Scientific Research Publishing

Journal of Computer and Communications, 2023, 11, 177-193
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Secure Wireless Multicasting through Nakagami-*m* Fading Channels with Multi-Hop Relaying

Md. Mizanur Rahman, Md. Zahurul Islam Sarkar, Mohammad Mahmud Hasan

Department of Electrical and Electronic Engineering, RUET, Rajshahi, Bangladesh
Email: mizan.eee07@gmail.com, islam89118@gmail.com, mmh_mahmudhasan@yahoo.com

How to cite this paper: Rahman, M.M., Sarkar, M.Z.I. and Hasan, M.M. (2023) Secure Wireless Multicasting through Nakagami-*m* Fading Channels with Multi-Hop Relaying. *Journal of Computer and Communications*, **11**, 177-193.
https://doi.org/10.4236/jcc.2023.115013

Received: April 6, 2023
Accepted: May 28, 2023
Published: May 31, 2023

Abstract

The additional diversity gain provided by the relays improves the secrecy capacity of communications system significantly. The multiple hops in the relaying system is an important technique to improve this diversity gain. The development of an analytical mathematical model of ensuring security in multicasting through fading channels incorporating this benefit of multi-hop relaying is still an open problem. Motivated by this issue, this paper considers a secure wireless multicasting scenario employing multi-hop relaying technique over frequency selective Nakagami-*m* fading channel and develops an analytical mathematical model to ensure the security against multiple eavesdroppers. This mathematical model has been developed based on the closed-form analytical expressions of the probability of non-zero secrecy multicast capacity (PNSMC) and the secure outage probability for multicasting (SOPM) to ensure the security in the presence of multiple eavesdroppers. Moreover, the effects of the fading parameter of multicast channel, the number of hops and eavesdropper are investigated. The results show that the security in multicasting through Nakagami-*m* fading channel with multi-hop relaying system is more sensitive to the number of hops and eavesdroppers. The fading of multicast channel helps to improve the secrecy multicast capacity and is not the enemy of security in multicasting.

Keywords

Frequency Selective Fading, Multi-Hop Relaying, Probability of Non-Zero Secrecy Multicast Capacity, Secure Outage Probability for Multicasting

1. Introduction

The multi-hop technique enhances the system performance significantly over

Nakagami-*m* Fading channel [1]. On the other hand, multicasting is an efficient wireless communication technique for group-oriented and personal communication such as video-conferencing, e-learning etc. Due to the increase of application areas and the mobility of users with network components, the security is a crucial aspect in wireless multicasting systems because of the fact that the medium of wireless multicasting is open and susceptible to eavesdropping and fraud.

1.1. Related Works

Recently, Srinivas *et al.* [2] studied multicast capacity of wireless ad-hoc networks over Nakagami-*m* fading channel. In [3], G. C. Alexandropoulos *et al.* analyzed decode-and-forward dual-hop networks over Nakagami-*m* fading channel and showed that the relaying is always beneficial for system performance. Chun.*et al.* [4], studied the multicast transmission capacity (MTC) and multicast outage probability of multi-hop wireless network and showed that an appropriate number of retransmission can significantly enhances the MTC. In [5], Y. Zou *et al.* studied the relay selection for improving physical layer security in cooperative wireless network. Nguyen *et al.* [6], analyzed the performance of wireless energy harvest cluster based multi-hop networks. The technique of enhancing security using partial relay selection strategy was studied in [7]. In [8], authors studied multicasting through multicellular networks and showed how the loss of security due to the effects of interference power can be compensated using the opportunistic relaying technique. The diversity order provided by the asymmetric cooperative relays was used in [9] to enhance the security of multicast networks. In [10], A. S. M. Badrudduza *et al.* studied the effects of correlation on the security in multicasting and showed how the effects of correlated can be compensated by using the opportunistic relaying technique. In [11], D. K. Sarkar *et al.* developed a mathematical model to enhance the security of wireless multicasting using the additional diversity provided by the best relay among a number of amplify-and-forward cooperative relays. A. P. Shrestha *et al.* [12] developed a mathematical model for the physical layer security of cooperative multi-hop routing wireless network. Toan *et al.* [13] studied the end-to-end performance of multi-hop wireless-powered relaying networks cognitively operating with primary networks over Nakagami-*m* fading channels. In [14], A. K. Kamboj *et al.* developed the machine learning algorithms for relay selection to improve the physical layer security of a dual-hop non-regenerative wireless cooperative network.

However, to the best of authors knowledge, the aforementioned works did not develop an analytical mathematical model to ensure the security in multicasting considering the diversity order provided by the multi-hop relaying technique. This research gap is fulfilled in this paper considering a multicasting scenario through Nakagami-*m* fading channel with multi-hop relaying technique.

1.2. Contributions

Based on the aforementioned scenario available in the literature and motivated

by the benefits of multi-hop technique. This paper considers a secure wireless multicasting scenario over frequency selective Nakagami-m fading channel and develops an analytical mathematical model to ensure the security of the proposed model incorporating the benefits of the multi-hop relaying technique. The major contributions of this paper can be summarized as follows.

- At first, based on the probability density function (PDF) of multi-hop relaying technique over frequency selective Nakagami-m fading channels, the expressions for the PDFs of the minimum signal-to-noise ratio (SNR) of multicast channels and the maximum SNR of eavesdropper's channels, and denote them by $f_{d_{\min}}\left(\gamma_{M_{n_1}}\right)$ and $f_{d_{\max}}\left(\gamma_{E_{n_2}}\right)$, respectively are derived.
- Secondly, using the analytical expressions of $f_{d_{\min}}\left(\gamma_{M_{n_1}}\right)$ and $f_{d_{\max}}\left(\gamma_{E_{n_2}}\right)$, the closed-form analytical expressions for the PNSMC and the SOPM are derived.
- Finally, the effects of the fading parameter of multicast channel, the SNR of eavesdropper's channel, and the number of hops and eavesdroppers on the the PNSMC and SOPM have been investigated. Also the concept of enhancing the level of security of the proposed model minimizing the loss of security due to the effects of eavesdroppers and the SNR of eavesdropper's channel has been explained in this work.

The remainder of this paper is organized as follows. Sections II and III describe the system model and problem formulation, respectively. The expressions for the PNSMC and the SOPM are derived, respectively in Section IV and V. Numerical results are presented in Section VI. Finally, Section VII draws the conclusions of this work.

2. System Model

A secure wireless multicasting scenario as shown in **Figure 1** is considered through multi-hop Nakagami-m fading channel in the presence of P eavesdroppers. A transmitter equipped with n_t antennas sends a common stream of information to the M multicast users and P eavesdroppers observe the communication between transmitter and multicast users. The key objective of this research is to protect this information from eavesdropping. Each multicast user and eavesdropper are equipped with n_r and n_e antennas, respectively. The channel between transmitter and multicast user is known as multicast channel and the channel between transmitter and eavesdropper is known as eavesdropper's channel. Both the multicast and eavesdropper's channels are assumed to be Nakagami-m fading channels. m_1 is the fading parameter of the each multicast channel and m_2 is the fading parameter of each eavesdropper's channel. $\overline{\gamma}_{n_1}$ and $\overline{\gamma}_{n_2}$ are the average SNR of the multicast channels and eavesdropper's channel respectively. There are N hops between transmitter and multicast users.

3. Problem Formulation

In this section, this paper explores the PDFs of the multicast channels and eavesdropper's channels from the PDFs of their sub-channels.

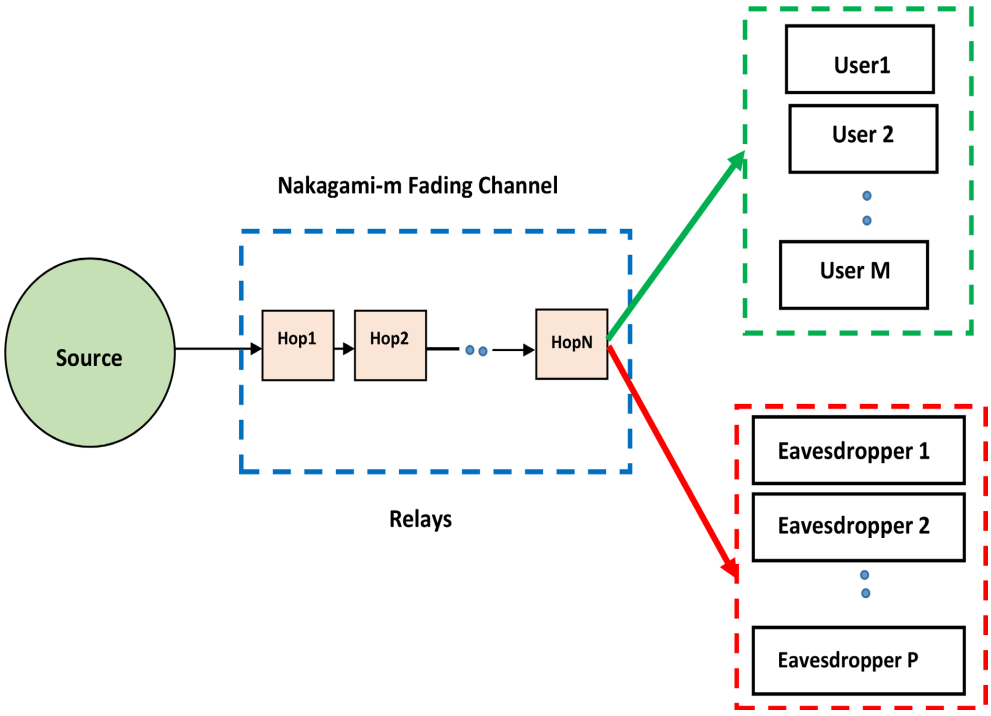

Figure 1. System model.

Let γ_i denotes the SNR of ith hop of multi-hop Nakagami-m fading channel. Then, the PDF of γ_i, denoted by $f_{\gamma_i}(\gamma_i)$ is given by [1]:

$$f_{\gamma_i}(\gamma_i) = \frac{(m_i)^{m_i}\,\gamma_i^{m_i-1}\mathrm{e}^{-\frac{m_i\gamma_i}{\bar{\gamma}_i}}}{(\bar{\gamma}_i)^{m_i}\,\Gamma(m_i)}, \tag{1}$$

where m_i Nakagami-m fading parameter of ith hop and $i=1,\cdots,N$. Let γ_{end} denotes the end-to-end SNR *i.e.* SNR at the destination user, then $\gamma_{end} = \sum_{i=1}^{N}\gamma_i$.

3.1. PDF and CDF of Each Sub-Channel of Multicast Channels

Let $\gamma_{M_{n_1}}$ denotes the SNR of n_1th multicast channel. Then, following equation (i), the PDF of $\gamma_{M_{n_1}}$ over multi-hop Nakagami-m fading channel is given by [15]

$$f_{\gamma_{M_{n_1}}}(\gamma_{M_{n_1}}) = \frac{(m_{n_1})^{m_{n_1}}\,\gamma_{M_{n_1}}^{m_{n_1}-1}\mathrm{e}^{-\frac{m_{n_1}\gamma_{M_{n_1}}}{\bar{\gamma}_{n_1}}}}{(\bar{\gamma}_{n_1})^{m_{n_1}}\,\Gamma(m_{n_1})} = A_1\gamma_{M_{n_1}}^{m_{n_1}-1}\mathrm{e}^{-B_1\gamma_{M_{n_1}}}, \tag{2}$$

where $A_1 = \frac{(m_{n_1})^{m_{n_1}}}{(\bar{\gamma}_{n_1})^{m_{n_1}}\,\Gamma(m_{n_1})}$, $B_1 = \frac{m_{n_1}}{\bar{\gamma}_{n_1}}$ and $n_1 = 1,\cdots,M$. The CDF of n_1th multicast channel denoted by $F_{\gamma_{M_{n_1}}}(\gamma_{M_{n_1}})$ is defined as [15]

$$F_{\gamma_{M_{n_1}}}(\gamma_{M_{n_1}}) = \int_0^{\gamma_{M_{n_1}}} f_{\gamma_{M_{n_1}}}(\gamma_{M_{n_1}})\mathrm{d}\gamma_{M_{n_1}}. \tag{3}$$

Substituting the value of $f_{\gamma_{M_{n_1}}}(\gamma_{M_{n_1}})$ from Equation (2) and performing integration by using identity 3.381(8) of [16]

$$\int_0^u x^m \mathrm{e}^{-\beta x^n} \mathrm{d}x = \frac{\gamma\left(v, \beta u^n\right)}{n\beta^v}$$

and identity 8.354(1) of [16]

$$\gamma\left(x,\alpha\right) = \sum_{n=0}^{\infty} \frac{-1^n x^{\alpha+n}}{n!\left(\alpha+n\right)}$$

it can be found,

$$F_{\gamma_{M_{n_1}}}\left(\gamma_{M_{n_1}}\right) = A_1 A_3 \gamma_{M_i}^{m_{n_1}}, \tag{4}$$

where $A_3 = \sum_{q_1=0}^{\infty} \frac{(-1)^{q_1} B_1^{q_1}}{q_1!\left(m_{n_1}+q_1\right)}$.

3.2. PDF and CDF of Each Sub-Channel of Eavesdropper's Channels

Let $\gamma_{E_{n_2}}$ denotes the SNR of n_2th eavesdropper's channel. Then, the PDF of $\gamma_{E_{n_2}}$ over multi-hop Nakagami-m fading channel is given by [15]

$$f_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right) = \frac{\left(m_{n_2}\right)^{m_{n_2}} \gamma_{E_{n_2}}^{m_{n_2}-1} \mathrm{e}^{-\frac{m_{n_2}\gamma_{E_{n_2}}}{\bar{\gamma}_{n_2}}}}{\left(\bar{\gamma}_{n_2}\right)^{m_{n_2}} \Gamma\left(m_{n_2}\right)} = A_2 \gamma_{E_{n_2}}^{m_{n_2}-1} \mathrm{e}^{-B_2\gamma_{E_{n_2}}}, \tag{5}$$

where $A_2 = \frac{\left(m_{n_2}\right)^{m_{n_2}}}{\left(\bar{\gamma}_{n_2}\right)^{m_{n_2}} \Gamma\left(m_{n_2}\right)}$, $B_2 = \frac{m_{n_2}}{\bar{\gamma}_{n_2}}$ and $n_2 = 1, \cdots, P$. The CDF of n_2th eavesdropper's channel denoted by $F_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right)$ is defined as [15]

$$F_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right) = \int_0^{\gamma_{E_{n_2}}} f_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right) \mathrm{d}\gamma_{E_{n_2}}. \tag{6}$$

Substituting the value of $f_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right)$ from Equation (5) and performing integration,using identity 3.381(8) and 8.354(1) of [16] it can be found

$$F_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right) = A_2 \gamma_{E_{n_2}}^{m_{n_2}} \sum_{q_2=0}^{\infty} \frac{(-1)^{q_2} B_2^{q_2} \gamma_{E_{n_2}}^{q_2}}{q_2!\left(m_{n_2}+q_2\right)} \tag{7}$$

3.3. PDF of Minimum SNR of Multicast Channels

Let $d_{\min} = \min_{1\le n_1 \le M} \gamma_{M_{n_1}}$. Then, the PDF of $d_{\min}$ denoted by $f_{d_{\min}}\left(\gamma_{M_{n_1}}\right)$ can be defined as [15]

$$f_{d_{\min}}\left(\gamma_{M_{n_1}}\right) = M f_{\gamma_{M_{n_1}}}\left(\gamma_{M_{n_1}}\right) \times \left\{1 - F_{\gamma_{M_{n_1}}}\left(\gamma_{M_{n_1}}\right)\right\}^{M-1} \tag{8}$$

Substituting the values of $f_{\gamma_{M_{n_1}}}\left(\gamma_{M_{n_1}}\right)$ and $F_{\gamma_{M_{n_1}}}\left(\gamma_{M_{n_1}}\right)$ from Equations (2) and (4), respectively and performing integration and simplifying by the use of identity 1.110 of [16] it is found

$$\begin{aligned} f_{d_{\min}}\left(\gamma_{M_{n_1}}\right) = {} & M A_1 \gamma_{M_i}^{m_{n_1}-1} \mathrm{e}^{-B_1\gamma_{M_i}} - (M-1) M A_3 \\ & \times \left[\frac{A_1^2 \gamma_{M_i}^{v_1-1}}{\mathrm{e}^{B_1\gamma_{M_i}}} - \frac{(M-2) M A_1^3 A_3 \gamma_{M_i}^{v_2-1}}{2} \right], \end{aligned} \tag{9}$$

where $v_1 = 2m_{n_1} + q_1$ and $v_2 = 3m_{n_1} + 2q_1$.

3.4. PDF of Maximum SNR of Eavesdropper's Channels

Let $d_{\max} = \max_{1\le n_2 \le P} \gamma_{E_{n_2}}$. Then, the PDF of $d_{\max}$ denoted by $f_{d_{\max}}\left(\gamma_{E_{n_2}}\right)$ can be defined as [15]

$$f_{d_{\max}}\left(\gamma_{E_{n_2}}\right) = P f_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right)\left\{F_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right)\right\}^{P-1} \tag{10}$$

Substituting the values of $f_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right)$ and $F_{\gamma_{E_{n_2}}}\left(\gamma_{E_{n_2}}\right)$ from equations (5) and (7), respectively and performing integration and simplifying by the use of identity 0.314 of [16] it can be found

$$f_{d_{\max}}\left(\gamma_{E_{n_2}}\right) = C_0 P A_2 A_4 \gamma_{E_{n_2}}^{Pm_{n_2}-1} \mathrm{e}^{-B_2\gamma_{E_{n_2}}} + C_1 P A_2 A_4 \gamma_{E_{n_2}}^{m_{n_2}+v_3-1} \mathrm{e}^{-B_2\gamma_{E_{n_2}}}, \tag{11}$$

where $v_3 = Pm_{n_2} - m_{n_2} + 1$, $A_4 = \left(A_2\right)^{P-1}$, $C_0 = \left(\dfrac{1}{m_{n_2}}\right)^{P-1}$ and

$C_1 = \left(m_{n_2}\right)^{2-P}\left(P-1\right)\left(\dfrac{-B_2}{m_{n_2}+1}\right)$.

4. Probability of Non-Zero Secrecy Multicast Capacity

The probability of non-zero secrecy multicast capacity denoted by $Pr\left(C_{smcast} > 0\right)$ can be defined as [17]

$$Pr\left(C_{smcast} > 0\right) = \int_0^\infty f_{d_{\min}}\left(\gamma_{M_{n_1}}\right) \times \left\{\int_0^{\gamma_{M_{n_1}}} f_{d_{\max}}\left(\gamma_{E_{n_2}}\right) \mathrm{d}\gamma_{E_{n_2}}\right\} \mathrm{d}\gamma_{M_{n_1}} \tag{12}$$

Substituting the values of $f_{d_{\min}}\left(\gamma_{M_{n_1}}\right)$ and $f_{d_{\max}}\left(\gamma_{E_{n_2}}\right)$ in Equation (12) and performing integration, the closed-form analytical expression for the $Pr\left(C_{smcast} > 0\right)$ is given in,

$$\begin{aligned} Pr\left(C_{smcast} > 0\right) = MPA_1A_2A_4 \Bigg[& \left\{\frac{C_0A_5\Gamma w_1}{B_1^{w_1}} + \frac{C_1A_6\Gamma w_2}{B_1^{w_2}}\right\} \\ & -\left(M-1\right)A_1A_3\left\{\frac{C_0A_5\Gamma w_3}{B_1^{w_3}} + \frac{C_1A_6\Gamma w_4}{B_1^{w_4}}\right\} \\ & -\frac{1}{2}\left(M-1\right)\left(M-2\right)A_1^2A_3^2\left\{\frac{C_0A_5\Gamma w_5}{B_1^{w_5}} + \frac{C_1A_6\Gamma w_6}{B_1^{w_6}}\right\}\Bigg] \end{aligned} \tag{13}$$

where $A_5 = \sum_{q_3=0}^{\infty} \dfrac{(-1)^{q_3} B_2^{q_3}}{q_3!\left(pm_{n_2}+q_3\right)}$, $A_6 = \sum_{q_4=0}^{\infty} \dfrac{(-1)^{q_4} B_2^{q_4}}{q_4!\left(m_{n_2}+v_3+q_4\right)}$,

$w_1 = m_{n_1} + pm_{n_2} + q_3$, $w_2 = m_{n_1} + pm_{n_2} + 1 + q_4$, $w_3 = 2m_{n_1} + pm_{n_2} + q_1 + q_3$,

$w_4 = 2m_{n_1} + pm_{n_2} + q_1 + q_4 + 1$ $w_5 = 3m_{n_1} + pm_{n_2} + 2q_1 + q_3$ and

$w_6 = 3m_{n_1} + pm_{n_2} + 2q_1 + q_4$.

5. Secure Outage Probability for Multicasting

The secure outage probability for multicasting denoted by $P_{out}\left(R_{smcast}\right)$ can be defined as [18]

$$P_{out}\left(R_{smcast}\right)=1-\int_0^{\infty} f_{d_{\max}}\left(\gamma_{E_{n_2}}\right)\times\left\{\int_x^{\infty} f_{d_{\min}}\left(\gamma_{M_{n_1}}\right)\mathrm{d}\gamma_{M_{n_1}}\right\}\mathrm{d}\gamma_{E_{n_2}}, \tag{14}$$

where $x=\mathrm{e}^{2R_{smcast}}\left(1+\gamma_{n_2}\right)-1$ and R_{smcast} denotes the target secrecy multicast rate. Substituting the values of $f_{d_{\min}}\left(\gamma_{M_{n_1}}\right)$ and $f_{d_{\max}}\left(\gamma_{E_{n_2}}\right)$ in Equation (14) and performing integration, the closed-form analytical expression for the $P_{out}\left(R_{smcast}\right)$ is given in,

$$\begin{aligned}P_{out}\left(R_{smcast}\right)=1-MPA_1A_2A_4A_13\Bigg[C_0\Bigg\{&\frac{A_7A_{10}\Gamma u_1}{B_4^{u_1}}-\frac{(M-1)A_1A_3A_8A_{11}\Gamma u_2}{B_4^{u_2}}\\&+\frac{(M-2)(M-1)}{2}\frac{A_1^2A_3^2A_9A_{12}\Gamma u_3}{B_4^{u_3}}\Bigg\}+C_1\Bigg\{A_7A_{10}\frac{\Gamma u_4}{B_4^{u_4}}\\&-(M-1)A_1A_3A_8A_{11}\frac{\Gamma u_5}{B_4^{u_5}}+\frac{(M-2)(M-1)}{2}\times\frac{A_1^2A_3^2A_9A_{12}\Gamma u_6}{B_4^{u_6}}\Bigg\}\Bigg]\end{aligned} \tag{15}$$

where $A_7=\dfrac{\Gamma m_{n_1}}{B_1^{m_{n_1}}}\sum_{q_5=0}^{m_{n_1}-1}\dfrac{B_1^{q_5}}{q_5!}$, $A_8=\dfrac{\Gamma v_1}{B_1^{v_1}}\sum_{q_6=0}^{v_1-1}\dfrac{B_1^{q_6}}{q_6!}$, $A_9=\dfrac{\Gamma v_2}{B_1^{v_2}}\sum_{q_7=0}^{v_2-1}\dfrac{B_1^{q_7}}{q_7!}$,

$$A_{10}=\sum_{k_1=0}^{q_5}\frac{\dfrac{q_5!}{k_1!(q_5-k_1)!}}{\left(\mathrm{e}^{2R_s}-1\right)^{k_1}\left(\mathrm{e}^{2R_s}\right)^{-q_5+k_1}},\quad B_4=B_2+B_3,$$

$$A_{11}=\sum_{k_2=0}^{q_6}\frac{\dfrac{q_6!}{k_2!(q_6-k_2)!}\left(\mathrm{e}^{2R_s}-1\right)^{k_2}}{\left(\mathrm{e}^{2R_s}\right)^{-q_6+k_2}},\quad B_3=B_1\mathrm{e}^{2R_s},$$

$$A_{12}=\sum_{k_3=0}^{q_7}\frac{\dfrac{q_7!}{k_3!(q_7-k_3)!}\left(\mathrm{e}^{2R_s}-1\right)^{k_3}}{\left(\mathrm{e}^{2R_s}\right)^{-q_7+k_3}},\quad A_{13}=\mathrm{e}^{-B_1}\left(\mathrm{e}^{2R_s}-1\right),\quad u_1=pm_{n_2}+q_5-k_1,$$

$u_2=pm_{n_2}+q_6-k_2$, $u_3=pm_{n_2}+q_7-k_3$, $u_4=pm_{n_2}+2m_{n_2}+q_5-k_1+1$,

$u_5=pm_{n_2}+2m_{n_2}+q_6-k_2+1$ and $u_6=pm_{n_2}+2m_{n_2}+q_7-k_3+1$.

6. Numerical Results

In this section, some analytical results are shown from the closed-form analytical expressions of the PNSMC and the SOPM. The analytical results are verified via Monte-Carlo simulation. In order to generate the simulation results, at first, the Nakagami-*m* fading channel is modeled using MATLAB code. Then, by using this channel, PNSMC and the SOPM are calculated considering multi-hop relaying from transmitter to receivers and eavesdroppers. More than 110,000 realizations for the PNSMC and the SOPM are taken and averaged to find the final simulation results of PNSMC and the SOPM.

The PNSMC, $Pr\left(C_{smcast}>0\right)$ is shown in **Figure 2** as a function of the average SNR of the multicast channel, $\bar{\gamma}_{n_1}$, for selected values of *P*. This figure describes the effects of *P* on the $Pr\left(C_{smcast}>0\right)$ for selected values of system parameters. It is observed that the $Pr\left(C_{smcast}>0\right)$ decreases with *P*. This is because, the probability of eavesdropping increasing with *P* which causes a reduction

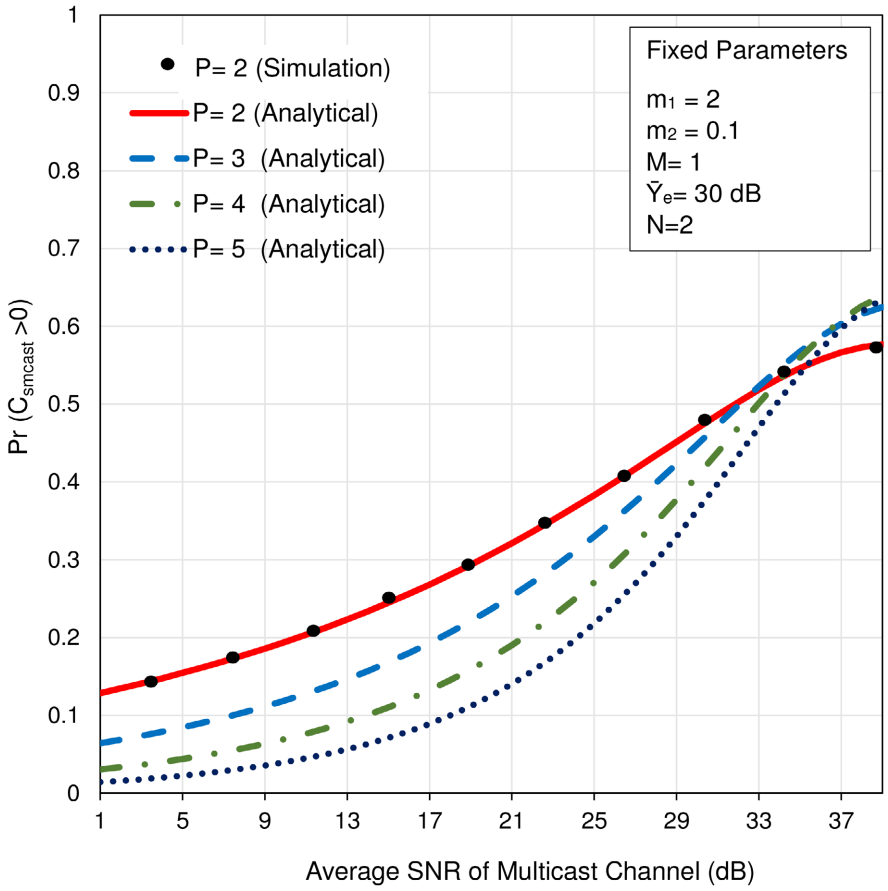

Figure 2. The effects of the number of eavesdropper, P, on the $Pr\left(C_{smcast}>0\right)$ with $m_{n_1}=m_1=2$, $m_{n_2}=m_2=0.1$, $M=1$, $\overline{\gamma}_{n_2}=\overline{\gamma}_e=30$ dB and $N=2$.

in the secrecy multicast capacity.

Figure 3 shows the $Pr\left(C_{smcast}>0\right)$ as a function of $\overline{\gamma}_{n_1}$, for selected values of m_{n_1} with the system parameters mentioned on the figure. It is observed that $Pr\left(C_{smcast}>0\right)$ increases with m_1. Because, fading in the multicast channels create a protection against eavesdropping which causes an improvement in the secrecy capacity.

The $Pr\left(C_{smcast}>0\right)$ is shown in **Figure 4** as a function of $\overline{\gamma}_{n_1}$ for selected values of the number of hops, N. This figure describes the effects of N on the $Pr\left(C_{smcast}>0\right)$ for selected values of system parameters. It is found that the $Pr\left(C_{smcast}>0\right)$ increases with N. This is because, the cooperative diversity provided by the relays increases with N which causes an improvement in the secrecy capacity. **Figure 5** shows the effects of N on the $Pr\left(C_{smcast}>0\right)$ for different values of m_{n_1} (denoted by m_1). It is observed that the $Pr\left(C_{smcast}>0\right)$ increases when the value of m_1 increases from 2 to 4 with $N=2$. But the $Pr\left(C_{smcast}>0\right)$ increases with keeping the value of $m_1=2$, as one expects.

The $Pr\left(C_{smcast}>0\right)$ is shown in **Figure 6** as a function of $\overline{\gamma}_{n_1}$ for selected values of N and P. This figure describes the effects of N for different values of P on the $Pr\left(C_{smcast}>0\right)$. It is observed that, at $N=2$, $Pr\left(C_{smcast}>0\right)$ decreases

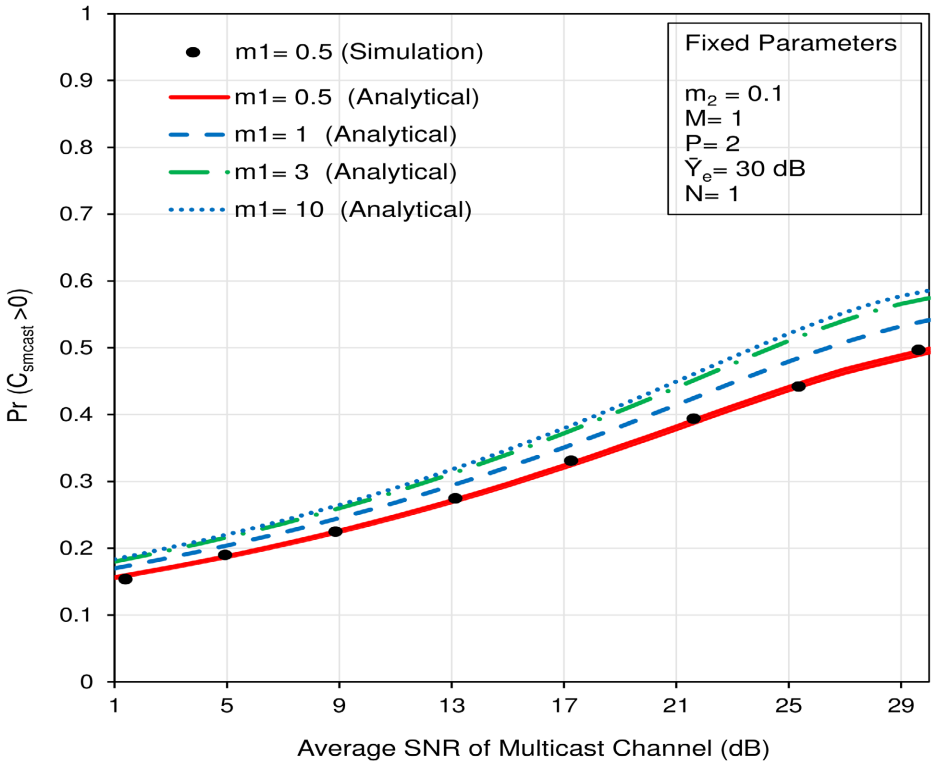

Figure 3. The effects of fading parameter of multicast channel, m_{n_1} (denoted by m_1), on the $Pr\left(C_{smcast}>0\right)$ for $m_{n_2}=m_2=0.1$, $M=1$, $P=2$, $\overline{\gamma}_{n_2}=\overline{\gamma}_e=20\,\text{dB}$ and $N=1$.

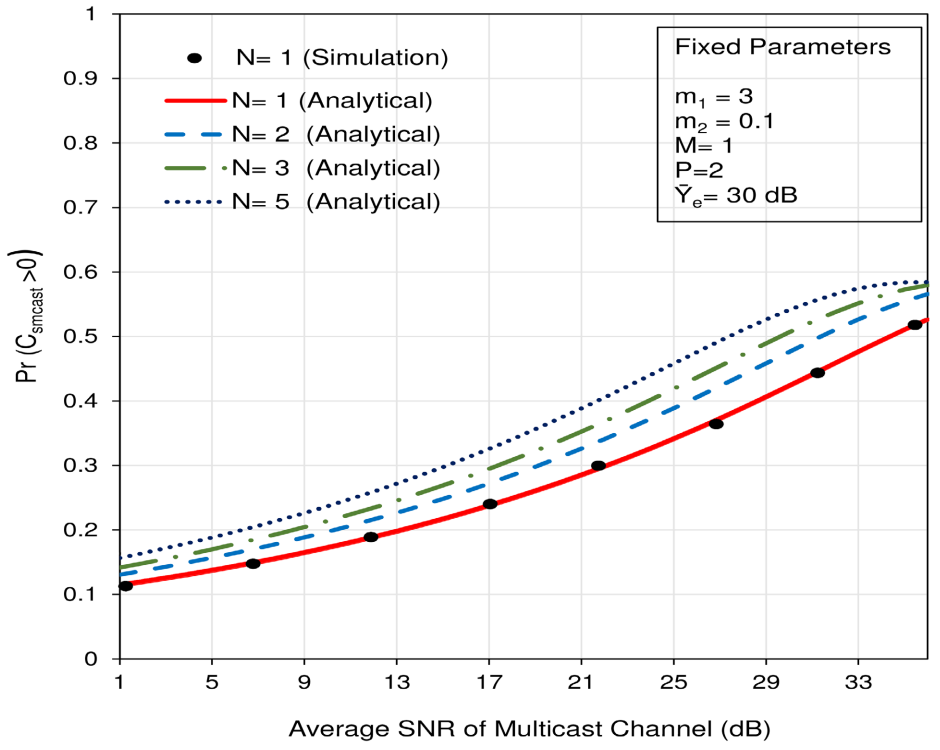

Figure 4. The effects of the number of hop, N, on the $Pr\left(C_{smcast}>0\right)$ for $m_{n_1}=m_1=3$, $m_{n_2}=m_2=0.1$, $M=1$, $P=2$ and $\overline{\gamma}_{n_2}=\overline{\gamma}_e=30\,\text{dB}$.

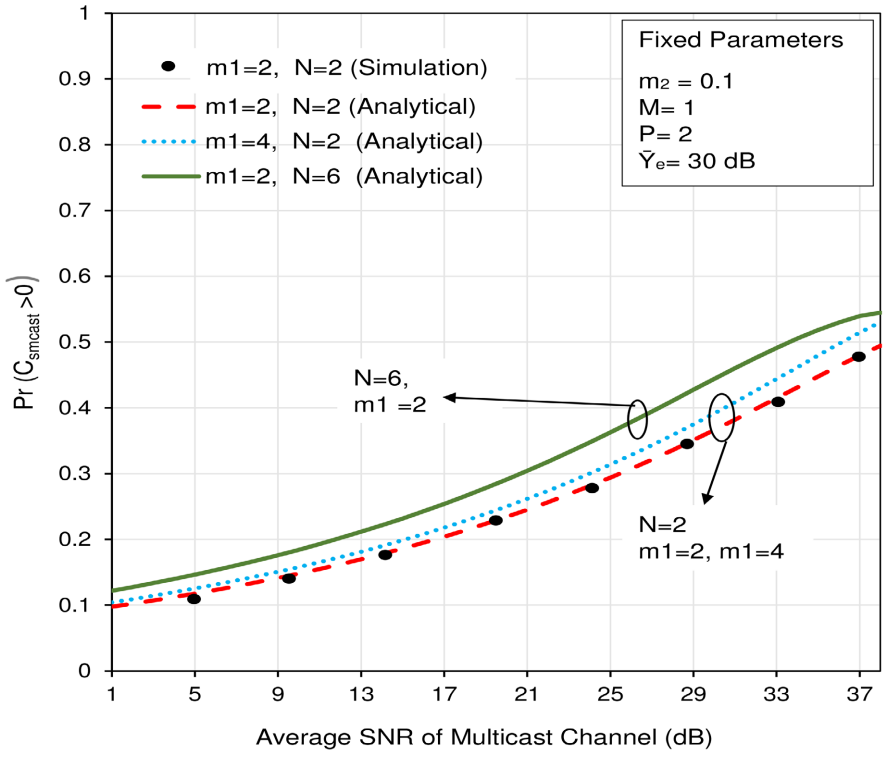

Figure 5. The effects of number of hop, N, for selected values of m_{n_1} (denoted as m_1) on the $Pr\left(C_{smcast}>0\right)$ with $m_{n_2}=m_2=0.1$, $M=1$, $P=2$ and $\overline{\gamma}_{n_2}=\overline{\gamma}_e=30\,\text{dB}$.

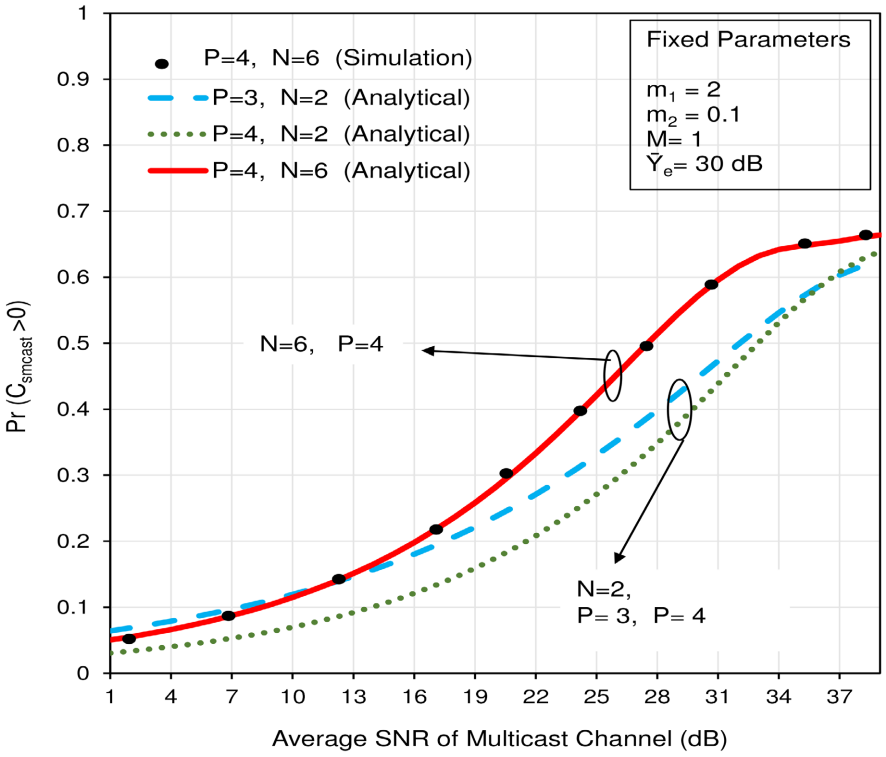

Figure 6. The effects of number of hop, N, for selected values of P on the $Pr\left(C_{smcast}>0\right)$ with $m_{n_1}=m_1=2$, $m_{n_2}=m_2=0.1$, $M=1$ and $\overline{\gamma}_{n_2}=\overline{\gamma}_e=30\,\text{dB}$.

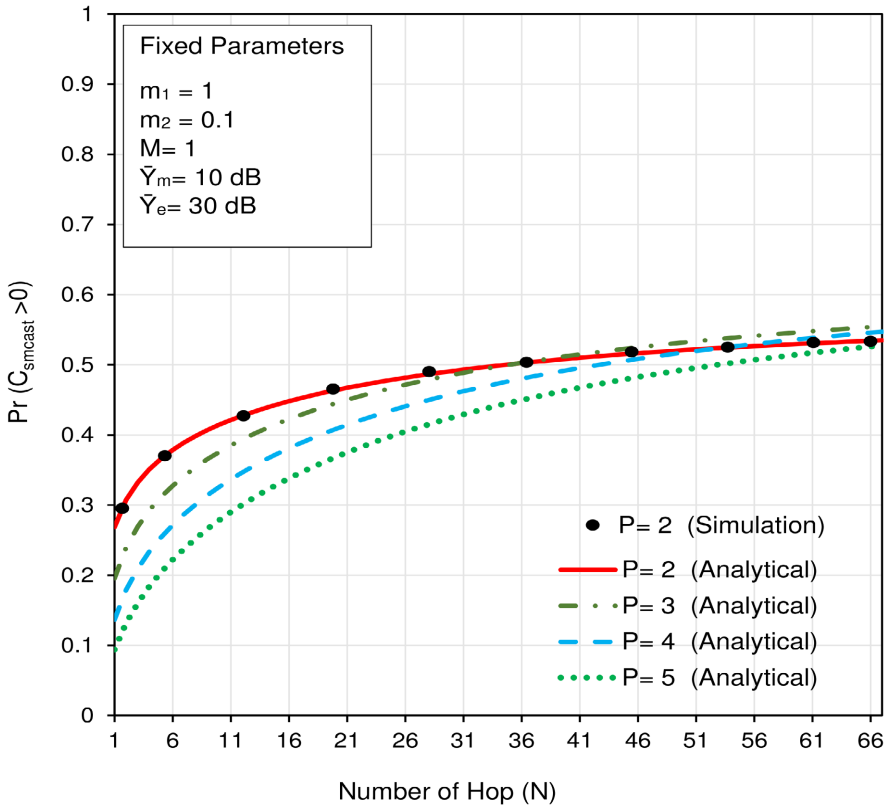

Figure 7. The effects of the number of eavesdropper, P, on the $Pr\left(C_{smcast}>0\right)$ as a function of N when $m_{n_1}=m_1=1$, $m_{n_2}=m_2=0.1$, $M=1$, $\overline{\gamma}_{n_1}=\overline{\gamma}_m=10$ dB and $\overline{\gamma}_{n_2}=\overline{\gamma}_e=20$ dB.

with P. But this reduction of $Pr\left(C_{smcast}>0\right)$ can be compensated by increasing the value of N.

Figure 7 shows the $Pr\left(C_{smcast}>0\right)$ as a function of N for selected values of P. This figure describes the effects of P on the $Pr\left(C_{smcast}>0\right)$ for selected values of system parameters. It is observed that the $Pr\left(C_{smcast}>0\right)$ decreases with P. This is because, the probability of eavesdropping increases with P and causes a reduction in the secrecy capacity.

The $Pr\left(C_{smcast}>0\right)$ is shown in **Figure 8** as a function of N, for selected values of fading parameter of multicast channel, m_{n_1} (denoted by m_1 on the figure). This figure describes the effects of m_1 on the $Pr\left(C_{smcast}>0\right)$ for selected values of system parameters. Clearly it is found that $Pr\left(C_{smcast}>0\right)$ increases with N and m_1. But the effects of both N and m_1 decreases at the higher values of N and m_1.

The secure outage probability for multicasting denoted by $P_{out}\left(R_{smcast}\right)$ shown in **Figure 9** as a function of $\overline{\gamma}_{n_1}$ for selected values of P. It is observed that the $P_{out}\left(R_{smcast}\right)$ increases with P which causes the reduction in the secrecy multicast capacity.

Figure 10 shows the $P_{out}\left(R_{smcast}\right)$ as a function of $\overline{\gamma}_{n_1}$ for selected values of number of hop N. it is found that the $P_{out}\left(R_{smcast}\right)$ decreases with N. This is

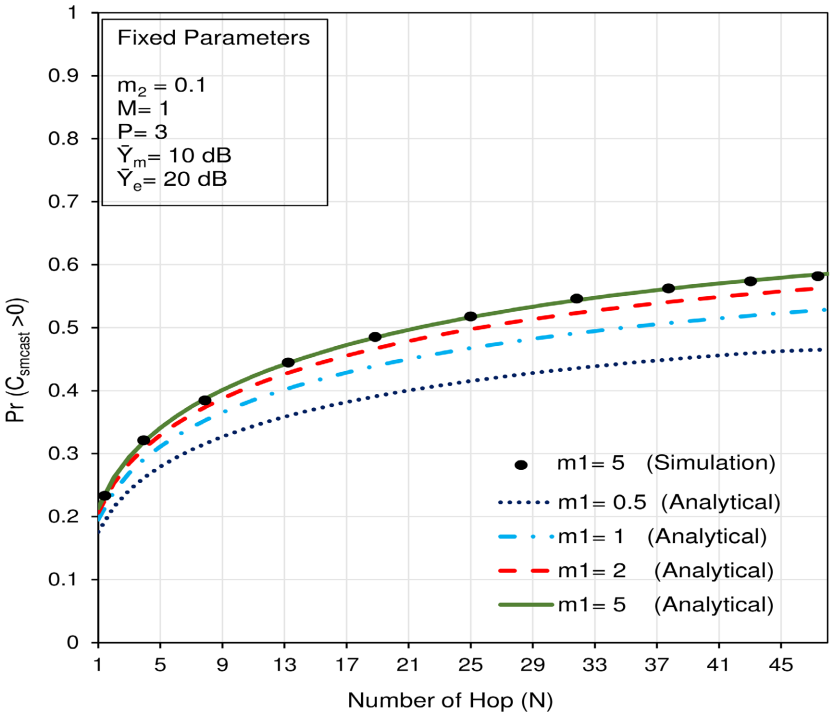

Figure 8. The effects of fading parameter of multicast channel, m_{n_1} (denoted as m_1), on the $Pr\left(C_{smcast}>0\right)$ as a function of N for $m_{n_2}=m_2=0.1$, $M=1$, $P=3$, $\overline{\gamma}_{n_1}=\overline{\gamma}_m=10$ and $\overline{\gamma}_{n_2}=\overline{\gamma}_e=20$ dB.

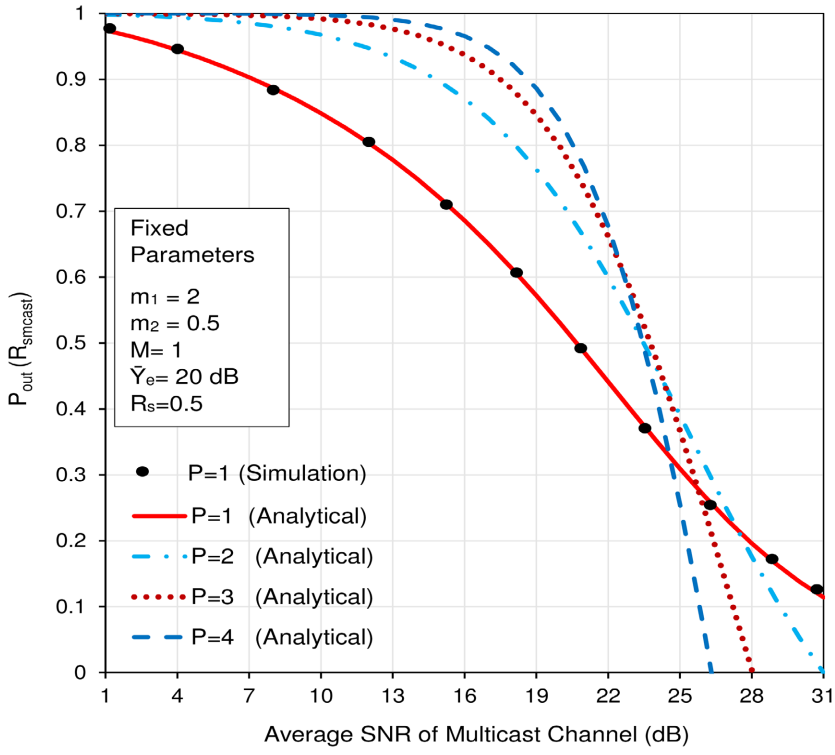

Figure 9. The effects of the number of eavesdropper, P, on the $P_{out}\left(R_{smcast}\right)$ with $m_{n_1}=m_1=2$, $m_{n_2}=m_2=0.5$, $M=1$, $\overline{\gamma}_{n_2}=\overline{\gamma}_e=20$ dB, $R_s=0.5$ and $N=2$.

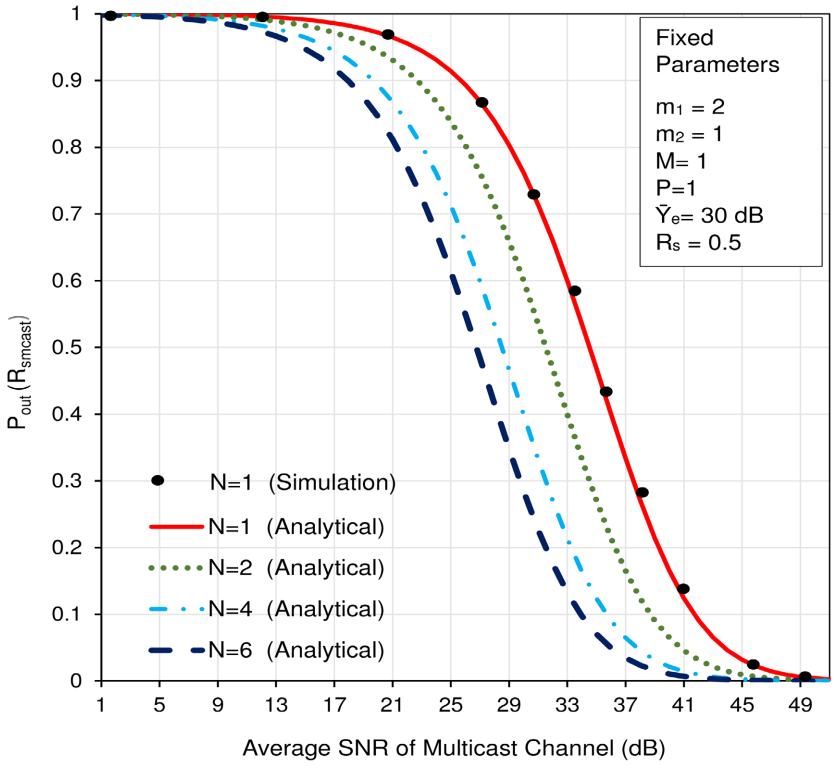

Figure 10. The effects of number of hop, N, on the $P_{out}\left(R_{smcast}\right)$ with $m_{n_1}=m_1=2$, $m_{n_2}=m_2=1$, $M=1$, $P=1$, $\overline{\gamma}_{n_2}=\overline{\gamma}_e=30\,\text{dB}$ and $R_s=0.5$.

because, the cooperative diversity provided by the relays increases the secrecy capacity. Moreover, the cooperative diversity increases with the number of hops which enhances the level of security.

Figure 11 shows the effects of N on the $P_{out}\left(R_{smcast}\right)$ for selected values of P. It is observed that, when $N=2$, $P_{out}\left(R_{smcast}\right)$ increases with P. It means that the security degrades with P. On the other hand, when $P=3$, $Pr\left(C_{smcast}>0\right)$ decreases with N which means that the security enhances with N. Therefore, the loss of security due to the effects of P can be compensated by increasing the number of hops, N.

Figure 12 shows the effects of N on the $P_{out}\left(R_{smcast}\right)$ for selected values of m_{n_1} (denoted as m_1). It is observed that, when $N=2$, $P_{out}\left(R_{smcast}\right)$ decreases with m_1. It means that the security enhances with m_1. On the other hand, when $m_1=1.5$, $Pr\left(C_{smcast}>0\right)$ decreases with N which means that the security enhances with N. Fading parameter is the property of wireless medium, the manual change of which is not possible. But the improvement of security by increasing the number of hops is a practical case.

The $P_{out}\left(R_{smcast}\right)$ is shown in **Figure 13** as a function of N for selected values of m_{n_1} (denoted as m_1) and P. This figure describes the effects of m_1 and P on the $P_{out}\left(R_{smcast}\right)$ for selected values of system parameters. We see that the $P_{out}\left(R_{smcast}\right)$ increases with P which indicates that the security degrades with P. on the other hand, $P_{out}\left(R_{smcast}\right)$ decreases with m_1 which indicates that the

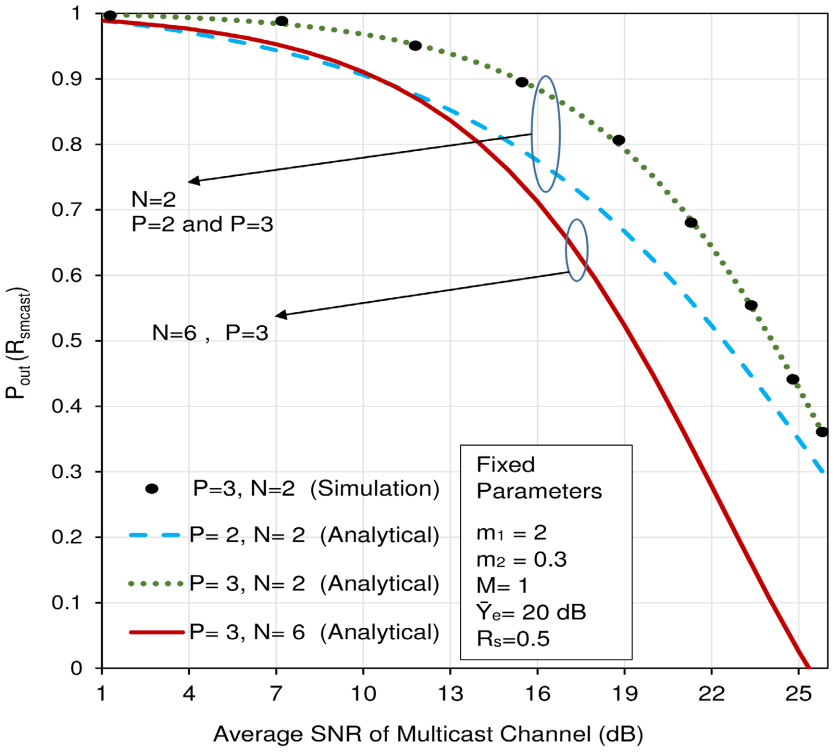

Figure 11. The effects of number of hop, N, on the $P_{out}\left(R_{smcast}\right)$ for selected values of P with $m_{n_1} = m_1 = 2$, $m_{n_2} = m_2 = 0.3$, $M = 1$, $\overline{\gamma}_{n_2} = \overline{\gamma}_e = 20$ dB and $R_s = 0.5$.

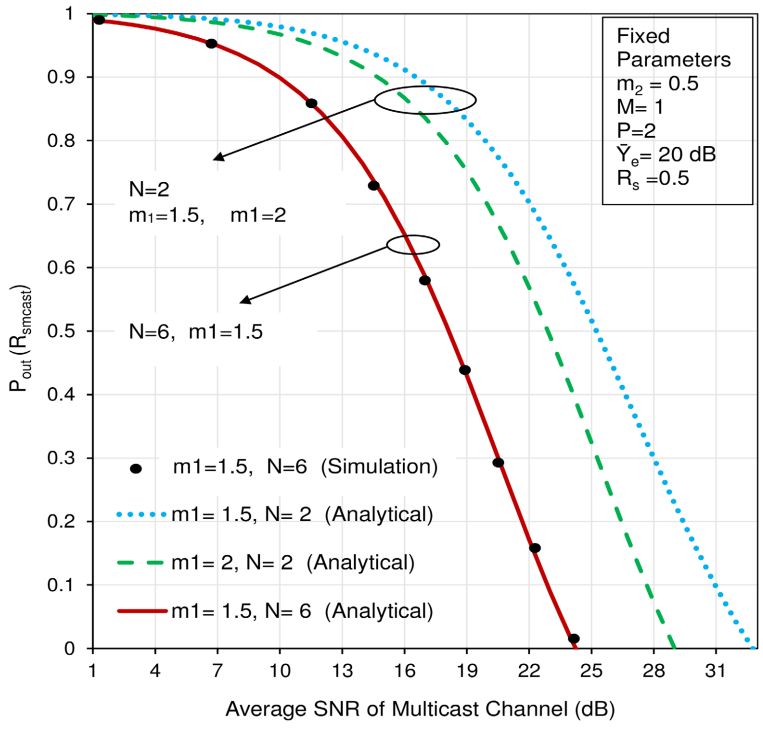

Figure 12. The effect of number of hop, N, on the $P_{out}\left(R_{smcast}\right)$ for selected values of m_{n_1} (denoted as m_1) with $m_{n_2} = m_2 = 0.5$, $M = 1$, $P = 2$, $R_s = 0.5$ and $\overline{\gamma}_{n_2} = \overline{\gamma}_e = 20$ dB.

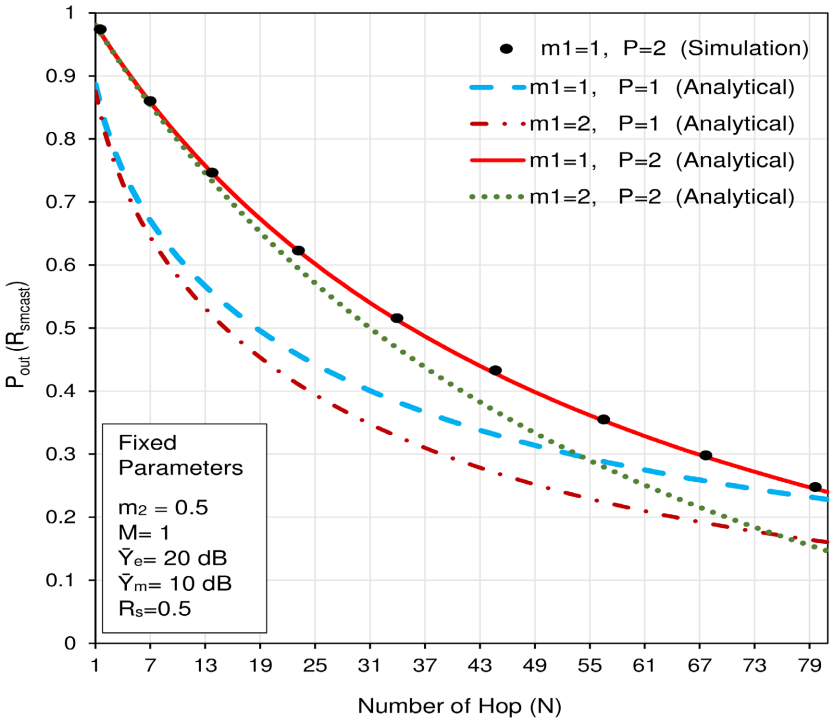

Figure 13. The effect of number of eavesdropper, P, on the $P_{out}\left(R_{smcast}\right)$ for selected values of m_{n_1} (denoted as m_1) with $m_{n_2} = m_2 = 0.5$, $M = 1$, $N = 2$, $R_s = 0.5$ and $\overline{\gamma}_{n_2} = \overline{\gamma}_e = 20$ dB.

security enhances with m_1. In the above figures, the matching between the simulation and analytical results justifies the validity of derived analytical expressions for the PNSMC and SOPM.

Based on the observations of above numerical results, the main findings of this paper can be summarized as follows:

- The mathematical model developed in this paper to ensure the security in multicasting through Nakagami-*m* fading channels employing multi-hop relaying is a valid model and this model can be further extended to enhance the security level employing opportunistic relaying technique.
- The degradation of security levels in multicasting through Nakagami-*m* fading channels due to the effects of the number of eavesdroppers [19] and the SNR of eavesdropper's channel can be compensated by increasing the number of hops. The optimum number of hops can also be determined for a particular number of eavesdroppers.
- The fading of multicast channel enhances the security level and is not the enemy of secrecy multicast capacity [19]. Like jamming against the eavesdroppers, the fading of multicast channel protects the eavesdroppers to decode any information from the multicast channels.

7. Conclusion

This paper focuses on the development of an analytical mathematical model to

ensure the security in wireless multicasting through Nakagami-*m* fading channels employing multi-hop relaying. The validity of developed analytical model is verified via Monte-Carlo simulation. This model is helpful to realize the insight of the effects of system parameters such as fading parameter of multicast channel, the number of eavesdroppers and the number of hops on the security in wireless multicasting through multi-hop Nakagami-*m* fading channels. The observation of numerical results concludes that the loss of security due to the effects of the number of eavesdroppers and the SNR of eavesdropper's channel can be compensated by increasing the number of hops and without increasing the transmit signal power. This work has been carried out in a multicasting scenario with multiple hop system, but this research pave the way of employing different relaying techniques such as opportunistic relaying, asymmetric relaying, multiple cooperative relaying to enhance the security of wireless multicasting without changing the transmit signal power.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Karagiannidis, G.K., Tsiftsis, T.A. and Mallik, R.K. (2006) Bounds for Multi-Hop Relayed Communications in Nakagami-m Fading. *IEEE Transactions on Communications*, **54**, 18-22. https://doi.org/10.1109/TCOMM.2005.861679

[2] Shakkottai, S., Liu, X. and Srikant, R. (2007) The Multicast Capacity of Large Multihop Wireless Networks. *Proceedings of the* 8*th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Montreal, 9-14 September 2007, 247-255. https://doi.org/10.1145/1288107.1288141

[3] Alexandropoulos, G.C., Papadogiannis, A. and Berberidis, K. (2010) Performance Analysis of Cooperative Networks with Relay Selection over Nakagami-m Fading Channels. *IEEE Signal Processing Letters*, **17**, 441-444. https://doi.org/10.1109/LSP.2010.2042992

[4] Liu, C.H. and Andrews, J.G. (2011) Multicast Outage Probability and Transmission Capacity of Multi-Hop Wireless Networks. *IEEE Transactions on Information Theory*, **57**, 4344-4358. https://doi.org/10.1109/TIT.2011.2146030

[5] Zou, Y., Wang, X. and Shen, W. (2013) Optimal Relay Selection for Physical Layer Security in Cooperative Wireless Networks. *IEEE Journal on Selected Areas in Communications*, **31**, 2099-2111. https://doi.org/10.1109/JSAC.2013.131011

[6] Van, N.T., Do, T.N., Bao, V.N.Q. and An, B. (2018) Performance Analysis of Wireless Energy Harvesting Multihop Cluster-Based Networks over Nakagami-m Fading Channels. *IEEE Access*, **6**, 3068-3084. https://doi.org/10.1109/ACCESS.2017.2787055

[7] Sarkar, D.K., Sarkar, M.Z.I. and Anower, M.S. (2021) Enhancing Security in Multicasting with Partial Relay Selection over Composite Fading Channels. *Wireless Personal Communications*, **121**, 1067-1084. https://doi.org/10.1007/s11277-021-08672-0

[8] Ali, S.M.R. and Sarkar, M.Z.I. (2022) Enhancing Security in Multicellular Multicast

Channels Reducing Interference Power with the Best Relay Selection. *Journal of Computer and Communications*, **10**, 1-26. https://doi.org/10.4236/jcc.2022.101001

[9] Sarkar, D.K., Sarkar, M.Z.I. and Anower, M.S. (2022) Multicast Network Security with Asymmetric Cooperative Relaying. *International Journal of Wireless Information Networks*, **29**, 303-313. https://doi.org/10.1007/s10776-022-00566-7

[10] Badrudduza, A.S.M., Sarkar, M.Z.I. and Kundu, M.K. (2020) Enhancing Security in Multicasting through Correlated Nakagami-m Fading Channels with Opportunistic Relaying. *Physical Communication*, **43**, Article ID: 101177. https://doi.org/10.1016/j.phycom.2020.101177

[11] Sarkar, D.K., Sarkar, M.Z.I. and Anower, M.S. (2018) Secure Wireless Multicasting through AF-Cooperative Networks with Best Relay Selection. *Wireless Networks*, **26**, 1717-1730. https://doi.org/10.1007/s11276-018-1861-6

[12] Shrestha, A.P., Jung, J. and Kwak, K.S. (2013) Secure Wireless Multicasting in Presence of Multiple Eavesdroppers. *Proceedings of* 13*th International Symposium on Communications and Information Technologies* (*ISCIT*), Surat Thani, 4-6 September 2013, 814-817. https://doi.org/10.1109/ISCIT.2013.6645929

[13] Nguyen, T.V. and An, B. (2019) Cognitive Multihop Wireless Powered Relaying Networks over Nakagami-m Fading Channels. *IEEE Access*, **7**, 154600-154616. https://doi.org/10.1109/ACCESS.2019.2949081

[14] Kamboj, A.K., Jindal, P. and Verma, P. (2021) Intelligent Physical Layer Secure Relay Selection for Wireless Cooperative Networks with Multiple Eavesdroppers. *Wireless Personal Communications*, **120**, 2449-2472. https://doi.org/10.1007/s11277-021-08458-4

[15] Hasan, M.M. and Sarkar, M.Z.I. (2022) Security in Multicast Over α-μ Fading Channels with Orthogonal Frequency Division Multiplexing. *Journal of Computer and Communications*, **10**, 72-90. https://doi.org/10.4236/jcc.2022.1011006

[16] Gradshteyn, I.S. and Ryzhik, I.M. (2007) Table of Integrals, Series, and Products. 7th Edition. Academic Press, Cambridge.

[17] Sarkar, M.Z.I. and Ratnarajah, T. (2011) Secure Wireless Multicasting through Nakagami-m Fading Miso Channel. 2011 *Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers* (*ASILOMAR*), Pacific Grove, 6-9 November 2011, 300-304. https://doi.org/10.1109/ACSSC.2011.6190006

[18] Sarkar, M.Z.I. and Ratnarajah, T. (2010) Information-Theoretic Security in Wireless Multicasting. *International Conference on Electrical & Computer Engineering* (*ICECE 2010*), Dhaka, 18-20 December 2010, 53-56. https://doi.org/10.1109/ICELCE.2010.5700551

[19] Badrudduza, A., Sarkar, M. and Kundu, M.K. (2020) Enhancing Security in Multicasting through Correlated Nakagami-*m* Fading Channels with Opportunistic Relaying. *Physical Communication*, **43**, Article ID: 101177. https://doi.org/10.1016/j.phycom.2020.101177