Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 8921895, 6 pages
https://doi.org/10.1155/2018/8921895

Research Article

On the Performance of Security-Based Nonorthogonal Multiple Access in Coordinated Multipoint Networks

Yue Tian[1], **Xianling Wang**[1] **and Zhanwei Wang**[2]

[1]*Fujian Key Laboratory of Communication Network and Information Processing, School of Opto-Electronic and Communication Engineering, Xiamen University of Technology, Xiamen, China*
[2]*School of Information Engineering, Zhengzhou University, Zhengzhou, China*

Correspondence should be addressed to Yue Tian; yue.tian.xmut@outlook.com

Received 10 December 2017; Revised 12 February 2018; Accepted 4 March 2018; Published 4 April 2018

Academic Editor: Imran S. Ansari

The conventional nonorthogonal multiple access (NOMA) strategy has secrecy challenge in coordinated multipoint (CoMP) networks. Under the secrecy considerations, this paper focuses on the security-based NOMA system, which aims to improve the physical layer security issues of conventional NOMA in the coordinated multipoint (NOMA-CoMP) networks. The secrecy performance of S-NOMA in CoMP, that is, the secrecy sum-rate and the secrecy outage probability, is analysed. In contrast to the conventional NOMA (C-NOMA), the results show that the proposed S-NOMA outperforms C-NOMA in terms of the secrecy outage probability and security-based effective sum-rate.

1. Introduction

As a promising candidate for the multiple access schemes in the fifth-generation (5G) mobile system, nonorthogonal multiple access (NOMA) has received widespread attention [1]. In contrast to the conventional orthogonal multiple access, NOMA provides higher capacity and better energy efficiency and supports massive connectivity by enabling users to use the same time, frequency, and code resources for information conveying [2–4]. Coordinated multipoint (CoMP) is one of the promising enhancements in LTE-A, owing to its ability to improve the coverage of high data rate, increase the system throughput, and control the co-channel interference [5, 6]. However, there was a challenge in the downlink of the CoMP network; that is, if an access point allocates a channel to a cell edge user, this channel cannot be used by other users at the same time [7]. Thus, the spectral effectiveness of the CoMP system degrades when the cell edge users increase in number. Recently, studies showed that, by introducing NOMA in coordinated multipoint (CoMP, i.e., a key enhancement for LTE-Advance) networks, not only can the resource efficiency of the whole network be further enhanced [7], but also the complexity of NOMA can be reduced by using proper user-scheduling strategy [8]. Apart from [7, 8], there are several research contributions in the context of improving the cooperative networks performance by using NOMA [9–11]. In [9], the researchers investigated the outage performance of the relay-aided NOMA downlink and compared it to the conventional OMA strategy. In [10], Tian et al. conceived a user-relay-based multitier NOMA strategy, which aimed to improve the coverage of CoMP network. Reference [11] investigated the performance of multicell MIMO-NOMA networks, applying coordinated beamforming for dealing with the intercell interference in order to enhance the cell-edge users' throughput.

However, it should be noted that, due to the fact that the multiple users' signals in NOMA are sharing the same resource channels, the NOMA-CoMP network is confronted with a security issue; that is, the eavesdroppers in the NOMA-CoMP network could listen to the legal users' messages, which creates a secrecy challenge in the physical layer communications.

The physical layer security issue in wireless channel was proposed by Wyner in 1975 [12] and has been researched in diverse scenarios [13–16]. In spite of tremendous research in NOMA, very few existing NOMA researches focus on the security issues in NOMA transmissions. In [17], the authors investigated the maximization of the secrecy sum-rate of

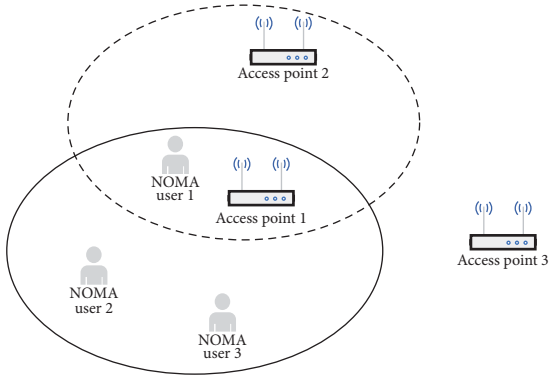

Figure 1: System model of downlink CoMP network.

NOMA in a single-input-single-output (SISO) network. In [18], an optimal design of decoding order for NOMA is proposed under the secrecy considerations; the authors showed that the proposed decoding strategy is an optimal solution for NOMA when considering the secrecy outage constraints. Reference [19] investigated the physical layer security of NOMA in the large-scale networks; the authors showed that the security issues of NOMA can be alleviated by generating a protected zone for the legal users and by creating artificial noise at the transmitters. In this paper, to enhance the physical layer security of NOMA-CoMP system, we proposed a security-based NOMA (S-NOMA) strategy, which combines the coordinated user-scheduling strategy and minimise-information-leakage-based joint transmission strategy in the downlink of a CoMP network. In contrast to the conventional NOMA (C-NOMA), we show that the proposed S-NOMA outperforms C-NOMA in terms of the secrecy outage probability and security-based effective sum-rate.

2. System Model

In this paper, we consider that the proposed CoMP network includes B APs with M antennas each and K single-antenna users, where the sets are defined as $\mathbf{B} = \{1, 2, \ldots, B\}$, $\mathbf{M} = \{1, 2, \ldots, M\}$, and $\mathbf{K} = \{1, 2, \ldots, K\}$. In such CoMP network, define $\mathbf{S}_i$ as the set of APs whose service area can cover the user i; the set of users in the coverage area of AP b is given by $\mathbf{W}_b$; for example, in Figure 1, the circle with the solid line denotes AP 1's service area, and the APs that can cover user 1 are in the circle with the dotted line.

Here we assume that, for any user $i \in \mathbf{K}$, it can be served and coordinated by more than one AP, that is, $\text{card}(\mathbf{S}_i) > 1$. In such NOMA-CoMP system, the observation at the user i can be expressed as

$$y_i = \sum_{b \in \mathbf{S}_k} \sum_{m \in \mathbf{M}} h_{i,b}^m \left(\sum_{j \in \mathbf{W}_b} \sqrt{a_j P} s_j \right) + n_i, \tag{1}$$

where a_i denotes the superposition coding (SC) power allocation coefficient of the signal s_i, P denotes normalized transmission power, and n_i denotes the additive white Gaussian noise at the user i. The point-to-point channel from the mth antenna at an AP b to a user i is given by $\mathbf{h}_{i,b}^m$. For any AP $b \in \mathbf{B}$ and user $i \in \mathbf{K}$, the channel $h_{i,b}^m$ is considered as a Rayleigh fading channel, where $h_{i,b}^m = \sqrt{\alpha_{i,b}^m} g_{i,b}^m$; the factor $g_{i,b}^m$ is the independent and identically distributed circular symmetric complex Gaussian random variable (RV) with zero mean and variance σ_i^2, representing fast fading; the factor $\alpha_{i,b}^m$ denotes the slow fading. The MISO channel from the AP b to the user i is denoted by $\mathbf{h}_{i,b}$, where $\mathbf{h}_{i,b} \in \mathbb{C}^{1 \times M}$.

3. Security-Based NOMA Strategy in CoMP Networks

During the broadcast transmissions in NOMA-CoMP [8], the set of users, whose observation contains the message of the user i, is denoted by

$$\mathbf{O}_i = \bigcup_{i \in \mathbf{S}_i} (\mathbf{W}_i). \tag{2}$$

Define $\mathbf{E}_i$ as a subset of $\mathbf{O}_i$, where the users in such subset can be trusted by the user i. Let the complementary set $\mathbf{E}_i^c$ denote the users that cannot be trusted by the user i; that is, the users in the set $\mathbf{E}_i^c$ are suspected as the eavesdropper to the user i. In the conventional NOMA-CoMP, the message of user i can also be obtained by the users in $\mathbf{E}_i^c$. To reduce the risk of information leakage, that is, to avoid the users in set $\mathbf{E}_i^c$ monitoring user i's message, a security-based NOMA (S-NOMA) strategy is proposed.

The basic idea of the S-NOMA strategy is to minimise the leakage of the signals from a target user to its untrusted users during the NOMA transmission process. Define ϵ_i as a channel quality threshold value at the user i; the S-NOMA strategy can be implemented via the following processes.

Step 1 (security-based AP selection strategy and beamforming design). Assume that the power allocation range at transmitters is from $P_{\min}$ to $P_{\max}$. $\forall b \in \mathbf{B}$ and $\forall j \in \mathbf{E}_i^c$, if $\epsilon_j > P_{\max} \|\mathbf{h}_{i,b}\|^2 \geq \epsilon_i$, add the node's index to $\mathbf{S}_i'$, where $\|\cdot\|$ denotes the Frobenius norm. $\mathbf{S}_i'$ is user i's preferred AP set considering the security problem. If AP b belongs to $\mathbf{S}_i'$, it means that such AP cannot be seen by the untrusted user i; then it can be selected to transmit signal to the target user i, and this AP can be considered as an unconditioned secure AP to the user i. Therefore, if $\text{card}(\mathbf{S}_i') \geq 1$, user i can be served by at least one unconditioned secure AP; if $\text{card}(\mathbf{S}_i') < 1$, that means user i cannot be served by the unconditioned secure AP; then the minimise-information-leakage-based strategy should be used to prevent the untrusted users of user i.

Let $\mathbf{v}_i$ denote the precoding matrix from the APs in set $\mathbf{S}_i'$ to user i. If $\text{card}(\mathbf{S}_i') \geq 1$, set $\mathbf{v}_i = a_i \mathbf{I}_i$, where a_i denotes the power allocation coefficient to user i (i.e., the NOMA superposition coding (SC) coefficient to user i [4]) and I_i denotes an all-ones matrix, where $I_i \in \mathbb{C}^{M \times 1}$. If $\text{card}(\mathbf{S}_i') = 0$, then set $\mathbf{S}_i' = \mathbf{S}_i$ and let $\mathbf{v}_i = a_i \cdot \phi_{i,b}$, where $\phi_{i,b} \in \mathbb{C}^{M \times 1}$ denotes a minimum-leakage-based precoding vector that aims to minimise information leakage from the

AP b to user i. Let SLNR denote the value of signal-to-leakage-plus-noise ratio (SLNR), which is given by $\mathrm{SLNR}_{i,b} = \|\mathbf{h}_{i,b}\phi_{i,b}\|^2\{\mathrm{tr}[\phi_{i,b}(\phi_{i,b})^H] + \sum_{j\in\mathbf{E}_i^c}\|\mathbf{h}_{i,b}\phi_{i,b}\|^2\}^{-1}$ [20]; then, for the AP b in set $\mathbf{S}_i$, $\phi_{i,b}$ can be achieved as

$$\phi_{i,b} = \arg\max_{\phi_{i,b}\in\mathbb{C}^{M\times 1}} \left(\mathrm{SLNR}_{i,b}\right), \tag{3}$$

where $\mathrm{tr}(\cdot)$ indicates the trace.

Step 2 (superposition coding design). Considering that the precoding matrix is normalised, then, by considering the fairness of cell-edge users and the complexity of successive-interference-cancellation (SIC) strategy in NOMA-CoMP [8], the order of SC coefficients is designed based on the following conditions: (a) if $\mathrm{card}(\mathbf{S}_1') \geq \cdots \geq \mathrm{card}(\mathbf{S}_K')$, then $a_1 \geq \cdots \geq a_K$; (b) for the case that $\mathrm{card}(\mathbf{S}_1') = \cdots = \mathrm{card}(\mathbf{S}_K')$, the order of SC coefficients will be sorted based on $\widehat{\mathbf{h}}_k$, where $\widehat{\mathbf{h}}_k = \sum_{b\in\mathbf{S}_k'}\mathbf{h}_{k,b}$; that is, for the case that $\mathrm{card}(\mathbf{S}_1') = \cdots = \mathrm{card}(\mathbf{S}_K')$, if $\|\widehat{\mathbf{h}}_1\| \leq \cdots \leq \|\widehat{\mathbf{h}}_K\|$, then $a_1 \geq \cdots \geq a_K$.

Step 3 (NOMA broadcasting and SIC decoding). Define s_i as user i's desired message. $\forall b \in \mathbf{B}$, AP b broadcasts a combined signal $\sum_{i\in\mathbf{W}_b}\sqrt{a_i P}s_i$, where P is a normalised transmit power. $\forall i \in \mathbf{K}$, user i decodes its observations based on SIC.

4. Performance Analysis of S-NOMA in CoMP Network

The physical layer reaches to secure transmissions when the capacity of the legal user channel is higher than that of the eavesdropper channel [12]; that is, the data can be transmitted at a rate equal to the capacity difference between the legal user and eavesdropper channel capacity. Via the S-NOMA strategy, the SINR at user i, γ_i, is given by

$$\gamma_i = \frac{\sum_{b\in\mathbf{S}_i'}\left\|\mathbf{h}_{i,b}\mathbf{v}_i\right\|^2}{\sum_{b\in\mathbf{S}_i'}\left\|\mathbf{h}_{i,b}\right\|^2\sum_{m\in\mathbf{O}_i}\left\|\mathbf{v}_m\right\|^2 + \beta_i}, \tag{4}$$

where $a_m < a_i$, $\beta_i = |\varphi_i|^2 + P^{-1}\sigma_i^2$, and φ_i is the interference from the APs in the set $\{\mathbf{B}\setminus\mathbf{S}_i'\}$.

Remark 1. It should be noted that φ_i can be very small, as the power range of φ_i is limited by the threshold value; that is, for all $b' \in \{\mathbf{B}\setminus\mathbf{S}_i'\}$, there is $P_{\max}\|h_{i,b'}\|^2 < \epsilon_i$.

The secrecy rate of user i can be expressed as

$$I_i = \log_2(1+\gamma_i) - \log_2\left(1+\gamma_{j'}\right), \tag{5}$$

where j' denotes the user with a maximum data rate in set $\mathbf{E}_i^c$, given as

$$j' = \arg\max_{j\in\mathbf{E}_i^c}\left[\log_2\left(1+\gamma_j\right)\right]. \tag{6}$$

The channels from the APs in set $\mathbf{S}_i'$ to user i, that is, $\sum_{b\in\mathbf{S}_i'}\|\mathbf{h}_{i,b}\|^2$, satisfy the chi-square distribution, where the probability density function (PDF) is given by

$$f_i(x) = \frac{x^{Y_i/2-1}e^{-x/2}}{2^{Y_i/2}\Gamma\left(Y_i/2\right)}, \tag{7}$$

where $Y_i = \mathrm{card}(\mathbf{S}_i)$ and $\Gamma(\cdot)$ is the gamma function. Define R_i as the target rate at user i, and let $\theta_i = 2^{R_i} - 1$.

Then security outage will happen when $I_i < R_i$, which means that the security capacity of user i does not meet the requirement. Here we define the security outage event as $E_i = \{I_i < R_i\}$, where

$$\begin{aligned} E_i = \{I_i < R_i\} &= \left\{\frac{\gamma_i - \gamma_{j'}}{1+\gamma_{j'}} < \theta_i\right\} \\ &= \left\{\gamma_i - (\theta_i+1)\gamma_{j'} < \theta_i\right\}. \end{aligned} \tag{8}$$

Here we firstly consider an ideal case, where, for all $q \in \{W_l : l \in S_i'\}$ and $a_q > a_i$, the message of a user q can be successfully detected by user i; then, according to (5) and (8), the secrecy outage probability (SOP) at user i is given by [19]

$$\mathbb{P}_i^s = \Pr(E_i) = \int_0^\infty f_{\gamma_{j'}}(x)\, F_{\gamma_i}\left((\theta_i+1)x + \theta_i\right)\mathbf{d}x, \tag{9}$$

where the CDF $F_{\gamma_i}(x)$ is given by

$$F_i(x) = \Gamma^{-1}\left(\frac{Y_i}{2}\right)\int_0^{x/2} t^{Y_i/2-1}e^{-t}\mathbf{d}t. \tag{10}$$

Then the SOP in such NOMA-CoMP system can be derived as

$$\begin{aligned} \mathbb{P}_i^s &= 1 - \int_0^{\theta_j}\int_0^{((\theta_i+1)x+\theta_i)/2} \frac{x^{Y_j/2-1}e^{-x/2}t^{Y_i/2-1}}{2^{Y_j/2}\Gamma\left(Y_j/2\right)\Gamma\left(Y_i/2\right)}e^{-t}\mathbf{d}t\,\mathbf{d}x \\ &\approx 1 - \frac{\Gamma\left(Y_i/2\right)\theta_j{}^{Y_j/2}\left(\theta_j+\theta_j\theta_i\right)^{Y_i/2}\left(\Gamma\left(Y_i+Y_j/2\right) - \Gamma\left(Y_i+Y_j/2, \theta_j+\theta_j\theta_i/2\right)\right)}{2^{Y_j/2}\Gamma\left(Y_j/2\right)e^{\theta_i/2}\left(\theta_j(2+\theta_i)\right)^{(Y_i+Y_j)/2}}. \end{aligned} \tag{11}$$

For the nonideal case, the message of user q, where $q \in \{\mathbf{W}_b \cap E_i,\ b \in \mathbf{S}_i'\}$ and $a_q > a_i$, may not be successfully detected by the target user i. The generalized SOP for the nonideal case is given by

$$\mathbb{P}_i = 1 - \left(1 - \mathbb{P}_i^o\right)\left(1 - \mathbb{P}_i^s\right) = \mathbb{P}_i^o + \mathbb{P}_i^s - \mathbb{P}_i^o\mathbb{P}_i^s, \quad (12)$$

where $\mathbb{P}_i^o$ denotes the normal outage probability that user i cannot successfully detect its own message.

Let $R'_{i,q}$ denote user i's target data rate when detecting the message of user q. Then the outage event may happen when $R'_{i,q} < R_i$. Here we define $E'_{i,q}$ as such event, where

$$\begin{aligned} E'_{i,q} &= \left\{ \frac{\sum_{b\in\mathbf{S}'_i} \left\|\mathbf{h}_{i,b}\right\|^2 \mathbf{v}_q}{\sum_{b\in\mathbf{S}'_i} \left\|\mathbf{h}_{i,b}\right\|^2 \sum_{m\in\mathbf{O}_i} \left\|\mathbf{v}_m\right\|^2 + \beta_i} < \theta_q \right\} \\ &\overset{(a)}{=} \left\{ \sum_{b\in\mathbf{S}'_i} \left\| \sqrt{d_{i,b}}\mathbf{h}_{i,b} \right\|^2 < u_n \right\}, \end{aligned} \quad (13)$$

where $d_i = (1 - \theta_q \sum_{m\in\mathbf{O}_i}(\|\mathbf{v}_q\|^2/\|\mathbf{v}_m\|^2))$ and $u_n = \theta_n(\beta_k\|\mathbf{v}_n\|^2)^{-1}$. Note that step (a) follows the condition that, for all $b \in \mathbf{S}'_i$, there exist $d_i > 0$.

Let $\|\mathbf{H}_{i,b}\|^2 = \|\sqrt{d_{i,b}\alpha_{i,b}}g_{i,b}\|^2$; $\|\mathbf{H}_{i,b}\|^2$ can be regarded as the generalized chi-square distribution [21, 22] with variance $d_{i,b}\sigma_{i,b}^2$.

The PDF of the unordered generalized chi-square random variable $\|\mathbf{H}_{i,b}\|^2$ is given by

$$f_i(x) = \frac{(\gamma_{i,b})^{Y_i} x^{Y_i-1} \exp(-\gamma_{i,b}x)}{\Gamma(Y_i)}, \quad (14)$$

where $\Gamma(\cdot)$ denotes the gamma function. Define

$$L_b = \operatorname{card}\left\{\mathbf{W}_b \cap E_i,\ b \in \mathbf{S}'_i\right\}, \quad (15)$$

and assume that s_i's decoding order at user i is $l_b(i)$.

Define

$$\phi = \max\{u_1, \ldots, u_i\}. \quad (16)$$

Based on the high-order statistics in [20], the normal outage probability of user i, $\mathbb{P}_i^o$, can be derived as

$$\begin{aligned} \mathbb{P}_i^o &= \int_0^\phi \frac{L_b! f(x) (F(x))^{l_b(i)-1} (1 - F(x))^{L_b - l_b(i)}}{(l_b(i) - 1)! (L_b - l_b(i))!} \mathbf{d}x \\ &\overset{(b)}{=} \sum_{j=0}^{L_b - l_b(i)} \frac{(-1)^j (F_i(\phi))^{l_b(i)+j} L_b!}{(L_b - l_b(i))! (l_b(i) - 1 - j)! j! \gamma_{i,b} (l_b(i) + j)}, \end{aligned} \quad (17)$$

where step (b) follows the power series of exponential functions. The cumulative distribution function (CDF) $F_i(\phi)$ can be derived by integration of PDF $f_i(x)$ as

$$\begin{aligned} F_i(\phi) &= \int_0^\phi \frac{\left(d_{i,b}\sigma_{i,b}^2\right)^{Y_i} x^{Y_i-1} \exp\left(-d_{i,b}\sigma_{i,b}^2 x\right)}{\Gamma(Y_i)} \mathbf{d}x \\ &\overset{(c)}{=} 1 - \sum_{t=0}^{Y_i-1} \frac{\left(d_{i,b}\sigma_{i,b}^2\phi\right)^t \exp\left(-d_{i,b}\sigma_{i,b}^2\phi\right)}{\Gamma(t+1)}, \end{aligned} \quad (18)$$

where step (c) follows the power series of exponential functions. The similar derivation process of (17) and (18) can be seen in our previous research outputs [8].

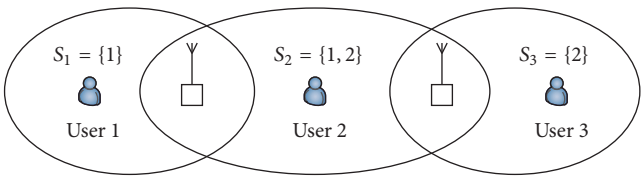

Figure 2: Service area of the two APs, that is, $S_1 = \{1\}$, $S_2 = \{1, 2\}$, and $S_3 = \{2\}$.

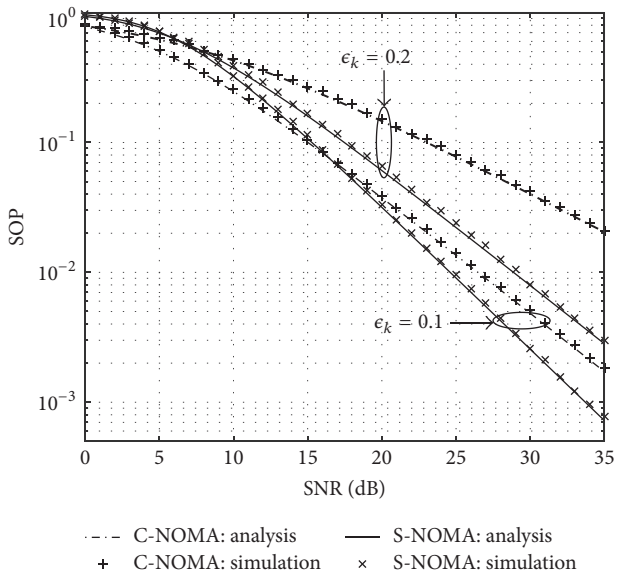

Figure 3: Secrecy outage probability of NOMA-CoMP as a function of SNR.

5. Performance Evaluation

In this section, to evaluate the performance of S-NOMA, we consider a CoMP network that contains two APs with two antennas each ($M = 2$) and three users. Let $\mathbf{B}$ and $\mathbf{K}$ denote the APs and users, respectively.

In such CoMP network, assume that the locations of the three users are randomly distributed in the service area of the two APs; that is, for a user i, if $\mathbf{S}'_i = \{1\}$ or $S'_i = \{2\}$, then $|\mathbf{h}_{i,b}|^2 > \epsilon_i > |\mathbf{h}_{i,b_o}|^2$, where $b \in S'_i$ and $b_o \in \{\mathbf{B} \setminus b\}$; if $\mathbf{S}'_i = \{1, 2\}$, then, for all $b \in \mathbf{B}$, there exist $|\sqrt{\mathbf{h}_{i,b}}|^2 > \epsilon_i$. Assume that, in this CoMP network, user 2 can be trusted by user 3 but will not be trusted by user 1; user 1 and user 3 are not trusted by each other; that is, $\mathbf{E}_1^c = \{2, 3\}$, $\mathbf{E}_2^c = \{1\}$, and $\mathbf{E}_3^c = \{1\}$. The service area of the two APs is considered in Figure 2.

Let l_i denote the SIC decoding order of s_i; then the SC coefficient allocated to s_i is given by

$$a_i = \left(\operatorname{card}(\mathbf{K}) - l_i + 1\right) c^{-1}, \quad (19)$$

where c denotes a constant to ensure that $\sum_{i\in\{\mathbf{W}_b, b\in\mathbf{B}\}} a_i = 1$. Figure 3 provides a comparison of the SOP between the conventional NOMA (C-NOMA) and the S-NOMA with different threshold values; that is, $\epsilon_k = 0.1$ and $\epsilon_k = 0.2$. The target data rate of each user is set to $R_k = 1$ bit per channel

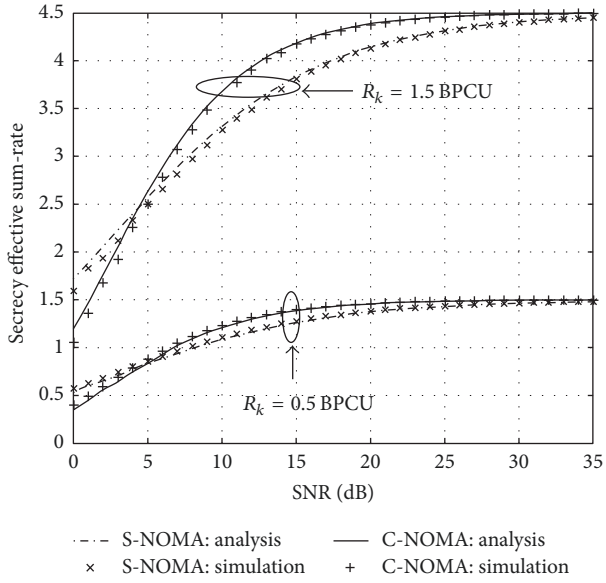

Figure 4: Secrecy effective sum-rate as a function of SNR under different data rate, R.

use (BPCU). In contrast to the C-NOMA, the proposed S-NOMA strategy shows better SOP performance, especially at a high value of ϵ_k. In Figure 3, it should be noted that when SNR is low, the noise will impact on the SLNR-based precoding vector; therefore the S-NOMA's performance is somehow lower than the C-NOMA's; when SNR is high, the performance of S-NOMA is significantly improved.

Figure 4 compares the security-based effective sum-rate (SESR) between S-NOMA and C-NOMA with different data rate. Let $\mathbb{P}_i(R_k)$ denote the SOP at user k under data rate R_k; the SESR is defined as

$$R_{\text{eff}} = \sum_{k \in \mathbf{K}} R_k \mathbb{P}_i \left(1 - R_k\right). \tag{20}$$

The threshold value is set to $\epsilon_k = 0.1$. It can be concluded that when SNR is low (less than 5 dB), the effective sum-rate of S-NOMA is lower than the C-NOMA, as the outage probability of S-NOMA is worse than C-NOMA in this case. The performance gain that is provided by the S-NOMA becomes significant when SNR is larger than 5 dB, especially under the higher target data rate. When SNR is larger than 30 dB, the effective sum-rates of the two schemes are very close, because the outage probability is very small under the high SNR.

Remark 2. If a user m is regarded as an untrusted user of user n, then the data rate of detecting the message of user n at user m will be considered as the eavesdropping data rate. Therefore, the capacity of C-NOMA (the secrecy capacity) is smaller than the CoMP system capacity when considering the physical layer security issue. In contrast to the C-NOMA, the S-NOMA strategy reduces the leakage of information to the untrusted users; therefore the secrecy capacity of S-NOMA is more close to the upper bond capacity (the system capacity), so S-NOMA has a better performance than C-NOMA in terms of secrecy outage probability and secrecy effective sum-rate.

6. Conclusion

This paper focuses on the performance of NOMA-CoMP under secure considerations. We proposed a security-based NOMA strategy, which aims to improve the physical layer security issues in the conventional NOMA-CoMP networks. The secrecy performance of the proposed S-NOMA in CoMP, that is, the secrecy sum-rate and the secrecy outage probability, is analysed and evaluated. In contrast to the conventional NOMA, the results show that the proposed S-NOMA has advantages over C-NOMA, especially when the target transmission data rate is high.

Conflicts of Interest

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

Acknowledgments

This work was supported by the Natural Science Foundation of Fujian Province, China (Grant no. 2016J01323).

References

[1] 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 Challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 721–742, 2017.

[2] 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 Signal Processing Letters*, vol. 21, no. 12, pp. 1501–1505, 2014.

[3] H. Zhang, Y. Qiu, K. Long, G. K. Karagiannidis, X. Wang, and A. Nallanathan, "Resource Allocation in NOMA based Fog Radio Access Networks," *IEEE Wireless Communications*, 2018.

[4] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proceedings of the IEEE 77th Vehicular Technology Conference (VTC '13)*, pp. 1–5, Dresden, Germany, June 2013.

[5] M. Sawahashi, Y. Kishiyama, A. Morimoto, D. Nishikawa, and M. Tanno, "Coordinated multipoint transmission/reception techniques for LTE-advanced," *IEEE Wireless Communications Magazine*, vol. 17, no. 3, pp. 26–34, 2010.

[6] V. Jungnickel, K. Manolakis, W. Zirwas et al., "The role of small cells, coordinated multipoint, and massive MIMO in 5G," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 44–51, 2014.

[7] J. Choi, "Non-orthogonal multiple access in downlink coordinated two-point systems," *IEEE Communications Letters*, vol. 18, no. 2, pp. 313–316, 2014.

[8] Y. Tian, A. R. Nix, and M. Beach, "On the Performance of Opportunistic NOMA in Downlink CoMP Networks," *IEEE Communications Letters*, vol. 20, no. 5, pp. 998–1001, 2016.

[9] J. Men and J. Ge, "Non-Orthogonal Multiple Access for Multiple-Antenna Relaying Networks," *IEEE Communications Letters*, vol. 19, no. 10, pp. 1686–1689, 2015.

[10] Y. Tian, A. R. Nix, and M. Beach, "On the Performance of Multi-tier NOMA Strategy in Coordinated Multi-Point Networks," *IEEE Communications Letters*, 2017.

[11] W. Shin, M. Vaezi, B. Lee, D. J. Love, J. Lee, and H. V. Poor, "Coordinated beamforming for multi-cell MIMO-NOMA," *IEEE Communications Letters*, vol. 21, no. 1, pp. 84–87, 2017.

[12] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[13] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 359–368, 2012.

[14] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 6, pp. 2653–2661, 2014.

[15] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, 2011.

[16] H. Zhang, Y. Qiu, K. Long, G. K. Karagiannidis, X. Wang, and A. Nallanathan, "Resource Allocation in NOMA based Fog Radio Access Networks," in *IEEE Wireless Communications*, Early Access, 2018.

[17] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access," *IEEE Communications Letters*, vol. 20, no. 5, pp. 930–933, 2016.

[18] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the Design of Secure Non-Orthogonal Multiple Access Systems," *IEEE Communications Letters*, vol. 35, no. 10, pp. 2196–2206, 2017.

[19] 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 Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[20] M. Sadek, A. Tarighat, and A. H. Sayed, "A lakagebased precoding scheme for downlink multi-user MIMO channels," *IEEE Transactions on Wireless Communications*, vol. 6, no. 5, pp. 1711–1721, 2007.

[21] D. Hammarwall, M. Bengtsson, and B. Ottersten, "Acquiring partial CSI for spatially selective transmission by instantaneous channel norm feedback," *IEEE Transactions on Signal Processing*, vol. 56, no. 3, pp. 1188–1204, 2008.

[22] J. E. Gentle, *Computational Statistics*, Springer, New York, NY, USA, 2009.