Improving Physical-Layer Security in Wireless Communications Using Diversity Techniques

Yulong Zou, Jia Zhu, Xianbin Wang, and Victor C.M. Leung

Abstract

Due to the broadcast nature of radio propagation, wireless transmission can be readily overheard by unauthorized users for interception purposes and is thus highly vulnerable to eavesdropping attacks. To this end, physical-layer security is emerging as a promising paradigm to protect the wireless communications against eavesdropping attacks by exploiting the physical characteristics of wireless channels. This article is focused on the investigation of diversity techniques to improve physical-layer security differently from the conventional artificial noise generation and beamforming techniques, which typically consume additional power for generating artificial noise and exhibit high implementation complexity for beamformer design. We present several diversity approaches to improve wireless physical-layer security, including multiple-input multiple-output (MIMO), multiuser diversity, and cooperative diversity. To illustrate the security improvement through diversity, we propose a case study of exploiting cooperative relays to assist the signal transmission from source to destination while defending against eavesdropping attacks. We evaluate the security performance of cooperative relay transmission in Rayleigh fading environments in terms of secrecy capacity and intercept probability. It is shown that as the number of relays increases, both the secrecy capacity and intercept probability of cooperative relay transmission improve significantly, implying there is an advantage in exploiting cooperative diversity to improve physical-layer security against eavesdropping attacks.

In wireless networks, transmission between legitimate users can easily be overheard by an eavesdropper for interception due to the broadcast nature of the wireless medium, making wireless transmission highly vulnerable to eavesdropping attacks. In order to achieve confidential transmission, existing communications systems typically adopt the cryptographic techniques to prevent an eavesdropper from tapping data transmission between legitimate users [1, 2]. By considering symmetric key encryption as an example, the original data (called plaintext) is first encrypted at the source node by using an encryption algorithm along with a secret key that is shared only with the destination node. Then the encrypted plaintext (also known as ciphertext) is transmitted to the destination, which will decrypt its received ciphertext with the preshared secret key. In this way, even if an eavesdropper overhears the ciphertext transmission, it is still difficult for the eavesdropper to interpret the plaintext from its intercepted ciphertext without the secret key. It is pointed out that ciphertext transmission is not perfectly secure, since the ciphertext can still be decrypted by an eavesdropper through an exhaustive key search, which is also known as a brute-force attack. To this end, physical-layer security is emerging as an alternative paradigm to protect wireless communications against eavesdropping attacks, including brute-force attacks.

Physical-layer security work was pioneered by Wyner in [3], where a discrete memoryless wiretap channel was examined for secure communications in the presence of an eavesdropper. It was proved in [3] that perfectly secure data transmission can be achieved if the channel capacity of the main link (from source to destination) is higher than that of the wiretap link (from source to eavesdropper). Later on, in [4], Wyner's results were extended from the discrete memoryless wiretap channel to the Gaussian wiretap channel, where a so-called *secrecy capacity* was developed, and shown as the difference between the channel capacity of the main link and that of the wiretap link. If the secrecy capacity falls below zero, the transmission from source to destination becomes insecure, and the eavesdropper can succeed in intercepting the source transmission (i.e., an intercept event occurs). In order to improve transmission security against eavesdropping attacks, it is of importance to reduce the probability of occurrence of an intercept event (called *intercept probability*) through enlarging secrecy capacity. However, in wireless communications, secrecy capacity is severely degraded due to the fading effect.

Yulong Zou and Jia Zhu are with the Nanjing University of Posts and Telecommunications.

Xianbin Wang is with the University of Western Ontario.

Victor C.M. Leung is with the University of British Columbia.

As a consequence, there are extensive works aimed at increasing the secrecy capacity of wireless communications by exploiting multiple antennas [5] and cooperative relays [6]. Specifically, the multiple-input multiple-output (MIMO) wiretap channel was studied in [7] to enhance the wireless secrecy capacity in fading environments. In [8], cooperative relays were examined for improving the physical-layer security in terms of the secrecy rate performance. A hybrid cooperative beamforming and jamming approach was investigated in [9] to enhance the wireless secrecy capacity, where partial relay nodes are allowed to assist the source transmission to the legitimate destination with the aid of distributed beamforming, while the remaining relay nodes are used to transmit artificial noise to confuse the eavesdropper. More recently, a joint physical-application layer security framework was proposed in [10] for improving the security of wireless multimedia delivery by simultaneously exploiting physical-layer signal processing techniques as well as upper-layer authentication and watermarking methods. In [11], error control coding for secrecy was discussed for achieving the physical-layer security. Additionally, in [12, 13], physical-layer security was further investigated in emerging cognitive radio networks.

At the time of writing, most research efforts are devoted to examining the artificial noise and beamforming techniques to combat eavesdropping attacks, but they consume additional power resources to generating artificial noise and increase the computational complexity in performing beamformer design. Therefore, this article is motivated to enhance the physical-layer security through diversity techniques without additional power costs, including MIMO, multiuser diversity, and cooperative diversity, aimed at increasing the capacity of the main channel while degrading the wiretap channel. For illustration purposes, we present a case study of exploiting cooperative relays to improve the physical-layer security against eavesdropping attacks, where the best relay is selected and used to participate in forwarding the signal transmission from source to destination. We evaluate the secrecy capacity and intercept probability of the proposed cooperative relay transmission in Rayleigh fading environments. It is shown that with an increasing number of relays, the security performance of cooperative relay transmission significantly improves in terms of secrecy capacity and intercept probability. This confirms the advantage of using cooperative relays to protect wireless communications against eavesdropping attacks.

The remainder of this article is organized as follows. The next section presents the system model of physical-layer security in wireless communications. After that, we focus on the physical-layer security enhancement through diversity techniques, including MIMO, multiuser diversity, and cooperative diversity. For the purpose of illustrating the security improvement through diversity, we present a case study of exploiting cooperative relays to assist signal transmission from source to destination against eavesdropping attacks. Finally, we provide some concluding remarks.

Physical-Layer Security in Wireless Communications

Figure 1 shows a wireless communications scenario with one source and one destination in the presence of an eavesdropper, where the solid and dashed lines represent the main channel (from source to destination) and the wiretap channel (from source to eavesdropper), respectively. When the source node transmits its signal to the destination, an eavesdropper may overhear such transmission due to the broadcast nature of the wireless medium. Considering the fact that today's wireless systems are highly standardized, the eavesdropper can readily obtain the transmission parameters, including the signal waveform, coding and modulation scheme, encryption algorithm, and so on. Also, the secret key may be figured out at the eavesdropper (e.g., through an exhaustive search). Thus, the source signal could be interpreted at the eavesdropper by decoding its overheard signal, leading to insecurity of the legitimate transmission.

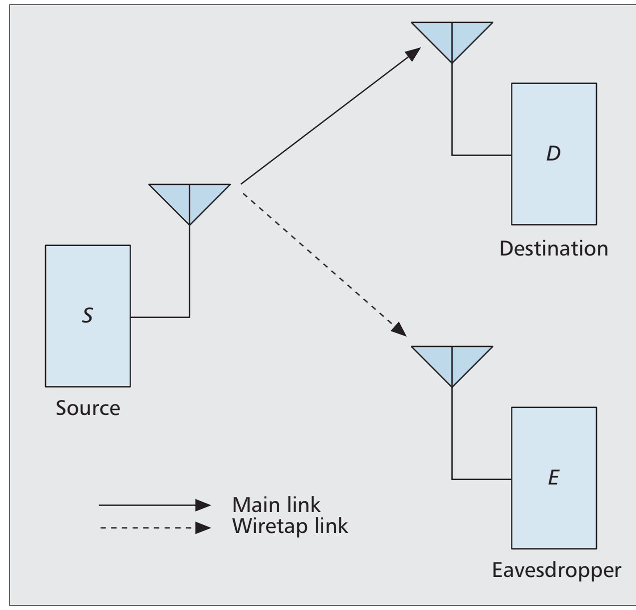

Figure 1. A wireless communications scenario consisting of one source and one destination in the presence of an eavesdropping attack.

As a result, physical-layer security emerges as an alternative means to achieve perfect transmission secrecy from source to destination. In the physical-layer security literature [3, 4], a so-called *secrecy capacity* is developed and shown as the difference between the capacities of the main link and the wiretap link. It has been proven that perfect secrecy is achieved if the secrecy capacity is positive, meaning that when the main channel capacity is larger than the wiretap channel capacity, the transmission from source to destination can be perfectly secure. This can be explained by using the Shannon coding theorem from which it is impossible for a receiver to recover the source signal if the channel capacity (from source to receiver) is smaller than the data rate. Thus, given a positive secrecy capacity, the data rate can be adjusted between the capacities of the main and wiretap channels so that the destination node successfully decodes the source signal and the eavesdropper fails to decode it. However, if the secrecy capacity is negative (i.e., the main channel capacity falls below the wiretap channel capacity), the eavesdropper is more likely than the destination to succeed in decoding the source signal. In an information-theoretic sense, when the main channel capacity becomes smaller than the wiretap channel capacity, it is impossible to guarantee that the destination succeeds and the eavesdropper fails to decode the source signal. Therefore, an intercept event is seen to occur when the secrecy capacity falls below zero, and the probability of occurrence of an intercept event is called *intercept probability* throughout this article.

At present, most existing work is focused on improving physical-layer security by generating artificial noise to confuse an eavesdropping attack, where the artificial noise is sophisticatedly produced such that only the eavesdropper experiences interference, and the desired destination can easily cancel out such noise without performance degradation. More specifically, given a main channel matrix $\mathbf{H}_m$, the artificial noise (denot-

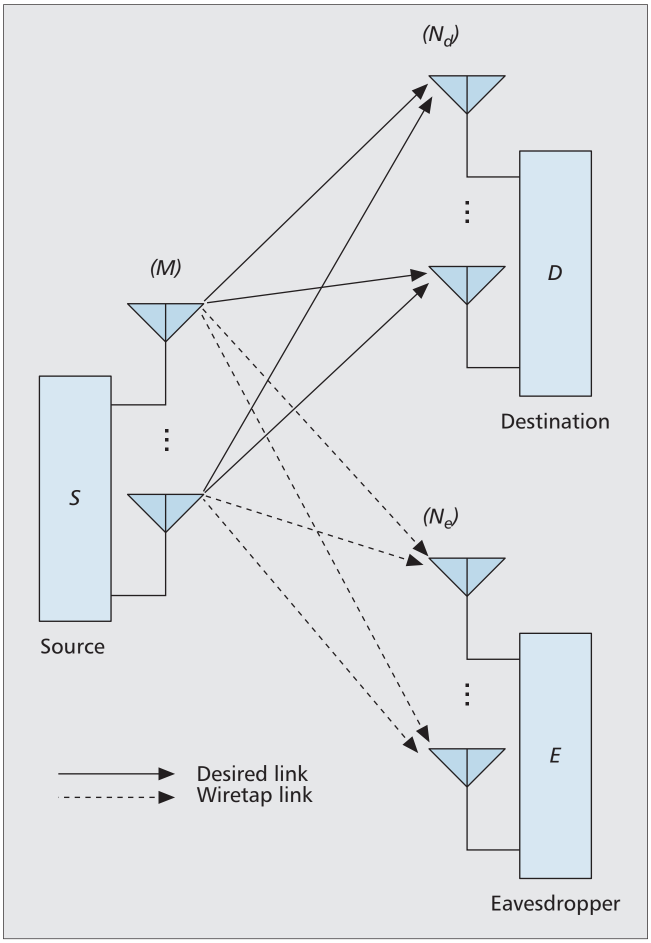

Figure 2. A MIMO wireless system consisting of one source and one destination in the presence of an eavesdropping attack.

ed by $\mathbf{w}_n$) is designed in the null space of matrix $\mathbf{H}_m$ such that $\mathbf{H}_m\mathbf{w}_n = 0$, making the desired destination unaffected by the noise. Since the wiretap channel is independent of the main channel, the null space of the wiretap channel is in general different from that of the main channel; thus, the eavesdropper cannot null out the artificial noise, which results in the performance degradation at the eavesdropper. Notice that the above-mentioned null space based noise generation approach needs the knowledge of main channel $\mathbf{H}_m$ only, which can be further optimized if the wiretap channel information is also known. It needs to be pointed out that additional power resources are required for generating artificial noise to confuse the eavesdropper. For a fair comparison, the total transmit power of artificial noise and desired signal should be constrained. Also, the power allocation between the artificial noise and desired signal is important, and should be adapted to the main and wiretap channels to optimize the physical-layer security performance, for example, in terms of secrecy capacity. Different from the artificial noise generation approach, this article is mainly focused on the investigation of diversity techniques for enhancing physical-layer security.

Diversity for Physical-Layer Security

In this section, we present several diversity techniques to improve physical-layer security against eavesdropping attacks. Traditionally, diversity techniques are exploited to increase transmission reliability, which also have great potential to enhance wireless security. In the following, we discuss the physical-layer security improvement through the use of MIMO, multiuser diversity, and cooperative diversity, respectively. Notice that the MIMO and multiuser diversity mechanisms are generally applicable to various cellular and WiFi networks, since the cellular and WiFi networks typically consist of multiple users, and, moreover, today's cellular and WiFi devices are equipped with multiple antennas. In contrast, the cooperative diversity mechanism is only applicable to some advanced cellular and WiFi networks that have adopted the relay architecture, such as the Long Term Evolution (LTE)-Advanced system and IEEE 802.16j/m, where relay stations are introduced to assist wireless data transmission.

MIMO Diversity

This subsection presents MIMO diversity for physical-layer security of wireless transmission against eavesdropping attacks. As shown in Fig. 2, all the network nodes are equipped with multiple antennas, where M, N_d, and N_e represent the number of antennas at the source, destination, and eavesdropper, respectively. As is known, MIMO has been shown as an effective means to combat wireless fading and increase the capacity of the wireless channel. However, the eavesdropper can also exploit the MIMO structure to enlarge the capacity of a wiretap channel from the source to the eavesdropper. Thus, without proper design, increasing the secrecy capacity of wireless transmission with MIMO may fail. For example, if conventional open-loop space-time block coding is considered, the destination should first estimate the main channel matrix $\mathbf{H}_m$ and then perform the space-time decoding process with an estimated $\hat{\mathbf{H}}_m$, leading diversity gain to be achieved for the main channel. Similarly, the eavesdropper can also estimate the wiretap channel matrix $\mathbf{H}_w$ and then conduct the corresponding space-time decoding algorithm to obtain diversity gain for the wiretap channel. Hence, the conventional space-time block coding is not effective to improve physical-layer security against eavesdropping attacks.

Generally speaking, if the source node transmits its signal to the desired destination with M antennas, the eavesdropper also receives M signal copies for interception purposes. In order to defend against eavesdropping attacks, the source node should adopt a preprocess that needs to be adapted to the main and wiretap channels $\mathbf{H}_m$ and $\mathbf{H}_w$ such that diversity gain can be achieved only at the destination, whereas the eavesdropper benefits nothing from the multiple transmit antennas at the source. This means that an *adaptive transmit process* should be included at the source node to increase the main channel capacity while decreasing the wiretap channel capacity. Ideally, the objective of such an adaptive transmit process is to maximize the secrecy capacity of MIMO transmission, which, however, requires the channel state information (CSI) of both the main and wiretap links (i.e., $\mathbf{H}_m$ and $\mathbf{H}_w$). In practice, the wiretap channel information $\mathbf{H}_w$ may be unavailable, since the eavesdropper is usually passive and stays silent. If only the main channel information $\mathbf{H}_m$ is known, the adaptive transmit process can be designed to maximize the main channel capacity, which does not require knowledge of wiretap channel $\mathbf{H}_w$. Since the adaptive transmit process is optimized based on the main channel information $\mathbf{H}_m$, and the wiretap channel is typically independent of the main channel, the main channel capacity is significantly increased with MIMO, and no improvement is achieved for the wiretap channel capacity.

As for the aforementioned adaptive transmit process, we here present three main concrete approaches: transmit beamforming, power allocation, and transmit antenna selection. Transmit beamforming is a signal processing technique combining multiple transmit antennas at the source node in such a way that desired signals transmit in a particular direction to the destination. Considering that the eavesdropper and destination generally lie in different directions relative to the source node, the desired signals (with transmit beamforming) received at the eavesdropper experience destructive interference and become very weak. Thus, transmit beamforming is effective in defending against eavesdropping attacks when the destination and eavesdropper are spatially separated. The power allocation maximizes the main channel capacity (or secrecy capacity if both $\mathbf{H}_m$ and $\mathbf{H}_w$ are known) by allocating the transmit power among M antennas at the source. In this way, the secrecy capacity of MIMO transmission is significantly increased, showing the security benefits of using power allocation against eavesdropping attacks. In addition, the transmit antenna selection is also able to improve the physical-layer security of MIMO wireless systems. Depending on whether the global CSI of the main and wiretap channels (i.e., $\mathbf{H}_m$ and $\mathbf{H}_w$) is available, an optimal transmit antenna at the source node is selected and used to transmit source signals. More specifically, if both $\mathbf{H}_m$ and $\mathbf{H}_w$ are available, the transmit antenna with the highest secrecy capacity is chosen. Studying the case of the global available CSI provides a theoretical upper bound on the security performance of wireless systems. Notice that the CSI of wiretap channels may be estimated and obtained by monitoring the eavesdroppers' transmissions as discussed in [8] and [14]. If only $\mathbf{H}_m$ is known, the transmit antenna selection is to maximize the main channel capacity. One can observe that the above-mentioned three approaches (i.e., transmit beamforming, power allocation, and transmit antenna selection) all have great potential to improve the physical-layer security of MIMO wireless systems against eavesdropping attacks.

Multiuser Diversity

This subsection discusses the multiuser diversity for improving physical-layer security. Figure 3 shows that a base station (BS) serves multiple users where M users are denoted by $\mathcal{U} = \{U_i | i = 1, 2, \cdots, M\}$. In cellular networks, M users typically communicate with a BS through an orthogonal multiple access mechanism such as orthogonal frequency-division multiple access (OFDMA) and time-division multiple access (TDMA). Taking OFDMA as an example, orthogonal frequency-division multiplexing (OFDM) subcarriers are allocated to different users. In other words, given an OFDM subcarrier, we need to determine which user should be assigned to access and use the subcarrier for data transmission. Traditionally, the user with the highest throughput is selected to access the given OFDM subcarrier, aiming to maximize the transmission capacity. This relies on knowledge of main channel information $\mathbf{H}_m$ only and can provide significant multiuser diversity gain for performance improvement. However, if a user is far away from a BS and experiences severe propagation loss and deep fading, it may have no chance of being selected as the "best" user for channel access. To this end, user fairness should be further considered in multiuser scheduling, where two competing interests need to be balanced: maximizing the main channel capacity while at the same time guaranteeing each user with certain opportunities to access the channel.

With multiuser scheduling, a user is first selected to access a channel (i.e., an OFDM subcarrier in OFDMA or a time slot in TDMA) and then starts transmitting its signal to a BS. Meanwhile, due to the broadcast nature of wireless transmission, an eavesdropper overhears such transmission and attempts to interpret the source signal. In order to effectively defend against the eavesdropping attack, multiuser scheduling should be performed to minimize the wiretap channel capacity

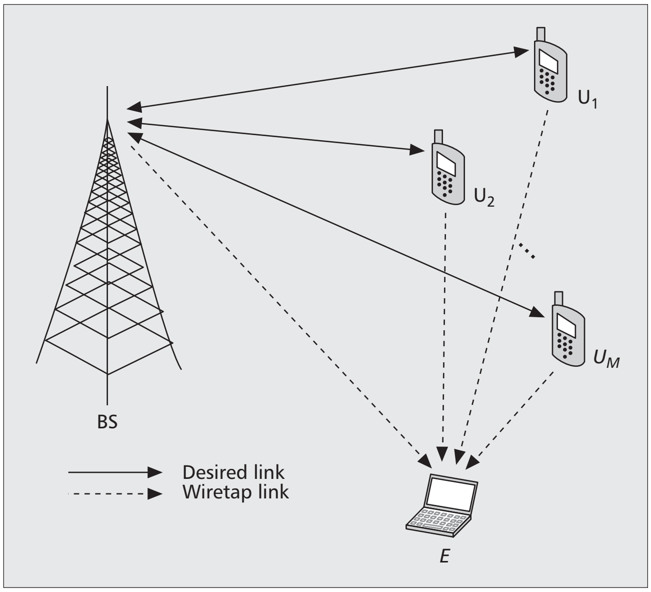

Figure 3. A multiuser wireless communications system consisting of one base station (BS) and multiple users in the presence of an eavesdropper.

while maximizing the main channel capacity, which requires the CSI of both the main and wiretap links. If only the main channel information $\mathbf{H}_m$ is available, we may consider the use of conventional multiuser scheduling where the wiretap channel information $\mathbf{H}_w$ is not taken into account. It needs to be pointed out that conventional multiuser scheduling still has great potential to enhance physical-layer security, since the main channel capacity is significantly improved with conventional multiuser scheduling while the wiretap channel capacity remains the same.

Cooperative Diversity

In this subsection, we focus mainly on cooperative diversity for wireless security against eavesdropping attacks. Figure 4 shows a cooperative wireless network including one source, M relays, and one destination in the presence of an eavesdropper, where M relays are exploited to assist the signal transmission from source to destination. To be specific, the source node first transmits its signal to M relays, which then forward their received source signals to the destination. At present, there are two basic relay protocols: amplify-and-forward (AF) and decode-and-forward (DF). In the AF protocol, a relay node simply amplifies and retransmits its received noisy version of the source signal to the destination. In contrast, the DF protocol requires the relay node to decode its received signal and forward its decoded outcome to the destination node. It is concluded that multiple-relay-assisted source signal transmission consists of two steps:

1. The source node broadcasts its signal.
2. Relay nodes retransmit their received signals.

Each of the two transmission steps is vulnerable to eavesdropping attack and needs to be carefully designed to prevent an eavesdropper from intercepting the source signal.

Typically, the main channel capacity with multiple relays can be significantly increased by using cooperative beamforming. More specifically, multiple relays can form a virtual antenna array and cooperate with each other to perform transmit beamforming such that the signals received at the intended destination experience constructive interference, while the others (received at the eavesdropper) experience destructive interference. One can observe that with cooperative beamforming, the received signal strength of the destina-

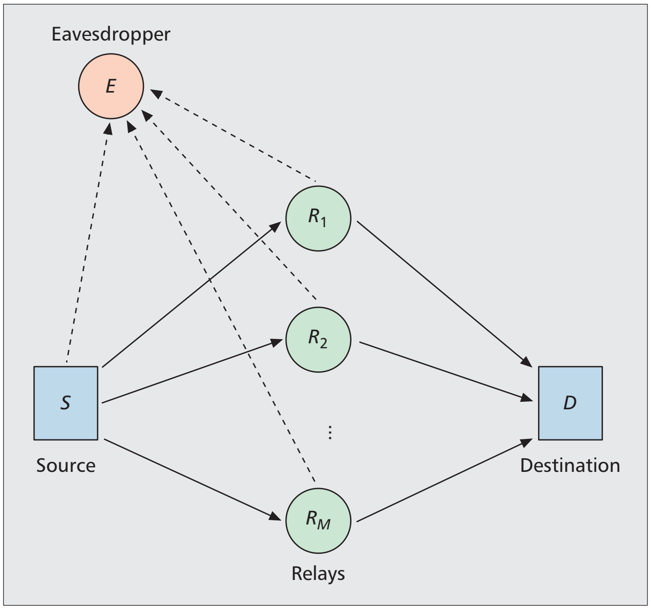

Figure 4. A cooperative diversity system consisting of one source, M relays, and one destination in the presence of an eavesdropper.

tion is much higher than that of the eavesdropper, implying physical-layer security improvement. In addition to the aforementioned cooperative beamforming, the best relay selection is another approach to improve wireless transmission security against eavesdropping attacks. In the best relay selection, a relay node with the highest secrecy capacity (or highest main channel capacity if only the main channel information is available) is chosen to participate in assisting the signal transmission from source to destination. In this way, cooperative diversity gain is achieved for physical-layer security enhancement.

Case Study: Security Evaluation of Cooperative Relay Transmission

In this section, we present a case study to show the physical-layer security improvement by exploiting cooperative relays, where only a single best relay is selected to assist the signal transmission from source to destination. This differs from existing research efforts in [8], where multiple cooperative relays participate in forwarding the source signal to the destination. For comparison purposes, we first consider conventional direct transmission as a benchmark scheme, where the source node directly transmits its signal to the destination without relay. Meanwhile, an eavesdropper is present and attempts to intercept the signal transmission from source to destination. As discussed in [3, 4], the secrecy capacity of conventional direct transmission is shown as the difference between the capacities of the main channel (from source to destination) and the wiretap channel (from source to eavesdropper), which is written as

$$C_s = \log_2\left(1+\frac{P|h_{sd}|^2}{N_0}\right) - \log_2\left(1+\frac{P|h_{se}|^2}{N_0}\right), \tag{1}$$

where P is the transmit power at the source, N_0 is the variance of additive white Gaussian noise (AWGN), $\gamma_s = P/N_0$ is regarded as the signal-to-noise ratio (SNR), and h_{sd} and h_{se} represent fading coefficients of the channel from source to destination and from source to eavesdropper, respectively. Presently, there are three commonly used fading models (i.e., Rayleigh, Rician, and Nakagami), and we consider the use of theRayleigh fading model to characterize the main and wiretap channels. Thus, $|h_{sd}|^2$ and $|h_{se}|^2$ are independent and exponentially distributed random variables with means σ_{sd}^2 and σ_{se}^2, respectively. Also, an ergodic secrecy capacity of the direct transmission can be obtained by averaging the instantaneous secrecy capacity C_s^+ over the fading coefficients h_{sd} and h_{se}, where $C_s^+ = \max(C_s, 0)$. In addition, if the secrecy capacity C_s falls below zero, the source transmission becomes insecure, and the eavesdropper will succeed in intercepting the source signal. Thus, using Eq. 1 and denoting $x = |h_{sd}|^2$ and $y = |h_{se}|^2$, an intercept probability of the direct transmission can be given by

$$\begin{aligned} P_{\text{intercept}} &= \Pr(C_s < 0) \\ &= \Pr\left(|h_{sd}|^2 < |h_{se}|^2\right) \\ &= \iint_{x<y} \frac{1}{\sigma_{sd}^2\sigma_{se}^2}\exp\left(-\frac{x}{\sigma_{sd}^2}-\frac{y}{\sigma_{se}^2}\right)dx\,dy \\ &= \frac{\sigma_{se}^2}{\sigma_{sd}^2+\sigma_{se}^2}, \end{aligned} \tag{2}$$

where the third equation arises from the fact that random variables $|h_{sd}|^2$ and $|h_{se}|^2$ are independent exponentially distributed, and σ_{sd}^2 and σ_{se}^2 are the expected values of $|h_{sd}|^2$ and $|h_{se}|^2$, respectively. As can be observed from Eq. 2, the intercept probability of conventional direct transmission is independent of the transmit power P, meaning that increasing the transmit power cannot improve physical-layer security in terms of intercept probability. This motivates us to explore the use of cooperative relays to decrease the intercept probability. For notational convenience, let λ_{me} represent the ratio of average main channel gain σ_{sd}^2 to an eavesdropper's average channel gain σ_{se}^2, that is, $\lambda_{me} = \sigma_{sd}^2/\sigma_{se}^2$, which is referred to as the main-to-eavesdropper ratio (MER) throughout this article. In the following, we present the cooperative relay transmission scheme where multiple relays are used to assist the signal transmission from source to destination. Here, the AF relaying protocol is considered, and only the best relay will be selected to participate in forwarding the source signal to the destination. To be specific, the source node first broadcasts its signal to M relays. Then the best relay node is chosen to forward a scaled version of its received signal to the destination [15]. Note that during the above mentioned cooperative relay transmission process, the total amount of transmit power at source and relay should be constrained to P to make a fair comparison with the conventional direct transmission scheme. We here consider the equal power allocation; thus, the transmit power at the source and relay is given by $P/2$.

Now, given M relays, it is crucial to determine which relay should be selected as the best one to assist the source signal transmission. Ideally, the best relay selection should aim to maximize the secrecy capacity, which, however, requires the CSI of both the main and wiretap channels. Since the eavesdropper is passive, and the wiretap channel information is difficult to obtain in practice, we consider the main channel capacity as the objective of best relay selection, which relies on knowledge of the main channel only. Accordingly, the best relay selection criterion with AF protocol is expressed as

$$\text{Best Relay} = \arg\max_{i\in\mathcal{R}} \frac{|h_{si}|^2|h_{id}|^2}{|h_{si}|^2+|h_{id}|^2}, \tag{3}$$

where $\mathcal{R}$ denotes a set of M relays, and $|h_{si}|^2$ and $|h_{id}|^2$ represent fading coefficients of the channel from source to relay R_i and that from relay R_i to destination, respectively. One can see from Eq. 3 that the proposed best relay selection criterion only requires the main channel information, $|h_{si}|^2$ and $|h_{id}|^2$, with which the main channel capacity is maximized. Since the main and wiretap channels are independent of each other, the wiretap channel capacity will benefit nothing from the proposed best relay selection. Similar to Eq. 1, the secrecy capacity of best relay selection can be obtained through subtracting the main channel capacity from the corresponding wiretap channel capacity. Also, the intercept probability of best relay selection is easily determined by computing the probability that the secrecy capacity becomes less than zero.

In Fig. 5, we provide the ergodic secrecy capacity comparison between the conventional direct transmission and proposed best relay selection schemes for different numbers of relays M with γ_s = 12 dB, σ_{sd}^2 = 0.5, and $\sigma_{sr}^2 = \sigma_{rd}^2 = 2$. It is shown in Fig. 5 that for the cases of M = 2, M = 4, and M = 8, the ergodic secrecy capacity of the best relay selection scheme is always higher than that of direct transmission, showing the wireless security benefits of using cooperative relays. Also, as the number of relays M increases from M = 2 to M = 8, the ergodic secrecy capacity of best relay selection significantly increases. This means that increasing the number of cooperative relays can improve the physical-layer security of wireless transmission against eavesdropping attacks.

Figure 6 shows the intercept probability vs. MER of the conventional direct transmission and proposed best relay selection schemes for different numbers of relays M with γ_s = 12 dB, σ_{sd}^2 = 0.5, and $\sigma_{sr}^2 = \sigma_{rd}^2 = 2$. Note that the intercept probability is obtained by calculating the rate of occurrence of an intercept event when the capacity of the main channel falls below that of the wiretap channel. Observe from Fig. 6 that the best relay selection scheme outperforms conventional direct transmission in terms of intercept probability. Moreover, as the number of cooperative relays M increases from M = 2 to M = 8, the intercept probability improvement of best relay selection over direct transmission becomes much more significant. It is also shown from Fig. 6 that the slope of the intercept probability curve of the best relay selection scheme in high MER regions becomes steeper with an increasing number of relays. In other words, as the number of relays increases, the intercept probability of best relay selection decreases at a much higher speed with an increasing MER. This further confirms that the diversity gain is achieved by the proposed relay selection scheme for physical-layer security improvement.

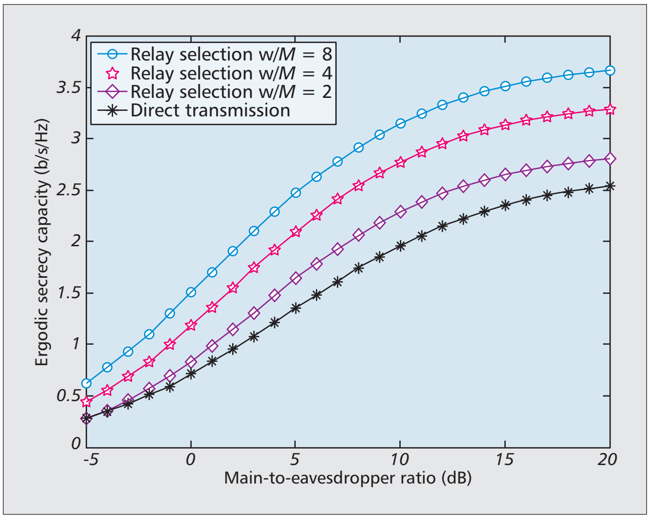

Figure 5. Ergodic secrecy capacity vs. MER of the direct transmission and best relay selection schemes with γ_s = 12 dB, σ_{sd}^2 = 0.5, and $\sigma_{sr}^2 = \sigma_{rd}^2 = 2$.

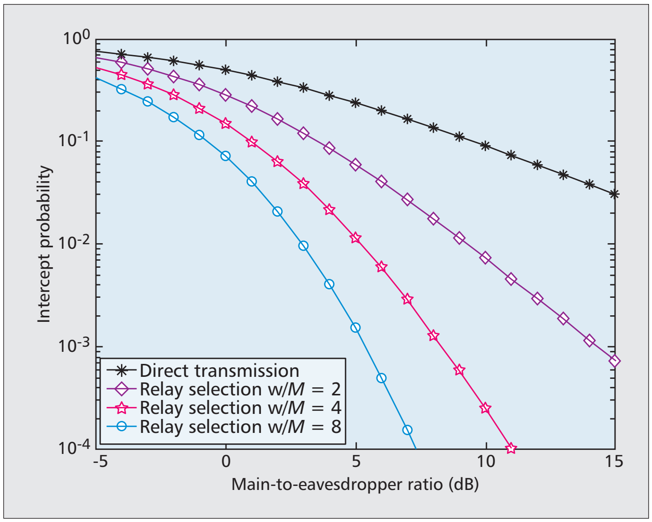

Figure 6. Intercept probability vs. MER of the direct transmission and best relay selection schemes with γ_s=12 dB, σ_{sd}^2 = 0.5, and $\sigma_{sr}^2 = \sigma_{rd}^2 = 2$.

Conclusion

This article studies physical-layer security of wireless communications and presents several diversity techniques for improving wireless security against eavesdroping attacks. We discuss the use of MIMO, multiuser diversity, and cooperative diversity for the sake of increasing the secrecy capacity of wireless transmission. To illustrate the security benefits through diversity, we propose a case study of physical-layer security in cooperative wireless networks with multiple relays, where the best relay is selected to participate in forwarding the signal transmission from source to destination. The secrecy capacity and intercept probability of the conventional direct transmission and proposed best relay selection schemes are evaluated in Rayleigh fading environments. It is shown that the best relay selection scheme outperforms direct transmission in terms of both secrecy capacity and intercept probability. Moreover, as the number of cooperative relays increases, the security improvement of the best relay selection scheme over direct transmission becomes much more significant.

Although extensive research efforts have been devoted to wireless physical-layer security, many challenging but interesting issues remain open for future work. Specifically, most of the existing works in this subject are focused on enhancing the wireless secrecy capacity against the eavesdropping attack only, but have neglected the joint consideration of different types of wireless physical-layer attacks, including both eavesdropping and denial of service (DoS) attacks. It is of great importance to explore new techniques of jointly defending against multiple different wireless attacks. Furthermore, security, reliability, and throughput are the main driving factors for the research and development of next-generation wireless networks, which are typically coupled and affect each other. For example, the security of the wireless physical layer may be improved by generating artificial noise to confuse an eavesdropping attack, which, however, comes at the expense of degrading wireless reliability and throughput performance, since artificial noise generation consumes some power resources, and less transmit power becomes available for the desired information transmission. Thus, it is of interest to investigate the joint optimization of security, reliability, and throughput for the wireless physical layer, which is a challenging issue to be solved in the future.

Acknowledgment

This work was supported by the "1000 Young Talents Program" of China, the National Natural Science Foundation of China (Grant No. 61302104), and the Scientific Research Foundation of Nanjing University of Posts and Telecommunications (Grant No. NY213014).

References

[1] M. E. Hellman, "An Overview of Public Key Cryptography," *IEEE Commun. Mag.*, vol. 16, no. 6, May 2002, pp. 42–49.

[2] S. V. Kartalopoulos, "A Primer on Cryptography In Communications," *IEEE Commun. Mag.*, vol. 20, no. 4, Apr. 2006, pp. 146–51.

[3] A. D. Wyner, "The Wire-Tap Channel," *Bell Sys. Tech. J.*, vol. 54, no. 8, Aug. 1975, pp. 1355–87.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wiretap Channel," *IEEE Trans. Info. Theory*, vol. 24, no. 7, July 1978, pp. 451–56.

[5] G. J. Foschini and M. J. Gans, "On Limits of Wireless Communications in a Fading Environment when Using Multiple Antennas," *Wireless Personal Commun.*, vol. 6, no. 3, Mar. 1998, pp. 311–35.

[6] Y. Zou, Y.-D. Yao, and B. Zheng, "Opportunistic Distributed Space-Time Coding For Decode-And-Forward Cooperation Systems," *IEEE Trans. Signal Processing*, vol. 60, no. 4, Apr. 2012, pp. 1766–81.

[7] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Trans. Info. Theory*, vol. 57, no. 8, Aug. 2011, pp. 4961–72.

[8] L. Dong *et al.*, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Trans. Signal Processing*, vol. 58, no. 3, Mar. 2010, pp. 1875–88.

[9] H.-M. Wang *et al.*, "Hybrid Cooperative Beamforming and Jamming for Physical-Layer Security of Two-Way Relay Networks," *IEEE Trans. Info. Forensics Sec.*, vol. 8, no. 12, Dec. 2013, pp. 2007–20.

[10] L. Zhou *et al.*, "Joint Physical-Application Layer Security for Wireless Multimedia Delivery," *IEEE Commun. Mag.*, vol. 52, no. 3, Mar. 2014, pp. 66–72.

[11] W. Harrison *et al.*, "Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security," *IEEE Signal Processing Mag.*, vol. 30, no. 5, Sept. 2013, pp. 41–50.

[12] Z. Shu, Y. Qian, and S. Ci, "On Physical Layer Security for Cognitive Radio Networks," *IEEE Network*, vol. 27, no. 3, June 2013, pp. 28–33.

[13] Y. Zou, X. Wang, and W. Shen, "Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks," *IEEE Trans. Commun.*, vol. 61, no. 12, Dec. 2013, pp. 5103–13.

[14] M. Bloch *et al.*, "Wireless Information-Theoretic Security," *IEEE Trans. Info. Theory*, vol. 54, no. 6, June 2008, pp. 2515–34.

[15] Y. Zou, X. Wang, and W. Shen, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks," *IEEE JSAC*, vol. 31, no. 10, Oct. 2013, pp. 2099–2111.

Biographies

YULONG ZOU [S'07, M'12, SM'13 (yulong.zou@njupt.edu.cn) is a professor at Nanjing University of Posts and Telecommunications (NUPT), China. He received his B.Eng. degree in information engineering from NUPT in July 2006, his first Ph.D. degree in electrical engineering from the Stevens Institute of Technology, New Jersey, in May 2012, and his second Ph.D. degree in signal and information processing from NUPT in July 2012.

JIA ZHU (jiazhu@njupt.edu.cn) is an associate professor at the Nanjing University of Posts and Telecommunications NUPT. She received her B.Eng. degree in computer science and technology from Hohai University, Nanjing, China, in July 2005, and her Ph.D. degree in signal and information processing from NUPT in April 2010.

XIANBIN WANG [S'98, M'99, SM'06] (xianbin.wang@uwo.ca) is a professor at the University of Western Ontario and a Canada Research Chair in Wireless Communications. He received his Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2001.

VICTOR C. M. LEUNG [S'75, M'89, SM'97, F'03] (vleung@ece.ubc.ca) is a professor in electrical and computer engineering, and holds the TELUS Mobility Research Chair at the University of British Columbia, Vancouver, Canada, where he received his Ph.D. and B.A.Sc. degrees in electrical engineering in 1977 and 1982, respectively. He is a Fellow of the Royal Society of Canada, the Canadian Academy of Engineering, and the Engineering Institute of Canada.