Outage Probability and Secrecy Capacity of a Non-orthogonal Multiple Access System

Thi My Chinh Chu and Hans-Jürgen Zepernick
Blekinge Institute of Technology, SE-37179 Karlskrona, Sweden
E-mail: {cch, hjz}@bth.se

***Abstract*—In this paper, we analyze the outage probability and secrecy capacity of a non-orthogonal multiple access (NOMA) system in the presence of an eavesdropper. In order to enhance spectral efficiency, a base station communicates with two users simultaneously in the same frequency band by superpimposing the transmit signals to the users in the power domain. Specifically, the user with the worse channel conditions is allocated higher power such that it is able to directly decode its signal from the received superimposed signal. At the user with the better channel conditions, the interference due to NOMA is processed by successive interference cancelation. Given these system settings and accounting for decoding thresholds, we analyze the outage probability of the NOMA system over Rayleigh fading channels. Furthermore, based on the locations of the users and eavesdropper, the secrecy capacity is analyzed to assess the level of security provided to the legitimate users in the presence of an eavesdropper. Here, the decoding thresholds of legitimate users and eavesdropper are also included in the analysis of the secrecy capacity. Through numerical results, the effects of network parameters on system performance are assessed as well as the the superiority of NOMA in terms of secrecy capacity over traditional orthogonal multiple access.**

I. Introduction

Due to superior spectral efficiency, non-orthogonal multiple access (NOMA) has attracted attention as a promising candidate for 5G networks that may cope with the tremendous demand on capacity [1]–[3]. In contrast to conventional orthogonal multiple access (OMA), NOMA allows multiple users within the same cell to simultaneously share the same radio resources. The two major NOMA approaches focus on the code domain [4], [5] and the power domain [6]–[8]. In the code domain, before transmitting, the signals of different users are mapped to different codewords or sequences. In contrast to direct sequence spread spectrum systems which use orthogonal sequences, the sets of sequences in NOMA comprise either non-orthogonal cross-correlation sequences having low correlation coefficient or sparse sequences [4]. NOMA in the power domain adopts superposition coding (SC) at the transmitter to accommodate the signals of multiple users in the same frequency band at the same time but with different power levels [9]. In this technique, the transmitter allocates power to users proportionally to the inverse of their channel gains [10], i.e., less power is allocated to the user with better channel condition. In this way, the receiver associated with the worst channel conditions can directly decode its signal because the interference from the remaining superimposed signals is kept relatively small. As for the receivers corresponding to better channels, successive interference cancelation (SIC) [11] is adopted to remove interference caused by the stronger signals of the other users until they are able to decode their own signals.

Although NOMA has recently regained significant attention in the context of 5G networks, various aspects have already been addressed. Early works mainly focused on comparing the benefits of NOMA and OMA systems in terms of system performance [12] and fairness among users [13]. The work in [10] solved the max-min fairness among users for the two cases of statistical and instantaneous channel state information (CSI). Further, in [14], the asynchronism problem for NOMA uplink transmissions applying interference cancelation has been addressed. In [15], the superiority of NOMA in terms of spectral efficiency over OMA was investigated with randomly located users. Moreover, the outage probability and ergodic sum rate of NOMA were analyzed in [16]. The works in [17] integrated half-duplex relaying communications with NOMA. Furthermore, in [18], full-duplex relaying was deployed for a NOMA system in which near-distance receivers took the role of relays to decode and forward the messages of far-distance receivers. In addition, transmitters and receivers with multiple antennas were used in the NOMA system suggested in [19] to improve the spatial diversity gain.

Apart from the above performance aspects, security is a very important aspect of wireless communication networks due to the broadcasting nature of the underlying wireless transmission medium. However, as with many novel technologies in their early stage, studies of the security aspects of NOMA are still rather limited. In [20], the secrecy outage probability of NOMA users was derived relying on channel ordering. Furthermore, in [21], the secrecy sum rate of a NOMA system subject to quality of service requirements was analyzed. However, all these works did not consider the decoding threshold at each user and the eavesdropper when analyzing the sum rate of NOMA.

In view of the above, in this paper, we focus on examining the outage probability and secrecy capacity of a NOMA system with both performance metrics accounting for decoding thresholds. In particular, we exploit the channel gain differences between a pair of users including a near-distance user and a far-distance user in order to simultaneously transmit the superimposed signals in the same time-frequency channel by utilizing power domain NOMA. As such, the far-distance user can directly decode its signal as it has been allocated more

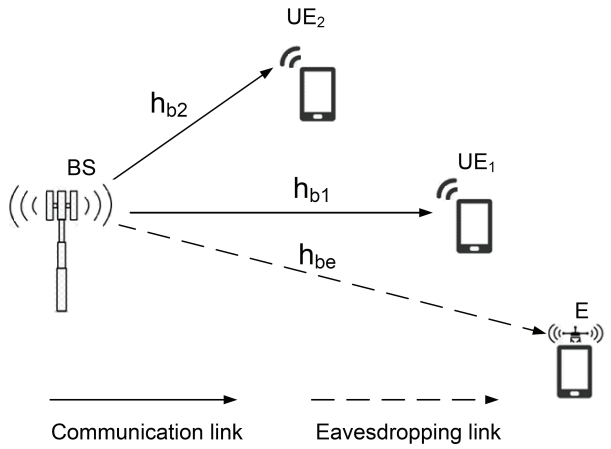

Fig. 1. System model of the considered NOMA system.

power compared to the near-distance user. In order to cancel the interference caused to the weaker signal, SIC is applied at the near-distance user. Given this system setting, we derive expressions for the outage probability and secrecy capacity of the legitimate users in the presence of an eavesdropper. The analysis framework accounts for the effect of the locations of the legitimate users and eavesdropper, fading conditions, and the decoding thresholds at the legitimate users and eavesdropper. Finally, numerical results are provided to reveal the effects of network parameters on system performance as well as to show the superiority of NOMA over OMA in terms of secrecy capacity.

The rest of this paper is organized as follows. In Section II, the system and channel model are introduced as well as the various signal-to-interference-plus-noise ratios (SINRs) and signal-to-noise ratios (SNRs). Section III analyses the outage probability of the NOMA system accounting for the decoding thresholds associated with the two legitimate users. The secrecy capacities of the far-distance user, near-distance user, and NOMA system are analysed in Section IV with decoding thresholds included in the derivations. In Section V, numerical results are provided to illustrate the effect of system parameters on the performance of the NOMA system and to show the superiority of NOMA over OMA. A summary is given in Section VI.

II. System and Channel Model

In the sequel, we consider a NOMA system with the topology shown in Fig. 1. The NOMA system consists of a base station BS which simultaneously communicates with two users UE_1 and UE_2 in the presence of an eavesdropper E. Let BS deploy superposition coding, i.e. NOMA in the power domain, to simultaneously transmit the respective signals to UE_1 and UE_2. In particular, BS allocates transmit power based on the locations of users, i.e., more power is allocated to the signal for the user that is farther away. In this context, h_{b1}, h_{b2}, and h_{be} in Fig. 1 denote the channel coefficients of the links $\mathrm{BS}\rightarrow\mathrm{UE}_1$, $\mathrm{BS}\rightarrow\mathrm{UE}_2$, and $\mathrm{BS}\rightarrow\mathrm{E}$, respectively.

Let $x_1(t)$ and $x_2(t)$ denote the information signals with unit power that BS transmits to UE_1 and UE_2, respectively. Without loss of generality, it is assumed that UE_1 is farther away from BS than UE_2. In this case, UE_1 is given a power allocation coefficient $\alpha > 0.5$ while UE_2 is given a lower power allocation coefficient $1-\alpha < 0.5$. Let P_1 and P_2 be the transmit powers that the BS allocates to the transmit signals $x_1(t)$ and $x_2(t)$, respectively. Then, given the total transmit power P_b of the BS, we have $P_1 = \alpha P_b$ and $P_2 = (1-\alpha)P_b$ and the superimposed transmit signal of the BS is written as

$$x(t) = \sqrt{P_1}x_1(t) + \sqrt{P_2}x_2(t) \tag{1}$$

Because UE_1's signal is allocated more power than UE_2's signal, UE_1 considers UE_2's signal as noise and can directly decode $x_1(t)$. Hence, the SINR with respect to $x_1(t)$ at UE_1 is obtained as

$$\gamma_1 = \frac{P_1 X_{b1}}{P_2 X_{b1} + N_0} \tag{2}$$

where $X_{b1} = |h_{b1}|^2$ is the channel power gain of the channel from BS to UE_1. However, UE_2 cannot directly decode $x_2(t)$ because UE_2's signal is allocated less power and as a result is somewhat hidden behind UE_1's signal. Instead, UE_2 applies SIC to first cancel UE_1's signal and then decode its own signal $x_2(t)$. As a result, the SINR γ_c applicable for the interference cancelation process to remove $x_1(t)$ from the received superimposed signal and the subsequent SNR γ_2 at UE_2 to decode $x_2(t)$ are, respectively, obtained as

$$\gamma_c = \frac{P_1 X_{b2}}{P_2 X_{b2} + N_0} \tag{3}$$

$$\gamma_2 = \frac{P_2 X_{b2}}{N_0} \tag{4}$$

where $X_{b2} = |h_{b2}|^2$ is the channel power gain of the channel from BS to UE_2. Similarly, the SINR and SNR that the eavesdropper applies to decode the signals $x_1(t)$ and $x_2(t)$ of UE_1 and UE_2 are, respectively, given by

$$\gamma_{e1} = \frac{P_1 X_{be}}{P_2 X_{be} + N_0} \tag{5}$$

$$\gamma_{e2} = \frac{P_2 X_{be}}{N_0} \tag{6}$$

where $X_{be} = |h_{be}|^2$ denotes the channel power gain of the channel from BS to E.

In support of the subsequent analysis of system performance, the cumulative distribution function (CDF) and probability density function (PDF) of channel power gain X_i for Rayleigh fading with channel mean power $\Omega_i = \mathbb{E}\{X_i\}$ are provided as

$$F_{X_i}(x_i) = 1 - \exp\left(-\frac{x_i}{\Omega_i}\right), \quad i \in \{b1, b2, be\} \tag{7}$$

$$f_{X_i}(x_i) = \frac{1}{\Omega_i}\exp\left(-\frac{x_i}{\Omega_i}\right) \tag{8}$$

III. Outage Probability

Let us now analyse the outage probability of the NOMA system assuming that UE_1 and UE_2 decode their respective signals if given decoding thresholds are met, otherwise an outage occurs. Specifically, let $\gamma_{th,1}$ denote the decoding threshold of UE_1. Then, UE_1 decodes its signal $x_1(t)$ if the SINR at UE_1 is greater than or equal to the decoding threshold $\gamma_{th,1}$. Therefore, the outage probability for the transmission to UE_1 is given by

$$P_{out,1} = F_{\gamma_1}\left(\gamma_{th,1}\right) \tag{9}$$

where the CDF of γ_1 can be calculated from (2) and (7) as

$$F_{\gamma_1}(\gamma) = \begin{cases} 1 - \exp\left(-\frac{1}{\Omega_{b1}} \frac{\gamma N_0}{P_1 - \gamma P_2}\right) & \frac{P_1}{P_2} \geq \gamma \\ 1 & \frac{P_1}{P_2} < \gamma \end{cases} \tag{10}$$

The calculation of the outage probability for UE_2 is more involved as SIC has to be included. In order to decode $x_2(t)$, first, UE_2 must remove $x_1(t)$ of UE_1 during the interference cancelation process. As such, the SINR γ_c must be greater than or equal to $\gamma_{th,2}$ for removing $x_1(t)$ from the superimposed received signal at UE_2. Subsequently, after having canceled UE_1's signal, UE_2 decodes its own signal given that the SNR γ_2 is greater than or equal to the decoding threshold $\gamma_{th,2}$. In other words, UE_2 falls into outage if UE_2 cannot cancel UE_1's signal or subsequently cannot decode its own signal. The first event occurs if $\gamma_c < \gamma_{th,2}$ while the second event occurs if $\gamma_c \geq \gamma_{th,2}$ but $\gamma_2 < \gamma_{th,2}$. Thus, the outage probability of UE_2 is given by

$$P_{out,2} = F_{\gamma_c}\left(\gamma_{th,2}\right) + \left[1 - F_{\gamma_c}\left(\gamma_{th,c}\right)\right] F_{\gamma_2}\left(\gamma_{th,2}\right) \tag{11}$$

where the CDFs of γ_c and γ_2 can be calculated from (3), (4), and (7) as

$$F_{\gamma_c}(\gamma) = \begin{cases} 1 - \exp\left(-\frac{1}{\Omega_{b2}} \frac{\gamma N_0}{P_1 - \gamma P_2}\right) & \frac{P_1}{P_2} \geq \gamma \\ 1 & \frac{P_1}{P_2} < \gamma \end{cases} \tag{12}$$

$$F_{\gamma_2}(\gamma) = \begin{cases} 1 - \exp\left(-\frac{N_0}{\Omega_{b2} P_2} \gamma\right) & \gamma \geq 0 \\ 0 & \gamma < 0 \end{cases} \tag{13}$$

Note that the powers allocated to the signals transmitted to UE_1 and UE_2 must guarantee that $\gamma_{th,1} < P_1/P_2$ and $\gamma_{th,2} < P_1/P_2$, respectively. Otherwise, the transmission to UE_1 and UE_2 falls into outage with certainty because γ_1 in (2) and γ_c in (3) are always less than P_1/P_2.

As for the outage probability of the NOMA system, we declare an outage if both UE_1 and UE_2 are in outage. Therefore, we can express the outage probability of the NOMA system as

$$P_{out} = P_{out,1} P_{out,2} \tag{14}$$

IV. Secrecy Capacity

In order to guarantee secure transmission for UE_1 and UE_2 in the physical layer, the data rates of the signals $x_1(t)$ and $x_2(t)$ for UE_1 and UE_2 are adapted at the BS based on the channel conditions and the decode processes at the corresponding receivers and eavesdropper. In particular, the secrecy capacity for the transmission of the signal $x_1(t)$ to UE_1 is defined as the difference between the channel capacity of the main channel from BS to UE_1 and the eavesdropper channel from BS to E. Mathematically, the secrecy capacity $C_{s,1}$ for the transmission of signal $x_1(t)$ from BS to UE_1 is formulated as

$$C_{s,1} = C_1 - C_{e,1} \tag{15}$$

where the channel capacity C_1 and $C_{e,1}$ of the main and eavesdropper channel, respectively, are given by

$$C_1 = \int_{\gamma_{th,1}}^{\infty} \log_2(1+\gamma) f_{\gamma_1}(\gamma) d\gamma \tag{16}$$

$$C_{e,1} = \int_{\gamma_{th,e}}^{\infty} \log_2(1+\gamma) f_{\gamma_{e,1}}(\gamma) d\gamma \tag{17}$$

and $\gamma_{th,e}$ denotes the decoding threshold at eavesdropper E. In other words, the eavesdropper cannot decode the signals if the SINR or SNR at E falls below $\gamma_{th,e}$. In view of (2), the SINR γ_1 is always less than or equal to $\frac{P_1}{P_2}$. Thus, we can rewrite (16) as

$$C_1 = \int_{\gamma_{th,1}}^{\frac{P_1}{P_2}} \log_2(1+\gamma) f_{\gamma_1}(\gamma) d\gamma \tag{18}$$

In order to solve (18), we use integration by parts and obtain

$$C_1 = \frac{\ln\left(1 + \frac{P_1}{P_2}\right) F_{\gamma_1}\left(\frac{P_1}{P_2}\right) - \ln\left(\gamma_{th,1} + 1\right) F_{\gamma_1}\left(\gamma_{th,1}\right)}{\ln(2)} - \frac{1}{\ln(2)} \int_{\gamma_{th,1}}^{\frac{P_1}{P_2}} \frac{F_{\gamma_1}(\gamma)}{1+\gamma} d\gamma \tag{19}$$

Substituting (10) into (19), after some modifications, we obtain

$$C_1 = \frac{\ln\left(1+\gamma_{th,1}\right) \exp\left(-\frac{1}{\Omega_{b1}} \frac{\gamma_{th,1} N_0}{P_1 - \gamma_{th,1} P_2}\right)}{\ln(2)} + \frac{\phi\left(\gamma_{th,1}, \Omega_{b1}\right)}{\ln(2)} \tag{20}$$

where

$$\phi(x,y) = \int_x^{\frac{P_1}{P_2}} \frac{\exp\left(\frac{N_0}{y} \frac{\gamma}{\gamma P_2 - P_1}\right)}{1+\gamma} d\gamma \tag{21}$$

Similarly, the channel capacity of the eavesdropper link with respect to overhearing $x_1(t)$ is given by

$$C_{e,1} = \frac{\ln\left(1+\gamma_{th,e}\right) \exp\left(-\frac{1}{\Omega_{be}} \frac{\gamma_{th,e} N_0}{P_1 - \gamma_{th,e} P_2}\right)}{\ln(2)} + \frac{\phi\left(\gamma_{th,e}, \Omega_{be}\right)}{\ln(2)} \tag{22}$$

Substituting (20) and (22) into (15), we finally obtain the secrecy capacity C_1 for the transmission of signal $x_1(t)$ from BS to UE_1.

For the transmission of signal $x_2(t)$ from BS to UE_2, the

secrecy capacity $C_{s,2}$ is defined as

$$C_{s,2} = C_2 - C_{e,2} \tag{23}$$

where C_2 and $C_{e,2}$ denote the channel capacity of the corresponding main and eavesdropper channel, respectively. In order to calculate C_2 and $C_{e,2}$, let us recall that UE_2 falls into outage if it cannot remove $x_1(t)$ during the interference cancelation process or is able to decode $x_1(t)$ but cannot decode $x_2(t)$. Further, it can be seen from (3) that the SINR γ_c associated with the interference cancelation process of x_1(t) is always less than $\frac{P_1}{P_2}$. Therefore, the channel capacity of the main channel from BS to UE_2 is given by

$$C_2 = \int_{\gamma_{th,2}}^{\frac{P_1}{P_2}} \int_{\gamma_{th,2}}^{\infty} \log_2(1+\gamma) f_{\gamma_c}(x) f_{\gamma_2}(\gamma) dx d\gamma \tag{24}$$

Applying integration by parts, after some algebraic modifications, we can rewrite (24) as

$$C_2 = \frac{F_{\gamma_c}\left(\frac{P_1}{P_2}\right) - F_{\gamma_c}(\gamma_{th,2})}{\ln(2)} \Bigg[\ln(1+\gamma_{th,2})(1-F_{\gamma_2}(\gamma_{th,2})) + \int_{\gamma_{th,2}}^{\infty} \frac{1-F_{\gamma_2}(\gamma)}{1+\gamma} d\gamma \Bigg] \tag{25}$$

Substituting (12) and (13) into (25), we have

$$C_2 = \frac{\exp\left(-\frac{1}{\Omega_{b2}} \frac{\gamma_{th,2} N_0}{P_1 - \gamma_{th,2} P_2}\right)}{\ln(2)} \Bigg[\ln(1+\gamma_{th,2}) \exp\left(-\frac{N_0 \gamma_{th,2}}{\Omega_{b2} P_2}\right) + \int_{\gamma_{th,2}}^{\infty} \frac{\exp\left(-\frac{N_0}{\Omega_{b2} P_2}\gamma\right)}{1+\gamma} d\gamma \Bigg] \tag{26}$$

Applying [22, eq. (3.354 .2)] to solve the integral in (26), we obtain the channel capacity for the transmission of the signal $x_2(t)$ in the main channel from BS to UE_2 as

$$C_2 = \frac{\exp\left(-\frac{1}{\Omega_{b2}} \frac{\gamma_{th,2} N_0}{P_1 - \gamma_{th,2} P_2}\right)}{\ln(2)} \Bigg[\ln(1+\gamma_{th,2}) \exp\left(-\frac{N_0 \gamma_{th,2}}{\Omega_{b2} P_2}\right) - \exp\left(\frac{N_0}{\Omega_{b2} P_2}\right) \text{Ei}\left(-\frac{N_0}{\Omega_{b2} P_2}(\gamma_{th,2}+1)\right) \Bigg] \tag{27}$$

where Ei(.) is the exponential integral function defined in [22, eq. (3.352 .4)].

Similarly, the channel capacity on the eavesdropper link with respect to overhearing $x_2(t)$ is obtained as

$$C_{e2} = \frac{\exp\left(-\frac{1}{\Omega_{be}} \frac{\gamma_{th,e} N_0}{P_1 - \gamma_{th,e} P_2}\right)}{\ln(2)} \Bigg[\ln(1+\gamma_{th,e}) \exp\left(-\frac{N_0 \gamma_{th,e}}{\Omega_{be} P_2}\right) - \exp\left(\frac{N_0}{\Omega_{be} P_2}\right) \text{Ei}\left(-\frac{N_0}{\Omega_{be} P_2}(\gamma_{th,e}+1)\right) \Bigg] \tag{28}$$

Substituting (27) and (28) into (23), we obtain the secrecy capacity C_2 for the transmission of signal $x_2(t)$ from BS to UE_2.

Given the expressions for the secrecy capacities $C_{s,1}$ and $C_{s,2}$ in (15) and (23), respectively, the sum secrecy capacity of the considered NOMA system with two users is straightforwardly obtained as

$$C_s = C_{s,1} + C_{s,2} \tag{29}$$

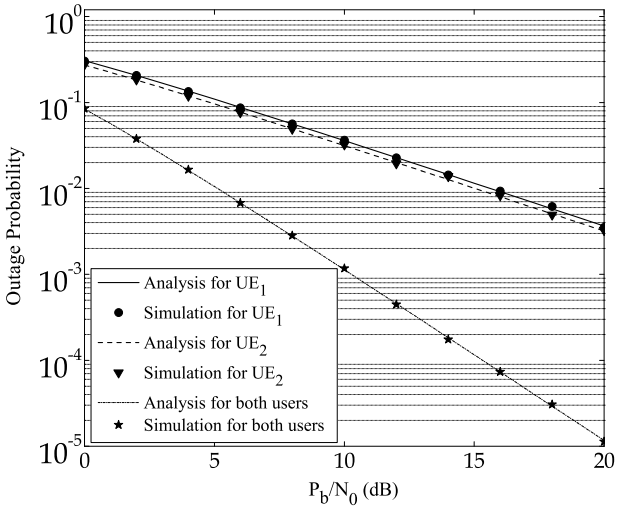

Fig. 2. Outage probability of UE_1, UE_2, and the NOMA system versus transmit SNR P_b/N_0.

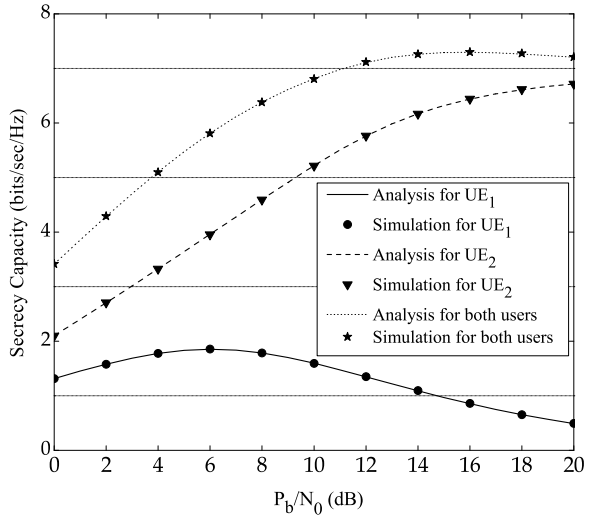

Fig. 3. Secrecy capacity of UE_1, UE_2, and the NOMA system versus transmit SNR P_b/N_0.

V. Numerical Results

In this section, we provide numerical results to illustrate the effects of network parameters on the outage probability, secrecy capacity for each user, and the sum secrecy capacity of the NOMA system. In particular, we consider the impact of the total transmit SNR P_b/N_0 at BS, power allocation coefficient α, and link distance d_{be} from BS to E. In the sequel, $d_i, i \in \{b1, b2, be\}$, are used to denote the normalized distances of the links BS $\rightarrow$ UE_1, BS $\rightarrow$ UE_2, and BS $\rightarrow$ E, respectively. Further, the system is assumed to operate in a suburban environment such that the average channel power gain is attenuated with transmission distance d_i as $\Omega_i = d_i^{-3}$ and path-loss exponent 3. Depending on the location of UE_1 and UE_2, the total transmit power P_b of BS is distributed with

power allocation coefficient α to UE_1 and power allocation coefficient $1-\alpha$ to UE_2. Furthermore, the outage thresholds for both UE_1 and UE_2 are selected as $\gamma_{th,1} = \gamma_{th,2} = 2$ dB.

Firstly, we investigate the effect of the total transmit SNR P_b/N_0 of BS on the outage probability and secrecy capacity of the NOMA system as shown in Fig. 2 and Fig. 3, respectively. The normalized link distances are selected as $d_{b1} = 0.5$, $d_{b2} = 0.3$, and $d_{be} = 1.5$. The power allocation coefficients are calculated based on the average channel power gains of the links BS $\rightarrow$ UE_1 and BS $\rightarrow$ UE_2 as follows:

$$\alpha = \frac{\Omega_{b2}}{\Omega_{b1} + \Omega_{b2}} \tag{30}$$

$$1 - \alpha = \frac{\Omega_{b1}}{\Omega_{b1} + \Omega_{b2}} \tag{31}$$

Fig. 2 reveals that the outage probability of UE_1 and UE_2 are almost the same, i.e., the difference is insignificant. This is due to the fact that, with the power allocation coefficients for the users being selected as inverse of the channel mean powers, the SINR and SNR of UE_1 and UE_2 are rather similar. It can also be observed that the outage probability decreases as the total transmit SNR increases. Given the definition of the NOMA system being in outage if both UE_1 and UE_2 are in outage, the outage probability of the NOMA system is significantly lower than the individual outage probabilities of UE_1 and UE_2.

In contrast, as can be seen from Fig. 3, the secrecy capacity of UE_1 is significantly lower than the secrecy capacity of UE_2. This is because the signals $x_1(t)$ and $x_2(t)$ reach E over the same eavesdropper link from BS to E. Therefore, the SINR of $x_1(t)$ is much higher than that of $x_2(t)$ due to larger power allocation coefficient being given by the BS to the signal for UE_1. Thus, the secrecy capacity on the link from BS to UE_1 is much lower than for the link from BS to UE_2. Specifically, the progression of the secrecy capacity of UE_1 increases for the low total transmit SNR regime until a certain threshold is reached. A further increase of the total transmit SNR beyond this threshold causes a decrease of the secrecy capacity of UE_1. This behaviour can be explained as follows. Because UE_1 is located farther away from BS than UE_2, BS allocates more power to $x_1(t)$ than to $x_2(t)$ which allows UE_1 to directly decode the received superimposed signal given that the SINR is above the decoding threshold. In the low total transmit SNR regime, the signal component of $x_2(t)$ in the superimposed transmit signal causes little interference to UE_1 and to E resulting in an increase of secrecy capacity $C_{s,1}$ with increasing total transmit SNR. Once the total transmit SNR reaches a certain value, the interference from the signal component $x_2(t)$ becomes significant and a further increase causes a decrease in secrecy capacity $C_{s,1}$. As for UE_2, the related secrecy capacity $C_{s,2}$ appears to always increase as the total transmit SNR increases because it applies SIC to first cancel the interference from signal $x_1(t)$ before decoding its own signal $x_2(t)$. Given this progression of the secrecy capacities offered to the two legitimate users, the sum secrecy capacity C_s also increases with the increase of total transmit SNR but tends to converge to a constant once the total transmit SNR becomes sufficiently high.

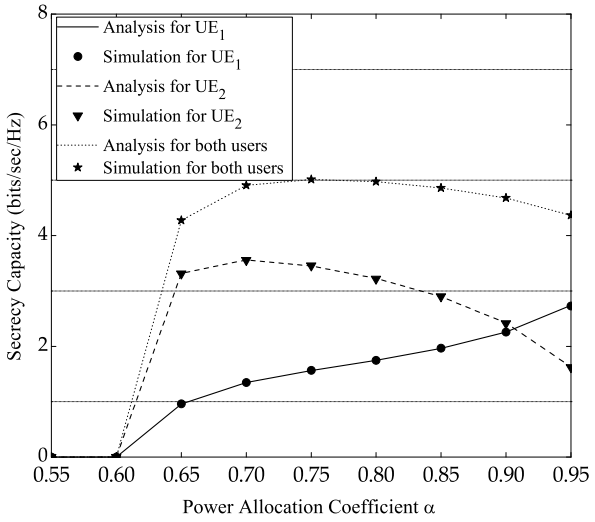

Fig. 4. Secrecy capacity of UE_1, UE_2, and the NOMA system versus power allocation coefficient α.

Secondly, we investigate the effect of the power allocation coefficient α on the secrecy capacity of UE_1, UE_2, and the NOMA system as shown in Fig. 4. In this example, the link distances are selected as $d_{b1} = 0.5$, $d_{b2} = 0.4$, and $d_{be} = 1.5$. Furthermore, the total transmit SNR of BS is set to $P_b/N_0 = 7$ dB. It can be observed from Fig. 4 that the secrecy capacity is zero when the power allocation coefficient α is less than a certain value which can be explained as follows. As can be seen from (2) and (3), the SINR γ_1 at UE_1 and SNR γ_c applicable for interference cancelation at UE_2 are always less than $P1/P2 = \alpha/(1-\alpha)$. Thus, when the ratio $\alpha/(1-\alpha)$ is smaller than the outage thresholds $\gamma_{th,1} = \gamma_{th,2} = 2$ dB, the system always falls into outage and the secrecy capacity for both users and the NOMA system is zero. It can also be observed that, given a fixed total transmit SNR, there is a trade-off between the secrecy capacity of UE_1 and UE_2 with the increase of the power allocation coefficient α. While an increase of α results in more power being allocated to $x_1(t)$, the secrecy capacity of UE_1 increases while at the same time less power is allocated to $x_2(t)$ resulting in a decrease of secrecy capacity of UE_2. As for the NOMA system, there exists an optimal power allocation coefficient α that maximizes the sum secrecy capacity which is around $\alpha \approx 0.75$ for the selected scenario.

Finally, we investigate the effect of the distance d_{be} from BS to E on the secrecy capacity of UE_1, UE_2, and the NOMA system as shown in Fig. 5. In this example, we fix the total transmit SNR at BS as $P_b/N_0 = 10$ dB. The normalized distance from BS to UE_1 and BS to UE_2 are selected as $d_{b1} = 0.5$ and $d_{b2} = 0.2$, respectively. As expected, the secrecy capacity increases as the distance between BS and E increases. More importantly, it is interesting to observe that the NOMA system can still maintain some level of secure transmission even when the eavesdropper E is located close to BS. In this example, UE_1 is farther away from BS than UE_2,

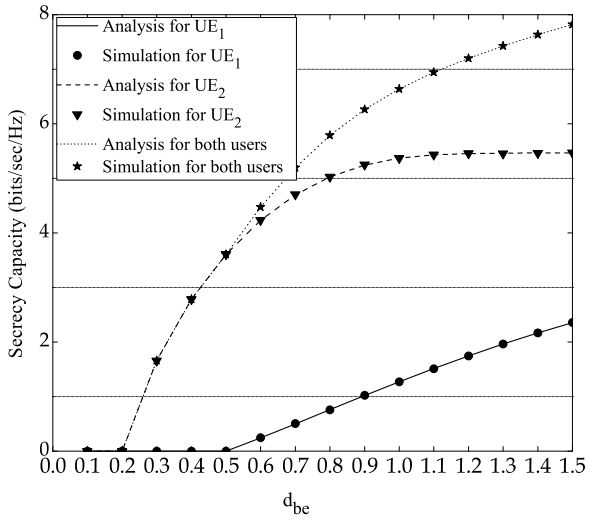

Fig. 5. Secrecy capacity of a NOMA system versus distance d_{be} from the base station BS to eavesdropper E.

i.e. $d_{b1} = 0.5$ and $d_{b2} = 0.2$. Once E is closer to BS than UE_1 but still farther away than UE_2, i.e. $0.2 < d_{be} \leq 0.5$, the secrecy capacity of UE_1 becomes zero while the secrecy capacity of UE_2 and that of the NOMA system is still non-zero. Only if E is closer to BS than both users, the sum secrecy capacity of the NOMA system becomes zero as both users have to suspend their transmissions.

VI. Summary

This work has assessed the performance of a power domain NOMA system in the presence of an eavesdropper in which a base station simultaneously communicates with two users in the same frequency band. In particular, analytical expressions for the outage probability and secrecy capacity for each user and the NOMA system have been derived for the case of Rayleigh fading. The decoding ability of the legitimate users and eavesdropper has been included in the analysis framework through decoding thresholds. The numerical examples that have been provided illustrate the effect of the total transmit power at the base station, the power allocation coefficient to each user, and the position of the eavesdropper on the performance of the NOMA system. A benefit of the NOMA system over OMA has also been shown, i.e. being able to still maintain some level of secrecy capacity even if the eavesdropper moves closer to the base station.

References

[1] Q. C. Li, H. Niu, A. T. Papathanassiou, and G. Wu, "5G network capacity: Key elements and technologies," *IEEE Veh. Technol. Mag.*, vol. 9, no. 1, pp. 71–78, Mar. 2014.

[2] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C. L. I, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[3] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. Bhargava, "A Survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. PP, no. 99, pp. 1–1, 2017.

[4] H. Nikopour and H. Baligh, "Sparse code multiple access," in *Proc. IEEE Int. Symp. on Personal, Indoor and Mobile Radio Commun.*, London, UK, Sep. 2013, pp. 332–336.

[5] M. Al-Imari, P. Xiao, M. A. Imran, and R. Tafazolli, "Uplink non-orthogonal multiple access for 5G wireless networks," in *Proc. Int. Symp. on Wireless Commun. Syst.*, Barcelona, Spain, Aug. 2014, pp. 781–785.

[6] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[7] J. B. Kim and I. H. Lee, "Non-orthogonal multiple access in coordinated direct and relay transmission," *IEEE Commun. Lett.*, vol. 19, no. 11, pp. 2037–2040, Nov. 2015.

[8] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challanges)," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 2, pp. 721–742, 2017.

[9] M. Zeng, G. I. Tsiropoulos, O. A. Dobre, and M. H. Ahmed, "Power allocation for cognitive radio networks employing non-orthogonal multiple access," in *Proc. IEEE Global Commun. Conf*, Washington DC, USA, Dec. 2016, pp. 1–5.

[10] S. Timotheou and I. Krikidis, "Fairness for non-orthogonal multiple access in 5G systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1647–1651, Oct. 2015.

[11] Y. Gao, B. Xia, K. Xiao, Z. Chen, X. Li, and S. Zhang, "Theoretical analysis of the dynamic decode ordering SIC receiver for Uplink NOMA systems," *IEEE Commun. Lett.*, vol. PP, no. 99, pp. 1–1, 2017.

[12] Y. Liu, G. Pan, H. Zhang, and M. Song, "On the capacity comparison between MIMO-NOMA and MIMO-OMA," *IEEE Access*, vol. 6, no. 6, pp. 2123–2129, Jun. 2016.

[13] X. Chen, A. Benjebbour, A. Li, and A. Harada, "Multi-user proportional fair scheduling for uplink non-orthogonal multiple Access (NOMA)," in *Proc. IEEE Veh. Technol. Conf.*, Seoul, Korea, May 2014, pp. 1–5.

[14] H. Haci, H. Zhu, and J. Wang, "Performance of non-orthogonal multiple access with a novel asynchronous interference cancellation technique," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1319–1335, Mar. 2017.

[15] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)," in *Proc. IEEE Int. Symp. Personal, Indoor Mobile Radio Commun.*, London, U.K., Sep. 2013, pp. 611–615.

[16] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.

[17] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[18] J. So and Y. Sung, "Improving non-orthogonal multiple access by forming relaying broadcast channel," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1816–1819, Sep. 2016.

[19] J. Men and J. Ge, "Non-orthogonal multiple access for multiple-antenna relaying networks," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1686–1689, Oct. 2015.

[20] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[21] Y. Zhang, H. M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.

[22] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.