American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-5, Issue-10, pp-283-290
www.ajer.org
Research Paper Open Access

Security in Multicasting System with Diversity Combining Techniques

Rosni Sayed[1], A. S. M. Badrudduza [2], Tonmoy Ghosh[3]

[1,3]Electrical and Electronic Engineering Department, Pabna University of Science & Technology, Bangladesh.
[2]Department of Electrical and Electronic Engineering, Rajshahi University of Engineering & Technology, Bangladesh.

ABSTRACT: *This paper is concerned with a Rayleigh fading multicasting SIMO network, where a single source transmits to a group of users in the presence of an eavesdropper. We consider selection combining (SC) and maximal ratio combining (MRC) diversity techniques at the receivers and eavesdropper. We derive the closed-form analytical expressions for the probability of nonzero secrecy multicast capacity, and ergodic secrecy multicast capacity. This analysis shows, how the channel diversity enhances security in multicast channels. We also present a comparison between SC and MRC diversity techniques to show which technique is better for secure wireless multicasting.*

Keywords: *Diversity, MRC, multicasting, secrecy multicast capacity, SC.*

I. INTRODUCTION

Security is an important issue in the multicasting wireless communication system, since the wireless medium is susceptible to eavesdropping and wireless multicasting networks are used to transmit personal and confidential information. Security enables the destined to successfully obtain the source information. On the other hand, channel diversity has been proved as an effective technique in wireless communication system to increase secrecy capacity. The theory of secrecy of communication systems was first developed by Shannon in [1].

Several work have been done in this field. Recently, bounds on the secrecy capacity with SC and MRC diversity techniques was studied in [2] for Rayleigh fading channel. The authors showed that the reduction of secrecy capacity due to the lack of transmit signal power can be improved by exploiting diversity combining. In [3], authors quantified the loss of security due to the channel estimation error and showed, how the channel diversity overcomes that loss. In [4], authors studied the security of cognitive radio network using secure switch-and-stay combining (SSSC) techniques and showed that SSSC reduces the channel estimation complexity significantly.

In this paper, we define the secrecy multicast capacity so that the eavesdropper can not be able to decode any information from the main channel (i.e., channel between transmitter and receiver). Then, we drive the closed-form analytical expressions for the probability of non-zero secrecy multicast capacity and ergodic secrecy capacity for with SC and MRC diversity techniques.

The rest of the paper is organized as follows. The system model is discussed in section II. Section III defines secrecy multicast capacity and section IV derives the Probability Density Function (PDF) of multicast capacity of the proposed system. Closed-form expressions for the probability of non-zero secrecy multicast capacity and ergodic secrecy multicast capacity for multicasting are described in Sections V and VI, respectively. Section VII provides the numerical results. Finally, Section VIII draws the conclusion of this work.

II. SYSTEM MODEL

This paper is concerned with a multicasting scenario, where a source transmits a common stream of information to a group of M client receivers in the presence of an eavesdropper shown in Fig. 1. Each client receiver and eavesdropper are equipped with n_R and n_E antennas, respectively. All the channels are considered as Rayleigh fading. Therefore, the received signal at ith receiver, where, i=1,2,….,M, is given by (1), that is:

$$\boldsymbol{y}_{\boldsymbol{m}_{\boldsymbol{i}}} = \boldsymbol{h}_i x + \boldsymbol{z}_i \tag{1}$$

Where h_i denotes the direct channel coefficient between the source and the ith receiver, x denotes the transmitted signal and $\boldsymbol{z}_{\boldsymbol{i}} \sim \widetilde{\mathcal{N}}(0, N_{m0} I_{nR})$ is the Gaussian noise, imposed on the ith receiver. $\widetilde{\mathcal{N}}(0, N_{m0} I_{nR})$

means Gaussian distribution with zero mean and $N_{m\,0}I_{n\,R}$ variance, where $N_{m\,0}$ denotes the noise power of the ith receiver and $I_{n\,R}$ is an identity matrix of $n_R \times n_R$.
Again, the received signal at eavesdropper is shown in (2) and is given by:

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

Where $\boldsymbol{g}_e$ denotes the channel coefficient between the source and eavesdropper and $\boldsymbol{z_e} \sim \widetilde{\mathcal{N}}(0, N_{e\,0}I_{n\,E})$ is the Gaussian noise, imposed on the receiver of eavesdropper. $\widetilde{\mathcal{N}}(0, N_{e\,0}I_{n\,E})$ means Gaussian distribution with zero mean and $N_{e\,0}I_{n\,E}$ variance, where $N_{e\,0}$ denotes the noise power of the receiver of eavesdropper and $I_{n\,E}$ is an identity matrix of $n_E \times n_E$.

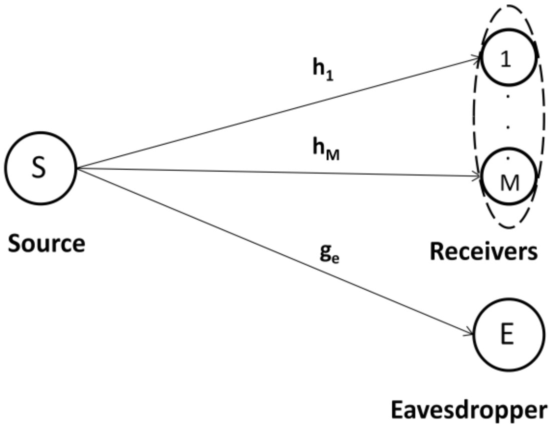

Fig.1: System Model

III. MULTICAST SECRECY CAPACITY

From (1), the received signal at the i^{th} receiver is given by:

$$\boldsymbol{y_{m_i}} = \boldsymbol{h}_i x + \boldsymbol{z}_i$$

Mutual information at i^{th} receiver is given by (3), that is:

$$I(x; \boldsymbol{y_{m_i}}) = h(\boldsymbol{y_{m_i}}) - h(\boldsymbol{z_i}) \tag{3}$$

Here $h(.)$ denotes entropy. Let the variance of x is given by $Q_x = \mathbb{E}\,(\mathrm{xx}^{\dagger}) = \mathrm{P}$, where $\mathbb{E}(.)$and $(.)^{\dagger}$ denote the expectation and conjugate transpose operations, respectively.
Now, co-variance of received signal can be derived as follows

$$\begin{aligned}
\boldsymbol{R}_{\boldsymbol{y_{m_i}}} &= \mathbb{E}\,(\boldsymbol{y_{m_i}}, \boldsymbol{y_{m_i}}^{+}) \\
&= \mathbb{E}\{(\boldsymbol{h}_i x + \boldsymbol{z}_i)(\boldsymbol{h}_i x + \boldsymbol{z}_i)^{+}\} \\
&= \mathbb{E}\{(\boldsymbol{h}_i x + \boldsymbol{z}_i)(x^{+}\boldsymbol{h}_i^{+} + \boldsymbol{z}_i^{+})\} \\
&= \mathbb{E}(\boldsymbol{h}_i x\, x^{+}\boldsymbol{h}_i^{+} + \boldsymbol{z}_i\boldsymbol{z}_i^{+}) \\
&= \boldsymbol{h}_i \mathbb{E}(x\, x^{+})\boldsymbol{h}_i^{+} + \mathbb{E}(\boldsymbol{z}_i\boldsymbol{z}_i^{+}) \\
&= \boldsymbol{h}_i P \boldsymbol{h}_i^{+} + N_{m_o}\boldsymbol{I}_{n\,R}
\end{aligned}$$

Similarly, covariance of noise signal is given by,

$$\boldsymbol{R}_{\boldsymbol{z_i}} = \mathbb{E}(\boldsymbol{z}_i\boldsymbol{z}_i^{+}) = N_{m_o}\boldsymbol{I}_{n\,R}$$

Hence, the entropy of $\boldsymbol{y_{m_i}}$ is given by

$$\therefore h(\boldsymbol{y}_{m\,i}) = \log_2 \det\left(\pi e R_{y_{m\,i}}\right) = \log_2 det[\pi e(\boldsymbol{h}_i P \boldsymbol{h}_i^{+} + N_{m_o}\boldsymbol{I}_{n\,R})]$$

Similarly, the entropy of $\boldsymbol{z}_i$is given by

$$h(\boldsymbol{z}_i) = \log_2 det(\pi e R_{\boldsymbol{z_i}}) = \log_2 det(\pi e N_{m_o}\boldsymbol{I}_{n\,R})$$

Hence the mutual information at the i^{th} receiver is shown in (4) and is given by:

$$\begin{aligned}
I(x; \boldsymbol{y}_{m\,i}) &= \log_2 \frac{\det\left(\pi e\, R_{y_{m\,i}}\right)}{\det\left(\pi e\, R_{\boldsymbol{z}_i}\right)} \\
&= \log_2 \frac{\det[\pi e(\boldsymbol{h}_i P \boldsymbol{h}_i^{+} + N_{m_o}\boldsymbol{I}_{n\,R})]}{\det(N_{m_o}\boldsymbol{I}_{n\,R})}
\end{aligned}$$

$$= \log_2 \frac{\det[\boldsymbol{n}_{m_o}(\frac{P}{N_{m_o}}||\boldsymbol{h}_i||^2 + \boldsymbol{I}_{n_R})]}{\det(N_{m_o}\boldsymbol{I}_{n_R})}$$

$$= \log_2(1 + \frac{P}{N_{m_o}}||\boldsymbol{h}_i||^2) \qquad (4)$$

Multicast capacity of i^{th} receiver is given by (5), that is:

$$C_m = \log_2(1 + \frac{P}{N_{m_o}} \min_{1<i<M} ||\boldsymbol{h}_i||^2)$$

$$= \log_2\left(1 + \theta_1 \min_{1\leq i\leq M} \gamma_{m_i}\right) \qquad (5)$$

where,$\theta_1 = \frac{P}{N_{m_o}}$ and $\min_{1<i<M} \gamma_{m_i}$ is the minimum instantaneous SNR among all the receivers.

Here, from (2) the received signal at the eavesdropper is given by

$$\boldsymbol{y_e} = \boldsymbol{g}_e x + \boldsymbol{z}_e$$

Similarly, the mutual information at the eavesdropper is:

$$I(x; \boldsymbol{y_e}) = h(\boldsymbol{y}_e) - h(\boldsymbol{z}_e)$$

Now, co-variance of received signal at the eavesdropper is:

$$\begin{aligned} R_{y_e} &= \mathbb{E}\,(y_e, \boldsymbol{y}_e^+) \\ &= \mathbb{E}\{(\boldsymbol{g}_e x + \boldsymbol{z}_e)(\boldsymbol{g}_e x + \boldsymbol{z}_e)^+\} \\ &= \mathbb{E}\{(\boldsymbol{g}_e x + \boldsymbol{z}_e)(x^+\boldsymbol{g}_e^+ + \boldsymbol{z}_e^+)\} \\ &= \mathbb{E}(\boldsymbol{g}_e x\, x^+ \boldsymbol{g}_e^+ + \boldsymbol{z}_e\boldsymbol{z}_e^+) \\ &= \boldsymbol{g}_e \mathbb{E}(x\, x^+)\boldsymbol{g}_e^+ + \mathbb{E}(\boldsymbol{z}_e\boldsymbol{z}_e^+) \\ &= \boldsymbol{g}_e P \boldsymbol{g}_e^+ + N_{e_o}\boldsymbol{I}_{n_E} \end{aligned}$$

Similarly, covariance of noise signal is given by:

$$R_{z_e} = \mathbb{E}(\boldsymbol{z}_e\boldsymbol{z}_e^+) = N_{e_o}\boldsymbol{I}_{n_E}$$

Hence, the entropy of $\boldsymbol{y}_e$ is given by:

$$\begin{aligned} h\left(\boldsymbol{y}_{e_j}\right) &= \log_2 \det\left(\pi e R_{y_e}\right) \\ &= \log_2 \det[\pi e(\boldsymbol{g}_e P \boldsymbol{g}_e^+ + N_{e_o}\boldsymbol{I}_{n_E})] \end{aligned}$$

Similarly, the entropy of w_j is given by

$$\begin{aligned} h(\boldsymbol{z}_e) &= \log_2 det(\pi e R_{z_e}) \\ &= \log_2 \det(\pi e N_{e_o}\boldsymbol{I}_{n_E}) \end{aligned}$$

Hence the mutual information at the eavesdropper is given by (6) and is given by:

$$I(x; \boldsymbol{y}_e) = \log_2 \frac{\det\left(\pi e R_{y_e}\right)}{\det\left(\pi e R_{z_e}\right)}$$

$$= \log_2 \frac{\det[\pi e(\boldsymbol{g}_e P \boldsymbol{g}_e^+ + N_{e_o}\boldsymbol{I}_{n_E})]}{\det\left(\pi e N_{e_o}\boldsymbol{I}_{n_E}\right)}$$

$$= \log_2 \frac{\det[N_{e_o}(\frac{P}{N_{e_o}}||\boldsymbol{g}_e||^2 + \boldsymbol{I}_{n_E})]}{\det\left(N_{e_o}\boldsymbol{I}_{n_E}\right)}$$

$$= \log_2(1 + \frac{P}{N_{e_o}}||\boldsymbol{g}_e||^2) \qquad (6)$$

Capacity of eavesdropper is given by (7) and that is:

$$C_e = \log_2(1 + \frac{P}{N_{e_o}}||\boldsymbol{g}_e||^2)$$

$$= \log_2(1 + \theta_2\gamma_e) \qquad (7)$$

where, $\theta_2 = \frac{P}{N_{e_o}}$ and γ_e is the SNR of the eavesdropper channel.

Under perfect secrecy, the secrecy multicast capacity with is given by (8):

$$C_s = \max_{f(x)}(C_m - C_e)$$

$$= \log_2(1 + \theta_1 \min_{1\le i\le M} \gamma_{m\,i}) - \log_2(1 + \theta_2\gamma_e)$$
$$= \log_2[\tfrac{1+\theta_1 \min_{1\le i\le M} \gamma_{m\,i}}{1+\theta_2\boldsymbol{\gamma}_e}] \tag{8}$$

IV. PDF OF CAPACITY

The Probability Density Function (PDF) of capacity is important parameter to justify a channel quality because it helps to determine the capacity which brings the most benefit.

4.1 Maximal Ratio Combining

The PDF of instantaneous received SNRs $\gamma_{m\,i}$ and γ_e at the MRC output of users and eavesdropper can be expressed in (9) and (10), respectively as [5]:

$$f_{\gamma_m}^{MRC}(\gamma_{m\,i}) = \frac{{\gamma_{m\,i}}^{n_R-1}}{(n_R-1)!\gamma_{m\,o}^{n_R}} e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}} \tag{9}$$

$$f_{\boldsymbol{\gamma}_e}^{MRC}(\gamma_e) = \frac{{\boldsymbol{\gamma}_e}^{n_E-1}}{(n_E-1)!{\boldsymbol{\gamma}_e}^{n_E}} e^{-\frac{\boldsymbol{\gamma}_e}{\boldsymbol{\gamma}_{e\,o}}} \tag{10}$$

Here, $\gamma_{m\,o}$ and $\gamma_{e\,o}$ are average SNRs per symbol at user and eavesdropper, respectively. Distribution of the minimum SNR among all the users can be derived using (11)

$$f_{d_{min}}^{MRC}(\gamma_{m_i}) = M f_{\gamma_m}^{MRC}(\gamma_{m\,i})[1 - F_{\gamma_m}^{MRC}(\gamma_{m\,i})]^{M-1} \tag{11}$$

The cumulative distribution function (CDF) of $\gamma_{m\,i}$ can be derived as

$$F_{\gamma_m}^{MRC}(\gamma_{m\,i}) = \int_0^{\gamma_{m\,i}} f_{\gamma_m}^{MRC}(\gamma_{m\,i})\, d\gamma_{m\,i}$$
$$= \int_0^{\gamma_{m\,i}} \frac{\gamma_{m_i}^{n_R-1}}{(n_R-1)!\gamma_{m\,o}^{n_R}} e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}}\, d\gamma_{m\,i}$$

Using the identity of [6, eq. (3.351.1) & eq. (3.351.2)],

$$\int_0^u x^n e^{-\mu x}\, dx = \frac{n!}{\mu^{n+1}} - e^{-\mu u} \sum_{k=0}^{n} \frac{n!}{k!} \frac{u^k}{\mu^{n-k+1}} = \frac{n!}{\mu^{n+1}} - \mu^{-n-1}\Gamma(n+1, \mu u)$$

we have the final expression of CDF, shown in (12):

$$F_{\gamma_m}^{MRC}(\gamma_{m\,i}) = \frac{1}{(n_R-1)!\,\gamma_{m_o}^{n_R}} \left[\frac{(n_R-1)!}{\left(\frac{1}{\gamma_{m\,o}}\right)^{n_R}} - \left(\frac{1}{\gamma_{m\,i}}\right)^{-n_R} \frac{1}{(n_R-1)!} \Gamma\left(n_R, \frac{\gamma_{m\,i}}{\gamma_{m\,o}}\right) \right]$$
$$= 1 - \frac{\Gamma\left(n_R, \frac{\gamma_{m\,i}}{\gamma_{m\,o}}\right)}{(n_R-1)!} \tag{12}$$

Using (9) and (12) into (11), we get

$$f_{d_{min}}^{MRC}(\gamma_{m_i}) = M \frac{\gamma_{m_i}^{n_R-1}}{(n_R-1)!\,\gamma_{m_o}^{n_R}} e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}} \left[1 - (1 - \frac{\Gamma\left(n_R, \frac{\gamma_{m_i}}{\gamma_{m\,o}}\right)}{(n_R-1)!}) \right]^{M-1}$$
$$= M \frac{\gamma_{m_i}^{n_R-1}}{(n_R-1)!\,\gamma_{m_o}^{n_R}} e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}} \left[\frac{\Gamma\left(n_R, \frac{\gamma_{m_i}}{\gamma_{m\,o}}\right)}{(n_R-1)!} \right]^{M-1}$$
$$= M \frac{\gamma_{m_i}^{n_R-1}}{(n_R-1)!^M\,\gamma_{m_o}^{n_R}} e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}} \left[\Gamma\left(n_R, \frac{\gamma_{m\,i}}{\gamma_{m\,o}}\right) \right]^{M-1} \tag{13}$$

Proposition 4.1:

Let the probability density function of x is denoted by f(x). Then the probability density function of $C = \log_e(1 + \theta x)$ *is given by,*

$$q(c) = \frac{e^c}{\theta} f(\frac{e^c - 1}{\theta})$$

Proof:

We have, $C = \log_e(1 + \theta x)$. The probability density function of C, can be written as,

$$q(c) = \int \delta(C - \log_e(1 + \theta x)) f(x) dx$$

The following mathematical facts have been used for this proof ;

i) $\delta\big(f(x)\big) = \sum_l \frac{\delta(x-x_l)}{\left|\frac{df}{dx}\right|_{x_l}}$, where x_l are the zeros of $f(x)$, i.e. $f(x_l) = 0$;

ii) $\int_a^b \delta(x - x_1)\delta(x - x_2)dx = \delta(x_1 - x_2)$ for $a < x_1, x_2 < b$; and

iii) $\int_V f(x)\delta(x - x_o)dx = \begin{cases} f(x_o), & x_o \epsilon V \\ 0, & otherwise \end{cases}$

Assuming $\kappa = 1 + \theta x,$ we have $f(\kappa) = C - \log_e \kappa$ and $f^{'}(\kappa) = -\frac{1}{\kappa}$. Now from $f(\kappa) = 0, \kappa = e^C and\ f^{'}(k)|_{\kappa = e^C} = -\frac{1}{e^c}$. Using the above mathematical facts, we have

$$q(c) = \int e^C\, \delta(1 + \theta x - e^C) f(x) dx$$

$$= e^c \int \delta\left(\theta\left(x - \frac{e^C - 1}{\theta}\right)\right) f(x)dx$$

$$= \frac{e^c}{\theta} \int \delta\left(x - \frac{e^C - 1}{\theta}\right) f(x)dx, Since, \delta(dz) = \frac{1}{|d|}\delta(z)$$

$$= \frac{e^c}{\theta} f\left(\frac{e^C - 1}{\theta}\right),$$

Where, $\delta(.)$ is a delta function.

Using proposition 4.1, the PDF of C_m can be determined as shown in (14), that is:

$$q^{MRC}(C_m) \;= \frac{e^{C_m}}{\theta_1} f_{d_{min}}^{MRC}\left(\frac{e^{C_m} - 1}{\theta_1}\right)$$

$$= \frac{e^{C_m}}{\theta_1} M \frac{\left(\frac{e^{C_m} - 1}{\theta_1}\right)^{n_R - 1}}{(n_R - 1)!^M\, \gamma_{m_o}^{n_R}} = e^{C_m} M \frac{(e^{C_m} - 1)^{n_R - 1}}{(n_R - 1)!^M\, \gamma_{m_o}^{n_R}} e^{-\frac{e^{C_m} - 1}{\gamma_{m\,o}}} \left[\Gamma\left(n_R, \frac{e^{C_m} - 1}{\gamma_{m\,o}}\right)\right]^{M-1}$$

Using the identity$\Gamma(n, x) = (n - 1)!\, e^{-x} \sum_{m=0}^{n-1} \frac{x^m}{m!}$ of [6, eq. (8.352.7)], we have

$$q^{MRC}(C_m) = \sum_{t=0}^{(n_R-1)(M-1)} \frac{M\beta_t(n_R, M-1)}{{\gamma_{m\,0}}^{n_R+t}(n_R-1)!} e^{C_m} (e^{C_m} - 1)^{n_R+t-1} e^{-\frac{M}{\gamma_{m\,0}}(e^{C_m}-1)} \tag{14}$$

Here, θ_1 is assumed 1 for simplicity and $\beta_t(n_R, M - 1)$ denotes the coefficient of $(e^{C_m} - 1)^t$ in the expansion of $\left[\Gamma\left(n_R, \frac{e^{C_m}-1}{\gamma_{m\,o}}\right)\right]^{M-1}$.

Similarly, the PDF of C_e is derived and shown in (15):

$$q^{MRC}(C_e) \;= \frac{e^{C_e}(e^{C_e}-1)^{n_E-1}}{(n_E-1)!(e^{C_e}-1)^{n_E}} e^{-\frac{e^{C_e}-1}{\gamma_{e\,o}}} \tag{15}$$

4.2 Selection Combining

The PDF of instantaneous received SNRs γ_{m_i} and γ_e at the SC output of i^th receiver and eavesdropper are given by (16) and (17) [5]:

$$f_{\gamma_m}^{SC}(\gamma_{m\,i}) = \frac{n_R}{\gamma_{m\,o}}\left[1 - e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}}\right]^{n_R - 1} e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}} \tag{16}$$

$$f_{\gamma_e}^{SC}(\gamma_e) = \frac{n_E}{\gamma_{e\,o}}\left[1 - e^{-\frac{\gamma_e}{\gamma_{e\,o}}}\right]^{n_R - 1} e^{-\frac{\gamma_e}{\gamma_{e\,o}}} \tag{17}$$

Here, γ_{m_o} and γ_{e_o} are average SNRs per symbol at user and eavesdropper, respectively.

Distribution of the minimum SNR among all users can be expressed as shown in (18)

$$f_{d_{min}}^{SC}(\gamma_{m_i}) = M f_{\gamma_m}^{SC}(\gamma_{m\,i})[1 - F_{\gamma_m}^{SC}(\gamma_{m\,i})]^{M-1} \tag{18}$$

The cumulative distribution function (CDF) of $\gamma_{m\,i}$ can be derived as

$$F_{\gamma_m}^{SC}(\gamma_{m\,i}) = \int_0^{\gamma_{m\,i}} f_{\gamma_m}^{SC}(\gamma_{m\,i})\, d\gamma_{m\,i}$$

$$= \int_0^{\gamma_{m\,i}} \frac{n_R}{\gamma_{m\,o}}\left[1 - e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}}\right]^{n_R - 1} e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}}\, d\gamma_{m\,i}$$

Let, $1 - e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}} = z \Rightarrow \frac{1}{\gamma_{m\,o}} e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}} d\gamma_{m\,i} = dz$

For, $\gamma_{m\,i} = 0, z = 0$ and for $\gamma_{m\,i} = \gamma_{m\,i}$, $z = 1 - e^{-\frac{\gamma_{m\,i}}{\gamma_{m\,o}}}$. Substituting these values, we get

$$\therefore\ F_{\gamma_m}^{SC}\left(\gamma_{m_i}\right) = \int_0^{1-e^{-\frac{\gamma_{m_i}}{\gamma_{m_o}}}} n_R z^{n_R-1}\,dz$$

$$= \left[\frac{n_R z^{n_R}}{n_R}\right]_0^{1-e^{-\frac{\gamma_{m_i}}{\gamma_{m_o}}}} = \left(1 - e^{-\frac{\gamma_{m_i}}{\gamma_{m_o}}}\right)^{n_R} \tag{19}$$

Using (16), (18) and (19), we get

$$f_{d_{min}}^{SC}\left(\gamma_{m_i}\right) = M\frac{n_R}{\gamma_{m_o}}\left[1 - e^{-\frac{\gamma_{m_i}}{\gamma_{m_o}}}\right]^{n_R-1} e^{-\frac{\gamma_{m_i}}{\gamma_{m_o}}}\left[1 - \left(1 - e^{-\frac{\gamma_{m_i}}{\gamma_{m_o}}}\right)^{n_R}\right]^{M-1} \tag{20}$$

Using proposition 4.1, the PDF of C_m can be determined, that is shown in (21).

$$q^{SC}(C_m) = \frac{e^{C_m}}{\theta_1} f_{d_{min}}^{SC}\left(\frac{e^{C_m} - 1}{\theta_1}\right)$$

$$= \frac{e^{C_m}}{\theta_1} M\frac{n_R}{\gamma_{m_o}}\left[1 - e^{-\frac{e^{C_m}-1}{\theta_1\gamma_{m_o}}}\right]^{n_R-1} e^{-\frac{e^{C_m}-1}{\theta_1\gamma_{m_o}}}\left[1 - \left(1 - e^{-\frac{e^{C_m}-1}{\theta_1\gamma_{m_o}}}\right)^{n_R}\right]^{M-1}$$

$$= e^{C_m} M\frac{n_R}{\gamma_{m_o}}\left[1 - e^{-\frac{e^{C_m}-1}{\gamma_{m_o}}}\right]^{n_R-1} e^{-\frac{e^{C_m}-1}{\gamma_{m_o}}}\left[1 - \left(1 - e^{-\frac{e^{C_m}-1}{\gamma_{m_o}}}\right)^{n_R}\right]^{M-1}$$

Using the identity $(\mathrm{a} + \mathrm{x})^{\mathrm{n}} = \sum_{k=0}^{n}\binom{n}{k}x^k a^{n-k}$ of [6, eq.(1.111)] and assuming $\theta_1 = 1$ for simplicity, we have

$$q^{SC}(C_m) = \sum_{k_1=0}^{M-1}\sum_{k_2=0}^{n_R-1+n_Rk_1}(-1)^{k_1+k_2}\binom{M-1}{k_1}\binom{n_R-1+n_Rk_1}{k_2} M\frac{n_R}{\gamma_{m_o}} e^{C_m} e^{-\frac{(k_1+k_2+1)(e^{C_m}-1)}{\gamma_{m_o}}} \tag{21}$$

Similarly, the PDF of C_e is given by (22):

$$q^{SC}(C_e) = \frac{n_E e^{C_e}}{\gamma_{e_o}}\left[1 - e^{-\frac{e^{C_e}-1}{\gamma_{e_o}}}\right]^{n_E-1} e^{-\frac{e^{C_e}-1}{\gamma_{e_o}}} \tag{22}$$

V. PROBABILITY OF NONZERO SECRECY MULTICAST CAPACITY

The probability of non-zero secrecy capacity in the presence of eavesdropper can be defined as given in (23), based on the definition of positive secrecy capacity in [1].

$$Pr(C_s > 0) = Pr(C_m > C_e)$$

$$= \int_0^{\infty}\int_0^{C_m} q(C_m)q(C_e)dC_e dC_m \tag{23}$$

Using (14), (15) into (23) and performing integration, we get the expression of probability of nonzero secrecy capacity using MRC diversity as shown in (24)

$$\mathrm{Pr}^{MRC}(C_s > 0) = \sum_{t=0}^{(n_R-1)(M-1)}\frac{M\beta_t(n_R,M-1)}{{\gamma_{m_0}}^{n_R+t}(n_R-1)!}\left(\frac{M}{\gamma_{m_0}}\right)^{-n_R-t}\Gamma(n_R+t) - \sum_{d=0}^{n_E-1}\frac{1}{{\gamma_{e_0}}^d d!}\left(\frac{M}{\gamma_{m_0}} + \frac{1}{\gamma_{e_0}}\right)^{-n_R-t-d}$$

$$\times\,\Gamma(n_R + t + d) \tag{24}$$

Again using (21), (22) into (23) and performing integration we get the expression of probability of nonzero secrecy capacity using SC diversity as shown in (25)

$$\mathrm{Pr}^{SC}(C_s > 0) = \sum_{k_1=0}^{M-1}\sum_{k_2=0}^{n_R-1+n_Rk_1}\sum_{k_3=0}^{n_E-1} M\frac{n_Rn_E}{\gamma_{m_o}(1+k_3)}(-1)^{k_1+k_2+k_3}\binom{M-1}{k_1}\binom{n_R-1+n_Rk_1}{k_2}\binom{n_E-1}{k_3}\left(\frac{\gamma_{m_o}}{k_1+k_2+1} - \frac{\gamma_{m_o}\gamma_{e_o}}{\gamma_{e_o}(k_1+k_2+1)+\gamma_{m_o}(1+k_3)}\right) \tag{25}$$

VI. ERGODIC SECRECY MULTICAST CAPACITY

Ergodic capacity is related to channel capacity. It is same as Shannon channel capacity. It is the average capacity of the channel.

The ergodic secrecy capacity is the average of the instantaneous secrecy capacity that is given by (26):

$$\langle C_s\rangle = \mathbb{E}[C_m] - \mathbb{E}[C_e]$$

$$= \int_0^{\infty} C_m q(C_m)dC_m - \int_0^{\infty} C_e q(C_e)dC_e \tag{26}$$

Using (14), (15) into (26) and performing integration we get the expression of probability of nonzero secrecy capacity using MRC diversity as shown in (27)

$$\langle C_s\rangle^{MRC} = \sum_{t=0}^{(M-1)(n_R-1)} \frac{M\beta_t(n_R,M-1)}{(n_R-1)!\gamma_{mo}^{n_R+t}} \sum_{k_1=0}^{n_R-1+t} \frac{(n_R-1+t)!}{(n_R-1+t-k_1)!} \Bigg((-1)^{n_R-1+t-k_1-1}\left(\frac{\gamma_{mo}}{M}\right)^{1+k_1} e^{\frac{M}{\gamma_{mo}}} Ei\left(-\frac{M}{\gamma_{mo}}\right) + \sum_{k_2=1}^{n_R-1+t-k_2} \frac{(k_2-1)!}{(-1)^{n_R-1+t-k_1-k_2}}\left(\frac{\gamma_{mo}}{M}\right)^{1+k_1+k_2} \Bigg) - \frac{1}{(n_E-1)!} \sum_{k_3=0}^{n_E-1} \frac{(n_E-1)!}{(n_E-1-k_3)} \Bigg(\frac{(-1)^{(n_E-2-k_3}}{\gamma_{e_0}{}^{(n_E-1-k_3)}} e^{\frac{1}{\gamma_{e_0}}} Ei\left(-\frac{1}{\gamma_{e_0}}\right) + \sum_{k_4=1}^{(n_E-1-k_3)} \frac{(k_4-1)!}{(-\gamma_{e_0})^{(n_E-1-k_3-k_4)}} \Bigg) \tag{27}$$

Again using (21), (22) into (26) and performing integration we get the expression of probability of nonzero secrecy capacity using SC diversity as shown in (28)

$$\langle C_s\rangle^{SC} = \sum_{k_1=0}^{M-1} \sum_{k_2=0}^{n_R-1+n_R k_1} (-1)^{k_1+k_2} \binom{M-1}{k_1} \binom{n_R-1+n_R k_1}{k_2} M \frac{n_R}{1+k_2} e^{\frac{1+k_2}{\gamma_{m0}}} \Gamma\left(0, \frac{1+k_2}{\gamma_{m0}}\right) - \sum_{k_3=0}^{n_E-1} n_E (-1)^{k_3} \binom{n_E-1}{k_3} \frac{e^{\frac{1+k_3}{\gamma_{e0}}} \Gamma\left(0, \frac{1+k_3}{\gamma_{e0}}\right)}{1+k_3} \tag{28}$$

VII. NUMERICAL RESULTS

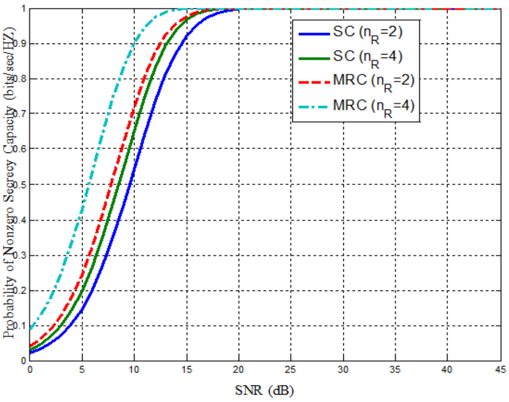

Fig. 2: The probability of non-zero secrecy multicast capacity versus average SNR of main channel for selected values of n_R with M = 2.

Fig.2 shows the probability of non-zero secrecy multicast capacity as a function of the average SNR of the main channel with SC and MRC diversity schemes. We see that for a particular number of antennas at the receivers, MRC diversity enhances security more significantly than SC diversity.

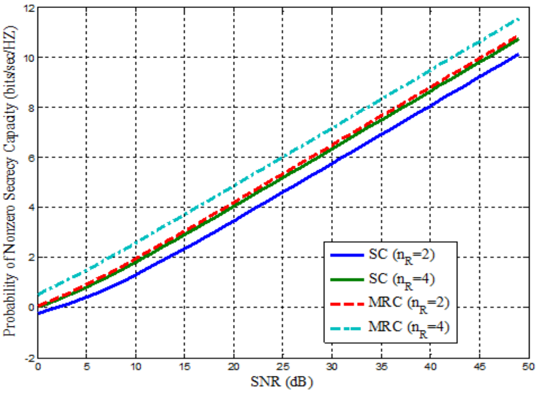

Fig. 3: The ergodic secrecy multicast capacity versus average SNR of main channel for selected values of n_R with M = 2.

Fig.3 shows the ergodic secrecy multicast capacity as a function of the average SNR of the main channel with SC and MRC diversity schemes. From the figure, it is observed that ergodic secrecy multicast capacity increases with the number of receive antennas but for a particular number of receiving antennas, MRC diversity enhances security more than the SC diversity.

VIII. CONCLUSION

In this paper, we study the security of a multicasting scenario in the presence of a single eavesdropper. Here the closed-form analytical expressions for the ergodic secrecy multicast capacity and probability of non-zero secrecy multicast capacity are derived for multicasting with MRC and SC diversity schemes at the receivers and eavesdropper. According to the numerical results, we can conclude that both the MRC and SC diversity enhance security in multicast networks but the effect of MRC diversity is more significant than SC diversity.

REFERENCES

[1]. C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, *28(4)*, 1949: 656–715.

[2]. M. Sarkar and T. Ratnarajah, Bounds on the secrecy capacity with diversity combining techniques: Proc. *IEEE Wireless Communications and Networking Conference* , April 2012: 2847–2851.

[3]. K. S. Ahn, S.-W. Choi, and J.-M. Ahn, Secrecy performance of maximum ratio diversity with channel estimation error, *IEEE Signal Processing Letts.*, vol. 22, no. 11, November 2015: 2167–2171.

[4]. L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, Secure switch-and-stay combining (sssc) for cognitive relay networks, *IEEE Transactions on Communications*, vol. 64, no. 1, January 2016: 70–82

[5]. A. Goldsmith, *Wireless Communication*, 7th ed. New York, NY, USA: Cambridge University Press, 2005.

[6]. I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA: Academic, 2007.