An Anti-Eavesdrop Transmission Scheduling Scheme Based on Maximizing Secrecy Outage Probability in Ad Hoc Networks

WANG Yajun[1], LIAO Tongqing[2] , WANG Chuanan[1]

[1]School of Mathematical and Information Engineering ,Anhui Science and Technology University, Anhui 233100,China
[2]Ministry of Educational Key Laboratory of Intelligent Computing and Signal Processing, Anhui University, Hefei 230039, China

Abstract: In this paper, we consider a wireless ad hoc network consisting of multiple source nodes transmitting to their respective destinations, where an eavesdropper attempts to intercept their transmissions. We propose an optimal transmission scheduling scheme to defend against the eavesdropper, where a source node having the highest secrecy rate is scheduled to access the wireless medium for transmitting to its destination in an opportunistic manner. To be specific, the secrecy rate between a pair of the source and destination in the presence of an eavesdropper varies temporally due to the wireless fading effect. The proposed optimal transmission scheduling scheme opportunistically selects a source node with the highest secrecy rate to transmit its data for the sake of maximizing the security of the ad hoc network against eavesdropping attacks. For comparison purposes, we also consider the conventional round-robin scheduling as a benchmark, where multiple source nodes take turns in accessing their shared wireless medium for transmitting to their respective destinations. We derive closed-form secrecy outage probability expressions of both the round-robin scheduling and the proposed optimal scheduling schemes over Rayleigh fading environments. Numerical results show that the proposed transmission scheduling scheme outperforms the conventional round-robin method in terms of its secrecy outage probability. Additionally, upon increasing the number of source-destination pairs, the secrecy outage probability of the round-robin scheme keeps unchanged, whereas the secrecy outage performance of the proposed transmission scheduling significantly improves, showing the security benefits of exploiting transmission scheduling for protecting wireless ad hoc networks against eavesdropping.

Keywords: transmission scheduling; eavesdropping; secrecy outage probability; secrecy rate; rayleigh fading

I. INTRODUCTION

Wireless ad hoc networks are decentralized without any infrastructure, where all network devices have an equal status and can directly communicate with each other without the need of a centralized node [1]-[3]. The decentralized nature of ad hoc networks makes them suitable for various application scenarios [4], [5], such as the environment monitoring, battlefield surveillance, and so on. Since no centralized infrastructure is available and the network nodes are mobile, the topology of

The authors proposed an optimal transmission scheduling scheme for protecting the ad hoc network against eavesdropping.

wireless ad hoc networks is highly dynamic and changes frequently [6]. In wireless ad hoc networks, the nodes need to compete with each other for accessing their shared wireless medium, which often results in transmission collisions. Exploiting user cooperation and coordination amongst different network nodes improves their ability to reduce the collisions, but this introduces new security challenges, since the confidential information is exposed to cooperative users which may be compromised and become untrusted [7], [8].

Cryptographic techniques relying on secret keys are typically employed to protect the confidentiality of data communications against eavesdropping attacks [9]-[11]. The secret key distribution and management requires a trusted infrastructure, which, unfortunately, is unavailable in a wireless ad hoc network due to its decentralized nature. As an alternative, physical-layer security (PLS) is now emerging as an effective means of achieving perfect secrecy against eavesdropping by exploiting physical characteristics of wireless channels (e.g., the fading amplitude and phase information) [12]. In [13] and [14], the PLS work was studied for a wiretap channel model comprised of a single source and a destination in the face of an eavesdropper, where the notion of *secrecy capacity* is introduced and shown to be the difference between the source-to-destination channel capacity and the source-to-eavesdropper channel capacity. It can be observed that the secrecy capacity is affected by the quality of the source-to-destination channel. In wireless networks, the source-to-destination transmission experiences a wireless fading process, which fluctuates in time and results in a degradation of the secrecy capacity. For example, if the source-to-destination channel is deeply faded, the secrecy capacity of wireless transmissions will drop dramatically.

Presently, extensive efforts have been devoted to the research and development of wireless secrecy capacity enhancement techniques to combat the fading effect. In [15]-[17], the authors proposed the artificial noise generation method to improve the wireless secrecy capacity in multiple-input multiple-output (MIMO) systems by generating the specifically designed artificial noise to confuse the eavesdropper while imposing no interference on the desired destination. Later on, in [18], beamforming techniques were studied for enhancing the wireless security in cooperative relay networks under the assumption that the perfect channel state information (CSI) of both the main link and the wiretap link is known. Motivated by the fact that the eavesdropper is passive and its CSI is challenging to obtain in practice, the authors of [19] examined the beamforming for wireless secrecy capacity improvement without the need of the eavesdropper's CSI knowledge. In order to allow low-complexity joint estimation and data detection at high signal-to-noise ratio(SNR), the authors studied joint carrier frequency offset and channel estimation in OFDM-based two-way relay networks[20]. Recently, in [21], the multiuser scheduling was investigated for improving the PLS of cognitive radio networks in terms of the secrecy capacity and intercept probability. In current, channel estimation errors were considered for enhancing the security and reliability performance in the cloud radio access network[22]. In [23], the authors, depended on whether the source node had the global CSI, researched the antenna selection at the source and proposed the optimal antenna selection schemes in MIMO system. In this paper, we explore the transmission scheduling in a wireless ad hoc networks consisting of multiple source-destination pairs in the presence of an eavesdropper, which is different from the multiuser scheduling for cognitive radio networks as studied in [21]. Moreover, we focus on analyzing the secrecy outage probability of transmission scheduling against eavesdropping, instead of the intercept probability analysis presented in [21].

The following summarizes the main contributions of this paper. First, an optimal transmission scheduling scheme is proposed for the sake of enhancing the security of wireless ad hoc networks against eavesdropping attacks. More specifically, in the proposed transmis-

sion scheduling scheme, a source node which achieves the highest secrecy rate to its destination is chosen to access the wireless medium for transmission. By contrast, the conventional round-robin scheduling allows the multiple source nodes to take turns in accessing the channel. Second, we derive closed- form expressions of the secrecy outage probability for both the round-robin scheduling and the proposed optimal transmission scheduling in Rayleigh fading environments. Third, numerical secrecy outage results of the two scheduling schemes are evaluated and provided.

The remainder of this paper is organized as follows. In Section II, we describe the system model of a wireless ad hoc network in the face of an eavesdropper and present the round-robin scheduling and the optimal transmission scheduling schemes. Then, Section III drives closed-form expressions of the secrecy outage probability for both the round-robin scheduling and the proposed optimal transmission scheduling in Rayleigh fading environments. In Section IV, numerical performance comparison between the two scheduling schemes is carried out in terms of the secrecy outage probability. Finally, we provide some concluding remarks in Section V.

II. Transmission Scheduling in Wireless Ad Hoc Networks

2.1 System model

In Fig. 1, we show a wireless ad hoc network comprised of multiple source-destination pairs, where all network nodes are equipped with a single antenna and the solid and dash lines denote the main and wiretap links, respectively. In Fig. 1, N source nodes (i.e., s_1, s_2, …, s_N) intend to transmit their respective destinations denoted by d_1, d_2,…,d_N. Meanwhile, an eavesdropper (e) attempts to tap the source-destination transmissions. The source and destination nodes of Fig. 1 are connected and communicated through a shared wireless medium by using an orthogonal multiple access approach, e.g., the time division multiple access (TDMA), the frequency division multiple access (FDMA), and the code division multiple access (CDMA). Considering the TDMA method, only one source node is allowed to transmit at a time to avoid interfering with different transceivers.

Traditionally, given a wireless channel, a source node with the highest instantaneous throughput is chosen to access the channel for transmission, aiming at improving the capacity of ad hoc networks. This process is focused on maximizing the throughput of legitimate main links without considering the minimization of the eavesdropping throughput of wiretap links. In this paper, **we** explore the transmission scheduling against eavesdropping, which should take into account the channel state information (CSI) of both the main and wiretap links. Throughout this paper, the CSI knowledge of the main and wiretap links is assumed to be available for performing the transmission scheduling. Moreover, both the main and wiretap channels are characterized by using the Rayleigh fading model. Although only the Rayleigh fading is considered in this paper, similar performance analysis and results can be obtained for other fading models e.g. the Rician fading and the Nakagami fading. Additionally, an additive white Gaussian noise (AWGN) received at any network node is assumed to have a zero mean and a variance of N_0.

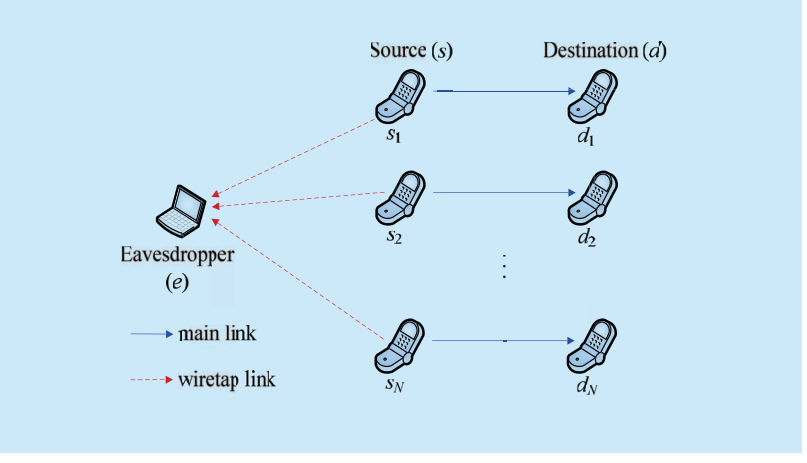

Fig.1 *A wireless ad hoc network consisting of multiple pairs of source (s) and destination (d) in the presence of an eavesdropper (e)*

2.2 Round-robin transmission scheduling

In this subsection, we present the conventional round-robin transmission scheduling as a baseline for performance comparisons. In the round-robin scheduling, the N source nodes take turns in accessing their shared wireless medium and each source has an equal opportunity to transmit to its destination. Without loss of generality, let us consider that the source node s_i is allowed to access the wireless medium for transmitting its signal x_i at a power of P and a secrecy rate of R_s. Hence, the signal received at the destination node d_i is expressed as

$$y_i = \sqrt{P}\, h_{ii} x_i + n_i \,, \tag{1}$$

where h_{ii} represents a fading coefficient of the legitimate channel from the source s_i to its destination d_i and n_i represents a zero-mean AWGN sample with a variance of N_0. Using the Shannon's capacity formula, we obtain the s_i-to-d_i channel capacity as

$$C_{ii} = \log_2(1 + |h_{ii}|^2\gamma) \,, \tag{2}$$

where $\gamma = \dfrac{P}{N_0}$ .Meanwhile, the s_i-to-d_i transmission is also overheard by the eavesdropper, which attempts to decode and intercept the source signal x_i. Thus, the signal received at the eavesdropper is written as

$$y_{ie} = \sqrt{P}\, h_{ie} x_i + n_e \,, \tag{3}$$

where h_{ie} represents a fading coefficient of the wiretap channel from s_i to the eavesdropper and n_e represents a zero-mean AWGN with a variance of N_0. Using (3), we obtain the s_i-to-d_i channel capacity as

$$C_{ie} = \log_2(1 + |h_{ie}|^2\gamma) \,. \tag{4}$$

As shown in [13], the secrecy capacity of the source-destination transmission in the presence of an eavesdropper is given by the capacity difference between the legitimate main channel (from the source to the destination) and the wiretap channel (from the source to the eavesdropper). Accordingly, the secrecy capacity of the transmission of i-th source-destination pair (i.e., s_i-to-d_i) can be given by

$$C_i^{\text{sec recy}} = \log_2\left(\frac{1 + |h_{ii}|^2\gamma}{1 + |h_{ie}|^2\gamma}\right) \tag{5}$$

which completes the modeling of the s_i-to-d_i transmission in terms of secrecy capacity.

2.3 Optimal transmission scheduling

This subsection proposes an optimal transmission scheduling scheme, which always selects a source-destination pair with the highest individual secrecy capacity for the sake of maximizing the overall secrecy capacity of the ad hoc network of Fig. 1. In this way, the optimal transmission scheduling criterion can be obtained from (5) as

$$Optimal\ S-D\ \text{Pair} = \arg\max_{i\in 1,2,\cdots,N} \frac{1 + |h_{ii}|^2\gamma}{1 + |h_{ie}|^2\gamma}. \tag{6}$$

Hence, an overall secrecy capacity of the ad hoc network of Fig. 1 relying on the proposed optimal transmission scheduling can be obtained from (6) as

$$C_{proposed}^{\text{sec recy}} = \max_{i\in 1,2,\cdots,N} \log_2\left(\frac{1 + |h_{ii}|^2\gamma}{1 + |h_{ie}|^2\gamma}\right). \tag{7}$$

Throughout this paper, the Rayleigh model is used to characterize the fading of a wireless channel between any two network nodes of Fig. 1. Hence, random variables (RVs) $|h_{ii}|$ and $|h_{ie}|$ both follow the Rayleigh distribution, leading to the fact that the fading squared magnitudes $|h_{ii}|^2$ and $|h_{ie}|^2$ are exponentially distributed RVs with respective means of σ_{ii}^2 and σ_{ie}^2. Notice that RVs $|h_{ii}|^2$ and $|h_{ie}|^2$ are independent of each other. Denoting $X = |h_{ii}|^2$ and $Y = |h_{ie}|^2$, we can obtain the joint probability density function of (X, Y) as

$$f(x,y) = \frac{1}{\sigma_{ii}^2\sigma_{ie}^2} \exp\left(-\frac{x}{\sigma_{ii}^2} - \frac{y}{\sigma_{ie}^2}\right), \tag{8}$$

for $(x>0, y>0)$.

III. Secrecy Outage Probability Analysis

In this section, we carry out the secrecy outage analysis of the conventional round-robin transmission scheduling as well as the proposed optimal transmission scheduling schemes in Rayleigh fading environments.

3.1 Round-robin transmission scheduling

As known in [13], a secrecy outage event is deemed to occur, when the secrecy capacity falls below the predefined secrecy rate R_s. Thus, the probability of occurrence of a secrecy outage, called *secrecy outage probability*(SOP), for the s_i-to-d_i transmission can be obtained from (5) as

$$\begin{aligned} Pout_i &= \Pr[C_i^{\text{sec recy}} < R_s] \\ &= \Pr\left(\frac{1+|h_{ii}|^2\gamma}{1+|h_{ie}|^2\gamma} < 2^{R_s}\right), \end{aligned} \tag{9}$$

where $|h_{ii}|^2$ and $|h_{ie}|^2$ are exponentially distributed RVs and independent of each other. Denoting $x=|h_{ii}|^2$ and $y = |h_{ie}|^2$, we can rewrite (9) as

$$Pout_i = \Pr(x - 2^{R_s} y < \Delta), \tag{10}$$

where $\Delta = \frac{2^{R_s}-1}{\gamma}$.Using the joint probability density function of RVs (x , y) as given by (8), we arrive at

$$\begin{aligned} Pout_i &= 1 - \int_{\Delta}^{\infty} \frac{1}{\sigma_{ii}^2}\exp(-\frac{x}{\sigma_{ii}^2})dx \int_0^{\frac{x-\Delta}{2^{R_s}}} \frac{1}{\sigma_{ie}^2}\exp(-\frac{y}{\sigma_{ie}^2})dy \\ &= 1 - \int_{\Delta}^{\infty} \frac{1}{\sigma_{ii}^2}\exp(-\frac{x}{\sigma_{ii}^2})[1-\exp(-\frac{x-\Delta}{\sigma_{ie}^2 2^{R_s}})]dx \\ &= 1 - \exp(-\frac{\Delta}{\sigma_{ii}^2}) + \frac{\sigma_{ie}^2 2^{R_s}}{\sigma_{ie}^2 2^{R_s} + \sigma_{ii}^2}\exp(-\frac{\Delta}{\sigma_{ii}^2}), \end{aligned} \tag{11}$$

which can be further simplified to

$$Pout_i = 1 - \frac{\sigma_{ii}^2}{\sigma_{ii}^2 + \sigma_{ie}^2 2^{R_s}}\exp(-\frac{\Delta}{\sigma_{ii}^2}). \tag{12}$$

As aforementioned, the round-robin transmission scheduling scheme allows the N source- destination pairs take turns in accessing their shared wireless medium. This implies that the secrecy outage probability of the ad hoc network relying on the round-robin transmission scheduling is the mean value of the N source-destination transmissions secrecy outage probabilities, yielding

$$Pout_{round-robin} = \frac{1}{N}\sum_{i=1}^{N} Pout_i, \tag{13}$$

where N is the number of source-destination pairs in the ad hoc network. Substituting (12) into (13) gives

$$\begin{aligned} &Pout_{round-robin} \\ &= 1 - \frac{1}{N}\sum_{i=1}^{N} \frac{\sigma_{ii}^2}{\sigma_{ii}^2 + \sigma_{ie}^2 2^{R_s}}\exp(-\frac{\Delta}{\sigma_{ii}^2}), \end{aligned} \tag{14}$$

which is a closed-form expression of the secrecy outage probability for the conventional round- robin scheduling scheme.

3.2 Proposed optimal transmission scheduling

In this subsection, we present the secrecy outage probability analysis for the proposed optimal transmission scheduling scheme over Rayleigh fading channels. As above mentioned, a secrecy outage event happens if the secrecy capacity becomes lower than the secrecy rate R_s. Hence, from (7), we obtain the secrecy outage probability of the proposed optimal transmission scheduling scheme as

$$\begin{aligned} Pout_{pro} &= \Pr(C_{proposed}^{\text{sec recy}} < R_s) \\ &= \Pr\left[\max_{i\in 1,2,\cdots,N} \log_2\left(\frac{1+|h_{ii}|^2\gamma}{1+|h_{ie}|^2\gamma}\right) < R_s\right] \\ &= \Pr\left[\max_{i\in 1,2,\cdots,N}\left(\frac{1+|h_{ii}|^2\gamma}{1+|h_{ie}|^2\gamma}\right) < 2^{R_s}\right], \end{aligned} \tag{15}$$

where N is the number of the source-destination pairs. Noting that RVs $|h_{ii}|^2$ and $|h_{ie}|^2$ are independent of each other for different source-destination pairs, we can rewrite (15) as

$$Pout_{pro} = \prod_{i=1}^{N} \Pr\left[\frac{1+|h_{ii}|^2\gamma}{1+|h_{ie}|^2\gamma} < 2^{R_s}\right]. \tag{16}$$

Combining (12) and (16), we have

$$Pout_{pro} = \prod_{i=1}^{N}\left[1 - \frac{\sigma_{ii}^2}{\sigma_{ii}^2 + \sigma_{ie}^2 2^{R_s}}\exp(-\frac{\Delta}{\sigma_{ii}^2})\right], \tag{17}$$

where $\Delta = \frac{2^{R_s}-1}{\gamma}$.We have now derived closed-form expressions of the secrecy outage probability for both the round-robin transmission scheduling and the proposed optimal transmission scheduling schemes in Rayleigh fading channels.

IV. Numerical Results and Discussions

In this section, we present the numerical performance comparison between the round-robin transmission scheduling and the proposed optimal transmission scheduling in terms of their secrecy outage probabilities. Specifically,

numerical secrecy outage results of the two transmission scheduling schemes are evaluated by using (14) and (17). Both the main links (spanning from the source nodes to their destinations) and the wiretap links (spanning from the source nodes to the eavesdropper) characterized by using the Rayleigh fading model, where the fading variances are specified to $\sigma_{ii}^2 = 1$ and $\sigma_{ie}^2 = 0.2$. Additionally, an SNR of γ=10dB and a secrecy rate of R_s =1bit/s/Hz are used in the numerical evaluation, unless otherwise stated.

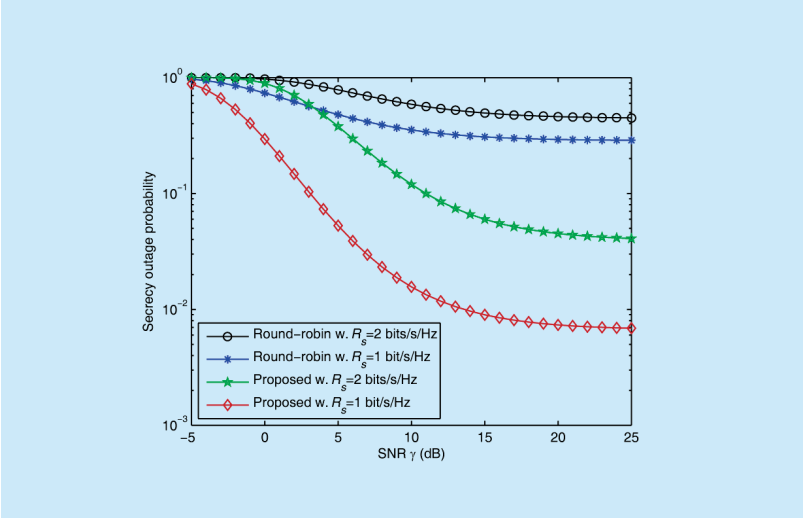

Fig.2 *Secrecy outage probability versus SNR γ of the conventional round-robin transmission scheduling and proposed optimal transmission scheduling schemes for different secrecy rates with N=4,* $\sigma_{ii}^2 = 1$ *and* $\sigma_{ie}^2 = 0.2$

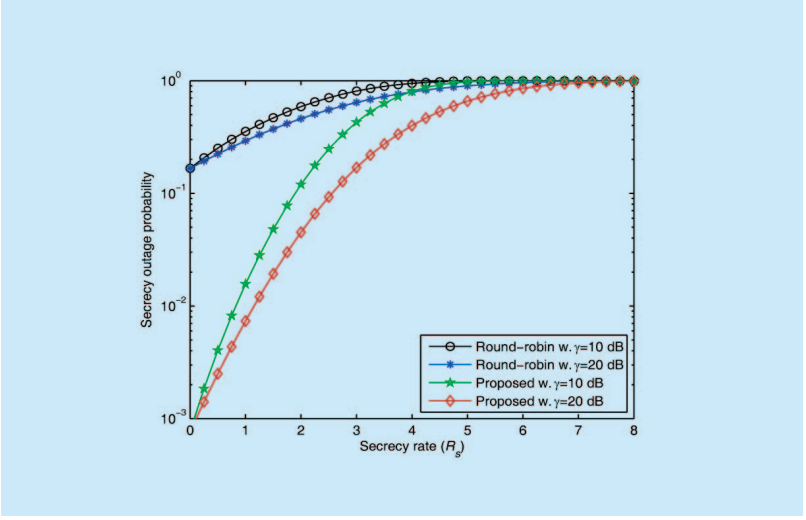

Fig.3 *Secrecy outage probability versus secrecy rate Rs of the conventional round-robin transmission scheduling and proposed optimal transmission scheduling schemes for different SNRs with N = 4,* $\sigma_{ii}^2 = 1$ *and* $\sigma_{ie}^2 = 0.2$

Fig. 2 shows the secrecy outage probability versus SNR γ of the conventional round-robin transmission scheduling and proposed optimal transmission scheduling schemes for different secrecy rates. It is seen from Fig. 2 that for both the cases of *Rs*=1bit/s/Hz and *Rs*=2bits/s/Hz, as the SNR γ increases, the secrecy outage probabilities of the round-robin transmission scheduling and the proposed optimal transmission schemes first decrease and finally converge to their respective secrecy outage floors. This implies that given a sufficiently high SNR, continuing to increase the transmit power will not enhance the ad hoc network security against eavesdropping. Fig. 2 also shows that as the secrecy rate increases from *Rs*=1 bit/s/Hz to *Rs*=2 bits/s/Hz, the secrecy outage probabilities of the round-robin transmission scheduling and the proposed optimal transmission schemes both increase accordingly. Additionally, one can observe from Fig. 2 that the proposed optimal transmission scheduling outperforms the conventional round-robin transmission scheduling in terms of its secrecy outage probability.

In Fig. 3, we depict the secrecy outage probability versus secrecy rate R_s of the conventional round-robin transmission scheduling and proposed optimal transmission scheduling schemes for different SNRs. As shown in Fig. 3, with an increasing secrecy rate, the secrecy outage probabilities of both the round-robin transmission scheduling and the proposed optimal transmission schemes increase and finally converge to the probability of one (i.e. the legitimate transmission can be always successfully intercepted by the eavesdropper). In other words, although increasing the secrecy rate can improve the transmission throughput of the ad hoc network, this is achieved at the cost of a security performance degradation. Fig. 3 also demonstrates that as the SNR increases from γ=10 dB to γ= 20 dB, the transmission security of the two scheduling schemes is improved in terms of their secrecy outage probabilities.

Fig. 4 illustrates the secrecy outage prob-

ability versus SNR γ of the conventional round-robin transmission scheduling and the proposed optimal transmission scheduling schemes for different number of the source-destination pairs *N*. It is shown from Fig. 4 that the secrecy outage probability of the round-robin transmission scheduling scheme corresponding to the number of source-destination pairs *N* =4 is identical to that corresponding to *N*=6, whereas the secrecy outage probability of the proposed optimal transmission scheduling significantly decreases as *N* increases from *N*=4 to *N*=6. Fig. 4 also shows that for both the cases of *N*=4 and *N*=6, the proposed transmission scheduling performs better than the round-robin transmission scheduling in terms of its secrecy outage probability.

Fig. 5 shows the secrecy outage probability versus the number of source-destination pairs *N* of the round-robin transmission scheduling and the proposed optimal transmission scheduling schemes for different secrecy rates. One can observe from Fig. 5 that for both the cases of *Rs*=1 bit/s/Hz and *Rs*=2 bits/s/Hz, the secrecy outage probability of the round-robin transmission scheduling scheme remains unchanged, as the number of source-destination pairs *N* increases. By contrast, upon increasing the number of source-destination pairs, the security of the proposed transmission scheduling significantly improves in terms of its secrecy outage probability. This further confirms the security advantages of the proposed transmission scheduling over the round-robin method.

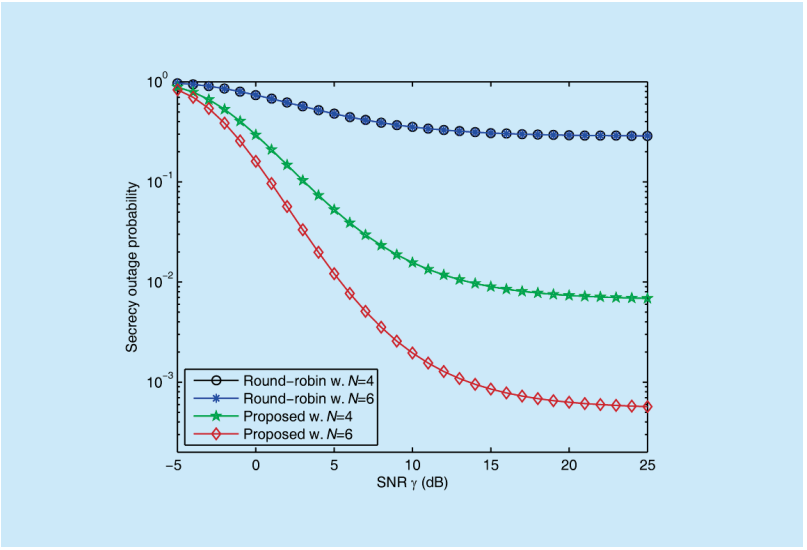

Fig.4 *Secrecy outage probability versus SNR γ of the conventional round-robin transmission scheduling and proposed optimal transmission scheduling schemes for different number of the source-destination pairs N with Rs = 1 bit/s/Hz ,* $\sigma_{ii}^2 = 1$ *and* $\sigma_{ie}^2 = 0.2$

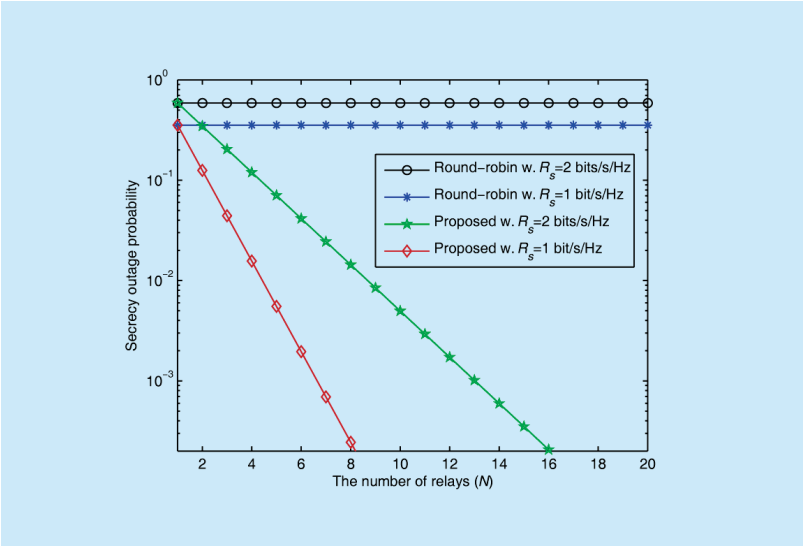

Fig.5 *Secrecy outage probability versus the number of source-destination pairs N of the conventional round-robin transmission scheduling and proposed optimal transmission scheduling schemes for different secrecy rates with γ= 10 dB,* $\sigma_{ii}^2 = 1$ *and* $\sigma_{ie}^2 = 0.2$

V. Conclusion

In this paper, we explored the transmission scheduling in a wireless ad hoc network comprised of multiple source-destination pairs in the presence of an eavesdropper. We proposed an optimal transmission scheduling scheme for protecting the ad hoc network against eavesdropping, where a source-destination pair with the highest secrecy rate is scheduled to access their shared wireless medium for data transmissions. The conventional round-robin transmission scheduling approach was also considered as a benchmark, in which the multiple source-destination pairs take turns in accessing the wireless medium. We derived closed-form secrecy outage expressions of both the round-robin transmission scheduling and the proposed optimal transmission scheduling

schemes in Rayleigh fading environments. Numerical results showed that the proposed transmission scheduling performs better than the conventional round-robin scheduling in terms of its secrecy outage probability. Finally, upon increasing the number of source-destination pairs, the secrecy outage probability of the proposed optimal transmission scheduling scheme improves significantly, explicitly showing the security benefits of exploiting the transmission scheduling against eavesdropping attacks.

Acknowledgements

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped to improve the quality of this paper. This work was supported by the Natural Science Foundation of Anhui Provincial Education Department under Grant No. KJ2013Z048 and the Natural Science Foundation of Anhui Provincial Colleges and Universities under Grant No. KJ2014A234.

References

[1] CONTI M , GIORDANO S, "Mobile ad hoc networking: Milestones, challenges, and new research directions", *IEEE Communications Magazine,* vol. 52, no. 1, pp 85-96, January, 2014.

[2] SADJADPOUR H R, WANG Z, and GARCIA-LUNA-ACEVES J J, "The capacity of wireless ad hoc networks with multi-packet reception", *IEEE Transactions on Communications,* vol. 58, no. 2, pp 600-610, Feburary, 2014.

[3] RANGANATHAN K and ARORA S,"Enabling grassroots communication: A memory-aided broadcast mechanism for a community radio service on an ad hoc device-to-device mobile network"□*IEEE Transactions on Communications,* vol. 62, no. 3, pp1138-1150, March, 2014.

[4] Mukunda N S, Padmanabhi V, and Srinivas A, "A remote patient monitoring system in an ad hoc sensor network environment", *International Conference on Information Technology and Multimedia*, Lumpur India, November ,2011.

[5] OCHIAI H, MITRAN P, POOR H , V et al. ,"Collaborative beamforming for distributed wireless ad hoc sensor networks", *IEEE Transactions on Signal Processing* , vol. 53, no. 11, pp 4110-4124, November, 2005.

[6] MELODIA T, POMPILI D, and AKYILDIZ I F, "On the interdependence of distributed topology control and geographical routing in ad hoc and sensor networks", *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 3, pp 520-532, March, 2005.

[7] JEONG C, KIM I, and DONG K," Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system", *IEEE Transactions on Signal Processing,* vol. 60, no. 1, pp 310-325, January, 2012.

[8] MUKHERJEE A, "Imbalanced beamforming by a multi-antenna source for secure utilization of an untrusted relay", *IEEE Communications Letters,* vol. 17, no. 7, pp 1309-1312 , Jul. 2013.

[9] SHANNON C E, "Communication theory of secrecy systems", *Bell System Technical Journal,* vol. 28, pp 656-715, 1949.

[10] STAMP M. *Information security Principles and practice*, 2nd Edition , John Wiley & Sons, 2011.

[11] WHITMAN M, MATTORD H, *Principles of information security*, 4th Edition, Delmar Cengage Learning, 2012.

[12] ZOU Y, ZHU J, WANG X et al. , "Improving physical-layer security in wireless communications using diversity techniques", *IEEE Network,* vol. 29, no.1, pp 42-48, January, 2015.

[13] WYNER A D, "The wire-tap channel", *Bell System Technical Journal,* vol. 54, no. 8, pp 1355-1387, August. 1975.

[14] LEUNG-YAN-CHEONG S K, Hellman M E, "The Gaussian wiretap channel", *IEEE Transactions on Information Theory*, vol.24, pp451-456, July, 1978.

[15] Goel S ,Negi R, "Guaranteeing secrecy using artificial noise", *IEEE Transactions on Wireless Communications*, vol.7, no.6, pp2180-2189, July , 2008.

[16] ZHOU X, MCKAY M, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation", *IEEE Transactions on Vehicular Technology, vol.59, no.8, pp*3831-3842, August, 2010.

[17] GOECKEL D, VASUDEVAN S, TOWSLEY D et al. , "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks", *IEEE Journal on Selected Areas in Communications,* vol. 29, no. 10, pp 2067-2076, October, 2011.

[18] ZHANG J, GURSOY M C, "Collaborative Relay Beamforming for Secrecy", *IEEE International Conference on Communications*, Cape Town, South Africa, May , 2010.

[19] MUKHERJEE A, SWINDLEHURST A L, " Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI", *IEEE Transactions on Signal Processing*, vol. 59, no.1, pp 351-361, January, 2011.

[20] WANG G, GAO F, Wu Y C, et al. , "Joint CFO and Channel Estimation for OFDM-based Two-Way Relay Networks", *IEEE Transactions on Wireless Communications,* vol.10, no.2, pp 456-465, Feb-

ruary, 2011.
[21] ZOU Y, WANG X, SHEN W, "Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks", *IEEE Transactions on Communications,* vol. 61, no. 12, pp 5103-5113, December, 2013.
[22] YOU J, ZHONG Z, WANG G, et al. , "Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors", *IEEE Access,*vol.2, pp 1348-1358 , 2014.
[23] ZHU J, ZOU Y, WANG G, et al., " On Secrecy Performance of Antenna Selection Aided MIMO Systems Against Eavesdropping ", *IEEE Transactions on Vehicular Technology*, accepted, 2015. DOI: 10.1109/TVT. 2015. 2397195.

Biographies

WANG Yajun, received his M.S. degree in computer science from Anhui University, Hefei,Anhui, China ,in 2012. He is a Lecturer of School of Mathematical and Information Engineering in Anhui Science and Technology University. His main research interests include wireless network security, quality of service (QoS), and routing and congestion control protocols for ad hoc networks.E-mail: wangyajun_1978@sina.cn

LIAO Tongqing, Associate Professor at the School of Electronic and Information Engineering, AnHui University, Hefei, China. He received his M.S. degree in electronic science and technology from AnHui University, Hefei, China, and the Ph.D. degree in optical from Nankai University, Tianjin, China in 2005 and 2009 respectively. His research interests include microwave technology, antennas and propagation ,optical communication and fiber sensing technology.

WANG Chuanan, received his M.S. degree in School of Computer from Jiangsu University,Zhenjiang,Jiangsu,China,in 2010. He is currently working towards his Ph.D.degree at the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China. He is a Lecturer of School of Mathematical and Information Engineering in Anhui Science and Technology University. His research interests include network security and computer application technology.