Journal of Southeast University (English Edition) Vol. 32, No. 3, pp. 261 - 266 Sept. 2016 ISSN 1003—7985

Joint jammer and user scheduling scheme for wireless physical-layer security

Ding Xiaojin[1] Song Tiecheng[1] Zou Yulong[2] Chen Xiaoshu[1]

([1]National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China)

([2]School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: In order to improve the performance of the security-reliability tradeoff (SRT), a joint jammer and user scheduling (JJUS) scheme is proposed. First, a user with the maximal instantaneous channel capacity is selected to transmit its signal to the base station (BS) in the transmission time slot. Then, when the user transmits its signal to BS, the jammer is invoked for transmitting artificial noise in order to perturb the eavesdropper's reception. Simulation results show that increasing the number of users can enhance the SRT performance of the proposed JJUS scheme. In addition, the SRT performance of the proposed JJUS scheme is better than that of the traditional round-robin scheduling and pure user scheduling schemes. The proposed JJUS scheme can guarantee the secure transmission even in low main-to-eavesdropper ratio(MER) regions.

Key words: security-reliability tradeoff (SRT); multi-user scheduling; artificial noise; physical-layer security

DOI: 10.3969/j.issn.1003 - 7985.2016.03.001

The security aspects of multi-user scheduling with the limited radio resource have attracted increasing attention from academia, as the eavesdroppers may be deployed around the legitimate users to intercept the confidential information deliberately. In order to consider the fairness between multiple users, a round-robin scheduling scheme was investigated in Ref. [1], wherein each user has the same chance to access the radio resource. In Ref. [2], robust rate adaptation and robust proportional fair (PF) scheduling were presented. In general, if a legitimate user with low instantaneous channel gain is selected in the time slot, neither the instantaneous transmit rate will be adjusted to meet the demand of the reliability, nor the transmit power will be improved according to the transmit rate. Meanwhile, the low instantaneous transmit rate or high transmit power will increase the risk of being intercepted by the eavesdroppers. Thus, more attention should be paid to the security issues caused by the multi-user scheduling schemes. Moreover, in Ref. [3], untrusted nodes were explored, which attempt to deceive the legitimate users into tapping wireless transmissions.

Physical-layer security[4] is emerging as an effective approach to improving the security of wireless communications. In Refs. [5 - 6], MIMO schemes were explored to improve the security of wireless communications. In Refs. [7 - 8], beamforming techniques were investigated, which are used for enhancing secure transmissions. Moreover, relay selection schemes[9-10] can be used in the enhancement of the physical-layer security of wireless communications. As an alternative, jamming schemes[11-14] were explored to improve the SRT performance. In Ref. [15], the round-robin scheduling scheme and the optimal and suboptimal user scheduling scheme were proposed to improve the security of CUs-CBS transmissions. Moreover, the secrecy outage of the proposed scheduling schemes was analyzed. Both the instantaneous channel gain of the main links and that of wiretap links were considered in Ref. [15]. However, the instantaneous channel gains of wiretap links are difficult to estimate, as the eavesdroppers are silent.

Although extensive research efforts had been devoted to improving the SRT performance of the multi-user scheduling network, less attention has been paid to the joint jammer and user scheduling network. Motivated by the above considerations, we investigate a wireless multi-user network in the presence of multiple eavesdroppers and one jammer. Furthermore, different from Refs. [11 - 15], we take both jammer and multi-user scheduling into account, and analyze the SRT performance. The main contributions of this paper are summarized as follows. 1) We propose a JJUS scheme to improve the SRT of a wireless multi-user scheduling network. 2) We present the mathematical SRT analysis of the proposed JJUS scheme as well as the round-robin scheme. 3) It is shown that the proposed JJUS scheme outperforms the round-robin scheme in terms of the SRT, even in very low MER regions.

1 System Model and Multi-user Scheduling

1.1 System model

As shown in Fig. 1, we investigate a wireless network

Received 2016-02-21.

Biographies: Ding Xiaojin (1981—), male, graduate; Song Tiecheng (corresponding author), male, doctor, professor, songtc@seu.edu.cn.

Foundation items: The National Natural Science Foundation of China (No. 61271207, 61372104), the Science and Technology Project of SGCC(No. SGRIXTKJ[2015]349).

Citation: Ding Xiaojin, Song Tiecheng, Zou Yulong, et al. Joint jammer and user scheduling scheme for wireless physical-layer security[J]. Journal of Southeast University (English Edition), 2016, 32(3): 261 - 266. DOI: 10.3969/j.issn.1003 - 7985.2016.03.001.

consisting of one base station, denoted by BS, and N users, denoted by $U=\{U_i \mid i=1,2,\ldots,N\}$, in the presence of one jammer, denoted by J, and M eavesdroppers, denoted by $E=\{E_l \mid l=1,2,\ldots,M\}$, where E is assumed to be inside the coverage area of both J and U, which means that E can overhear the signal transmitted by both U and J. All transmission links are modeled as Rayleigh fading channels. Let h_{ib}, h_{ie_l}, h_{jb} and h_{je_l}, $i\in\{1,2,\ldots,N\}$, $l\in\{1,2,\ldots,M\}$, denote the U_i-BS, U_i-E_l, J-BS and J-E_l channels gain, respectively. We assume that the channel coefficients h_{ib}, h_{ie_l}, h_{jb} and h_{je_l} are mutually independent zero-mean complex Gaussian random variables with variances σ_{ib}^2, $\sigma_{ie_l}^2$, σ_{jb}^2 and $\sigma_{je_l}^2$, respectively.

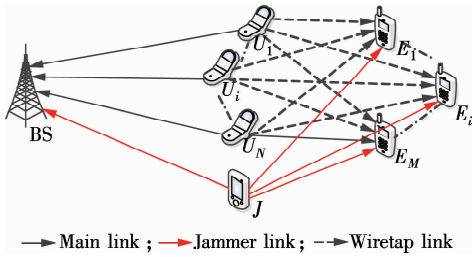

Fig. 1 A wireless network consisting of one base station, multiple users, multiple eavesdroppers and one jammer

The transmit powers of U and J are denoted by P_s and P_j, respectively. The thermal noise received at any node is modeled as a complex Gaussian random variable with zero mean and variance N_0, denoted by n_b and n_{e_l}, respectively. Meanwhile, let x_s and x_j denote the signal transmitted by the users and jammer, respectively. Without loss of generality, we assume $E[\,|x_s|^2\,]=1$, where $E[\,\cdot\,]$ represents the expected value operator. Similarly to x_s, we assume $E[\,|x_j|^2\,]=1$. Furthermore, J transmits the artificial noise to disrupt the eavesdroppers. Due to the broadcast nature of the wireless channels, the artificial noise will tamper BS inevitably. In order to accord with the actual systems, due to the channel state information (CSI) estimation error, the artificial noise will interfere with both the legitimate destination and the eavesdroppers, which are called self-interfering and jamming, respectively. The self-interfering factor and jamming factor are denoted by ρ and η, respectively.

1.2 Model of wireless transmissions

Given a time slot, a user will be selected to transmit its signal to BS. Without loss of generality, we assume that U_i is selected to transmit its signal at this time slot. In addition, J is adopted for transmitting the artificial noise simultaneously. Hence, the received signal at BS can be given by

$$y_{ib}=\sqrt{P_s}h_{ib}x_i+\sqrt{\rho P_j}h_{jb}x_j+n_b \tag{1}$$

From Eq. (1), the capacity of the U_i-BS channel is obtained in the presence of a jammer as

$$C_{ib}=\log_2\left(1+\frac{|h_{ib}|^2\gamma_s}{\rho|h_{jb}|^2\gamma_j+1}\right) \tag{2}$$

where $\gamma_s=P_s/N_0$ and $\gamma_j=P_j/N_0$.

Meanwhile, the U_i-BS channel can be overheard by E_l, and the received signal at E_l can be shown as

$$y_{ie_l}=\sqrt{P_s}h_{ie_l}x_i+\sqrt{\eta P_j}h_{je_l}x_j+n_{e_l} \tag{3}$$

From Eq. (3), we can obtain the capacity of the U_i-E_l channel in the presence of a jammer as

$$C_{ie_l}=\log_2\left(1+\frac{|h_{ie_l}|^2\gamma_s}{\eta|h_{je_l}|^2\gamma_j+1}\right) \tag{4}$$

In this paper, we consider that the eavesdroppers are independent of each other in intercepting the transmissions of the U_i-BS link, which means that the signal transmitted by U_i will be tapped successfully if any eavesdropper succeeds in decoding the signal. Thus, the overall capacity of U_i-E channels can be written as

$$C_{ie}=\max_l C_{ie_l}=\max_l\log_2\left(1+\frac{|h_{ie_l}|^2\gamma_s}{\eta|h_{je_l}|^2\gamma_j+1}\right) \tag{5}$$

1.3 Proposed joint jammer and user scheduling scheme

As aforementioned, the user will be selected to transmit its signal in the given time slot. This subsection presents a joint jammer and user scheduling (JJUS) scheme. In this scheme, a user with the maximal instantaneous capacity will be selected as the optimal user to transmit the signal to BS in the given time slot. Thus, the optimal user scheduling criterion can be shown as

$$o=\arg\max_i C_{ib} \tag{6}$$

where o denotes the index of the optimal user.

Using Eq. (2), Eq. (6) can be rewritten as

$$o=\arg\max_i\frac{|h_{ib}|^2\gamma_s}{\rho|h_{jb}|^2\gamma_j+1}=\arg\max_i|h_{ib}|^2 \tag{7}$$

2 SRT Analysis of Rayleigh Fading Channels

In this section, we analyze the security-reliability tradeoff of the traditional round-robin scheduling scheme and the proposed JJUS scheme.

2.1 Analysis of the traditional round-robin scheduling scheme

As a benchmark scheme, we analyze the traditional round-robin scheduling scheme firstly for comparison purposes. For the sake of a fair comparison with the scenario without jammer[15], the transmit powers of P_s and P_j are denoted by $P_s=P_j=\frac{P}{2}$, leading to $\gamma_s=\gamma_j=\frac{\gamma_p}{2}$, where P

denotes the transmit power of the main user[15], and $\gamma_p = \frac{P}{N_0}$. As aforementioned, the security and reliability can be quantified by the intercept probability and outage probability. Therefore, based on Ref. [16], the outage probability of U_i with the traditional round-robin scheme can be shown as

$$P_{o\_i} = \Pr(C_{ib} < R) \tag{8}$$

where R denotes the target rate of the wireless links.

Substituting Eq. (2) into Eq. (8), Eq. (8) can be rewritten as

$$P_{o\_i} = \Pr\left(\frac{|h_{ib}|^2}{\rho |h_{jb}|^2 \gamma_p + 2} < \Delta\right) \tag{9}$$

Denoting $X = |h_{jb}|^2$, it yields to

$$P_{o\_i} = 1 - \int_0^{\infty} \frac{1}{\sigma_{jb}^2} \exp\left(-\frac{x}{\sigma_{jb}^2} - \frac{\Delta\rho x\gamma_p + 2\Delta}{\sigma_{ib}^2}\right) dx = 1 - \frac{\sigma_{ib}^2}{\sigma_{ib}^2 + \Delta\rho\gamma_p\sigma_{jb}^2} \exp\left(-\frac{2\Delta}{\sigma_{ib}^2}\right) \tag{10}$$

where $\Delta = (2^R - 1)/\gamma_p$.

Based on Ref. [9], the signal can be intercepted when the channel capacity of the wiretap channel becomes larger than the data rate. Hence, we can obtain the intercept probability of U_i with the traditional round-robin scheme as

$$P_{t\_i} = \Pr(C_{ie} > R) \tag{11}$$

From Eq. (5), Eq. (10) can be rewritten as

$$P_{t\_i} = \Pr\left(\max_l \frac{|h_{ie_l}|^2}{\eta |h_{je_l}|^2 \gamma_p + 2} > \Delta\right) = 1 - \prod_l \Pr\left(\frac{|h_{ie_l}|^2}{\eta |h_{je_l}|^2 \gamma_p + 2} < \Delta\right) \tag{12}$$

Using Eq. (10), Eq. (12) can be shown as

$$P_{t\_i} = 1 - \prod_l \left(1 - \frac{\sigma_{ie_l}^2}{\sigma_{ie_l}^2 + \Delta\eta\gamma_p\sigma_{je_l}^2} \exp\left(-\frac{2\Delta}{\sigma_{ie_l}^2}\right)\right) = \sum_{k=1}^{2^M-1} (-1)^{|E_k|+1} \left(\frac{\sigma_{ie_l}^2}{\sigma_{ie_l}^2 + \Delta\eta\gamma_p\sigma_{je_l}^2}\right)^{|E_k|} \times \exp\left(-\sum_{l \in E_k} \frac{2\Delta}{\sigma_{ie_l}^2}\right) \tag{13}$$

where E_k denotes the k-th non-empty subset of the elements of E; $|E_k|$ is the cardinality of set E_k.

Meanwhile, in the round-robin scheduling scheme, all users can take turns in transmitting the signals to BS. Consequently, from Eqs. (10) and (13), the outage probability and intercept probability can be expressed as

$$P_o^{\text{robin}} = \frac{1}{N} \sum_{i=1}^{N} P_{o\_i} \tag{14}$$

$$P_t^{\text{robin}} = \frac{1}{N} \sum_{i=1}^{N} P_{t\_i} \tag{15}$$

2.2 Analysis of the proposed JJUS scheme

Based on Ref. [16], from Eq. (6), the outage probability of the proposed JJUS scheme can be shown as

$$P_o^{\text{JJUS}} = \Pr(\max_i C_{ib} < R) \tag{16}$$

Substituting Eq. (7) into Eq. (16), we have

$$P_o^{\text{JJUS}} = \Pr\left(\max_i \frac{|h_{ib}|^2}{\rho |h_{jb}|^2 \gamma_p + 2} < \Delta\right) \tag{17}$$

Denoting $X = |h_{je_i}|^2$, it can be rewritten as

$$P_o^{\text{JJUS}} = \int_0^{\infty} \prod_i \left(1 - \exp\left(-\frac{\Delta\rho x\gamma_p + 2\Delta}{\sigma_{ib}^2}\right)\right) \frac{1}{\sigma_{jb}^2} \exp\left(-\frac{x}{\sigma_{jb}^2}\right) dx = \int_0^{\infty} \frac{1}{\sigma_{jb}^2} \exp\left(-\frac{x}{\sigma_{jb}^2}\right) \times \left(1 + \sum_{m=1}^{2^{|U|}-1} (-1)^{|U_i(m)|} \exp\left(-\sum_{i \in U_i(m)} \frac{\Delta\rho\gamma_p x + 2\Delta}{\sigma_{ib}^2}\right)\right) dx = 1 - \sum_{m=1}^{2^N-1} (-1)^{|U_m|+1} \frac{1}{1 + \sum_{i \in U_m} \frac{\Delta\rho\gamma_p\sigma_{jb}^2}{\sigma_{ib}^2}} \exp\left(-\sum_{i \in U_m} \frac{2\Delta}{\sigma_{ib}^2}\right) \tag{18}$$

where U_m denotes the m-th non-empty subset of the elements of U, and $|U_m|$ is the cardinality of set U_m.

As aforementioned, the intercept probability definition has been presented. Similarly to Eq. (11), the intercept probability of the proposed JJUS scheme is obtained as

$$P_t^{\text{JJUS}} = \Pr(C_{oe} > R) \tag{19}$$

Using the law of total probability[17], Eq. (19) can be shown as

$$P_t^{\text{JJUS}} = \sum_{i=1}^{N} \Pr\left(\max_l \frac{|h_{ie_l}|^2}{\eta |h_{je_l}|^2 \gamma_p + 2} > \Delta, \max_{k,k \neq i} |h_{kb}|^2 < |h_{ib}|^2\right) = \sum_{i=1}^{N} \left(1 - \Pr\left(\max_l \frac{|h_{ie_l}|^2}{\eta |h_{je_l}|^2 \gamma_p + 2} < \Delta\right)\right) \times \Pr(\max_{k,k \neq i} |h_{kb}|^2 < |h_{ib}|^2) \tag{20}$$

Letting $y = |h_{ib}|^2$, we have

$$\Pr(\max_{k,k \neq i} |h_{kb}|^2 < |h_{ib}|^2) = \int_0^{\infty} \frac{1}{\sigma_{ib}^2} \exp\left(-\frac{y}{\sigma_{ib}^2}\right) \prod_{k,k \neq i} \left(1 - \exp\left(-\frac{y}{\sigma_{kb}^2}\right)\right) dy = \int_0^{\infty} \frac{1}{\sigma_{ib}^2} \exp\left(-\frac{y}{\sigma_{ib}^2}\right) \left(1 + \sum_{m=1}^{2^{|N|-1}-1} (-1)^{|C_m|} \exp\left(-\sum_{k \in C_m} \frac{y}{\sigma_{kb}^2}\right)\right) dy = 1 - \sum_{m=1}^{2^{N-1}-1} (-1)^{|C_m|+1} \frac{1}{1 + \sum_{k \in C_m} \frac{\sigma_{ib}^2}{\sigma_{kb}^2}} \tag{21}$$

where C_m denotes the m-th non-empty subset of the elements of $U - \{i\}$, and $|C_m|$ is the cardinality of set C_m.

Substituting Eqs. (13) and (21) into Eq. (20), we have

$$P_{\mathrm{t}}^{\mathrm{JJUS}} = \sum_{i=1}^{N}\left(P_{\mathrm{t},i}\left(1 - \sum_{m=1}^{2^{N-1}-1}(-1)^{|U_m|+1}\frac{1}{1+\sum_{k\in U_m}\frac{\sigma_{ib}^2}{\sigma_{kb}^2}}\right)\right) \tag{22}$$

3 Numerical Results

In this section, we present the simulation results of the proposed JJUS scheme and the traditional round-robin scheme in terms of their SRTs. It is pointed out that λ_{me} is defined as $\lambda_{me} = \sigma_b^2/\sigma_e^2$, where σ_b^2 and σ_e^2 are the average channel gains of the U-BS link and the U-E link, respectively. In order to examine the correctness of the analytic results, the Rayleigh fading channel is used to generate the instantaneous channel gains. Moreover, we denote $\sigma_{ib}^2 = \alpha_{ib}\sigma_b^2$ and $\sigma_{ie_i}^2 = \alpha_{ie_i}\sigma_e^2$, where α_{ib} and α_{ie_i} are assumed to be 1 in this simulation. Additionally, the analytic intercept probabilities and outage probabilities of the round-robin and JJUS schemes are obtained by plotting Eqs. (15), (14), (22) and (18), respectively. Furthermore, R is assumed to be 1 bit/(s · Hz).

Fig. 2 depicts the SRT of the round-robin, PUS, and JJUS schemes for different N. Simulation results and analytic results of the SRT for the JJUS scheme are provided in this figure. One can see from Fig. 2 that as the number of users increases, the SRT of the JJUS and PUS[15] schemes improve, due to the diversity gain of multi-users. In other words, we can improve the security of wireless transmissions by increasing the number of users. However, the SRT of the round-robin scheme remains unchanged, which cannot achieve the performance gain from the increasing number of users. In Fig. 2, it is also shown that the proposed JJUS scheme outperforms the traditional round-robin and PUS schemes in terms of the SRT for $N = 2, 4, 8$ cases. Furthermore, the difference between the simulation results and theoretical SRT is negligible, proving the correctness of the SRT analysis.

In Fig. 3, we show the SRT of the round-robin, PUS and JJUS schemes for different M. One can observe from Fig. 3 that as the number of eavesdroppers M increases from $M = 1$ to 4, the SRT performance of all schemes degrades, which means that increasing the number of eavesdroppers worsens the security of wireless transmissions. In addition, Fig. 3 also shows that the SRT performance of the proposed JJUS scheme is better than that of the round-robin and PUS schemes for $M = 1, 2, 4$ cases. Moreover, the round-robin scheme considers the fairness of multi-user scheduling, which may sacrifice the SRT

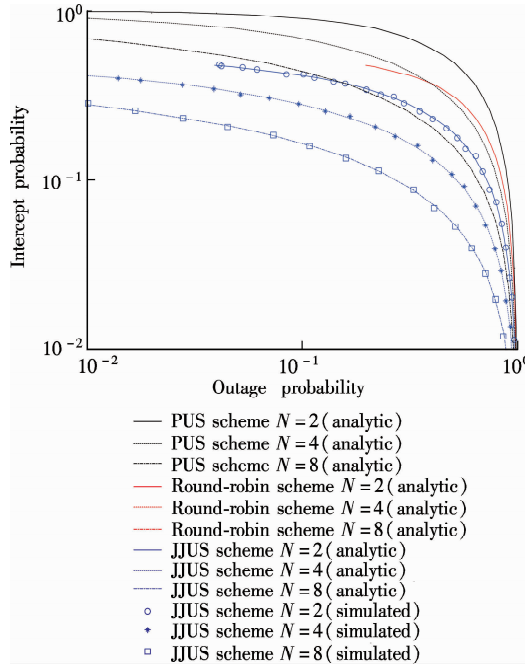

Fig. 2 SRT of the traditional round-robin, PUS and the proposed JJUS schemes for different numbers of users with $M = 2$, $\lambda_{me} = 0$ dB, $\rho = 0.01$, and $\eta = 0.99$

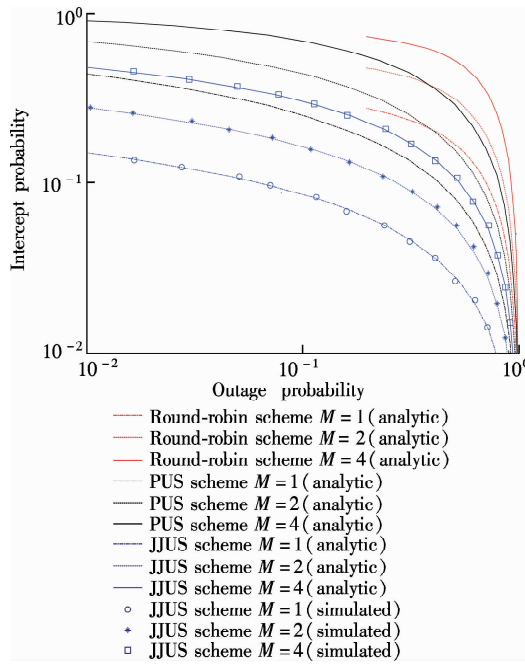

Fig. 3 SRT of the traditional round-robin, PUS and the proposed JJUS schemes for different numbers of eavesdroppers with $N = 8$, $\lambda_{me} = 0$ dB, $\rho = 0.01$, and $\eta = 0.99$

performance, particularly in the multi-eavesdropper regions.

Fig. 4 illustrates the SRT of the round-robin and JJUS schemes for different pairs of (ρ, η). One can see from Fig. 4 that as the factor ρ degrades and η upgrades, the SRT of the JJUS scheme improves accordingly. This is due to the fact that for an improved reliability of transmiting artificial noise, the interference of artificial noise to the main links will be decreased, and the interference of

artificial noise to wiretap links will be increased. In other words, we can improve the security of wireless transmissions by increasing the accuracy of transmission of artificial noise. Furthermore, Fig. 4 also illustrates that the proposed JJUS scheme outperforms the traditional round-robin scheme in terms of the SRT for both $(\rho, \eta) = (0.02, 0.99)$ and $(\rho, \eta) = (0.15, 0.9)$ cases.

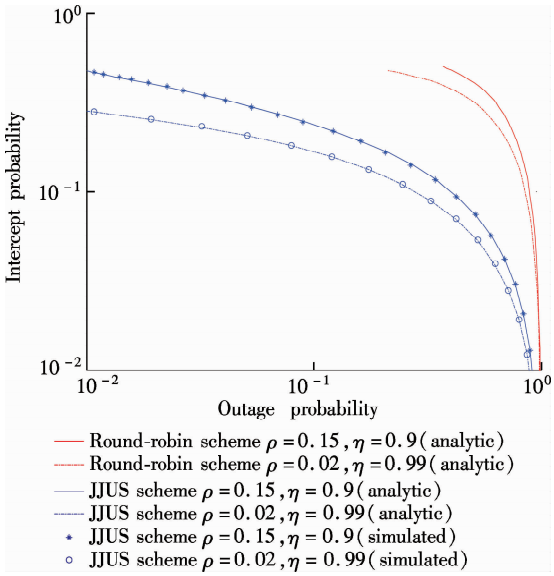

Fig. 4 SRT of the traditional round-robin and the proposed JJUS schemes for different pairs of ρ and η with $\lambda_{me} = 0$ dB, $N = 8$, and $M = 2$

Fig. 5 illustrates the SRT of the round-robin, PUS and JJUS schemes for different λ_{me} cases. One can see from Fig. 5 that as the λ_{me} increases from -3 to 3 dB case, the SRT of the round-robin, PUS and JJUS schemes are enhanced obviously. Moreover, it is shown that the JJUS scheme outperforms the round-robin and PUS schemes in terms of the SRT for $\lambda_{me} = -3, 0, 3$ dB cases. In $\lambda_{me} = -3$ dB region, the SRT of the proposed JJUS scheme is better than that of the round-robin scheme for $\lambda_{me} = 0, 3$ dB cases, wherein the $\lambda_{me} = -3$ dB case means that the average channel gain of the wiretap links is two times better than that of the main links. Moreover, the proposed JJUS scheme can guarantee secure transmission even in the very low $\lambda_{me} = -3$ dB region.

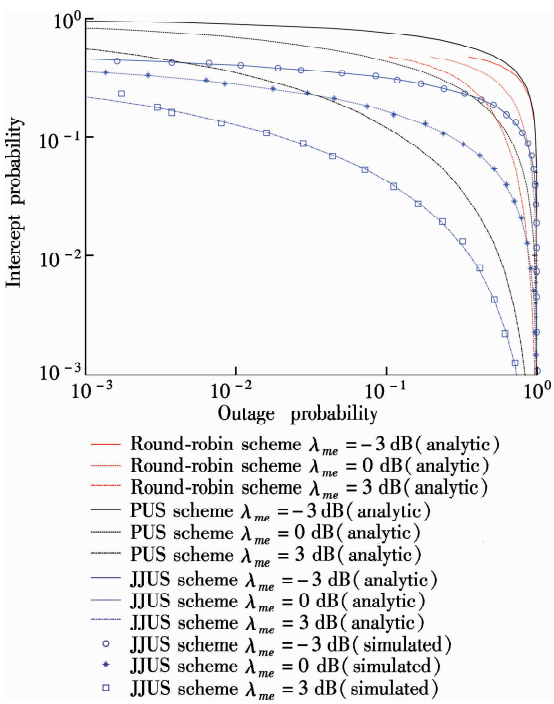

Fig. 5 SRT of the traditional round-robin, PUS and the proposed JJUS schemes for different λ_{me} with $N = 8$, $M = 2$, $\rho = 0.01$, and $\eta = 0.99$

4 Conclusion

In this paper, we investigate a wireless network consisting of multiple users and one base station in the presence of multiple eavesdroppers and one jammer, where the eavesdroppers are deployed to intercept the transmissions of the main links deliberately. We propose a joint jammer and user scheduling scheme to improve the security-reliability tradeoff in the considering scenario. Moreover, we analyze the SRT performance of the proposed JJUS scheme, as well as the traditional round-robin scheme for comparison purposes. It is illustrated that the JJUS scheme outperforms the round-robin and PUS schemes in terms of the SRT. Furthermore, even in the very low λ_{me} region, the SRT performance of the JJUS scheme is significantly better than that of the round-robin and PUS schemes.

References

[1] Al-Ghadhban S. Opportunistic round robin scheduling for V-BLAST systems over multiuser MIMO channels [J]. *EURASIP Journal on Wireless Communications and Networking*, 2014, **2014**: 128. DOI: 10.1186/1687-1499-2014-128.

[2] Fritzsche R, Rost P, Fettweis G. Robust rate adaptation and proportional fair scheduling with imperfect CSI [J]. *IEEE Transactions on Wireless Communications*, 2015, **14**(8): 4417-4427. DOI: 10.1109/twc.2015.2420564.

[3] Long H, Xiang W, Wang J, et al. Cooperative jamming and power allocation with untrusty two-way relay nodes [J]. *IET Communications*, 2014, **8**(13): 2290-2297. DOI: 10.1049/iet-com.2013.0580.

[4] Wyner A D. The wire-tap channel [J]. *Bell System Technical Journal*, 1975, **54**(8): 1355-1387. DOI: 10.1002/j.1538-7305.1975.tb02040.x.

[5] Li N, Tao X F, Xu J. Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback [J]. *IEEE Communications Letters*, 2014, **18**(6): 969-972.

[6] Geraci G, Egan M, Yuan J H, et al. Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding [J]. *IEEE Transactions on Communications*, 2012, **60**(11): 3472-3482. DOI: 10.1109/tcomm.2012.072612.110686.

[7] Zhao P, Zhang M, Yu H, et al. Robust beamforming

design for sum secrecy rate optimization in MU-MISO networks [J]. *IEEE Transactions on Information Forensics and Security*, 2015, **10**(9): 1812 - 1823. DOI: 10.1109/tifs.2015.2423263.

[8] Krikidis I, Ottersten B. Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling [J]. *IEEE Signal Processing Letters*, 2013, **20**(2): 141 - 144. DOI: 10.1109/lsp.2012.2234109.

[9] Zou Y L, Wang X B, Shen W M, et al. Security versus reliability analysis of opportunistic relaying [J]. *IEEE Transactions on Vehicular Technology*, 2014, **63**(6): 2653 - 2661. DOI: 10.1109/tvt.2013.2292903.

[10] Kundu C, Ghose S, Bose R. Secrecy outage of dual-hop regenerative multi-relay system with relay selection [J]. *IEEE Transactions on Wireless Communications*, 2015, **14**(8): 4614 - 4625. DOI: 10.1109/twc.2015.2423290.

[11] Chu Z, Cumanan K, Ding Z G, et al. Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer [J]. *IEEE Transactions on Vehicular Technology*, 2015, **64**(5): 1833 - 1847.

[12] Lee J, Choi W. Multiuser diversity for secrecy communications using opportunistic jammer selection: Secure DOF and JOF scaling law [J]. *IEEE Transactions on Signal Processing*, 2014, **62**(4): 828 - 851. DOI: 10.1109/tsp.2013.2293979.

[13] Tang X J, Liu R H, Spasojevic P, et al. Interference assisted secret communication [J]. *IEEE Transactions on Information Theory*, 2011, **57**(5): 3153 - 3167. DOI: 10.1109/tit.2011.2121450.

[14] Garnaev A, Baykal-Gursoy M, Poor H V. A game theoretic analysis of secret and reliable communication with active and passive adversarial modes [J]. *IEEE Transactions on Wireless Communications*, 2016, **15**(3): 2155 - 2163. DOI: 10.1109/twc.2015.2498934.

[15] Zou Y L, Li X L, Liang Y C. Secrecy outage and diversity analysis of cognitive radio systems [J]. *IEEE Journal on Selected Areas in Communications*, 2014, **32**(11): 2222 - 2236. DOI: 10.1109/jsac.2014.141121.

[16] Shannon C E. A mathematical theory of communication [J]. *Bell System Technical Journal*, 1948, **27**(3): 379 - 423. DOI: 10.1002/j.1538 - 7305.1948.tb01338.x.

[17] Zou Y, Zhu J, Zheng B, et al. An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks [J]. *IEEE Transactions on Signal Processing*, 2010, **58**(10): 5438 - 5445. DOI: 10.1109/tsp.2010.2053708.

一种基于联合干扰与用户调度的无线物理层安全机制

丁晓进[1] 宋铁成[1] 邹玉龙[2] 陈晓曙[1]

([1] 东南大学移动通信国家重点实验室, 南京 210096)
([2] 南京邮电大学通信与信息工程学院, 南京 210003)

摘要: 为了提高无线传输的安全与可靠性折中性能,提出了一种基于联合干扰与用户的调度机制. 首先,在传输时隙中,具有最大瞬时信道容量的用户节点会被选择与基站进行数据传输;然后,当用户节点与基站进行数据传输时,干扰节点会被用于发送人工噪声信号,以干扰窃听节点窃听用户与基站间的数据传输. 仿真结果表明,增加用户数目可以提高所提出机制的安全与可靠性折中性能. 此外,与传统的轮询调度及纯粹的用户调度这 2 种机制相比,该机制能够取得更好的安全与可靠性折中性能,尤其是在主信道与窃听信道增益比较低时,该机制还能够确保安全传输.

关键词: 安全与可靠性折中;多用户调度;人工噪声;物理层安全

中图分类号: TN929.5