Impact of Wireless Backhaul and Imperfect Channel Estimation on Secure Communication Networks

Cheng Yin[1(✉)], Xinkai Cheng[2], Yijiu Li[1], and Haoran Liu[1]

[1] Queen's University Belfast, Belfast, UK
{cyin01,yli84,hliu18}@qub.ac.uk
[2] Wuhan University of Science and Technology, Wuhan, China

Abstract. This paper investigates the system performance of secure communication networks under unreliable backhaul and imperfect channel estimation. We first incorporate a transmitter selection approach that could achieve maximize signal-to-noise ratio at the receiver to improve secrecy performance. Then we derive the closed-form expressions of the secrecy outage performance under the impact of wireless backhaul and imperfect channel estimation. Our Monte-Carlo simulations verify that the analytical results match the simulation well, therefore validating the correctness of our expressions. Our theoretical analysis and simulations reveal the influence of the number of transmitters, the backhaul reliability, the channel estimation errors and the position of the eavesdropper on the secrecy system performance.

Keywords: Wireless backhaul · Imperfect channel estimation · Secure communication network

1 Introduction

In the fifth generation (5G) and beyond, there is a significant demand for massive connections among people, machines, and environments. A large number of wireless devices bring threats to network security. According to the broadcast nature, transmission is vulnerable to be attacked [3]. Therefore, it is a challenge to secure wireless network. The conventional approach to secure systems is mainly based on cryptography applied in high layers and assuming perfect physical layer with zero-error. In addition, the conventional method requires a large amount of power for encrypting and decrypting, which is not desirable for lightweight devices. Thus, physical layer security (PLS) has attracted increasing attention to meet the challenges in wireless communications.

Several studies have made a remarkable contribution to the literature by investigating the secrecy system performance in the presence of an eavesdropper [1,2,5–8,14,16,18–21]. However, all these works assume that the backhaul and

Supported by organization x.

N.-S. Vo et al. (Eds.): INISCOM 2022, LNICST 444, pp. 231–240, 2022.
https://doi.org/10.1007/978-3-031-08878-0_16

the channel estimation are perfect, which is ideal and unrealistic in practical future wireless communication systems. For instance, the authors investigated energy harvesting relay networks with an eavesdropper without considering the impact of unreliable backhaul and channel estimation on the system secrecy performance [14].

Wireless backhaul connections need to be deployed for future high dense networks. Conventional backhaul, such as copper and optical fibre, are highly reliable, but the deployment cost is high [4,17]. Wireless backhaul is a promising alternative to wired ones with lower cost. However, it suffers from unreliability because of non-LOS propagation, and channel fading [12]. There has been research considering wireless backhaul in cooperative system [11] and PLS scenarios [10,23] and the results prove that backhaul unreliability has shown negatively impact on the system performance [9]. Therefore, it is crucial to take undesirable outcomes of the wireless backhaul into account in the performance analysis in future wireless systems.

Several existing works in secure communications considered unreliable backhaul in performance analysis [10,23], however the authors assume that the channel estimation is perfect at the receiver side, which is not achievable in practical wireless systems [24]. The impact of imperfect channel state information (CSI) on system performance has been studied in secure communication systems [13,15,22]. In [13], the authors considered the influence of imperfect CSI in a wireless powered communication network with multiple eavesdroppers. Furthermore, a secure cellular vehicle-to-everything network was proposed, and the impact of imperfect CSI on system performance was considered [15]. In addition, a secure massive MIMO system with imperfect CSI has been proposed, and the authors analysed the impacts of imperfect CSI on the system secrecy performance [22].

Motivated by the above research, we study the system performance with the impact of both wireless backhaul unreliability and imperfect channel estimation in this work. As far as we know, this work, for the first time, addresses both the wireless backhaul unreliability and channel estimation uncertainties in wireless system performance analysis.

2 System Model

We investigate a secure communication network, consisting of a macro base station S connected to K small-cell transmitters, $T_{\{1,\cdots,K\}}$, via unreliable backhaul links, a receiver, D, in presence of an eavesdropper, E, as in Fig. 1. A selected transmitter T_k^* sends its information to D while E is listening to the transmission from the transmitter to the destination. Reliability of the k^{th} backhaul is modelled as a Bernoulli process $\mathbb{I}_k$. The success probability is defined as s_k, where $\mathbb{P}(\mathbb{I}_{k^*} = 1) = s_k$ and $\mathbb{P}(\mathbb{I}_{k^*} = 0) = 1 - s_k$, which demonstrates that T_k forwards the message to the destination via the wireless backhaul with success probability s_k and unsuccessful probability $1 - s_k$. All the channels are supposed to undergo Rayleigh fading. In addition, the transmitters and the receiver are equipped with single antenna.

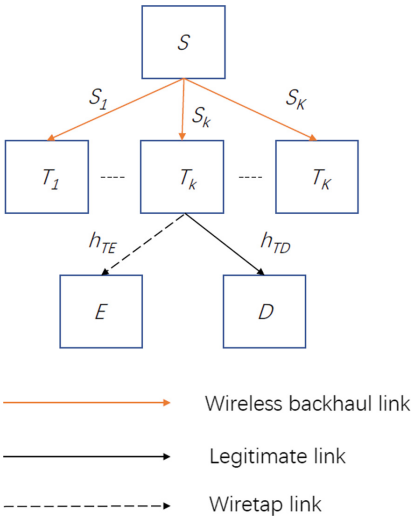

Fig. 1. System model

An sub-optimal transmitter selection approach is applied, the transmitter T_k^* with the largest SNR at D is selected as the best to forward the information to D, i.e.,

$$k^* = \arg \max_{1 \le k \le K} \mathrm{SNR}_{T_k D}, \tag{1}$$

where k^* indicates the index of the selected transmitter and $\mathrm{SNR}_{T_k D}$ is the SNR of the link from T_k to D. In addition, $h_{T_{k^*} D}$, $h_{T_{k^*} E}$ are the channel coefficient link from the selected transmitter T_k^* to D and E.

In practical systems, channel state information (CSI) cannot be perfectly obtained at D. We assume that the receiver D and the eavesdropper E estimate the CSI of $\widehat{h}_{T_{k^*} D}$, $\widehat{h}_{T_{k^*} E}$ and perform imperfect channel estimation of $h_{T_{k^*} D}$, $h_{T_{k^*} E}$ as follow,

$$h_{T_{k^*} D} = \widehat{h}_{T_{k^*} D} + e_{TD}, \tag{2}$$

$$h_{T_{k^*} E} = \widehat{h}_{T_{k^*} E} + e_{TE}, \tag{3}$$

where e_{TD} and e_{TE} represent the estimation error, i.e., $e_{TD} \sim CN(0, \epsilon_D^2)$,$e_{TE} \sim CN(0, \epsilon_E^2)$. According to channel estimation, $\epsilon_D = E[|h_{T_{k^*} D}|^2] - E[|\widehat{h}_{T_{k^*} D}|^2]$, similarly, $\epsilon_E = E[|h_{T_{k^*} E}|^2] - E[|\widehat{h}_{T_{k^*} E}|^2]$, where $E[\cdot]$ represents the expectation. We assume that all the channel estimation errors follow the same distribution, $e \sim CN(0, \epsilon^2)$.

Taking into account the selected transmitter T_k^*, E experiences the SNR without wireless backhaul. Therefore, the received information at the receiver D and eavesdropper E are of the following forms,

$$y_D = \sqrt{P_T}(\widehat{h}_{T_{k^*}D} + e)\mathbb{I}_{k^*}x + z, \tag{4}$$

$$y_E = \sqrt{P_T}(\widehat{h}_{T_{k^*}E} + e)x + z, \tag{5}$$

where x is the unit power transmitted symbol of the transmission and P_T is the transmitted power of T_{k^*}. We assumed that D and E are experienced by the same noise indicated by z, which represents the complex additive white Gaussian noise (AWGN) with zero mean and variance σ, i.e., $z \sim CN(0, \sigma^2)$.

3 SNR Distributions

To assess the secrecy system performance, the SNR distributions at E and D need to be firstly derived. According to Eqs. 4 and 5, the received SNRs at E and D from the selected transmitter T_k^* can be written as,

$$SNR_{k^*D} = \frac{P_0\widehat{h}_{T_{k^*}D}\mathbb{I}_{k^*}}{P_0\epsilon\mathbb{I}_{k^*} + 1}, \tag{6}$$

$$SNR_{T_{k^*}E} = \frac{P_0\widehat{h}_{T_{k^*}E}}{P_0\epsilon + 1}, \tag{7}$$

where $P_0 = P_T/\sigma^2$. As all the channels follow Rayleigh fading, the cumulative distribution function (CDF) and probability density function (PDF) of the channel associated with the unreliable backhaul are,

$$F(x) = 1 - s_k \exp(-\lambda x), \tag{8}$$

$$f(x) = s_k\lambda \exp(\lambda x), \tag{9}$$

where s_k indicates the backhaul unreliability from the macro base station to the selected transmitter T_k^*. Therefore, the CDF of SNR_{kD} are derived utilizing Eq. 8,

$$F_{SNR_{kD}}(x) = 1 - s_k \exp(-\frac{\lambda_D(P_0\epsilon\mathbb{I}_k + 1)x}{P_0}). \tag{10}$$

The best transmitter T_k^* is selected according to the sub-optimal selection rule described in Eq. 1, thus the CDF of SNR_{k^*D} with the best transmitter is,

$$F_{SNR_{k^*D}}(x) = F_{SNR_{kD}}(x)^K. \tag{11}$$

Similarly, the CDF and PDF of E are can be obtained as follows,

$$F_{SNR_{T_{k^*}E}}(x) = 1 - \exp(-\frac{-\lambda_E(P_0\epsilon + 1)x}{P_0}), \tag{12}$$

$$f_{SNR_{T_{k^*}E}}(x) = \frac{-\lambda_E(P_0\epsilon + 1)x}{P_0} \exp(-\frac{-\lambda_E(P_0\epsilon + 1)x}{P_0}). \tag{13}$$

In this section, we obtain the SNR distributions of the links from the selected transmitter T_k^* to D and E. Then, we derive the CDF of PDF of the related SNR distributions under the impact of wireless backhaul and channel estimation imperfections. In the next section, we will assess the system secrecy performance.

4 Secrecy Performance Analysis

In this section, we investigate the secrecy system performance under the impact of wireless backhaul and imperfect channel estimation. We derive the secrecy outage probability (SOP) utilizing the SNR distributions given in the above section. SOP is an metric which has been widely used to assess the system performance, it is defined as the secrecy capacity being below a certain threshold θ. To achieve the general results working in most cases with wireless backhaul and imperfect channel estimation in practice, we measure the SOP in terms of two scenarios: (1) single transmitter and (2) multiple K transmitters.

Firstly, we derive the SOP with a single transmitter with both wireless backhaul and channel estimation imperfection. The expression is derived as follows,

$$\begin{aligned} F(\theta) &= \int_0^\infty F_{SNR_{k_D}}(2^{2\theta}(1+x) - 1) f_{SNR_{T_k E}}(x) dx \\ &= s_k \exp(-\frac{\lambda_D(P_0\epsilon\mathbb{I}_k + 1)(2^{2\theta} - 1)}{P_0}) \\ &\quad \frac{\lambda_E(P_0\epsilon + 1)}{\lambda_D(P_0\epsilon\mathbb{I}_k + 1)2^{2\theta} + \lambda_E(P_0\epsilon + 1)}. \end{aligned} \tag{14}$$

Next, we consider a more practical scenario that multiple transmitter exist. According to the sub-optimal selection rule introduced in Eq. 11, the SOP can be derived as,

$$\begin{aligned} F_k(\theta) &= \int_0^\infty F_{SNR_{k^*D}}(2^{2\theta}(1+x) - 1) f_{SNR_{T_{k^*}E}}(x) dx \\ &= 1 + \sum_1^K \binom{K}{k} (-1)^k {s_k}^k \exp(-\frac{\lambda_D(P_0\epsilon\mathbb{I}_k + 1)k(2^{2\theta} - 1)}{P_0}) \\ &\quad \frac{\lambda_E(P_0\epsilon + 1)}{\lambda_D(P_0\epsilon\mathbb{I}_k + 1)k2^{2\theta} + \lambda_E(P_0\epsilon + 1)}. \end{aligned} \tag{15}$$

Compare with Eq. 14, Eq. 15 is power to the number of transmitter K, due to Eq. 14 is smaller than 1, Eq. 15 is smaller than Eq. 14 on the condition that K is larger than 1. This illustrates that increasing the number of transmitter leads to a lower SOP and better system secrecy performance.

5 Numerical Results

We evaluate the numerical results with Monte-Carlo simulations. The threshold θ of SOP is assumed to be 1 bits/s/Hz. We also assume that the positions of transmitters, receiver and eavesdropper are located in Cartesian coordinate system, which are $T_k = (0,0)$, $D = (1,0)$ and $E = (4,1)$. The distance between every two nodes is written as $d_{ab} = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$, where $a, b = \{T_k, D, E\}$. It is also assumed that the average SNR of transmission link depends on the pass loss pl: $1/\lambda = 1/d_{ab}^{pl}$, and pl is 4. The variance of channel estimation errors is modelled as $\epsilon^2 = \frac{\omega}{1+\delta p \omega}$, where ω and p are the variance of channel gains and the average transmit SNR, and δ indicates the channel quality parameter. In the following figures, we use 'Sim' to indicate the simulation results, and 'Ana' to indicate the analytical results.

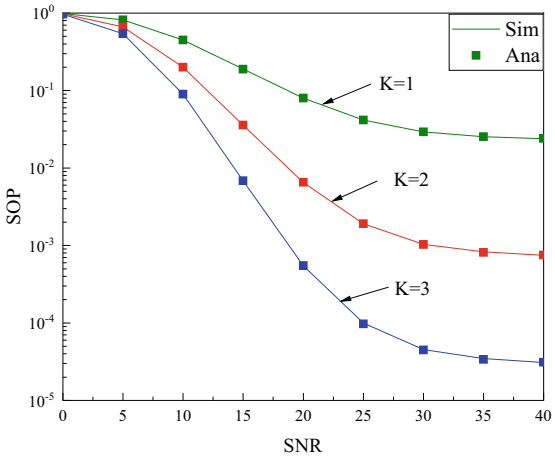

Fig. 2. The influence of the number of transmitter K on the SOP

Figure 2 illustrates the influence of the number of transmitter K on the SOP. Wireless backhaul reliability s is assumed to be 0.99, the position of E is (4,1) and K is an integer ranging from 1 to 3. As shown in the figure, with the increase of K, SOP decreases significantly. This is because with the increase number of transmitters, there are more choices to transmit to the destination, thus showing better secrecy system performance. In another aspect, the reason of presenting increasing performance can be refereed to Sect. 4. The SOP of the scenario with multiple transmitter is powered to K compared with the SOP with single transmitter, and SOP is smaller than 1, so the SOP becomes smaller after powering to K when K is greater than 1. Therefore, when the number of transmitter grows, the system achieves better performance.

Figure 3 shows the impact of backhaul unreliability on SOP. The position of E is (4,1) and $K = 3$. As shown in the figure, the system has a lower SOP

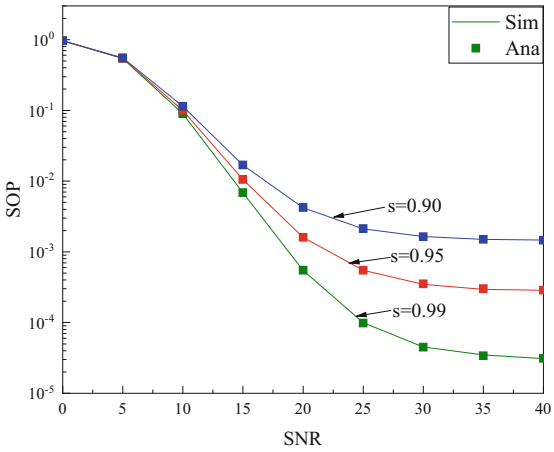

Fig. 3. The influence of backhaul reliability s on the SOP

when s becomes larger. This indicates that when the wireless backhaul is more reliable, the system has better performance.

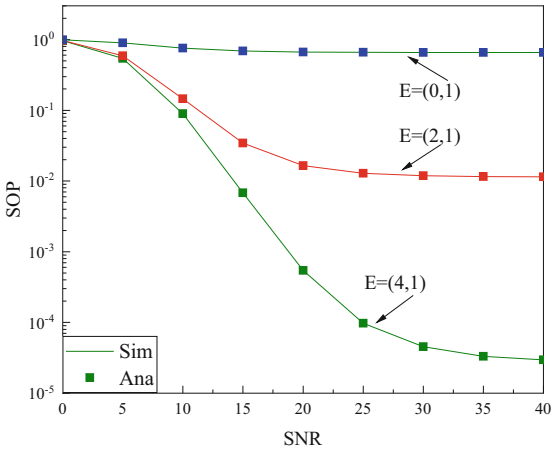

Fig. 4. The influence of the position of the eavesdropper E on the SOP

Figure 4 presents the impact the position of the eavesdropper E on SOP. The number of transmitter K equals 3 and $s = 0.99$. We consider two scenarios: 1) The distance between the transmitter and the receiver is the same as that from the transmitter to the eavesdropper; 2) The eavesdropper locates further than the receiver. The position of E is assumed to dynamic from (0,1), (2,1) to (4,1). The eavesdropper locates at (0,1) indicates that the distance between

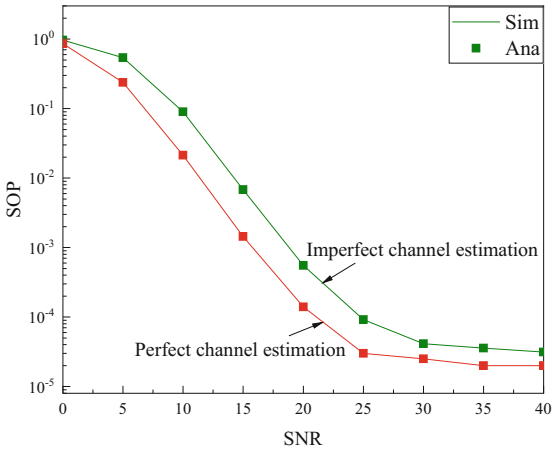

Fig. 5. Comparison of perfect channel estimation and imperfect channel estimation

the transmitter and the receiver is the same as that from the transmitter to the eavesdropper. The figure shows that the SOP almost achieve 1 no matter how the SNR changes. This means that when the distance between the transmitter and the eavesdropper is smaller or equal to the distance between the transmitter and the receiver, it is difficult to secure the wireless security in physical layer aspects, more approaches need to be applied to enhance security. In addition, when E locates (2,1) and (4,1), the SOP decreases obviously. This illustrates that the system could obtain better secrecy performance when the distance between the transmitter and eavesdropper increases.

Figure 5 shows the impact of channel estimation imperfection on system secrecy performance and compares the differences between perfect and imperfect channel estimations in secure wireless networks. We could observe a clearly gap between these two cases, the SOP with the perfect channel estimation is lower than that with imperfect channel estimation. The figure demonstrates that the SOP is significantly affected by the channel estimation errors.

6 Conclusion

This paper fills the gap in exploring the system secrecy performance of secure communication network under unreliable backhaul and imperfect channel estimation. The remarkable contribution is the novel derivation of the closed-form expressions of secrecy outage probability under both wireless backhaul and channel estimation imperfections. In addition, we reveal the impact of backhaul unreliability and channel uncertainty on system secrecy performance. Our results show that when the wireless backhaul is more reliable, the system has better performance. The system secrecy performance with perfect and imperfect channel estimation is also compared, the SOP with perfect channel estimation is

lower than that of imperfect channel estimation. Moreover, we discuss the influence of the number of transmitters and the location of the eavesdropper on the secrecy outage probability. The results show that the system performs better when the number of transmitter increase. Furthermore, when the distance between the transmitter to the eavesdropper is larger, the system presents better performance. However, when the distance between the transmitter to the eavesdropper is equal or smaller than that from the transmitter to the destination, the system cannot be secured. In this situation, more approaches needs to be deployed to secure the wireless system.

References

1. Fan, L., Lei, X., Duong, T.Q., Elkashlan, M., Karagiannidis, G.K.: Secure multiuser communications in multiple amplify-and-forward relay networks. IEEE Trans. Commun. **62**(9), 3299–3310 (2014)
2. Fan, L., Yang, N., Duong, T.Q., Elkashlan, M., Karagiannidis, G.K.: Exploiting direct links for physical layer security in multiuser multirelay networks. IEEE Trans. Wirel. Commun. **15**(6), 3856–3867 (2016)
3. Fan, L., Zhang, S., Duong, T.Q., Karagiannidis, G.K.: Secure switch-and-stay combining (SSSC) for cognitive relay networks. IEEE Trans. Commun **64**(1), 70–82 (2015)
4. Ge, X., Cheng, H., Guizani, M., Han, T.: 5G wireless backhaul networks: challenges and research advances. IEEE Netw. **28**(6), 6–11 (2014)
5. Hoang, T.M., Duong, T.Q., Suraweera, H.A., Tellambura, C., Poor, H.V.: Cooperative beamforming and user selection for improving the security of relay-aided systems. IEEE Trans. Commun. **63**(12), 5039–5051 (2015)
6. Hu, J., Shu, F., Li, J.: Robust synthesis method for secure directional modulation with imperfect angle information. IEEE Commun. Lett. **20**(16), 1084–1087 (2016)
7. Hu, J., Yan, S., Shu, F., Wang, J., Li, J., Zhang, Y.: Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays. IEEE Access **5**, 1658–1667 (2017)
8. Huang, Y., Wang, J., Zhong, C., Duong, T.Q., Karagiannidis, G.K.: Secure transmission in cooperative relaying networks with multiple antennas. IEEE Trans. Wirel. Commun. **15**(10), 6843–6856 (2016)
9. Khan, T.A., Orlik, P., Kim, K.J., Heath, R.W.: Performance analysis of cooperative wireless networks with unreliable backhaul links. IEEE Commun. Lett. **19**(8), 1386–1389 (2015)
10. Kim, K.J., Khan, T.A., Orlik, P.V.: Performance analysis of cooperative systems with unreliable backhauls and selection combining. IEEE Trans. Veh. Technol. **66**(3), 2448–2461 (2017)
11. Kim, K.J., Orlik, P.V., Khan, T.A.: Performance analysis of finite-sized cooperative systems with unreliable backhauls. IEEE Trans. Wirel. Commun. **15**(7), 5001–5015 (2016)
12. Kim, K.J., Yeoh, P.L., Orlik, P.V., Poor, H.V.: Secrecy performance of finite-sized cooperative single carrier systems with unreliable backhaul connections. IEEE Trans. Signal Process. **64**(17), 4403–4416 (2016)
13. Li, M., Yin, H., Huang, Y., Wang, Y., Yu, R.: Physical layer security of WPCNs with imperfect CSI and full-duplex receiver aided jamming. IEEE Access **7**, 55318–55328 (2019)

14. Nguyen, N.P., Duong, T.Q., Ngo, H.Q., Hadzi-Velkov, Z., Shu, L.: Secure 5g wireless communications: a joint relay selection and wireless power transfer approach. IEEE Access **4**, 3349–3359 (2016)
15. Qiu, B., Xiao, H., Chronopoulos, A.T., Zhou, D., Ouyang, S.: Optimal access scheme for security provisioning of C-V2X computation offloading network with imperfect CSI. IEEE Access **8**, 9680–9691 (2020)
16. Shu, F., Wu, X., Li, J., Chen, R., Vunetic, B.: Robust synthesis scheme for mult-beam directional modulation in broadcasting systems. IEEE Access **5**, 6614–6623 (2016)
17. Tipmongkolsilp, O., Zaghloul, S., Jukan, A.: The evolution of cellular backhaul technologies: current issues and future trends. IEEE Commun. Surv. Tutor. **13**(1), 97–113 (2011)
18. Wang, L., Elkashlan, M., Huang, J., Tran, N.H., Duong, T.Q.: Secure transmission with optimal power allocation in untrusted relay networks. IEEE Wirel. Commun. Lett. **3**(3), 289–292 (2014)
19. Wang, L., Kim, K.J., Duong, T.Q., Elkashlan, M., Poor, H.V.: Security enhancement of cooperative single carrier systems. IEEE Trans. Inf. Forensics Secur. **10**(1), 90–103 (2015)
20. Yan, S., Yang, N., Geraci, G., Malaney, R., Yuan, J.: Optimization of code rates in SISOME wiretap channels. IEEE Trans. Wirel. Commun. **14**(11), 6377–6388 (2015)
21. Yan, S., Yang, N., Malaney, R., Yuan, J.: Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels. IEEE Trans. Wirel. Commun. **13**(3), 1656–1667 (2014)
22. Yang, T., Zhang, R., Cheng, X., Yang, L.: Secure massive MIMO under imperfect CSI: performance analysis and channel prediction. IEEE Trans. Inf. Forensics Secur. **14**(6), 1610–1623 (2018)
23. Yin, C., Nguyen, H.T., Kundu, C., Kaleem, Z., Garcia-Palacios, E., Duong, T.Q.: Secure energy harvesting relay networks with unreliable backhaul connections. IEEE Access **6**, 12074–12084 (2018)
24. Yoo, T., Goldsmith, A.: Capacity and power allocation for fading MIMO channels with channel estimation error. IEEE Trans. Inf. Theory **52**(5), 2203–2214 (2006)