Physical Layer Security for 5G Non-orthogonal Multiple Access in Large-scale Networks

Zhijin Qin[†], **Yuanwei Liu** [†], Zhiguo Ding [♯], Yue Gao[†] and Maged Elkashlan [†]
[†] Queen Mary University of London, London, UK
[♯] Lancaster University, Lancaster, UK

December 17, 2016

Outline

Key Advantages of NOMA

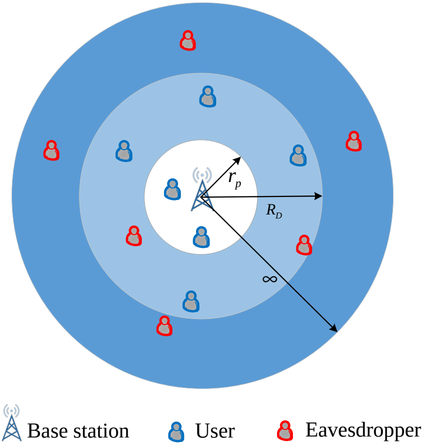
- High spectrum efficiency
- Ultra-high connectivity (e.g. IoT scenarios)
- Well compatibility: ”add-on” technique to any existing OMA techiniques (e.g., TDMA/FDMA/CDMA/OFDMA)
- Open flexibility and low complexity compared to other existing non-orthogonal techniques (e.g., SCMA/MUSA/PDMA)

Security Issue in NOMA Networks

- Susceptibility to physical capture
- The use of insecure wireless communication channels
- SIC decoding at the receiver side, which makes the use of public key cryptography bring much complexity
- Strong detection ability at the eavesdropper side

Physical layer security is therefore important in protecting the secure transmission of NOMA networks.

Network Model



- Network model for the NOMA transmission protocol under malicious attempt of eavesdroppers in large-scale networks, where r_p, R_D, and ∞ are the radius of the protected zone, NOMA user zone, and an infinite two dimensional plane for eavesdroppers, respectively.

Network Model

- One BS (Alice) communicates with M users (Bobs) by applying the NOMA transmission protocol under the malicious attempt of eavesdroppers (Eves).
- The M randomly deployed Bobs are uniformly distributed within the disc.
- The spatial topology of all Eves are modeled using homogeneous poisson point processes (PPPs), denoted by Φ_e with density λ_e.
- all the channels between Alice and Bobs follow the order of $|h_1|^2 \leq \cdots |h_m|^2 \leq \cdots |h_n|^2 \leq \cdots |h_M|^2$.
- It is considered that the m-th user (poor user) and the n-th user (good user) are paired to perform NOMA.

Network Model—SINR for NOMA users

Based on the aforementioned assumptions, the instantaneous signal-to-interference-plus-noise ratio (SINR) for the *m*-th user and signal-to-plus-noise ratio (SNR) for the *n*-th user can be given by

$$\gamma_{B_m} = \frac{a_m |h_m|^2}{a_n |h_m|^2 + \frac{1}{\rho_b}}, \tag{1}$$

and

$$\gamma_{B_n} = \rho_b a_n |h_n|^2, \tag{2}$$

respectively. We denote $\rho_b = \frac{P_A}{\sigma_b^2}$ as the transmit SNR, where P_A is the transmit power at Alice and σ_b^2 is the variance of additive white Gaussian noise (AWGN) at Bobs.

Network Model—SNR for the Eavesdroppers

The instantaneous SNR for detecting the information of the m-th user and the n-th user at the most detrimental Eve can be expressed as follows:

$$\gamma_{E_\kappa} = \rho_e a_\kappa \max_{e\in\Phi_e, d_e \geq r_p} \left\{ |g_e|^2 L\left(d_e\right) \right\}. \tag{3}$$

It is assumed that $\kappa \in \{m, n\}$, $\rho_e = \frac{P_A}{\sigma_e^2}$ is the transmit SNR with σ_e^2 is the variance of AWGN at Eves.

- In this paper, we assume that Eves can be detected if they are close enough to Alice. Therefore, a protect zone with radius r_p is introduced to keep Eves away from Alice.

Secrecy Outage Probability

The secrecy rate of the *m*-th user and the *n*-th user can be expressed as

$$I_m = [\log_2(1+\gamma_{B_m}) - \log_2(1+\gamma_{E_m})]^+, \tag{4}$$

and

$$I_n = [\log_2(1+\gamma_{B_n}) - \log_2(1+\gamma_{E_n})]^+, \tag{5}$$

respectively, where $[x]^+ = \max\{x, 0\}$.

Exact Secrecy Outage Probability

Given the expected secrecy rate R_m and R_n for the m-th and n-th users, a secrecy outage is declared when the instantaneous secrecy rate drops below R_m and R_n, respectively. Based on (4), the secrecy outage probability for the m-th and n-th user is given by

$$\begin{aligned} P_m\left(R_m\right) &= \Pr\left\{I_m < R_m\right\} \\ &= \int_0^\infty f_{\gamma_{E_m}}\left(x\right) F_{\gamma_{B_m}}\left(2^{R_m}\left(1+x\right)-1\right) dx. \end{aligned} \tag{6}$$

and

$$\begin{aligned} P_n\left(R_n\right) &= \Pr\left\{I_n < R_n\right\} \\ &= \int_0^\infty f_{\gamma_{E_n}}\left(x\right) F_{\gamma_{B_n}}\left(2^{R_n}\left(1+x\right)-1\right) dx, \end{aligned} \tag{7}$$

respectively.

Exact Secrecy Outage Probability

We define the secrecy outage probability for the selected user pair as that of either the *m*-th user or the *n*-th user outage. Hence, the secrecy outage probability for the selected user pair can be expressed as

$$P_{mn} = 1 - (1 - P_m)(1 - P_n)\,. \tag{8}$$

- We consider the secrecy outage occurs in the *m*-th user and the *n*-th user are independent. In other words, the secrecy outage probability of the *m*-th user has on effect on that of the *n*-th user and vice versa.

Secrecy Diversity Analysis

The secrecy diversity order can be given by

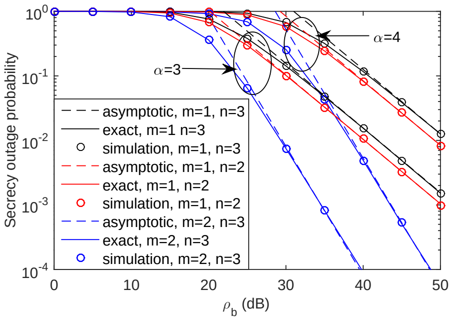
$$d_s = -\lim_{\rho_b \to \infty} \frac{\log\left(P_m^\infty + P_n^\infty - P_m^\infty P_n^\infty\right)}{\log \rho_b} = m, \tag{9}$$

The asymptotic secrecy outage probability for the user pair can be expressed as

$$P_{mn}^\infty = P_m^\infty + P_n^\infty - P_m^\infty P_n^\infty \approx P_m^\infty G_m(\rho_b)^{-D_m}. \tag{10}$$

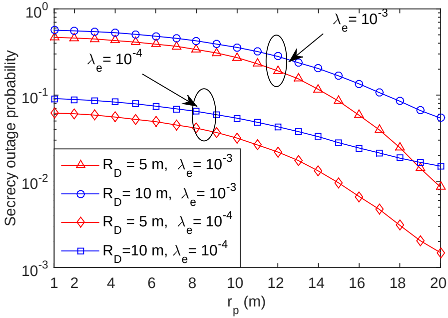
Remarks: It indicates that the secrecy diversity order and the asymptotic secrecy outage probability for the user pair are determined by the *m*-th user.

Numerical Results



- The red curves and the black curves have the same slopes. While the blue curves can achieve a larger secrecy outage slope.
- It is due to the fact that the secrecy diversity order of the user pair is determined by the poor one *m*.
- This phenomenon also consists with the obtained insights in **Remark 1**.

Numerical Results



- The secrecy outage probability decreases as the radius of the protected zone increases, which demonstrates the benefits of the protected zone.
- Smaller density λ_e of Eves can achieve better secrecy performance, because smaller λ_e leads to less number of Eves, which lower the multiuser diversity gain when the most detrimental Eve is selected.

Conclusions

- In this paper, the secrecy performance of applying NOMA protocol in large-scale networks was examined.
- Stochastic geometry approaches were used to model the locations of NOMA users and eavesdroppers in the considered networks.
- New analytical expressions were derived in terms of the secrecy outage probability to determine the system secrecy performance.
- The secrecy diversity order of the user pair was also characterized. It was analytically demonstrated that the secrecy diversity order was determined by the poor one of the user pair.
- It was concluded that enhancing the secrecy performance can be achieved by enlarging the scope of the protected zone or reducing the scope of the user zone.

Promising Future Directions

- Physical layer security on MIMO-NOMA systems
- Enhance PLS with relay and jamming selection in cooperative NOMA
- Power allocation on secrecy enhancement for NOMA
- Energy constraint/efficient NOMA transmission
- Interplay between NOMA and cognitive radio
- Fairness issues in NOMA systems
- Efficient dynamic user paring/clustering algorithms design for MIMO-NOMA/Hybrid-MA systems

- Thank you for your attention.
- Questions?