International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), 11-12 July, 2019

Enhancing Wireless Security Over Weibull Fading Multicast Channel

Z. I. Borshon
Department of ETE
RUET, Rajshahi-6204, Bangladesh.
zashidiqbal1554@gmail.com

A. S. M. Nafis
Department of ETE
RUET, Rajshahi-6204, Bangladesh.
abusaleh_nafis@yahoo.com

A. S. M. Badruduzza
Department of ETE
RUET, Rajshahi-6204, Bangladesh.
asmb.kanon@gmail.com

M. K. Kundu
Department of ECE
RUET, Rajshahi-6204, Bangladesh.
mkkeee002@gmail.com

M. Z. I. Sarkar
Department of EEE
RUET, Rajshahi-6204, Bangladesh.
msarkar01@qub.ac.uk

***Abstract*—This paper aims to the study of security in wireless transmission system through Weibull fading single-input multiple-output multicast channels considering multiple receivers and eavesdroppers. At first, the analytical expressions for the probability of non-zero secrecy multicast capacity and the ergodic secrecy multicast capacity are derived in closed-form to illustrate the numerical results. Then the closed-form expression for the secure outage probability is obtained to examine the secure outage behaviour. Finally, a comparison between Weibull and Rayleigh fading channel is presented to demonstrate the impact of Weibull fading parameter on the secrecy performance of the proposed scenario.**

***Index Terms*—secrecy multicast capacity, secure outage probability, secure wireless multicasting, weibull fading.**

I. Introduction

Security in wireless multicasting communication system has become of great momentousness due to the open nature of radio propagation and being approachable by both legitimate receivers and unwanted eavesdroppers. Wireless transmission is more susceptible to malicious incursions which not only includes eavesdropping but also active jamming to obstruct legitimate transmissions. Due to these reasons, researchers are devising different proficient defense mechanisms against security vulnerabilities for improving the wireless network security [1].

In [2], authors considered Weibull fading single-input single-output (SISO) channel where confidential information was transmitted in existence of multiple eavesdroppers. Here authors came up with veritable characterization of maximum transmission rate at which eavesdroppers were incapable to decipher any messages. They also provided the average secrecy capacity (ASC) for multicasting and secure outage probability (SOP) of Weibull fading SISO channel. Authors have considered a multiple-input single-output (MISO) independent but not necessarily identical Weibull fading channel in [3] and derived the exact analytical expressions of effective rate at high and low signal-to-noise ratio (SNR) zones, applicable to the real-time communication system framework. ASC of a wireless network subjected to Weibull fading channel is also investigated in [4] to generalize the analysis on Rayleigh fading. Authors in [5] evaluated an independent and identically distributed (i.i.d) Weibull fading channel to study the characteristics of cooperative diversity in Amplify and Forward relaying with best-relay selection.

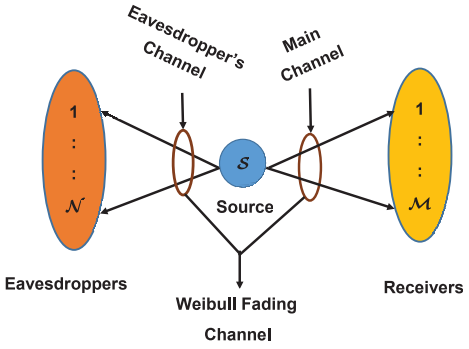

Fig. 1. System model.

In this paper, we consider the Weibull single-input multiple-output (SIMO) multicast channels to obtain the closed-form expressions for the probability of non-zero secrecy multicast capacity (PNSMC),the ergodic secrecy multicast capacity (ESMC) and the secure outage probability (SOP) in the presence of multiple receivers and multiple eavesdroppers.

The rest of the paper is organized as follows. Section II describes our system model and problem formulation. The derivation of the PNSMC, ESMC and SOP is done in section III, IV, and V, respectively. Section VI shows the numerical analysis of the derived expressions. Finally, Section VII draws the conclusion of this work.

II. System Model and Problem Formulation

We consider a system model (Fig. 1),where a single antenna source, $\mathcal{S}$ is dispatching confidential information to a group of $\mathcal{M}$ legal receivers in the presence of $\mathcal{N}$ eavesdroppers. All receivers are outfitted with n_R antennas. The direct channel

978-1-7281-3060-6/19/$31.00

gain between the source and the first receiver is denoted as $\mathbf{h}_1$. So, the direct channel gain between the source and i^{th} receiver is $\mathbf{h}_i$ where, $i = 1, 2, 3.....\mathcal{M}$. This information transmission is espied by a group of eavesdroppers. The secrecy of the communication between the source and the receivers is constrained through the appearance of the eavesdroppers. Each eavesdropper is outfitted with n_E antennas. We've denoted the direct channel coefficient between the source and the first eavesdropper as $\mathbf{g}_1$. So, the direct channel coefficient between the source and j^{th} eavesdropper is $\mathbf{g}_j$ where, $j = 1, 2, 3.....\mathcal{N}$. The channels between the source and the receivers are the main channels and the channels between the source and the eavesdroppers are the eavesdropper channels. Let the transmitted signal is denoted by x. Then the receive signals at the i^{th} receiver and j^{th} eavesdropper are given by

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

$$\mathbf{y}_{e,j} = \mathbf{g}_j x + \mathbf{w}_j, \tag{2}$$

where, the Gaussian noises imposed on the ith receiver and jth eavesdropper are denoted by $\mathbf{z}_i \sim \widetilde{\mathcal{N}}(0, N_M \mathbf{I}_{n_R})$ and $\mathbf{w}_j \sim \widetilde{\mathcal{N}}(0, N_E \mathbf{I}_{n_E})$, respectively. Here, N_M and N_E are the noise power of the receivers and the eavesdroppers and I_p is a $p \times p$ identity matrix. The instantaneous Signal to Noise Ratios (SNRs) of the main channel and the eavesdroppers channel are given by $\gamma_{M_i} = \frac{P_T}{N_M}\|\mathbf{h}_i\|^2$ and $\gamma_{E_j} = \frac{P_T}{N_E}\|\mathbf{g}_j\|^2$, respectively, where P_T is the transmit signal power.

A. The Probability Density Function for SIMO Channel

The Chi-square distribution of SNRs for Weibull fading channel is given by [6, eq. 2.27]

$$f_\alpha(\alpha) = C\left(\frac{\Gamma(1+\frac{2}{C})}{\Omega}\right)^{\frac{C}{2}} \alpha^{C-1} e^{-\left(\frac{\alpha^2\Gamma(1+\frac{2}{C})}{\Omega}\right)}, \tag{3}$$

where, α is the channel fading amplitude, Ω is the average SNR and C is the weibull fading parameter. For i.i.d. Weibull fading SIMO main channel, (3) is expressed as

$$f_\alpha(\alpha) = \frac{Cn_R}{\alpha^{1-Cn_R}}\left(\frac{\Gamma(1+\frac{2}{Cn_R})}{\Omega_M n_R}\right)^{\frac{Cn_R}{2}} e^{-\frac{\alpha^2\Gamma\left(1+\frac{2}{Cn_R}\right)}{\Omega_M n_R}}. \tag{4}$$

Let, $\alpha^2 = \gamma_{M_i}$. Then the probability density function (PDF) of γ_{M_i} is obtained as [7]

$$f(\gamma_{M_i}) = \left.\frac{f_\alpha(\alpha)}{2\alpha}\right|_{\alpha^2=\gamma_{M_i}} \tag{5}$$

By substituting (4) into (5) we get

$$f(\gamma_{M_i}) = \Phi\gamma_{M_i}^{\frac{Cn_R}{2}-1} e^{-\Psi\gamma_{M_i}^{\frac{Cn_R}{2}}}, \tag{6}$$

where, Ω_M is the average SNR of the main channel,

$$\Phi = \frac{1}{2}Cn_R\left[\frac{\Gamma(1+\frac{2}{Cn_R})}{\Omega_M n_R}\right]^{\frac{Cn_R}{2}}$$

and

$$\Psi = \left[\frac{\Gamma(1+\frac{2}{Cn_R})}{\Omega_M n_R}\right]^{\frac{Cn_R}{2}}.$$

Similarly, the PDF of γ_{E_j} is given by

$$f(\gamma_{E_j}) = \Upsilon\gamma_{E_j}^{\frac{Cn_E}{2}-1} e^{-\Lambda\gamma_{E_j}^{\frac{Cn_E}{2}}}, \tag{7}$$

where, Ω_E is the average SNR of the eavesdropper's channel,

$$\Upsilon = \frac{1}{2}Cn_E\left[\frac{\Gamma(1+\frac{2}{Cn_E})}{\Omega_E n_E}\right]^{\frac{Cn_E}{2}}$$

and

$$\Lambda = \left[\frac{\Gamma(1+\frac{2}{Cn_E})}{\Omega_E n_E}\right]^{\frac{Cn_E}{2}}.$$

B. The Cumulative Distribution Function Calculations

The cumulative distribution function (CDF) of γ_{M_i} is given by

$$F(\gamma_{M_i}) = \int_0^{\gamma_{M_i}} f(\gamma_{M_i}) d\gamma_{M_i}. \tag{8}$$

Substituting (6) into (8) and using the identity of [8, eq. 3.381.8]

$$\int_0^s t^u e^{-bt^v} dt = \frac{\gamma(\nu, bs^v)}{vb^\nu},$$

we get,

$$F(\gamma_{M_i}) = 1 - e^{-\Psi\gamma_{M_i}^{\frac{Cn_R}{2}}}, \tag{9}$$

where, $\gamma(.,.)$ is a incomplete gamma function and $\nu = \frac{u+1}{v}$. Similarly the corresponding CDF of γ_{E_j} is expressed as

$$\begin{aligned} F(\gamma_{E_j}) &= \int_0^{\gamma_{E_j}} f(\gamma_{E_j}) d\gamma_{E_j} \\ &= 1 - e^{\Lambda\gamma_{E_j}^{\frac{Cn_E}{2}}}. \end{aligned} \tag{10}$$

C. The PDFs of minimum and maximum SNRs

Denoting $d_{min} = min_{1\le\gamma_{M_i}\le\mathcal{M}}$, the minimum SNR of the main channel and $d_{max} = max_{1\le\gamma_{E_j}\le\mathcal{N}}$, the maximum SNR of eavesdropper's channel, the pdfs of d_{min} and d_{max} is given by

$$f_{d_{min}}(\gamma_{M_i}) = \mathcal{M} f_{\gamma_{M_i}}(\gamma_{M_i})[1 - F_{\gamma_{M_i}}(\gamma_{M_i})]^{\mathcal{M}-1}, \tag{11}$$

$$f_{d_{max}}(\gamma_{E_j}) = \mathcal{N} f_{\gamma_{E_j}}(\gamma_{E_j})[F_{\gamma_{E_j}}(\gamma_{E_j})]^{\mathcal{N}-1}, \tag{12}$$

respectively. Substituting (6) and (9) into (11), we get

$$f_{d_{min}}(\gamma_{M_i}) = \mathcal{M}\Phi\gamma_{M_i}^{\frac{Cn_R}{2}-1} e^{-\mathcal{M}\Psi\gamma_{M_i}^{\frac{Cn_R}{2}}}. \tag{13}$$

Similarly, using the following identity of [8, eq.(1.111)],

$$(z+q)^p = \sum_{w=0}^{p}\binom{p}{w} z^{p-w} q^w,$$

and substituting (7), (10) into (12), we have

$$f_{d_{max}}(\gamma_{E_j}) = \sum_{K=0}^{\mathcal{N}-1} \frac{\binom{\mathcal{N}-1}{K}\mathcal{N}\Upsilon\gamma_{E_j}^{\frac{Cn_E}{2}-1}}{(-1)^{-K}e^{\Lambda(1+K)\gamma_{E_j}^{\frac{Cn_E}{2}}}}. \quad (14)$$

III. Probability of Non-zero Secrecy Multicast Capacity

In the presence of multiple eavesdroppers, the PNSMC is interpreted as,

$$P_r(C_s > 0) = P_r(d_{min} > \gamma_{E_j}) = \int_0^{\infty}\int_0^{\gamma_{M_i}} f_{d_{min}}(\gamma_{M_i}) f_{d_{max}}(\gamma_{E_j}) d\gamma_{E_j} d\gamma_{M_i}, \quad (15)$$

where, $P_r(.)$ denotes the probability operator. Substituting (13) and (14) in (15) and using the identity of [8, eq. 1.211.1]

$$e^w = \sum_{g=0}^{\infty} \frac{w^g}{g!},$$

we get the following closed form expression of PNSMC.

$$P_R(C_s > 0) = 2\mathcal{M}\Phi \sum_{K=0}^{\mathcal{N}-1} \binom{\mathcal{N}-1}{K} \frac{(-1)^K \mathcal{N}\Upsilon}{Cn_E(\Lambda+\Lambda K)} - \frac{2\Theta Cn_E K_1}{Cn_R}(\Psi\mathcal{M})^{(-\frac{Cn_E}{Cn_R}-\frac{2K_1}{Cn_R}-1)}, \quad (16)$$

where,

$$\Theta = 2\mathcal{M}\mathcal{N}\Phi\Upsilon \sum_{K_1=0}^{\infty}\sum_{K=0}^{\mathcal{N}-1} \left(\frac{\binom{\mathcal{N}-1}{K}(-1)_1^{K+K_1}\gamma_{M_i}^{\frac{Cn_R}{2}-1}}{Cn_E K_1!(\Lambda+\Lambda K_1)^{1-K}} \right).$$

IV. Ergodic Secrecy Multicast Capacity

ESMC is defined as the average value of the instantaneous secrecy multicast capacity. It can be expressed as follows.

$$\langle C_s^m \rangle = \mathbb{E}[C_s^m] = \int_0^{\infty} log_e(1+\gamma_{M_i}) f_{d_{min}}(\gamma_{M_i}) d\gamma_{M_i} - \int_0^{\infty} log_e(1+\gamma_{E_j}) f_{d_{max}}(\gamma_{E_j}) d\gamma_{E_j}, \quad (17)$$

where, $\mathbb{E}[.]$ denotes the expectation operator. Substituting the values of (13) and (14) in (17) and using the following identity of [8, eq. 4.293.3]

$$\int_0^{\infty} log_e(1+t)t^{u-1}dt = \frac{\pi}{usin(u\pi)},$$

we get the final closed form analytical expression of ESMC as given below.

$$< C_s^m >= \sum_{K_2=0}^{\infty} \left(\frac{2\mathcal{M}\Phi(-1)^{K_2}(\Psi\mathcal{M})^{K_2}\pi}{\sin[\frac{Cn_R}{2}(K_2+1)\pi]Cn_R(K_2+1)} \right) - \sum_{K_3}^{\infty}\sum_{K=0}^{\mathcal{N}-1} \left(\frac{2\mathcal{N}\Upsilon\binom{\mathcal{N}-1}{K}(-1)^{K+K_3}(\Lambda+\Lambda K)^{K_3}\pi}{K_3! Cn_E(K_3+1)\sin[\frac{Cn_E}{2}(K_3+1)\pi]} \right). \quad (18)$$

V. Secure Outage Probability

The SOP can be defined as the probability of secrecy multicast capacity falling below R_s, where R_s is a target secrecy rate. It can be expressed as,

$$P_O(R_s) = P_r(C_s^m < R_s) = 1 - \int_0^{\infty}\int_D^{\infty} f_{d_{max}}(\gamma_{E_j}) f_{d_{min}}(\gamma_{M_i}) d\gamma_{M_i} d\gamma_{E_j}, \quad (19)$$

where, $D = 2^{R_s}(1+\gamma_{E_j}) - 1$ and $R_s > 0$. Substituting (13) and (14) in (19) and performing integration using the following identity of [8, eq. 3.381.9]

$$\int_s^{\infty} t^u e^{-bt^v} dt = \frac{\Gamma(\nu, bs^v)}{vb^{\nu}},$$

we get the following closed form expression of SOP as given in (20), where $\Gamma(.,.)$ is a incomplete gamma function and $\nu = \frac{u+1}{v}$.

VI. Numerical Results

Fig. 2 depicts the PNSMC as a function of average SNR of the main channel to investigate the effect of receivers antennas, n_R for selected values of $\mathcal{M}$ with $\mathcal{N}$=n_E=2. It is observed that, for a specific number of receivers, PNSMC increases with the receiver's antennas. The PNSMC is also

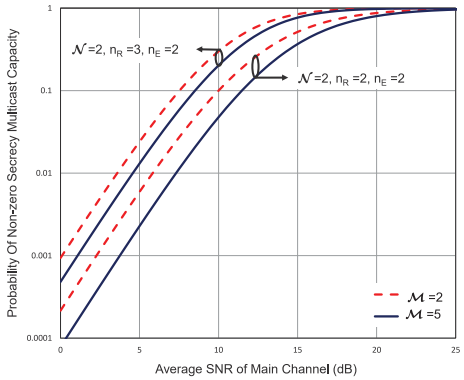

Fig. 2. The PNSMC versus average SNR of main channel.

$$P_O(R_s) = 1 - \sum_{K=0}^{\mathcal{N}-1}\sum_{K_1=0}^{\infty}\sum_{K_2=0}^{\frac{Cn_R K_1}{2}} \frac{\binom{\mathcal{N}-1}{K}(-1)^{K+K_1}\mathcal{N}\Upsilon(\Psi\mathcal{M})^{K_1}\binom{\frac{Cn_R K_1}{2}}{K_2}2^{R_S K_2}(2^{R_S}-1)^{\frac{Cn_R K_1}{2}-K_2}(\frac{K_2}{\Lambda})!}{K_1!\frac{Cn_e}{2}(\Lambda+\Lambda K)^{1+\frac{K_2}{\Lambda}}}. \quad (20)$$

shown as a function of the receivers which shows that the secrecy multicast capacity decreases with the receivers.

The ESMC versus average SNR of the main channel is plotted in Fig. 3 for specific values of $\mathcal{N}$,n_R,n_E to show the effect of n_E on the secrecy performance of the proposed model. The figure shows that for a particular number of $\mathcal{N}$ and n_R the ESMC decreases with the receivers as well as the eavesdropper's antennas.

Fig. 4 illustrates the SOP versus average SNR of main

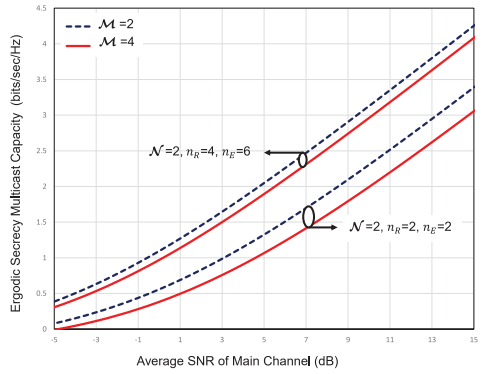

Fig. 3. The ESMC versus average SNR of main channel.

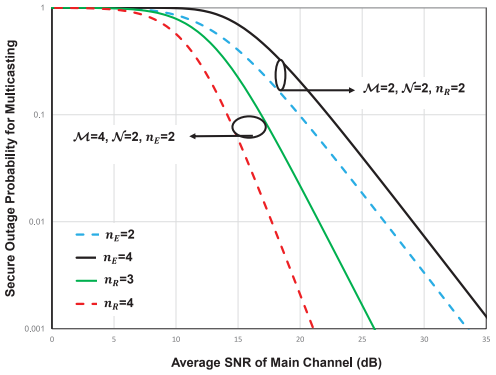

Fig. 4. The SOP versus average SNR of main channel.

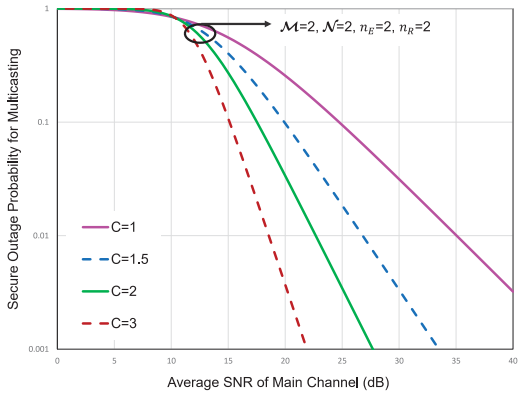

Fig. 5. The SOP versus average SNR of main channel for various fading parameter .

channel to show the effects of n_E and n_R with $\mathcal{M} = \mathcal{N} = 2$ and $\mathcal{M} = 4, \mathcal{N} = 2$. The figure shows that the secure outage performance is degraded with the eavesdropper's antenna and enhanced with the receiver's antenna.

Fig. 5 depicts the SOP as a function of average SNR of main channel to compare among exponential distribution ($C = 1$), Weibull distribution ($C < 2$ and $C > 2$) and Rayleigh distribution ($C = 2$). The figure shows that weibull fading channel is worse than Rayleigh fading for $C < 2$ and better than Rayleigh fading for $C > 2$. It is also observed that secrecy and outage behavior of the system enhances significantly with the Weibull fading parameter, C.

VII. Conclusion

In this paper, a multicasting scenario with multiple eavesdroppers is presented to analyze the secercy and outage feature of the proposed model. Our center of attention is to derive the analytical expressions for the ESMC, the PNSMC and the SOP for multicasting in closed-form. The numerical results indicate that the proposed system performance is deteriorated with the number of receivers and eavesdroppers, but the secrecy capacity is still enhanced for the antenna diversity provided by the multiple antennas at the receivers. The Rayleigh fading channel is shown as a special case of Weibull distribution. On the basis of the comparison between the two channels it can be concluded that the Weibull fading channel may exibit inferior or superior performance than the Rayleigh fading channel depending on the Weibull fading parameter.

References

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] J. Giti and S. Chowdhury, "Secure outage performance analysis of wireless multicasting through weibull fading channel," in *2015 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)*, 19-20 Dec 2015, pp. 199–202.

[3] M. You, H. Sun, J. Jiang, and J. Zhang, "Effective rate analysis in weibull fading channels," *IEEE Commun. Letts.*, vol. 5, no. 4, pp. 340–343, 25 April 2016.

[4] X. Liu, "Average secrecy capacity of the weibull fading channel," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 9-12 Jan 2016, pp. 841–844.

[5] N. Kumar and V. Bhatia, "Analysis of symbol error rate for amplify-and-forward networks with best-relay selection over weibull fading channels," in *2015 International Conference on Signal Processing and Communication (ICSC)*, 16-18 March 2015, pp. 111–115.

[6] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. Hoboken, New Jersey: Wiley-IEEE Press, 2004.

[7] A. M. Magableh and M. M. Matalgah, "Capacity of simo systems over non-identically independent nakagami-m channels," in *2007 IEEE Sarnoff Symposium*, 16 July 2007, pp. 1–5.

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