFE

Substituting AFE value, we get,

$$\text{AILR}=(e^{\frac{-(1+\beta P_j)n}{P_t}}\left(1-\frac{R_b}{R_s}\right)+\frac{R_b}{R_s}e^{\frac{-(1+\beta P_j)p}{P_t}} - \frac{1}{R_s\, ln(2)}\left(e^{\frac{(1+\beta P_j)}{P_t}} E_i\left(\frac{(1+\beta P_j)(1+p)}{P_t}\right) + e^{\frac{-(1+\beta P_j)p}{P_t}} ln(1+p)\right) + \frac{1}{R_s\, ln(2)}\left(e^{\frac{(1+\beta P_j)}{P_t}} E_i\left(\frac{(1+\beta P_j)(1+n)}{P_t}\right) + e^{\frac{-(1+\beta P_j)n}{P_t}} ln(1+n)\right) * R_s$$

IV.RESULTS AND DISCUSSIONS

A.GSOP outputs:

1.GSOP vs transmission power(P_t)

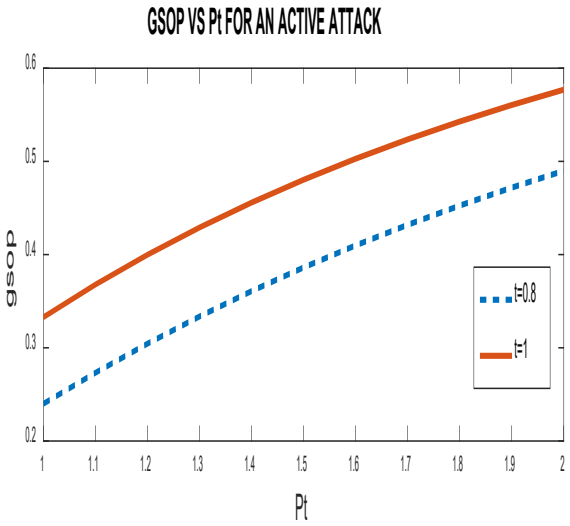

Fig.1 GSOP VS Transmission power curve

With transmission power average SNR at Eve increases and as SNR increases outage increases (as $C_b = \log_2(1+\gamma_b)$) . So, the secrecy outage probability increases which is observed in the curve.

2.GSOP VS self-interference to power ratio:

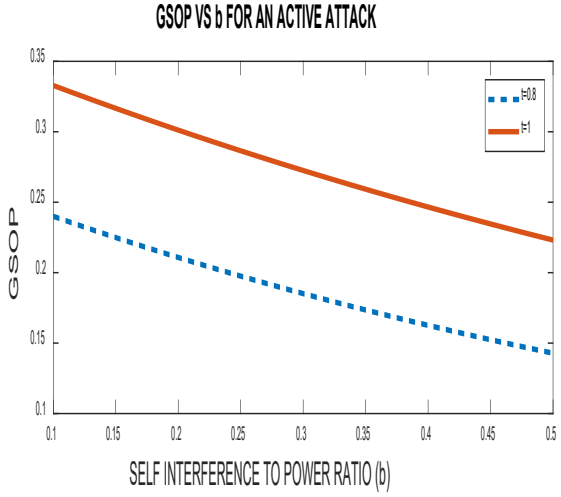

Fig.2 GSOP VS self-interference to power ratio

- As self-interference to power ratio increases, the interference between eavesdropped signal and jamming signal increases so signal occurs so decreases.

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 01, ISSN No. 2455-2143, Pages 268-272
Published Online May 2023 in IJEAST (http://www.ijeast.com)

3.GSOP VS jamming power:

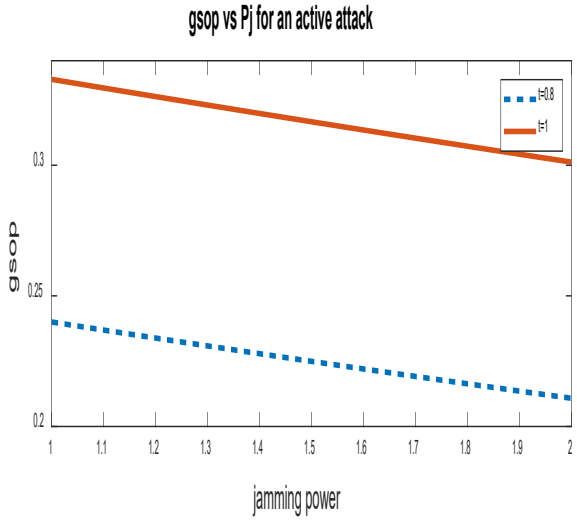

Fig.3 GSOP VS jamming power curve

- As jamming power increases, interference between eavesdropped signal and jamming signal increases, so, signal loss occurs and so GSOP decreases.

B. AFE, AILR outputs:

1.AFE, AILR vs transmission power:

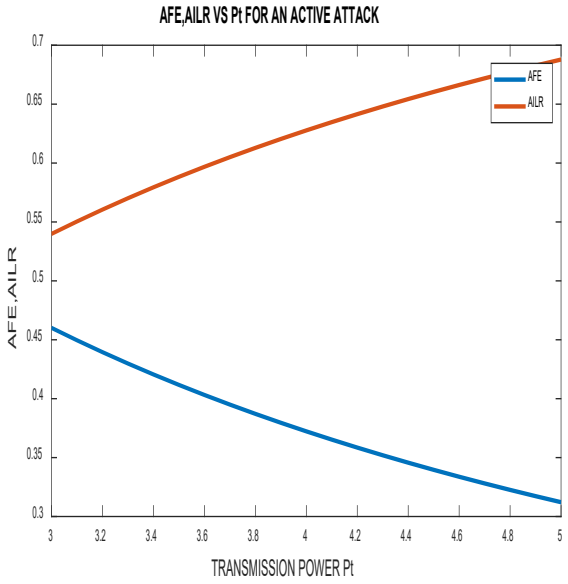

Fig.4 AFE, AILR VS transmission power

- As transmission power increases, SNR at Eve increases and with SNR the capacity of Eve channel increases. So, outage at Eve increases so the outage probability (GSOP) increases.

2.AFE,AILR vs self-interference to power ratio:

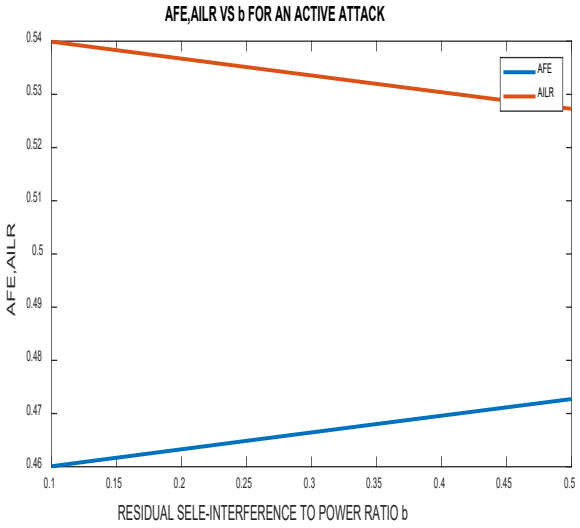

Fig.5 AFE, AILR VS self-interference to power ratio

- As self-interference to power ratio increases, interference between eavesdropped signal and jamming signal increases so signal loss occurs. So, the error at Eve increases so AFE increases. Also because of interference outage decreases so information leakage rate (AILR) decreases.

3. AFE,AILR vs jamming power:

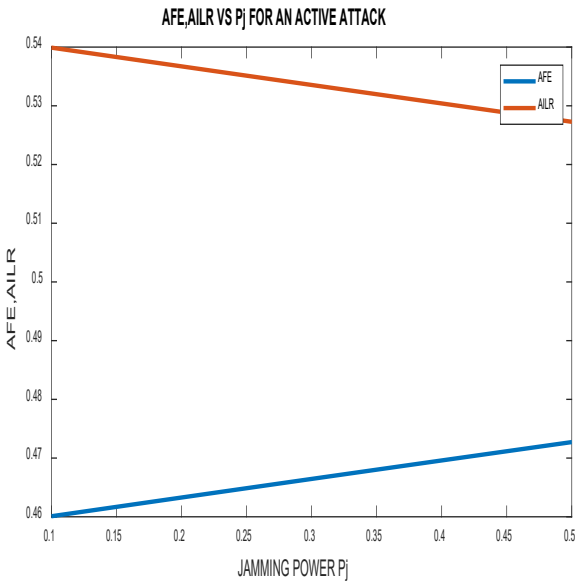

Fig.6 AFE, AILR VS jamming power

- As jamming power increases, interference between eavesdropped signal and jamming signal increases so signal loss occurs. So, the error at Eve increases so AFE

increases. Also because of interference outage decreases so information leakage rate (AILR) decreases.

V. CONCLUSIONS AND FUTURE SCOPE

We have calculated three metrics namely, GSOP, AFE, AILR for an active attack and analyzed how they vary by varying SNR at Eve, transmission power, jamming power, self-interference to power ratio(β).
We can also extend this work to Multi-input and Multi-output system. These metrics can also be calculated for other fading channels like Rician fading, Nakagami fading.

VI. REFERENCES

[1]. Biao He, Xiangyun Zhou, A. Lee Swindlehurst, Fellow, October 2016, "On Secrecy Metrics for Physical Layer Security Over Quasi-Static Fading Channels", IEEE transactions on wireless communications , vol. 15, no. 10.

[2]. B. He and X. Zhou, Dec. 2014, "New physical layer security measures for wireless transmissions over fading channels", in Proc. IEEE GLOBECOM, pp. 722–727.

[3]. M. Bloch and J. Barros, 2011, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge, U.K.: Cambridge Univ. Press.

[4]. C. E. Shannon, Oct. 1949 "Communication theory of secrecy systems," Bell Labs Tech. J., vol. 28, no. 4, pp. 656–715.

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

[6]. I. Csiszár and J. Körner, May 1978, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348.

.

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

[8]. P. K. Gopala, L. Lai, and H. El Gamal, Oct. 2008, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698.

[9]. Y. Liang, H. V. Poor, and S. Shamai (Shitz), Dec. 2014, "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008. B. He and X. Zhou, "New physical layer security measures for wireless transmissions over fading channels," in Proc. IEEE GLOBECOM, pp. 722–727.

[10]. X. Zhou, L. Song, and Y. Zhang, 2013, "Physical Layer Security in Wireless Communications", Boca Raton, FL, USA: CRC Press.

[11]. Allipuram Sujatha, Mohapatra Parthajit, and Chakrabarti Saswath, "Secrecy Performance of an Artificial Noise Assisted Transmission Scheme with Active Eavesdropper" ,IEEE Communications Letters.

[12]. W. Huang, W. Chen, B. Bai, and Z. Han, 2018, "Wiretap channel with full-duplex proactive eavesdropper: A game theoretic approach," IEEE Transactions on Vehicular Technology, vol. 67, no. 8, pp. 7658–7663.

[13]. J. Y. Ryu, J. Lee, and T. Q. Quek, 2016, "Transmission strategy against opportunistic attack for MISO secure channels," IEEE Communications Letters, vol. 20, no. 11, pp. 2304–2307.