World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:9, No:11, 2015

Average Secrecy Mutual Information of the Non-Identically Independently Distributed Hoyt Fading Wireless Channels

Md. Sohidul Islam, Mohammad Rakibul Islam

***Abstract*—**In this paper, we consider a non-identically independently distributed (non-i.i.d.) Hoyt fading single-input multiple-out put (SIMO) channel, where the transmitter sends some confidential information to the legitimate receiver in presence of an eavesdropper. We formulated the probability of non-zero secrecy mutual information; secure outage probability and average secrecy mutual information (SMI) for the SIMO wireless communication system. The calculation has been carried out using small limit argument approximation (SLAA) on zeroth-order modified Bessel function of first kind. In our proposed model, an eavesdropper observes transmissions of information through another Hoyt fading channel. First, we derived the analytical expression for non-zero secrecy mutual information. Then, we find the secure outage probability to investigate the outage behavior of the proposed model. Finally, we find the average secrecy mutual information. We consider that the channel state information (CSI) is known to legitimate receiver.

***Keywords*—**Hoyt fading, main channel, eavesdropper channel, secure outage probability, average secrecy mutual information.

I. Introduction

THE broadcast nature of wireless communication makes it more vulnerable to eavesdropping. The privacy and the security in wireless communication are playing very important role, as these networks are using to deliver private information. We have to ensure that illegitimate person must not get unauthorized access to the content of the original signal. The information-theoretic security was first introduced by Shannon [1] to characterize fundamental limits of secure communication over fading channel. When the main channel is better than the eavesdropper's channel, the positive secrecy capacity is achievable presented in [2]. For SISO case, they [3] have shown the effect of quasi-static fading on secrecy capacity (i.e. the maximum transmission rate at which the eavesdropper is unable to attain any information). Recently, in [4], they have shown secure communication through Rayleigh fading SIMO channel in presence of multiple eavesdroppers.

In addition to security issues, another unavoidable concern in most wireless communication systems is energy-efficient operation especially when wireless units are powered by batteries. From an information-theoretic perspective, energy efficiency can be measured by the energy required to send one information bit reliably. It is well-known that for no fading and fading Gaussian channels subject to average input power constrains, energy efficiency improves as one operates at low SNR levels. Also, operating at low SNR levels has its benefits in terms of limiting the interference.

Majority of the research related to secrecy mutual information of SIMO system has focused on Rayleigh and Nakagami-m distributions. There are other types of fading distributions which serves good models under certain circumstances. Hoyt (also known as Nakagami-q) fading allows the modeling of propagation environment without a dominant component over the scattered waves (a situation of Non-line of Sight). It has found application in the error performance evaluation of digital communication systems over generalized fading channel [5]. Recently, the Hoyt model is being used more frequently in performance analysis and other studies related to mobile radio communications.

The rest of the paper organized as follows. System model and the SLA approximation are presented in Section II. Section III shows the probability distribution function (PDF) calculations and analytical expression for both main and eavesdropper's channel. The numerical results are described in Section IV. Finally, Section V describes the concluding remarks of this work.

II. System Model

The system model of our work is shown in Fig. 1. A legitimate transmitter communicates with its corresponding receiver in presence of an eavesdropper. The transmitter equipped with single antenna. At the receiver, the legitimate receiver and eavesdropper's receiver are equipped with $n_R$and n_E antennas respectively. The received signal for the legitimate receiver can be written as,

$$\boldsymbol{y}_M = \boldsymbol{h}x + \boldsymbol{z}_M \quad (1)$$

Md. Sohidul Islam is with the Department of Electrical and Electronics Engineering, Islamic University of Technology (IUT), Dhaka, Bangladesh. (Corresponding author e-mail: msohidul@iut-dhaka.edu).

Mohammad Rakibul Islam is with the Department of Electrical and Electronics Engineering, Islamic University of Technology (IUT), Dhaka, Bangladesh.

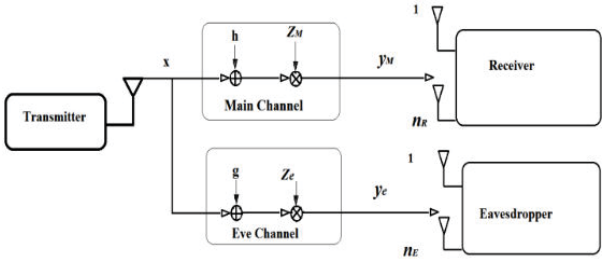

Fig. 1 System Model

where x is the transmitted signal, $\boldsymbol{h} \in \mathbb{C}^{n_R} \times 1$ is the subchannel gain from transmitter to main channel and $\boldsymbol{z}_M$ with variance σ^2. Received signal for eavesdropper (Eve channel) is given by,

$$\boldsymbol{y}_e = \boldsymbol{g}x + \boldsymbol{z}_e \tag{2}$$

where $\boldsymbol{g} \in \mathbb{C}^{n_E} \times 1$ is the subchannel gain from transmitter to eavesdropper channel and $\boldsymbol{z}_e$ is zero mean circularly symmetric complex Gaussian noise with variance σ^2. Now we consider both the vectors $\boldsymbol{h}$ and $\boldsymbol{g}$ be the sum of magnitudes of complex Gaussian random variables. Let Ω_M and Ω_e are the average signal to noise ratio (SNR) for different sub channels of main and eve channel respectively.

In [6], the PDF of Hoyt distribution is given by,

$$P_{\gamma(\gamma)} = \frac{(1+q^2)}{2\,q\,\Omega} e^{-\frac{(1+q^2)^2\gamma}{4\,q^2\Omega}} I_0\left(\frac{(1-q^4)\gamma}{4\,q^2\Omega}\right), \gamma \geq 0 \tag{3}$$

where $I_0(\cdot)$is the zeroth-order modified Bessel function of the first kind and q is the Hoyt fading parameter ranges from 0 to 1. Ω and γ are average SNR and instantaneous SNR respectively. The Hoyt distribution spans the range from one-sided Gaussian fading ($q = 0$) to Rayleigh fading when $q = 1$. The $v\ th$ order modified Bessel function of the first kind can be written as,

$$I_v(x) \approx \frac{\left(\frac{x}{2}\right)^v}{\Gamma(v+1)} \tag{4}$$

Using small argument limit approximation [9], $x \to 0$ for the zeroth-order modified Bessel function of the first kind can be approximated as,

$$I_0(x) \approx 1 \tag{5}$$

Using the approximation (5), the Hoyt distribution given in (3) can be written as,

$$P_{\gamma(\gamma)} = \frac{(1+q^2)}{2\,q\,\Omega} e^{-\frac{(1+q^2)^2\gamma}{4\,q^2\Omega}}, \gamma \geq 0 \tag{6}$$

III. Problem Formulations

A. Secrecy Mutual Information

For any discrete memory less channel, the secrecy mutual information defined as,

$$I_S = I(u;\boldsymbol{y}_M) - I(u;\boldsymbol{y}_e) = I_M - I_E \tag{7}$$

From (1), the mutual information of the main channel is given by,

$$I_M = log_e\left(1 + \frac{P}{\sigma_M^2}\boldsymbol{h}^H\,\boldsymbol{h}\right) = log_e\left(1 + \rho_M \sum_{i=1}^{n_R} \| h_i \|^2\right) \tag{8}$$

where $\rho_M = \frac{P}{\sigma_M^2}$, is the transmitted SNR of the main channel. P corresponds to the average transmit signal power. The channel is power limited in the sense $\mathbb{E}\{|x|^2\} = P$. For different subchannels $i = 1,2,3,\ldots,n_R$ and $k = 1,2,3,\ldots,n_E$ are the main channel and eavesdropper's channel respectively. Defining $r = \sum_{i=1}^{n_R} \| h_i \|^2$, we have $r \sim \chi^2_{2n_R}$, where $\chi^2_{2n_R}$ is the central chi-square variable with $2n_R$ degree of freedom. Now we consider the distribution of r for non-identically independent Hoyt distribution. The probability density function of r for (6) is given by,

$$f(r) = \frac{(1+Q_0^2)}{2\,Q_0\Omega_M} e^{-\frac{\left(1+Q_0^2\right)^2 r}{4Q_0^2\Omega_M}} \tag{9}$$

From [7], where $Q_0 = \frac{\left(\sum_{i=1}^{n_R}\Omega_{Mi}\right)}{\sum_{i=1}^{n_R}\left(\frac{\Omega_{Mi}^2}{q}\right)}$ and $\Omega_M = \sum_{i=1}^{n_R}\Omega_{Mi}$ as all the subchannels have non-identical gains (i.e.$q_i \neq q,\ \Omega_{Mi} \neq \Omega_M$). Mutual information of eavesdropper's channel using (2) is given by,

$$I_E = log_e\left(1 + \frac{P}{\sigma_e^2}\boldsymbol{g}^H\boldsymbol{g}\right) = log_e\left(1 + \rho_e \sum_{k=1}^{n_E} \| g_k \|^2\right) \tag{10}$$

where$\rho_e = \frac{P}{\sigma_e^2}$ is the transmitted SNR of the eavesdropper's channel. Defining $t = \sum_{k=1}^{n_E} \| g_k \|^2$, we have $t \sim \chi^2_{2n_E}$, where $\chi^2_{2n_E}$ is the central chi-square variable with $2n_E$ degree of freedom. The probability density function of t is given by,

$$f(t) = \frac{(1+W_0^2)}{2\,W_0\Omega_e} e^{-\frac{\left(1+W_0^2\right)^2 t}{4W_0^2\Omega_e}} \tag{11}$$

where $W_0 = \frac{\left(\sum_{k=1}^{n_E}\Omega_{ek}\right)}{\sum_{k=1}^{n_E}\left(\frac{\Omega_{ek}^2}{q}\right)}$ and $\Omega_e = \sum_{k=1}^{n_E}\Omega_{ek}$ as all the subchannels have non-identical gains (i.e.$q_k \neq q, \Omega_{ek} \neq \Omega_e$). The secrecy mutual information of Hoyt fading SIMO channel is given by using (7), (8) and (10),

$$I_S = log_e\left(\frac{1 + \rho_M\,\boldsymbol{h}^H\,\boldsymbol{h}}{1 + \rho_e\,\boldsymbol{g}^H\,\boldsymbol{g}}\right) \tag{12}$$

B. Probability Density Function of I_M and I_E

Using proposition 1 from [3], let $\nu \sim \chi^2_{2n}$ and probability density function of ν denoted by $f(\nu)$. Then the probability density function of $I = log_e(1 + \theta\,\nu)$ is given by,

$$m(I) = \frac{e^I}{\theta}\left(\frac{e^I - 1}{\theta}\right) \tag{13}$$

Using (13) and (9), the probability density function of I_M (main channel) is given by,

$$m(I_M) = \frac{1}{\rho_M}\left(\Upsilon_M\, e^{I_M} e^{-\Psi_M\left(e^{I_M}-1\right)}\right) \tag{14}$$

where $\Upsilon_M = \frac{\left(1+Q_0^2\right)}{2\,Q_0\Omega_M}$ and $\Psi_M = \frac{\left(1+Q_0^2\right)^2}{4Q_0^2\Omega_M\rho_M}$. Similarly, Using (13) and (11), the probability density function of I_E (eavesdropper's channel) is given by,

$$m(I_E) = \frac{1}{\rho_e}\left(\Upsilon_E e^{I_E} e^{-\Psi_E\left(e^{I_E}-1\right)}\right) \tag{15}$$

where $\Upsilon_E = \frac{\left(1+W_0^2\right)}{2\,W_0\Omega_E}$ and $\Psi_E = \frac{\left(1+W_0^2\right)^2}{4W_0^2\Omega_e\rho_e}$

C. Probability of Positive Secrecy Mutual Information

This section presents an analytical expression for probability of non-zero secrecy mutual information for Hoyt fading SIMO channel in presence of an eavesdropper. Invoking independence between main channel and eavesdropper's channel, the probability of existence of a non-zero secrecy mutual information as,

$$Pr(I_S > 0) = \Pr(I_M > I_E) = \int_0^\infty \int_0^{I_M} m(I_M)\, m(I_E)\; dI_E\, dI_M \tag{16}$$

From (14)-(16), non-zero secrecy mutual information, $Pr(I_S > 0)$ is given by,

$$Pr(I_S > 0) = \frac{4\,q^2 n_E\left(1+W_0^2\right) n_R^3\,\beta_M}{\left(1+Q_0^2\right)\left(\alpha^2\beta_e+\xi^2\beta_M\right)} \tag{17}$$

where $\beta_M = \Omega_M\rho_M, \beta_e = \Omega_e\rho_e, \alpha = n_E(1+Q_0^2)$, and

$$\xi = n_R(1+W_0^2)$$

In [8], the authors have shown that there exists a non-zero secrecy capacity in fading channel even when the eavesdropper's channel is statistically better than the main channel. From our (15), we can obtain special result for Rayleigh fading SISO channel i.e. $n_R = 1, n_E = 1\ and\ \Omega_{Mi} = \Omega_M\ and\ \Omega_{ek} = \Omega_e$, fading parameter $q = 1$ and at least even when $\Omega_{Mi} = \Omega_{ek}$.

$$Pr(I_S > 0) = \frac{\rho_M}{\rho_M + \rho_e}$$

which is exactly (7) in [3].

D. Secure Outage Probability

Now we will characterize the outage probability

$$P_{out}(R_s) = \Pr(I_S < R_s),\quad R_s > 0$$

The significance of the definition is that when the secrecy rate is set to R_s, the confidential communication will be ensured only if $I_S < R_s$, otherwise secure transmission of information will not be guaranteed. From the total probability theorem, we can get secure outage probability.

$$\begin{aligned} P_{out}(R_s) = {} & Pr\,(I_S < R_s | I_M > I_E)\; Pr(I_M > I_E) \\ & + Pr\,(I_S < R_s | I_M \le I_E)\; Pr(I_M \le I_E) \end{aligned} \tag{18}$$

Now,

$$\begin{aligned} Pr\,(I_M < R_s + I_E | I_M > I_E)\, Pr(I_M > I_E) = {} & Pr(I_M > I_E) - \\ & \int_0^\infty \int_{R_s+I_E}^\infty m(I_M)\, m(I_E)\, dI_M\, dI_E \end{aligned}$$

and $Pr\,(I_S < R_s | I_M \le I_E) = 1$, since $I_S = 0$ when $I_M \le I_E$ Therefore, (18) can be written as,

$$P_{out}(R_s) = 1 - \int_0^\infty \int_{R_s+I_E}^\infty m(I_M)\, m(I_E)\, dI_M\, dI_E \tag{19}$$

The analytical expression of (19) is given by,

$$P_{out}(R_s) = 1 - \frac{\mu\, e^{\delta_M\left(1-e^{R_S}\right)}}{\delta_M(\delta_E+\delta_M e^{R_S})} \tag{20}$$

where $\mu = \frac{\left(1+Q_0^2\right)\left(1+W_0^2\right)}{4\,Q_0 W_0\beta_M\beta_e}$, $\delta_M = \frac{\left(1+Q_0^2\right)^2}{4\,Q_0^2\beta_M}$ and $\delta_E = \frac{\left(1+W_0^2\right)^2}{4\,W_0^2\beta_e}$

From our (20), we can obtain special result for Rayleigh fading SISO channel i.e. $n_R = 1, n_E = 1\ and\ \Omega_{Mi} = \Omega_M\ and\ \Omega_{ek} = \Omega_e$, fading parameter $q = 1$ and at least even when $\Omega_{Mi} = \Omega_{ek}$.

$$P_{out}(R_s) = 1 - \frac{\rho_M}{(\rho_M+\rho_e e^{R_S})}\exp\left(-\frac{e^{R_S}-1}{\rho_M}\right) \tag{21}$$

which corresponds (9) in [3]. This special result also derived in (16) in [4].

E. Average Secrecy Mutual Information

This section presents an analytical expression for the average secrecy mutual information. It is calculated as the average instantaneous secrecy mutual information over I_M and I_E. For a given I_M, the average secrecy mutual information over I_E is given by,

$$\langle I_S(I_M)\rangle = \int_0^{I_M} I_S\, m(I_E) dI_E \tag{22}$$

After simplification using (12), (14) and (15), the (22) becomes

$$\langle I_S(I_M)\rangle = \frac{2W_0}{\left(1+W_0^2\right)}\left(I_M + e^{\delta_E}\, Ei(-\delta_E) - e^{\delta_E} Ei(-e^{I_M}\delta_E)\right) \tag{22a}$$

where exponent integral defines as, $Ei(x) = \int_x^\infty \frac{e^{-t}}{t} dt$

The analytical expression of average secrecy mutual information obtained by using (14) and (22a) is given by,

$$\langle I_S\rangle = \int_0^\infty \langle I_S(I_M)\rangle\, m(I_M) dI_M \tag{23}$$

After simplifications the resultant analytical expression for the average secrecy mutual information, $\langle I_S\rangle$ becomes in (24) is

$$\begin{aligned} \langle I_S\rangle = {} & \frac{n_E\left(1+Q_0^2\right)}{2\,\delta_M n_R\beta_M\left(1+W_0^2\right)}\Bigg(e^{\delta_M}\Big(2\,Ei(-\delta_E-\delta_M) - Log(-\delta_E-\delta_M) + \\ & Log\left(-\frac{1}{(\delta_M+\delta_E)}\right) + 2\,Log\,(\delta_M+\delta_E)\Big) + 2\,G_{1,2}^{2,0}\left(\left(\delta_M\middle|\begin{matrix}1\\0,0\end{matrix}\right)\right)\Bigg) \end{aligned} \tag{24}$$

where $G_{p,q}^{m,n}\left(x\middle|\begin{matrix}a_p\\b_q\end{matrix}\right)$is the Meijer G-function.

IV. Numerical Results

Numerical and analytical simulation results for probability of non-zero secrecy mutual information, secure outage probability and average secrecy mutual information are presented in this section.

A. The Impact of Probability of Non-Zero Secrecy Mutual Information on SNR of the Main Channel

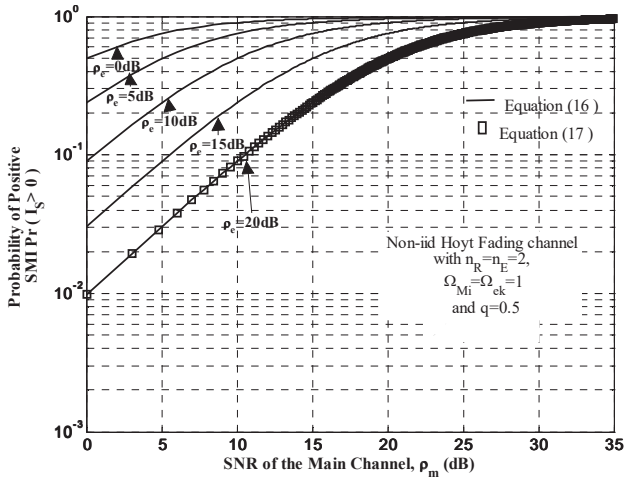

Fig. 2 A comparison between $Pr(I_S > 0)$ of (16) and (17) as a function of ρ_M, for selected values of ρ_e with $q = 0.5, n_R = n_E = 2, and\ \Omega_{Mi} = \Omega_{ek} = 1$.

Fig. 2 shows the comparison of numerical (16) and analytical (17) simulation for probability of non-zero secrecy mutual information as a function of ρ_M, for selected values of $\rho_e$and $n_R = n_E = 2$. Matching between the results justifies the validity of analytical expression. The probability of non-zero secrecy mutual information increases with the SNR of the main channel. Also the probability of non-zero secrecy mutual information decreases with increase in SNR of the eavesdropper's channel. The existence of non-zero secrecy mutual information can be shown from the figure, when the main channel is degraded ($\rho_M = 0\ dB$) than eavesdropper's channel ($\rho_e = 20\ dB$). So, we can conclude that for a fixed value of ρ_e, the better the main channel, the larger the probability of non-zero secrecy mutual information.

B. The Impact of Secure Outage Probability on Both SNR of the Main Channel and Secrecy Rates

Fig. 3 depicts the comparison of numerical (19) and analytical (20) simulation for secure outage probability as a function of SNR of the main channel, ρ_M for selected values of SNR of the eavesdropper's channel, ρ_e with secrecy rate, $R_s = 0.1$ and the number of receiving antennas for legitimate receiver is $n_R = 2$. Matching between the results justifies the validity of analytical expression. We see that the secure outage probability increases with SNR of the eavesdropper's channel and decrease with the SNR of the main channel. So, the observation we expect is that better the SNR of the main channel, the smaller the secure outage probability.

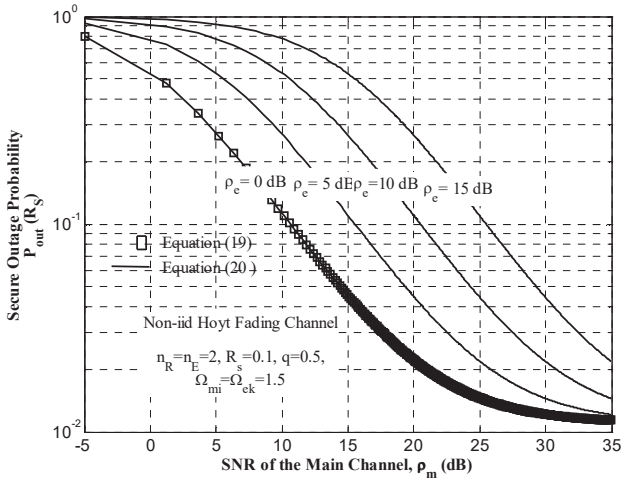

Fig. 3 Numerical and analytical simulation of $P_{out}(R_s)$for selected values of ρ_e with $R_s = 0.1$ and $n_R = n_E = 2$.

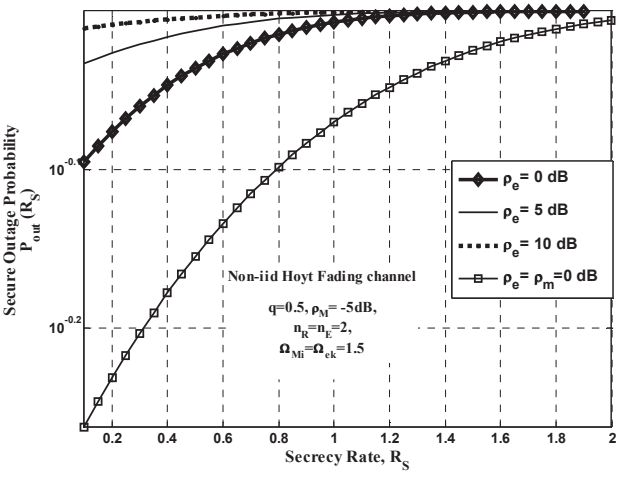

Fig. 4 Numerical and analytical comparison of $P_{out}(R_s)$ versus R_s for selected values of ρ_e with $\rho_M = -5dB$ and $n_R = n_E = 2$.

Fig. 4 explains that the secure outage probability as a function of secrecy rates R_s. If we increase the secrecy rate, the outage probability of the system is increased. Larger the R_s , higher the outage probability is. Therefore, by reducing the secrecy rates, $R_s$better performance of the system can be achieved.

C. The Impact of Average Secrecy Mutual Information on Both SNR of the Main Channel and Number of Eavesdropper

In Fig. 5, we plot the average secrecy mutual information, $\langle I_S \rangle$ versus SNR of the main channel, ρ_M. Matching of results between (23) and (24) justifies the validity of our analytical expression. The the average secrecy mutual information, $\langle I_S \rangle$ increases with the SNR of the main channel ρ_M and decreases with SNR of the eavesdropper channel, ρ_e. We can conclude

that, better the main channel, the larger the average secrecy mutual information, $\langle I_S \rangle$.

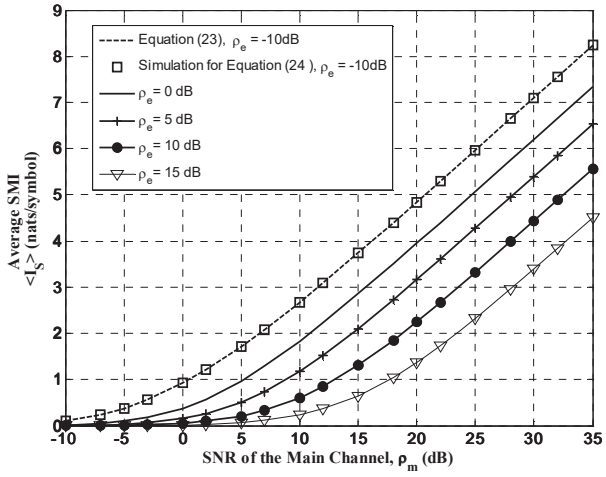

Fig. 5 Numerical and analytical simulation of average secrecy mutual information as a function of ρ_M, for selected values of ρ_e with $n_R = n_E = 2$.

V. Conclusion

In this paper, we derive analytical expression for the probability of non-zero secrecy mutual information, secure outage probability and average secrecy mutual information over Hoyt fading SIMO channel in presence of an eavesdropper. We present both numerical simulation and analytical simulation results. Matching between simulation and analytical result justifies the validity of analytical expression. It is observed that in presence of fading when SNR of the eavesdropper's channel is better than SNR of the main channel, the positive secrecy mutual information exists. We found that the secure outage probability increases with SNR of the eavesdropper's channel and decreases with the SNR of the main channel. Also, larger the secrecy rate, the higher the secure outage probability. The average secrecy mutual information increases with SNR of the main channel and decreases with SNR of the eavesdropper's channel. We have shown that the results in [3] correspond to some special cases of our work.

Acknowledgment

The author would like to thank Md. Zahurul I. Sarkar, Rajshahi University of Engineering & Technology, for his helpful comments and suggestions of this work.

References

[1] C. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, 29, pp. 656–715, 1949.
[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[3] 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, 2008.
[4] Sarkar, M.Z.I.; Ratnarajah, T.," Secure communication through Rayleigh fading SIMO Channel with multiple eavesdroppers", *International Conference on Communications (ICC)*, IEEE, 2010.
[5] Fraidenraich, Gustavo and Lévêque, Olivier and Cioffi, John M., "On the MIMO channel capacity for the dual and asymptotic cases over Hoyt channels." *IEEE Communications Letters*,11, 2007, pp.31-33.
[6] M. K. Simon and M.S. Alouini, *Digital Communication over Fading Channels*, 2nd edition, New York. Wiley, 2000.
[7] A. M. Magableh and M. M. Matalgah, "Capacity of SIMO systems over non-identically independent nakagami-m channels," *in Proc. IEEE Sarnoff Symposium*, April 2007, pp. 1–5.
[8] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT2007)*, Nice, France, 2007, pp. 1301–130.
[9] Md. Sohidul Islam and Mohammad Rakibul Islam, "Positive Secrecy Mutual Information over non-identically independently distributed Nakagami-q Fading Wireless Channel," *in proc. International Conference on Engineering, Research, Innovation and Education*, p.477-482, Sylhet, 2013.

Md. Md. Sohidul Islam received his B.Sc. in Computer Engineering from American International University Bangladesh (AIUB), and MS on Telecommunication Engineering from East West University (EWU), Bangladesh in 2007 and 2010 respectively. Currently he is a PhD student in the Islamic University of Technology (IUT). His research interest includes wireless information theoretic securities, secrecy capacity, wireless communications, satellite communications computer networks and quantum communications.

Mohammad Rakibul Islam received the B.Sc.Engg. and M.Sc.Engg. degree in Electrical and Electronic Engineering from Bangladesh University of Engineering and Technology (BUET), Bangladesh in 1998 and 2004 respectively. He also received MBA degree in Marketing from the Institute of Business Administration (IBA) under the University of Dhaka in 2006. He received his PhD degree in the department of Electronics and Radio Engineering from Kyung Hee University, South Korea in the year 2010. He joined the Department of Electrical and Electronic Engineering, Islamic University of Technology (IUT) as a faculty on 1999 and serving as a Professor there. His research interests include cooperative technique for wireless sensor networks, LDPC and QC-LDPC codes, secrecy capacity and other wireless applications.