Hindawi
Security and Communication Networks
Volume 2020, Article ID 8868550, 6 pages
https://doi.org/10.1155/2020/8868550

Research Article

Secrecy Performance Analysis of the NOMA System on High-Speed Railway

Wenwu Xie, Jinxia Yang, Xinzhong Liu, Zhihe Yang, Xin Peng, Jianwu Liao, and Tingyu Huang

School of Information Science and Engineering, Hunan Institute of Science and Technology, Yueyang, Hunan 414006, China

Correspondence should be addressed to Xinzhong Liu; liuxinzhong@hnist.edu.cn

Received 15 August 2020; Revised 20 November 2020; Accepted 8 December 2020; Published 22 December 2020

Academic Editor: Zhe-Li Liu

High-speed railway (HSR) wireless communications are required to ensure strict security. In this work, we study the secrecy performance of a nonorthogonal multiple access- (NOMA-) aided HSR wireless communication system in the case of an eavesdropping user. Specifically, applying NOMA technology to the HSR communication system can effectively improve the data rates. Therefore, we study the secrecy performance of the downlink NOMA system under the HSR wireless communication. In particular, the exact analytical results for the secrecy outage probability (SOP) based on no small-scale channel state information (CSI) are derived. We also provide all of the parameterizations for the proposed channel model. Finally, the correctness of theoretical derivation is verified via simulations. Results show the positive effect of utilizing the NOMA for enhancing wireless systems secrecy performance.

1. Introduction

Recently, the rapid development of HSR has brought great convenience to people's travel. At the same time, high quality and data rate wireless communication are required for passenger services. The high-speed movement of HSR has brought about problems such as the wireless Doppler effect and signal shielding in train compartments, which will cause a series of phenomena, such as the difficulty of a mobile phone call and poor voice signal quality. Thus, railway transportation communication becomes an interesting topic. Researchers have carried out research on improving the data rate on HSR wireless communication in various aspects [1–3]. For example, the traditional multiple antenna and beamforming technology are introduced into the HSR scenario for the first time in [1] where the security capacity and SOP are compared and analyzed. In addition to the security requirements, the high broadband services for passengers are required. Therefore, the authors in [2] proposed the tapped delay line model for a MIMO channel in HSR scenarios. Compared with the existing channel model, the MIMO channel model is efficient and yet flexible in the HSR environment. More recently, to satisfy the fifth generation (5G) on HSR, the authors in [3] focus on the study of channel modeling combined with the 5G technology such as multiple-input multiple-output (MIMO) and millimeter-wave (mm wave). Hence, applying 5G technology to HSR wireless communication is to be a significant work for future wireless systems.

As a major technology of 5G, nonorthogonal multiple access (NOMA) can schedule multiple users with the same time-frequency resources. Combined with the successive interference cancellation (SIC) technology, multiple signals can be sent and demodulated at the same time, which can effectively improve the spectrum efficiency [4]. In [5], the performance of downlink NOMA is studied by calculating the BER of perfect and imperfect SIC conditions; compared to the orthogonal multiple access (OMA) techniques, the NOMA technique can provide better performance gains. Thus, the authors in [6] analyzed and compared the performance of different NOMA schemes applied in HSR scenarios and proved that choosing the right NOMA scheme has a great effect on improving the data rate in HSR. However, in practice, it is challenging to ensure the

security of data transmission in HSR wireless communication.

In recent years, based on Wyner's eavesdropping channel model, the main indicators to measure the secrecy of wireless communication systems are secrecy outage probability (SOP) and average secrecy capacity (ASC). In the research of physical layer security, the CSI of each channel affects the secrecy performance of the system. Generally, the sources knew the CSI of the main channel. For the CSI of the eavesdropping channel, if the eavesdropping terminal is active eavesdropping, we use ASC to quantify the security performance of the system. Otherwise, we use SOP to measure communication security [7]. The authors in the literature [8] analyse the secrecy performance of the different systems by calculating SOP and ASC.

In this work, we study the secrecy performance of the downlink NOMA system for HSR. More specifically, we assume that no small-scale CSI of the channels is known; hence, the channels are sorts according to distances between the base station and the legitimate users. Besides, we consider that the system model exists as a static eavesdropper near the base station. To measure the secrecy performance of the system, the paper provides a closed-form expression for the SOP, and the simulation results show the positive effect of applying the NOMA for improving the system secrecy performance for HSR.

2. System Methods

In the HSR scenario, the secure communication mode of the downlink NOMA system is shown in Figure 1. The base station (BS) is located at the track side, and the height of the BS transmitting antenna relative to the horizontal plane is h_z. The legitimate user is the passenger on the HSR. We denote the length of the HSR is L_t, the vertical distance between the base station and HSR is l_z, the distance between the legitimate user and the vertical point of the base station is x, and the distance between the legitimate user and the BS transmitting antenna is d_u. HSR runs away from the BS according to the speed v from the nearest position to the BS. There is a static eavesdropper at the distance d_e, which attempts to obtain the information from the BS. Also, this paper makes the following assumptions: (1) all users and BS are equipped with a single antenna, and the legitimate users communicate directly with the BS; (2) the legitimate users are fixed on the HSR, and the distance between the two users follows the uniform distribution with $L_u/2$ mean; and (3) the legitimate channel is composed of Rician fading and large-scale fading [9].

2.1. Main Link. According to the NOMA scheme, the transmitted signal from BS to all of the legitimate users can be expressed as

$$x = \sum_{l=1}^{M} \sqrt{\alpha_l P_t} x_l, \tag{1}$$

where α_l is the power allocation factor with $\sum_{l=1}^{M} \alpha_l = 1$, set $\alpha_1 < \alpha_2 < \cdots < \alpha_M$, P_t is the transmitting power of the BS, and x_l is the transmission signal of the l^{th} user. Then, the signal received by the k^{th} legitimate user U_k can be expressed as

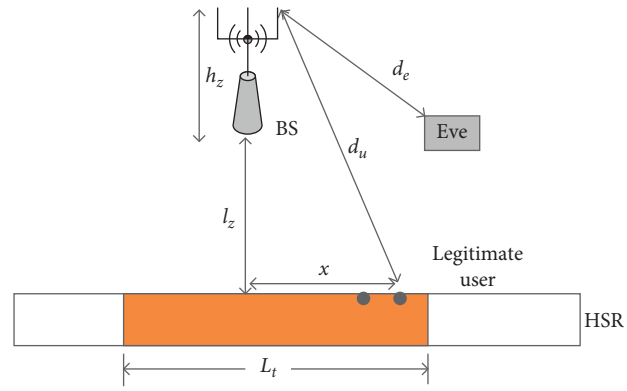

Figure 1: System model.

$$y_k = g_k \sum_{l=1}^{M} \sqrt{\alpha_l P_t} x_l + n_k, \tag{2}$$

where n_k follows the additive white Gaussian noise (AWGN) with the mean zero and variance σ_k^2. For simplicity, the variance is assumed to $\sigma_1^2 = \sigma_2^2 = \cdots = \sigma^2$. The channel gain between the k^{th} legitimate user and the BS can be given by $g_k = h_k \beta_k^{1/2}$, where h_k and β_k represent small-scale and large-scale fading, respectively, and the expression of β_k is related to the distance d_k. Set $d_1 < d_2 < \cdots < d_M$; according to order statistics, the probability density function (PDF) of d_k from the BS to the k^{th} nearest legitimate user is given by [9]

$$f_{d_k}(x) = k \binom{M}{k} \sum_{j=0}^{M-k} (-1)^j \binom{M-k}{j} \frac{x\left(\sqrt{x^2 - h_z^2 - l_z^2}\right)^{k+j-2}}{L_t^{k+j}}, \tag{3}$$

where $\sqrt{h_z^2 + l_z^2} < x \le \sqrt{L_t^2 + h_z^2 + l_z^2}$. According to the knowledge of the successive interference cancellation (SIC) receiver [10], for the k^{th} user, the signal-to-interference-plus-noise ratio (SINR) of the k^{th} user can be expressed as

$$\gamma_{D_k} = \frac{\rho \alpha_k |h_k|^2 \beta_k}{\rho |h_k|^2 \beta_k \sum_{l=1}^{k-1} \alpha_l + 1}, \tag{4}$$

where P_t is the transmitted power, and $\rho = P_t/\sigma^2$ is denoted as the average signal-to-noise ratio (SNR). In equation (6), since the small-scale fading channel h_k is the Rician fading channel, we define $\overline{\gamma} = s^2 + 2\lambda_k^2$. Thus, the $|h_k|^2$ is the noncentral chi-square random variable with two degree of freedom, and its PDF and cumulative distribution function (CDF) are given as [11]

$$f_{|h_k|^2}(y) = \frac{(1+K)e^{-K}}{\overline{\gamma}} \exp\left[-\frac{(1+K)y}{\overline{\gamma}}\right] I_0 \cdot \left(2\sqrt{\frac{(1+K)Ky}{\overline{\gamma}}}\right), \quad y > 0, \tag{5}$$

$$F_{|h_k|^2}(y) = 1 - Q_1\left(\sqrt{2K}, \frac{\sqrt{y}}{\lambda_k}\right),$$

where $I_0(x)$ is the modified Bessel function of the zero kind, and $Q_1(a,b)$ is the first order Marcum Q-function [12]. $K = s^2/2\lambda_k^2$ denotes the Rician factor, and similar to [9], we generally set $K = 7\,\mathrm{dB}$ on HSR scenario. Therefore, the conditional CDF of the $F_{|g_k|^2|d_k}(y|d_k)$ can be obtained as

$$F_{|g_k|^2|d_k}(y|d_k) = 1 - Q_1\left(\sqrt{2K}, \frac{\sqrt{\beta^{-1}(d_k)y}}{\lambda_k}\right), \tag{6}$$

where $\beta(d_k) = d_k^{-\chi}$, and χ is the path loss exponent. Since the small-scale fading and the large-scale fading are independent of each other. According to equations (3) and (6), the CDF of $|g_k|^2$ can be written as

$$\begin{aligned} F_{|g_k|^2}(y) &= \int_{\sqrt{h_z^2+l_z^2}}^{\sqrt{L_t^2+h_z^2+l_z^2}} F_{|g_k|^2|d_k}(y|x) f_{d_k}(x)\mathrm{d}x \\ &= \int_{\sqrt{h_z^2+l_z^2}}^{\sqrt{L_t^2+h_z^2+l_z^2}} \left(1 - Q_1\left(\sqrt{2K}, \frac{\sqrt{\beta^{-1}(x)y}}{\lambda_k}\right)\right) k \binom{M}{k} \sum_{j=0}^{M-k} (-1)^j \binom{M-k}{j} \frac{x\left(\sqrt{x^2 - h_z^2 - l_z^2}\right)^{k+j-2}}{L_t^{k+j}} \mathrm{d}x. \end{aligned} \tag{7}$$

Unfortunately, evaluating the integrals in equation (7) is very difficult. Thus, by using the Gauss–Chebyshev quadrature [13], equation (7) can be approximated as

$$\begin{aligned} F_{|g_k|^2}(y) = \sum_{i=1}^{n} \frac{\pi k}{4n} &\left(1 - Q_1\left(\sqrt{2K}, \frac{\sqrt{c_1 y}}{\lambda_k}\right)\right) \binom{M}{k} \\ &\cdot \sum_{j=0}^{M-k} (-1)^j \binom{M-k}{j} \left(\sqrt{\frac{t_i+1}{2}}\right)^{k+j-2} \sqrt{1-t_i^2}, \end{aligned} \tag{8}$$

where $c_1 = \beta^{-1}(((t_i+1)/2)L_t^2 + h_z^2 + l_z^2)$, $t_i = \cos((2i-1)/2n)\pi$, and n is the approximate order of Chebyshev, which can be selected according to the accuracy and complexity requirements.

Then, the CDF of γ_{D_k} can be readily formulated as

$$\begin{aligned} F_{\gamma_{D_k}}(z) &= P\left(\frac{\rho\alpha_k|g_k|^2}{\rho|g_k|^2\sum_{l=1}^{k-1}\alpha_l + 1} < z_k\right) \\ &= \sum_{i=1}^{n} \left(\frac{\pi k}{4n}\left(1 - Q_1\left(\sqrt{2K}, \frac{1}{\lambda_k}\sqrt{\frac{c_1 z_k}{\rho\left(\alpha_k - \sum_{l=1}^{k-1}\alpha_l z_k\right)}}\right)\right) \binom{M}{k} \sum_{j=0}^{M-k} (-1)^j \binom{M-k}{j} \left(\sqrt{\frac{t_i+1}{2}}\right)^{k+j-2} \sqrt{1-t_i^2}\right). \end{aligned} \tag{9}$$

2.2. Eavesdropping Link. For the eavesdropper, we assume that the eavesdropper attempts to obtain the signal coming from the direct link, and the eavesdropping link is also a hybrid channel similar to the main link. Moreover, the small-scale fading v_k of eavesdropping link experiences independent Rayleigh distribution, and the received signal of an eavesdropper can be expressed as

$$y_E = q_k \sum_{l=1}^{M} \sqrt{\alpha_l P_t} x_l + n_e, \tag{10}$$

where $q_k = v_k \beta_{ek}^{1/2}$ is the channel gain, $\beta_{ek} = d_e^{-\chi}$ represents the large-scale fading, which is related to the distance d_e between the eavesdropper and the BS, and $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ is the AWGN at the eavesdropper. Assuming that the eavesdropper has a strong decoding ability to the transmitted signals, the eavesdropper can decode the mixed signal s to obtain separate signals x_l [14]. Hence, the received SNR of the eavesdropper is given by

$$\gamma_{E_k} = \frac{\alpha_k \rho_e |q_k|^2}{\rho_e |q_k|^2 \sum_{l=1}^{k-1}\alpha_l + 1}, \tag{11}$$

where $\rho_e = P_t/\sigma_e^2$ is the average SNR. Similarly, $|q_k|^2$ is an exponent distribution random variable with parameter η_k. For simplicity, set $\eta_1 = \eta_2 = \cdots = \eta_M$. Then, the PDF of γ_{E_k} can be expressed as

Table 1: Simulation parameter configuration.

Index	Variable/Unit	Value	Description
1	Lt/m	201	Train length
2	Hz/m	30	BS height
3	lz/m	100	Horizontal distance between BS and rail
4	K/dB	7	Rician channel factor
5	fc/MHz	2.5*e*3	Carrier frequency
6	v/Km/h	350	Speed
7	B/MHz	10	Bandwidth
8	Rs/KHz	4.8	Rate
9	kai/dB	3	Attenuation factor
10	SNR_SD	20	Legitimate user SNR
11	SNR_SE	10	Eavesdropping user SNR
12	M	2	Number of the legitimate user

$$f_{\gamma_{E_k}}(y)=\begin{cases}\dfrac{\alpha_k}{\eta_k\rho_e\beta_{ek}\left(\alpha_k-\sum_{l=1}^{k-1}\alpha_l y\right)^2}e^{-y/\left(\eta_k\beta_{ek}\left(\alpha_k\rho_e-\rho_e\Sigma_{l=1}^{k-1}\alpha_l y\right)\right)}, & y<\dfrac{\alpha_k}{\sum_{l=1}^{k-1}\alpha_l},\\ 0, & y\geq\dfrac{\alpha_k}{\sum_{l=1}^{k-1}\alpha_l}.\end{cases}\tag{12}$$

3. Performance Analysis

SOP is a typical performance metrics to analyse the secrecy performance for physical layer secrecy, which is defined that the instantaneous secrecy rate is less than a certain threshold. In this section, we analyse the SOP to determine the security of using NOMA in the HSR scenario. Since the main channel and eavesdropping channel are independent, the SOP of the user U_k can be expressed as [7]

$$\begin{aligned}\mathrm{SOP}&=\Pr\left\{\ln\left(1+\gamma_{D_k}\right)-\ln\left(1+\gamma_{E_k}\right)<C_{\mathrm{th}}\right\}\\&=\int_0^{\infty}F_{\gamma_{D_k}}\left(\theta\gamma_{E_k}+\theta-1\right)f_{\gamma_{E_k}}\left(\gamma_{E_k}\right)\mathrm{d}\gamma_{E_k},\end{aligned}\tag{13}$$

where C_{th} is the target secrecy rate, and $\theta=e^{C_{\mathrm{th}}}$. Then, by using the Gauss–Laguerre [13] and substituting (9) and (13) into (14), we can obtain the approximate expression of SOP as

$$\begin{aligned}\mathrm{SOP}=&\sum_{j=1}^{m}\sum_{i=1}^{n}w\left(x_j\right)e^{x_j}\frac{\pi}{4n}\left(1-Q_1\left(\sqrt{2K},\frac{\sqrt{\beta^{-1}\left(\sqrt{((t_i+1)/2)L_t^2+h_z^2+l_z^2}\right)\left(\theta x_j+\theta-1\right)}}{\lambda_u\sqrt{\rho\left(\alpha_k-\sum_{l=1}^{k-1}\alpha_l\left(\theta x_j+\theta-1\right)\right)}}\right)\right)\\&\times\frac{\sqrt{((t_i+1)/2)L_t^2+h_z^2+l_z^2}}{\sqrt{(t_i+1)/2}}\sqrt{1-t_i^2}\ \frac{\alpha_k}{\eta_k\rho_e\beta_{ek}\left(\alpha_k-\sum_{l=1}^{k-1}\alpha_l x_j\right)^2}e^{-x_j/\left(\eta_k\beta_{ek}\left(\alpha_k\rho_e-\rho_e\sum_{l=1}^{k-1}\alpha_l x_j\right)\right)},\end{aligned}\tag{14}$$

where N is the approximate order terms of Laguerre, $w_j=x_j/\left((m+1)^2[L_{m+1}(x_j)]^2\right)$, and $j<33$ is the weight of Laguerre polynomial x_j.

4. Simulation and Analysis

In this section, we present a numerical example to illustrate our analytical results, and the simulation parameters are shown in Table 1 [15].

In Figure 2, we plot the SOP versus transmitted power P_t in the presence of an eavesdropper based on the NOMA scheme on the HSR scenario. It is observed that the analytical results match well with the simulation, which verifies the theoretical derivation. Moreover, increasing the number of P_t results in decreasing SOP for two users. As expected, we note that floors appear at relatively high P_t. Therefore, the SOP of the near user is much better than the far user based on the NOMA scheme. Finally, to improve the performance of SOP, we can increase the transmitting power which is not the only scheme but needs to be optimized together with other schemes to ensure the security of communication.

In Figure 3, we present the SOP curves for the different distances between the eavesdropper and BS. As can be observed, a better secrecy performance will be obtained with the increases of d_e. More specifically, the slopes of performance curves of near users are large than the far users; while $d_e>100$, the change trend of SOP is gentle. Thus, the change

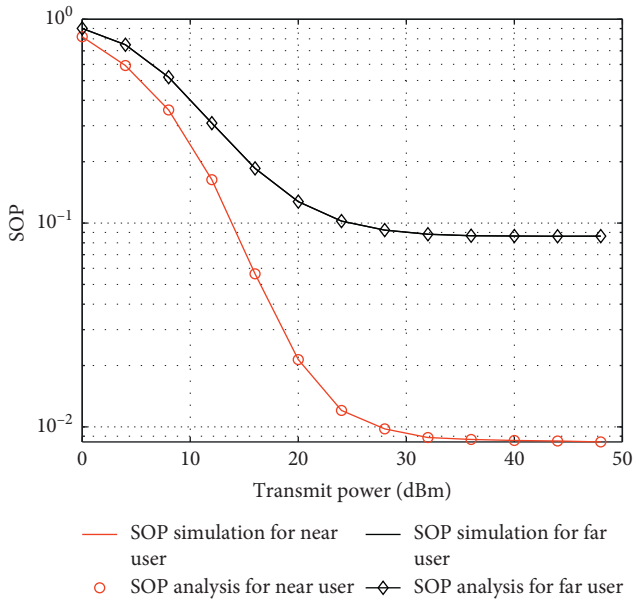

Figure 2: SOP curve of P_t for near user and far user.

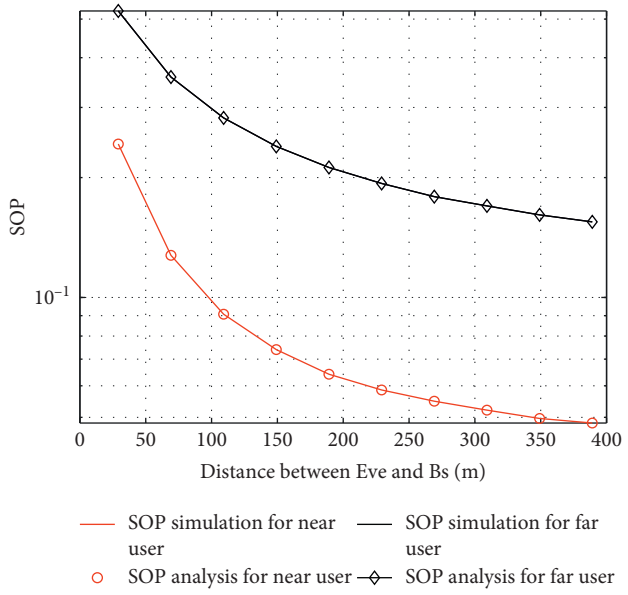

Figure 3: SOP curve of d_e for near user and far user.

of the distance between the eavesdropper and BS has a greater impact on the secrecy performance of the near users than on far users.

In Figure 4, we plot the SOP versus for a different power allocation coefficient α_1 of near user based on the NOMA scheme. It is clearly shown that increasing α_1 near users can significantly improve the near user secrecy performance, and the impact of α_1 on near users is greater than that on far users from the slope of the SOP versus. Thus, it is necessary to select an appropriate α_1 to ensure secure communication in both near user and far user.

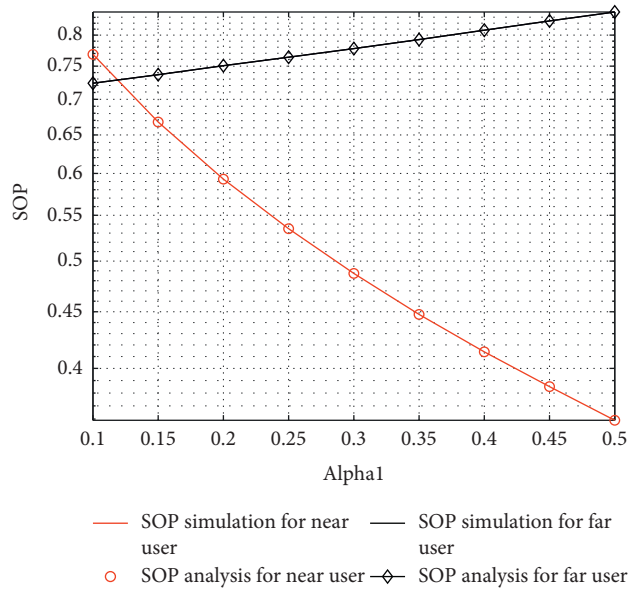

Figure 4: SOP curve of α_1 for near user and far user.

5. Conclusions

In this work, we provide secrecy performance analysis for the HSR scenario in the presence of an eavesdropper with the help of NOMA. More specially, the expression for SOP was derived and verified by simulation. Numerical results showed that the secrecy performance can be improved by choosing the appropriate power allocation coefficient α_1 based on the NOMA scheme.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Wenwu Xie and Xin Peng conceived and designed the study. Xinzhong Liu and Zhihe Yang performed the simulations. Jinxia Yang wrote the paper. All authors reviewed and edited the manuscript. All authors read and approved the final manuscript.

Acknowledgments

This work was in part supported by the National Natural Science Foundation of China (No. 61772195), the Hunan Natural Science Foundation (Nos.2019JJ40043, 2018JJ2154, and 2018JJ2156), the Key Research Foundation of Education Bureau of Hunan Province (No.18A320), the Outstanding Youth Project of Hunan Provincial Education Department (Nos.18B353 and 19K037), the Hunan Emergency Communication Engineering Technology Research Centre (No.2018TP2022), the Hunan Institute of Science and Technology for Postgraduate (No.YCK2020A38), the Hunan

Province for Postgraduate (No.CX20201139), and the National College Student Innovation and Entrepreneurship Training Program (s202010543042).

References

[1] Y. P. Cui and X. M. Fang, "A physical layer secure wireless communication scheme for high speed railway," in *Proceedings of the Sixth International Workshop on Signal Design and Its Applications in Communications*, pp. 114–117, Tokyo, Japan, November 2013.

[2] J. Yang, B. Ai, S. Salous et al., "An efficient MIMO channel model for LTE-R network in high-speed train environment," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3189–3200, 2019.

[3] T. Zhou, H. Li, Y. Wang, L. Liu, and C. Tao, "Channel modeling for future high-speed railway communication systems: a survey," *IEEE Access*, vol. 7, pp. 52818–52826, 2019.

[4] Y. Liang, X. Li, J. Zhang, and Z. Ding, "Non-orthogonal random access for 5G networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, pp. 4817–4831, 2017.

[5] M. R. Usman, A. Khan, M. A. Usman, Y. S. Jang, and S. Y. Shin, "On the performance of perfect and imperfect SIC in downlink non orthogonal multiple access (NOMA)," in *Proceedings of the International Conference on Smart Green Technology in Electrical and Information Systems (ICSGTEIS)*, pp. 102–106, Bali, Indonesia, October 2016.

[6] D. Feng, "Performance comparison on NOMA schemes in high speed scenario," in *Proceedings of the 2019 IEEE 2nd International Conference on Electronics Technology (ICET)*, pp. 112–116, Chengdu, China, May 2019.

[7] Z. Liao, L. Yang, J. Chen, H.-C. Yang, and M.-S. Alouini, "Physical layer security for dual-hop VLC/RF communication systems," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2603–2606, 2018.

[8] H. Lei, Z. Yang, K.-H. Park et al., "Secrecy outage analysis for cooperative NOMA systems with relay selection schemes," *IEEE Transactions on Communications*, vol. 67, no. 9, pp. 6282–6298, 2019.

[9] J. Fan, J. Zhang, S. Chen, J. Zheng, and B. Ai, "The application of NOMA on high-speed railway with partial CSI," in *Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pp. 1–5, Honolulu, HI, USA, September 2019.

[10] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, "Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 4, pp. 938–953, 2016.

[11] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, Wiley-Interscience, New York, NY, USA, 2 edition, 2005.

[12] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic, San Diego, CA, USA, 7 edition, 2007.

[13] F. B. Hildebrand, *Introduction to Numerical Analysis*, Courier Corporation, North Chelmsford, MA, USA, 1987.

[14] G. Brante, H. Alves, R. D. Souza, and M. Latva-aho, "Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter," *IEEE Transactions on Communications*, vol. 63, no. 4, pp. 1330–1342, 2015.

[15] F. Hasegawa, A. Taira, G. Noh et al., "High-speed train communications standardization in 3GPP 5G NR," *IEEE Communication Standard. Magazine*, vol. 2, no. 1, pp. 44–52, 2018.