SCIENCE CHINA
Information Sciences

• LETTER •

October 2021, Vol. 64 209302:1–209302:2
https://doi.org/10.1007/s11432-020-3015-y

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*

Received 4 May 2020/Revised 14 July 2020/Accepted 21 July 2020/Published online 1 September 2021

Citation Lv L, Li Z, Ding H Y, et al. Secure NOMA and OMA coordinated transmission schemes in untrusted relay networks. Sci China Inf Sci, 2021, 64(10): 209302, https://doi.org/10.1007/s11432-020-3015-y

Dear editor,

Safeguarding physical-layer non-orthogonal multiple access (NOMA) transmissions using relays has been received widespread attention [1, 2]. However, a relay may be data-level untrusted and serve as an eavesdropper to decode its forwarded messages. Hence, information security needs to be guaranteed if an untrusted relay is involved.

In the literature, only limited studies (such as [3–6]) studied secure NOMA against an untrusted relay, where a typical two-user scenario (one near user and one far user) is considered. Up to now, a multi-user NOMA with an untrusted relay has not been investigated yet. Theoretically, in a multi-user scenario, an appropriate joint design of user scheduling and cooperative jamming can significantly improve the signal reception quality of the legitimate users as well as degrading the decoding capability of the untrusted relay, which is beneficial to the physical-layer security. Furthermore, although the use of NOMA increases the ergodic secrecy sum rate, the ergodic secrecy rate (ESR) of the far user does not increase with the signal-to-noise ratio (SNR) but converges to a constant in the high SNR regime [6]. This fails to balance the rate performance between the near user and far user and cannot promise user fairness. How to design a user fairness oriented secrecy transmission scheme is still not known.

Motivated by the above observations, this work investigates a secrecy transmission design for untrusted relay networks with multiple near users and a far user, where novel secure NOMA and OMA coordinated transmission schemes are proposed to combat an untrusted relay. The performance of the proposed schemes is evaluated theoretically and numerically. The results show that the NOMA scheme achieves a high sum ESR, while the OMA scheme balances the ESR between the near user and far user, thereby guaranteeing user fairness with secrecy considerations.

System model and scheme description. We consider a cooperative network with a source S, an untrusted relay R, a far user F, and K near users $\{N_1,\ldots,N_K\}$. The direct S-F channel does not exist owing to severe path-loss attenuation. Thus, S communicates with F via R, while directly communicating with $\{N_1,\ldots,N_K\}$. All wireless channels are assumed to be reciprocal and quasi-static with independent Rayleigh fading. The channel between nodes i and j is denoted by $h_{ij}\sim\mathcal{CN}(0,\lambda_{ij})$ for $i,j\in\{s,r,f,1,\ldots,K\}$ and $i\neq j$. We assume that $\lambda_{sk}=\lambda_{sn}$, $\lambda_{rk}=\lambda_{rn}$, $k\in\mathcal{K}=\{1,\ldots,K\}$, and $\lambda_{sn}>\lambda_{sr}$. The additive white Gaussian noise at node i is denoted by $\eta_i\sim\mathcal{CN}(0,\lambda_0)$ for $i\in\{s,r,f,1,\ldots,K\}$.

(1) NOMA scheme. In the first time slot, assuming that N_k is scheduled as the receiving near user, S transmits a superimposed signal of x_k and x_f to N_k and R, where $x_k\in\mathcal{CN}(0,1)$ and $x_f\in\mathcal{CN}(0,1)$ are the signals intended for N_k and F. Simultaneously, the remaining $(K-1)$ near users (called jammers) cooperatively transmit a jamming signal $z\in\mathcal{CN}(0,1)$ to confuse R. The received signals at N_k and R are written as

$$y_i=\sqrt{\alpha_kP}h_{si}x_k+\sqrt{\alpha_fP}h_{si}x_f+\sqrt{P}\boldsymbol{h}_i\boldsymbol{f}_1z+\eta_i,\quad i\in\{k,r\},\tag{1}$$

where P is the transmit power, α_k and α_f are the power allocation coefficients satisfying $\alpha_k+\alpha_f=1$ and $\alpha_f>\alpha_k$, $\boldsymbol{h}_k$ and $\boldsymbol{h}_r$ denote the channels from jammers to N_k and R, and $\boldsymbol{f}_1$ denotes the beamforming vector. To guarantee that z will not affect the signal reception of N_k, the beamforming vector should be designed based on the zero-forcing metric, i.e., $\boldsymbol{h}_k\boldsymbol{f}_1=0$ and $\boldsymbol{f}_1^{\mathrm{H}}\boldsymbol{f}_1=1$. In this time slot, F can receive and cache z for the subsequent jamming cancellation.

In the second time slot, R forwards its received signals to F. To compensate the jamming service offered by the jammers, one jammer, say $\bar{N}_k$, is scheduled to receive its own signal $\bar{x}_k\in\mathcal{CN}(0,1)$ in this time slot. Coordinated with R's transmission, S transmits a superimposed signal of $\bar{x}_k$ and x_k to $\bar{N}_k$, where x_k is used to enable $\bar{N}_k$'s interference cancellation. The received signals at F and $\bar{N}_k$ are

$$y_f=\varphi_1h_{rf}y_r+\eta_f,\tag{2}$$

$$y_{\bar{k}}=\varphi_1h_{r\bar{k}}y_r+h_{s\bar{k}}(\sqrt{P-P_k}\bar{x}_k+w_kx_k)+\eta_{\bar{k}},\tag{3}$$

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

where $\varphi_1 = \sqrt{1/(\lambda_{sr} + \lambda_{rn} + 1/\rho)}$ is the relay amplifying gain, P_k is the transmit power of x_k, and w_k is the weighting coefficient of x_k satisfying $\mathbb{E}[|w_k|^2] = P_k$. Owing to R's half-duplex feature, it cannot listen to S's signal transmission, and the transmission of $\bar{x}_k$ is secured.

The detailed signal detection and performance metric are shown in Appendix A.

User scheduling. We propose an user scheduling criterion as follows:

$$k^* = \arg\max_{k\in\mathcal{K}} \gamma_{k:x_k}, \ \bar{k}^* = \arg\max_{\bar{k}\in\mathcal{K}\setminus k^*} \gamma_{\bar{k}:\bar{x}_k}, \quad (4)$$

where $\gamma_{k:x_k}$ and $\gamma_{\bar{k}:\bar{x}_k}$ are given in Appendix A.

Lemma 1. The user scheduling (4) is optimal in maximizing the secrecy rates of x_k, x_f, and $\bar{x}_k$.

Proof. See Appendix B.

(2) OMA scheme. In the first time slot, S transmits x_f to R and all $\{N_1, \ldots, N_K\}$ transmit z in a collaborative manner to intentionally confuse R. The received signals at R are given by

$$y_r = \sqrt{P} h_{sr} x_f + \sqrt{P} \boldsymbol{h}_{rn} \boldsymbol{f}_2 z + \eta_r, \quad (5)$$

where $\boldsymbol{h}_{rn}$ is the channels between $\{N_1, \ldots, N_K\}$ and R, and $\boldsymbol{f}_2$ is the beamforming vector given by $\boldsymbol{f}_2 = [h_{r1}^\dagger/|h_{r1}|, \ldots, h_{rK}^\dagger/|h_{rK}|]^{\mathrm{T}}$. In this slot, F also receives z and caches it for the subsequent jamming cancellation.

In the second time slot, R forwards its received signals to F and S coordinately transmit a superimposed signal of x_k and x_f to N_k, where x_f is aimed at N_k's interference cancellation. The received signals at F and N_k are

$$y_f = \varphi_2 h_{rf} y_r + \eta_f, \quad (6)$$

$$y_k = \varphi_2 h_{rk} y_r + h_{sk}\left(\sqrt{P - P_f} x_k + w_f x_f\right) + \eta_k, \quad (7)$$

where $\varphi_2 = \sqrt{1/(\lambda_{sr} + \bar{\mu}_r + 1/\rho)}$ denotes the relay amplifying gain in OMA with $\bar{\mu}_r = \mathbb{E}[\mu_r]$, P_f is the transmit power of x_f, and w_f is the weighting coefficient of x_f with $\mathbb{E}[|w_f|^2] = P_f$. While R cannot overhear the transmitted signals from S in this time slot owing to the half-duplex constraint.

The detailed signal detection and performance metric are discussed in Appendix C.

User scheduling. The near user who has the largest SNR is scheduled as follows:

$$k^* = \arg\max_{k\in\mathcal{K}} \hat{\gamma}_{k:x_k}, \quad (8)$$

where $\hat{\gamma}_{k:x_k}$ is defined in Appendix C. Clearly, this user scheduling maximizes the secrecy rate of x_k.

(3) Implementation. For the proposed schemes, the following channel state information (CSI) is assumed: S and N_k know h_{sr}, h_{sk}, and h_{rk} to set the weighting coefficients and perform cooperative jamming and user scheduling. The CSI can be estimated using the channel training method similar to [6], where details are omitted owing to page limit.

Using the available CSI, user scheduling can be implemented in a distributed manner. To be specific, each N_k uses a virtual timer and sets an initial value for the timer in inversely proportional to $\gamma_{k:x_k}$ and $\gamma_{\bar{k}:\bar{x}_k}$ in NOMA and $\hat{\gamma}_{k:x_k}$ in OMA. The near user whose timer expires first is selected as the best one for signal reception.

Main results. We derive the ESR lower bound and its scaling law.

Theorem 1. The NOMA scheme achieves a positive sum ESR, which indicates that perfect secrecy is definitely guaranteed.

Proof. See Appendix D.

Corollary 1. With a finite K and $\rho \to \infty$, we obtain that: (1) the ESR of N_k scales as $\frac{1}{2}\log\rho$; (2) the ESR of $\bar{N}_k$ scales as $\frac{1}{2}\log\rho$, which is achieved by the power allocation of $\alpha_f = \frac{c}{\rho}$ given a positive constant c, otherwise, the ESR of $\bar{N}_k$ converges to a constant; (3) the ESR of F converges to a constant.

When ρ is limited and $K \to \infty$, we achieve that: (1) the ESR of N_k scales as $\frac{1}{2}\log\log K$; (2) the ESR of $\bar{N}_k$ scales as $\frac{1}{2}\log\log(K-1)$; (3) the ESR of F finally converges to a constant.

Proof. See Appendix E.

Theorem 2. The OMA scheme achieves a positive sum ESR, thus ensuring perfect secrecy.

Proof. See Appendix F.

Corollary 2. With a finite K and $\rho \to \infty$, the ESRs of N_k and F both scale as $\frac{1}{2}\log\rho$.

When ρ is limited and $K \to \infty$, we obtain that: (1) the ESR of N_k scales as $\frac{1}{2}\log\log K$; (2) the ESR of F converges to a constant.

Proof. Similar to the proof of Corollary 1.

Simulation results are provided in Appendix G to verify the derived analytical results and demonstrate the secrecy enhancement of the proposed schemes.

Discussion. The proposed schemes can be extended to a scenario with multiple far users. For both NOMA and OMA schemes, one best far user who has the largest received SINR is chosen as the receiver to enhance the signal reception quality.

The proposed schemes can also be extended to a multiple-relay scenario, where all relays perform distributed beamforming to forward the received signals to the far user. The beamforming vector $\boldsymbol{f}_2$ of the near users is designed to simultaneously jam all relays.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61901313, 61941105, 61825104, 61771366), Natural Science Basic Research Plan of Shaanxi Province (Grant No. 2020JQ-306), and Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (Grant No. 2020D07).

Supporting information Appendixes A–G. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Lei H J, Yang Z X, Park K H, et al. Secrecy outage analysis for cooperative NOMA systems with relay selection schemes. IEEE Trans Commun, 2019, 67: 6282–6298

2 Li B, Qi X H, Huang K, et al. Security-reliability tradeoff analysis for cooperative NOMA in cognitive radio networks. IEEE Trans Commun, 2019, 67: 83–96

3 Arafa A, Shin W, Vaezi M, et al. Secure relaying in non-orthogonal multiple access: trusted and untrusted scenarios. IEEE Trans Inform Forensic Secur, 2020, 15: 210–222

4 Xiang Z W, Yang W W, Pan G F, et al. Secure transmission in non-orthogonal multiple access networks with an untrusted relay. IEEE Wirel Commun Lett, 2019, 8: 905–908

5 Lv L, Zhou F H, Chen J, et al. Secure cooperative communications with an untrusted relay: a NOMA-inspired jamming and relaying approach. IEEE Trans Inform Forensic Secur, 2019, 14: 3191–3205

6 Lv L, Jiang H, Ding Z G, et al. Secrecy-enhancing design for cooperative downlink and uplink NOMA with an untrusted relay. IEEE Trans Commun, 2020, 68: 1698–1715