SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Secure NOMA and OMA coordinated transmission schemes in untrusted relay networks

Lu LV[1,2], Zan LI[1], Haiyang DING[1,3] & Jian CHEN[1*]

[1] *State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071*, China;*
[2] *National Mobile Communications Research Laboratory, Southeast University, Nanjing* 210096*, China;*
[3] *School of Information and Communications, National University of Defense Technology, Xi'an* 710106*, China*

Appendix A Signal detection and performance metric for the NOMA scheme

1. The first time slot: Based on (1), N_k first decodes x_f by treating x_k as noise and then removes x_f using successive interference cancellation (SIC) to decode x_k, yielding signal-to-interference-plus-noise ratio (SINR) and signal-to-noise ratio (SNR) as $\gamma_{k:x_f} = \frac{\alpha_f |h_{sk}|^2}{\alpha_k |h_{sk}|^2 + 1/\rho}$ and $\gamma_{k:x_k} = \alpha_k \rho |h_{sk}|^2$, where $\rho = P/\lambda_0$ is the average SNR. Similarly, R also uses SIC to decode the signals, which yields the received SINRs given by $\gamma_{r:x_f} = \frac{\alpha_f |h_{sr}|^2}{\alpha_k |h_{sr}|^2 + |\mathbf{h}_r \mathbf{f}_1|^2 + 1/\rho}$ and $\gamma_{r:x_k} = \frac{\alpha_k |h_{sr}|^2}{|\mathbf{h}_r \mathbf{f}_1|^2 + 1/\rho}$.
2. The second time slot: Based on (2), F first subtracts z from its observations because z is a copy which is already cached by F in the previous time slot. Then, F decodes x_f with SINR as $\gamma_{f:x_f} = \frac{\alpha_f \rho |h_{sr}|^2 |h_{rf}|^2}{\alpha_k \rho |h_{sr}|^2 |h_{rf}|^2 + |h_{rf}|^2 + 1/\varphi_1^2}$. On the other hand, using (3), $\bar{N}_k$ first cancels z since z is a copy which is previously transmitted by $\bar{N}_k$, and then tries to cancel x_k. To achieve this, we have the following equality $\sqrt{\alpha_k P}\varphi_1 h_{sr} h_{r\bar{k}} x_k + w_k h_{s\bar{k}} x_k = 0$, from which the solution is derived as $w_k = -\sqrt{\alpha_k P}\varphi_1 h_{sr} h_{r\bar{k}} / h_{s\bar{k}}$. Using $\mathbb{E}[|w_k|^2] = P_k$, we obtain that $P_k = \alpha_k \frac{\lambda_{sr}\lambda_{rn}}{\lambda_{sn}(\lambda_{sr}+\lambda_{rn}+1/\rho)} P$. Since $\frac{\lambda_{sr}\lambda_{rn}}{\lambda_{sn}(\lambda_{sr}+\lambda_{rn}+1/\rho)} < \frac{\lambda_{sr}\lambda_{rn}}{\lambda_{sn}(\lambda_{sr}+\lambda_{rn})} \approx \frac{\min(\lambda_{sr},\lambda_{rn})}{\lambda_{sn}} < \frac{\lambda_{sr}}{\lambda_{sn}} < 1$, $P_k < P$ always satisfies. This indicates that x_k can be perfectly cancelled by $\bar{N}_k$. After that, $\bar{N}_k$ decodes $\bar{x}_k$ using SINR as $\gamma_{\bar{k}:\bar{x}_k} = \frac{\varpi_1 \rho |h_{s\bar{k}}|^2}{\varphi_1^2 \alpha_f \rho |h_{sr}|^2 |h_{r\bar{k}}|^2 + \varphi_1^2 |h_{r\bar{k}}|^2 + 1}$, where $\varpi_1 = 1 - \alpha_k \frac{\lambda_{sr}\lambda_{rn}}{\lambda_{sn}(\lambda_{sr}+\lambda_{rn}+1/\rho)}$.
3. Performance metric: In this work, we consider the secrecy rate as the performance metric, which is defined as the difference between the rate of the legitimate channel (from the source to the far user or the scheduled near user) and that of the wiretap channel (from the source to the untrusted relay). Given this definition, the secrecy rates for x_k, x_f, and $\bar{x}_k$ are obtained, respectively, by

$$C_{x_k}^{\text{noma}} = \frac{1}{2}\Big[\log\big(1+\gamma_{k:x_k}\big) - \log\big(1+\gamma_{r:x_k}\big)\Big]^+, \tag{A1}$$

$$C_{x_f}^{\text{noma}} = \frac{1}{2}\Big[\log\big(1+\min(\gamma_{k:x_f},\gamma_{f:x_f})\big) - \log\big(1+\gamma_{r:x_f}\big)\Big]^+, \tag{A2}$$

$$C_{\bar{x}_k}^{\text{noma}} = \frac{1}{2}\Big[\log\big(1+\gamma_{\bar{k}:\bar{x}_k}\big) - 0\Big]^+, \tag{A3}$$

where $[x]^+ = \max(x,0)$ and the first term in (A2) follows the fact that x_f needs to be decoded by N_k in SIC.

Appendix B Proof of Lemma 1

From (A1) and (A3), it can be known that R's eavesdropping rates for x_k and $\bar{x}_k$ do not depend on k^* and $\bar{k}^*$. Thus, the maximization of the secrecy rates for x_k and $\bar{x}_k$ is equivalent to the transmission rates for x_k and $\bar{x}_k$, which is exactly the user scheduling criterion (4).

On the other hand, according to (A2), it is necessary to maximize the transmission rate for x_f towards the secrecy rate maximization, which is discussed in two cases: 1) When $\gamma_{k:x_f} \leqslant \gamma_{f:x_f}$, the transmission rate for x_f is dominated by $\gamma_{k:x_f}$. In this case, since $\gamma_{k:x_f}$ monotonically increases with $|h_{sk}|^2$, it can be concluded that the maximization of $\gamma_{k:x_f}$ is equivalent to the maximization of $\gamma_{k:x_k}$. This indicates that k^* is also optimal in the secrecy rate for x_f. 2) When $\gamma_{k:x_f} > \gamma_{f:x_f}$, the transmission rate for x_f is dominated by $\gamma_{f:x_f}$, which is not related to k^*. With these results, Lemma 1 is proved.

* Corresponding author (email: jianchen@mail.xidian.edu.cn)

Appendix C Signal detection and performance metric for the OMA scheme

1. The first time slot: Using (5), R tries to decode x_f with SINR as $\hat{\gamma}_{r:x_f} = \frac{|h_{sr}|^2}{\mu_r+1/\rho}$, where $\mu_r = \left|\sum_{k=1}^{K}|h_{rk}|\right|^2$.
2. The second time slot: Using (6), F first removes z since F already caches a copy of z and then decodes x_f with SNR as $\hat{\gamma}_{f:x_f} = \frac{\rho|h_{sr}|^2|h_{rf}|^2}{|h_{rf}|^2+1/\varphi_2^2}$. Using (7), N_k first cancels z since z is a copy which is previously transmitted by N_k and then removes x_f. For this, equality $\sqrt{P}\varphi_2 h_{sr}h_{rk}x_f + w_f h_{sk}x_f = 0$ should hold, such that we have $w_f = -\sqrt{P}\varphi_2 h_{sr}h_{rk}/h_{sk}$ and $P_f = \frac{\lambda_{sr}\lambda_{rn}}{\lambda_{sn}(\lambda_{sr}+\bar{\mu}_r+1/\rho)}P$. Based on the fact that $\lambda_{rn} < \bar{\mu}_r$ and $\lambda_{sr} < \lambda_{sn}$, inequality $P_f < P$ holds, which implies that N_k's interference cancellation is always successful. Then, N_k decodes x_k with SNR as $\hat{\gamma}_{k:x_k} = \frac{\varpi_2\rho|h_{sk}|^2}{\varphi_2^2|h_{rk}|^2+1}$, where $\varpi_2 = 1 - \frac{\lambda_{sr}\lambda_{rn}}{\lambda_{sn}(\lambda_{sr}+\bar{\mu}_r+1/\rho)}$.
3. Performance metric: Based on the above results, the secrecy rates for x_k and x_f are given, respectively, by

$$C_{x_k}^{\text{oma}} = \frac{1}{2}\Big[\log\left(1+\hat{\gamma}_{k:x_k}\right) - 0\Big]^+, \tag{C1}$$

$$C_{x_f}^{\text{oma}} = \frac{1}{2}\Big[\log\left(1+\hat{\gamma}_{f:x_f}\right) - \log\left(1+\hat{\gamma}_{r:x_f}\right)\Big]^+. \tag{C2}$$

Appendix D Proof of Theorem 1

Using Jensen's inequality, the ESRs of N_k, F, and $\bar{N}_k$ can be lower bounded, respectively, by

$$\bar{C}_{x_k,\text{lb}}^{\text{noma}} = \frac{1}{2}\left[A_1 - A_2\right]^+, \tag{D1}$$

$$\bar{C}_{x_f,\text{lb}}^{\text{noma}} = \frac{1}{2}\left[A_3 - A_4\right]^+, \tag{D2}$$

$$\bar{C}_{\bar{x}_k,\text{lb}}^{\text{noma}} = \frac{1}{2}A_5, \tag{D3}$$

where $A_1 = \mathbb{E}[\log(1+\gamma_{k^*:x_k})]$, $A_2 = \mathbb{E}[\log(1+\gamma_{r:x_k})]$, $A_3 = \mathbb{E}[\log(1+\min(\gamma_{k^*:x_f},\gamma_{f:x_f}))]$, $A_4 = \mathbb{E}[\log(1+\gamma_{r:x_f})]$, and $A_5 = \mathbb{E}[\log(1+\gamma_{\bar{k}^*:\bar{x}_k})]$.

Based on the user scheduling criterion (4), we can derive A_1 as

$$\begin{aligned} A_1 &= \int_0^\infty \frac{\sum_{i=1}^{K}\binom{K}{i}(-1)^{i+1}e^{-\frac{ix}{\alpha_k\rho\lambda_{sn}}}}{1+x}dx \\ &= \sum_{i=1}^{K}\binom{K}{i}(-1)^i e^{\frac{i}{\alpha_k\rho\lambda_{sn}}}\,\text{Ei}\Big(-\frac{i}{\alpha_k\rho\lambda_{sn}}\Big), \end{aligned} \tag{D4}$$

where we use [1, eq. (3.352.4)]. Also, since $|\mathbf{h}_r\mathbf{f}_1|^2$ is exponentially distributed with λ_{rn}, the cumulative distribution function (CDF) of $\gamma_{r:x_k}$ is $F_{\gamma_{r:x_k}}(x) = 1 - \frac{\delta}{x+\delta}e^{-\frac{x}{\alpha_k\lambda_{sr}}}$, where $\delta = \alpha_k\lambda_{sr}/\lambda_{rn}$. By using this result, A_2 can be computed by

$$\begin{aligned} A_2 &= \int_0^\infty \left(\frac{\delta/(1-\delta)}{x+\delta} - \frac{\delta/(1-\delta)}{x+1}\right)e^{-\frac{x}{\alpha_k\lambda_{sr}}}dx \\ &= \frac{\delta[e^{\frac{1}{\lambda_{rn}}}\,\text{Ei}(-1/\lambda_{rn}) - e^{\frac{1}{\alpha_k\lambda_{sr}}}\,\text{Ei}(-1/(\alpha_k\lambda_{sr}))]}{\delta-1}. \end{aligned} \tag{D5}$$

Substituting (D4) and (D5) into (D1), a closed-form $\bar{C}_{x_k,\text{lb}}^{\text{noma}}$ is derived.

Denote $X = \min(\gamma_{k^*:x_f},\gamma_{f:x_f})$, its CDF is obtained by $F_X(x) = 1 - e^{-\frac{(K\lambda_{sr}+\lambda_{sn})x}{\rho\lambda_{sr}\lambda_{sn}(\alpha_f-\alpha_k x)}}\xi(x)K_1(\xi(x))$, where $\xi(x) = \frac{2}{\varphi_1}\sqrt{\frac{x}{\rho\lambda_{sr}\lambda_{rf}(\alpha_f-\alpha_k x)}}$. Thus, A_3 can be calculated as

$$\begin{aligned} A_3 &= \int_0^{\frac{\alpha_f}{\alpha_k}} \frac{e^{-\frac{(K\lambda_{sr}+\lambda_{sn})x}{\rho\lambda_{sr}\lambda_{sn}(\alpha_f-\alpha_k x)}}}{1+x}\xi(x)K_1(\xi(x))dx \\ &\approx \frac{\pi}{M}\sum_{m=1}^{M}\frac{\alpha_f(1-x_m^2)^{\frac{1}{2}}}{2\alpha_k+\alpha_f(x_m+1)}e^{-\frac{(K\lambda_{sr}+\lambda_{sn})(x_m+1)}{\rho\lambda_{sr}\lambda_{sn}\alpha_k(1-x_m)}}\xi\Big(\frac{\alpha_f(x_m+1)}{2\alpha_k}\Big)K_1\Big(\xi\Big(\frac{\alpha_f(x_m+1)}{2\alpha_k}\Big)\Big), \end{aligned} \tag{D6}$$

where we use the Gauss-Chebyshev quadrature approximation and $K_1(\cdot)$ is the modified first-order Bessel function of the second kind. Similar to the derivation of A_2, we can approximate A_4 as

$$A_4 \approx \frac{\pi}{M}\sum_{m=1}^{M}\frac{\alpha_k(1-x_m)^{\frac{3}{2}}e^{-\frac{x_m+1}{\rho\alpha_k(1-x_m)}}}{(2\alpha_k/\alpha_f+1+x_m)(\lambda_{rn}+\alpha_k+(\lambda_{rn}-\alpha_k)x_m)}. \tag{D7}$$

Substituting (D6) and (D7) into (D2), a closed-form $\bar{C}_{x_f,\text{lb}}^{\text{noma}}$ is obtained.

Since the user scheduling processes in the first and second time slots are disjoint, the CDF of $\gamma_{\bar{k}:\bar{x}_k}$ is attained as $F_{\gamma_{\bar{k}:\bar{x}_k}}(x) = \left(1+\varepsilon(x)e^{-\frac{x}{\rho\lambda_{sn}\varpi_1}+\varepsilon(x)+\frac{1}{\lambda_{sr}\alpha_f}}\,\text{Ei}(-\varepsilon(x)-\frac{1}{\lambda_{sr}\alpha_f})\right)^{K-1}$, where $\varepsilon(x) = \frac{\rho\lambda_{sn}\varpi_1}{\lambda_{sr}\lambda_{rn}\varphi_1^2\alpha_f x}$. Thus, a semi-closed-form of A_5 is derived as follows:

$$A_5 = \int_0^\infty (1-F_{\gamma_{\bar{k}:\bar{x}_k}}(x))/(1+x)dx, \tag{D8}$$

which can be easily evaluated using standard software such as Matlab or Mathematica.

Now, by combining the results in (D4)–(D8), we learn that a positive sum ESR is achieved. This completes the proof of Theorem 1.

Appendix E Proof of Corollary 1

Using the fact that $\max(x_1, x_2, \ldots, x_K) \geqslant x_k$, $\gamma_{k^*:x_k}$ can be lower bounded as: $\gamma_{k^*:x_k} \geqslant \alpha_k \rho |h_{sk}|^2$. While $\gamma_{r:x_k}$ converges to a constant if ρ is sufficiently large. Thus, we can asymptotically express $\bar{C}^{\text{noma}}_{x_k,\text{lb}}$ as $\bar{C}^{\text{noma}}_{x_k,\text{lb}} \sim \log(\alpha_k\rho) \sim \log\rho$. Similarly, we can prove the ESR scaling laws of $\bar{N}_k$ and F.

On the other hand, according to the extreme-value theory [2], we have $\max_{k\in\{1,\ldots,K\}} \gamma_{k:x_k} \sim \log K + O(\log\log K)$ and $\max_{\bar{k}\in\{1,\ldots,K\}\setminus k^*} \gamma_{\bar{k}:\bar{x}_k} \sim \log(K-1) + O(\log\log(K-1))$, while $\gamma_{r:x_k}$ is independent of K. Thus, we obtain that $\bar{C}^{\text{noma}}_{x_k,\text{lb}} \sim \frac{1}{2}\log\log K$ and $\bar{C}^{\text{noma}}_{\bar{x}_k,\text{lb}} \sim \frac{1}{2}\log\log(K-1)$. Furthermore, using the fact that $\min(\gamma_{k^*:x_f}, \gamma_{f:x_f}) \leqslant \gamma_{f:x_f}$ which is independent of K, and $\gamma_{r:x_f}$ is also independent of K, we know that $\bar{C}^{\text{noma}}_{x_f,\text{lb}}$ converges to a constant. Hence, we complete the proof of Corollary 1.

Appendix F Proof of Theorem 2

The ESRs of N_k and F can be lower bounded, respectively, by

$$\bar{C}^{\text{oma}}_{x_k,\text{lb}} = \frac{1}{2} B_1, \tag{F1}$$

$$\bar{C}^{\text{oma}}_{x_f,\text{lb}} = \frac{1}{2} [B_2 - B_3]^+, \tag{F2}$$

where $B_1 = \mathbb{E}[\log(1+\hat{\gamma}_{k^*:x_k})]$, $B_2 = \mathbb{E}[\log(1+\hat{\gamma}_{f:x_f})]$, and $B_3 = \mathbb{E}[\log(1+\hat{\gamma}_{r:x_f})]$.

With the user scheduling (8), we can calculate the CDF of $\hat{\gamma}_{k^*:x_k}$ as $F_{\hat{\gamma}_{k^*:x_k}}(x) = \sum_{i=1}^{K} \binom{K}{i} (-1)^{i+1} (\frac{\epsilon}{x+\epsilon})^i e^{-\frac{ix}{\varpi_2\rho\lambda_{sn}}}$, where $\epsilon = \frac{\varpi_2\rho\lambda_{sn}}{\varphi_2^2\lambda_{rn}}$. Based on this result, a semi-closed-form expression of B_1 can be obtained as

$$B_1 = \sum_{i=1}^{K} \binom{K}{i} (-1)^{i+1} \int_0^\infty \log(1+x) \Big(\frac{\epsilon}{x+\epsilon}\Big)^i e^{-\frac{ix}{\varpi_2\rho\lambda_{sn}}} dx. \tag{F3}$$

The CDF of $\hat{\gamma}_{f:x_f}$ is given by $F_{\hat{\gamma}_{f:x_f}}(x) = 1 - \nu(x)K_1(\nu(x))e^{-\frac{x}{\rho\lambda_{sr}}}$, where $\nu(x) = \frac{2}{\varphi_2}\sqrt{\frac{x}{\rho\lambda_{sr}\lambda_{rf}}}$. Then, we can derive B_2 in semi-closed-form as

$$B_2 = \int_0^\infty \frac{\nu(x)K_1(\nu(x))}{1+x} e^{-\frac{x}{\rho\lambda_{sr}}} dx. \tag{F4}$$

On the other hand, B_3 can be upper bounded by

$$\begin{aligned} B_3 &= \int_0^\infty \frac{1 - F_{\hat{\gamma}_{r:x_f}}(x)}{1+x} dx \\ &= \int_0^\infty \frac{e^{-\frac{x}{\rho\lambda_{sr}}} \int_0^\infty e^{-\frac{xy}{\lambda_{sr}}} dF_{\mu_r}(y)}{1+x} dx \\ &\leqslant \int_0^\infty \frac{e^{-\frac{x}{\rho\lambda_{sr}}} \int_0^\infty e^{-\frac{xy}{\lambda_{sr}}} dF_{\mu_r,\text{ub}}(y)}{1+x} dx, \end{aligned} \tag{F5}$$

where the inequality in (F5) is obtained by using the well-known arithmetic-geometric mean inequality and $F_{\mu_r,\text{ub}}(y)$ is given by [3, eq. (20)]. Overall, by combining the expressions of B_2 and B_3, a semi-closed-form lower bound for $\bar{C}^{\text{oma}}_{x_f,\text{lb}}$ is obtained.

Therefore, summarizing the results in (F3)–(F5), it is concluded that a positive sum ESR is achieved by the secure OMA coordinated transmission scheme, which proves Theorem 2.

Appendix G Simulation results

We provide simulation results to characterize the secrecy performance achieved by the proposed secure NOMA and OMA coordinated transmission schemes. Without loss of generality, we assume that the average channel gains are set as $\lambda_{sr} = 0.8$, $\lambda_{sn} = 1$, $\lambda_{rf} = 0.7$, and $\lambda_{rn} = 1$, respectively.

Figure G1(a) shows the ESR achieved by the proposed secure NOMA coordinated transmission scheme with $K = 2$ and $\alpha_f = \min(0.1, 1/\rho)$. It is clear from Figure G1(a) that the derived ESR lower bounds exactly match the simulation results for N_k, F, and $\bar{N}_k$ and a positive sum ESR is achieved by the proposed scheme. The results confirm our derived theoretical analysis and demonstrate Theorem 1. As can be observed from Figure G1(a), the ESR lower bounds of N_k and $\bar{N}_k$ improve with the increased ρ and increase to $\frac{1}{2}\log\rho$ in the high ρ regime. However, when α_f is fixed to 0.8, the ESR lower bound of $\bar{N}_k$ saturates in the high ρ regime. The above observations are consistent to the conclusions in Corollary 1. Furthermore, it is also observed from Figure G1(a) that the ESR of F converges to a constant in the high ρ regime. This is because F decode its x_f by treating x_k as interference, and the received power of x_f and x_k both increase with ρ, such that the ESR of F goes to a constant when ρ is sufficiently large.

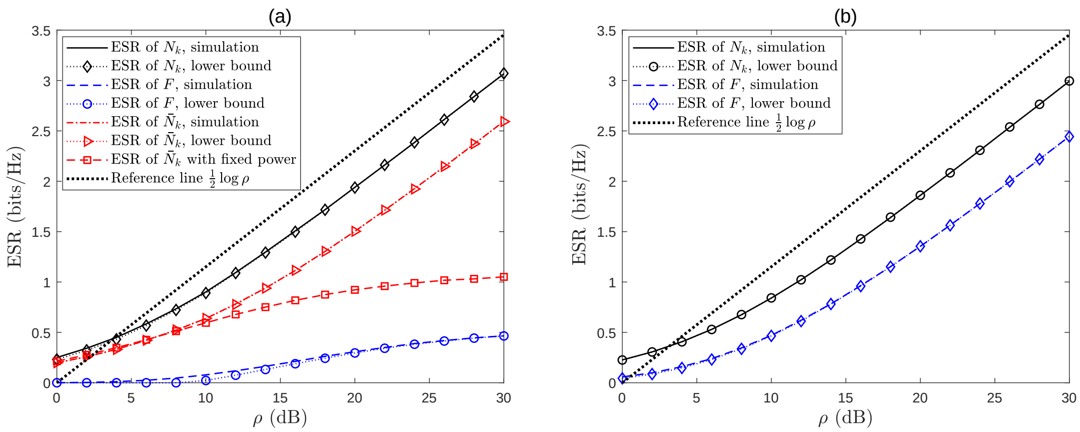

Figure G1 ESR performance: (a) the secure NOMA coordinated transmission scheme; (b) the secure OMA coordinated transmission scheme.

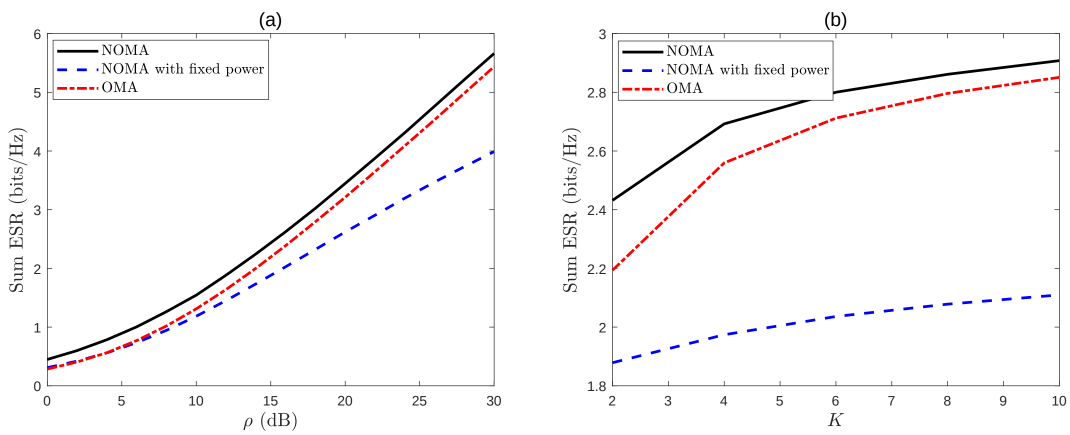

Figure G2 ESR comparison: (a) as a function of ρ; (b) as a function of K.

Figure G1(b) plots the ESR achieved by the proposed secure OMA coordinated transmission scheme with $K = 2$. It can be seen that the derived ESR lower bounds agree well with the simulated ones throughout the whole ρ regime. Compared with the secure NOMA coordinated transmission scheme given in Figure G1(a), it can be seen from Figure G1(b) that both the ESR lower bounds of N_k and F achieved by the secure OMA transmission scheme increase by increasing ρ and scale as $\frac{1}{2}\log\rho$ in the high ρ regime, which validates the result in Corollary 2. Therefore, the secure OMA coordinated transmission scheme achieves a balanced tradeoff for the secrecy rate performance between the near user and the far user.

Figure G2(a) and (b) compare the ergodic secrecy sum rate achieved by the secure NOMA and OMA coordinated transmission schemes, where the ergodic secrecy sum rates are defined as $\bar{C}_{\rm sum}^{\rm noma} \triangleq \bar{C}_{x_k,{\rm lb}}^{\rm noma} + \bar{C}_{x_f,{\rm lb}}^{\rm noma} + \bar{C}_{\bar{x}_k,{\rm lb}}^{\rm noma}$ for NOMA and $\bar{C}_{\rm sum}^{\rm oma} \triangleq \bar{C}_{x_k,{\rm lb}}^{\rm oma} + \bar{C}_{x_f,{\rm lb}}^{\rm oma}$ for OMA, respectively. We assume $K = 2$ in Figure G2(a) and $\rho = 15$ dB in Figure G2(b). As can be observed from Figure G2(a), the secure NOMA and OMA coordinated transmission schemes exhibit a very similar increasing trend in the high ρ regime, and the secure NOMA coordinated transmission scheme achieves a higher ergodic secrecy sum rate than that of the secure OMA coordinated transmission scheme. It can be also observed from Figure G2(b) that the ergodic secrecy sum rate of the secure NOMA coordinated transmission scheme with fixed power becomes inferior to that of the secure OMA coordinated transmission scheme in the medium to high ρ regime, due to its reduced ESR scaling law of $\bar{N}_k$, as indicated by Corollary 1. Similarly, as can be observed from Figure G2(b), the secure NOMA coordinated transmission scheme achieves the highest ergodic secrecy sum rate versus K. Furthermore, the ergodic secrecy sum rates of all the schemes increase with the same slope in the large K region, which confirms Corollaries 1 and 2.

References

1 Gradshteyn I S, Ryzhik I M. Table of Integrals, Series, Products. San Diego, CA, USA: Academic, 2007

2 Leadbetter M R, Lindgren G, Rootzen H. Extremes and Related Properties of Random Sequences and Processes. New York: Springer-Verlag, 1983

3 Karagiannidis G K, Tsiftsis T A, Sagias N C. A closed-form upper-bound for the distribution of the weighted sum of Rayleigh variates. IEEE Commun Lett, 2005, 9: 589–591