Secrecy Capacity of Nakagami-m Fading Wireless Channels in the Presence of Multiple Eavesdroppers

Md. Zahurul I. Sarkar, Tharmalingam Ratnarajah and Mathini Sellathurai
ECIT, Queen's University Belfast
Queen's Road, Queen's Island
Belfast, BT3 9DT, UK
Email: msarkar01@qub.ac.uk

***Abstract*—This paper is concerned with the transmission of confidential message through Nakagami-m fading wireless channel in the presence of multiple eavesdroppers. The eavesdroppers are mutually independent and the information is secure if it cannot be eavesdropped by any eavesdropper. Considering the problem of secret communications between two nodes over Nakagami-m fading channel where a number of eavesdroppers observes their transmissions through other Nakagami-m fading channels, we characterize the probability of non-zero secrecy capacity and secure outage probability to investigate the secrecy capacity in terms of secure outage probability. We also present a formulation of the ergodic secrecy capacity in the presence of multiple eavesdroppers.**

***Index Terms*—Multiple eavesdroppers, eavesdropper's channel, secure outage probability, outage secrecy capacity, ergodic secrecy capacity.**

I. Introduction

The privacy and security in wireless communication networks have taken on an increasingly important role, as these networks are used to transmit personal information, and that information must be strongly protected to guard against unauthorized access to the contents of signals. The conception of information-theoretic security was first introduced by shannon [1] to characterize fundamental limits of secure communications over wireless channels. Recently, the secrecy capacity for both the transmitter and receiver equipped with single antenna (SISO) case [2], the transmitter with single antenna and the receiver with multiple antenna (SIMO) case [3], the transmitter with multiple antenna and the receiver with single antenna (MISO) case [4], and both the transmitter and receiver equipped with multiple antenna (MIMO) case [5], [6] were characterized in case of Rayleigh fading channels. The secrecy capacity of SISO case has also been extended with multiple eavesdroppers [7] considering the channel as quasi-static Rayleigh fading. In [8], the secrecy capacity of Gaussian Multiple Access Wire-Tap (GMAC-WT) channel was studied, where multiple users communicate with an intended receiver in the presence of an eavesdropper.

On the other hand, a great number of distributions exists to describe the statistics of the mobile radio signal. Among them, the Nakagami-m distribution has been given a special attention for its ease of manipulation and wide range of applicability [9]. This distribution provides more flexibility in matching experimental data than the Rayleigh, log-normal or Rician distributions. It has the advantages of including Rayleigh as a special case and it can model fading conditions which are more or less severe than that of Rayleigh. More importantly, the Nakagami-m distribution has been found to be very good fitting for the mobile radio channel [10]. Recently, the upper bound of secret key rate for Nakagami-m fading SISO channel in the presence of an eavesdropper was determined in [11]. However, to the best of author's knowledge, the secrecy capacity of Nakagami-m fading channel in the presence of multiple eavesdropper has not been reported in the literature.

Devoted to the general problem of securing transmissions over wireless channels, in this paper, we consider the transmission of confidential data over Nakagami-m fading channel to find the secrecy capacity in the presence of multiple eavesdroppers. We first derive the expressions for the probability of non-zero secrecy capacity and secure outage probability. Then we find the outage secrecy capacity in terms of secure outage probability. Finally, we find the expression for ergodic secrecy capacity in the presence of multiple eavesdroppers.

The rest of the paper is organized as follows. Section II characterizes the system model of the problem. The formulation of the problem is discussed in Section III. Section IV provides the numerical results of this paper. Finally, Section V describes the concluding remarks of this work.

II. System Model

The system model is shown in Fig.1. A legitimate user communicates with its corresponding receiver in the presence of N eavesdroppers. The transmitter, receiver and each eavesdropper are equipped with single antenna. We assume that all the eavesdroppers are mutually independent and the information received at the receiver is secured if it cannot be eavesdropped by any eavesdropper. The channel is known to the receiver only and transmitter sends message with constant power level. At the transmitter, the message block w is encoded into the codeword $x^n = [x(1), x(2), ..., x(i), ..., x(n)]$, which is suitable to be transmitted over the Nakagami-m fading channel. The receiver can obtain information about transmitted message by decoding the signal received. At the legitimate receiver, the received signal can be written as

$$y_{\mathrm{M}}(i) = h_{\mathrm{M}}(i)x(i) + z_{\mathrm{M}}(i) \tag{1}$$

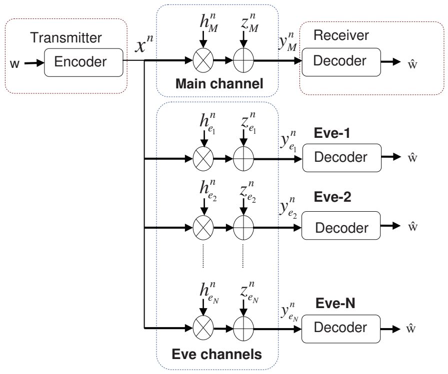

Fig. 1. System Model.

where $h_{\mathrm{M}}(i)$ is the complex channel coefficient from transmitter to the receiver (main channel), $z_{\mathrm{M}}(i) \sim \tilde{\mathcal{N}}(0, \sigma_{\mathrm{M}}^2)$ is the zero-mean circularly symmetric complex Gaussian noise of the main channel[1]. At the kth eavesdropper, the received signal is given by

$$y_{\mathrm{e_k}}(i) = h_{\mathrm{e_k}}(i)x(i) + z_{\mathrm{e_k}}(i), k = 1, 2, 3, ..., N \tag{2}$$

where $h_{\mathrm{e_k}}(i)$ denotes the complex channel coefficient from transmitter to the kth eavesdropper and $z_{\mathrm{e_k}}(i) \sim \tilde{\mathcal{N}}(0, \sigma_{\mathrm{e_k}}^2)$. The channel is power limited in the sense that $\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left\{|x(i)|^2\right\} = P$, where P corresponds to the average transmit signal power.

Using (1) and (2), the instantaneous SNRs at the legitimate receiver and the kth eavesdropper receiver conditioned on $h_{\mathrm{M}}(i)$ and $h_{\mathrm{e_k}}(i)$ are given by $\gamma_{\mathrm{M}}(i) = \frac{|h_{\mathrm{M}}(i)|^2 P}{\sigma_{\mathrm{M}}^2}$ and $\gamma_{\mathrm{e_k}}(i) = \frac{|h_{\mathrm{e_k}}(i)|^2 P}{\sigma_{\mathrm{e_k}}^2}$, respectively.

III. Problem Formulation

In this section, we first consider the realization of probability density function (pdf) and compute the secrecy capacity of Nakagami-m fading channel with multiple eavesdroppers. Then, we discuss the probability of non-zero secrecy capacity and the secure outage probability to characterize the secrecy capacity in terms of secure outage probability. Finally, we derive the expression for ergodic secrecy capacity in the presence of multiple eavesdroppers.

A. Secrecy Capacity with Multiple Eavesdroppers

The capacity of main channel conditioned on $h_{\mathrm{M}}(i)$ is given by,

$$C_{\mathrm{M}} = \log_2(1 + \gamma_{\mathrm{M}}) \quad \text{bps/Hz} \tag{3}$$

where γ_{M} is the instantaneous SNR of main channel, whose distribution function is

$$f(\gamma_{\mathrm{M}}) = \frac{m^m \gamma_{\mathrm{M}}^{m-1}}{\overline{\gamma}_{\mathrm{M}}^m \Gamma(m)} \exp\left(-\frac{m\gamma_{\mathrm{M}}}{\overline{\gamma}_{\mathrm{M}}}\right), \quad \gamma_{\mathrm{M}} > 0 \tag{4}$$

[1]$\tilde{\mathcal{N}}(\mu, \sigma^2)$ denotes a circularly symmetric complex Gaussian distribution with mean μ and variance σ^2.

Here, m is the Nakagami fading parameter and $\overline{\gamma}_{\mathrm{M}}$ is the average SNR of main channel and is given by,

$$\overline{\gamma}_{\mathrm{M}} = \frac{P\,\mathbb{E}\left\{|h_{\mathrm{M}}(i)|^2\right\}}{\sigma_{\mathrm{M}}^2}$$

In order to simplify the analysis, we assume that the eavesdropper's channels are mutually independent and their channel gains satisfy the same distribution. We can transmit message through the main channel so that no eavesdropper is able to decode any information from the main channel only when the effective channel gain of main channel is larger than that of any eavesdropper's channel. Therefore, the capacity of the eavesdropper's channel conditioned on $\{h_{\mathrm{e_k}}(i)\}_{k=1}^{N}$is given by,

$$C_{\mathrm{e}} = \log_2\{1 + \max_k \gamma_{\mathrm{e_k}}(i)\} = \log_2(1 + \gamma_{\mathrm{E}}) \quad \text{bps/Hz} \tag{5}$$

where γ_{E} is the maximum instantaneous SNR among all the eavesdroppers, whose distribution is given by,

$$f(\gamma_{\mathrm{E}}) = \frac{m^{mN} \gamma_{\mathrm{E}}^{mN-1}}{\overline{\gamma}_{\mathrm{E}}^{mN} \Gamma(mN)} \exp\left(-\frac{m\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right), \quad \gamma_{\mathrm{E}} > 0 \tag{6}$$

Here, $\overline{\gamma}_{\mathrm{E}}$ is the maximum average SNR of all the eavesdroppers and is given by,

$$\overline{\gamma}_{\mathrm{E}} = \max_k \frac{P\,\mathbb{E}\left\{|h_{\mathrm{e_k}}(i)|^2\right\}}{\sigma_{\mathrm{e_k}}^2}$$

Under perfect secrecy, the secrecy capacity of the Nakagami-m fading channel with multiple eavesdroppers conditioned on the channels is given by,

$$C_s = \begin{cases} \log_2(1 + \gamma_{\mathrm{M}}) - \log_2(1 + \gamma_{\mathrm{E}}), & \text{if } \gamma_{\mathrm{M}} > \gamma_{\mathrm{E}} \\ 0 & \text{if } \gamma_{\mathrm{M}} \leq \gamma_{\mathrm{E}} \end{cases} \tag{7}$$

B. Probability of Non-zero Secrecy Capacity

The probability of non-zero secrecy capacity in the Rayleigh fading channel with single eavesdropper is shown in [2]. In this paper, we find the probability of non-zero secrecy capacity for Nakagami-m fading channel in the presence of multiple eavesdroppers and is given by,

$$\begin{aligned} Pr\left(C_s > 0\right) &= Pr\left(\gamma_{\mathrm{M}} > \gamma_{\mathrm{E}}\right) \\ &= 1 - \frac{m^m}{\Gamma(m)} \sum_{i=0}^{mN-1} \frac{m^i \overline{\gamma}_{\mathrm{E}}^m \overline{\gamma}_{\mathrm{M}}^i \Gamma(m+i)}{i!\{m(\overline{\gamma}_{\mathrm{M}} + \overline{\gamma}_{\mathrm{E}})\}^{m+i}} \end{aligned} \tag{8}$$

We can also show a special result corresponding to the case of one eavesdropper and for Rayleigh fading channel i.e. for $N = 1$ and $m = 1$.

$$Pr\left(C_s > 0\right) = 1 - \frac{\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{M}} + \overline{\gamma}_{\mathrm{E}}} = \frac{\overline{\gamma}_{\mathrm{M}}}{\overline{\gamma}_{\mathrm{M}} + \overline{\gamma}_{\mathrm{E}}},$$

which is exactly the Eq. (7) in [2].

C. Secure Outage Probability

The secure outage probability that the instantaneous secrecy capacity C_s is less than a target secrecy rate $R_s > 0$, is

$$P_{out}\left(R_s\right) = Pr\left(C_s < R_s\right)$$

The significance of the definition is that when the secrecy rate is set to R_s, the confidential communication will be ensured only if $C_s > R_s$, otherwise the secure transmission will not be guaranteed.

Now, recalling the total probability theorem,

$$\begin{aligned} P_{out}\left(R_s\right) &= Pr\left(C_s < R_s|\gamma_{\mathrm{M}} > \gamma_{\mathrm{E}}\right) Pr\left(\gamma_{\mathrm{M}} > \gamma_{\mathrm{E}}\right) \\ &+ Pr\left(C_s < R_s|\gamma_{\mathrm{M}} \leq \gamma_{\mathrm{E}}\right) Pr\left(\gamma_{\mathrm{M}} \leq \gamma_{\mathrm{E}}\right) \end{aligned}$$

we get the secure outage probability as shown in equation (9) at the bottom of this page, where

$$g = \frac{2^{R_s} m}{\overline{\gamma}_{\mathrm{M}}} + \frac{m}{\overline{\gamma}_{\mathrm{E}}}, \quad r = mN, \quad \xi = \frac{2^{R_s}}{2^{R_s} - 1}$$

and $L_n^{\alpha}(x)$ is the Laguerre polynomial of order n defined as [12, eq. (8.970.1)]

$$L_n^{\alpha}(x) = \frac{1}{n!} e^x x^{-\alpha} \frac{d^n}{dx^n}\left(e^{-x} x^{n+\alpha}\right) = \sum_{l=0}^{n} (-1)^l \binom{n+\alpha}{n-l} \frac{x^l}{l!}$$

From equation (9), we can also get a special result in the case of one eavesdropper and for Rayleigh fading channel i.e. for $N = 1$ and $m = 1$.

$$P_{out}\left(R_s\right) = 1 - \frac{\overline{\gamma}_{\mathrm{M}}}{\overline{\gamma}_{\mathrm{M}} + 2^{R_s}\overline{\gamma}_{\mathrm{E}}} \exp\left(-\frac{2^{R_s} - 1}{\overline{\gamma}_{\mathrm{M}}}\right)$$

which corresponds to the Eq. (9) in [2].

D. Outage Secrecy Capacity

The ϵ-outage secrecy capacity is defined as the largest secrecy rate such that the outage probability is less than ϵ i.e.

$$p_{out}(C_{out}(\epsilon)) = \epsilon \tag{10}$$

It is hard to find the outage secrecy capacity analytically since the outage probability is a complicated function of the secrecy rate but it is possible to compute its value numerically based on equation (9).

E. Ergodic Secrecy Capacity

The ergodic secrecy capacity is calculated as the average of instantaneous secrecy multicast capacity over γ_{M} and γ_{E}. First, for a given γ_{M}, the average secrecy capacity over γ_{E} can be written as shown in equation (11) at the bottom of the next page.

Therefore, the ergodic secrecy capacity is

$$\begin{aligned} \langle C_s \rangle &= \int_0^{\infty} \langle C_s(\gamma_{\mathrm{M}}) \rangle f(\gamma_M) d\gamma_M \\ &= \int_0^{\infty} G f(\gamma_{\mathrm{M}}) d\gamma_{\mathrm{M}} - \int_0^{\infty} H f(\gamma_{\mathrm{M}}) d\gamma_{\mathrm{M}} \end{aligned} \tag{12}$$

Now, from equation (4), (11) and (12), we get the analytical expression of ergodic secrecy capacity as shown in equation (13), at the bottom of the last page, where

$$a = \frac{m^m (mN-1)!}{\Gamma(m)\Gamma(mN)\overline{\gamma}_{\mathrm{M}}^m}, \quad E_1(x) = \int_x^{\infty} \frac{\exp(-t)}{t} dt,$$

$$b = \frac{(m-1)!}{\left(\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right)^m}, \quad \beta = \frac{(mN+m-1)! mN}{\left(\frac{m}{\overline{\gamma}_{\mathrm{E}}} + \frac{m}{\overline{\gamma}_{\mathrm{M}}}\right)^{mN+m}},$$

$$c = \frac{m^i (m+i-1)!}{i! \overline{\gamma}_{\mathrm{E}}^i \left(\frac{m}{\overline{\gamma}_{\mathrm{M}}} + \frac{m}{\overline{\gamma}_{\mathrm{E}}}\right)^{m+1}}, \quad d = \frac{m^{mN+m-2}}{\Gamma(mN)\Gamma(m)(N)^2 \overline{\gamma}_{\mathrm{E}}^{mN} \overline{\gamma}_{\mathrm{M}}^m}$$

and $E(\cdot)$ is the 'MacRobert's E-Function'.

IV. Numerical Results

Figs.2 and 3 show the probability of non-zero secrecy capacity as a function of $\overline{\gamma}_{\mathrm{M}}$ and N respectively, for selected values of $\overline{\gamma}_{\mathrm{E}}$ with $m = 1.5$. We see that for a fixed N as shown in Fig.2, the better the main channel, the larger the probability of positive secrecy capacity. From figure 3, it is observed that probability of positive secrecy capacity decreases with N for a fixed value of $\overline{\gamma}_{\mathrm{M}}$.

Figs.4 and 5 show the secure outage probability as a function of $\overline{\gamma}_{\mathrm{M}}$ and N respectively, for selected values of $\overline{\gamma}_{\mathrm{E}}$ with $m = 1.0$ and $R_s = 0.1$. From these figures, it is observed that $P_{out}\left(R_s\right)$ increases with $\overline{\gamma}_{\mathrm{E}}$ and N and decreases with $\overline{\gamma}_{\mathrm{M}}$.

Figs.6 and 7 provide the 10% outage secrecy capacity ($C_{s,out}$) as a function of $\overline{\gamma}_{\mathrm{M}}$ and N respectively, for selected values of $\overline{\gamma}_{\mathrm{E}}$ and m. We see that $C_{s,out}$ decreases with N and

$$P_{out}\left(R_s\right) = \begin{cases} 1 - \sum_{i=0}^{1-m} \left[\left(\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right)^i \times \frac{\left(2^{R_s}-1\right)^i m^{mN} exp\left(-\frac{m\left(2^{R_s}-1\right)}{\overline{\gamma}_{\mathrm{M}}}\right)}{i! \overline{\gamma}_{\mathrm{E}}^{mN} \Gamma(mN)} \times \frac{\Gamma(mN)}{\left(\frac{m \times 2^{R_s}}{\overline{\gamma}_{\mathrm{M}}} + \frac{m}{\overline{\gamma}_{\mathrm{E}}}\right)^{mN}} \right] & \text{if } \frac{1}{2} \leq m \leq 1 \\ 1 - \sum_{j=1}^{m-1} \left[\left(\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right)^j \times \frac{\left(2^{R_s}-1\right)^j m^{mN} exp\left(-\frac{m\left(2^{R_s}-1\right)}{\overline{\gamma}_{\mathrm{M}}}\right)}{j! \overline{\gamma}_{\mathrm{E}}^{mN} \Gamma(mN)} \times \frac{\pi^2}{g^r \Gamma(j) sin\{\pi(r+j)\}} \right. & \\ \left. \times \left\{ \left(\frac{g}{\xi}\right)^j \frac{L_j^{j-r}\left(\frac{g}{\xi}\right)}{sin(-\pi j)\Gamma(r-1)} - \left(\frac{g}{\xi}\right)^r \frac{L_{-r}^{r-j}\left(\frac{g}{\xi}\right)}{sin(-\pi r)\Gamma(j+1)} \right] & \text{if } m > 1 \end{cases} \tag{9}$$

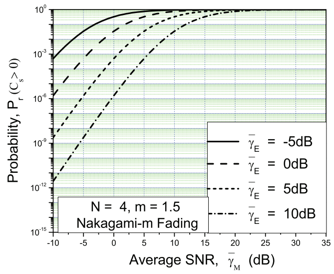

Fig. 2. The probability of non-zero secrecy capacity versus $\overline{\gamma}_{\mathrm{M}}$, for selected values of $\overline{\gamma}_{\mathrm{E}}$ with $m=1.5$ and $N=4$.

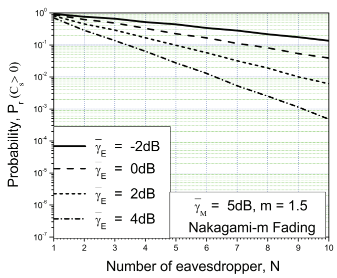

Fig. 3. The probability of non-zero secrecy capacity versus number of eavesdropper, N, for selected values of $\overline{\gamma}_{\mathrm{E}}$ with $m=1.5$ and $\overline{\gamma}_{\mathrm{M}}=5$dB.

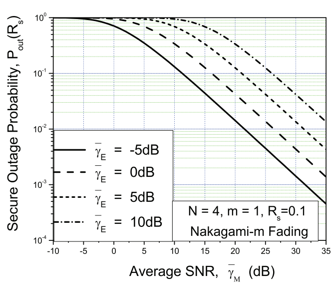

Fig. 4. The secure outage probability versus $\overline{\gamma}_{\mathrm{M}}$, for selected values of $\overline{\gamma}_{\mathrm{E}}$ with $R_s=0.1$, $N=4$ and $m=1$.

$\overline{\gamma}_{\mathrm{E}}$ and increases with $\overline{\gamma}_M$ and m. But the effect of m on the $C_{s,out}$ decreases with the increase in $\overline{\gamma}_{\mathrm{E}}$.

The ergodic secrecy capacity as a function of $\overline{\gamma}_{\mathrm{M}}$ and N, for selected values of $\overline{\gamma}_{\mathrm{E}}$ and m are shown in Figs.8 and 9,

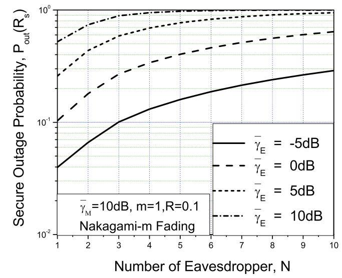

Fig. 5. The secure outage probability versus number of eavesdropper, N, for selected values of $\overline{\gamma}_{\mathrm{E}}$ with $R_s=0.1$, $\overline{\gamma}_{\mathrm{M}}=10$dB and $m=1$.

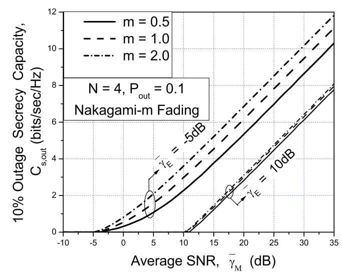

Fig. 6. The outage secrecy capacity versus $\overline{\gamma}_{\mathrm{M}}$, for selected values of $\overline{\gamma}_{\mathrm{E}}$ and m with $N=4$ and $P_{out}=0.1$.

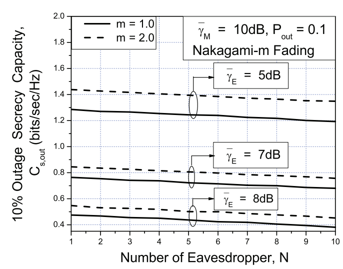

Fig. 7. The outage secrecy capacity versus number of eavesdropper, N, for selected values of $\overline{\gamma}_{\mathrm{E}}$ and m with $\overline{\gamma}_{\mathrm{M}}=10$dB and $P_{out}=0.1$.

respectively. It is found that $\langle C_s\rangle$ increases with $\overline{\gamma}_{\mathrm{M}}$ and m and decreases with N and $\overline{\gamma}_{\mathrm{E}}$.

$$\langle C_s(\gamma_{\mathrm{M}})\rangle = \int_0^{\gamma_{\mathrm{M}}} C_s f(\gamma_{\mathrm{E}})d\gamma_{\mathrm{E}} = \underbrace{\frac{(mN-1)!\log(1+\gamma_{\mathrm{M}})}{\Gamma(mN)}\left\{1-exp\left(-\frac{m\gamma_{\mathrm{M}}}{\overline{\gamma}_{\mathrm{E}}}\right)\sum_{i=o}^{mN-1}\frac{m^i\gamma_{\mathrm{M}}^i}{i!\gamma_{\mathrm{E}}^i}\right\}}_{G}$$

$$-\underbrace{\frac{m^{mN}\gamma_{\mathrm{M}}^{mN}exp(-\frac{m\gamma_{\mathrm{M}}}{\overline{\gamma}_{\mathrm{E}}})}{\Gamma(mN)\overline{\gamma}_{\mathrm{E}}^{mN}(mN)^2}\left\{-1+mN\log_e\left(1+\gamma_{\mathrm{M}}\right)+{}_2F_1\left(mN,1;\,1+mN\,;-\gamma_{\mathrm{M}}\right)\right\}}_{H} \qquad (11)$$

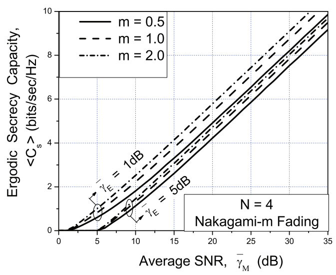

Fig. 8. The ergodic secrecy capacity versus $\overline{\gamma}_{\mathrm{M}}$, for selected values of $\overline{\gamma}_{\mathrm{E}}$ and m with $N = 4$.

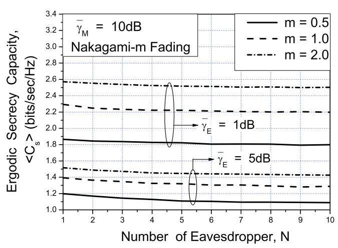

Fig. 9. The ergodic secrecy capacity versus number of eavesdropper, N, for selected values of $\overline{\gamma}_{\mathrm{E}}$ and m with $\overline{\gamma}_{\mathrm{M}} = 10$dB.

V. Conclusion

We characterize the probability of non-zero secrecy capacity, secure outage probability, outage secrecy capacity and ergodic secrecy capacity for Nakagami-m fading channel in the presence of multiple eavesdroppers. It is observed that, the secure outage probability increases with N and $\overline{\gamma}_{\mathrm{E}}$, which in turn causes the reduction of outage secrecy capacity in the Nakagami-m fading channel with multiple eavesdroppers. Both the outage and ergodic secrecy capacity increases with m, since the increase in Nakagami parameter m decreases the severity of fading in the channel.

Acknowledgement

This work was supported by the UK Engineering and Physical Sciences Research Council under grant number EP/G026092/1.

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.

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

[3] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT05)*, 2005, pp. 2152–2155.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *Arxiv preprint arXiv:0708.4219*, 2007.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channe," *Arxiv preprint arXiv:0710.1920*, 2007.

[6] A. Khisti and G. Wornell, "The MIMOME channel," *Arxiv preprint arXiv:0710.1325*, 2007.

[7] 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. 1301–1305.

[8] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT2006), Seatle, USA*, 2006, pp. 1164–1168.

[9] N. C. Beaulieu and C. Cheng, "Efficient nakagami-m fading channel simulation," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 2, pp. 413–424, 2005.

[10] H. Suzuki, "A statistical model for urban radio propagation," *IEEE Transactions on Communications*, vol. COM-25, no. 7, pp. 673–680, 1977.

[11] A. Shahzadi, M. G. Madiseh, and A. A. B. Shirazi, "Secret key capacity for wireless nakagami and suzuki fading channels," *IJCSNS International Journal of Computer Science and Network Security*, vol. 7, no. 3, pp. 296–303, 2007.

[12] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. San Diego, CA: Academic, 2000.

$$
\begin{aligned}
\langle C_s \rangle = a\Bigg[& b\Bigg\{1+\sum_{j=1}^{m-1}\frac{1}{(m-j)!}\left(-\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right)^{m-j}\Bigg\} exp\left(\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right) E_1\left(\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right) + b\Bigg\{\sum_{j=1}^{m-1}\sum_{k=1}^{m-j}\sum_{l=1}^{k}\frac{(-1)^{m-j-k}\left(\frac{\overline{\gamma}_{\mathrm{M}}}{m}\right)^{j+l-m}}{k(m-j-k)!(k-l)!}\Bigg\} \\
& -\sum_{i=0}^{mN-1} c\Bigg\{1+\sum_{u=1}^{m+i-1}\frac{1}{(m+i-u)!}\left(-\frac{m}{\overline{\gamma}_{\mathrm{M}}}-\frac{m}{\overline{\gamma}_{\mathrm{E}}}\right)^{m+i-u}\Bigg\} exp\left(\frac{m}{\overline{\gamma}_{\mathrm{M}}}+\frac{m}{\overline{\gamma}_{\mathrm{E}}}\right) E_1\left(\frac{m}{\overline{\gamma}_{\mathrm{M}}}+\frac{m}{\overline{\gamma}_{\mathrm{E}}}\right) \\
& -\sum_{i=0}^{mN-1} c\Bigg\{\sum_{u=1}^{m+i-1}\sum_{v=1}^{m+i-u}\sum_{w=1}^{v}\frac{(-1)^{m+i-u-v}\left(\frac{1}{\frac{m}{\overline{\gamma}_{\mathrm{M}}}+\frac{m}{\overline{\gamma}_{\mathrm{E}}}}\right)^{u+w-m-i}}{v(m+i-u-v)!(v-w)!}\Bigg\}\Bigg] - d\Bigg[-(mN+m-1)!\left(\frac{m}{\overline{\gamma}_{\mathrm{E}}}+\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right)^{-mN-m} \\
& +\beta\Bigg\{1+\sum_{\rho=1}^{mN+m-1}\frac{(-1)^{mN+m-\rho}}{(mN+m-\rho)!}\left(\frac{m}{\overline{\gamma}_{\mathrm{E}}}+\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right)^{mN+m-\rho}\Bigg\} exp\left(\frac{m}{\overline{\gamma}_{\mathrm{E}}}+\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right) E_1\left(\frac{m}{\overline{\gamma}_{\mathrm{E}}}+\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right) \\
& +\beta\Bigg\{\sum_{\rho=1}^{mN+m-1}\sum_{\lambda=1}^{mN+m-\rho}\sum_{\tau=1}^{\lambda}\frac{(-1)^{mN+m-\rho-\lambda}\left(\frac{1}{\frac{m}{\overline{\gamma}_{\mathrm{E}}}+\frac{m}{\overline{\gamma}_{\mathrm{M}}}}\right)^{\rho+\tau-mN-m}}{\lambda(mN+m-\rho-\lambda)!(\lambda-\tau)}\Bigg\} + \frac{E\left(mN, 1, mN+m : 1+mN : \frac{m}{\overline{\gamma}_{\mathrm{M}}}+\frac{m}{\overline{\gamma}_{\mathrm{M}}}\right)}{\frac{\Gamma(mN)}{\Gamma(1+mN)}\left(\frac{m}{\overline{\gamma}_{\mathrm{M}}}+\frac{m}{\overline{\gamma}_{\mathrm{E}}}\right)^{-(mN+m)}}\Bigg]
\end{aligned}
\tag{13}
$$