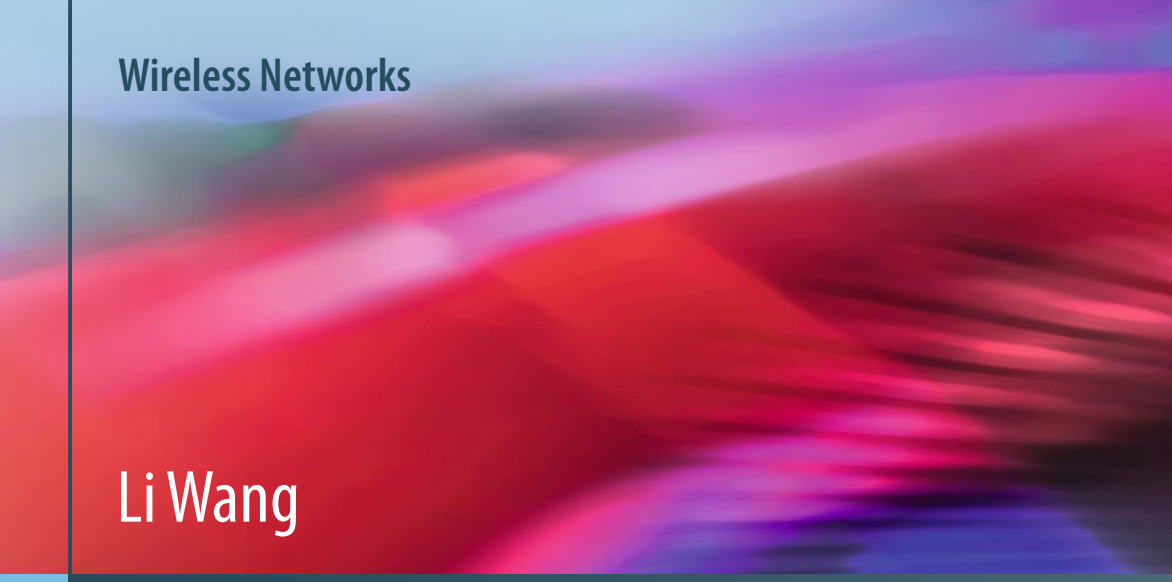


Wireless Networks

Li Wang

Physical Layer Security in Wireless Cooperative Networks

Springer

Wireless Networks

Series editor

Xuemin (Sherman) Shen
University of Waterloo, Waterloo, Ontario, Canada

More information about this series at http://www.springer.com/series/14180

Li Wang

Physical Layer Security in Wireless Cooperative Networks

Springer

Li Wang
School of Electronic Engineering
Beijing University of Posts and Telecommunications
Beijing, China

ISSN 2366-1186 ISSN 2366-1445 (electronic)
Wireless Networks
ISBN 978-3-319-61862-3 ISBN 978-3-319-61863-0 (eBook)
DOI 10.1007/978-3-319-61863-0

Library of Congress Control Number: 2017948731

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To my family, friends, and students
- Li Wang

Acknowledgments

The author sincerely acknowledges the support from the National Natural Science Foundation of China under Grant No. 61571056, the open research fund of the National Mobile Communications Research Laboratory of Southeast University (China) under Grant 2016D04.

Special thanks to Prof. Sherman Shen who made this book possible. The author would like to express her deepest gratitude to Prof. Gordon L. Stüber of Georgia Institute of Technology (Gatech), Prof. Zhu Han of the University of Houston (UH), and Prof. Bingli Jiao of Peking University for their advice during the writing of this monograph.

The author would also like to express appreciation to graduate students Ruoguang Li, Qing Wei, and Yutong Ai of Beijing University of Posts and Telecommunications (BUPT), and Yingyang Chen of Peking University for their strong support during the preparation of this monograph.

Contents

Acronyms

3GPP	Third generation partnership project
AES	Advanced encryption standard
AF	Amplify-and-forward
AN	Artificial noise
AP	Access point
APM	Amplitude phase modulation
AWGN	Additive white Gaussian noise
BD	Block diagonalization
BER	Bit error rate
BPSK	Binary phase shift keying
BS	Base station
CAS	Centralized antenna system
CDMA	Code division multiple access
CIR	Channel impulse response
CR	Cognitive radio
CRN	Cognitive radio network
CRP	China restaurant process
CSI	Channel state information
CSIR	Channel state information at receiver
CSIT	Channel state information at transmitter
CUE	Cellular user equipment
D2D	Device-to-device
DARPA	Defense Advanced Research Projects Agency
DAS	Distributed antenna system
DBF	Distributed beamforming
DF	Decode-and-forward
DL	Downlink
DMC	Discrete memoryless channel
DSA	Dynamic spectrum access
DT	Direct transmission

DTR	Distributed time reversal
DUE	Device-to-device user equipment
EGT	Equal gain transmission
GA	Genetic algorithm
GSSK	Generalized space shift keying
IAS	Inter antenna synchronization
ICI	Inter channel interference
IFC	Interference channel
IoT	Internet of things
ISI	Inter symbol interference
LDPC	Low density parity check
LoS	Line-of-sight
LTE	Long term evolution
LTE-A	Long term evolution advanced
M2M	Machine-to-machine
MAC	Multiple access channel/media access control
MIMO	Multiple input multiple output
MIMOME	Multiple input multiple output multiple-antenna eavesdropper
MISO	Multiple input single output
MISOME	Multiple input single output multiple-antenna eavesdropper
MISOSE	Multiple input single output single-antenna eavesdropper
ML	Maximum likelihood
MMSE	Minimum mean square error
MRC	Maximal ratio combining
MRT	Maximal ratio transmission
MU-MIMO	Multiuser multiple input multiple output
OFDM	Orthogonal frequency division multiplexing
OSR	Outage secrecy region
P2P	Peer-to-peer
PDF	Probability density function
PN	Pseudo noise
PSM	Precoding-aided spatial modulation
PU	Primary user
QAM	Quadrature amplitude modulation
QoS	Quality of service
RB	Resource block
RRC	Root-raised cosine
RSA	Rivest-Shamir-Adleman
SA	Simulated annealing
SC	Selection combining
SDMA	Space division multiple access
SDoF	Secrecy degrees of freedom
SEE	Secrecy energy efficiency
SINR	Signal-to-interference plus noise ratio
SM	Spatial modulation

SNR	Signal-to-noise ratio
SSK	Space shift keying
STD	Space time diversity
SU	Secondary user
SVD	Singular value decomposition
TAS	Transmit antenna selection
TCP	Transport control protocol
TDD	Time division duplexing
TR	Time reversal
UHF	Ultra-high frequency
UL	Uplink
UWB	Ultra wideband
V2V	Vehicle-to-vehicle
V-BLAST	Vertical-Bell Laboratories Layered Space-Time
WSN	Wireless sensor network
ZF	Zero forcing

Notations

$\mathscr{CN}(\mu, \sigma^2)$	Complex Gaussian distribution with mean μ and variance σ^2
$H(X)$	Shannon entropy of discrete random variable X
$H(X\|Y)$	Conditional entropy of X given Y
$\mathbb{R}$	Field of real numbers
$\mathbb{C}$	Field of complex numbers
$I(X;Y)$	Mutual information of discrete variables X and Y
$[x]^+$	Positive part of x, which is $\max(0, x)$
$\delta(t)$	Dirac delta function/unit-impulse function
$h^*(t)$	Conjugate transpose of $h(t)$
$\otimes$	Convolution operation
$p_\tau(t)$	Probability density function of random variable τ
$\mathrm{E}(f(x))$	Expectation of function $f(x)$
C_N^n	The number of n-combination from a given set of N elements
Diag	Diagonal matrix
$\|\cdot\|$	Absolute value
$\parallel \mathbf{x} \parallel$	Euclidean norm of vector $\mathbf{x}$
$\mathbf{x}^T$	Transpose of vector $\mathbf{x}$
$\mathbf{x}^H$	Hermitian transpose of $\mathbf{x}$
$\mathbf{x}^{-1}$	Inverse of $\mathbf{x}^{-1}$
$\mathbf{h}$	Column vector
$\mathbf{H}$	Matrix
$Tr(\mathbf{H})$	Trace of matrix $\mathbf{H}$
$\mathbf{H}_\perp$	Null space of matrix $\mathbf{H}$
$\mathbf{det}(\mathbf{H})$	Determinant of matrix $\mathbf{H}$
$\mathbf{H}^{-1}$	Reverse of matrix $\mathbf{H}$
$\mathbf{Exp}(\lambda)$	Exponential distribution with mean λ
$\lambda_{max}(\mathbf{A}, \mathbf{B})$	Maximum generalized eigenvalue of matrices pair $(\mathbf{A}, \mathbf{B})$

Chapter 1
Introduction

1.1 Basics of Physical Layer Security

Wireless communication is one of important means for connecting everyone from anywhere in the world at any time. Though the prevalence of wireless technologies brings many advantages, the nonnegligible fact is that the users are more exposed to the attacks of adversaries due to the broadcast nature of wireless signals. In view of that, the communication security has been drawn more and more attention. The traditional manner to reinforce the security of communication is to use the encryption techniques to protect user data in the upper layers of the communication stack. Even though current efforts provide solutions from certain perspectives, these methods are neither adaptive nor flexible enough to provide security mechanism due to the computational tasks and system complexity. Furthermore, the characteristics of wireless channels, such as difference, reciprocity and so forth, make it possible to transmit signals safely between transmitter and receiver in the physical layer. Such an idea has been verified to effectively improve the security of communication. With the development of wireless communication techniques, physical layer security has become one of hot topics. In this section, we will give some brief introduction about physical layer security from concept, technical evolution, to its applications in wireless networks.

1.1.1 Concept and Evolution of Physical Layer Security

1.1.1.1 Shannon's Pioneering Work

The typical network where issues of secrecy and confidentiality are considered in the physical layer is a three-node system involving a transmitter, a legitimate receiver, and an adversary, wherein the transmitter wishes to send a private message

L. Wang, *Physical Layer Security in Wireless Cooperative Networks*, Wireless Networks, DOI 10.1007/978-3-319-61863-0_1

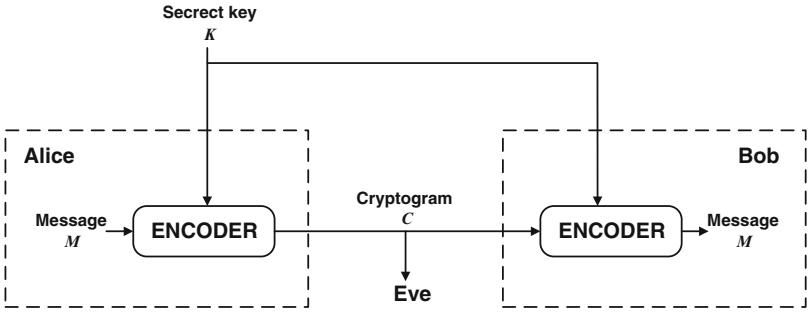


Fig. 1.1 Shannon's model of a secrecy system

to the receiver without the interception or attack from the adversary. Generally, the transmitter, the receiver, and the adversary are often referred to "Alice", "Bob", and "Eve", respectively. The basic principle of physical layer security can be traced back to the information-theoretic model of crypto-system introduced by Shannon. In his classic treatise in 1949 [1], Shannon presented a secrecy system where a non-reusable private key K is used by both the transmitter and legitimate receiver to encrypt the confidential message M. M is encrypted into a codeword C, which can be also observed by the adversary during the transmission, as shown in Fig. 1.1. Herein, the perfect secrecy can be achieved if the *a posteriori* probability of the secret message calculated by the adversary is equal to the *a priori* probability of the message [2]. From the information-theoretic perspective, it can be expressed as

$$H(M|C) = H(M), \tag{1.1}$$

where $H(M|C)$ is the conditional entropy of the message under the given cryptotext C, or the eavesdropper's *equivocation*. Equation (1.1) can be expressed in a more familiar manner

$$I(M;C) = 0, \tag{1.2}$$

where $I(\cdot;\cdot)$ is mutual information. Equation (1.2) indicates that M and C are statistically independent. The absence of correlation ensures that there is no method for the adversary to obtain the message. So the *perfect secrecy* can be guaranteed only if $H(K) \geq H(M)$, i.e., the secret key K should have at least as much entropy as the message M, or the uncertainty about the key must be at least as high as the uncertainty about the message [3].

A classic method to achieve the perfect secrecy is Vernam's one-time pad cipher [4] in the subsequent years, where the binary message or ciphertext is XORed. However, it is hard to be implemented in practice because it needs to produce a huge number of random keys, which needs to be managed and assigned in a more difficult way.

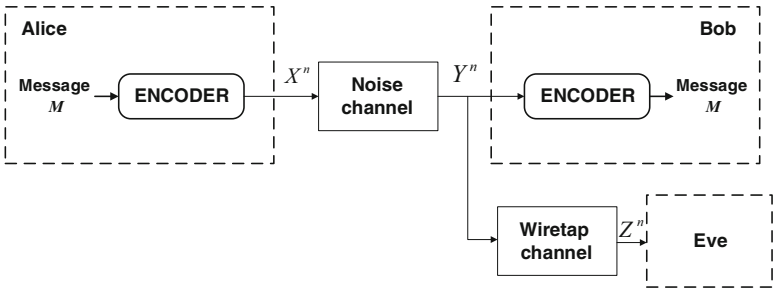


Fig. 1.2 Wyner's wiretap channel model [5]

1.1.1.2 Wyner's Wiretap Channel

In 1975, Wyner led to a new era in information-theoretic security by proposing the *wiretap channel* in [5]. Compared with Shannon's original secrecy system, Wyner's system considered random noise channel which is regarded as an intrinsic element of physical communications, and both the legitimate channel and wiretap channel are modeled as the discrete memoryless channels (DMC). Besides, the transmitter encodes the message M into a codeword X^n consisting of n symbols, where $X^n = [X_1, \ldots, X_n]$, and then is sent to the legitimate receiver as a degraded message Y^n, where $Y^n = [Y_1, \ldots, Y_n]$ and via a wiretap channel to the adversary as Z^n, where $Z^n = [Z_1, \ldots, Z_n]$, as shown in Fig. 1.2.

In addition, Wyner suggested an alternative definition for the perfect secrecy. Instead of holding the Eq. (1.1), a new secrecy condition is required that the *equivocation rate* $R_e = (1/n)H(M|Z^n)$ should be close to the *entropy rate* R of the message $(1/n)H(M)$ when n is sufficiently large. Note that $R - R_e = (1/n)I(M; Z^n)$ means the information that is leaked to the adversary. Thus, message M is gradually perfectly secure from the adversary if $(1/n)I(M; Z^n) \leq \varepsilon$ [6]. Moreover, Wyner defined the *secrecy capacity* as the supremum of achievable transmission rates to the legitimate receiver at which one can guarantee reliability and information-theoretic security against the eavesdropper.

1.1.1.3 General Wiretap Channel Scenarios

After Wyner's far-reaching work, in 1978 Csiszàr and Körner considered a non-degraded version of Wyner's system in broadcast channel with two receivers [7], as shown in Fig. 1.3. Private message is transmitted to the first receiver and common message is transmitted to both receivers, while keeping the second receiver as ignorant of the private messages as possible. They obtained the characterization of private message rate, equivocation rate, and common message rate, with achievable triples. In this case where no common messages exist, the secrecy capacity is achieved by maximizing overall joint probability distributions such that a Markov

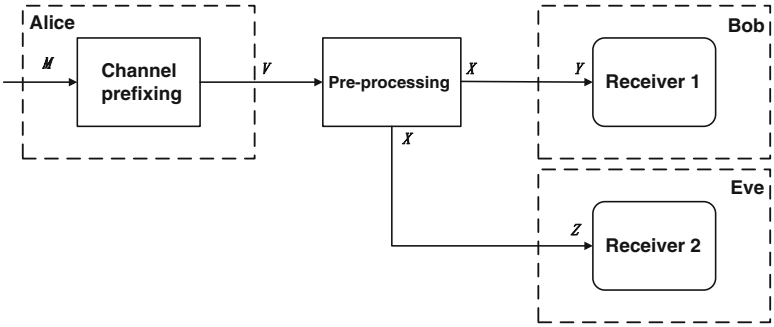


Fig. 1.3 General wiretap channel model (Csiszàr and Körner's work)

chain $V \to X \to YZ$ holds, is defined as

$$C_s = \max_{V \to X \to YZ} I(V;Y) - I(V;Z), \tag{1.3}$$

where V is a purposely designed auxiliary variable. Moreover, when the wiretap channel is degraded, i.e., X, Y, Z form a Markov chain $X \to Y \to Z$, the secrecy capacity expression reduces to [8]

$$C_s = \max_{X} I(X;Y) - I(X;Z). \tag{1.4}$$

We can see that due to the Markov chain, there is no need for channel prefixing, so the auxiliary random variable V disappears.

Soon after, in [9] Cheong and Hellman examined the secrecy capacity for Gaussian degraded wiretap channel, assuming that all channels are discrete memoryless real channels. They presented that both the legitimate channel and wiretap channel can be maximized, and the secrecy capacity is the difference between the capacities of the main and wiretap channel, which can be given by

$$C_s = C_M - C_W = \frac{1}{2}\log_2(1 + \frac{P}{\sigma_M^2}) - \frac{1}{2}\log_2(1 + \frac{P}{\sigma_W^2}), \tag{1.5}$$

where P is the transmit power, σ_M^2 and σ_W^2 are the variances of noise in legitimate channel and wiretap channel, respectively. In general, it is expected that the legitimate channel has a larger Signal-to-Noise Ratio (SNR) than that of the eavesdropper, so the secrecy capacity should be a positive value which can be expressed as

$$C_s = [C_M - C_W]^+, \tag{1.6}$$

where $[x]^+ = \max(0, x)$.

Moreover, the secrecy capacity in complex Additive White Gaussian Noise (AWGN) fading channels has been investigated by many researchers and can be expressed as [10, 11]

$$C_s = [\log_2(1 + \frac{P \mid h_M \mid^2}{\sigma_M^2}) - \log_2(1 + \frac{P \mid h_W \mid^2}{\sigma_W^2})]^+, \tag{1.7}$$

where h_M and h_W are the channel gains of legitimate and wiretap channel, respectively. In the following parts of this book, we only consider the complex AWGN fading channels for convenience.

1.1.1.4 Multiple-Antenna System

With the development of wireless techniques, the communication facilities can be equipped with multiple antennas. By exploiting multiple antennas on the transmitter and receiver, i.e., Multiple-Input-Multiple-Output technique (MIMO), the reliability and efficiency of communication system can be significantly improved. It has been verified that the MIMO technique is one of the most powerful tools for secure communications. The work by Hero [12] was the first to consider secret communication in a MIMO system, promoting a concerted development in terms of applying and extending the single-antenna wiretap model to a multi-antenna one. In a general scenario where a fading MIMO wiretap channel is considered, Alice, Bob, and Eve are equipped with multiple antennas, namely Multiple-Input-Multiple-Output Multiple-antenna Eavesdropper (MIMOME) as shown in Fig. 1.4. In this case, the secrecy capacity can be expressed as [13]

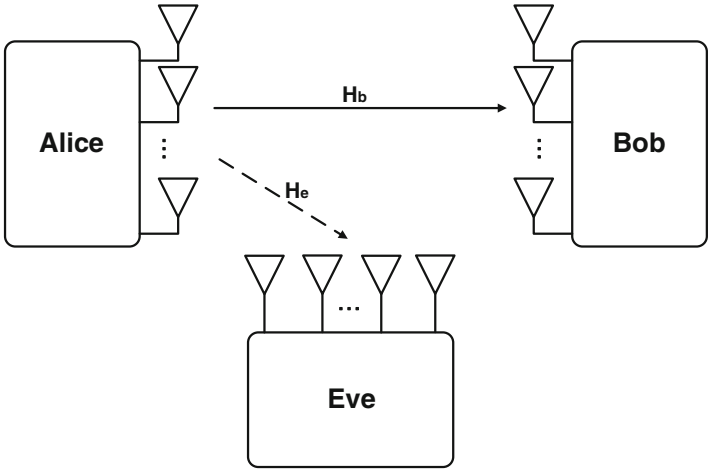


Fig. 1.4 MIMO wiretap channel model (MIMOME)

$$C_s = \max_{\mathbf{K_x} \succ \mathbf{0}, \mathbf{tr}(\mathbf{K_x}) \preceq P} \frac{\log\det(\mathbf{I} + \mathbf{H_b}\mathbf{K_x}\mathbf{H_b}^H)}{\log\det(\mathbf{I} + \mathbf{H_e}\mathbf{K_x}\mathbf{H_e}^H)}, \tag{1.8}$$

where $\mathbf{K_x}$ is the covariance matrix of the transmit signal $\mathbf{x}$, P is the power constraint, $\mathbf{H_b} \in \mathbb{C}^{N_r \times N_t}$ and $\mathbf{H_e} \in \mathbb{C}^{N_e \times N_t}$ are the MIMO complex Gaussian channel matrices of legitimate link and wiretap link, respectively.

With the fast development of MIMO techniques, both the industrial and academic fields were also inspired and paid more attention on physical layer security by considering other scenarios. The basic system model has been extended to a more complicated one, such as multiple antenna channel [15], relay channel [16], interference channel (IFC) [17], multiple access channel (MAC) [18], and multiuser channel [19], etc.

1.1.2 The Relationship Between Cryptography and Physical Layer Security

1.1.2.1 The Differences Between Encryption and Physical Layer Security

Figure 1.5 illustrates the fundamental differences between cryptography and physical layer security [20]. Cryptographic encryption is a conventional way for protecting data transmission. In general, related methods are implemented in the upper layer of the protocol stack of the networking architecture to achieve information security. The basic idea of cryptography is using a *secret key* to encrypt the transmitted signal at the source and convert it into ciphertext. For instance, the combination of state-of-the-art algorithms like Rivest-Shamir-Adleman (RSA) and

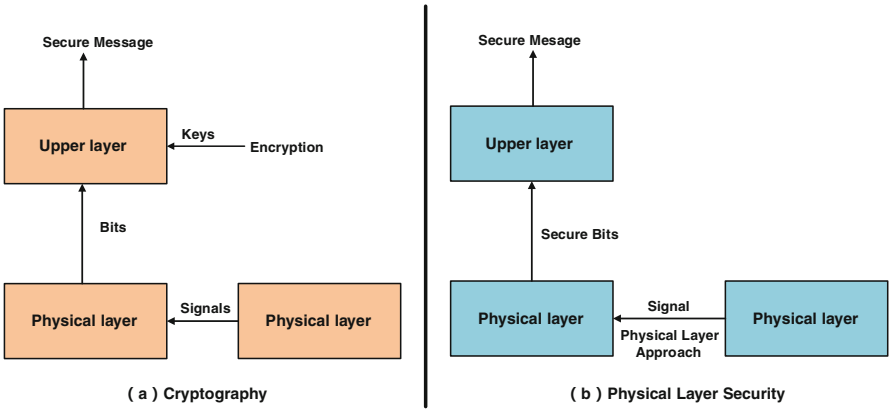


Fig. 1.5 The difference between cryptography and physical layer security approaches [20]. (**a**) Cryptography. (**b**) Physical layer security

the Advanced Encryption Standard (AES) is deemed secure for a large number of applications [21]. But it is true that for the encryption systems, the secret key distribution and management is very vulnerable in wireless networks, since the eavesdroppers can easily intercept the transmission of secret key due to the broadcast nature of the wireless medium. In contrast, physical layer security approaches can prevent data transmission form interception, by exploiting the characteristics of wireless channels via appropriate signaling and channel coding without upper layer data encryption. One of the most important advantages of physical layer security comes from the facts that the related approaches achieve provable security regardless of the unlimited computational power the eavesdroppers may possess. However, we must admit that there are also some disadvantages in physical layer security. It always relies on average information measures, so it might not be possible to guarantee confidentiality with probability one [22]. Moreover, we also need to make assumptions about the conditions of the communication channels that might not be accurate in practice.

1.1.2.2 Cooperating with Upper layers: Cross-Layer Protocols for Physical Layer Security

Although Fig. 1.5 indicates that the secrecy approaches at physical layer can guarantee the security independently of cryptography, it also has potential to cooperate with upper encryption methods for further enhancing security performance. Designing protocols that combine traditional cryptographic techniques with physical layer techniques, which are so called *cross-layer protocols*, is also a promising way. An essential part of this research is how to design a standard that makes an accurate assessment on the performance of cross-layer designing schemes. Xiao et al. [23] considered that in a wireless sensor network, the cross layer design should work collaboratively to detect the adversaries while enabling the efficient power consumption. A cross-layer scheme for secure communication in an MIMO system has been proposed in [24], which combines the spatial modulation and upper layer key stream. This scheme can effectively control the space modulation/demodulation process by sharing two control sequences between two legitimate users, which are formed by the upper layer key stream. Unknown the control sequences, the eavesdropper can only use the traditional spatial demodulation method to guess the control sequence so the eavesdropper is impossible to restore the original signal. Besides, a cross-layer security policy in a relay cooperative network has been studied in [25]. In the proposed scheme, some of the relays cooperate for enhancing physical layer security performance, while the others ensure information security rely on upper layer crypto-system. In [26], medium access control (MAC) layer is exploited to further improve the secure communication of the physical layer. The design of MAC protocol used to consider the link quality, transmission rate, and transmission delay. But in this scheme, MAC protocol will accomplish the packet transmission, when the secrecy rate or secrecy capacity satisfies the requirement for guaranteeing the secure transmission in the physical layer. Otherwise,the transmission will stop so as to achieve the secure transmission of communication.

1.1.3 Classification of Attacks in Physical Layer Security

According to the different abilities of illegitimate nodes, attacks in the physical layer security can be categorized into two aspects: passive attacks and active attacks.

- **Passive attacks**: illegitimate node plays a role as an ***eavesdropper*** which does not transmit any signal so it can conceal its presence. Therefore, it is not going to disrupt network operation, and the goal of the node is to intercept transmitted information from legitimate wireless channels [27]. In some cases, such node can further analyze the information received from Alice. Thus, we have to prevent the eavesdroppers from intercepting the information by elaborately designing the signal.
- **Active attacks**: illegitimate node is able to afford the risk of being detected by the legitimate nodes, and then it has a powerful ability to actively attack. Such node plays a role as a ***spoofer*** to transmit a deceiving signal to generate confusion at Bob, intercepts and forges messages to deteriorate the security performance. Such type of attacks is also referred to *masquerade attack* [28]. On the other side, malicious node also has capability of being a ***jammer*** to transmit a noisy signal to Bob for interrupting the communication [29]. When Bob receives desired signal and jamming signal at the same time, legitimate signal would be less trustworthy. Therefore, the signal would not be decoded. Active attacks can significantly influence the normal network operations because an adversary often tries to change the network data. When the attack is held, it needs to be identified by legitimate users, and the signal needs to be protected accordingly.

1.1.4 Performance Metrics in Physical Layer Security

The conventional encryption systems always testify the performance of the encryption algorithm by measuring the number of attacks that the system suffered. In contrast, there are different performance measurements in physical layer security according to different communication scenarios.

1.1.4.1 Key Factor: Channel State Information (CSI)

In wireless communications, channel state information (CSI), which is sometimes also known as channel gain, refers to the knowledge of channel properties about a wireless communication link. CSI describes how a signal propagates from the transmitter to the receiver and represents the corresponding effect, such as scattering, fading and power attenuation with distance. The CSI makes it possible to adapt transmissions to current channel conditions, which is crucial for achieving reliable communications with high data rates in multi-antenna systems. The method for obtaining CSI is called channel estimation. In general, the CSI at the transmitter and receiver is different, and the CSI at the transmitter is referred to CSIT and the other at the receiver is referred to CSIR.

Typically, the CSI can be classified as two categories: namely *instantaneous CSI* and *statistical CSI*.

- **Instantaneous CSI**: the channel conditions in the current time slot are known, which can be regarded as having the knowledge of the impulse response of the filter. Instantaneous CSI gives an opportunity to allow the transmitted signal to adapt the impulse response and thereby optimize the received signal for achieving higher data rate and lowering bit error rates. In some cases where the instantaneous CSI of whole wireless nodes are known, we can say that the ***full CSI*** of the wireless communication system is known.
- **Statistical CSI**: when the instantaneous CSI cannot be obtained, a statistical characterization of the channel can be used. This knowledge generally involves some statistical information, such as the fading distribution, the average channel gain, the line-of-sight (LoS) component, and the spatial correlation. Similar to the case of instantaneous CSI, this information also can be used for resource optimization or scheduling. In some cases where the instantaneous CSI of some nodes and the statistical CSI of others are known, we can say that the ***partial CSI*** of the system is obtained.

The availability of CSI plays a very important role in designing the optimal transmission strategy and choosing a proper secrecy performance metric in physical layer security. In general, in order to maximize the achievable secrecy rate, both instantaneous CSI of main channel and wiretap channel are needed. Once the full CSI is available, secrecy performance can be considerably improved by maximizing the received SNR at the destination, while minimizing the received SNR at the eavesdroppers. However, in practice, full CSI may not be obtained due to the estimation error, or the intentionally concealing of eavesdropper, which will negatively impact the secrecy performance. For example, when CSI estimation error exists, jamming signals for disturbing eavesdroppers cannot be perfectly eliminated at the destination, which will cause interference to the legitimate channel consequently. Likewise, lacking of eavesdropper's CSI will impact the signal design at the transmitter to protect against interception. In this case, we often assume that the statistic CSI of the wiretap channel can be obtained according to the propagation environment, to maximize the ergodic secrecy rate or minimize the secrecy outage probability. Next, we will give some details about the corresponding performance metrics.

1.1.4.2 Secrecy Rate

In most cases, the problem of obtaining secrecy capacity is very difficult since we have to solve a optimization problem with probability distribution of transmitted message X. The secrecy rate of Gaussian noise wiretap channel is defined as the difference between the achievable rates of the main channel and the wiretap channel with Gaussian codebook [30]. It can be expressed as

$$R_s = [R_b - R_e]^+, \tag{1.9}$$

where R_b and R_e are the achievable rate of legitimate link and eavesdropping link, respectively. In general, secrecy capacity C_s is the maximum achievable perfect secrecy rate R_s.

1.1.4.3 Ergodic Secrecy Capacity/Rate

Secrecy capacity/rate is often used under the assumption of fixed channels, and usually does not take the channel fading into consideration. To characterize the time varying feature of a channel, the ergodic secrecy capacity is considered if the secrecy message spans sufficient channel realizations to capture the ergodic features of the channel. Ergodic secrecy capacity measures the average ability of secrecy transmission over fading channels, which can be achieved by performing rate and power adaption according to CSI.

Ergodic secrecy capacity is for the case of both CSI of the main channel and legitimate channel are known, and the case of only CSI of main channel is known, have been investigated in [31]. If the full CSI is known, it means that the probability density function (PDF) can be obtained. Likewise, knowing the partial CSI means that only the PDF of main channel can be obtained. Averaging over all fading realizations, we can formulate the ergodic secrecy capacity of fading channels with full CSI as [31]

$$\begin{aligned}\tilde{C}_s^{Full} &= \max_{\mathrm{E}\{P(|h_M|^2,|h_E|^2)\}\le\overline{P}} \mathrm{E}[C_M - C_E]^+ \\ &= \max_{P\left(|h_M|^2,|h_E|^2\right)} \int_0^\infty \int_{h_E}^\infty \left[\log\left(1+|h_M|^2 P\left(|h_M|^2,|h_E|^2\right)\right)\right. \\ &\quad \left. -\log\left(1+|h_E|^2 P\left(|h_M|^2,|h_E|^2\right)\right)\right] \\ &\quad f\left(|h_M|^2\right) f\left(|h_E|^2\right) d|h_M|^2 d|h_E|^2, \end{aligned} \tag{1.10}$$

where h_M and h_E are the channel gains of main channel and wiretap channel, respectively. $f(|h_M|^2)$ and $f(|h_E|^2)$ are the PDFs of $|h_M|^2$ and $|h_E|^2$, respectively. $\mathrm{E}\{P(|h_M|^2, |h_E|^2)\} \le \overline{P}$ means the optimal power allocation policy should satisfy the average transmit power constraint. Similarly, when only the channel gain of the legitimate receiver is known at the transmitter, the secrecy capacity is written as [31]

$$\begin{aligned}\tilde{C}_s^{Partial} &= \max_{\mathrm{E}\{P(|h_M|^2)\}\le\overline{P}} \mathrm{E}[C_M - C_E]^+ \\ &= \max_{P\left(|h_M|^2\right)} \int\int \left[\log\left(1+|h_M|^2 P\left(|h_M|^2\right)\right) - \log\left(1+h_E P\left(|h_M|^2\right)\right)\right]^+ \\ &\quad f\left(|h_M|^2\right) f\left(|h_E|^2\right) d|h_M|^2 d|h_E|^2. \end{aligned} \tag{1.11}$$

Note that the optimal transmission scheme is allowed only when $|h_M|^2 > |h_E|^2$. Though Eqs. (1.10) and (1.11) have a similar form, the optimization of power control policies are different according to the obtained CSI.

The achievable ergodic secrecy rate is strictly smaller than secrecy capacity. Nevertheless, in most cases it is more computationally efficient, which is usually taken as the optimization objective function, being a lower bound of the ergodic secrecy capacity [32].

1.1.4.4 Secrecy Outage Probability

In some scenarios, Alice does not have the perfect CSI of Bob and Eve. Therefore, the secrecy outage probability is considered as the performance metric. When the current secrecy rate R_s is not more than a pre-defined threshold R_0, the secrecy outage occurs, which means the current secrecy rate cannot guarantee the security requirement. The secrecy outage probability is the probability for measuring the likeness that the secrecy outage happens with a particular fading distribution [33]:

$$P_{out} = Pr\{R_s < R_0\}, R_0 > 0. \tag{1.12}$$

Equation (1.12) can be interpreted as two aspects: (1) it involves the outage probability that Bob cannot decode the received signal from Alice; (2) it also involves how safe about the transmit signal from Alice.

1.1.4.5 Secrecy Outage Capacity

The largest secrecy rate that can be achieved with a certain outage probability is referred to secrecy outage capacity. Mathematically, the secrecy outage capacity can be defined as the largest secrecy rate R_0 when the secrecy outage probability is less than or equal to a certain value ε_0 [33]:

$$R_0 = P_{out}^{-1}(\varepsilon_0), \tag{1.13}$$

where $P_{out}^{-1}(\cdot)$ is the inverse function of Eq. 1.12. Therefore, perfect secrecy transmission at a rate R_s can only be guaranteed by a probability $1 - P_{out}$.

1.1.4.6 Secrecy Region/Outage Secrecy Region

Secrecy region is used to measure the security performance from the perspective of large scale fading channel, which is defined as a geometrical region in which the secrecy capacity is positive. Assume that (x_e, y_e) is the coordinates of the eavesdropper, secrecy region can be expressed as a set of coordinates [34]

$$R_{region} = \{(x_e, y_e), C_e(x_e, y_e) < C_m\}, \tag{1.14}$$

where $C_e(x_e, y_e)$ is the capacity of the wiretap channel with geographical coordinate (x_e, y_e), C_m is the capacity of main channel. In addition, secrecy region also can indicate that a region in which Eve cannot appear. In [35], Chang et al. proposed a similar term *secure zone* in which inside a certain radius of the transmitter, the eavesdropper is not present.

Besides, Li et al. first proposed *Outage Secrecy Region* (OSR) [36]. For a given transmission rate R_0 and a pre-defined outage probability ε, OSR is defined as a region in which the secrecy outage probability with the given R_0 is not larger than ε, and can be formulated as

$$R_{region-out} = \{\theta_e | P_{out}(R < R_0) \leq \varepsilon\}, \tag{1.15}$$

where θ_e is the geographical coordinate vector of Eve, with respect to the position of Alice, which is chosen to be the origin of the coordinate system.

1.1.4.7 Secrecy Degrees of Freedom

In some scenarios, especially where multiple users exist, it is hard to find the exact secrecy region. In such case, the secrecy degrees of freedom (SDoF) is studied [37, 38], which is the pre-log[1] of the secrecy capacity at high SNR and captures the asymptotic behavior of the achievable secrecy rate in high SNR regime. The SDoF can be formulated as [39]

$$SDoF = \lim_{\rho \to \infty} \frac{R_s(\rho)}{\log_2(\rho)}, \tag{1.16}$$

where ρ represents SNR.

1.1.4.8 Other Performance Metrics

According to different scenarios in terms of physical layer security, some conventional measurements can be used to test the security performance, such as SNR, signal-to-interference plus noise ratio (SINR), mean square error (MSE), and bit error rate (BER), etc. By using such measurements, the system security can be improved while the quality of service (QoS) and the effectiveness of the coding scheme can be guaranteed. For example, strategies of physical layer security based on signal processing method can take advantage of more traditional performance metrics by designing transmission schemes for decreasing the BER at eavesdroppers to pre-defined thresholds [40].

[1] For the case in which capacity increases logarithmically in the SNR, pre-log means the asymptotic ratio between channel capacity and the logarithm of SNR.

Moreover, the energy consumption is also an inevitable problem. In general, a myriad of optimal power allocation schemes are proposed to achieve the maximum secrecy rate/capacity. And in recent researches, a novel criteria *secrecy energy efficiency* (SEE) [41] is widely used which is defined as the ratio between the channel capacity and total consumed energy [42],

$$SEE = \frac{C_s}{E_{total}} \quad \text{bits/joule}, \tag{1.17}$$

where C_s is the secrecy capacity and E_{total} is the total energy consumed by the system.

1.2 Overview of Wireless Cooperative Networks

The origin of *cooperate* comes from the Latin words *co-* and *operate*, whose connotation is "working together". Cooperation indicates the process of a group of people or animals working together for achieving a common goal or mutual benefit. Inspired by the cooperative behaviors in nature, especially among human beings, researchers exploit ideas of cooperation in terms of wireless communication networks. In the past decades, wireless cooperative networks are gaining more and more attention since such network paradigms can remarkably improve capability of wireless communications and provide a more flexible environment. In the following part, we will illustrate the concept of cooperation in terms of classification, technical aspect, and some typical applications.

1.2.1 Classification of Wireless Cooperative Networks

Cooperation has different connotations and meanings in wireless communications. Fitzek's book [43] gave the detailed description of classification of cooperation in wireless networks. Here we categorize the cooperative wireless networks mainly from the technical perspective, in which cooperation in wireless networks involves a number of techniques making use of the synergetic interaction of wireless partners for achieving high performance. From an upper layer aspect, or so-called "macro" in Fitzek's book, techniques like cooperative diversity, cooperative coding, cooperative protocols, etc, can be used for enhancing the performance. Besides, from a lower layer aspect, or so-called "micro" in the book, cooperation includes the concreted designs of virtual staff, such as signals, functions, algorithms, processing elements, etc., based on different scenarios and requirement of wireless communication environment. Figure 1.6 illustrates the classification of cooperation in wireless networks as described above. Now we will consider some examples of practical applications.

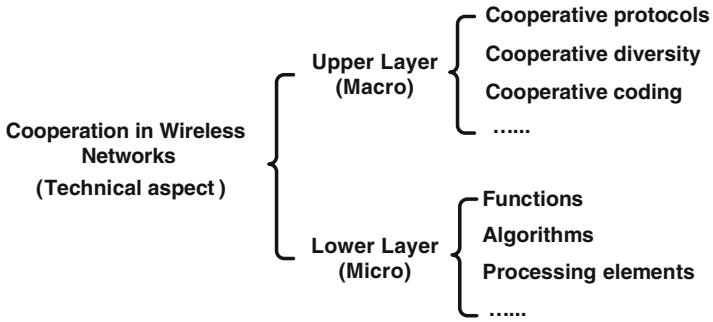


Fig. 1.6 Illustration of classification of cooperation from technical aspect [43]

1.2.1.1 Cooperative Protocols

The idea of cooperative protocols comes from Fitzek's book [43]. **Transport Control Protocol (TCP)** and **ALOHA** protocol are good examples for cooperative protocols. TCP is one of the main transport protocols in the Internet, improving fairness among users by using a flow control. The flow control limits a user to occupy the maximum link capacity for protecting routers in the Internet being overloading, causing unacceptable delays and losses for other traffic links which go through such routers [44].

The ALOHA protocol is another example of cooperative protocols that is a simple medium access protocol with a minimum signaling overhead. It was invented by the University of Hawaii in the 70s and then became the reference for many other protocols. ALOHA was designed for distributed wireless systems without central control. The protocol allows users to access the central computer via the wireless medium under a number of rules. Whenever a station has a packet to send, it does so. For achieving the successful reception, it is important to ensure that only one wireless node is transmitting at one time slot.

1.2.1.2 Cooperative Diversity

The term "cooperation" in wireless communications is often referred to *relaying*. Relaying is a technique to virtually extend the communication range with the help of the wireless nodes to forward transmitted signals. Cooperative diversity, which can be interpreted as a virtual multiple antenna technique based on multiple relays, can improve the networks performance, e.g., maximize total network throughput while enhancing the reliability of the system. By doing so, user diversity is exploited by jointly decoding the signal from the relay and the transmitter. In a conventional direct transmission, the receiver only decodes the signal based on the direct link while regarding the signals from other links as interference, but the cooperative diversity considers the other signals as supplement.

The ground-breaking work of Cover and Gamal for the information-theoretic characteristics of relay channel [45] can be viewed as the first work on cooperative diversity. About 20 years later, Sendonaris et al. published a number of far-reaching papers for relay channels, inspiring and motivating much of the recent researches in terms of wireless cooperative networks. One of the prominent works is illustrated in [46], in which the authors proposed a two-user cooperation for CDMA system, and verified that relay cooperation can significantly improve the system throughput and extend the coverage. Besides, the remarkable contributions from Laneman, whose Ph.D thesis [47] studied the transmission schemes and performance metrics of certain important relaying protocols in fading environment, also facilitated the development of cooperative diversity.

There are at least two fundamental relaying protocols based on which the source and relay nodes can provide some help for forwarding the signals to achieve the highest throughput possible for any known coding scheme. Such relaying protocols can be classified as decode-and-forward relay and amplify-and-forward relay [48]:

- **Decode-and-Forward (DF)**: the relay has ability of decoding its received signal, which will be re-encoded by the relay and forwarded then. The DF protocol is nearly optimal if the quality of the channel from the transmitter to relay is perfect, which practically happens when the source and relay are geographically close to each other.
- **Amplify-and-Forward (AF)**: the relay just amplifies the received signal (including the noise) and retransmits a degraded version of the initial signal, conditioned on the level of transmit power. Though noise is amplified due to the forwarding, the receiver can benefit from the cooperation by combining the two independently received signals from the source and relay, respectively.

1.2.1.3 Cooperative Coding

Though DF and AF protocols have ability of improving system reliability and throughput, there are still some weaknesses to limit the performance: (1) both protocols cannot fully exploit the spectral efficiency since some retransmission will happen if the error occurs; (2) DF protocol could even transmit the incorrectly decoded signals, and AF protocol could transmit the noise version of signals to deteriorate the performance; (3) in order to obtain the maximum likelihood (ML) detection, both AF and DF protocols need to know the BER and SNR about the users' channels. However, in practice, it is difficult to have as much as enough information to recover the analog signal.

In view of that, Hunter and Nosratinia proposed a novel strategy namely cooperative coding [49, 50], which is a method that combines cooperation with channel coding schemes. The basic idea of coded cooperation is sending each user's codewords via two fading links which are independent with each other. The principle behind coded cooperation is that each user in wireless networks tries to transmit incremental redundancy for his partner. Figure 1.7 shows how the

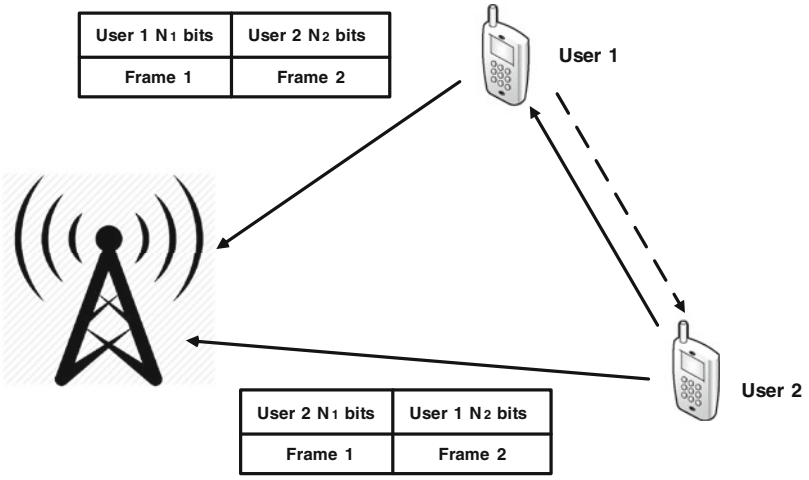


Fig. 1.7 Coded cooperation [50]

coded cooperation works. In the first frame, user 1 and user 2 transmit a codeword consisting of the N_1-bit code partition. Both users in the wireless networks also try to decode the signal from its partner. By checking the CRC code, the users can determine whether such attempt is successful. In the second frame, both users calculate and transmit the second code partition of its partner, containing N_2 bits. Otherwise, the user transmits its own second partition, again containing N_2 bits. Thus, each user always transmits a total of $N = N_1 + N_2$ bits over the two frames [51].

Stefanov and Erkip designed and analyzed the cooperative codes for slow fading environments [52]. They demonstrated that an overall block fading channel model is appropriate in the case of user-cooperation, since the cooperating terminals observe independently faded channels towards the destination. Chakrabarti et al. proposed an irregular expurgated coding protocol in a relay network, and a density evolution approach is used for code design. The proposed coding scheme is based on conventional density evolution, by which the performance are approximated to that of standard LDPC codes with low computational resource [53]. In addition, the integration of network coding and cooperative diversity is also investigated in [54], in which the network coding can provide a better channel among users than that employing time sharing, so a higher cooperative diversity can be achieved.

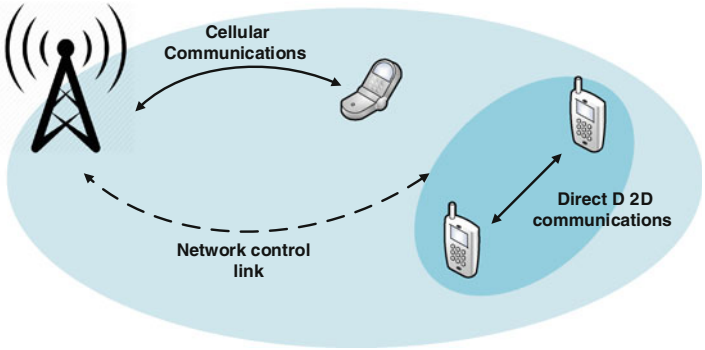


Fig. 1.8 D2D communications

1.2.2 Applications of Wireless Cooperative Networks

1.2.2.1 Device-to-Device (D2D) Networks

With the drastic emergence of a myriad of smart phones, user demands for mobile broadband are undergoing an unprecedented rise. The considerable growth of applications that need more bandwidth such as video streaming and multimedia file sharing have already exposed the limits of current cellular system. To handle such problems, Third Generation Partnership Project (3GPP) Long Term Evolution (LTE) is planning to provide technologies for high data rates and spectral efficiency. Device-to-Device (D2D) communications, as a technology component for LTE-Advanced (LTE-A), allows direct wireless links between mobile users without routing data through a network infrastructure [55]. The mobile users communicate directly without transmitting the information through the base station (BS), while just remaining controlled under the BS, as shown in Fig. 1.8. Therefore, to some extent, D2D communications can improve system throughput, increasing spectrum efficiency and energy efficiency, and reduce transmission delay, etc.

1.2.2.2 Ad Hoc Networks

The term “ad hoc” indicates that the network is typically established for some special applications, which are served in an extemporaneous manner. All of wireless nodes in an ad hoc network are willing to transmit data to other nodes, without forming a pre-existing configuration [56]. The earliest wireless ad hoc networks were called “packet radio” networks in early 70s, which were constructed by the Defense Advanced Research Projects Agency (DARPA), which promoted the basic principles of wireless ad hoc networks. Wireless mobile ad hoc networks are dynamic networks in which nodes can move and self-configure without any limitation. Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks for their common purpose, as shown in Fig. 1.9.

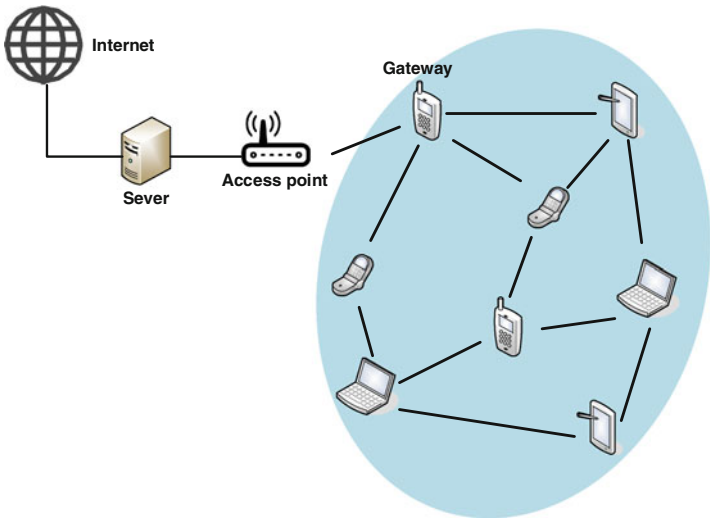


Fig. 1.9 Ad hoc networks

Due to the mobile and self-configuring nature of wireless ad hoc networks, it also motivates the designing of corresponding devices. Given the perspective of the application level, mobile users in wireless ad hoc networks typically connect and cooperate with each other as teams (e.g., police, firefighters, medical personnel teams in a search and rescue mission). The corresponding applications always require efficient data transmission and lower delay tolerance.

1.2.2.3 Cognitive Radio Networks (CRN)

In general, in order to support wireless services, the spectrum regulators often provide fixed spectrum access policy, which is designed to allocate each piece of spectrum with certain bandwidth to one or more dedicated users. By doing so, only the users who are assigned licensed spectrum have the right to use the allocated spectrum, while remaining users are not allowed to use it, regardless of whether the spectrum is occupied by the licensed users [57]. With the remarkable development of wireless services, the available spectrum has fully been allocated, which results in the severe problem of spectrum scarcity. Moreover, the spectrum utilization measurements in the real world have revealed that a large portion of the licensed spectrum is idle, which decreases the utilization. CRN have ability of providing high bandwidth to mobile users with dynamic spectrum access techniques in heterogeneous wireless architectures. Thus, CR can be regarded as a promising technique by exploiting the under-utilized licensed spectrum.

Figure 1.10 illustrates a basic model of CRN from [58]. The principle of CR is to use dynamic spectrum access (DSA) to manage the radio spectrum more efficiently.

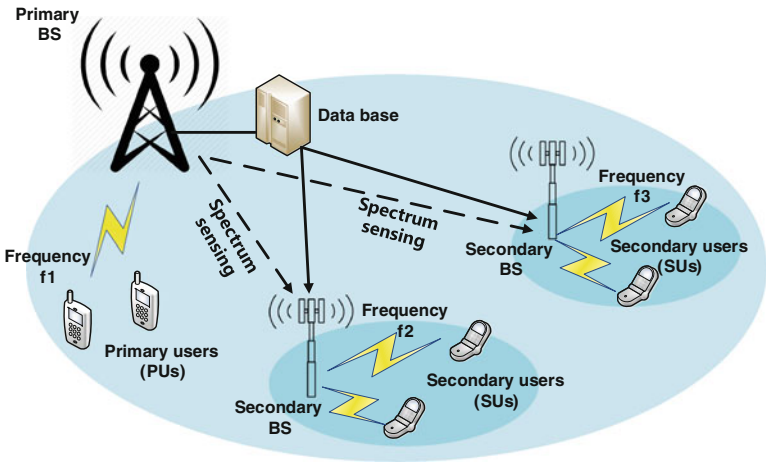


Fig. 1.10 Cognitive radio networks [58]

In DSA, a certain piece of licensed spectrum f1 is allocated to one or more users, namely primary users (PUs), which are monitored by the primary BS. However, the use of that spectrum is not exclusive to primary users. Other users, namely the secondary users (SUs) which have an opportunity to access the remaining spectrum f2 and f3 that the PUs do not use temporally, or share the spectrum with the PUs as long as the QoS of PUs can be properly protected [59]. The opportunity of occupying the idle spectrum can be enhanced with employing spectrum sensing by secondary BS. By doing so, the radio spectrum can be reused in an opportunistic manner or shared all the time; thus, the spectrum utilization efficiency can be significantly improved.

1.2.2.4 Wireless Sensor Networks (WSN)

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks, are formed by physically distributing sensor nodes to monitor or detect environmental conditions, such as temperature, concentration, pressure, etc., and to transmit the collected data with cooperation through the network to a monitor. A WSN typically involves a monitoring center to control the network and process the information delivered via the Internet, and a gateway/sink works as a merging node which is responsible for the connection between the senor and monitoring center, and multiple sensor clusters used for collecting the wanted information around them, as shown in Fig. 1.11. In general, each sensor node has a radio frequency (RF) transceiver for transmitting and receiving the signal, and an microcontroller for processing the collected signal, and an electronic circuit for connecting with the sensors and a battery. The development of WSN was motivated by military applications such as battlefield surveillance [60]. The topology of the WSN can be varied from a simple star network to an advanced multi-hop wireless mesh network.

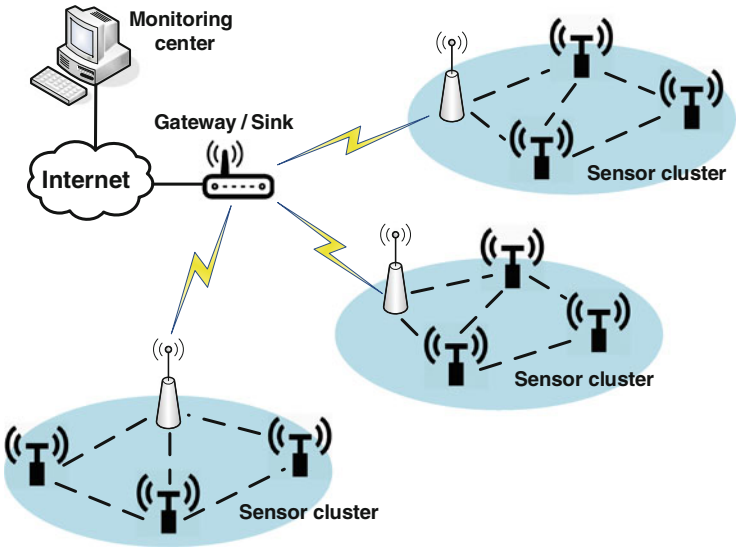


Fig. 1.11 Wireless sensor networks

1.2.2.5 Internet of Things (IoT)

IoT is expected to offer connectivity of all things around human beings, such as physical devices, vehicles, buildings, etc., while combining with electronics, software, sensors, and network connectivity that enable these objects to communicate with each other [61]. The interconnection of these embedded devices, is expected to usher in automation in almost all fields, while also enabling advanced applications like a smart grid and expanding to the areas such as smart cities [62]. In 2013, the Global Standard Initiative on Internet of Things defined the IoT as "the infrastructure of the information society". The IoT allows objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy, and economic benefit. In [63] the basic illustration of IoT is introduced, as shown in Fig. 1.12.

1.2.2.6 Social Networks

A social network is made up of a set of social actors, which are used to analyze the relationships between individuals, groups, organizations, or even entire societies. This attracts much more attention after the great success in the Internet and social applications. Social networking service (SNS), which is used by people to build social networks or social relations with other people who share similar personal or career interest, activities, backgrounds or real-life connections. Nowadays, the most significant portion of the Internet traffic is related to social networks, such as Facebook, YouTube, etc. Figure 1.13 illustrates a social network of individuals.

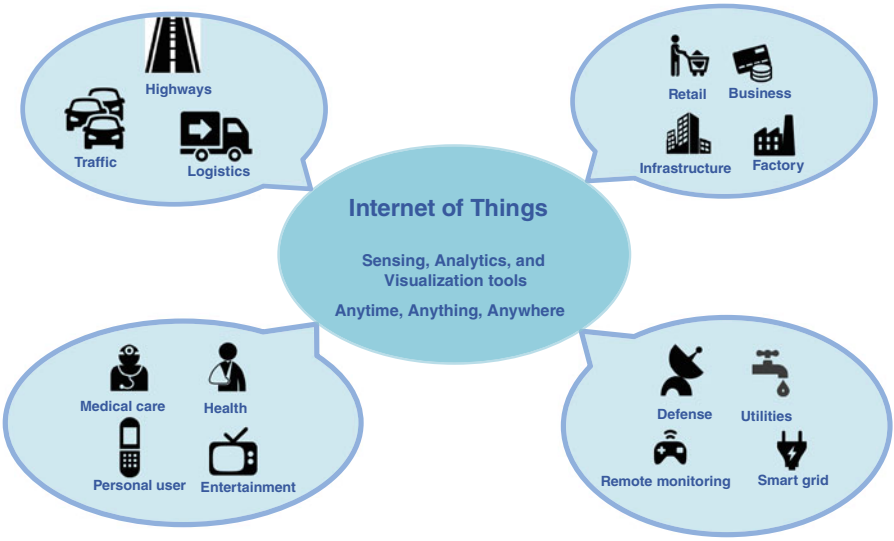
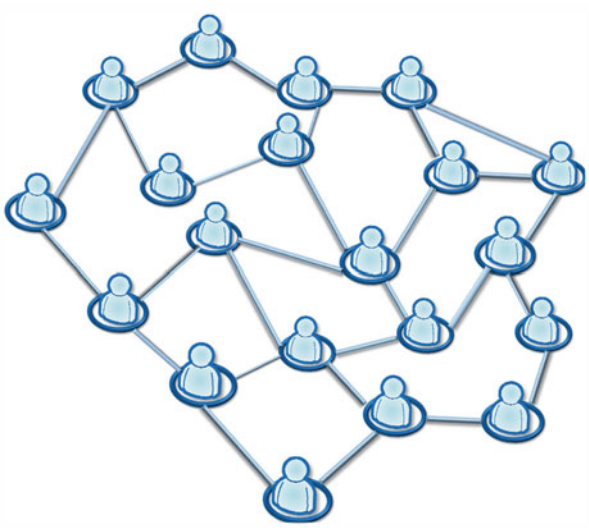


Fig. 1.12 Internet of things illustration [63]

Fig. 1.13 Social networks illustration



Social networks can be extremely useful to study many social and commercial behaviors. Such understanding is critical to applications and services of modern technology. A popular mean of seeking information is asking around [64]. A person may consult her friends until the information is found. Navigating for information via social networks works better than other methods like the Internet when people are searching for information which is location-specific, community-specific, or time-specific. This is because people are good sources of these types of information [65].

In addition, the social interaction among mobile users can significantly enhance the connectivity of IoT, namely "Social Internet of Things" [66]. The advantages of employing the idea of social characteristics in IoT involve creating a level of trustworthiness by leveraging the level of interaction among things, guaranteeing the network navigability to effectively reinforce the service discovery, and extending the conventional model in social networks to exploit the interaction among equipments.

1.3 Wireless Cooperation for Physical Layer Security Enhancement

The issue of physical layer security in wireless cooperative networks has been drawn much attention recently, which is regarded as an extended version of investigating the security issue in non-cooperative networks. The cooperative behavior among wireless nodes, is initially proposed to improve diversity gain for single-antenna wireless communications systems, is also promising to enhance the security at the physical layer. In this scheme, one/multiple cooperative nodes help the transmitter deliver information to the receiver and interrupt the behavior of eavesdropping from the malicious nodes.

In this section, we intentionally summarize the corresponding content of cooperative networks for secure communications in two aspects: **multi-antenna cooperation**, and **multi-user cooperation**. Note that such two aspects always overlap with each other due to the combination of techniques.

1.3.1 Multi-Antenna Cooperation

In a MIMO system, the cooperation among the antennas can be fully exploited to enhance the performance of physical layer security. In particular, the MIMO system with respect to the physical layer security can be divided into two categories: *centralized MIMO system*, or the centralized antenna system (CAS) where the antennas are co-located at the communicate entities, and *distributed MIMO system*, or the distributed antenna system (DAS) where antennas are separately located, significantly reducing the transmission distance between transmitter and receiver [67]. Compared to the CAS, DAS can exploit rich spatial diversity to combat path loss and shadowing for improving the signal reception quality, and the classic techniques in MIMO system such as space-time coding, spatial multiplexing, or beamforming can also be applied in DAS system [68].

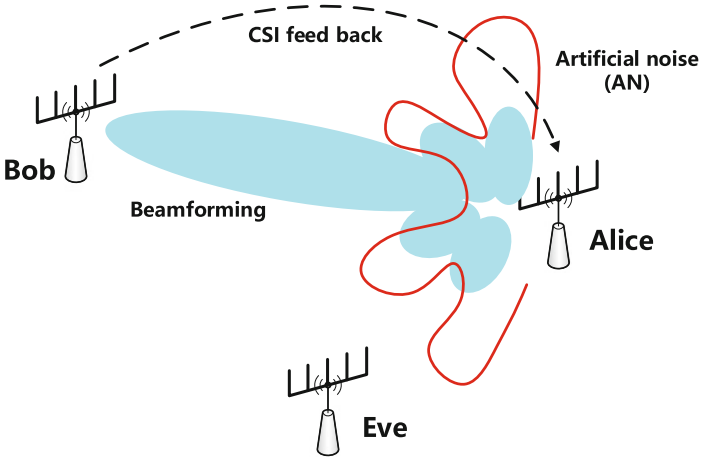


Fig. 1.14 Secrecy beamforming with AN in a multi-antenna wireless system [14]

1.3.1.1 Secrecy Beamforming

In transmitted signal design, beamforming and precoding techniques are the strategies which can effectively transmit signals in intentional directions that meet maximal difference of signals at the destination and the eavesdropper. Once directional transmission is employed, the receiver in the beam's direction can decode the transmitted signal successfully, while the eavesdropper only can obtain degraded version of signal. In general, beamforming refers to rank-1 transmissions by which only one data stream is delivered with the multiple antennas, but precoding refers to multi-rank transmissions by which several data stream are transmitted simultaneously [14]. Typically, beamforming serves as a special case of precoding but needs to be analyzed separately due to its simpler and more intuitive designs. Hong et al. [14] presents the principle of beamforming, as shown in Fig. 1.14.

In Shafiee and Ulukus's work [69], the optimal beamforming scheme was investigated in multiple-input-single-output single-antenna eavesdropper (MISOSE) scenario. The transmitted signal can be denoted as $\mathbf{x} = \boldsymbol{\omega} u$, where $\boldsymbol{\omega} \in \mathbb{C}^{N_t \times 1}$ is the beamforming vector and $Tr(\boldsymbol{\omega}^H \boldsymbol{\omega}) = P$ is the transmit power. Thus the optimal beamforming vector $\boldsymbol{\omega}^*$ can be expressed as [69]:

$$\boldsymbol{\omega}^* = \arg\max_{\boldsymbol{\omega}} \frac{1 + \mathbf{h_b} \boldsymbol{\omega}^H \boldsymbol{\omega} \mathbf{h_b}^H}{1 + \mathbf{h_e} \boldsymbol{\omega}^H \boldsymbol{\omega} \mathbf{h_e}^H}, \tag{1.18}$$

where $\mathbf{h_b} \in \mathbb{C}^{1 \times N_t}$ and $\mathbf{h_e} \in \mathbb{C}^{1 \times N_t}$ are the vectors of main channel and wiretap channel, respectively. Khisti verified that the secrecy capacity in this case is [70]:

$$C_s = [\log(\lambda_{max}(I + P\mathbf{h_b}\mathbf{h_b}^H, I + P\mathbf{h_e}\mathbf{h_e}^H))]^+, \tag{1.19}$$

where $\lambda_{max}(\boldsymbol{A},\boldsymbol{B})$ is the maximum generalized eigenvalue of matrices pair $(\boldsymbol{A},\boldsymbol{B})$. So the optimal beamforming vector is the generalized eigenvector corresponding to the maximum eigenvalue of $(I + P\mathbf{h_e}\mathbf{h_e}^H)^{-1}(I + P\mathbf{h_b}\mathbf{h_b}^H)$ [71]. Note that in MISOME system Eq. (1.19) is feasible as well.

Moreover, when the destination is equipped with multiple antennas, which is referred to as the multiple-input-multiple-output multiple-antenna eavesdropper (MIMOME) scenario, confidential messages can be spatially multiplexed onto multiple independent subchannels via precoding. In this case, the transmit signal vector is given by $\mathbf{x} = \mathbf{F}\mathbf{u}$ [72], where $\mathbf{F}$ is the $N_t \times k_s$ linear precoding matrix, $\mathbf{u} \sim \mathscr{CN}(0, \mathbf{I}_{k_s})$ is the Gaussian input, and k_s is the number of signal dimensions. In this case, by considering the power-covariance constraint (i.e., $0 \preceq \mathbf{K_x} = \mathbf{F}\mathbf{F}^H \preceq \mathbf{S}$), a closed-form solution can be obtained by exploiting the structure of the matrix $\mathbf{S}$ [73]. More specifically, assume that $\mathbf{C}$ is the generalized eigenvector matrix of the two symmetric positive definite matrices $\mathbf{I} + (\mathbf{S}^{1/2})^H\mathbf{H_e}^H\mathbf{H_e}S^{1/2}$ and $\mathbf{I} + (\mathbf{S}^{1/2})^H\mathbf{H_b}^H\mathbf{H_b}S^{1/2}$ such that $\mathbf{C}^H(\mathbf{I} + (\mathbf{S}^{1/2})^H\mathbf{H_e}^H\mathbf{H_e}\mathbf{S}^{1/2})\mathbf{C} = \mathbf{I}$ and $\mathbf{C}^H(\mathbf{I} + (\mathbf{S}^{1/2})^H\mathbf{H_b}^H\mathbf{H_b}\mathbf{S}^{1/2})\mathbf{C} = \boldsymbol{\Lambda}_m$, where $\boldsymbol{\Lambda}_m = \mathrm{Diag}(\lambda_1, \ldots, \lambda_{N_t})$, and m is the number of eigenvalues larger than 1 so that $\lambda_1 \geq \ldots \geq \lambda_m \geq 1 \geq \ldots \geq \lambda_{N_t}$. The optimal covariance matrix $\mathbf{K_x}^*$ is given by Hong et al. [14]

$$\mathbf{K_x}^* = \mathbf{F}\mathbf{F}^H = \mathbf{S}^{1/2}\mathbf{C}\begin{bmatrix}(\mathbf{C_1}^H\mathbf{C_1})^{-1} & 0\\ 0 & 0\end{bmatrix}\mathbf{C}^H(\mathbf{S}^{1/2})^H, \tag{1.20}$$

where $\mathbf{C} = [C_1\ C_2]$ with $\mathbf{C_1}$ being an $N_t \times m$ submatrix, and $\mathbf{C_2}$ being an $N_t \times (N_t - m)$ submatrix.

Besides, *zero-forcing (ZF)* beamforming also can be used for preventing signal transmission from interception. The basic idea of ZF method stems from cancelling the interference at intended receiver in multiuser communications. In a MISOSE system, the beamforming vector $\boldsymbol{\omega} \in \mathbb{C}^{N_t \times 1}$ should satisfy the following condition

$$\mathbf{h_e}\boldsymbol{\omega} = \mathbf{0}. \tag{1.21}$$

Defining the null-space of $\mathbf{h_e}$ as [74, 75]

$$\mathbf{h_{e\perp}} = \mathbf{I} - \mathbf{h_e}^H(\mathbf{h_e}\mathbf{h_e}^H)^{-1}\mathbf{h_e}. \tag{1.22}$$

Therefore, the optimal ZF-beamformer can be obtained as [76]

$$\boldsymbol{\omega}^* = \frac{\mathbf{h_{e\perp}}\mathbf{h_b}^H}{\| \mathbf{h_{e\perp}}\mathbf{h_b}^H \|_2}. \tag{1.23}$$

1.3.1.2 Artificial Noise Design

Deliberately deteriorating the quality of eavesdropper's channel in MIMO systems is promising to exploit. The artificial noise (AN)-based transmission has been regarded as an effective strategy to generate interference to the eavesdropper and interrupt the intercepting behavior. And the AN does not interfere the intended receiver by elaborating the signal design. As shown in Fig. 1.14, AN is also used by jointly combining beamforming techniques. The basic idea of leveraging AN to improve secrecy performance was first proposed in Goel and Negi's works [77, 78], in which AN is superimposed on the transmitted message to puzzle the eavesdropper. This can be achieved by designing the corresponding AN which is generated in the null space of the legitimate receiver's channel. Here we also consider a MISOME case, in which the signal transmitted by a source can be written as

$$\mathbf{x} = \boldsymbol{\omega} u + \boldsymbol{\nu}, \tag{1.24}$$

where $\boldsymbol{\omega} u \in \mathbb{C}^{N_t \times 1}$ is the bearing information and u is the Gaussian distributed signal with zero mean and variance σ_u^2. $\boldsymbol{\nu} \in \mathbb{C}^{N_t \times 1}$ is the AN signal.

Considering the design of AN in the same way as ZF-beamforming in Eq. (1.21), i.e., $\boldsymbol{\nu}$ is chosen to lie in the null space of main channel $\mathbf{h_b} \in \mathbb{C}^{N_t \times 1}$, we have [77]

$$\mathbf{h_b} \boldsymbol{\nu} = \mathbf{0}. \tag{1.25}$$

In general, $\boldsymbol{\nu}$ is always chosen to be i.i.d Gaussian random vectors in the null space of $\mathbf{h_b}$, which can be expressed as

$$\boldsymbol{\nu} = \mathbf{G}\boldsymbol{\alpha}, \tag{1.26}$$

where $\mathbf{G}$ is an orthogonal basis of the null space of $\mathbf{h_b}$ and is assumed that $\mathbf{G^H G} = \mathbf{I}$, and $\boldsymbol{\alpha}$ is chosen to be i.i.d. complex Gaussian vector with zero mean and variance σ_α^2. Therefore, the corresponding secrecy capacity can be expressed as [78]

$$C_s = [\log_2(1 + \frac{\sigma_u^2 \mathbf{h_b} \boldsymbol{\omega}^H \boldsymbol{\omega} \mathbf{h_b}^H}{\sigma_n^2}) - \log_2(1 + \frac{\sigma_u^2 \mathbf{H_e} \boldsymbol{\omega}^H \boldsymbol{\omega} \mathbf{H_e}^H}{\sigma_\alpha^2 \mathbf{H_e} \mathbf{G}^H \mathbf{G} \mathbf{H_e}^H + \sigma_e^2})]^+, \tag{1.27}$$

where σ_n^2 and σ_e^2 are the variances of additive white Guassian noise (AWGN) in main channel and wiretap channel, respectively.

1.3.1.3 Antenna Selection

As we have mentioned before, MIMO technique can significantly enhance the capacity and reliability of wireless communication. However, regardless of the

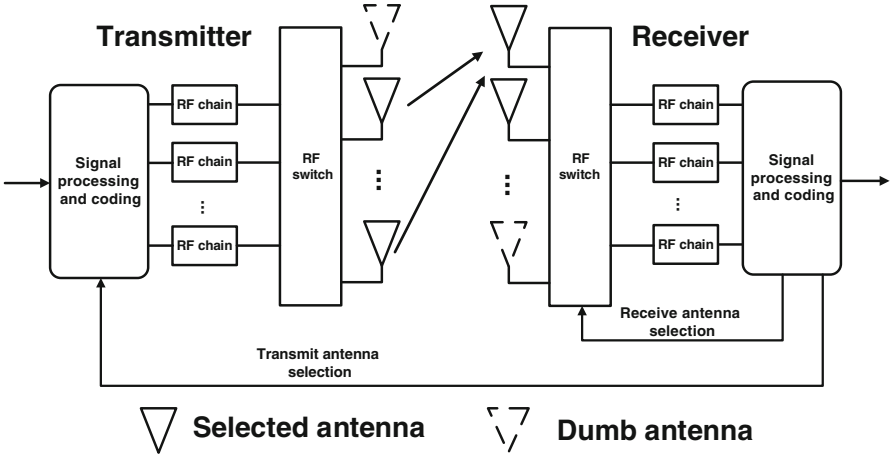


Fig. 1.15 Antenna selection in multi-antenna system [80]

diversity gain benefiting from the multiple antennas, MIMO systems typically have high complexity in terms of size, power and hardware [79]. Therefore, antenna selection is an effective alternative to lower the cost complexity while capturing many of the advantages of MIMO system.

Generally, there are two types of antenna selection in research field: *transmit antenna selection* and *receiver antenna selection* [80], as shown in Fig. 1.15. Transmit antenna selection (TAS) also has ability of enhancing the secrecy performance at physical layer in MIMO wireless systems. Different from transmit beamforming that requires the feedback of CSI and signal processing for all transmit antennas, TAS achieves lower feedback and computational overheads as it only requires feedback and signal processing for a single transmit antenna. Note that if the full CSI of both main and eavesdropping channels are known, the transmit antenna with the highest secrecy capacity is chosen [81]. Alves et al. studied TAS in MISOSE system where partial CSI is assumed between Bob and Alice [82, 83]. They demonstrated that high performance of security can be achieved as the number of transmit antenna increases, and Eve cannot exploit any additional diversity gain offered by Alice due to the implementation of TAS. Besides, Yang et al. further investigated the TAS scheme in MIMOME system [84, 85] by using maximal ratio combining (MRC) and selection combining (SC) at the legitimate receiver.

1.3.2 Multi-User Cooperation

Apart from the multi-antenna system, we will discuss another scenario, in which there are a number of mobile entities or terminals in the network. Generally, when considering security issues in this scenario, the nodes often play two roles:

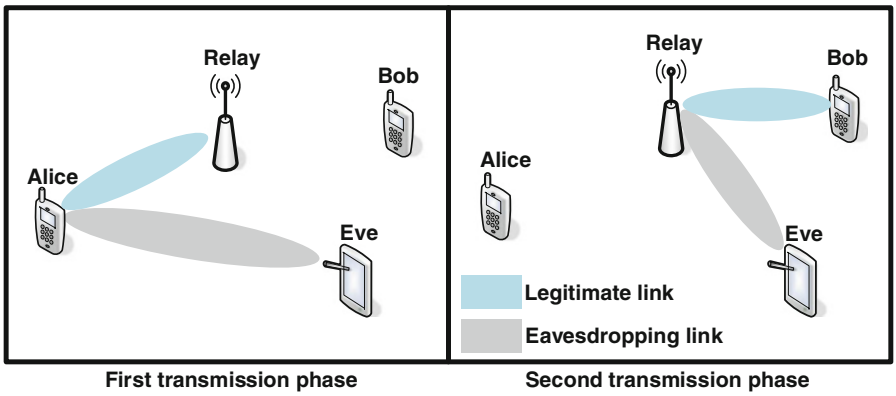


Fig. 1.16 Security threats in cooperative relaying networks, the signal has potential to be overheard twice

- **Cooperative relaying:** improves the security by enhancing channel quality between source and legitimate destination, as a relay should do;
- **Cooperative jamming:** decreases the interception by deteriorating the channel condition to the eavesdropper, also known as jammer.

1.3.2.1 Improving the Legitimate Channel: Relaying

During a conventional cooperative network, we always use relay nodes to expand coverage/distance of communication and combat fading. Therefore, in a secrecy transmission, cooperative nodes can serve as relays to combat the interception from the eavesdropper. The basic concept of cooperative relaying system in physical layer security was first described in [86] with the help of one relay node. The cooperation offered by the relay is separated into two phases, as shown in Fig. 1.16: (1) in the first phase, the transmitter broadcasts confidential signals to all the relay nodes so the eavesdroppers possibly receive signals at the same time; (2) in the second phase, the relay retransmits the received signals which gives eavesdroppers another opportunity to intercept the signals. Therefore, in this case the transmitted signal is more vulnerable to eavesdropping, so it is necessary to carefully design corresponding schemes to prevent an eavesdropper from interception.

Recall that we have mentioned that typically there are two relaying strategies, i.e., AF relaying strategy and DF relaying strategy. Due to their own transmission characteristics, the expressions of secrecy rates with such two strategies are different.

- **AF relaying protocol:** the relay will transmit a scaled version of its received signal to destination without any decoding. In this case, assume that transmit power of source and relay are P_s and P_r, respectively, and the channel gains from source to relay, relay to destination, source to eavesdropper, relay to

eavesdropper, and source to destination are h_{sr}, h_{rd}, h_{se}, h_{re}, and h_{sd}, respectively. σ^2 is the variances of noise in legitimate channel and eavesdropper channel. Thus, the secrecy rate can be expressed as [87, 88]

$$\begin{aligned} R_s^{AF} &= R_M^{AF} - R_W^{AF} \\ &= \left[\log_2 \left(1 + \frac{P_s}{\delta^2} |h_{sd}|^2 + \frac{\frac{P_s}{\delta^2} |h_{sr}|^2 \frac{P_r}{\delta^2} |h_{rd}|^2}{\frac{P_s}{\delta^2} |h_{sr}|^2 + \frac{P_r}{\delta^2} |h_{rd}|^2 + 1} \right) \right. \\ &\quad \left. - \log_2 \left(1 + \frac{P_s}{\delta^2} |h_{se}|^2 + \frac{\frac{P_s}{\delta^2} |h_{sr}|^2 \frac{P_r}{\delta^2} |h_{re}|^2}{\frac{P_s}{\delta^2} |h_{sr}|^2 + \frac{P_r}{\delta^2} |h_{re}|^2 + 1} \right) \right]^+ . \end{aligned} \tag{1.28}$$

- **DF relaying protocol:** the relay decodes and re-encodes the transmitted signal from the source, and we assume that both the relay and destination can fully decode the entire codeword without error. Also, MRC is used at the eavesdropper to combine the intercepted signals from the source and relay. According to [48, 89], the secrecy rate can be expressed as the following formulation

$$\begin{aligned} R_s^{DF} &= R_M^{DF} - R_W^{DF} \\ &= \left[\log_2 \left(1 + \min \left(\frac{P_s}{\sigma^2} |h_{sr}|^2, \frac{P_r}{\sigma^2} |h_{rd}|^2 + \frac{P_s}{\sigma^2} |h_{sd}|^2 \right) \right) \right. \\ &\quad \left. - \log_2 \left(1 + \frac{P_s}{\sigma^2} |h_{se}|^2 + \frac{P_r}{\sigma^2} |h_{re}|^2 \right) \right]^+ . \end{aligned} \tag{1.29}$$

The aforementioned basic scenarios can be extended to a secrecy transmission with one source-destination pair in the presence of more eavesdroppers with the help of multiple relay nodes, as shown in Fig. 1.17. Typically, ***cooperative beamforming*** which is the extended version of beamforming in multi-antenna system, can also significantly improve the main channel capacity with multiple relays. These relays form a virtual antenna array to provide both diversity and power gains for the destination such that the rate of the legitimate channel can be greatly enhanced. Concurrently, the forward signals from the relays can also be designed deliberately to perform transmit beamforming to deteriorate or even null out at the eavesdroppers. By doing so, the secrecy rate can be greatly increased. In [90] and [91], the basic beamforming strategy in dual-hop relaying network are investigated. The weights of the transmitted signal of the corresponding relays are derived to maximize the achievable secrecy rate. In [92], Bassily and Ulukus proposed beamforming strategies based on multiple relays with ZF. All the relays retransmitted the signal concurrently, then employing beamforming by transmitting scaled versions of the same signal to the receiver, while all the components of the signal can be eliminated from the eavesdropper's observation.

Another cooperative relaying scheme is to just select a single relay out of a group of relay nodes for cooperation under certain conditions with respect to the security

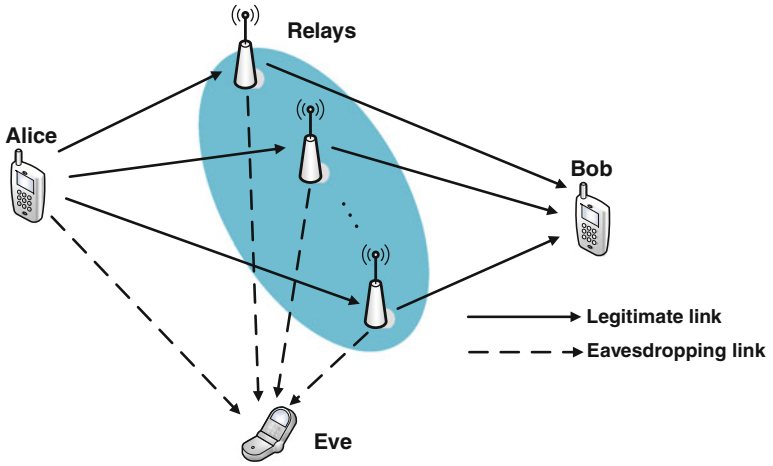


Fig. 1.17 Multi-relay transmission

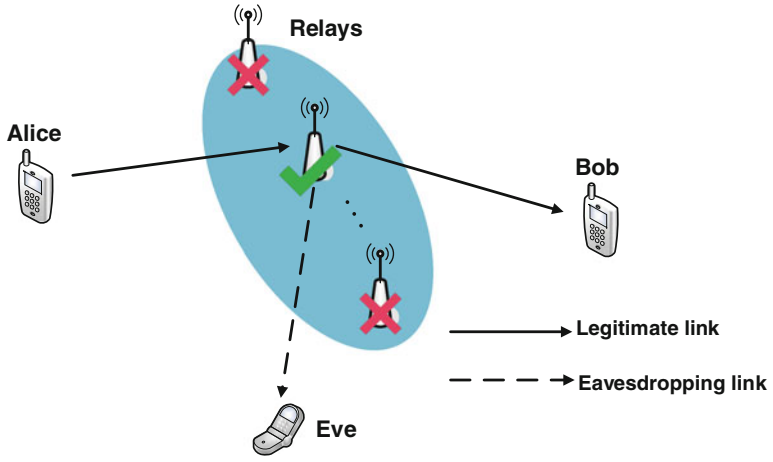


Fig. 1.18 Relay selection

performance. This is referred to ***relay selection***, as shown in Fig. 1.18. Intuitively, the relay which makes the ratio between the quality of channel to the receiver and the quality of channel to the eavesdropper biggest should be selected as the intended relay. Typically, the ratio of end-to-end SNRs between main channel and wiretap channel can be used as a criterion for selecting relay, which can be formulated as [93]

$$k^* = \arg\max_{k \in \mathcal{S}} \{\frac{\gamma_{srd}}{\gamma_{sre}}\}, \tag{1.30}$$

where $\mathscr{S}$ is the set of candidate relays, γ_{srd} and γ_{sre} are the end-to-end SNRs of source→relay→destination and source→relay→eavesdropper links, respectively. By doing so, the difference of the legitimate channel rate and the wiretap channel rate can be maximized, such that the secrecy performance can be greatly improved. Zou et al. considered different relay selection schemes [94] for both AF and DF relays, in which single and multiple relays exist. They demonstrated that the performance of interception probability with proposed optimal relay selection is much better than that of conventional relay selection scheme and multiple relay combining methods.

1.3.2.2 Degrading the Wiretap Channel: Jamming

Cooperative jamming can also be referred as cooperative AN transmission. In this case, cooperative nodes become friendly jammers to transmit AN to cover the confidential signals in case of being intercepted. Since the jamming signals will interfere with both legitimate receiver and eavesdropper, they should be deliberately designed to make quality of the legitimate channel better than that of the wiretap channel. This phenomenon was first clarified in [95]. In a most common cases, the cooperative jamming schemes can be classified into two categories: ***coordinated jamming*** and ***jammer selection*** [96].

In coordinated jamming, jamming signals transmitted from the multiple jammers should be designed coordinately in the direction of the wiretap channels while ignoring the legitimate channels, as shown in Fig. 1.19. Herein, many artificial jamming signals are used and could be divided into four categories [97, 98]: (1) Gaussian noise, which is the same as the additive noise at the receiver [99, 100]; (2)

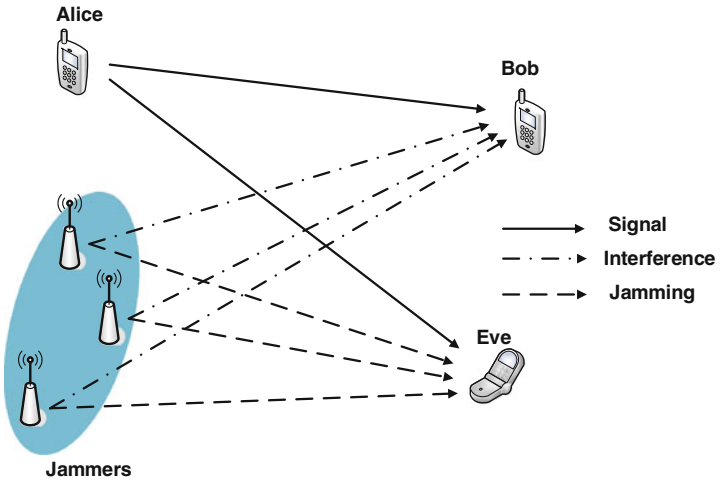


Fig. 1.19 Coordinated jamming

jamming signal, which is priory known at legitimate receiver, so it has an impact only on the eavesdropper's performance. This type of signal is better than the previous one because the jamming signals do not effect the legitimate receiver [101]; (3) an introduced randomization to the public codebook, which is provided by the interferer and the secrecy can be increased further. Assuming that the eavesdropper knows the codebook of the transmitter and the interferer, the legitimate receiver has the ability to decode and cancel the jamming signals sent by an independent interferer, even though receiver requires a complicated self-interference cancellation to decode the codewords. However, the eavesdropper cannot decode the codewords through the codebook because of the randomness brought by jamming signals [102]; (4) useful signals for the other legitimate nodes, such as the signals of multiple simultaneous source-destination pairs, but this kind of jamming is difficult to be applied due to the change of the multiple transmission pair [103, 104].

Jammer selection is an alternative to coordinated jamming with low complexity, where only one or multiple nodes are selected as a jammer or jammers. Like the coordinated behavior in relay selection scheme, jammer selection is also based on some certain conditions to improve the security performance of the system. Therefore, the corresponding criterion of selecting jammers should be deliberately designed.

1.3.2.3 Hybrid Cooperative Relaying/Jamming Strategies

Cooperative relaying and cooperative jamming schemes can significantly improve the secrecy performance in physical layer, however, there are still some drawbacks that we have to take into consideration: (1) for cooperative relaying schemes, since the two transmission phases are required for transmitting the signal from the source to destination, eavesdropper has an opportunity to intercept the information, which means the wiretap channel can also be improved. (2) if the relay works in a half-duplex mode, so cooperative beamforming or relay selection are only effective in the second phase. Therefore, the secure performance cannot be guaranteed because there is no wireless node preventing eavesdroppers from interception [96]. Besides, for cooperative jamming schemes, due to the influence from imperfectly designed jamming signal, the quality of the legitimate channel from source to destination may not be improved via cooperation. Especially for the situation where both the source and destination are only equipped with a single antenna, the secrecy capacity could be degraded essentially.

Based on all above situations, hybrid relaying/jamming schemes are proposed, which is the combination of pure relaying and jamming strategies [105]. In a hybrid relaying/jamming scheme, cooperative nodes are separated into two groups: one of them works as a relay group and another group works as a jammer group. The wireless nodes in the relay group help forward the confidential information, while those in the jammer group cooperate with each other to interfere the eavesdropper, as shown in Fig. 1.20. An effective way is letting a proportion of nodes work as relays performing distributed beamforming, and remaining nodes are required to be

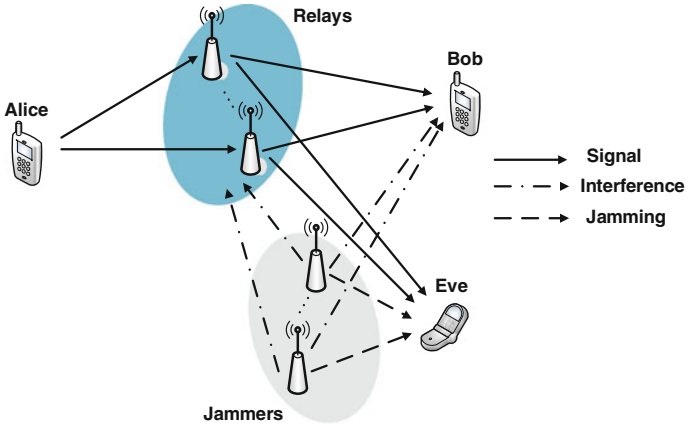


Fig. 1.20 Hybrid multi-relay and multi-jamming scheme

jammers to transmit AN to deteriorate the eavesdropper. By doing so, the legitimate channel is improved, and the wiretap channel is perturbed, consequently the secrecy performance is enhanced [106, 107].

1.4 Outline of the Book

This book focuses on security issue of physical layer in wireless cooperative communication systems, from the conceptual and technical perspectives. Chapter 1 presents an overview on physical layer security, cooperative networks and cooperation for physical layer security. In particular, this chapter involves fundamentals, technical development path, etc. Chapter 2 gives a brief description about some existing techniques of physical layer security in wireless cooperative networks, which will be specifically analyzed in the remaining of the book. We mainly focus on time reversal technique, spatial modulation technique, and D2D-enabled networks, in terms of their principles and applications, and so forth. In Chap. 3, time reversal (TR) is presented to show its ability of protecting against unintended signal leakage to eavesdroppers. The secrecy performance is analyzed with respect to the SNR improvement, and then we make a comparison with other sophisticated techniques including direct beamforming and distributed beamforming. Moreover, Chap. 4 presents physical layer security in terms of spatial modulation in MIMO system. space shift keying (SSK) and generalized space shift keying (GSSK) are also analyzed as benchmarks to show the advantages and weaknesses of SM-MIMO in secure communications. Besides, we further consider the scenario where multiple users are existed. Based on this, a precoding-aided spatial modulation (PSM) scheme is proposed to achieve security enhancement. Chapter 5 describes secure transmission with the help of cooperative jammers, especially in

D2D-enabled networks. By considering the social interaction of the jammers, joint power allocation and jammer selection schemes are investigated to improve secrecy and privacy of D2D communications. Finally, Chap. 6 provides the summary of the technical contents discussed in this book.

References

1. C. E. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.
2. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.
3. P. R. Geffe, "Secrecy systems approximating perfect and ideal secrecy," *Proceedings of the IEEE*, vol. 53, no. 9, pp. 1229–1230, Sept. 1965.
4. G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Transactions of American Institute Electrical Engineers*, vol. 55, no. 4, pp. 295–301, Jan. 1926.
5. A. D. Wyner, "The wire-tap channel" *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
6. R. Liu, T. Liu, H. V. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.
7. I. Csiszàr and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May. 1978.
8. R. Liu, and W. Trappe, *Securing wireless communications at the physical layer*, Springer, 2010.
9. S. L. Y. Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
10. J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. 2006 IEEE International Symposium on Information Theory*, Seattle, WA, USA, Jul. 2006, pp. 356–360.
11. M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
12. A. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
13. A. Khisti and G. Wornell, "Secure transmission with multiple antennas-II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
14. Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 29–40, Sept. 2013.
15. S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, Sept. 2009.
16. V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," in *Proc. 2009 Information Theory and Applications Workshop*, San Diego, CA, USA, Feb. 2009, pp. 295–300.
17. R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

18. X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Transactions on Information Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.
19. H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "On multiuser secrecy rate in flat fading channel," in *Proc. 2009 IEEE Military Communications Conference (MILCOM)*, Boston, MA, USA, Oct. 2009, pp. 1–7.
20. R. Bassily, E. Ekrem, X. He, and E. Tekin, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, Sept. 2013.
21. P. Mahajan and A. Sachdeva,"A study of encryption algorithms AES, DES and RSA for security," *Global Journal of Computer Science and Technology*, vol. 13. no. 15, pp. 15–22, Oct. 2013.
22. M. Bloch and J. Barros, *Physical-layer security: From information theory to security engineering*, Cambridge University Press, 2011.
23. M. Xiao, X. Wang, and G. Yang, "Cross-layer design for the security of wireless sensor networks," in *Proc. 2006 6th World Congress on Intelligent Control and Automation (WCICA)*, vol. 1, Dalian, China, Jun. 2006, pp. 104–108.
24. H. Wen and G. Gong, "A cross-layer approach to enhance the security of wireless networks based on MIMO," in *Proc. 2009 43rd Annual Conference on Information Sciences and Systems*, Baltimore, MD, USA, Mar. 2009, pp. 935–939.
25. M. Kaliszan, J. Mohammadi, and S. Stańczak, "Cross-layer security in two-hop wireless Gaussian relay network with untrusted relays," in *Proc. 2013 IEEE International Conference on Communications (ICC)*, Budapest, Hungary, Jun. 2013, pp. 2199–2204.
26. D. Sun, X. Wang, Y. Zhao, and Y. Wu, "SecDCF: An optimized cross-layer scheduling scheme based on physical layer security," in *Proc. 2011 IEEE International Conference on Communications (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.
27. D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
28. Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
29. P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proc. 2009 IEEE International Symposium on Information Theory*, Seoul, korea, Jun.-Jul. 2009, pp. 2442–2446.
30. H. M. Wang and T. X. Zheng, *Physical layer security in random cellular networks*, Springer, 2016.
31. P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
32. H. M. Wang and T. X. Zheng, *Wireless physical layer security*, Springer, 2016.
33. V. U. Prabhu and M. R. D.Rodrigues, "On wireless channels with antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Transactions on Information Forensics Security*, vol. 6, no. 3, pp. 853–860, Sept. 2011.
34. N. Marina and A. Hjorungnes, "Characterization of the secrecy region of a single relay cooperative system," in *Proc. 2010 IEEE Wireless Communication and Networking Conference*, Sydney, NSW, Australia, Apr. 2010, pp. 1–6.
35. N. Chang, C. Chae, J. Ha, and J. Kang, "Secrecy rate for MISO Rayleigh fading channels with relative distance of eavesdropper," *IEEE Communications Letters*, vol. 16, no. 9, pp. 1408–1411, Sept. 2012.
36. W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.
37. X. He and A. Yener, "Gaussian two-way wiretap channel with an arbitrarily varying eavesdropper," in *Proc. 2011 IEEE Global Communications Conference Workshops (GLOBECOM Workshops)*, Houston, TX, USA, Dec. 2011, pp.845–858.

38. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the K-user Gaussian interference channel," in *Proc. 2008 IEEE International Symposium on Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 384–388.
39. B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey." [Online]. Available: http://arxiv.org/abs/1307.4146
40. I. M. Kim, B. H. Kim, and J. K. Ahn, "BER-Based physical layer security with finite codelength: Combining strong converse and error amplification," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3844–3857, Sept. 2016.
41. D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2572–2585, Jul. 2012.
42. X. Chen and L. Lei, "Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee," *IEEE Communications Letters*, vol. 17, no. 4, pp. 637–640, Apr. 2013.
43. F. H. P. Fitzek and M. D. Katz, *Cooperation in wireless networks: Principles and applications*, Springer, 2006.
44. A. Akella, R. Karp, C. Papadimitrou, S. Seshan, and S. Shenker, "Selfish behavior and stability of the internet: A game-theoretic analysis of TCP," in *Proc. 2002 Association for Computing Machinery Special Interest Group on Data Communication Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, Pittsburgh, PA, USA, Aug. 2002, pp.117–130.
45. T. M. Cover and A. A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572–584, Sept. 1979.
46. A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity part I and part II," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1927–1948, Nov. 2003.
47. J. N. Laneman, *Cooperative diversity in wireless networks: Algorithms and architectures,* PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, 2002.
48. J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.
49. T. E. Hunter and A. Nosratinia, "Cooperative diversity through coding," in *Proc. 2002 IEEE International Symposium on Information Theory (ISIT)*, Laussane, Switzerland, Jul. 2002, p. 220.
50. T. E. Hunter and A. Nosratinia, "Diversity through coded cooperation," *IEEE Transactions on Wireless Communications*, vol. 5, no. 2, pp. 283–289, Feb. 2006.
51. A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 74–80, Oct. 2004.
52. A. Stefanov and E. Erkip, "Cooperative coding for wireless networks," *IEEE Transactions on Communications*, vol. 52, no. 9, pp. 1470–1476, Sept. 2004.
53. A. Chakrabarti, A. de Baynast, A. Sabharwal, and B. Aazhang, "LDPC code-design for the relay channel," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 281–291, Mar. 2006.
54. M. Yu, J. Li, and R. S. Blum, "User cooperation through network coding," in *Proc. 2007 IEEE International Conference on Communications*, Glasgow, UK, Jun. 2007, pp. 4064–4069.
55. K. Doppler, M. Rinne, C. Wijting, B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 42–49, Dec. 2009.
56. C. K. Toh, *Ad Hoc Mobile Wireless Networks*, Prentice Hall Publishers, 2002.
57. N. Devroye, M. Vu, and V. Tarokh, "Cognitive radio networks," *IEEE Signal Processing Magazine*, vol. 25, no. 6, pp. 12–23, Nov. 2008.
58. X. Chen, H. H. Chen, and W. Meng, "Cooperative communications for cognitive radio networks — from theory to applications," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1180–1192, Third Quarter 2014.

59. Y. C. Liang, K. C. Chen, G. Y. Li, and P. Mahonen, "Cognitive radio networking and communications: An overview," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 7, pp. 3386–3407, Sept. 2011.
60. I. F. Akyildiz and I.H. Kasimoglu, "Wireless sensor and actor networks: Research challenges," *Ad Hoc Networks*, vol. 2, no. 4, pp. 351–367, Oct. 2004.
61. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Jun. 2010.
62. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb. 2014.
63. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sept. 2013.
64. R. Cross, A. Parker, L. Prusak and S. P. Borgatti, "Knowing what we know: Supporting knowledge creation and sharing in social networks," *Organizational Dynamics*, vol. 30, no. 2, pp. 100–120, Nov. 2001.
65. M. Motani, V. Srinivasan, and P. Nuggehalli, "PeopleNet: Engineering a wireless virtual social network," in *Proc. 2005 11th Annual International Conference on Mobile Computing and Networking,* Cologne, Germany, Aug.- Sept. 2005, pp.243–257.
66. L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a social structure to the Internet of Things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, Nov. 2011.
67. X. H. You, D. M. Wang, B. Sheng, X. Q. Gao, X. S. Zhao, and M. Chen, "Cooperative distributed antenna systems for mobile communications," *IEEE Wireless Communications*, vol. 17, no. 3, pp. 35–43, Jun. 2010.
68. R. Heath, S. Peters, Y. Wang, and J. Zhang, "A current perspective on distributed antenna systems for the downlink of cellular systems," *IEEE Communications Magazine*, vol. 51, no. 4, pp. 161–167, Apr. 2013.
69. S. Shaifee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. 2007 IEEE International Symposium on Information Theory*, Nice, France, Jun. 2007, pp. 2466–2470.
70. A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, Aug. 2007.
71. G. Golub and C. F. V. Loan, *Matrix Computations*, The Johns Hopkins University Press, 1996.
72. F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
73. R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP Journal on Wireless Communications Network*, vol. 5, no. 3, pp. 2602–2606, Jul. 2009.
74. E. G. Larsson and E. A. Jorswieck, "Competition versus cooperation on the MISO interference channel," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 7, pp. 1059–1069, Sept. 2008.
75. S. Gerbracht, A. Wolf, and E. A. Jorswieck, "Beamforming for fading wiretap channels with partial channel information," in *Proc. 2010 International ITG Workshop on Smart Antennas (WSA)*, Bremen, Germany, Feb. 2010, pp. 394–401.
76. E. A. Jorswieck, E. G. Larsson, and D. Danev, "Complete characterization of the Pareto boundary for the MISO interference channel," *IEEE Transactions on Signal Processing*, vol. 56, no. 10, pp. 5292–5296, Oct. 2008.
77. R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. 2005 IEEE 62nd Vehicular Technology Conference*, vol. 3, Dallas, USA, Sept. 2005, pp. 1906–1910.
78. S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
79. L. Peng, J. Liu, B. Gu, and H. Xu, "Combined beam space time block coding transmit scheme with receive antenna selection," in *Proc. 2006 6th International Conference on ITS Telecommunications*, Chengdu, China, Jun. 2006, pp. 349–352.

80. S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 68–73, Oct. 2004.
81. Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, Jan.-Feb. 2015.
82. H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, Jun. 2012.
83. H. Alves, R. D. Souza, and M. Debbah, "Enhanced physical layer security through transmit antenna selection," in *Proc. 2011 IEEE Global Communications Conference Workshops (GLOBECOM Workshops)*, Houston, TX, USA, Dec. 2011, pp. 879–883.
84. N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
85. N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Communications Letters*, vol. 17, no. 9, pp. 1754–1757, Sept. 2013.
86. L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.
87. P. Zhang, J. Yuan, J. Chen, J. Wang, and J. Yang, "Analyzing amplify-and-forward and decode-and-forward cooperative strategies in Wyner's channel model," in *Proc. 2009 IEEE Wireless Communications and Networking Conference (WCNC)*, Budapest, Hungary, Apr. 2009, pp. 1–5.
88. L. Jiménez Rodríguez, N. H. Tran, and T. Le-Ngoc, "Optimal power allocation schemes for the single AF relay and jammer wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 3042–3056, May. 2016.
89. G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
90. J. Li, A. P. Petropulu, and S. Weber, "Optimal cooperative relaying schemes for improving wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
91. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
92. R. Bassily and S. Ulukus, "Secure communication in multiple relay networks through decode-and-forward strategies," *Journal of Communications and Networks*, vol. 14, no. 4, pp. 352–363, Aug. 2012.
93. I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Communications*, vol. 4, no. 15, pp. 1787–1791, Oct. 2010.
94. Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
95. E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proc. 2006 44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, USA, Sept. 2006, pp. 2466–2470.
96. H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 47–53, Dec. 2015.
97. H. Long, W. Xiang, J. Wang, Y. Zhang, and W. Wang, "Cooperative jamming and power allocation with untrusty two-way relay nodes," *IET Communications*, vol. 8, no. 13, pp. 2290–2297, Sept. 2014.
98. M. Atallah, G. Kaddoum, and L. Kong, "A survey on cooperative jamming applied to physical layer security," in *Proc. 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, Montreal, Canada, Oct. 2015, pp. 1–5.

99. R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Transactions on Signal Processing*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.
100. I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.
101. R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. 2010 Global Telecommunications Conference (GLOBECOM)*, Miami, FL, USA, Dec. 2010, pp. 1–6.
102. X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 3153–3167, May. 2011.
103. P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 2, pp. 242–256, Jun. 2009.
104. A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, "Physical layer security from inter-session interference in large wireless networks," in *Proc. 2012 Proceedings IEEE International Conference on Computer Communications*, Orlando, FL, USA, Mar. 2012, pp. 1179–1187.
105. L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, Dec. 2015.
106. H. M. Wang, M. Luo, Q. Yin, and X. G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013
107. L. Wang, C. Cao, M. Song, and Y. Cheng, "Joint cooperative relaying and jamming for maximum secrecy capacity in wireless networks," in *Proc. 2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, Australia, Sept. 2014, pp. 4448–4453.

Chapter 2
Existing Techniques in Physical Layer Security

Last chapter has demonstrated that wireless cooperative networks can significantly enhance the security performance at physical layer. In this chapter, we will give a brief overview of several existing prevalent methods with respect to the cooperation within multi-antenna networks and multi-user networks, for improving the confidentiality. Specifically, we mainly focus on time reversal (TR) technique, spatial modulation (SM) technique as the representative multi-antenna cooperative strategies, and D2D transmissions as typical scenarios for investigating cooperation behavior among mobile users. The reason why we elaborate such strategies is that they have their own specific characteristics for enhancing the security performance. Typically, the signal focusing property of TR can be exploited to reduce signal leakage to unintended users, hence the secrecy performance is improved. For SM transmission, the system can achieve the same degree of security compared to the conventional MIMO system, while effectively reducing the complexity of system. Finally, there are a number of cooperative techniques can be perfectly implemented in D2D communications, and due to the social interactions among the mobile users, the issues of security can be investigated from a novel perspective. Each of these methods will be discussed from two aspects: the basic corresponding principles of such techniques and their applications in physical layer security. Specifically, we elaborate the basic transmission models, characteristics, and their practical applications. The issues in physical layer security will be discussed with the current state of research.

L. Wang, *Physical Layer Security in Wireless Cooperative Networks*, Wireless Networks, DOI 10.1007/978-3-319-61863-0_2

2.1 Time Reversal Technique

2.1.1 Basic Principles of Time Reversal Technique

TR is a technique focusing the signal energy in both time and space domains. TR was first developed by M. Fink in the mid 1990s [1]. The basic principle of TR is that in the multiple-input-single-output (MISO) system, the receiver first sends a pilot signal with an impulse shape which then is transmitted through a scattering and multi-path channel and the resulting waveforms are received and recorded by the transmitter. Then, the transmitter time reverses (and conjugates, if the signal is complex valued) the channel impulse response as its signaling pulse over the same channel and transmits back to its intended receiver.

Generally, there are two basic assumptions for the TR communication system [2]:

- **Channel reciprocity**: the impulse responses of the forward link channel and the backward link channel are assumed to be identical.
- **Channel stationary**: the channel impulse responses (CIRs) are assumed to be stationary for at least one probing-and-transmitting cycle.

Now we analyze the TR transmission via a multi-path channel of the k-th antenna in a MISO system, as shown in Fig. 2.1. We assume that a sequence of information symbols transmitted from the k-th antenna are

$$x_k(t) = b_k \sum_{m=-\infty}^{\infty} a_m \delta(t - mT), \tag{2.1}$$

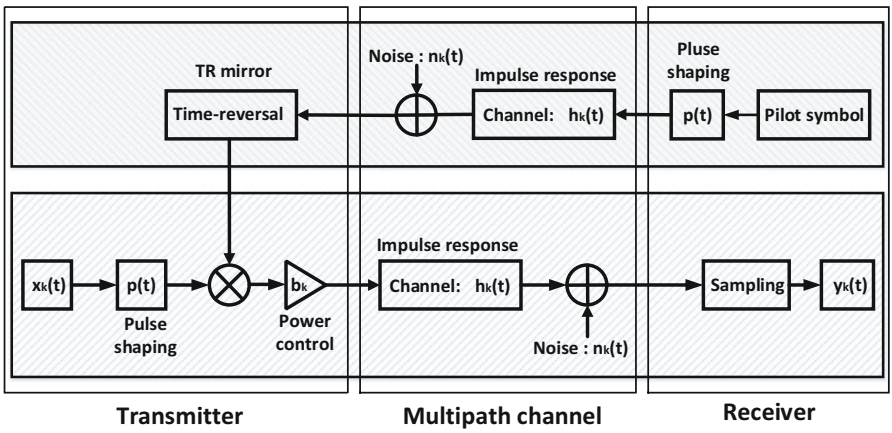


Fig. 2.1 Conventional time reversal communications (k-th antenna) [2]

where b_k is used for normalizing the power according to the k-th transmit antenna number. T is the symbol duration, and a_m is the consecutive symbols for the modulation scheme. For example, if binary phase shift keying (BPSK) is used, binary bits which are equal to 0 or 1 mapping to $a_m = -1$ or $a_m = +1$, respectively.

Besides, the CIR of the k-th antenna to the receiver can be written as

$$h_k(t) = \sum_{i=0}^{L_k} h_{ki}\delta(t - \tau_{ki}), \tag{2.2}$$

where h_{ki} is the complex channel gain of the i-th path of the CIR, and τ_{ki} is the corresponding path delay, and $L_k + 1$ is the total number of the multi-paths. Besides, L_k is assumed as a constant in our basic analysis and the collection $\{L_k\}$ is modeled as a set of independent random variables, each of them follows identical uniform distribution, where $\text{Prob}(L_k = \ell) = L^{-1}, \quad \ell = 0, 1, , \cdots, L - 1$.

1) Pilot Transmission Prior to the TR transmission from the transmitter, the receiver first sends out a pilot signal to assist the transmitter to estimate the perfect CSI. The pilot signal is transmitted through a pulse $p(t)$ of duration T, which then propagates to transmitter through the multi-path channel $h_k(t)$, where the transmitter keeps a record of the received waveform, $\widetilde{h}_k(t)$, which is the convolution of $h_k(t)$ and $p(t)$, represents as follows:

$$\widetilde{h}_k(t) = h_k(t) \otimes p(t) = \sum_{i=0}^{L_k} h_{ki} p(t - \tau_{ki}), \tag{2.3}$$

where $\otimes$ denoted the convolution operation, $\widetilde{h}_k(t)$ can be treated as an equivalent channel response for the system with a limited bandwidth.

2) Data Transmission Upon receiving the waveform, the transmitter time-reverses (and conjugates, when complex-valued) the equivalent channel response $\widetilde{h}_k(t)$. We denote $\widetilde{h}_k^*(T_p - t)$ as the time-reversed and conjugated channel response where T_p is the maximum multi-path delay, so the normalized TR waveform $\rho_k(t)$ can be expressed as [3]

$$\rho_k(t) = \frac{\widetilde{h}_k^*(T_p - t)}{\sqrt{E\left\{\int_{-\infty}^{\infty} \left|\widetilde{h}_k(t)\right|^2 dt\right\}}} = \frac{\widetilde{h}_k^*(T_p - t)}{\sqrt{E_k}}. \tag{2.4}$$

At transmitter, there is a sequence of information symbols $x_k(t)$ to be transmitted to receiver. Applying the TR waveform $\rho_k(t)$, the signal can be written as

$$s_k(t) = x_k(t) \otimes \rho_k(t) = b_k \sum_{m=-\infty}^{\infty} a_m \rho_k(t - mT). \tag{2.5}$$

Therefore the received signal in baseband can be expressed as

$$w_k(t) = s_k(t) \otimes p(t) \otimes h_k(t) + n_k(t) = b_k \sum_{m=-\infty}^{\infty} a_m \rho_k (t - mT) \otimes \sum_{i=0}^{L_k} h_{ki} p(t - \tau_{ki}) + n_k(t). \tag{2.6}$$

2.1.1.1 Main Properties of TR Technique

- **Temporal focusing:** by utilizing channel reciprocity, the re-emitted TR waves can retrace the incoming paths, ending up with a constructive sum of signals of all the paths at the intended location and a "spiky" signal-power distribution over the space. The received signal is compressed in the time domain. Owing to this property, the inter-symbol interference (ISI) at the receiver caused by the original multipath channel is significantly reduced [4].
- **Spatial focusing:** the received signal is focused on the intended user at some specific position, which is determined by the transmitter that uses the corresponding channel to pre-filter the intended data signal. Spatial focusing combats channel fading, maximizes delivered power to the intended receiver, as shown in Fig. 2.2 [5]. Therefore, the power can be saved at the transmitter side and the channel

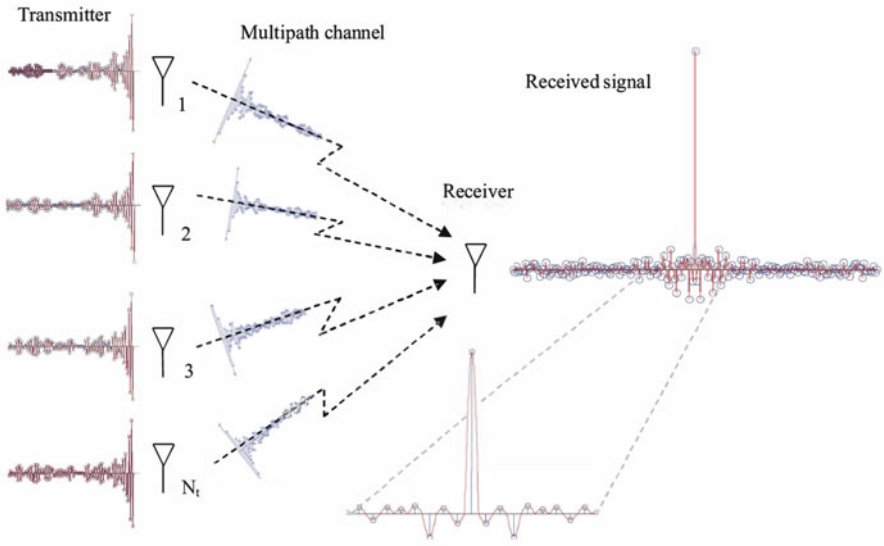


Fig. 2.2 Property of the spatial focusing in TR [5]

capacity and communication range can be increased as well. Spatial focusing also reduce power leakage to other locations. This is very useful to reduce interuser interference in multiuser configuration, which in turn allows a more effective use of space-division multiple access (SDMA) to boost the system capacity [6]. Spatial focusing also adds a degree of physical layer security to the system, making it hard for eavesdroppers away from the intended receiver's location to decode the signal.

2.1.2 Applications of Time Reversal Technique

- **Underwater communications:** underwater communications using acoustic waves are difficult to achieve high data rates due to the time varying nature of the dispersive multi-path environments. In this case, the TR technique has two effects: (1) temporal compression that reduces dispersion caused by the channel [7]; (2) the characteristic of spatial focusing mitigates the effects of fading. These characteristics also eliminate the need for diversity techniques such as multiple receive antennas [8]. In July of 1999, Edelman conducted underwater testing of a time reversal mirror for communications off the west coast of Italy [9]. The experiment was operated at 3.5 kHz with BPSK in three different underwater environments: an absorptive bottom, a reflective bottom, and a sloping bottom. The experiment transmitted 50 bits to the receiving array and decoded them. As an unique strategy, TR can not only decode all 50 bits correctly at the intended location, but also can cause more detection errors at other locations as an effective method.
- **Sensing radar:** most radar systems are designed under line-of-sight (LoS), not in multipath channel environments. Besides, the range of radar sensors is limited by LoS blackage due to the buildings, forests, and many other scatters. By using the TR technique, the transmission waveforms are tailored for the propagation medium and the target scattering characteristics. Hence, TR is a radar waveform adaptive transmission scheme [10]. Plumb and Leuschen applied a TR mirror to solve a remote sensing problem [11]. In ground penetrating radar, antennas transmit a pulse from the surface and then the signal is recorded either in the same location, or in a different location. The desired outcome of ground penetrating radar is to get an accurate picture of the object space. Plumb and Leuschen proposed to use TR technique as a matched filter to model the dielectric properties of the ground. This experiment shows the flexibility of TR theory.
- **Inhomogeneous medium:** in most cases, inhomogeneous environments cause problems for communication system. Replicas of the signal are incident on the receiver due to reflections, resulting in small scale fading. This problem is compounded when the environment or the user is in motion which results in Doppler shifts. In the case of TR methods, an inhomogeneous medium will actually improve the accuracy of the communication [12]. Random reflectors throughout the environment will focus more energy onto the antenna array.

- **Ultra Wideband communication:** an Ultra Wideband (UWB) communication system is defined as an antenna transmission for which transmitted signal bandwidth exceeds 500 MHz or 25% of the arithmetic center frequency. UWB has become a promising candidate for high-data rate and short range communication systems. However, due to the wide bandwidth property, UWB systems may suffer from a very long delay spread brought from multipath effect [13]. Due to the power focusing property of TR, it is a feasible technique to solve the existing problems in UWB by combining TR technique to improve the transmission rate and minimize the influences of channels thus increasing the quality of UWB systems [14].

2.1.3 Time Reversal Technique for Physical Layer Security

In ordinary wireless communication systems, each user's signal is broadcast in all directions. Knowing the users' frequency band, time slot, or code will allow someone to decode the information intended for that user. As mentioned before, Edelman's experiment showed that TR can let the transmit signal focus spatially and compress temporally on the intended receiver. This result verified that the TR can provide a more extended solution of security issues than other methods. In wireless communications, signal leakage to unintended receivers causes security risk and co-channel interference. The signal focusing property of TR can also be exploited to reduce signal leakage to unintended users, so it has potential to facilitate the physical layer secrecy in wireless communications.

It has been verified in [15] that TR with time-space focusing characteristic can be utilized to improve information transmission in terms of anti-detection/interception performance in the space of wireless sensor networks, reduce probability that the signal have been illegally detected in space-time domain, and improve information dissemination security in space. The effect of linear block precoding for distributed TR (DTR) in the discrete time domain has been studied in [16]. Given multiple distributed transmit antennas, each eavesdropper was assumed to have only one antenna. By focusing on block transmission schemes, including orthogonal frequency division multiple access (OFDMA), their work optimized the precoder and analyzed secrecy capacity by showing that high-rate messages can be transmitted towards an intended user without being decoded by other users from the viewpoint of information theoretic security. Moreover, experimental characterization of the confidentiality with an indoor MISO-TR transmission has been reported in [17]. The secrecy performances between TR and maximum ratio transmission (MRT) precoding techniques has been compared in [18] in terms of achievable secrecy rate in MISO-OFDM systems. They verified that the achievable secrecy rate of MISO-TR-OFDM is always better than its counterpart in MISO-MRT-OFDM. Besides, implementing TR technique in MIMO-UWB system has been also investigated in [19], which indicates that TR can be used to improve the secrecy capacity.

2.2 Spatial Modulation Technique

2.2.1 Basic Principles of Spatial Modulation

MIMO techniques are regarded as a crucial technology for modern wireless communications, which can be exploited in different ways to get multiplexing, diversity, or antenna gains. Regardless of the benefits brought from MIMO system such as spatial multiplexing, diversity, or smart antenna system, the main drawback of MIMO system is nonnegligible complexity and cost. This is primarily because of three main reasons [20]: (1) Inter-channel interference (ICI), which is introduced by superimposing independent information sequences to be transmitted by multiple transmit antennas; (2) Inter-antenna synchronization (IAS), which represents the baseline assumption for space-time and delay-diversity encoded methods; (3) multiple radio frequency (RF) chains, which are needed to transmit all the signals simultaneously and are expensive and do not follow Moore's law. These issues make the practical implementation of MIMO schemes difficult, especially in mobile stations, as the necessary hardware and digital signal processing require significant energy.

Hence, Spatial Modulation (SM) has been proposed as a novel multiple-antenna transmission technique which can effectively provide improved data rates with a very low system complexity, and robust error performance even in the uncorrelated channel environments. This is achieved by adopting a simple but effective coding mechanism that establishes a one-to-one mapping between blocks of information bits to be transmitted and the spatial positions of the transmit-antenna in the antenna-array.

The basic idea of SM was derived from Chau and Yu's work in 2001 [21], in which the receiver decodes the signals transmitted from the different antennas. Then the comprehensive interpretation of SM was proposed by Mesleh and Haas [22]. As a re-designed modulation concept for MIMO systems, SM aims at reducing the complexity and cost of multiple-antenna schemes without deteriorating the end-to-end system performance and still guaranteeing the required data rates. More specifically, the low-complexity transceiver design and high spectral efficiency are simultaneously achieved. The main idea of SM is to map a block of information bits into two information carrying units [23]:

- A symbol that is chosen from a complex signal constellation diagram.
- A unique transmit-antenna index that is chosen from the set of transmit-antenna in the antenna-array.

2.2.1.1 Transmitter and Receiver

Figure 2.3 illustrates a basic model for a SM system. Let us analyze the characteristics of SM in terms of transmitted signal and received signal, respectively.

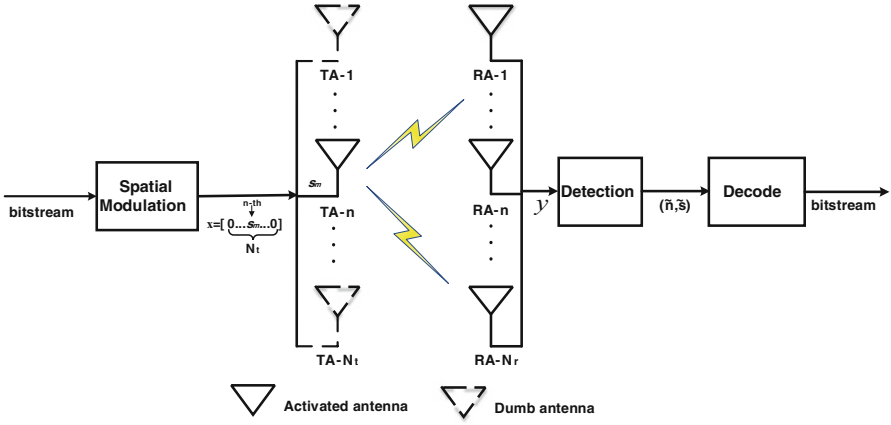


Fig. 2.3 System model of SM

- **Transmitter:** We assume that the n-th transmit antenna (TA-n) is activated, where $n \in L = \{1, 2, \ldots N_t\}$ and the channel is quasi-static frequency-flat fading, the received signal model of SM-MIMO is as follows:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{2.7}$$

where $\mathbf{y} \in \mathbb{C}^{N_r \times 1}$ is the complex received vector; $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$ is the complex channel matrix; $\mathbf{n} \in \mathbb{C}^{N_r \times 1}$ is the complex AWGN at the receiver; and $\mathbf{x} \in \mathbb{C}^{N_t \times 1}$ is the complex modulated vector and can be formulated as

$$\mathbf{x} = [0 \ldots 0 \underbrace{s_m}_{n-th} 0 \ldots 0]^T = \mathbf{e}_n s_m \tag{2.8}$$

where $s_m \in \mathbb{C}^{1 \times 1}$ is the Phase Shift Keying (PSK)/Quadrature Amplitude Modulation (QAM) modulated symbol belonging to the signal set $\mathscr{S}$, and $\mathbf{e}_n \in \mathbb{R}^{N_t \times 1}$ is the vector belonging to the spatial-constellation diagram $\mathscr{A}$ as follows:

$$\mathbf{e}_n = \begin{cases} 1, \text{if the } n\text{-th TA is active} \\ 0, \text{if the } n\text{-th TA is not active} \end{cases} \tag{2.9}$$

For convenience, $\mathbf{e}_n$ can be written as

$$\mathbf{e}_n = [0 \ldots 0 \underbrace{1}_{n-th} 0 \ldots 0]^T$$

- **Receiver:** Similarly, according to the characteristic of SM, if n-th (recall that $n \in L$) antenna is activated, the received signal also can be written as

$$\mathbf{y} = \mathbf{h}_n s_m + \mathbf{n}, \tag{2.10}$$

where $\mathbf{h}_n$ is the n-th column of $\mathbf{H}$, $s_m \in \mathscr{S}$.

In order to detect the transmitted signal from the noisy received signal $\mathbf{y}$, the receiver must know the channel impulse response of all the links, i.e., perfect CSI via channel estimation. According to the ML principle, the receiver computes the Euclidean distance (two-norm of a vector) between the received signal and the set of possible signals modulated by the wireless channel (including signal modulation if SM is used) and chooses the closest one. Specifically,

$$(\tilde{n}, \tilde{s})_{ML} = arg \min_{n \in L, s_m \in \mathscr{S}} \|\mathbf{y} - \mathbf{h}_n s_m\|^2, \tag{2.11}$$

where $\tilde{n}$, $\tilde{s}$ are the estimated activated antenna index and transmitted symbol, respectively.

2.2.1.2 Mapping Rule of SM Using Three-Dimensional Constellation Diagram

A simple instance of mapping rule in SM is illustrated in Fig. 2.4 with $N_t = 2$ and M-QAM modulation where M=4, where Q and I are the real axis and imaginary axis of the signal constellation, respectively. It shows a three-dimensional (3-D) constellation diagram of SM. The bitstream transmitted by a binary source is processed by a SM mapper, which splits each of them into two parts of $\log_2(N_t)$ and $\log_2(M)$ bits, respectively. The bits in the first part are used to determine the index of the activated antenna which is for data transmission, while remaining transmit antennas are kept dumb in the transmission time interval. Besides, the bits in the second part are used to choose a symbol in the signal-constellation diagram.

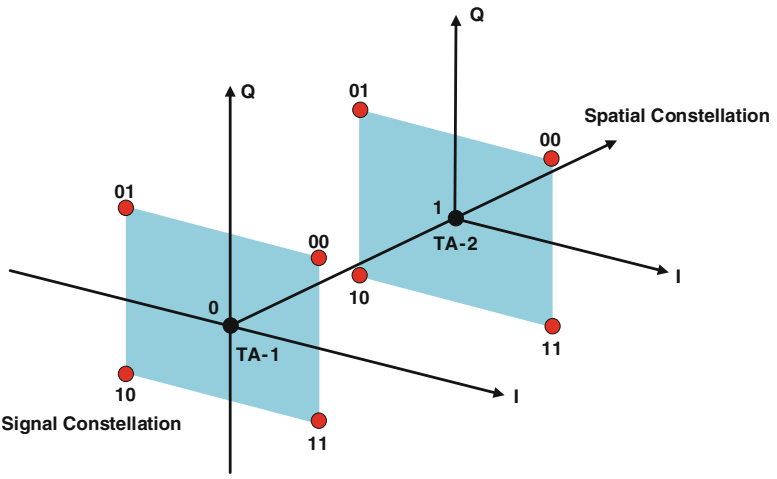


Fig. 2.4 Illustrations of SM mapper (4-QAM)

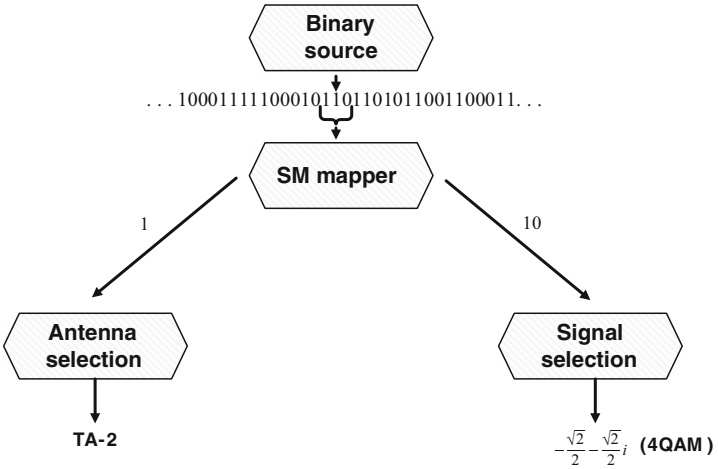


Fig. 2.5 Basic working principle of SM mapper

So it is obvious that the total bits transmitted in one time slot by using SM is $\log_2(N_t) + \log_2(M)$ [24]. Figure 2.5 illustrates a case in which bitstream "110" is emitted in current time slot. "1" indicates that the second transmit antenna is activated, and "10" determines the transmitted QAM symbol.

2.2.1.3 Advantages and Disadvantages of SM

Compared with other MIMO schemes, SM has its own advantages and disadvantages [24]:

- **Advantages:** (1) compared to the conventional MIMO techniques, such as Vertical-Bell Laboratories layered space-time (V-BLAST) and Alamouti space-time schemes, SM entirely avoids ICI and IAS, and only requires a single RF chain at the transmitter due to its working mechanism; (2) compared to conventional single-antenna systems, the 3-D constellation diagram in SM introduces a multiplexing gain in the spatial domain that increases systematically with the number of transmit-antenna; (3) the receiver design is inherently simpler than the V-BLAST scheme since complicated interference cancellation algorithms are not required to cope with the ICI: unlike conventional spatial-multiplexing methods for MIMO systems, SM can attain ML decoding via a simple single-stream receiver. (4) SM can still function effectively even if the number of receive antennas is fewer than the number of transmit antennas, i.e., $N_r < N_t$, as the MIMO configuration provides sufficient diversity gain.
- **Disadvantages:** (1) at least two transmit antennas are required to exploit the SM concept; (2) a rich-scattering environment is required to guarantee a significant improvement for the data rate, otherwise the SM might not be

used or might not achieve better performance; (3) the receiver requires perfect channel knowledge for data detection: this may pose complexity constraints on the channel estimation unit, as well as some overhead for channel estimation; (4) when compared to conventional MIMO techniques, such as V-BLAST, SM can offer only a logarithmic (instead of linear) increase of the data rate with the number of transmit antenna; (5) due to the working mechanism of SM, the number of RF chains is often low that will introduce negative effect on high-frequency transmission, e.g., millimeter-wave communications, which needs a high multiplexing gain and a high beamforming gain.

2.2.2 *Extended Versions: Space Shift Keying and General Space Shift Keying*

As the complements of SM technique, Space Shift Keying (SSK) and General Space Shift Keying (GSSK) have been investigated by J. Jeganathan in 2008 and 2009, respectively [20, 25]. Both of them can be regarded as simplified versions of SM, which have the same performance in terms of the throughput.

2.2.2.1 Space Shift Keying (SSK) Modulation

SSK modulation is a low-complexity implementation of SM, in which only antenna indices are used for transmitting bits, so the conventional amplitude/phase modulation (APM) techniques are not necessary. This elimination of APM provides SSK with notable differences and advantages over SM [20]: (1) detection complexity is lowered, while the performance is almost identical to SM under the optimal detection; (2) because phase and amplitude of the pulse do not convey information, transceiver requirements are less stringent than that of APM; (3) the simplicity of SSK's framework provides ease of integration within communication systems. For example, SSK has potential to be implemented in UWB system, where the pulses are used instead of APM signals.

In SSK modulation, the transmitter maps the data bits to the symbols $\mathbf{x}$, and encodes block of $k = \log_2(N_t)$ data bits into the index of a single transmit antenna which is switched on for data transmission, while the other antennas are kept silent. Therefore, input data vector $\mathbf{x}$ is shown, if n-th antenna is used, as

$$\mathbf{x} = [0 \dots 0 \underbrace{1}_{n-th} 0 \dots 0]^T = \mathbf{e}_n$$

Table 2.1 shows the corresponding modulation principle of SSK with modulation order $M = 4$. In general, the number of needed transmitting antenna N_t equals to M.

Table 2.1 Modulation principle of SSK [20]

Antenna index	Symbol	Transmitting bits $[b_1 \quad b_2]$	Transmitting vector $[x_1 \quad x_2 \quad x_3 \quad x_4]$
1	0	[0 0]	[1 0 0 0]
2	1	[0 1]	[0 1 0 0]
3	2	[1 0]	[0 0 1 0]
4	3	[1 1]	[0 0 0 1]

Table 2.2 Modulation principle of GSSK [25]

Antenna index combination	Transmitting bits $[b_1 \quad b_2 \quad b_3]$	Transmitting vector $x = [x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5]$
(1,2)	[0 0 0]	$[\frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad 0]$
(1,3)	[0 0 1]	$[\frac{1}{\sqrt{2}} \quad 0 \quad \frac{1}{\sqrt{2}} \quad 0 \quad 0]$
(1,4)	[1 1 0]	$[\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}} \quad 0]$
(1,5)	[1 1 1]	$[\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}}]$
(2,3)	[1 0 0]	$[0 \quad \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}} \quad 0 \quad 0]$
(2,4)	[1 0 1]	$[0 \quad \frac{1}{\sqrt{2}} \quad 0 \quad \frac{1}{\sqrt{2}} \quad 0]$
(2,5)	[1 1 0]	$[0 \quad \frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}}]$
(3,4)	[1 1 1]	$[0 \quad 0 \quad \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}} \quad 0]$

2.2.2.2 Generalized Space Shift Keying (GSSK) Modulation

Jeganathan et al. extended their work on SSK by allowing more than one antenna to be activated in every channel use and by encoding the information bits onto various combinations of multiple active antennas, which is referred to as GSSK [25]. The motivation of GSSK comes from the limitation of $N_t = M$ when M is very large. It has been shown in [25] that for the same number of transmit antenna elements the rate can be improved at the cost of increasing the number of RF chains, while tolerating some performance loss. Thus, at the cost of increasing the number of RF chains, GSSK-MIMO provides higher rates than SSK-MIMO. Moreover, this encoding scheme still preserves the ICI-free advantage even though more than one transmit antennas are active.

In GSSK modulation, if $n_t (N_t \geqslant n_t)$ transmit antennas are active in each time slot, there will be $M' = C_{N_t}^{n_t}$ available constellation points. Then select M combination from M' available constellation points to be the transmit antennas. The transmitter encodes block of $k = \log_2(M)$ data bits into the transmit antenna index. And the input data vector $\mathbf{x}$ has n_t non-zero entries, i.e.,

$$\mathbf{x} = \left[\frac{1}{\sqrt{n_t}} 0 \ldots 0 \frac{1}{\sqrt{n_t}} 0 \ldots 0 \frac{1}{\sqrt{n_t}}\right]^T$$

Table 2.2 shows the modulation principle of GSSK in which $N_t = 5$ and $n_t = 2$.

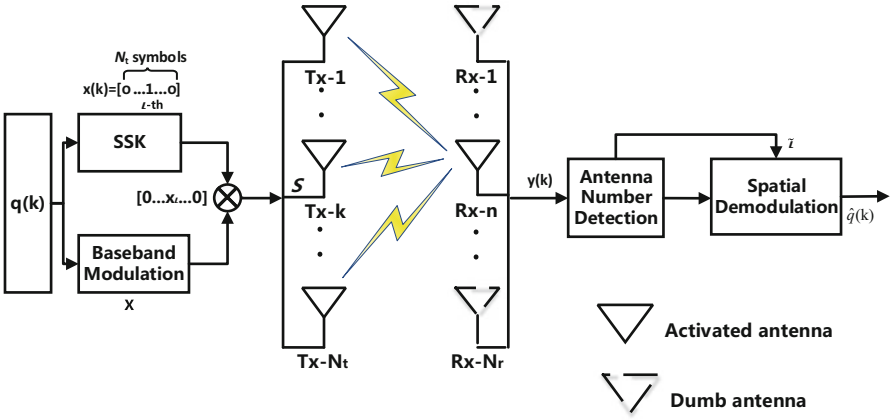


Fig. 2.6 System model of pre-coding aided spatial modulation[26]

2.2.3 Pre-Coding Aided Spatial Modulation Schemes

The conventional SM technique carries the spatial information with transmit antenna index and assumes perfect CSI at receiver (CSIR). However, in some practical scenarios, CSI is preferably to be exploited at transmitter (CSIT). So compared to the conventional one, the modified SM schemes exploit the receive antenna index, by doing so the complexity at receiver is effectively reduced.

Furthermore, it is widely recognized that the MIMO systems operated under CSIT mode have a range of advantages over that under the CSIR mode [26]. First, when a MIMO system has more transmit antennas than receive antennas, the capacity under the CSIT mode may be much higher than that under the CSIR mode. Second, opposite to the openloop space-time diversity (STD) schemes operated under CSIR mode, which can only attain the transmit diversity gain, the closed-loop STD schemes under CSIT mode are able to provide the receiver with the SNR gain, apart from the promised transmit diversity gain.

Based on these theories, [26] proposed a space-based modulation scheme, namely the *pre-coding aided spatial modulation* (PSM) scheme, which carries information using transmitter antennas and assumes CSIR.

The basic system model of PSM is shown in Fig. 2.6. T_x, R_x indicate transmit antenna and receive antenna, respectively. $\mathbf{q}(k) \in \mathbb{C}^{N_r \times 1}$ is denoted as PSM symbol determined by two components of information, one is $\mathbf{x}(k)$ conveyed by the indices of receive antennas, where $\mathbf{x}(k) = [0 \ldots 0 \underbrace{1}_{k-th} 0 \ldots 0]^T$ and k represents the activated receive antenna. The other component is x_l conveyed by the conventional APM where l is related to the modulation mode. Specifically, $\mathbf{q}(k) = \mathbf{x}(k) \cdot x_l = [0 \ldots 0 \quad x_l \quad 0 \ldots 0]^T$.

The PSM uses certain transmitter pre-coding scheme to identify the desired receive antenna, based on which the detector can acquire the first component of information carried in the spatial domain. The second component of information is recovered from the conventional APM in the traditional demodulation way.

Explicitly, the proposed PSM can be regarded as a dual modulation scheme of the SM for MIMO communications [29]. Similarly, in PSM, the received signal $\mathbf{y}(k) \in \mathbb{C}^{N_r \times 1}$ can be written as

$$\mathbf{y}(k) = \mathbf{H}^H \mathbf{P}\mathbf{q}(k) + \mathbf{n}, \tag{2.12}$$

where $\mathbf{H} \in \mathbb{C}^{N_t \times N_r}$ denotes the channel matrix between the transmitter and receiver and $\mathbf{P} \in \mathbb{C}^{N_t \times N_r}$ denotes complex pre-coding matrix. $\mathbf{n} \in \mathbb{C}^{N_r \times 1}$ is an additive Gaussian noise vector. According to [26], $\mathbf{P}$ can be designed as $\mathbf{P} = \boldsymbol{\beta}\mathbf{H}^* \left(\mathbf{H}^H \mathbf{H}^*\right)^{-1}$, where $\boldsymbol{\beta} \in \mathbb{C}^{N_t \times N_t}$ is the normalized matrix. Similar to the conventional SM scheme, a ML detector can be employed to detect the transmitted information.

Recall that in the PSM, two types of modulations, namely SSK and conventional APM, are jointly used to convey information. Specifically, SSK is implemented by the indices of receiver antennas, with the aid of zero forcing pre-coding (ZFP) or minimum mean square error pre-coding (MMSEP). Therefore, the PSM employs two distinctive advantages: additional information transmission in space domain, and low-complexity detection. In PSM, a portion of transmitted messages serve as a pseudo-noise (PN) sequence to randomly activate a receive antenna of the desired receiver, making the receive antenna hopping pattern controlled directly by the transmitted message. So it is hard for the eavesdropper to acquire the CSI of the desired receiver and, hence, barely possible to know the pre-coding matrix $\mathbf{P}$. It is widely shown that PSM can enhance the performance of communication system with proper design of $\mathbf{P}$, making the system achieve a better secrecy rate and overall BER performance to combat the eavesdropping.

So far, PSM has been investigated from different perspectives due to its merits. In order to guarantee the physical-layer security in presence of an unauthorized eavesdropper, a secret PSM (SPSM) was proposed in [27], which can significantly enhance the security of the PSM, in addition to inheriting all its merits. Apart from the PSM which activates only one receive antenna at the same time, the model of generalized PSM (GPSM), proposed in [28], is that a particular subset of receive antennas is activated so the activation pattern can convey partial information. Compared with PSM, both SPSM and GPSM have their unique advantages, which are illustrated in the following parts.

2.2.3.1 Secret Pre-Coding Aided Spatial Modulation (SPSM)

Assume that MIMO system confronts an eavesdropper trying to intercept the transmitted data, and the transmitter does not know its existence. From the analysis in above subsection, we can know that the knowledge of $\mathbf{P}$ to Eve determines the security of the PSM system. When the transmitter-receiver channels vary slow, the

pre-coding matrix $\mathbf{P}$ designed in Eq. (2.12) may change very slowly, which benefits Eve's eavesdropping. Therefore, the basic idea to design SPSM is to construct a fast time-varying pre-coding matrix $\hat{\mathbf{P}}$. By introducing some perturbation to the pre-coding matrix $\mathbf{P}$, SPSM can make the eavesdropper's detection impeded much more seriously[27].

Generally, Eve will retrieve the data through the blind estimation. In order to further decrease the probability of successful eavesdropping, we can design some perturbation to deteriorate the blind estimation at Eve, which can be realized in the following ways.

The SVD on channel matrix $\mathbf{H}$ can be written as

$$\mathbf{H} = \mathbf{U}\boldsymbol{\Sigma}[\mathbf{V}^{(1)} \ \mathbf{V}^{(0)}]^H, \tag{2.13}$$

where $\mathbf{V}^{(0)}$ is the null space of $\mathbf{H}$. Then, a matrix $\mathbf{T}$ can be designed as $\mathbf{T} = \mathbf{V}^{(0)}\mathbf{R}$, where $\mathbf{R}$ is a matrix whose elements are complex Gaussian random variables with zero mean and unit variance. The symbols in $\mathbf{R}$ keep time-varying and independent. Therefore, $\mathbf{T}$ is fast-varying. When the time-varying perturbation $\mathbf{T}$ is designed in pre-coding matrix $\mathbf{P}$ so that the fast time-varying pre-coding matrix $\hat{\mathbf{P}} = \mathbf{P} + \mathbf{T}$, it is clear that Bob is not affected by its interference because $\mathbf{T}$ lies in the *nullspace* of $\mathbf{H}$. On the contrary, Eve is greatly influenced by the time-varying perturbation $\mathbf{T}$, which largely decreases the precision of blind estimation.

By incorporating a random component, SPSM becomes much more secure than PSM. The SPSM is able to provide secure information transmission, even when the authorized receiver's CSI is leaked to an eavesdropper. It is also demonstrated that the SPSM can not only inherit the PSM's advantage of low-complexity detection, but also provide significantly improved secrecy performance.

2.2.3.2 Generalized Pre-Coding Aided Spatial Modulation (GPSM)

As mentioned above, SM conveys extra information by mapping proportional bits to the indices of transmit antennas, in addition to the traditional modulation schemes. On the contrary, the PSM schemes is able to convey extra information by appropriately exploiting the receive antenna. Apart from these two schemes, the further improved concept of GPSM is proposed, where the key idea is that a particular subset of receive antennas is activated and a part of useful information is conveyed by the activation pattern. This is different from the previously proposed SM and PSM schemes, which are realized by activating only one specific transmit/receive antenna. It is shown that the GPSM scheme constitutes a flexible alternative to the state-of-the-art MIMO transmission schemes, especially because it realizes a high throughput. Moreover, mapping information to the spatial domain rather than relying on conventional modulation has plenty of benefits in the high SNR region. Quantitatively, GPSM is capable of exhibiting an approximately 1 dB SNR gain compared to the conventional MIMO scheme with the same throughout and complexity [30].

Table 2.3 A comparison between SM, PSM, SPSM, and GPSM

Scheme	Activation pattern	Mode	Advantages
SM	Only a transmit antenna	CSIR	No ICI, low receiving complexity
PSM	Only a receive antenna	CSIT	Better secrecy rate and BER performance than SM
SPSM	Only a receive antenna	CSIT	Achieve higher secrecy rate when compared to PSM
GPSM	A subset of receive antennas	CSIT	Transmit more bits than PSM with same antenna number

Consider a MIMO system equipped with N_t transmit antennas and N_r receive antennas, where we suppose $N_t \geqslant N_r$. In this MIMO system, a maximum of N_r parallel data streams may be supported, conveying a total of $k = N_r k_{mod}$ bits altogether, where $k_{mod} = \log_2(M)$ denotes the number of bits per symbol of a conventional M-PSK/QAM scheme and M is denoted as modulation index. In contrast to the aforementioned traditional multiplexing of N_r data streams, in GPSM scheme, N_a receive antennas are activated in order to facilitate the concurrent transmission for N_a data streams, in which the particular pattern of N_a activated receive antennas conveys information consisting of spatial symbols in addition to the information carried by the conventional modulated symbols. Hence, the number of bits in GPSM conveyed by a spatial symbol becomes $k_{ant} = \log_2(C)$, where the set C contains all the combinations associated with choosing N_a activated receive antennas out of N_r receive antennas. As a result, the total number of bits transmitted by the GPSM scheme is $k = k_{ant} + N_a k_{mod}$, which is more than that in PSM scheme.

Table 2.3 presents the comparison of conventional SM, PSM, SPSM, and GPSM.

2.2.4 Spatial Modulation in Physical Layer Security

It can be found that the randomness and uniqueness properties of wireless channels are very important in both physical layer security and spatial modulation technique. In the SM paradigm, the symbols modulated on the antenna indices would be undistinguishable if all the channel are identical. Therefore, the feasibility of physical layer security and spatial modulation depends on the same nature of the wireless channels. So SM has potential to improve the physical layer security of wireless networks, by properly designing the transmission signal.

With respect to secrecy rate of SM-MIMO form the information theoretic perspective, the spatial transmission features of SM-MIMO make it attractive for secrecy capacity analysis. In [31], the authors demonstrated that SM-MIMO can achieve better secrecy capacity than that of its single antenna counterpart. Also, [32] established improved secrecy rate with growing number of transmit antennas in SM-MIMO system. To further strengthen the secrecy rate of SM-MIMO, the authors of [33] and their subsequent work [34] proposed a precoding-aided spatial modulation

method for enhancing physical layer security. Moreover, authors in [35] examined the secrecy rate enhancements that can be attained by applying CSI aided transmit signal design algorithms in SSK transmission.

2.3 D2D Communications in Cellular Networks

Apart from the security issues in aforementioned multiple-antenna systems, mobile users who are equipped with single antenna will also confront threats from malicious wireless nodes. D2D communication is a promising wireless technique which enables mobile user communicate to each other without the help or supervision of infrastructure. There will be new problems with respect to security issues in D2D communications. In this part, we are going to investigate some details of D2D communications and the security issues in such certain scenario.

2.3.1 Basic Principles of D2D Communications

The explosive growth in the demand of wireless mobile data expects the telecommunication industry to introduce new standards that can provide higher throughput, lower energy consumption, and better quality of service (QoS). Under this situation, there has been increased interest in D2D communication, as manifested by the WiFi Direct specifications and proposals for Long Term Evolution-Advanced (LTE-A) D2D standardization [36]. Increasingly, mobile stakeholders such as device manufacturers and network operators are accepting that D2D communications will be a cornerstone of future 5G networks, which drives the standardization of D2D technologies. After the 3GPP meeting held in June 2011 [37, 38], the concept of D2D discovery and communication was submitted and widely accepted by both industrial and academic fields.

D2D communications refer to a type of technology that enables devices to communicate directly with each other without the involvement of fixed networking infrastructures such as access points (APs), base station (BSs), etc. By sharing resource blocks (RBs) of cellular users, D2D communications can significantly improve the spectral efficiency.

In general, D2D users can communicate with other users in the following three manners [39]:

- **D2D Direct Link:** The simplest case of D2D communications occurs when transmitters and receivers exchange data directly with each other without intermediate nodes.
- **Relay-Assisted D2D Communications:** When user devices are at the edge or out of BS coverage, they can communicate with the BS through relaying their communication data via other covered devices.

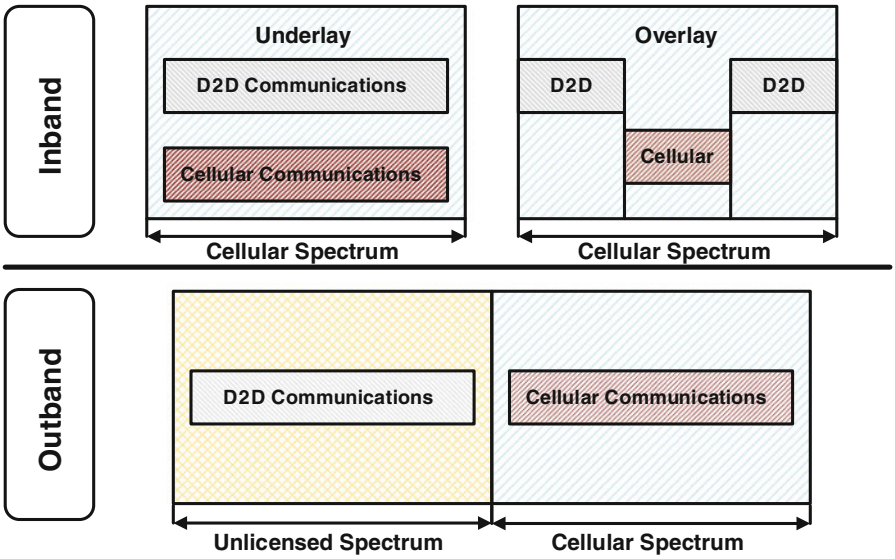


Fig. 2.7 Illustrations of D2D classification [40]

- **Cluster-Assisted D2D Communications:** In a content sharing or information diffusion scenario, users requesting the same file in a short range can potentially form a cluster to allow the desired file to be multicasted within the cluster to save both bandwidth and time delay.

Besides, in D2D communications, both unlicensed and licensed spectrum resources can be utilized by D2D users for communication, which can be classified as two categories shown in Fig. 2.7: *outband D2D* communications and *inband D2D* communications [40]:

- **Outband D2D:** D2D communications exploit unlicensed spectrum. The essential advantages of outband D2D communications lie in the elimination of interference between D2D links and cellular links since D2D communications occur on license-exempt bands. Notice that an extra radio interface is necessary for exploiting unlicensed spectrum, which brings up with other wireless technologies together, such as Wi-Fi, Wi-Fi Direct, Bluetooth. Outband D2D can be further divided into *controlled communication* in which the control of a second interface is under the cellular network, and *autonomous communication* in which the cellular network controls all the communication but leaves the D2D communication to the users [41].
- **Inband D2D:** D2D communications operate on licensed spectrum (i.e., cellular spectrum) which is also allocated to cellular links. High control over cellular (i.e., licensed) spectrum indicates that it is more convenient to provide better user experiences under a planned environment. Inband D2D communications can be further divided into two types, referred to *underlay D2D communications*

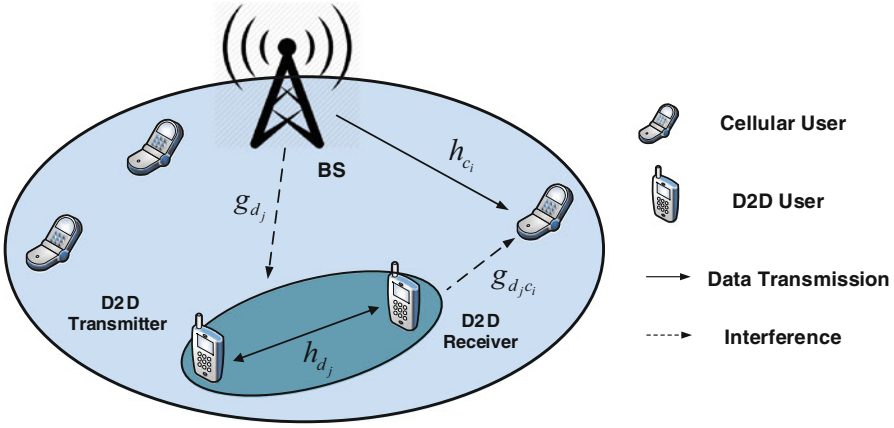


Fig. 2.8 Basic D2D communications in cellular networks

in which D2D users share the same spectrum resources with some other cellular users, and *overlay D2D communications* in which the dedicated cellular resources are allocated to the D2D links [42]. It is noted that though the spectrum efficiency and network throughput can be improved in the underlay D2D communications, the inevitable interference between D2D users and cellular users occurs during the spectrum sharing. In contrast, overlay D2D communications can effectively provide better system performance without co-channel interference at the costs of lower spectrum efficiency.

Here we consider a typical model of D2D network, as shown in Fig. 2.8. It is assumed that each cellular user is allocated equal number of RBs. In general, both the downlink (DL) resources and uplink (UL) resources can be reused in D2D communications, and here we consider the case of reusing the DL spectrum is reused. Let the channel gain between BS and a cellular user i, the channel gain between D2D transmitter and receiver, the channel gain of interference from BS to D2D pair j, and channel gain of interference of D2D pair j to cellular user i as h_{c_i}, h_{d_j}, g_{d_j} and $g_{d_j c_i}$. In D2D underlay communications, when j-th D2D pair shares RB with i-th cellular user, the Signal-to-Interference plus Noise Ratios (SINRs) at the cellular user and receiver of D2D pair can be expressed as

$$\gamma_{c_i} = \frac{P_{BS} h_{c_i}}{N_0 + P_{d_j} g_{d_j c_i}}, \tag{2.14}$$

$$\gamma_{d_j} = \frac{P_{d_j} h_{d_j}}{N_0 + P_{BS} g_{d_j}}, \tag{2.15}$$

where P_{BS} and P_{d_j} are the transmit power of BS and D2D transmitter, respectively. N_0 is variance of AWGN.

Besides, if D2D pairs work as overlay, the corresponding SINRs of cellular user and D2D pair can be given by

$$\gamma_{c_i} = \frac{P_{BS} h_{c_i}}{N_0}, \tag{2.16}$$

$$\gamma_{d_j} = \frac{P_{d_j} h_{d_j}}{N_0}. \tag{2.17}$$

2.3.2 *Applications of D2D Communications in Future 5G Networks*

Combined with the current development of wireless communication, some potential applications of 5G network in which D2D communication is considered but not limited to the following aspects.

2.3.2.1 Local Service

A typical application of local service is for social networks, which is the most basic application based on proximity service. For example, mobile users can find others who have similar interests through the D2D communications. Besides, a user can share data or play games with adjacent users.

Another basic application of local service is the local data transmission [41]. Local data transmission exploits the proximity and direct data transmission features of D2D to expand mobile communication application while saving spectrum resources, creating new revenue for operators. For example, local advertisement service based on proximity service can accurately target the users to maximize advertisement benefits. Shopping mall can send the advertisement which includes discounts and other information to make people want to buy something. Cinemas can push the movie information and schedules to nearby users. So D2D communications have potential to build a trustworthy 5G-grade D2D connectivity environment which considers both offline interactions (i.e., driven by user encounter patterns) and online interactions among mobile users (i.e., driven by social applications similar to Facebook, Twitter, and LinkedIn.) [43].

One of the most important advantages brought from local service is cellular traffic offloading [44]. The proliferation of smartphones also leads to a vast array of new wireless services, such as multimedia streaming, their massive traffic brings huge pressure on the core network. Now Cellular network is suffering from severe traffic overload [45]. The D2D-based local media service utilizes the local features of the D2D communication to offload the resource of core network and spectrum. For example, in some areas, the operator or content provider can deploy a media server which can store popular media content proactively. Mobile users who want

to watch the related video can directly download the content from the media server. Alternatively, other users can obtain the media content through their D2D partners who have owned the content, thereby alleviating the downlink transmission pressure of the operator cellular network. In addition, cellular communication between short-distance users can also be switched to the D2D communication mode to offload cellular network traffic.

2.3.2.2 Emergency Communication

The benefits brought from D2D include coverage extension, spectrum utilization improvement, higher throughput, and energy consumption reduction [46]. Thus, it is promising that proximity-based communications can be used for context-aware data collection and information diffusion in emergency situations when data has to be sent from the area where emergency happens to the central BS in both uplink and downlink through reliable and low latency links[47].

When severe natural disaster or catastrophe, e.g. earthquake happens, the infrastructure (e.g., BSs) of wireless networks will be damaged, greatly hampering the rescue efforts. This problem can be solved by using D2D communications. Even if the infrastructure is destroyed, wireless communication network can still be established between terminals through D2D connection. This means establishing an ad hoc network based on the multi-hop D2D can ensure smooth wireless communication between the terminals and provide protection for the disaster rescue. In addition, due to the terrain, buildings and other factors, blind spots always exists in wireless communication networks. With one-hop or multi-hop D2D communication, the user in the blind coverage area can be connected to user terminal in the network coverage areas, and then can be connected to the wireless communication network.

2.3.2.3 Internet of Things (IoT) Enhancement

One of the mean goals of developing mobile communication is to establish a wide range of interconnected networks containing various types of terminals, which is also one of the starting points of IoT development in the cellular communication framework. According to the forecast from industry, by 2020 there will be about 50 billion worldwide cellular access terminals, and most of them will be machine communication terminals with the IoT feature. If D2D technology and IoT can be combined, a truly interconnected wireless network will be created.

One of the typical applications of D2D-based IoT enhancement is Vehicle-to-Vehicle (V2V) communication. In particular, the possibility of exchanging information between cars will foster the appearance of many different applications. One of vital areas where such a revolution is to be expected are the enhancement of road safety[48]. When driving at high speed, the change of vehicle lane, deceleration, and other operational actions will send an early warning through D2D

communication by a vehicle. Based on the received warning, nearby vehicles alert drivers, or even autonomously control the driving to shorten the response time of the driver in emergency and hence reduce traffic accident rate. In addition, through D2D discovery technology, vehicles can reliably detect and identify specific vehicles nearby, such as potentially dangerous vehicles at intersections and those specific vehicles required special attention (such as vehicles carrying dangerous goods or school buses) and so on. Because of the communication delay and proximity discovery features of D2D based on direct terminal communication, there exist many inherent advantages for its application in vehicle network security.

In 5G network, since the number of IoT communication terminals is numerous, network access load has become a serious issue. D2D-based network access is expected to solve this problem. For example, in the scenario with a great number of terminals, low-cost terminals are not directly connected to the BS, while connecting to the adjacent terminal which has ability of processing transmission [49]. Through such terminals, the connection to the cellular network can be established. If the terminals are isolated geographically, the wireless resource used for low-cost access can be reused, which not only alleviates the access pressure of the BS, but also improves the spectrum efficiency. Moreover, compared with the current small cell structure in 4G network, this D2D-based access is more flexible and needs lower cost.

A primary aim of the IoT is to bring connectivity to every physical object[50]. For example, in intelligent home applications, an intelligent terminal can act as a special terminal. Household facilities with wireless communication capability such as home appliances access the intelligent terminal in D2D mode, and the intelligent terminal access the BS in a traditional cellular mode. The cellular-based D2D communication may bring about a real breakthrough in the development of smart home industry.

2.3.2.4 Other Applications

D2D applications in 5G networks also include multi-user MIMO (MU-MIMO) enhancement, cooperative relaying, virtual MIMO and other potential scenarios[51]. In the traditional multi-user MIMO technology, based on the respective terminal channel feedback, BSs determine the pre-coding weights to create nulls and finally eliminate the interference between multiple users. After the D2D is introduced, the paired users can exchange the CSI directly so that the terminal can feedback the combined CSI to the BS and improve the performance of the multi-user MIMO.

In addition, D2D can help solve the problems in new wireless communication scenarios. For example, indoor positioning system is an important component for developing various location based services such as indoor navigation in large complex buildings (e.g., commercial center and hospital). Meanwhile, it is challenging to design an effective solution which is able to provide high accuracy[52]. When the terminal is located indoors, satellite signals are often not available, so conventional satellite-based approaches will not work. In the D2D-based indoor positioning,

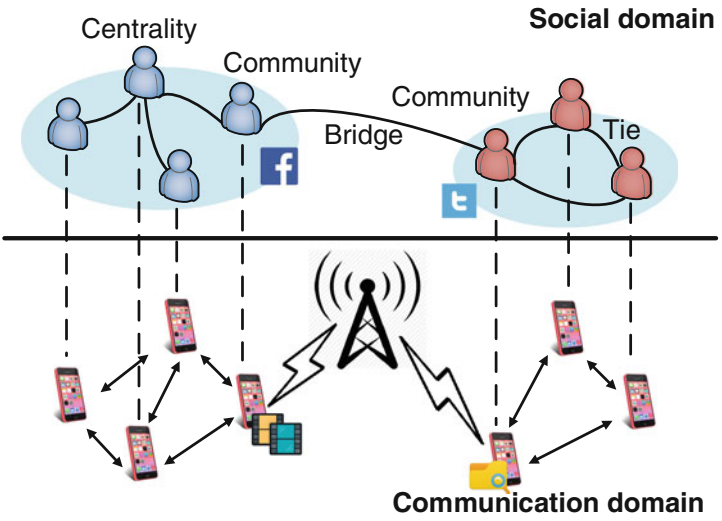


Fig. 2.9 Illustrations of social-aware D2D communications [55]

pre-deployed terminals with given location or the ordinary positioned terminal can determine the position of terminals to be positioned, which can support indoor positioning at a lower cost in 5G network.

2.3.3 Social Networks-Assisted D2D Communications

Due to the D2D link establishment among different mobile users, it is important to consider the relationship among the members of D2D communications. So the social-aware D2D communications, which leverage social networking characteristics of the cellular system, has been attracted more and more attention. Social characteristics, existing in social networks, not only define the behaviors of these entities but also depict the structure of entities that are connected to each other through some relations, where these entities exhibit homophily by sharing content items to those who have common interest and similar behaviors [53, 54].

It is obvious that the social behaviors and structures of social networks are good for designing efficient D2D communications. Based on the profound understanding of the social networks' properties, Li et al. reviewed the social characteristics in the following four categories [55], as shown in Fig. 2.9:

- **Social Ties:** The social ties are the most basic concept in a social network which represent the friend relations among the mobile users. Social ties can be built up among humans through friendship, kinship, colleague relationships, and altruistic behaviors that are observed in human activities [56]. In mobile

networks, social ties can measure how weak or strong the relationships among mobile users. Allocating more spectrum and energy resources to users with strong ties can increase the peer discovery ratio, avoid congestion, and improve spectral efficiency [57]. In some works, social tie is also called social trust or social reciprocity, by which the efficient cooperation among mobile users can be promoted [58].

The ***contact interval*** and ***contact duration*** among D2D users can be used for quantifying the social ties [59]. Contact interval $CI_{i,j}$ between user i and j is defined as the time duration for users coming into the connected range again, starting from the last time-instant t_0, when they meet with each other, and can be expressed as

$$CI_{i,j} = \min\left\{(t - t_0) : \left\|L_i(t) - L_j(t)\right\| \leq R_{i,j}, t > t_0\right\}, \tag{2.18}$$

where $L_i(t)$ and $L_j(t)$ are the geographical positions of user i and j at time t, respectively, while $R_{i,j}$ is the transmission range between i and j.

Besides, assume that nodes i and j come into the communication range at time t_c, i.e., $\left\|L_i\left(t_c^-\right) - L_j\left(t_c^-\right)\right\| \geq R_{i,j}$ and $\left\|L_i(t_c) - L_j(t_c)\right\| = R_{i,j}$, where t_c^- denotes the time before t_c. The D2D communication contact duration between users i and j is defined as the time during which they are in contact before moving out of the communication range [59], i.e.,

$$CT_{i,j} = \min_t\{(t - t_c) : \left\|L_i(t) - L_j(t)\right\| > R_{i,j}, t > t_c\}, \tag{2.19}$$

where t and t_c are in the continuous-time scale.

- **Social Community:** The social community often defines user clusters or groups which are formed by the mobile users who have similar social interests or behaviors [60]. In mobile networks, communities may represent real social groupings formed with location, interests or background, and different communities represent different groupings in which the members are usually interested in different content items. Thus, scheduling the resources among the users in a community can effectively decrease content duplication and increase the network throughput.

  The formation of a community can be regarded as the clustering process, and the *clustering probability* of a D2D user i selecting user j to form a cluster can be formulated through China Restaurant Process (CRP) [61]

$$P(i,j) = \begin{cases} \frac{f(s(i,j))}{\sum_{j \neq i} f(s(i,j)) + \alpha}, & if \quad i \neq j, \\ \frac{\alpha}{\sum_{j \neq i} f(s(i,j)) + \alpha}, & if \quad i = j, \end{cases} \tag{2.20}$$

where α is a constant parameter, $f(s(i,j))$ is the relationship function measuring user i and user j, which can be expressed as

$$f\left(s\left(i,j\right)\right)=\begin{cases}\beta\frac{1}{s_1(i,j)}+\left(1-\beta\right)\frac{1}{s_2(i,j)}, & if \quad d\left(i,j\right)\leq d_{max},\\ 0, & if \quad d\left(i,j\right)>d_{max},\end{cases} \tag{2.21}$$

where $\beta \in [0,1]$ is a weight parameter which equals to 1 if the cluster is formed by social preference and 0 if the cluster is formed by interest preference. d_{max} is the largest communication distance between two D2D users. $s_1\left(i,j\right) = -\log\left(p_1\left(i,j\right)\right)$ and $s_2\left(i,j\right) = -\log\left(p_2\left(i,j\right)\right)$ which are used for presenting the *social distance* and *interest distance*, respectively, where $p_1(i,j)$ and $p_2(i,j)$ are the social tie and interest similarity between user i and user j, respectively.

Also, the ***Community Impact Factor*** f_c is used for measuring how often the users in the community c ($c \in \mathscr{C}$, where $\mathscr{C}$ is the set of community) are contacting with each other and is calculated by averaging the contact rates (is simply defined as $1/E[CI_{i,j}]$) of all users [59],

$$f_c=\frac{1}{N_c}\sum_{i=1}^{N_c}\mu_i, \tag{2.22}$$

where node $i \in c$, and μ_i is the average contact rate of node i with other nodes in the community c, and N_c is the node number in community c.

- **Social Centrality:** The centrality in social network represents a node which has more communication links or friends within a social network, i.e., the member who plays a relatively more important role to connect other members. The mobile user in D2D communications has the ability of reducing congestion and increasing the network throughput by allocating more resources. The centrality can be measured in several ways, such as Freeman's degree, closeness, and betweenness measures [62, 63]. In [59], the social centrality of user i is defined as

$$S_i=\underset{c:i\in c,c\subseteq\mathscr{C}}{f_c}\left(1-\frac{\sum_{j\in N,j\neq i}\int_0^T\left(1-F_{CI_{i,j}}\left(x\right)\right)dx}{N-1}\right) \tag{2.23}$$

where T is the time that is taken to measure the centrality metric for the system, N is the number of mobile users and $F_{CI_{i,j}}$ is the cumulative distribution function (CDF) of $CI_{i,j}$.

- **Social Bridge:** The bridge structure indicates the connections between communities. A bridge acts as the interaction edge between two adjacent communities for information exchange. Hence, two devices forming a bridge can be allocated more resources compared to other devices.

2.3.4 Physical Layer Security in D2D Communications

In spite of the significant benefits of D2D communications, new applications also expose D2D services into some security threats. Compared with conventional connections between devices and BSs, direct connections among mobile users in D2D communications are more vulnerable to security threats with the following reasons [64]: (1) direct wireless connection between devices without supervision of BS; (2) a new relay transmission structure, for example, D2D communications enable mobile users to communicate with others who are not within the coverage of BS, so a malicious user can easily create multiple fake identities to communicate with legitimate users due to the lack of infrastructure; (3) the security issue could be more complicated due to mobility of users, BS handover and roaming in D2D communications; (4) privacy issues in social applications. If the security issues are not handled well, they may severely hinder successful deployment of D2D communications in practice.

It is more likely that maintaining data security is an essential task in D2D communications since the transmitted data among mobile users may be overheard by all of the surrounding devices [65]. This task becomes more hard to tackle particularly given the fact that the connected devices may not be able to handle complex signal processing algorithms as BSs do. One possible solution to tackle this task is *closed access* [66], in which the intended device has a list of "trusted" devices, and the devices which are not on the list can only communicate with the other devices through macro cell or micro cell. Hence, the establishment of closed access safeguards the data exchange between the intended device and the "trusted" devices against eavesdropping.

It is worth noting that closed access may not always be implemented, due to the lack of authentication in the macro cell or the micro cell. This scenario is called, in general, *open access* [66]. In open access, since authentication is absent, surrounding devices could act as potential eavesdroppers for the connected devices, or even play a role as relays without any restriction. To address security issues in open access, network designers need to construct new secure data exchange strategies that fully consider the physical characteristics of unintended or malicious devices, e.g. ambiguous location, uncertain mobility, and unknown configuration [67]. In addition, the potential attacks and threats induced by unintended devices and malicious BSs need to be carefully analyzed and incorporated into the construction.

Furthermore, some practical problems of security issues have been investigated. The basic model of physical layer security in D2D communications was investigated in [68]. And the exploitation of interference generated by D2D communications to enhance physical layer security of cellular communications was studied in [69]. [70] discussed the benefits of D2D communications for securing cellular communications, by building a weighted bipartite graph model to analyze the security impact of D2D communications. In [71], two secure capacity optimization problems for a MIMO secrecy channel with multiple D2D communications were studied and two conservative approximation approaches to convert the probability based constraints into the deterministic constraint have been addressed. Apart from

direct D2D connections, secure communications in relay-assisted D2D was also proposed [72]. In addition, considering that some mobile users have potential to be jammers to enhance the transmission security, cooperative jamming was investigated in D2D communications [73]. Since the social characteristics have been exploited as very important issues in D2D communications, some researches of social impact on physical layer security were investigated. It is feasible that trust relationship and reciprocity activities among human beings can be exploited to deal with security issues [74]. And the authors in [75] proposed a jammer selection scheme by identifying the trust level of different mobile users to enhance the physical layer security.

2.4 Chapter Summary

In this chapter, we have discussed some details about certain techniques from their basic principles to the issues in physical layer security. Specifically, TR technique, SM technique, and D2D communications were investigated. We have not only presented their basic ideas and formulations of transmit signals and received signals, but also their characteristics and applications. The issues of physical layer security has been discussed with current state of research, to establish a comprehensive insights about the relationship between the security and corresponding techniques. In the remaining chapters of this book, the technical design addressing physical layer security with TR, SM, and D2D communications will be investigated in greater detail.

References

1. M. Fink. *Time reversal mirror*, Acoustic Imaging, B.F. Jones, Ed., New York: Plenum, vol. 25, pp. 1–15, 1995.
2. Y. Chen, F. Han, Y. H. Yang, and H. Ma, "Time-reversal wireless paradigm for green Internet of things: An overview," *IEEE Internet of Things Journal,* vol. 1, no. 1, pp. 81–98, Feb. 2014.
3. L. Wang, R. Li, C. Cao, and G. L. Stüber, "SNR analysis of time reversal signaling on target and unintended receivers in distributed transmission," *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 2176–2191, May. 2016.
4. P. Blomgren, P. Kyritsi, A. D. Kim, and G. Papanicolaou, "Spatial focusing and intersymbol interference in multiple-input-single-output time reversal communication systems," *IEEE Journal of Oceanic Engineering*, vol. 33, no. 3, pp. 341–355, Jul. 2008.
5. H. T. Nguyen, I. Z. Kovacs, and P. C. F. Eggers, "A time reversal transmission approach for multiuser UWB communications," *IEEE Transactions on Antennas and Propagation*, vol. 54, no. 11, pp. 3216–3224, Nov. 2006.
6. T. Wang and T. Lv, "Canceling interferences for high data rate time reversal mimo UWB system: A precoding approach," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, pp. 1–10, Dec. 2011.
7. W. A. Kuperman, W. S. Hodgkiss, H. C. Song, T. Akal, C. Ferla, and D. R. Jackson, "Phase conjugation in the ocean: Experimental demonstration of an acoustic time-reversal mirror," *The Journal of the Acoustical Society of America,* vol. 103, no. 1, pp. 25–40, Aug. 1998.

8. H. C. Song, W. A. Kuperman, W. S. Hodgkiss, T. Akal, and C. Ferla, "Iterative time reversal in the ocean," *The Journal of the Acoustical Society of America,* vol. 105, no. 6, pp. 3176–3184, Aug. 1999.
9. G. F. Edelmann, T. Akal, W. S. Hodgkiss, S. Kim, W. A. Kuperman, and H. Song, "An initial demonstration of underwater acoustic communication using time reversal," *IEEE Journal of Oceanic Engineering,* vol. 27, no. 3, pp. 602–609, Jul. 2002.
10. Y. Jin, J. M. Moura, and N. O'Donoughue, "Time reversal in multiple-input-multiple-output radar," *IEEE Journal of Selected Topics in Signal Processing,* vol. 4, no. 1, pp. 210–225, Feb. 2010.
11. C. J. Leuschen and R. G. Plumb, "A matched filter based reverse-time migration algorithm for ground-penetrating radar data," *IEEE Transactions on Geoscience and Remote Sensing,* vol. 39, no. 5, pp 929–936, May. 2001.
12. L. Borcea, G. Papanicolaou, C. Tsogka, and J. Berryman, "Imaging and time-reversal in random media," *Inverse Problems,* vol. 18, pp. 1247–1279, Oct. 2002.
13. D. Cassioli, M. Win, and A. Molisch, "The ultra-wide bandwidth indoor channel: From statistical model to simulations", *IEEE Journal on Selected Areas in Communications,* vol. 20, no. 6, pp. 1247–1257, Nov. 2002.
14. R. C. Qiu, C. Zhou, N. Guo, and J. Q. Zhang, "Time reversal with MISO for ultrawideband communications: Experimental results," *IEEE Antennas and Wireless Propagation Letters,* vol. 5, no. 1, pp. 269–273, Dec. 2006.
15. D. Li, J. S. Hong, and B. Wang, "Improving anti-detection/interception performance for wireless sensor network based on time-reversal technology," in *Proc. 2009 5th International Conference Wireless Communications Network Mobile Computing (WiCOM),* Beijing, China, Sept. 2009, pp. 1–4.
16. K. A. Toshiaki, A. F. Molisch, C. Duan, Z. Tao, and P. Orlik, "Capacity, MSE and secrecy analysis of linear block precoding for distributed antenna systems in multi-user frequency-selective fading channels," *IEEE Transactions on Communications,* vol. 59, no. 3, pp. 888–900, Jan. 2011.
17. D. T. Phan-Huy, T. Sarrebourse, A. Gati, J. Wiart, and M. Helard, "Characterization of the confidentiality of a green time reversal communication system: Experimental measurement of the spy BER sink," in *Proc. 2013 IEEE Wireless Communications Network Conference (WCNC),* Shanghai, China, Apr. 2013, pp. 4783–4788.
18. W. Cao, J. Lei, W. Liu, and X. Li, "Secure performance of time reversal precoding technique in MISO OFDM systems," in *Proc. 2014 Communications Security Conference (CSC)*, Beijing, China, May. 2014, pp. 1–5.
19. V. T. Tan, D.-B. Ha, and D.-D. Tran, "Evaluation of physical layer security in mimo ultra-wideband system using time-reversal technique," in *Proc. 2014 2th IEEE International Conference on Computing, Managements and Telecommunications (ComManTel),* Da Nang, Vietnam, Apr. 2014, pp. 70–74.
20. J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space shift keying modulation for MIMO channels," *IEEE Transactions on Wireless Communications,* vol. 8, no. 7, pp. 3692–3703, Jul. 2009.
21. Y. Chau and S.-H. Yu, "Space modulation on wireless fading channels," in *Proc. 2001 IEEE Vehicular Technology Conference (VTC Fall),*vol. 3, Atlantic City, NJ, USA, Oct. 2001, pp. 1668–1671.
22. R. Mesleh, H. Haas, C. W. Ahn, and S. Yun, "Spatial modulation — A new low complexity spectral efficiency enhancing technique," in *Proc. 2006 1st International Conference on Communications and Networking in China (CHINACOM)*, Beijing, China, Oct. 2006, pp. 1–5.
23. R. Mesleh, H. Haas, S. Sinanović, C. W. Ahn, S. Yun, "Spatial modulation," *IEEE Transactions on Vehicular Technology,* vol. 57, no. 4, pp. 2228–2241, Jul. 2008.
24. M. D. Renzo, H. Haas, and P. M. Grant, "Spatial modulation for multiple-antenna wireless systems: A survey," *IEEE Communications Magazine,* vol. 49, no. 12, pp. 182–191, Dec. 2011.
25. J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Generalized space shift keying modulation for MIMO channels," in *Proc. 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, Cannes, France, Sept. 2008, pp. 1–5.

26. L. L. Yang, "Transmitter preprocessing aided spatial modulation for multiple-input multiple-output systems," in *Proc. 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, Budapest, Hungary, May. 2011, pp. 1–5.
27. F. Wu, C. Dong, L. L. Yang, and W. Wang, "Secure wireless transmission based on precoding-aided spatial modulation," in *Proc. 2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.
28. R. Zhang, L. L. Yang, and L. Hanzo, "Error probability and capacity analysis of generalised pre-coding aided spatial modulation," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 364–375, Jan. 2015.
29. F. Wu, R. Zhang, L. L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 467–471, Jan. 2016.
30. R. Zhang, L. L. Yang, and L. Hanzo, "Generalised pre-coding aided spatial modulation," *IEEE Transactions on Wireless Communications*, vol. 12, no. 11, pp. 5434–5443, Nov. 2013.
31. S. Sinanovic, M. Di Renzo, and H. Haas, "Secrecy rate of time switched transmit diversity system," in *Proc. 2011 IEEE Vehicular Technology Conference (VTC Spring),* Budapest, Hungary, May. 2011, pp. 1–5.
32. X. Guan, Y. Cai, and W. Yang, "On the secrecy mutual information of spatial modulation with finite alphabet," in *Proc. 2012 IEEE International Conference on Wireless Communications and Signal Processing (WCSP),* Huangshan, China, Oct. 2012, pp. 1–4.
33. F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Transactions on Vehicular Technology,* vol. 65, no. 1, pp. 467–471, Jan. 2016.
34. F. Wu, L.-L. Yang, W. Wang, and R. Zhang, "Secret precoding-aided spatial modulation," *IEEE Communications Letters,* vol. 19, no. 9, pp. 1544–1547, Sept. 2015.
35. S. Aghdam and T. Duman, "Physical layer security for space shift keying transmission with precoding," *IEEE Wireless Communications Letters,* vol. 5, no. 2, pp. 180–183, Jan. 2016.
36. K. Doppler, M. Rinne, C. Wijting, B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Communications Magazine,* vol. 47, no. 12, pp. 42–49, Dec. 2009.
37. 3GPP, Study on LTE direct, 3GPP S1–112017, Aug. 2011.
38. 3GPP, Study on Proximity-based services, 3GPP SP-110590, Sept. 2011.
39. L. Wang and H. Tang, *Device-to-device communications in cellular networks*, Springer, pp. 1–90, 2016.
40. A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Communications Surveys and Tutorials,* vol. 16, no. 4, pp. 1801–1819, Apr. 2014.
41. S. Mumtaz, K. M. S. Huq, and J. Rodriguez, "Direct mobile-to-mobile communication: Paradigm for 5G," *IEEE Wireless Communications,* vol. 21, no. 5, pp. 14–23, Oct. 2014.
42. L. Lei, Y. Kuang, X. Shen, C. Lin, and Z. Zhong, "Resource control in network assisted device-to-device communications: Solutions and challenges," *IEEE Communications Magazine,* vol. 52, no. 6, pp. 108–117, Jun. 2014.
43. A. Ometov, A. Orsino, L. Militano, D. Moltchanov, G. Araniti, and E. Olshannikova, "Toward trusted, social-aware D2D connectivity: Bridging across the technology and sociality realms," *IEEE Wireless Communications*, vol. 23, no. 4, pp. 103–111, Aug. 2016.
44. http://wwwen.zte.com.cn/endata/magazine/ztetechnologies/2015/no3/articles/201505/t20150506$_$433771.html
45. B. Han, P. Hui, V. S. A. Kumar, M. V. Marathe, J. Shao, and A. Srinivasan, "Mobile data offloading through opportunistic communications and social participation," *IEEE Transactions on Mobile Computing*, vol. 11, no. 5, pp. 821–834, May. 2012.
46. L. Lei, Z. Zhong, C. Lin, and X. Shen, "Operator controlled device-to-device communications in LTE-advanced networks," *IEEE Wireless Communications*, vol. 19, no. 3, pp. 96–104, Jun. 2012.

47. A. Orsino, L. Militano, G. Araniti, and A. Iera, "Social-aware content delivery with D2D communications support for emergency scenarios in 5G systems," in *Proc. 2016 22th European Wireless European Wireless Conference*, Oulu, Finland, Jun. 2016, pp. 1–6.
48. S. K. Noh, P. j. Kim, and J. H. Yoon, "Doppler effect on V2I path loss and V2V channel models," in *Proc. 2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, South Korea, Oct. 2016, pp. 898–902.
49. W. Zhang, K. Zheng, S. Sherman, *5G Mobile Communications*, Springer, 2016.
50. M. Elkhodr, S. Shahrestani, and H. Cheung, "A smart home application based on the Internet of Things management platform," in *Proc. 2015 IEEE International Conference on Data Science and Data Intensive Systems*, Sydney, NSW, Australia, Dec. 2015, pp. 491–496.
51. A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, no.1 , pp. 1206–1232, Jul. 2015.
52. T. D. Huynh, C. S. Chen, and S. W. Ho, "Localization method for device-to-device through user movement," in *Proc. 2015 IEEE International Conference on Communication Workshops (ICC workshops)*, London, UK, Jun. 2015, pp. 821–826.
53. A. Anderson, H. D. Uttenlocher, J. Kleinberg, and J. Leskovec, "Effects of user similarity in social media," in *Proc. 5th ACM International Conference on Web Search and Data Mining,* Seattle, USA, Feb. 2012, pp. 703–712.
54. C. R. Shalizi and A. C. Thomas, "Homophily and contagion are generically confounded in observational social network studies," *Sociological Methods and Research,* vol. 40, no. 2, pp. 211–239, May. 2011.
55. Y. Li, T. Wu, P. Hui, D. Jin, and S. Chen, "Social-aware D2D communications: Qualitative insights and quantitative analysis," *IEEE Communications Magazine,* vol. 52, no. 6, pp. 150–158, Jun. 2014.
56. S. Aral and D. Walker, "Identifying influential and susceptible members of social networks," *Science,* vol. 337, no. 6092, pp. 337–341, Jul. 2012.
57. N. Panwar, S. Shantanu, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Physical Communication,* vol. 18, no. 1, pp. 64–84, Mar. 2016.
58. X. Chen, B. Proulx, X. Gong, and J. Zhang, "Exploiting social ties for cooperative D2D communications: A mobile social networking case," *IEEE/ACM Transactions on Networking*, vol. 23, no. 5, pp. 1471–1484, Oct. 2015.
59. B. Zhang, Y. Li, D. Jin, P. Hui, and Z. Han, "Social-aware peer discovery for D2D communications underlaying cellular networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2426–2439, May. 2015.
60. C. Cao, L. Wang, M. Song, and Y. Zhang, "Admission policy based clustering scheme for D2D underlay communications," in *Proc. 2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, Washington, DC, USA, Sept. 2014, pp. 1937–1942.
61. Z. Wu, L. Wang, G. Araniti, and Z. Han, "Exploiting social-interest interactions on user clustering and content dissemination in device-to-device communications," in *Proc. 2015 IEEE/CIC International Conference on Communications in China (ICCC)*, Shenzhen, China, Nov. 2015, pp. 1–6.
62. R. M. Bond, C. J. Fariss, J. J. Jones, A. D. I. Kramer, C. Marlow and E. J. Settle, "A 61-million-person experiment in social influence and political mobilization," *Nature,* vol. 489, no. 7415, pp. 295–298, Sept. 2012.
63. N. Kayastha, D. Niyato, P. Wang, and E. Hossain, "Applications, architectures, and protocol design issues for mobile social networks: A survey," *Proceedings of the IEEE,* vol. 99, no. 12, pp. 2130–2158, Dec. 2011.
64. M. Wang, and Y. Zheng, "A survey on security in D2D communications," *Mobile Networks and Applications,* vol. 2016, no. 5, pp. 1–14, May. 2016.
65. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine,* vol. 53, no. 4, pp. 20–27, Apr. 2015.

66. M. Tehrani, M. Uysal, and H. Yanikomeroglu, “Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions,” *IEEE Communications Magazine,* vol. 52, no. 5, pp. 86–92, May. 2014.
67. N. Mahda and R. Nordin. “A Survey on interference management for device-to-device (D2D) communication and its challenges in 5G Networks,” *Journal of Network and Computer Applications (2016)*, vol. 2016, no. 71, pp. 130–150, Apr. 2016.
68. D. Zhu, A. L. Swindlehurst, S. A. A. Fakoorian, W. Xu, and C. Zhao, “Device-to-device communications: The physical layer security advantage,” in *Proc. 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, Italy, May. 2014, pp. 1606–1610.
69. C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, “Interference exploitation in D2D-enabled cellular networks: A secrecy perspective,” *IEEE Transactions on Communications,* vol. 63, no. 1, pp. 229–242, Jan. 2015.
70. H. Zhang, T. Wang, L. Song, and Z. Han, “Radio resource allocation for physical-layer security in D2D underlay communications,” in *Proc. 2014 IEEE International Conference on Communications (ICC),* Sydney, NSW, Australia, Jun. 2014, pp. 2319–2324.
71. Z. Chu, K. Cumanan, M. Xu, and Z. Ding, “Robust secrecy rate optimisations for multiuser multiple-input-single-output channel with device-to-device communications,” *The Institution of Engineering and Technology Communications,* vol. 9, no. 3, pp. 396–403, Feb. 2015.
72. S. A. M. Ghanem and M. Ara, “Secure communications with D2D cooperation,” in *Proc. 2015 IEEE International Conference on Communications, Signal Processing, and their Applications (ICCSPA),* Sharjah, Feb. 2015, pp. 1–6.
73. L. Wang and H. Wu, “Jamming partner selection for maximising the worst D2D secrecy rate based on social trust,” *IEEE Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 2, Feb. 2017.
74. Z. Yan and M. Wang, “Protect pervasive social networking based on two-dimensional trust levels,” *IEEE Systems Journal*, vol. 11, no. 1, pp. 207–218, Mar. 2017.
75. L. Wang, H. Wu, and G. Stuber. “Resource allocation with cooperative jamming in socially interactive secure D2D underlay,” in *Proc. 2016 IEEE 83rd. Vehicular Technology Conference (VTC Spring),* Nanjing, China, May. 2016, pp. 1–5.

Chapter 3
Secrecy Analysis with Time-Reversal Technique in Distributed Transmission System

In wireless communications, signal leakage to unintended receivers may cause severe security risk and co-channel interference. Multiple-antenna cooperation techniques have been exploited and attracted increasing interest because of their good ability to handle the security problem. Among the corresponding techniques, time reversal (TR) transmission is identified as a promising wireless technology for wide-band multi-path channels because it can focus energy spatially and temporally by exploiting multi-path propagation [1–3]. The signal focusing property of TR can also be exploited to reduce signal leakage to unintended users, typically at unknown locations [4–6]. This chapter analyzes the effect of distributed time-reversal (DTR) transmission scheme on the SNR at its intended and unintended receivers. By focusing the temporal and spatial signal energy on the intended receiver, DTR can effectively maintain a satisfactory SNR level while lowering received signal level at eavesdroppers or unintended co-channel users. The DTR performance is analyzed in terms of secrecy rate and SNR gap between the desired and unintended receivers. The SNR gain of DTR is also analyzed over traditional distributed direct transmission and several distributed beamforming transmission schemes.

3.1 System Model

A cooperative distributed antenna network is shown in Fig. 3.1, where a source communicates with a distant intended receiver through the distributed transmit antennas. An unintended receiver is present which is close to the target destination. We consider Ultra High Frequency (UHF) signaling (above 900 MHz), such that the carrier wavelength is very small. For such operating frequencies, in a rich scattering and multi-path channel environment, the coherence distance [7] is in the

L. Wang, *Physical Layer Security in Wireless Cooperative Networks*, Wireless Networks, DOI 10.1007/978-3-319-61863-0_3

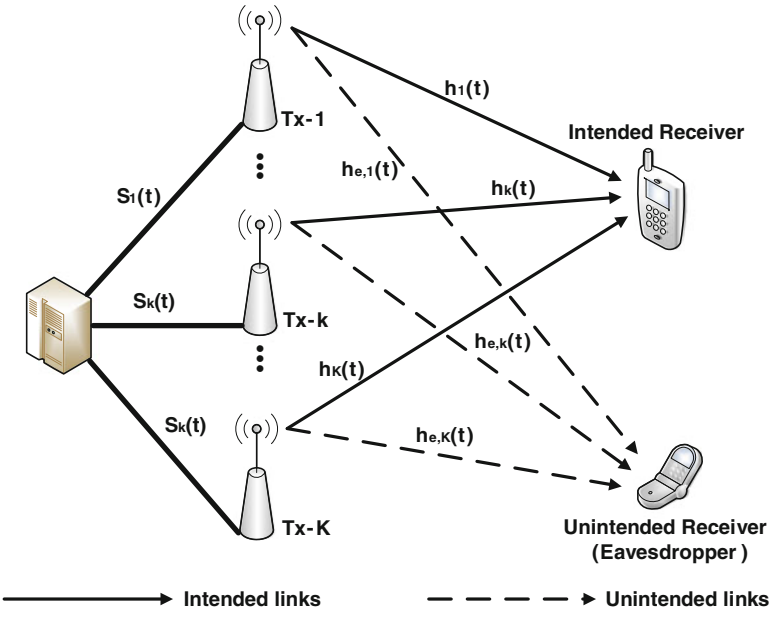


Fig. 3.1 System model with distributed transmission antennas

order of centimeters such that the channels between the distributed antennas and the destination are substantially uncorrelated and different from the channels between the distributed antennas and the unintended receiver.

The system model is characterized by links between the source-to-destination node and source-to-unintended node. The corresponding notations are shown in Table 3.1. For the number of multi-path delay, two separate cases are considered: firstly, L_k is assumed as a constant in our basic analysis; secondly, the collection $\{L_k\}$ is modeled as a set of independent random variables, each of them follows identical uniform distribution, where $\text{Prob}(L_k = \ell) = L^{-1}, \quad \ell = 0, 1, \ , \cdots, \ L-1$. i denotes the i-th path ($i = 0, \ldots, L_k$), and $L_k + 1$ is the number of channel paths for the k-th transmit antenna. The index set of transmit antennas is denoted by $\mathscr{K} = \{1, \cdots, K\}$. On the other hand, for the channel, we have following assumptions:

- The multi-path channel gains are assumed to be independent and identically distributed (i.i.d.) with Rayleigh fading, each with zero mean, i.e., $h_{ki} \sim \mathscr{CN}(0, {\sigma_B}^2)$, $h_{e,ki} \sim \mathscr{CN}(0, {\sigma_E}^2)$;
- Based on the assumption of a uniform power-delay profile, we assume that $\text{E}\{|h_{ki}|^2\} = \sigma_B^2$, $\text{E}\{|h_{ki}|^4\} = 2\sigma_B^4$, $\text{E}\{h_{ki}\} = \text{E}\{h_{ki}^2\} = 0$. Similarly, $\text{E}\{|h_{e,ki}|^2\} = \sigma_E^2$, $\text{E}\{|h_{e,ki}|^4\} = 2\sigma_E^4$, $\text{E}\{h_{e,ki}\} = \text{E}\{h_{e,ki}^2\} = 0$;
- Without loss of generality, let $E_p = \int_{-\infty}^{\infty} |p(t)|^2 dt = 1$;
- $\sigma_E = \sigma_B$.

Table 3.1 Notation summary

a_m	QAM source data symbol in constellation $\mathscr{Q}$
T	QAM symbol duration
$\rho_k(t)$	Normalized pulse for QAM symbol at antenna k
b_k	k-th antenna power scalar with $\sum_{k=1}^{K} \mathrm{E}\{b_k^2\} = 1$
$h_{ki}, h_{e,ki}$	i-th multi-path gain from transmit antenna k to destination and unintended receiver, respectively
$\tau_{ki}, \tau_{e,ki}$	i-th multi-path delay from transmit antenna k to destination and unintended receiver, respectively
T_p	Maximum multi-path delay
T_e, T_{e0}, T_{e1}	Sampling time at unintended receiver
$L_k + 1$	Number of multi-paths for transmit antenna k
$p(t)$	Root raised-cosine receiver filter impulse response
σ_B^2, σ_E^2	Variance of i.i.d. delay gains h_{ki} and $h_{e,ki}$, respectively
P_s	Transmit power of distributed antennas
K	Number of distributed antennas
C_M^m	Combinatorial choosing of m objects from M possibilities

Definition 1 The multi-path delay profile is modeled as exponential over the interval $(0, T_p)$. Specifically, τ_{ki} and $\tau_{e,ki}$ are assumed to independently follow the truncated exponential density function

$$p_{\tau_{e,ki}}(\tau) = p_{\tau_{ki}}(\tau) = \frac{e^{-\tau/T_0}}{T_0(1 - e^{-T_p/T_0})}[u(\tau) - u(\tau - T_p)]. \tag{3.1}$$

Note that for uniform power-delay profiles, $T_0 \to \infty$ such that τ_{ki} and $\tau_{e,ki}$ are uniform between $(0,\ T_p)$.

The target receiver is synchronized to the incoming signal, whereas the eavesdropper may be not. Without loss of generality, the target receiver samples the received signal at time T_p, which is the peak sampling time, whereas the unintended receivers sample their received signals at T_e. To give the unintended nodes the benefit of the doubt, the effect of synchronized sampling $T_e = T_p$ will be considered when comparing the received signal qualities later in the chapter.

3.1.1 Distributed Time Reversal Transmission

The DTR-based transmission is assumed to use time division duplexing (TDD). In TDD system, channel reciprocity is often assumed for wireless channels of sufficient coherence time. For large enough channel coherence time, channel reciprocity allows each node to assume its transmission channel and reception channel to be the same.

We have analyzed transmitted signal and channel impulse responses in Chap. 2 (see Eqs. (2.1)–(2.6)). Recall that

$$\rho_k(t) = \frac{\widetilde{h}_k^*(T_p - t)}{\sqrt{E\left\{\int_{-\infty}^{\infty} \left|\widetilde{h}_k(t)\right|^2 dt\right\}}} = \frac{\widetilde{h}_k^*(T_p - t)}{\sqrt{E_k}}, \tag{3.2}$$

$$h_k(t) = \sum_{i=0}^{L_k} h_{ki}\delta(t - \tau_{ki}), \tag{3.3}$$

$$\widetilde{h}_k(t) = h_k(t) \otimes p(t) = \sum_{i=0}^{L_k} h_{ki} p(t - \tau_{ki}), \tag{3.4}$$

$$s_k(t) = b_k \sum_{m=-\infty}^{\infty} a_m \rho_k(t - mT), \tag{3.5}$$

where $\rho_k(t)$ is the normalized TR waveform, $h_k(t)$ is channel impulse response, $\widetilde{h}_k(t)$ is the equivalent channel response (see more details in Eq. (2.3)), $\widetilde{h}_k^*(T_p - t)$ is the time-reversed and conjugated channel response and $s_k(t)$ is the transmitted signal (see more details in Eq. (2.6)).

We assume that the k-th average transmission power is $P_k = \frac{1}{T}\int_{-\infty}^{\infty} \mathrm{E}\{|s_k(t)|^2\} dt = \mathrm{E}\{|b_k|^2\} P_s \int_{-\infty}^{\infty} |\rho_k(t)|^2 dt = \mathrm{E}\{|b_k|^2\} P_s$. For simplicity, the waveform $\rho_k(t)$ is normalized to have unit energy $\int_{-\infty}^{\infty} |\rho_k(t)|^2 dt = 1$.

Note that in order to avoid a circular problem of having to define the receiver filter $p(t)$ to design time-reversal transmit impulse shape, the optimum receiver filter at both intended and unintended receivers is chosen to be a simple root-raised cosine (RRC) filter [11, 12], and the transfer function of receiver filter impulse $p(t)$ can be expressed as

$$|P(f)|^2 = \begin{cases} T, & |fT| \le \frac{1}{2}(1-\beta). \\ \frac{T}{2}\left\{1 - \sin\left[\frac{\pi}{\beta}\left(|fT| - \frac{1}{2}\right)\right]\right\}, & \frac{1}{2}(1-\beta) \le |fT| \le \frac{1}{2}(1+\beta). \\ 0, & |fT| \ge \frac{1}{2}(1+\beta). \end{cases} \tag{3.6}$$

where β is the roll-off factor. Using RRC filter offers several distinct advantages as follows [6]:

- it is not channel dependent;
- it can be optimum when there is no multi-path distortion;
- it can keep the T-spaced output noise samples white.

Similar to Eq. (3.4), the equivalent channel impulse response from the k-th transmit antenna to the unintended receiver is denoted as $\widetilde{h}_{e,k}(t)$, and by involving the receiver filter response $p(t)$ as part of the channel responses as seen at the transmitter, the multi-path propagation channel of transmitter to unintended receiver can be described as

$$\widetilde{h}_{e,k}(t) = \sum_{i=0}^{L_k} h_{e,ki} p(t - \tau_{e,ki}), \tag{3.7}$$

where $\tau_{e,ki}$ is the i-th path delay from k-th antenna to the unintended receiver. Note that $E_p = 1$ and thus the average energy of $h_k(t)$ is

$$E_k = \mathrm{E}\left\{\int_{-\infty}^{\infty} |\widetilde{h}_k(t)|^2 dt\right\} = \sum_{i=0}^{L_k} \sigma_B^2 \int_{-\infty}^{\infty} |p(t-\tau_{k,i})|^2 dt$$
$$= (L_k+1)\sigma_B^2 E_p = (L_k+1)\sigma_B^2. \tag{3.8}$$

According to Eq. (3.5), by using TR, antenna k now transmits a new signal that is of the form

$$s_k^{DTR}(t) = b_k \sum_{m=-\infty}^{\infty} \frac{a_m}{\sqrt{E_k}} \widetilde{h}_k^*(T_p - t + mT). \tag{3.9}$$

Recall that $P_s = \mathrm{E}\{|a_m|^2\}$. The normalization makes it simpler to control power distribution by adjusting b_k. Given K antennas, $b_k = 1/\sqrt{K}$ allows equal gain transmission (EGT) in DTR by exploiting only local CSI [9].

The delay T_p must be large enough to account for the maximum multi-path delay spread among all transmit antennas. Before sampling, the signals at the RRC receiver filter output from the k-th antenna at the destination and unintended receivers are, respectively,

$$d_k(t) = s_k^{DTR}(t) \otimes \widetilde{h}_k(t) + n_k(t), \tag{3.10}$$

$$e_k(t) = s_k^{DTR}(t) \otimes \widetilde{h}_{e,k}(t) + n_{e,k}(t). \tag{3.11}$$

where $n_k(t)$ and $n_{e,k}(t)$ are additive white Gaussian random processes of k-th path with power spectral densities σ_n^2 and σ_e^2, respectively.

For convenience, the received pulse at the destination is defined as

$$q_k(t) = \widetilde{h}_k^*(T_p - t) \otimes \widetilde{h}_k(t)/E_k^{1/2}$$
$$= \sum_{i=0}^{L_k}\sum_{\ell=0}^{L_k} \frac{h_{ki}h_{k\ell}^*}{\sqrt{E_k}} \int_{-\infty}^{\infty} p(v-\tau_{ki})p^*(T_p - t + v - \tau_{k\ell})dv. \tag{3.12}$$

Moreover, at the unintended receiver define the received pulse $q_{e,k}(t)$ as

$$q_{e,k}(t) = \widetilde{h}_k^*(T_p - t) \otimes \widetilde{h}_{e,k}(t)/E_k^{1/2} \tag{3.13}$$
$$= \sum_{i=0}^{L_k}\sum_{\ell=0}^{L_k} \frac{h_{e,ki}h_{k\ell}^*}{\sqrt{E_k}} \int_{-\infty}^{\infty} p(v-\tau_{e,ki})p^*(T_p - t + v - \tau_{k\ell})dv.$$

Now that the received signal pulse-shaping from time-reversal transmission has been specified, and the two received signals from a given transmit antenna can be rewritten as

$$d_k(t) = b_k \sum_{m=-\infty}^{\infty} a_m q_k(t - mT) + n_k(t), \tag{3.14a}$$

$$e_k(t) = b_k \sum_{m=-\infty}^{\infty} a_m q_{e,k}(t - mT) + n_{e,k}(t). \tag{3.14b}$$

It is important to note that the equivalent receiver filter output pulse for TR transmission at the destination has a maximum-power peak at time $t = T_p$, and

$$q_k(T_p) = \frac{1}{\sqrt{E_k}} \int_{-\infty}^{\infty} \left| \sum_{i=0}^{L_k} h_{ki} p(v - \tau_{ki}) \right|^2 dv. \tag{3.15}$$

This peak sampling property does not hold, however, for the unintended receiver node.

Since all K antennas perform the same functionality and transmit the same symbol a_m, the received signals at the two receivers are, respectively,

$$d(t) = \sum_{k=1}^{K} d_k(t) = \sum_m a_m \sum_{k=1}^{K} b_k q_k(t - mT) + n(t), \tag{3.16a}$$

$$e(t) = \sum_{k=1}^{K} e_k(t) = \sum_m a_m \sum_{k=1}^{K} b_k q_{e,k}(t - mT) + n_e(t). \tag{3.16b}$$

Recall that for the destination receiver, the peak SNR sampling instants are at $t_\ell = \ell T + T_p$. Since $p(t)$ is chosen as the well known RRC filter response, the T-spaced noise samples $n(\ell T + T_p)$ and $n_e(\ell T + T_e)$ taken at time intervals of ℓT are independent Gaussian random variables [7, 8].

Unlike traditional secrecy analysis that focuses on discrete channel models, our model is the practical analog signal model. To investigate the secrecy effect, idealistic receivers are assumed at both the destination and unintended receiver when determining the secrecy rate. In particular, it is assumed that

- both destination and unintended receiver have CSI from each distributed antenna to their respective receivers.
- both have a RRC front-end filter whose output is periodically sampled.
- both are capable of designing **an ideal and perfect receiver** to remove all ISI from their sampled RRC filter output signals.

3.1.2 Direct Transmission and Distributed Beamforming Transmission

3.1.2.1 Direct Transmission (DT)

In naïve direct transmission, each antenna sends the same pulse $\rho_k(t) = p^*(T_p - t)$ matched to the receiver RRC filter. Note that the pulse has energy $E_p = 1$. Recall that the received signals at the destination and unintended receivers from the k-th transmit antenna are, respectively,

$$d_k(t) = b_k \sum_{m=-\infty}^{\infty} a_m \rho_k(t - mT) \otimes \widetilde{h}_k(t) + n_k(t), \tag{3.17a}$$

$$e_k(t) = b_k \sum_{m=-\infty}^{\infty} a_m \rho_k(t - mT) \otimes \widetilde{h}_{e,k}(t) + n_{e,k}(t). \tag{3.17b}$$

Let us define the two combined responses

$$\bar{z}_k(t) = \widetilde{h}_k(t) \otimes p^*(T_p - t), \tag{3.18a}$$

$$\bar{z}_{e,k}(t) = \widetilde{h}_{e,k}(t) \otimes p^*(T_p - t). \tag{3.18b}$$

Thus, the signals received at the destination and the unintended receiver can be expressed, respectively, as

$$d(t) = \sum_{k=1}^{K} d_k(t) = \sum_m a_m \sum_{k=1}^{K} b_k \bar{z}_k(t - mT) + n(t), \tag{3.19}$$

$$e(t) = \sum_{k=1}^{K} e_k(t) = \sum_m a_m \sum_{k=1}^{K} b_k \bar{z}_{e,k}(t - mT) + n_e(t)\ . \tag{3.20}$$

The peak SNR sampling times for the destination and the unintended receiver are $t_\ell = T_p + \ell T$ and $T_{e0} + \ell T$, respectively. At the points of sampling and detection,

$$\bar{z}_k(T_p) = \sum_{i=0}^{L_k} h_{ki} \int_{-\infty}^{\infty} p(v - \tau_{ki}) p^*(v) dv = \sum_{i=0}^{L_k} h_{ki} R_p(\tau_{ki}), \tag{3.21a}$$

$$\begin{aligned} \bar{z}_{e,k}(T_{e0}) &= \sum_{i=0}^{L_k} h_{e,ki} \int_{-\infty}^{\infty} p(v - \tau_{e,ki}) p^*(T_p - T_{e0} + v) dv \\ &= \sum_{i=0}^{L_k} h_{e,ki} R_p(T_p - T_{e0} + \tau_{e,ki})\ . \end{aligned} \tag{3.21b}$$

3.1.2.2 Distributed Beamforming (DBF)

Cooperative beamforming is a widely used method to enhance the security of communications, where transmit antennas utilize distributed beamforming to concentrate the signal towards the intended destination and mitigate the information leakage to an unintended receiver.

DBF usually considers only a single path between a transmit antenna and the destination, while in practice the signals transmitted by the transmit antennas propagate through multi-path channels and the received signals at the unintended receiver(s) may not fully achieve coherent combining. Therefore, the achievable SNR for distributed beamforming will be analyzed considering both the one-path channel model and a practical multi-path channel model.

With distributed beamforming, the k-th transmit antenna uses the (normalized) pulse

$$\rho_k(t) = p^*(T_p - \tau_{ki_0} - t),$$

where

$$i_0 = \begin{cases} \arg \max\limits_{0 \le i \le L_k} |h_{ki}^*|, & \text{MGP}, \\ 0, & \text{Direct LoS}. \end{cases}$$

For maximum ratio transmission (MRT) [19], each antenna adopts a different gain $b_k = h_{ki_0}^*/\zeta$, thereby transmitting $b_k p^*(T_p - \tau_{ki_0} - t)$. Since h_{ki} is a random variable, $\arg\max_i |h_{ki}^*|$ is a special kind of random variable that requires order statistics [20]. Here ζ is used to normalize $\sum_1^K E\{|b_k|^2\} = 1$ for fairness.

In distributed beamforming, two different types of beamforming are considered for comparison:

- **LoS-DBF:** with line of sight beamforming, each transmit antenna sends a pulse $h_{k0}^* p^*(T_p - \tau_{k0} - t)/(\sigma_B\sqrt{K})$ that is matched to the first LoS delay only.
- **MGP-DBF:** with maximum gain path distributed beamforming, at each transmit antenna the strongest multi-path component is selected for distributed beamforming. Similar to LoS-DBF, each antenna sends a pulse $h_{ki_0}^* p^*(T_p - \tau_{ki_0} - t)/\zeta$ that is matched to the strongest delay path i_0 only.

  Order statistics can be used to determine the b_k. For $X_1, X_2, \ldots, X_n$ i.i.d. continuous random variables with probability density function (PDF) $f(x)$ and cumulative distribution function (CDF) $F(x)$, the PDF of the maximum is $f_{(n)}(x) = nf(x)F(x)^{n-1}$ [20]. Recall that $x_k = |h_{ki}^*|^2$ is a random variable following the exponential distribution [7]. Therefore, denoting $i_0 = \arg\max\limits_i |h_{ki}|$, yields

$$f_{|h_{ki_0}^*|^2}(x) = (L_k + 1)\frac{1}{\sigma_B^2}\exp\left(-\frac{x}{\sigma_B^2}\right)\left(1 - \exp\left(\frac{-x}{\sigma_B^2}\right)\right)^{L_k}, \quad x \ge 0, \qquad (3.22a)$$

$$\begin{aligned}\mathrm{E}(|b_k|^2) &= \frac{1}{\zeta^2}\int_0^\infty x f_{(n)}(x)dx \\ &= \frac{\sigma_B^2}{\zeta^2}(L_k+1)\sum_{i=0}^{L_k} C_{L_k}^i(-1)^i\int_0^\infty t\exp[-(i+1)t]dt \\ &= \frac{\sigma_B^2}{\zeta^2}(L_k+1)\sum_{i=0}^{L_k} C_{L_k}^i(-1)^i(i+1)^{-2} \\ &= \sigma_B^2\zeta^{-2}G_0,\end{aligned} \tag{3.22b}$$

where $G_0(L_k) = (L_k+1)\sum_{i=0}^{L_k} C_{L_k}^i(-1)^i(i+1)^{-2}$. Therefore, in MGP-DBF the normalization factor $\zeta = \sigma_B\sqrt{KG_0(L_k)}$ is used.

With DBF, K antennas cooperatively transmit their signals to the destination. Considering that the unintended receiver's channel information is unknown, with DBF the received signals at the destination and the unintended receiver from the k-th transmit antenna can be described as

$$d_k(t) = b_k\sum_m a_m h_k(t-mT)\otimes p^*(T_p-\tau_{ki_0}-t)+n_k(t), \tag{3.23a}$$

$$e_k(t) = b_k\sum_m a_m h_{e,k}(t-mT)\otimes p^*(T_p-\tau_{ki_0}-t)+n_{e,k}(t). \tag{3.23b}$$

For convenience, define

$$\begin{aligned}\bar{g}_k(t) &= \widetilde{h}_k(t)\otimes p^*(T_p-\tau_{ki_0}-t) \\ &= \sum_i^{L_k} h_{ki}\int_{-\infty}^{\infty} p(v-\tau_{ki})p^*(T_p-\tau_{ki_0}-t+v)dv,\end{aligned} \tag{3.24a}$$

$$\begin{aligned}\bar{g}_{e,k}(t) &= \widetilde{h}_{e,k}(t)\otimes p^*(T_p-\tau_{ki_0}-t) \\ &= \sum_i^{L_k} h_{e,ki}\int_{-\infty}^{\infty} p(v-\tau_{e,ki})p^*(T_p-\tau_{ki_0}-t+v)dv.\end{aligned} \tag{3.24b}$$

When K antennas cooperatively transmit to the destination via DBF, the received signals at the destination and the unintended receiver can be written as, respectively,

$$d(t) = \sum_{k=1}^K d_k(t) = \sum_m a_m\sum_{k=1}^K b_k\bar{g}_k(t-mT)+n(t), \tag{3.25a}$$

$$e(t) = \sum_{k=1}^K e_k(t) = \sum_m a_m\sum_{k=1}^K b_k\bar{g}_{e,k}(t-mT)+n_e(t). \tag{3.25b}$$

3.2 Basic SNR Analysis for Security Enhancement

Notice that DTR transmission focuses signal energy at the critical sampling instants based on the overall source-to-destination channel awareness. The focused signal energy leads to a substantial SNR improvement at sampling time instants and better signal quality at the destination, but not necessarily so for the unintended receiver whose channels are uncorrelated with destination's. Our objective is to analyze how this important energy focusing property of DTR transmission can significantly increase the performance gap between the intended and unintended receivers.

Specifically, the SNR of the T-spaced samples at the output of the receiver filter at the destination receiver is substantially higher than the SNR of the T-spaced samples at output of the receiver filter at the unintended receiver. For practical purpose, if DTR transmission can significantly increase the SNR at the desired receiver while keeping the SNR at the unintended receivers at unknown locations sufficiently low, then it can ensure good source-destination link performance while reducing co-channel interference to other nearby links. Moreover, a large SNR gap between the source-destination and source-unintended receiver links can likewise protect information from being decoded by eavesdroppers at locations unknown to the transmitter.

The receiver-dependent SNR may be translated into a corresponding secrecy rate, which has been discussed in Chap. 1. But it is of little practical interest to derive the secrecy rate R_s for a specific set of channel impulse responses. For practical utility, it is more meaningful to investigate the DTR performance for a typical class of random channels by determining the mean secrecy rate $\mathrm{E}\{R_s\}$ over the ensemble of such random channels. However, since the secrecy rate is a nonlinear function of both SNR_d at the destination and SNR_e at the unintended receiver, the ensemble averaged secrecy rate cannot be evaluated based on average received SNR values. Consequently, the respective SNR at the destination and the unintended receiver shall be analytically derived to characterize the benefits of DTR transmission. To obtain results that are meaningful and practical, the average SNR over an ensemble of random multi-path channels (including the number of multi-paths) shall be considered. As discussed later, perfect equalization at the intended and unintended receivers is assumed to cancel any ISI when determining the received SNR. Alternatively, pre-equalization at the source [14, 15] can be used for effective ISI removal at the cost of higher transmitter complexity.

Our analytical results and the accompanied numerical evaluation will demonstrate that DTR can achieve lower co-channel interference and a more degraded SNR at eavesdroppers than traditional DBF. To be fair, the receivers are assumed to be ideal with perfect equalization for either the DTR or DBF transmission schemes. Such ideal receivers with perfect equalization will provide a performance benchmark for the various transmission schemes under consideration. By utilizing the individual channel information from each distributed antenna to the destination, DTR will be shown to achieve the same level of SNR-gap (or secrecy rate) but with a fewer number of distributed transmit antennas than LoS-DBF.

3.3 SNR Analysis with Fixed Multi-Path Delay

3.3.1 SNR Analysis of Distributed Time Reversal Transmission

Recall that for the destination receiver, the peak SNR occurs at the sampling instants $t_\ell = \ell T + T_p$ where the peak pulse magnitude is obtained. However, for the unintended receiver, there may not be best sampling instants because of the random multi-path channels $h_{e,ki}$ and h_{ki} involved. Hence, the unintended receiver or eavesdropper samples the RRC filter output with the same period T but with an arbitrary time offset T_e, i.e., samples are taken at times $t_\ell^{(e)} = \ell T + T_e$. Thus, the two received signals after sampling are

$$d(t_\ell) = \sum_m a_m \sum_{k=1}^{K} b_k q_k(t_\ell - mT) + n(t_\ell), \tag{3.26a}$$

$$e(t_\ell^{(e)}) = \sum_m a_m \sum_{k=1}^{K} b_k q_{e,k}(t_\ell^{(e)} - mT) + n_e(t_\ell^{(e)}). \tag{3.26b}$$

Note that $d(t_\ell)$ and $e(t_\ell^{(e)})$ are used to detect symbol a_ℓ. Clearly, both destination and unintended receiver have to contend with ISI [17] at the receiver. The idealistic scenario will be considered, in which the destination receiver can acquire the perfect CSI with respect to $\sum_{k=1}^{K} b_k q_k(t - mT)$ such that all ISI at the receiver can be eliminated effectively through the use of a decision feedback equalizer without causing detection performance degradation [18]. At the transmitter, pre-equalization [15, 16] can also achieve effective ISI removal at higher transmitter complexity.

Perfect equalization and perfect CSI are impractical in actual communication systems. Residual ISI may result in receiver performance loss. However, the effect of unmitigated ISI at both the destination receiver and the unintended receivers varies with the channel delay profile, the length and type of pilot symbols, and the types of channel estimation and equalization algorithms, among other factors. Characterization of residual ISI effect would be system-dependent. Hence, this study focuses on investigating the best case scenario of perfect ISI suppression to provide a design benchmark. By establishing performance limit in terms of the received signal SNR, our results can provide useful design guidelines. Practitioners can develop additional ISI margins from measurement and experience.

3.3.1.1 Average SNR

For the ℓ-th QAM symbol, the receiver output (corresponding to the input $d(t_\ell)$) is given by

$$a_\ell \sum_k b_k q_k(T_p) = a_\ell \sum_k \beta_k \int_{-\infty}^{\infty} \left| \sum_{i=0}^{L_k} h_{ki} p(v - \tau_{ki}) \right|^2 dv,$$

where $\beta_k = b_k/\sqrt{E_k}$. Note that the QAM symbol a_ℓ has zero mean and average power $P_s = E\{|a_m|^2\}$. Since the noise $n(t_\ell)$ is $\mathscr{CN}(0, \sigma_n^2)$, the general expression of the received SNR for the destination is given by

$$\mathrm{SNR}_d = \frac{P_s}{\sigma_n^2}\mathrm{E}\left\{\left[\sum_k \beta_k \int_{-\infty}^{\infty}\left|\sum_{i=0}^{L_k} h_{ki}p(v-\tau_{ki})\right|^2 dv\right]^2\right\}. \tag{3.27}$$

To analyze the SNR, recall that the complex multi-path channel gains associated with the different transmit antennas and delays $\{h_{ki}\}$ are independent zero-mean complex Gaussian random variables with $\mathrm{E}\{|h_{ki}|^2\} = \sigma_B^2$, $\mathrm{E}\{|h_{ki}|^4\} = 2\sigma_B^4$, and $\mathrm{E}\{h_{ki}\} = E\{h_{ki}^2\} = 0$. Thus,

$$\begin{aligned} Q_{d1} =& \mathrm{E}\left\{\left[\sum_k \beta_k \int_{-\infty}^{\infty}\left|\sum_{i=0}^{L_k} h_{ki}p(v-\tau_{ki})\right|^2 dv\right]^2\right\} \\ =& \mathrm{E}\left\{\sum_{k_1}\beta_{k1}\int_v\left(\sum_{i_1=0}^{L_{k_1}} h_{k_1 i_1}p(v-\tau_{k_1 i_1})\sum_{i_2=0}^{L_{k_1}} h_{k_1 i_2}^* p^*(v-\tau_{k_1 i_2})\right)dv\right. \\ & \left.\times\sum_{k_2}\beta_{k2}\int_w\left(\sum_{j_1=0}^{L_{k_2}} h_{k_2 j_1}p(w-\tau_{k_2 j_1})\sum_{j_2=0}^{L_{k_2}} h_{k_2 j_2}^* p^*(w-\tau_{k_2 j_2})\right)dw\right\}. \end{aligned} \tag{3.28}$$

Let us define

$$E_p = \int_v |p(v-\tau)|^2\, dv = 1 \quad \text{and} \quad R_p(\tau_1-\tau_2) = \int_v p(v-\tau_1)p^*(v-\tau_2)dv. \tag{3.29a}$$

Using the i.i.d. property of $\{h_{ki}\}$ gives

$$\begin{aligned} Q_{d1} = \int_v\int_w\Bigg[\sum_k \beta_k^2\Bigg(& \sum_{i,j,i\neq j}^{L_k}\sigma_B^4\,|p(v-\tau_{ki})|^2\,|p(w-\tau_{kj})|^2 \\ &+ \sum_i^{L_k} 2\sigma_B^4\,|p(v-\tau_{ki})|^2\,|p(w-\tau_{ki})|^2 \\ &+ \sum_{i_1,i_2,i_2\neq i_1}^{L_k}\sigma_B^4 p(v-\tau_{ki_1})p^*(v-\tau_{ki_2})p(w-\tau_{ki_2})p^*(w-\tau_{ki_1})\Bigg)\Bigg. \end{aligned}$$

$$+\sum_{k_1}\sum_{k_2\neq k_1}\beta_{k1}\beta_{k2}\left(\sum_{i,j}^{L_{k_1},L_{k_2}}\sigma_B^4\left|p(v-\tau_{k_1 i})\right|^2\left|p(w-\tau_{k_2 j})\right|^2\right)\Bigg]dvdw$$

$$=\sigma_B^4\left(\sum_k\beta_k(L_k+1)\right)^2+\sigma_B^4\sum_k\beta_k^2\sum_{i_1=0}^{L_k}\sum_{i_2=0}^{L_k}|R_p(\tau_{ki_1}-\tau_{ki_2})|^2. \tag{3.29b}$$

Recall that $\beta_k=(\sqrt{K(L_k+1)}\sigma_B)^{-1}$. Thus,

$$Q_{d1}=\sigma_B^2\frac{1}{K}\left(\sum_k\sqrt{(L_k+1)}\right)^2+\frac{\sigma_B^2}{K}\sum_k\frac{1}{(L_k+1)}\sum_{i_1=0}^{L_k}\sum_{i_2=0}^{L_k}|R_p(\tau_{ki_1}-\tau_{ki_2})|^2. \tag{3.29c}$$

Besides, the unintended receiver will sample at time T_e to yield output sample

$$q_{e,k}(T_e)=\frac{1}{\sqrt{E_k}}\int\sum_{i=0}^{L_k}h_{e,ki}p(v-\tau_{e,ki})\sum_{j=0}^{L_k}h_{kj}^*p^*(T_p-T_e+v-\tau_{e,kj})dv, \tag{3.30}$$

whose SNR is

$$\mathrm{SNR}_e=\frac{P_s}{\sigma_e^2}\mathrm{E}\left\{\left|\sum_{k=1}^{K}b_kq_{e,k}(T_e)\right|^2\right\}. \tag{3.31}$$

Therefore, for a given L_k,

$$\begin{aligned}Q_{e1}=&\mathrm{E}\left\{\left|\sum_{k=1}^{K}b_kq_{e,k}(T_e)\right|^2\right\}\\=&\mathrm{E}\Bigg\{\sum_{k_1}\beta_{k1}\int_v\sum_{i_1=0}^{L_{k_1}}h_{e,k_1i_1}p(v-\tau_{e,k_1i_1})\sum_{i_2=0}^{L_{k_1}}h_{k_1i_2}^*p^*(T_p-T_e+v-\tau_{k_1i_2})dv\\&\times\sum_{k_2}\beta_{k2}\int_w\sum_{j_1=0}^{L_{k_2}}h_{e,k_2j_1}^*p^*(w-\tau_{e,k_2j_1})\sum_{j_2=0}^{L_{k_2}}h_{k_2j_2}p(T_p-T_e+w-\tau_{k_2j_2})dw\Bigg\}\\=&\int_v\int_w\sum_k\beta_k^2\Bigg[\sum_{i=0}^{L_k}\sum_{j=0}^{L_k}\mathrm{E}\left\{h_{e,ki}h_{e,ki}^*h_{kj}h_{kj}^*\right\}p(v-\tau_{e,ki})\\&p(T_p-T_e+v-\tau_{kj})p^*\big(T_p-T_e+w-\tau_{kj}\big)p^*(w-\tau_{e,ki})\Bigg]dvdw\end{aligned}$$

$$= \sum_k \beta_k^2 \sum_{i,j} \sigma_B^2 \sigma_E^2 |R_p(T_p - T_e - \tau_{kj} + \tau_{e,ki})|^2 \tag{3.32a}$$

$$= \frac{\sigma_E^2}{K} \sum_k \frac{1}{(L_k+1)} \sum_{i,j} R_p(T_p - T_e - \tau_{kj} + \tau_{e,ki})|^2. \tag{3.32b}$$

Hence given $L_k + 1$ multi-paths for each antenna, the SNR at the destination and the unintended receiver can be found, respectively, as

$$\text{SNR}_{d1} = \frac{P_s Q_{d1}}{\sigma_n^2} \quad \text{and} \quad \text{SNR}_{e1} = \frac{P_s Q_{e1}}{\sigma_e^2}. \tag{3.33}$$

Based on the above analysis, the SNR-gap between the intended and unintended receivers in DTR can be evaluated as $\text{SNR}_{gap1}(\text{dB}) = \text{SNR}_{d1}(\text{dB}) - \text{SNR}_{e1}(\text{dB})$.

3.3.1.2 Equal Gain Transmission in DTR

Our analytical results depend on the power distribution among transmit antennas b_k. Typically, the source central controller is not required to be aware of each antenna's channel gain. To avoid the complexity of centralized control and exchange of channel knowledge among antennas, equal power distribution can be applied among the transmit antennas. Thus, given K total antennas, the weights $b_k = 1/\sqrt{K}$ and $\beta_k = 1/\sqrt{KE_k}$ can be used to achieve equal gain transmission (EGT) in DTR unless otherwise specified. Since $E_k = (L_k + 1)\sigma_B^2$, Q_{d1} and Q_{e1} of Eq. (3.33) can be directly evaluated for EGT.

3.3.2 SNR Analysis of Direct Transmission

Likewise, we can analyze SNR performance of DT in the same way as DTR. According to Eqs. (3.21a) and (3.21b), the signal energy at the destination receiver at the sampling instant $t_\ell = T_p + \ell T$ is

$$Q_{d2} = \text{E}\left\{ \left| \sum_k b_k \bar{z}_k(T_p) \right|^2 \right\} = \sum_k {b_k}^2 \sum_{i=0}^{L_k} \sigma_B^2 \left| R_p(\tau_{ki}) \right|^2, \tag{3.34a}$$

while at the unintended receiver, the signal energy at the sampling instant $T_{e0} + \ell T$ is

$$Q_{e2} = \text{E}\left\{ \left| \sum_k b_k \bar{z}_{e,k}(T_{e0}) \right|^2 \right\} = \sum_k {b_k}^2 \sum_{i=0}^{L_k} \sigma_E^2 \left| R_p(T_p - T_{e0} + \tau_{e,ki}) \right|^2. \tag{3.34b}$$

Given $L_k + 1$ multi-paths for each transmit antenna, the SNRs at destination and unintended receiver are, respectively,

$$\text{SNR}_{d2} = \frac{P_s Q_{d2}}{\sigma_n^2}, \quad \text{and} \quad \text{SNR}_{e2} = \frac{P_s Q_{e2}}{\sigma_e^2}. \tag{3.35}$$

The SNR gap and the resulting secrecy rate can be quantified directly. For the most common case, equal gain transmission weights $b_k = 1/\sqrt{K}$ can be used to evaluate the SNR and SNR gap of Eq. (3.35) numerically.

3.3.3 SNR Analysis of Distributed Beamforming Transmission

Let the peak SNR sampling times for the destination and the unintended receiver be $T_p + \ell T$ and $T_{e1} + \ell T$, respectively. They follow that

$$\begin{aligned} Q_{d3} =& \text{E}\left\{\left|\sum_{k=1}^{K} b_k \bar{g}_k(T_p)\right|^2\right\} \\ =& \text{E}\left\{\sum_{k_1} \frac{h_{k_1 i_0}^*}{\zeta} \sum_{i}^{L_{k_1}} h_{k_1 i} \int_{-\infty}^{\infty} p(v - \tau_{k_1 i}) p^*(v - \tau_{k_1 i_0}) dv \right. \\ & \left. \sum_{k_2} \frac{h_{k_2 i_0}}{\zeta} \sum_{j}^{L_{k_2}} h_{k_2 j}^* \int_{-\infty}^{\infty} p^*(w - \tau_{k_2 j}) p(w - \tau_{k_2 i_0}) dw \right\}, \end{aligned} \tag{3.36a}$$

$$\begin{aligned} Q_{e3} =& \text{E}\left\{\left|\sum_{k=1}^{K} b_k \bar{g}_{e,k}(T_{e1})\right|^2\right\} \\ =& \text{E}\left\{\sum_{k_1} \frac{h_{k_1 i_0}^*}{\zeta} \sum_{i}^{L_{k_1}} h_{e,k_1 i} \int_{-\infty}^{\infty} p(v - \tau_{e,k_1 i}) p^*(T_p + v - T_{e1} - \tau_{k_1 i_0}) dv \right. \\ & \left. \times \sum_{k_2} \frac{h_{k_2 i_0}}{\zeta} \sum_{j}^{L_{k_2}} h_{e,k_2 j}^* \int_{-\infty}^{\infty} p^*(w - \tau_{e,k_2 j}) p(T_p + w - T_{e1} - \tau_{k_1 i_0}) dw \right\}. \end{aligned} \tag{3.36b}$$

3.3.3.1 LoS-DBF

For direct LoS beamforming, $i_0 = 0$ and $\zeta = \sigma_B \sqrt{K}$ such that

$$Q_{d3} = \frac{1}{K} \sum_{k1} \sum_{k2 \neq k1} \sigma_B^2 |E_p|^2 + \frac{1}{K} \sum_{k} \left(\sum_{i \neq i_0} \sigma_B^2 |R_p(\tau_{ki} - \tau_{ki_0})|^2 + 2\sigma_B^2 |E_p|^2 \right)$$

$$=\sigma_B^2(K+1)+\frac{1}{K}\sum_k\left(\sum_{i\neq 0}\sigma_B^2|R_p(\tau_{ki}-\tau_{k0})|^2\right), \tag{3.37a}$$

$$Q_{e3}=\frac{1}{K}\sum_k\left(\sum_i\sigma_E^2|R_p(T_p-T_{e1}-\tau_{k0}+\tau_{e,ki})|^2\right). \tag{3.37b}$$

When considering L_k+1 multi-paths for each transmit antenna, the SNRs at the destination and the unintended receiver are, respectively,

$$\mathrm{SNR}_{d3}=\frac{P_sQ_{d3}}{\sigma_n^2},\ \mathrm{SNR}_{e3}=\frac{P_sQ_{e3}}{\sigma_n^2}. \tag{3.38}$$

3.3.3.2 MGP-DBF

For MGP distributed beamforming, recall that $i_0=\arg\max_i|h_{ki}|$ such that $b_k=h_{ki_0}^*/(\sigma_B\sqrt{KG_0})$. Using the PDF in Eq. (3.22a) gives

$$\begin{aligned}\mathrm{E}(|b_k|^4)&=\frac{1}{\sigma_B^4K^2G_0(L_k)^2}\int_0^\infty x^2f_{(n)}(x)dx\\&=\frac{1}{[KG_0(L_k)]^2}(L_k+1)\sum_{i=0}^{L_k}C_{L_k}^i(-1)^i\int_0^\infty t^2\exp[-(i+1)t]dt\\&=K^{-2}G_1(L_k),\end{aligned} \tag{3.39a}$$

where

$$G_1(L_k)=\frac{(L_k+1)}{[G_0(L_k)]^2}2\sum_{i=0}^{L_k}C_{L_k}^i(-1)^i(i+1)^{-3}=(L_k+1)^{-1}\frac{2\sum_{i=0}^{L_k}C_{L_k}^i(-1)^i(i+1)^{-3}}{\left[\sum_{i=0}^{L_k}C_{L_k}^i(-1)^i(i+1)^{-2}\right]^2}. \tag{3.39b}$$

Therefore,

$$\begin{aligned}Q_{d4}&=\mathrm{E}\left\{\left|\sum_{k=1}^K b_k\bar{g}_k(T_p)\right|^2\right\}\\&=\sum_k\sigma_B^2\left(\sum_{i\neq i_0}\mathrm{E}\{|b_k|^2\}|R_p(\tau_{ki}-\tau_{ki_0})|^2+G_0K\mathrm{E}\{|b_k|^4)\}\right)\\&\qquad+\sum_{k1}\sum_{k2\neq k1}\sigma_B^2KG_0\mathrm{E}\{|b_{k1}|^2\}\mathrm{E}\{|b_{k2}|^2\}\end{aligned}$$

$$= K^{-1}\sigma_B^2 \sum_k \left(\sum_{i \neq i_0} |R_p(\tau_{ki} - \tau_{ki_0})|^2 \right) + G_1(L_k)G_0(L_k)\sigma_B^2 + (K-1)G_0(L_k)\sigma_B^2, \tag{3.40a}$$

$$Q_{e4} = K^{-1}\sigma_E^2 \sum_k \left(\sum_i |R_p(T_p - T_{e1} - \tau_{ki_0} + \tau_{e,ki})|^2 \right). \tag{3.40b}$$

The SNRs at the destination and the unintended receiver are, respectively,

$$\text{SNR}_{d4} = \frac{P_s Q_{d4}}{\sigma_n^2} \text{and } \text{SNR}_{e4} = \frac{P_s Q_{e4}}{\sigma_e^2}. \tag{3.41}$$

3.4 SNR Analysis with Random Multi-Path Delay

Recall that, Sect. 3.3 analyzes the SNR analysis with fixed multi-path delay, thus the more general and practical wireless scenario is now considered, where the number of multi-paths per transmit antenna is (L_k+1) and their respective multi-path delays are randomly uniformed. As mentioned in Sect. 3.1, this scenario captures the uncertain multi-path environment.

3.4.1 SNR Analysis of Distributed Time Reversal Transmission

For DTR transmission, an average can be taken over the L_k to obtain

$$\begin{aligned}
\text{E}_{L_k}\{Q_{d1}\} &= \sigma_B^4 \text{E}\Bigg\{ \sum_k \beta_k^2 \left[(L_k+1)L_k + 2(L_k+1)\right] \\
&\quad + \sum_{k_1} \sum_{k_2 \neq k_1} \beta_{k1}\beta_{k2}(L_{k_1}+1)(L_{k_2}+1) + \sum_k \beta_k^2 \sum_{i_1=0}^{L_k} \sum_{i_2 \neq i_1}^{L_k} |R_p(\tau_{ki_1} - \tau_{ki_2})|^2 \Bigg\} \\
&= \sigma_B^2 \sum_k b_k^2 \left(\frac{3+L}{2} \right) + \sigma_B^2 \left(\frac{1}{L} \sum_{L_k=0}^{L-1} \sqrt{L_k+1} \right)^2 \sum_{k_1} \sum_{k_2 \neq k_1} b_{k1} b_{k2} \\
&\quad + \sigma_B^2 \sum_k b_k^2 \frac{1}{L} \sum_{L_k=0}^{L-1} \frac{1}{L_k+1} \sum_{i_1=0}^{L_k} \sum_{i_2 \neq i_1}^{L_k} \text{E}\left\{ |R_p(\tau_{ki_1} - \tau_{ki_2})|^2 \right\}.
\end{aligned} \tag{3.42}$$

For independent and uniform $\tau_{ki_1} \neq \tau_{ki_2}$, the PDF of $\delta = \tau_{ki_1} - \tau_{ki_2}$ is symmetric, given by

$$\begin{aligned} f_\delta(x) &= \int_0^{T_p} p_{\tau_{ki}}(x+\tau) p_{\tau_{ki}}(\tau) d\tau, \quad |x| < T_p \\ &= \frac{e^{-T_p/T_0}}{T_0(1-e^{-T_p/T_0})^2} \cdot \sinh\left(\frac{T_p - |x|}{T_0}\right), \quad |x| < T_p. \end{aligned} \tag{3.43}$$

Thus, two quantities can be defined and numerically calculated as:

$$\rho_1 = \mathrm{E}\{|R_p(\tau_{ki_1} - \tau_{ki_2})|^2\} = \int_0^{T_p} 2 f_\delta(x) |R_p(x)|^2 dx, \tag{3.44a}$$

$$\rho_{1,e} = \mathrm{E}\left\{\left|R_p(T_p - T_e - \tau_{kj} + \tau_{e,ki})\right|^2\right\} = \int_{-T_p}^{T_p} f_\delta(x) \left|R_p(T_p - T_e + x)\right|^2 dx. \tag{3.44b}$$

Therefore,

$$\begin{aligned} \mathrm{E}\{Q_{d1}\} &= \sigma_B^2 \left(\frac{1}{L}\sum_{L_k=0}^{L-1} \sqrt{L_k+1}\right)^2 \sum_{k_1} \sum_{k_2 \neq k_1} b_{k1} b_{k2} \\ &\quad + \sigma_B^2 \sum_k b_k^2 \left(\frac{3+L}{2}\right) + \frac{\sigma_B^2 \rho_1}{L} \sum_k b_k^2 \sum_{L_k=0}^{L-1} L_k \\ &= \sigma_B^2 \left(\frac{1}{L}\sum_{L_k=0}^{L-1} \sqrt{L_k+1}\right)^2 \sum_{k_1} \sum_{k_2 \neq k_1} b_{k1} b_{k2} + \sigma_B^2 \left(\frac{3+L}{2}\right) + \frac{\sigma_B^2 \rho_1 (L-1)}{2}. \end{aligned} \tag{3.45a}$$

Besides, for the unintended receiver

$$\begin{aligned} \mathrm{E}\{Q_{e1}\} &= \mathrm{E}\left\{\sum_k \beta_k^2 \sum_{i,j} \sigma_B^2 \sigma_E^2 |R_p(T_p - T_e - \tau_{kj} + \tau_{e,ki})|^2\right\} \\ &= \sigma_E^2 \rho_{1,e} \sum_k b_k^2 \frac{1}{L} \sum_{L_k=0}^{L-1} (L_k+1) = \sigma_E^2 \rho_{1,e} \cdot \left(\frac{L+1}{2}\right). \end{aligned} \tag{3.45b}$$

3.4.2 SNR Analysis of Direct Transmission

For direct transmission, first define

$$\rho_2 = \mathrm{E}\left\{\left|R_p(\tau_{ki})\right|^2\right\} = \int_0^{T_p} p_{\tau_{ki}}(x)\left|R_p(x)\right|^2 dx, \tag{3.46a}$$

$$\rho_{2,e} = \mathrm{E}\left\{\left|R_p(T_p - T_{e0} + \tau_{e,ki})\right|^2\right\} = \int_0^{T_p} p_{\tau_{ki}}(x)|R_p(T_p - T_{e0} + x)|^2 dx. \tag{3.46b}$$

Accordingly,

$$\begin{aligned}\mathrm{E}\{Q_{d2}\} &= \mathrm{E}\left\{\sum_k {b_k}^2 \sum_{i=0}^{L_k} \sigma_B^2 \left|R_p(\tau_{ki})\right|^2\right\} \\ &= \sum_k {b_k}^2 \sigma_B^2 \frac{1}{L} \sum_{L_k=0}^{L-1} \sum_{i=0}^{L_k} \mathrm{E}\left\{\left|R_p(\tau_{ki})\right|^2\right\} \qquad (3.47a) \\ &= \rho_2 \sigma_B^2 \frac{1}{L} \sum_{L_k=0}^{L-1} (L_k+1) \sum_k {b_k}^2 = \frac{\rho_2 \sigma_B^2 (L+1)}{2}, \qquad (3.47b)\end{aligned}$$

$$\begin{aligned}\mathrm{E}\{Q_{e2}\} &= \mathrm{E}\left\{\sum_k {b_k}^2 \sum_{i=0}^{L_k} \sigma_E^2 \left|R_p(T_p - T_{e0} + \tau_{e,ki})\right|^2\right\} \\ &= \sum_k {b_k}^2 \sigma_E^2 \frac{1}{L} \sum_{L_k=0}^{L-1} \sum_{i=0}^{L_k} \mathrm{E}\left\{\left|R_p(T_p - T_{e0} + \tau_{e,ki})\right|^2\right\} \qquad (3.47c) \\ &= \rho_{2,e} \sigma_E^2 \frac{1}{L} \sum_{L_k=0}^{L-1} (L_k+1) \sum_k {b_k}^2 = \frac{\rho_{2,e} \sigma_E^2 (L+1)}{2}. \qquad (3.47d)\end{aligned}$$

3.4.3 SNR Analysis of Distributed Beamforming Transmission

Based on our previous analysis,

$$\rho_3 = \mathrm{E}\{|R_p(\tau_{ki} - \tau_{k0})|^2\} = \int_{-T_p}^{T_p} f_\delta(x)|R_p(x)|^2 dx, \tag{3.48a}$$

$$\rho_{3,e} = \mathrm{E}\left\{\left|R_p(T_p - T_{e1} - \tau_{k0} + \tau_{e,ki})\right|^2\right\} = \int_{-T_p}^{T_p} f_\delta(x)|R_p(T_p - T_{e1} + x)|^2 dx. \tag{3.48b}$$

Thus, for LoS-DBF, $i_0 = 0$, resulting in

$$\begin{aligned}\mathrm{E}\{Q_{d3}\} =& \frac{1}{K}\sum_{k}\left(\frac{1}{L}\sum_{L_k=0}^{L-1}\sum_{i\neq 0}^{L_k}\sigma_B^2\mathrm{E}\left\{|R_p(\tau_{ki}-\tau_{k0})|^2\right\}\right)+\sigma_B^2(K+1)\\ =&\sigma_B^2\rho_3\left(\frac{L-1}{2}\right)+\sigma_B^2(K+1),\end{aligned} \tag{3.49a}$$

$$\begin{aligned}\mathrm{E}\{Q_{e3}\} =& \frac{1}{K}\sum_{k}\left(\frac{1}{L}\sum_{L_k=0}^{L-1}\sum_{i}^{L_k}\sigma_E^2\mathrm{E}\left\{|R_p(T_p-T_{e1}-\tau_{k0}+\tau_{e,ki})|^2\right\}\right)\\ =&\frac{\sigma_E^2\rho_{3,e}(L+1)}{2}.\end{aligned} \tag{3.49b}$$

In MGP-DBF, i_0 is random and

$$\begin{aligned}\mathrm{E}\{Q_{d4}\} &= K^{-1}\sigma_B^2\sum_{k}\frac{1}{L}\sum_{L_k=0}^{L-1}\sum_{i\neq i_0}^{L_k}\mathrm{E}\{|R_p(\tau_{ki}-\tau_{ki_0})|^2\}\\ &+\frac{\sigma_B^2}{L}\sum_{L_k=0}^{L-1}\left[(K-1)+G_1(L_k)\right]G_0(L_k)\\ &= K^{-1}\sigma_B^2\sum_{k}\frac{1}{L}\sum_{L_k=0}^{L-1}\sum_{i\neq i_0}^{L_k}\rho_4+\frac{\sigma_B^2}{L}\sum_{L_k=0}^{L-1}\left[(K-1)+G_1(L_k)\right]G_0(L_k)\\ &=\frac{\sigma_B^2}{L}\left[\rho_4\frac{L(L-1)}{2}+(K-1)\sum_{L_k=0}^{L-1}G_0(L_k)+\sum_{L_k=0}^{L-1}G_1(L_k)G_0(L_k)\right],\end{aligned} \tag{3.50a}$$

$$\begin{aligned}\mathrm{E}\{Q_{e4}\} &= K^{-1}\sigma_E^2\sum_{k}\frac{1}{L}\sum_{L_k=0}^{L-1}\left(\sum_{i=0}^{L_k}\mathrm{E}\left\{|R_p(T_p-T_{e1}-\tau_{ki_0}+\tau_{e,ki})|^2\right\}\right)\\ &=\frac{\sigma_E^2\rho_{4,e}(L+1)}{2},\end{aligned} \tag{3.50b}$$

where

$$\rho_4 = \mathrm{E}\{|R_p(\tau_{ki}-\tau_{ki_0})|^2\} = \rho_3, \tag{3.50c}$$

$$\begin{aligned}\rho_{4,e} &= \mathrm{E}\left\{\left|R_p(T_p-T_{e1}-\tau_{ki_0}+\tau_{e,ki})\right|^2\right\}\\ &=\int_{-T_p}^{T_p}f_\delta(x)|R_p(T_p-T_{e1}+x)|^2dx.\end{aligned} \tag{3.50d}$$

3.5 Simulation and Numerical Results

The SNRs of different transmission schemes at the destination and unintended receiver can be compared to illustrate physical layer secrecy enhancement [21], by using the SNR gap between the desired destination and the eavesdropper, denoted in dB as $\text{SNR}_{gap} = \text{SNR}_d - \text{SNR}_e$.

The performance of the various schemes under consideration can be compared under different conditions. Numerical results are now presented to compare the performance of four different transmission schemes in terms of SNR gap (or secrecy rate): DTR, DT, LoS-DBF, and MGP-DBF. By varying the multi-path profiles of the source-to-destination channels and source-to-unintended-receivers, both fixed and random channel multi-path number L_k can be tested.

First, the two channels in the non-degraded wiretapping scenario [10, 13] are assumed to be i.i.d. with equal variance $\sigma_B^2 = \sigma_E^2 = 0.4\,\text{mW}$, and equal noise power $\sigma_n^2 = \sigma_e^2 = 0.1\,\text{mW}$. Throughout the simulation, a RRC pulse shape with roll-off factor of $\alpha = 0.2$ is used [7]. In the various graphs presented, the suffix "$-t$" or solid lines are used to label theoretical results, whereas the suffix "$-n$" or dotted lines are used to label numerical results for the four different schemes under comparison. For the exponential multi-path power delay profile, the parameter $T_0 = T$ is used without loss of generality and $T_p = 2T$[1].

In terms of the sampling instant at the unintended receiver node, let $T_e = T_{e0} = T_{e1} = T_p + \Delta$, where Δ is the sampling time offset. Two cases are tested: $\Delta = 0$ and uniform Δ on $(-0.5T, 0.5T)$. The first case gives the unintended receivers the benefit of the doubt such that they sample at the same moment $\ell T + T_e = \ell T + T_p$ as the target receiver. The second case takes into account the timing uncertainty, such that the unintended receivers may sample uniformly within $(-0.5T, 0.5T)$ of the sampling instants $\ell T + T_p$ at the target receivers, which is a typical case in practice.

3.5.1 Fixed Number L_k of Multi-Path Components

In this case, the received SNR for different schemes is assessed while fixing the number of transmit antennas K and the number of multi-paths L_k, for various levels of transmit power P_s. For numerical results, 1000 random multi-path channels and delays are generated for Monte Carlo evaluation.

Figures 3.2, 3.3, and 3.4 show both the theoretical and numerical results at different power levels P_s for $L_k = 3$. The SNR of DTR-based transmission, DT, LoS-DBF, and MGP-DBF are evaluated. As is expected from the analytical expression of the SNR results, the SNR increases linearly with P_s. Hence, when the

[1] For a uniform multi-path delay profile, the delay time is set as $T_0 = \infty$.

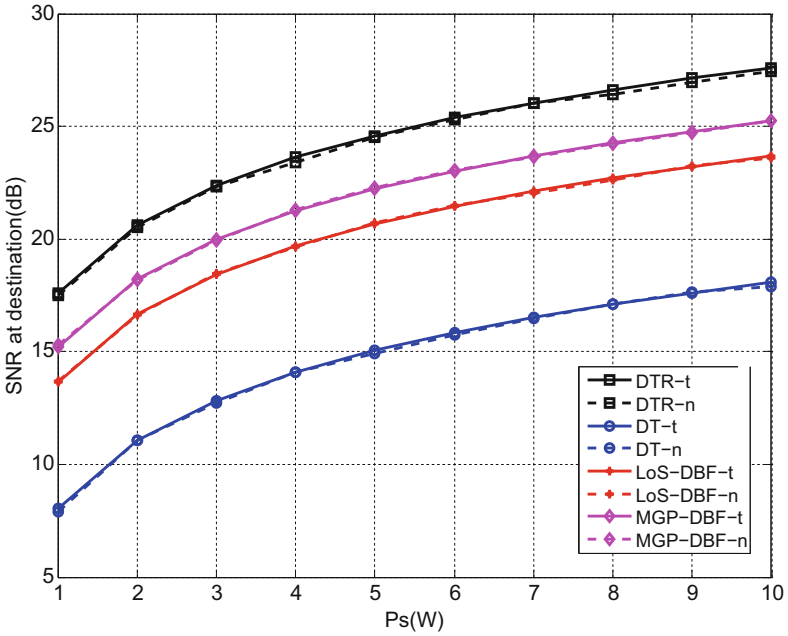


Fig. 3.2 Received signal SNR at intended receiver ($L_k = 3$, K = 3)

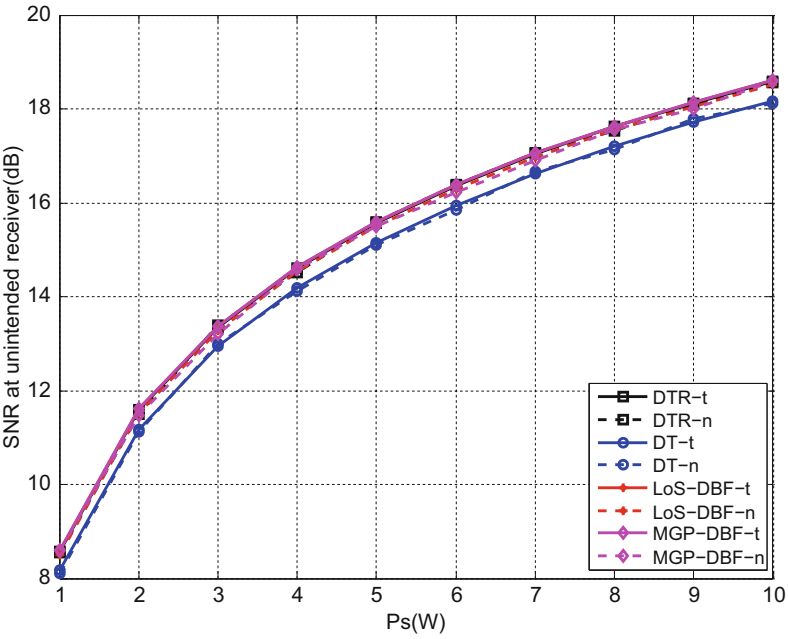


Fig. 3.3 SNR at unintended receiver ($L_k = 3$, K = 3, $\Delta = 0$)

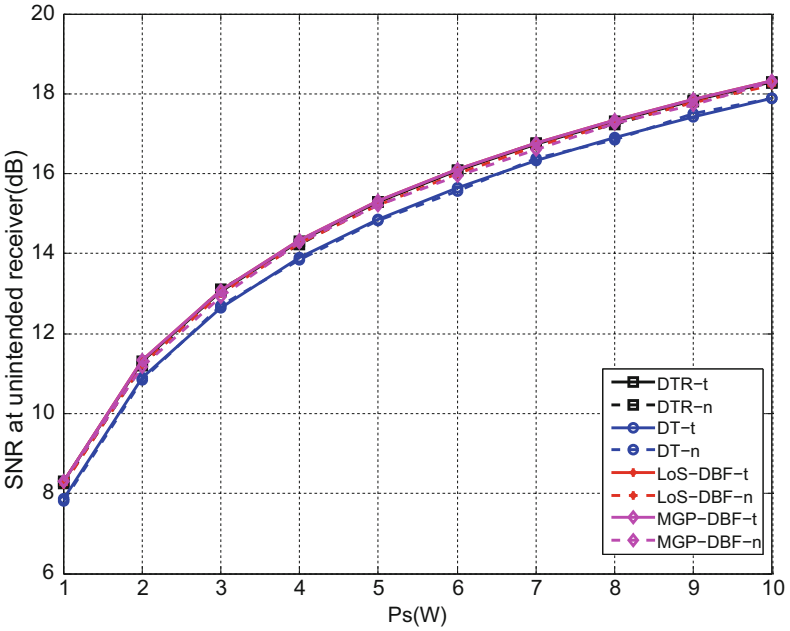


Fig. 3.4 SNR at unintended receiver ($L_k = 3$, K = 3, uniform Δ, $\Delta \in (-0.5T, 0.5T)$)

power P_s grows, the SNRs for all four schemes increase as shown in these figures. Note that the horizontal axis representing P_s has a linear scale, whereas the vertical axis representing SNR has a logarithmic scale. Close agreement is observed between analytical and numerical results for all four schemes. In order of performance, DTR achieves the highest SNR, with MGP and LoS beamforming trailing behind, followed by the least effective strategy of DT without considering the multi-path effect or the advantage of beamforming. Besides, when comparing the SNR at the unintended receivers, the received SNR is nearly identical in all four transmission strategies.

It is also clear that by letting $T_e = T_p$ which gives the benefit of the doubt to the unintended receivers in terms of symbol timing, the unintended receivers can see an approximately 0.3 dB SNR increase. Nevertheless, this slight change does not negate the significant SNR improvement as seen by the target receiver at the destination.

Similar results can also be obtained for different numbers of multi-paths, e.g., $L_k = 6$. Figures 3.5 and 3.6 compare the SNR gap of various transmission schemes for $L_k = 3$ and 6, respectively. Since the SNR for both nodes linearly grow with P_s, it is not surprising that the SNR gap remains flat for all four schemes. Among the four transmission schemes, DTR-based transmission provides the biggest SNR-gap between the destination node and unintended receivers. In fact, DTR is better than the MGP-DBF scheme which has a quite high complexity. This proves the

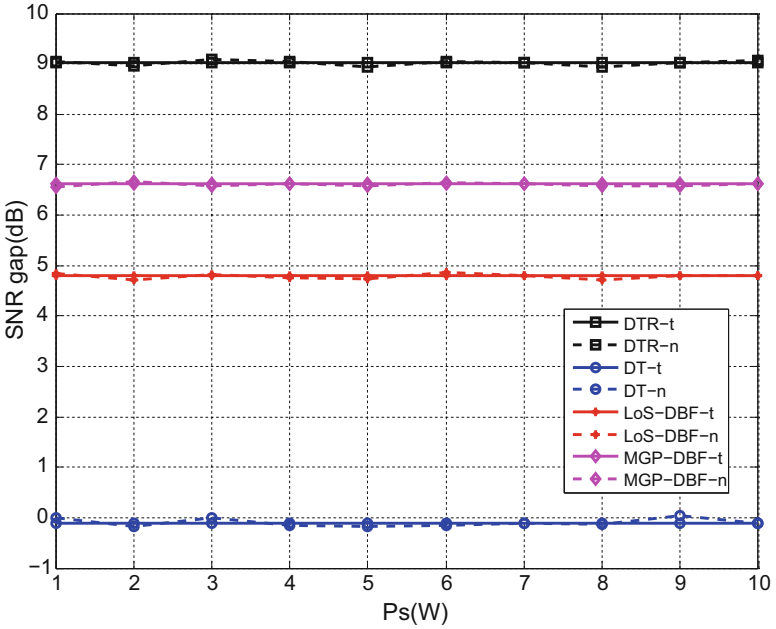


Fig. 3.5 Received signal SNR gap ($L_k = 3$, K = 3, $\Delta = 0$)

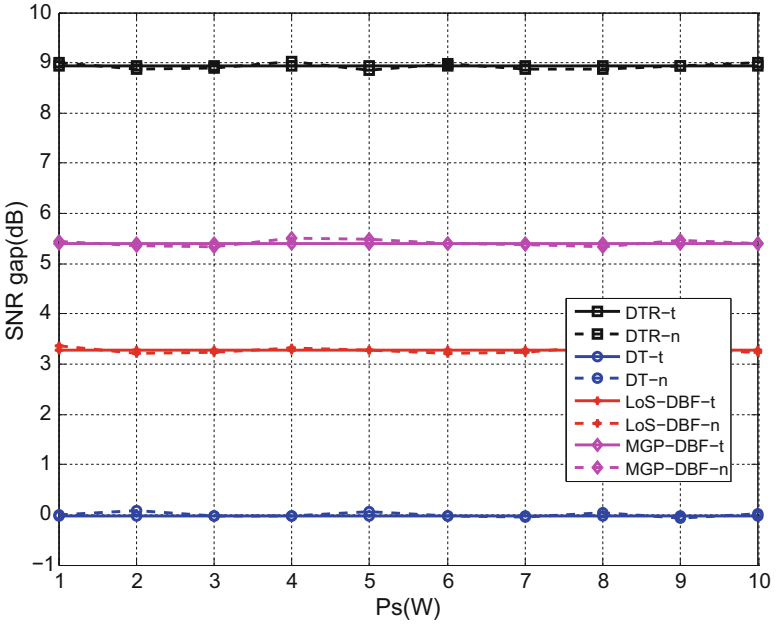


Fig. 3.6 Received signal SNR gap ($L_k = 6$, K = 3, $\Delta = 0$)

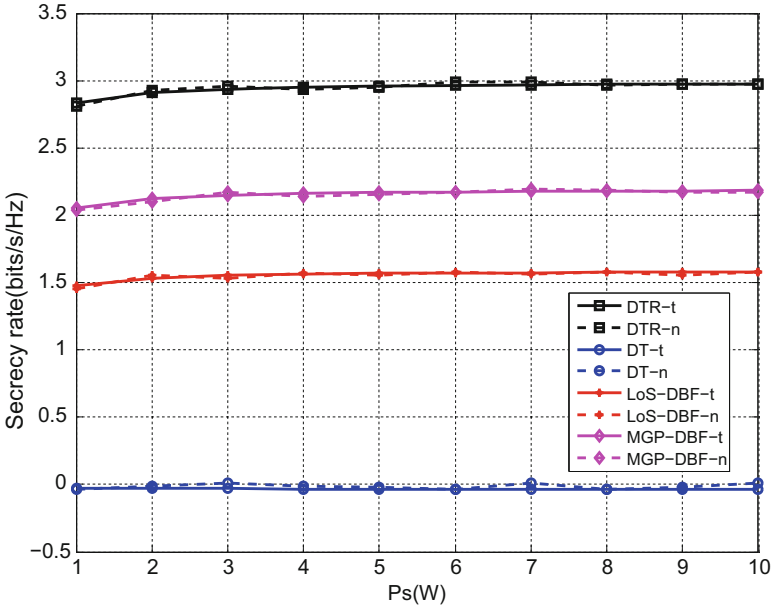


Fig. 3.7 Secrecy rate at destination ($L_k = 3$, K = 3, $\Delta = 0$)

simplicity and benefit of DTR transmission. Comparing the results of Figs. 3.5 and 3.6, observe the effect of the number of multi-path components. Assuming perfect receivers, as the number of multi-path components L_k grows from 3 to 6, the SNR gap of DTR remains nearly unchanged while the SNR gaps of LoS-DBF and MGP-DBF decrease. This effect is reasonable and expected. The observed performance loss in beamforming is due to the relative reduction of signal energy in either the LoS path or the maximum gain path when the number of signal paths L_k grows. Besides, DTR is robust to such uncertainties. In terms of corresponding secrecy rates, Figs. 3.7 and 3.8 illustrate similar results.

3.5.2 *Random Number L_k of Multi-Path Components*

In practical applications, the number of multi-path components, L_k, is uncertain and often time-varying. To obtain numerical results for such cases, 3000 random multi-path channels and delays are generated in Monte Carlo evaluation, for which L_k was assumed to be uniformly distributed in $\{0, \cdots, L-1\}$. All other parameters remain unchanged from the previous section.

Figures 3.9, 3.10, and 3.11 compare theoretical and numerical SNR results for different power levels P_s, given $L = 7$ and $K = 3$. The results compare the SNR of DTR transmission, DT, LoS-DBF, and MGP-DBF. Once again, close agreement

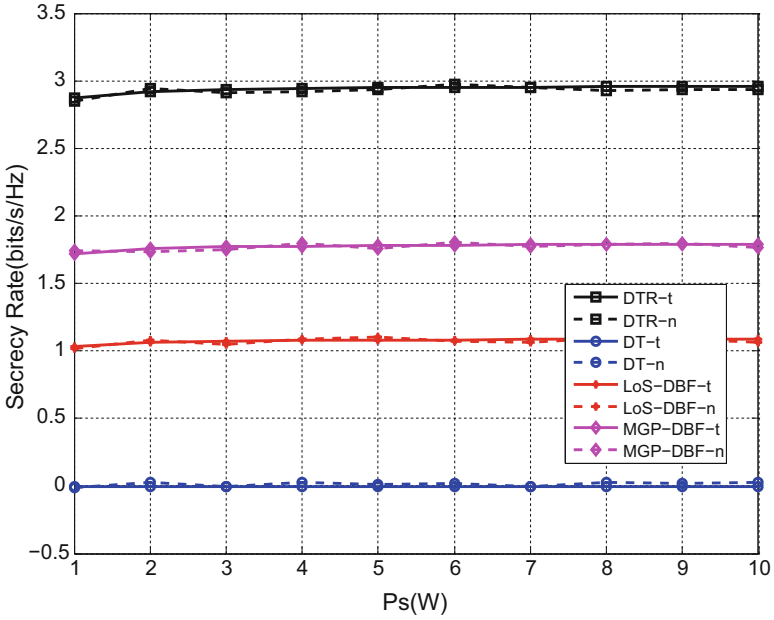


Fig. 3.8 Secrecy rate at destination ($L_k = 6$, K = 3, $\Delta = 0$)

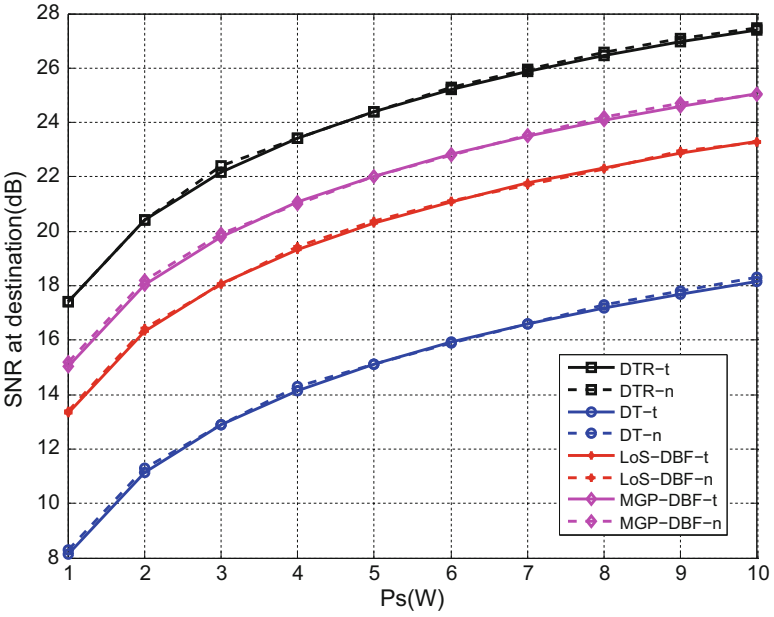


Fig. 3.9 Sampled signal SNR at target (L = 7, K = 3, $\Delta = 0$)

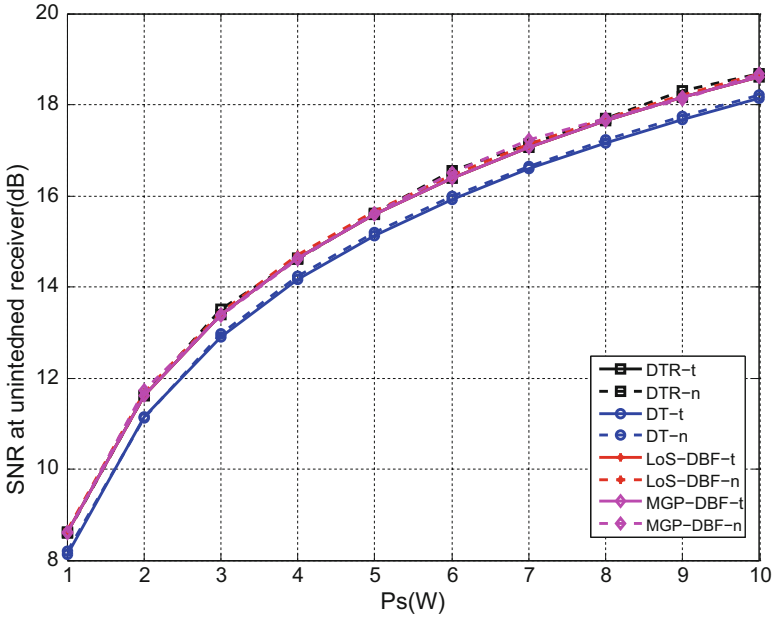


Fig. 3.10 SNR at unintended receiver (L = 7, K = 3, $\Delta = 0$)

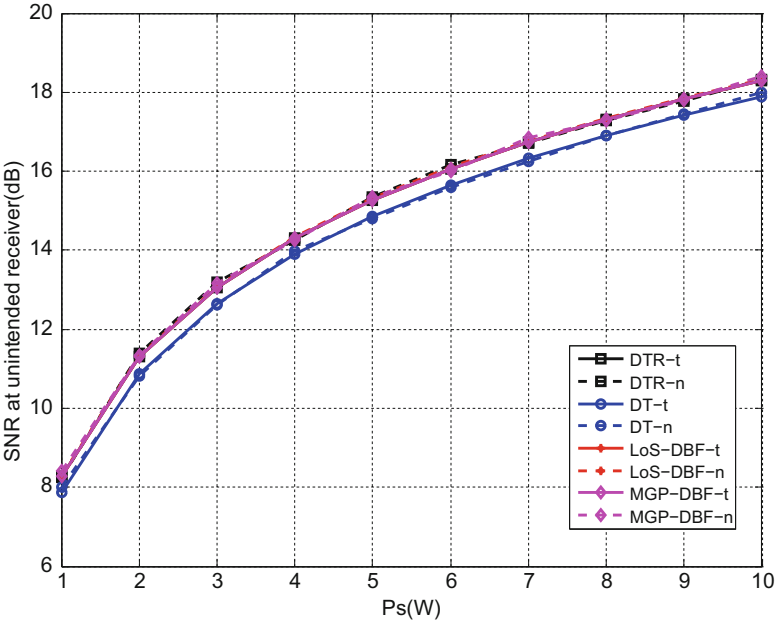


Fig. 3.11 SNR at unintended receiver (L = 7, K = 3, $\Delta \in (-0.5T, 0.5T)$)

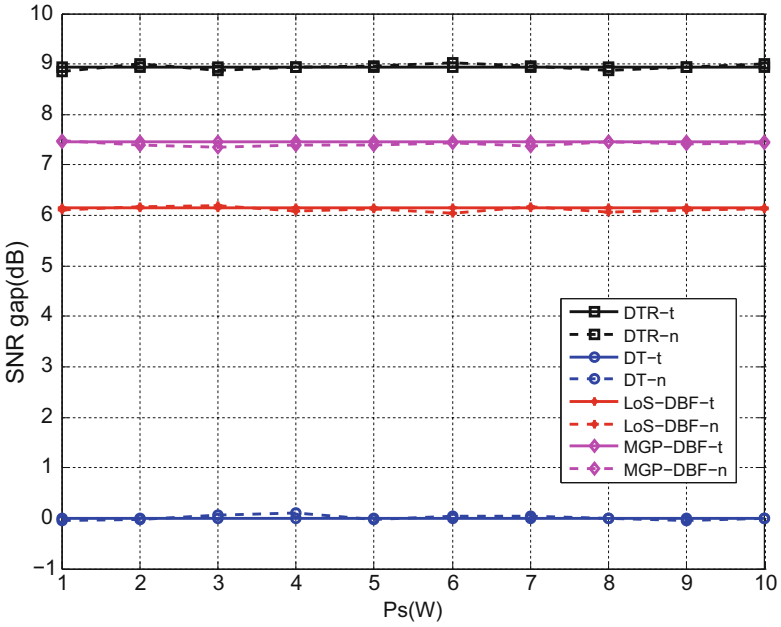


Fig. 3.12 Received signal SNR gap (L = 4, K = 3, $\Delta = 0$)

is observed between the analytical and numerical results for all four schemes. From the analytical expression for the SNR, the linear SNR growth with P_s is confirmed. Again, notice that the horizontal axis representing P_s has a linear scale, whereas the vertical axis representing SNR has a logarithmic scale. Similar to the case of fixed L_k, the DTR transmission leads to the highest destination SNR and better signal quality. Likewise, by giving unintended receivers the benefit of the doubt in terms of symbol timing, $\Delta = 0$ implies $T_e = T_p$. Compared with random Δ, the sampled signal SNR at the unintended receiver is only marginally higher.

Figures 3.12 and 3.13 illustrate the SNR gap between the destination and unintended receivers for four different schemes for $K = 3$ and $L = 4,\ 7$. Clearly, the SNR gap for DTR transmission is superior to that of three other schemes. Consistent with the previous results, for fixed L_k, DTR is robust to the distribution of the number of multi-path components, L. On the other hand, when the number of multi-path components grows, MGP-DBF and LoS-DBF provide less signal quality advantage at the destination receiver in terms of the SNR gap. The corresponding secrecy rates of Figs. 3.14 and 3.15 show similar results.

Next, the impact of the number of transmit antennas, K, on the SNR gap of the different schemes is studied. Figures 3.16 and 3.17 present the SNR result at the destination receiver and the SNR gap for $L = 4$ and $P_s = 10\,\text{W}$. Meanwhile, the secrecy rate at the destination for K distributed antennas is described in Fig. 3.18. Similar to earlier cases, the theoretical results agree well with the real simulation

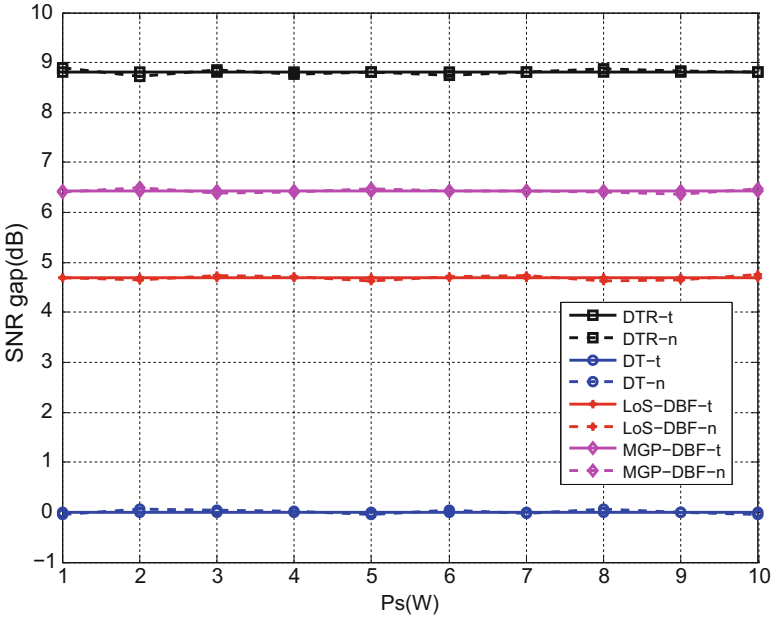


Fig. 3.13 Received signal SNR gap (L = 7, K = 3, $\Delta = 0$)

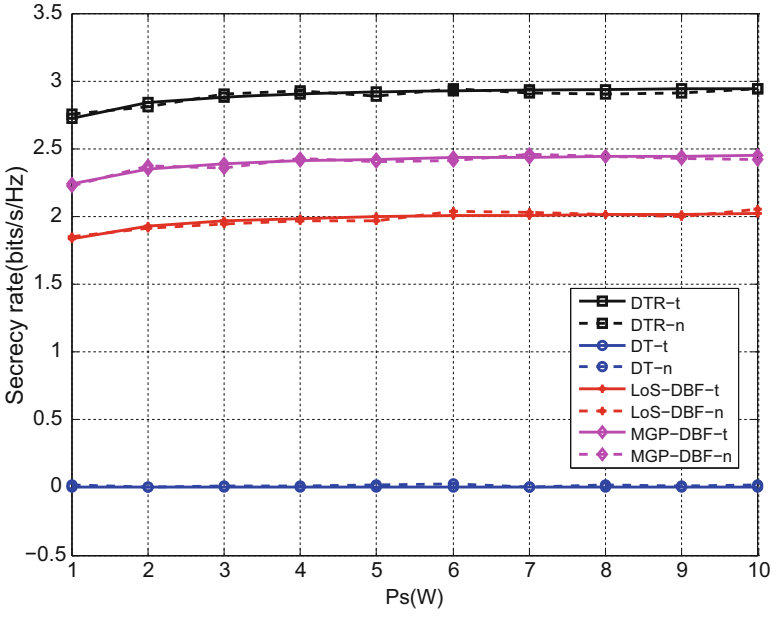


Fig. 3.14 Secrecy rate (L = 4, K = 3, $\Delta = 0$)

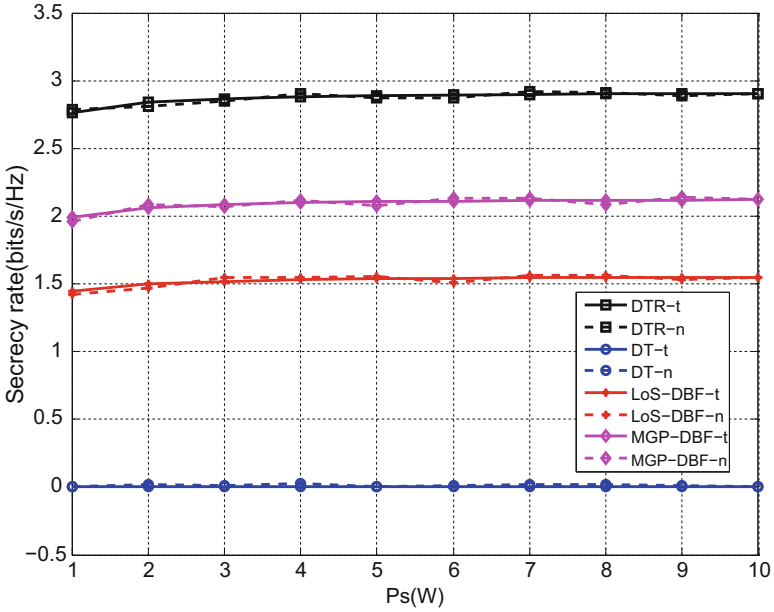


Fig. 3.15 Secrecy rate (L = 7, K = 3, $\Delta = 0$)

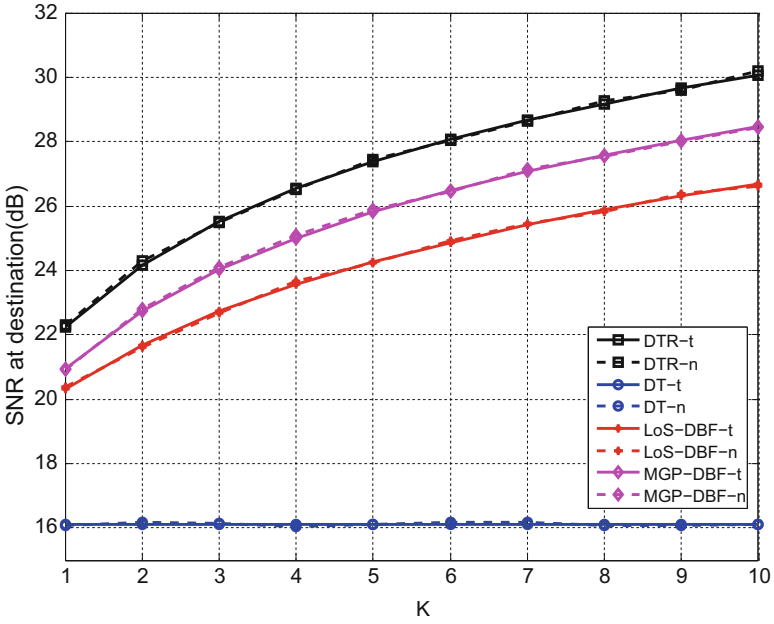


Fig. 3.16 Sampled signal SNR at destination for K distributed antennas (L = 4, P_s = 10W, $\Delta = 0$)

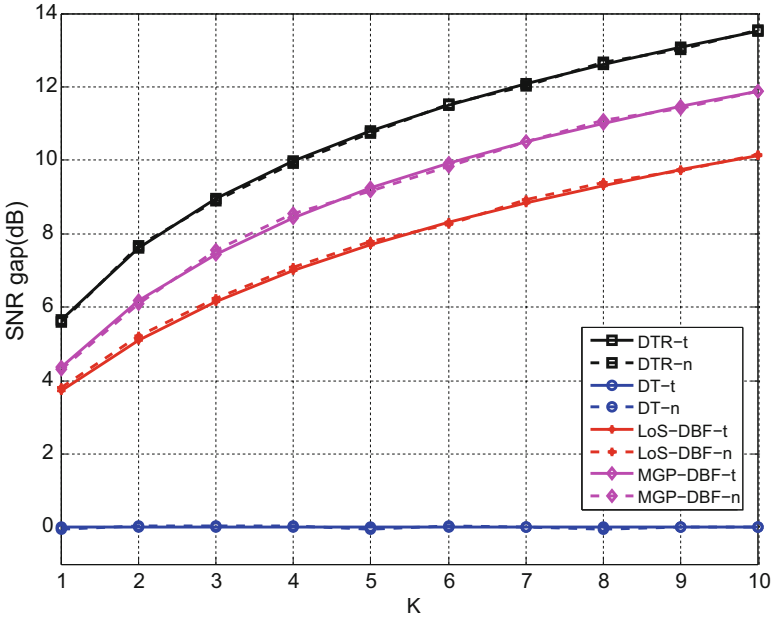


Fig. 3.17 Received signal SNR gap at destination for K distributed antennas (L $= 4$, $P_s = 10$W, $\Delta = 0$)

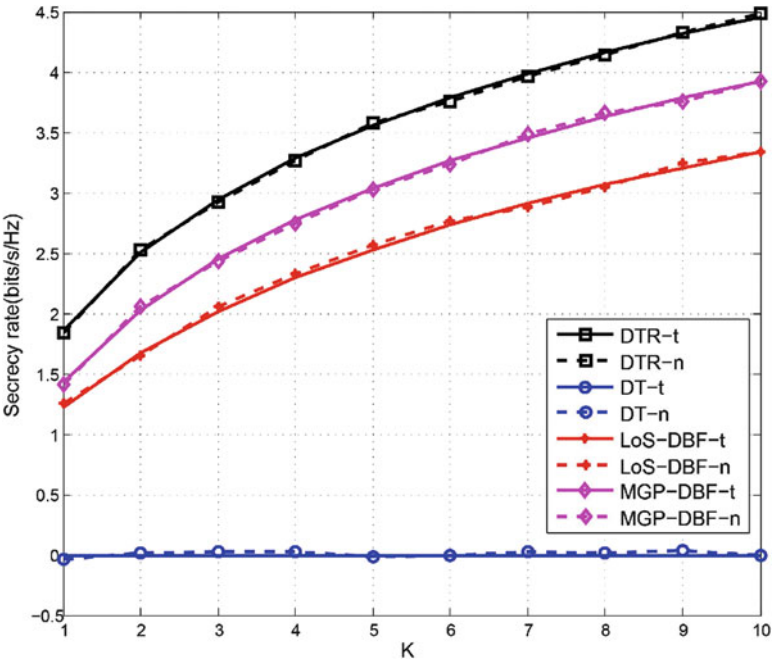


Fig. 3.18 Secrecy rate at destination for K distributed antennas (L $= 4$, $P_s = 10$W, $\Delta = 0$)

results. Not surprisingly, as the number of distributed antennas K increases, the SNR gaps for all three diversity transmission schemes increase. However, for DT, each antenna sends exactly the same pulse-shape without exploiting the diversity of the channels. As a result, a large number of distributed antennas fail to help elevate the SNR gap in direct transmission. Thus, the SNR gap for the direct transmission scheme is almost unchanged with increasing antenna diversity order K, while the SNR gap for other three schemes grow significantly for larger K. Overall, the SNR gap (and secrecy rate) for the DTR transmission scheme dominates the other three schemes. With respect to the impact of the temporal energy focusing effect by DTR, even with only $K = 2$ antennas the DTR-transmission scheme can achieve a SNR gap that is only achievable by MGP-DBF with $K = 4$ antennas or LoS-DBF with $K = 5$ antennas.

It was shown earlier that multi-path delay spread has a positive impact on DTR-based transmission, whereas the opposite is true for beamforming. This effect is illustrated more clearly by presenting another set of results where L is varied. Figures 3.19 and 3.20 compare the SNR gaps and the secrecy rates for different values of L to assess the effect of multi-path delay spread. Clearly, as L becomes larger, the SNR gaps for the DTR transmission and direct transmission schemes remain steady, while the SNR gaps for the remaining two DBF schemes decrease. Once again, the beamforming schemes suffer a larger performance loss as L grows, because the beamforming relies on one path (either dominant or LoS). As the

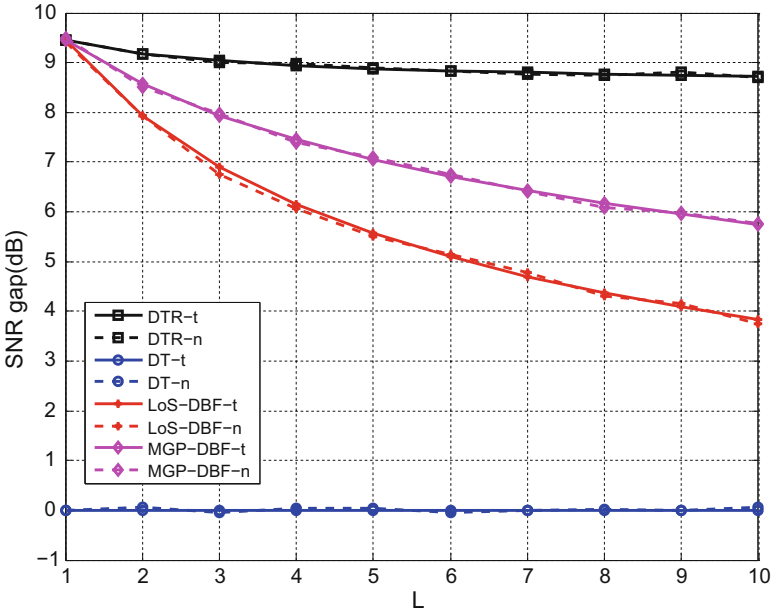


Fig. 3.19 Received SNR gap for variable L (K = 3, P_s = 10W)

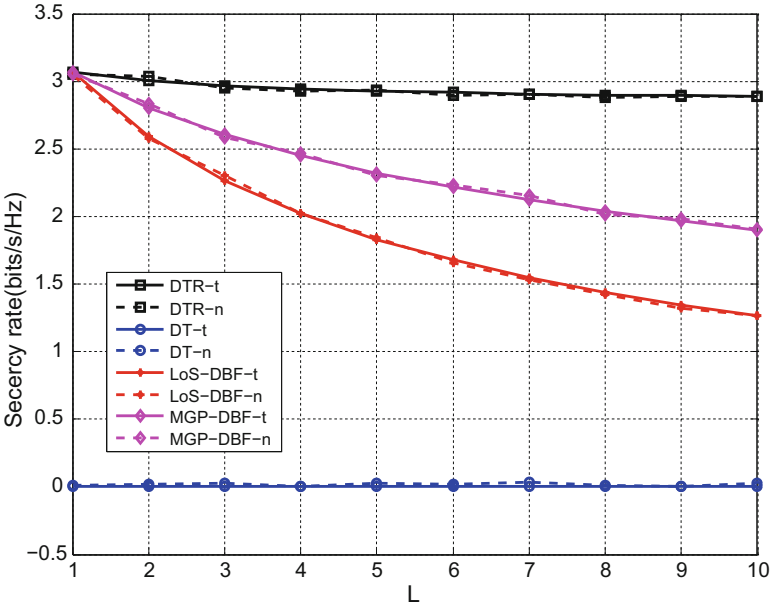


Fig. 3.20 Secrecy rate for variable L (K = 3, P_s = 10W)

number of multi-paths grows, the strength of a single path becomes relatively weaker. Hence, beamforming will increasingly rely on weaker multi-path channel gains $h_{i_0,k}$. As a result, the performance of the DBF strategies degrades as L becomes larger.

3.6 Chapter Summary

In this chapter we have analyzed the ability of distributed time-reversal (DTR) transmission to protect against unintended signal leakage to eavesdroppers. In DTR transmission, each transmit antenna individually exploits its local CSI and utilizes TR to focus signal energy at the destination receiver, by exploiting its multi-path channel to the destination receiver. The performance of DTR-based transmission, DT, LoS DBF, and MGP DBF have been analyzed and compared with respect to signal leakage, as measured by the SNR gap between the destination and unintended receivers. Numerical results have been presented that both the SNR improvement of the DTR-based transmission scheme and the validity of the performance analysis. Furthermore, given multi-path channels, DTR transmission is a much more effective signaling strategy against signal leakage to unintended receivers than traditional beamforming strategies, particularly when the number of multi-path components is large.

References

1. M. Emami, M. Vu, J. Hansen, A. J. Paulraj, and G. Papanicolaou, "Matched filtering with rate back-off for low compleity communications in very large delay spread channels," in *Proc. 2004 38th Asilomar Conference on Signals, Systems and Computers,* Pacific Grove, CA, USA, Nov. 2004, pp. 218–222.
2. C. Oestges, A. D. Kim, G. Papanicolaou, and A. J. Paulraj, "Characterization of space-time focusing in time-reversed random fields," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 1, pp. 283–293, Jan. 2005.
3. H. T. Nguyen, I. Z. Kovacs, and P. C. F. Eggers, "A time reversal transmission approach for multiuser UWB communications," *IEEE Transactions on Antennas and Propagation*, vol. 54, no. 11, pp. 3216–3224, Nov. 2006.
4. G. Lerosey, J. de Rosny, A. Tourin, A. Derode, G. Montaldo, and M. Fink, "Time reversal of electromagnetic waves," *Physical Review Letters*, vol. 92, no. 19, pp. 187–202, May. 2004.
5. H. El-Sallabi, P. Kyritsi, A. Paulraj, and G. Papanicolaou, "Experimental investigation on time reversal precoding for space-time focusing in wireless communications," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 6, pp. 1537–1543, Jun. 2010.
6. L. Wang, R. Li, C. Cao, and G. L. Stüber, "SNR analysis of time reversal signaling on target and unintended receivers in distributed transmission," *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 2176–2191, May. 2016.
7. G. L. Stüber, *Principles of Mobile Communication*, Springer, 2012.
8. K. K. Borah, R. A. Kennedy, Z. Ding, and I. Fijalkow, "Sampling and prefiltering effects on blind equalizer design," *IEEE Transactions on Signal Processing,* vol. 49, no. 1, pp. 209–218, Jan. 2001.
9. M.-S. Kim, M. Yoon, and C. Lee, "Performance analysis of a frequency-domain equal-gain-combining time-reversal scheme for distributed antenna systems," *IEEE Communications Letters*, vol. 16, no. 9, pp. 1454–1457, Sept. 2012.
10. A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
11. I. Slim, A. Mezghani, L. G. Baltar, J. Qi, and J. A. Nossek, "Frequency domain vs. time domain filter design of RRC pulse shaper for spectral confinement in high speed optical communications," in *Proc. 2013 ITG Symposium on Photonic Neworks*, Leipzig, Germany, May. 2013, pp. 1–3.
12. V. H. Rohit, Y. P. KR, V Ravichandran, S Sudhakar, S. Udupa, and N Valarmathi, "Performance analysis of root raised cosine filtering in CCSDS ACM," in *Proc. 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, Mar. 2016, pp.1750–1756.
13. I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May. 1978.
14. D.-T. Phan-Huy, S.Ben Halima, and M. Helard, "Dumb-to-perfect receiver throughput ratio maps of a time reversal wireless indoor system," in *Proc. 2013 20th International Conference on Telecommunications (ICT)*, Casablanca, Morocco, May. 2013, pp. 1–5.
15. P. Blomgren, K. Persefoni, A. D. Kim, and G. Papanicolaou, "Spatial focusing and intersymbol interference in multiple-input single-output time reversal communication systems," *IEEE Journal of Oceanic Engineering*, vol. 33, no. 3, pp. 341–355, Oct. 2008.
16. H. Nguyen, Z. Zhao, F. Zheng, and T. Kaiser, "Preequalizer design for spatial multiplexing SIMO-UWB TR systems," *IEEE Transactions on Vehicular Technology,* vol. 59, no. 8, pp. 3798–3805, Oct. 2010.
17. G. David Forney, "Maximum-likelihood sequence estimation of digital sequences in the presence of intersymbol interference," *IEEE Transactions on Information Theory*, vol. 18, no. 3, pp. 363–378, May. 1972.

18. J. Salz, “Optimum mean-square decision feedback equalization,” *Bell System Technical Journal*, vol. 52, no. 8, pp. 1341–1373, Oct. 1973.
19. T. K. Y. Lo, “Maximum ratio transmission,” *IEEE Transactions on Communications*, vol. 47, no. 10, pp. 1458–1461, Aug. 1999.
20. H. A. David and H. N. Nagaraja, *Order Statistics, Third Edition*, John Wiley and Sons, Inc., 2005.
21. L. Wang, L. Yang, X. Ma, and M. Song, “Security-oriented cooperation scheme in wireless cooperative networks,” *IET Communications*, vol. 8, no. 8, pp. 1265–1273, May. 2014.

Chapter 4
Spatial Modulation in Physical Layer Security

It has been revealed that the great capacity gains can be realized from multiple-input-multiple-output (MIMO) wireless communications [1–3]. Spatial modulation (SM), a MIMO based modulation, has recently emerged as a new transmission method which can effectively reduce the system complexity [4–7]. This chapter explores the physical layer security in SM systems. We present a secrecy rate analysis for multiple antenna receiver and eavesdropper. Targeting against passive eavesdroppers in unknown locations, we study the efficacy of active security measures through joint signal and jamming transmission without the typical requirement of eavesdropper channel information. On the other hand, under the same circumstance, we investigate the secrecy performance with space shift keying (SSK) and generalized space shift keying (GSSK), respectively. We demonstrate the tradeoff of secrecy rate and transmit power with active source jamming by testing the achieved secrecy rate and the bit error rate (BER) at different receivers, and show the different characteristics of these modulation schemes in terms of secrecy performance. Furthermore, we generalize the precoding-aided spatial modulation (PSM) to a multiuser downlink scenario. By elaborately designing the precoding vector, the proposed multiuser PSM scheme has the ability of resisting a multi-antenna eavesdropper [8–11].

4.1 Secrecy Enhancement with Artificial Noise in Spatial Modulation

4.1.1 System Model and Problem Description

We have analyzed the basic formulation of SM transmission in Chap. 2 (see Eqs. (2.7)–(2.11)). Now we consider a typical physical layer security model (Fig. 4.1) in which a transmitter Alice, a legitimate receiver Bob and an

L. Wang, *Physical Layer Security in Wireless Cooperative Networks*, Wireless Networks, DOI 10.1007/978-3-319-61863-0_4

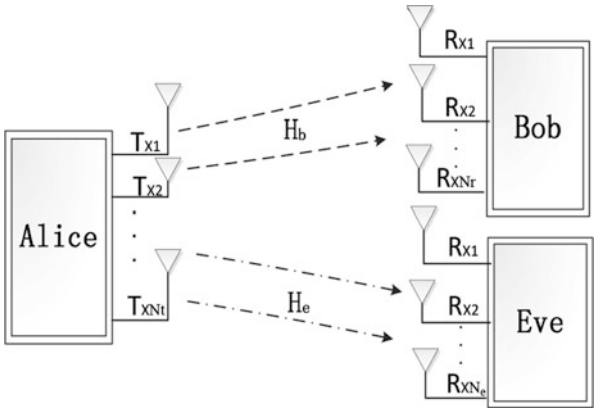


Fig. 4.1 System model of SM in physical layer security

eavesdropper Eve exist. Alice desires to transmit the confidential signal to Bob, and it is possible for Eve to intercept the information due to the broadcast characteristic of wireless channels. Note that in SM there are $L = L_1 + L_2$ transmitted bits where L_1 bits represent the index of transmit antenna chosen from $N_t = 2^{L_1}$ transmit antennas with the same probability and L_2 bits represent the modulated symbols chosen from $M = 2^{L_2}$ conventional Amplitude Phase Modulation (APM) symbols with the same probability [4].

As shown in Fig. 4.1, $\mathbf{H}_b$ and $\mathbf{H}_e$ represent the MIMO channel matrices between Alice and Bob and between Alice and Eve, respectively, whose sizes are $N_r \times N_t$ and $N_e \times N_t$, respectively. Hence the received signals at Bob and Eve are respectively expressed as

$$\mathbf{y}_b = \mathbf{H}_b\mathbf{x} + \mathbf{n}_b \quad \text{and} \quad \mathbf{y}_e = \mathbf{H}_e\mathbf{x} + \mathbf{n}_e, \tag{4.1}$$

where $\mathbf{n}_b$ and $\mathbf{n}_e$ are noise vectors at Bob and Eve, respectively.

Recall that

$$\mathbf{x} = \mathbf{s} = [0 \ldots 0 \underbrace{s_m}_{n-th} 0 \ldots 0]^T = \mathbf{e}_n s_m, \tag{4.2}$$

where $\mathbf{e}_n = [0 \ldots 0 \underbrace{1}_{n-th} 0 \ldots 0]^T$.

4.1.1.1 Artificial Noise Design

Notice that the transmitter knows channel matrix corresponding to Bob [12]. When an eavesdropper intends to intercept the transmitted data, it must find the position where transmitted symbols s_m is in the original signal $\mathbf{s}$ and decode the symbols s_m.

To prevent the transmitted data from being intercepted, we let the transmit antenna transmit not only the original signal $\mathbf{s}$ but also an artificial noise, i.e., a jamming signal vector $\mathbf{q}$ whose elements are randomly distributed. Over one single RF chains are activated through this jamming transmission, which improves the secrecy of system in a way. The data signal traverses through only one RF chain, while the jamming signal is emitted from multiple antennas. Due to the channel reciprocity, Alice is aware of Bob's channel condition, so the jamming signal can be conceived to minimize the interference to Bob. Here we assume $\text{rank}(\mathbf{H}_b) = r < N_t$.

As mentioned above, the jamming vector needs to be deliberately designed, which is described as follow. The singular value decomposition (SVD) of $\mathbf{H}_b$ is obtained as

$$\mathbf{H}_b = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H, \tag{4.3}$$

where the diagonal singular value matrix $\boldsymbol{\Sigma} = \text{Diag}\{\sigma_1, \sigma_2, \ldots, \sigma_r, \ 0 \cdots 0\}$. Since $\text{rank}(\mathbf{H}_b) = r < N_t$, it is clear that unitary matrix $\mathbf{V} = [\mathbf{v}_1 \ \mathbf{v}_2 \ \ldots \ \mathbf{v}_r \ \mathbf{v}_{r+1} \ \ldots \ \mathbf{v}_{N_t}] \in \mathscr{C}^{N_t \times N_t}$ contains the null space of $\mathbf{H}_b$, denoted as $\mathbf{V}_\perp = \left[\mathbf{v}_{r+1} \ \ldots \ \mathbf{v}_{N_t}\right]$. Thus, the transmitted signal $\mathbf{x}$ can be rewritten as

$$\mathbf{x} = \mathbf{s} + \underbrace{\left(\sum_{i=r+1}^{N_t} \alpha_i \mathbf{v}_i z_i\right)}_{\text{jamming signal } \mathbf{q}} = \mathbf{e}_n s_m + \mathbf{q}, \tag{4.4}$$

where z_i is independent and identically distributed (i.i.d.) with zero mean and σ_z variance complex Gaussian distribution, and the subspace vector $\mathbf{v}_i$ is weighted by random α_i [13]. In order to further improve the secrecy performance of the system, the weighted factor α_i is required to be randomly generated and the weight vector $\boldsymbol{\alpha} = [\alpha_{r+1}, \ \cdots, \ \alpha_{N_t}]$ is on the $(N_t - r)$-D sphere so that $\sum_{i=r+1}^{N_t} \alpha_i^2 = 1$. Thus, the jamming signal $\mathbf{q}$ satisfies $\text{E}\{\|\mathbf{q}\|^2\} = \text{E}\{\sum_{i=r+1}^{N_t} \alpha_i^2 |z_i|^2\} = \text{E}(\sum_{i=r+1}^{N_t} \alpha_i^2)\text{E}\{|z_i|^2\} = \sigma_z^2$.

The secrecy enhancement is realized by activating extra radio frequency (RF) antennas and consuming excess transmit power. Assuming $\text{E}\|s_m\|^2 = \sigma_s^2$, the total transmit power is expressed as

$$P_x = \text{E}\|\mathbf{x}\|^2 = \sigma_s^2 + \sigma_z^2. \tag{4.5}$$

Since $\mathbf{H}_b \cdot \mathbf{V}_\perp = \mathbf{0}$, we can rewrite $\mathbf{y}_b$ and $\mathbf{y}_e$ as

$$\mathbf{y}_b = \mathbf{H}_b\mathbf{s} + \mathbf{n}_b, \tag{4.6a}$$

$$\mathbf{y}_e = \mathbf{H}_e\mathbf{s} + \mathbf{H}_e\left(\sum_{i=r+1}^{N_t} \alpha_i \mathbf{v}_i z_i\right) + \mathbf{n}_e. \tag{4.6b}$$

4.1.2 Secrecy Rate Analysis

In this part, we analyze the secrecy rate of the SM communication system. Let $\mathbf{H}_b = [\mathbf{h}_1\ \mathbf{h}_2\ \cdots\ \mathbf{h}_{N_t}]$ and $\mathbf{H}_e = [\mathbf{g}_1\ \mathbf{g}_2\ \cdots\ \mathbf{g}_{N_t}]$. Recall that in each time slot, the received signal at Bob can be expressed as

$$\mathbf{y}_b = \mathbf{H}_b \mathbf{e}_n s_m = \mathbf{h}_n s_m + \mathbf{n}_b. \tag{4.7}$$

Note that the probability of selecting a certain transmit antenna is $1/N_t$ and the probability of selecting a certain symbol s_m in $M-$QAM is $1/M$. Therefore, the complex signal vector $\mathbf{y}_b$ obeys the distribution as follows [14]

$$p\left(\mathbf{y}_b\right) = \frac{1}{N_t M} \sum_{n=1}^{N_t} \sum_{m=1}^{M} \left[\frac{1}{\pi\sigma^2}\right]^{N_r} \exp\left[-\frac{\left\|\mathbf{y}_b - \mathbf{h}_n s_m\right\|^2}{\sigma^2}\right]. \tag{4.8}$$

With respect to the eavesdropper, because z_i and $\mathbf{n}_e$ are mutually independent, its interference plus noise can be expressed as $\mathbf{n}_e' = \mathbf{H}_e \cdot \left(\sum_{i=r+1}^{N_t} \alpha_i \mathbf{v}_i z_i\right) + \mathbf{n}_e$, which has zero mean and covariance matrix

$$\mathbf{R}_e = \sigma_z^2/(N_t - r)\mathbf{H}_e \cdot \left(\sum_{i=r+1}^{N_t} \mathbf{v}_i \mathbf{v}_i^H\right) \mathbf{H}_e^H + \sigma^2 \mathbf{I}. \tag{4.9}$$

Thus, we whiten the noise as

$$\mathbf{y}_e = \mathbf{g}_n s_m + \mathbf{n}_e'. \tag{4.10}$$

In this way, the mutual information $I\left(\mathbf{y}_e; [\mathbf{g}_n,\ s_m]\right)$ will not be affected.

Besides, we adopt a linear whitening transformation matrix $\mathbf{P} = \sigma \mathbf{R}_e^{-1/2}$ to whiten the jamming signal plus noise, resulting in

$$\mathbf{y}_e' = \underbrace{\mathbf{P}\mathbf{g}_n}_{\mathbf{g}_n'} s_m + \underbrace{\mathbf{P}\mathbf{n}_e'}_{\mathbf{n}_\epsilon} = \mathbf{g}_n' s_m + \mathbf{n}_\epsilon, \tag{4.11}$$

where $\mathbf{n}_\epsilon$ has covariance matrix $\sigma^2\mathbf{I}$. Notice that Eve needs to know Bob's channel to conceive such a whitening filter. If $\boldsymbol{\alpha}$ has been determined, then $\mathbf{n}_\epsilon$ obeys i.i.d. Gaussian distribution. Therefore, we can know $p\left(\mathbf{y}_e'\right) = \frac{1}{N_t M} \sum_{n=1}^{N_t} \sum_{m=1}^{M} \left(\frac{1}{\pi\sigma^2}\right)^{N_e} \exp\left[-\frac{\left\|\mathbf{y}_e' - \mathbf{g}_n' s_m\right\|^2}{\sigma^2}\right]$. Similar to [7], we let

$$\mathbf{d}_{n,m}^{n_2,m_2} = \mathbf{h}_n s_m - \mathbf{h}_{n_2} s_{m_2}, \tag{4.12}$$

$$\boldsymbol{\delta}_{n,m}^{n_2,m_2} = \mathbf{P}\left(\mathbf{g}_n s_m - \mathbf{g}_{n_2} s_{m_2}\right), \tag{4.13}$$

$$I(\mathbf{y}_b;[\mathbf{h}_n,\ s_m]) = \int \sum_n \sum_m p(\mathbf{y}_b,\mathbf{h}_n,s_m)\log_2\frac{p(\mathbf{y}_b,\mathbf{h}_n,s_m)}{p(\mathbf{y}_b)p(\mathbf{h}_n,s_m)}d\mathbf{y}_b \tag{4.14a}$$

$$= \frac{1}{MN_t}\sum_n\sum_m\int p(\mathbf{y}_b|\mathbf{h}_n,s_m)\log_2\frac{p(\mathbf{y}_b,|\mathbf{h}_n,s_m)}{p(\mathbf{y}_b)}d\mathbf{y}_b \tag{4.14b}$$

$$= \frac{1}{MN_t}\sum_n\sum_m\int p(\mathbf{y}_b|\mathbf{h}_n,s_m)\log_2\frac{MN_t\cdot p(\mathbf{y}_b,|\mathbf{h}_n,s_m)}{\sum_{n_2}\sum_{m_2}p(\mathbf{y}_b|\mathbf{h}_{n_2},s_{m_2})}d\mathbf{y}_b \tag{4.14c}$$

$$= \log_2 MN_t - \frac{1}{MN_t} \sum_n\sum_m\int p(\mathbf{y}_b|\mathbf{h}_n,s_m)\log_2\frac{\sum_{n_2}\sum_{m_2}p(\mathbf{y}_b|\mathbf{h}_{n_2},s_{m_2})}{p(\mathbf{y}_b,|\mathbf{h}_n,s_m)}d\mathbf{y}_b \tag{4.14d}$$

$$= \log_2 MN_t - \frac{1}{MN_t}\sum_{n=1}^{N_t}\sum_{m=1}^{M} \mathrm{E}_{\mathbf{n}_b}\left[\log_2\left(\sum_{n_2=1}^{N_t}\sum_{m_2=1}^{M}\exp\left(-\frac{1}{\sigma^2}\left[\left\|\mathbf{d}_{n,m}^{n_2,m_2}+\mathbf{n}_b\right\|^2-\|\mathbf{n}_b\|^2\right]\right)\right)\right], \tag{4.14e}$$

$$I\left(\mathbf{y}_e;[\mathbf{g}_n,\ s_m]\right) = I\left(\mathbf{y}_e';[\mathbf{g}_n',\ s_m]\right)$$

$$= \log_2 MN_t - \frac{1}{MN_t}\sum_{n=1}^{N_t}\sum_{m=1}^{M} \mathrm{E}_{\mathbf{n}_\epsilon}\left[\log_2\left(\sum_{n_2=1}^{N_t}\sum_{m_2=1}^{M}\exp\left(-\frac{1}{\sigma^2}\left(\left\|\boldsymbol{\delta}_{n,m}^{n_2,m_2}+\mathbf{n}_\epsilon\right\|^2-\|\mathbf{n}_\epsilon\|^2\right)\right)\right)\right], \tag{4.14f}$$

from Eqs. (4.14a)–(4.14f), the secrecy rate finally can be written as

$$R_s = \max\{0, I\left(\mathbf{y}_b;[\mathbf{h}_n,\ s_m]\right) - I\left(\mathbf{y}_e;[\mathbf{g}_n,\ s_m]\right)\}. \tag{4.15}$$

The ergodic secrecy rate can be calculated by the equation $\bar{R}_s = \mathrm{E}\{R_s\}$ over multiple channel realizations. Here our simulation results mainly consider the ensemble of Rayleigh flat fading channels.

4.1.3 Simulation and Numerical Results

In this section, we show the ergodic secrecy rate of (4.15) with different antenna configurations, signal-to-noise ratio (SNR), and excess jamming power to analyze their effects on the secrecy rate. Besides, we present the BER performance at Bob and Eve, respectively. Particularly, we mainly consider the randomly generated Rayleigh flat fading channels in the simulation.

At first, the modulated signal power is normalized to unity (σ_s^2=1) and the additive complex white Gaussian noise power is denoted as σ^2, so the SNR can be expressed as SNR $= \sigma_s^2/\sigma^2$. Besides, the jamming power is denoted as $\sigma_z^2 = \beta$, so the full transmission power can be written as $P_x = \sigma_s^2 + \sigma_z^2 = 1 + \beta$, where β is the excess power for secrecy enhancement at Bob. Since the active jamming power β is used for the generation of a random signal that exists in the nullspace of Bob's channel, Bob will never be interfered by the excess signal. However, because Eve's channel is almost impossible to be the same as Bob's, Eve's channel will suffer from a severe deterioration due to the jamming signal so that the system can finally guarantee security.

4.1.3.1 Secrecy Rate

Figure 4.2 presents the secrecy rate R_s of QPSK symbol by statistical evaluation with $N_t = 6$ and $N_r = 2$. We consider Eve with $N_e = 1, 3, 5$ antennas, respectively. The final simulation results are averaged over 100 random samples of $\boldsymbol{\alpha}$. In all 3 cases, as SNR increases, the secrecy rate grows steadily firstly and reaches a saturation point later. With respect to β, higher excess jamming power β leads to higher secrecy rate. As the number of receiver antenna at Eve increases, the secrecy rate will decrease apparently because additional antennas at Eve increase the probability of successful eavesdropping to some extent. Note that although Eve is equipped with 4 antennas, the secrecy rate is still very high with $\beta = 1$. Therefore, active jamming can improve the secrecy rate significantly.

The aforementioned simulation results are demonstrated again when 16QAM is employed, and thereinto $N_t = 4, N_r = 2, N_e = 1, 3$ in Fig. 4.3 and $N_t = 8, N_r = 4$, $N_e = 3, 5$ in Fig. 4.4. Note that higher dimensional APM yields both higher data rate and higher secrecy rate.

4.1.3.2 BER

To further illustrate the effects of active jamming on Eve's channel, we compare the BER performance at Bob with that at Eve when 16QAM signals are employed. Particularly, elements of $\boldsymbol{\alpha}$ are randomly generated in the simulation. Note that the jamming signal deteriorates the Eve's observation and degrades the eavesdropping channel. Besides, Eve will still gain relatively lower BER if it is equipped with enough antennas.

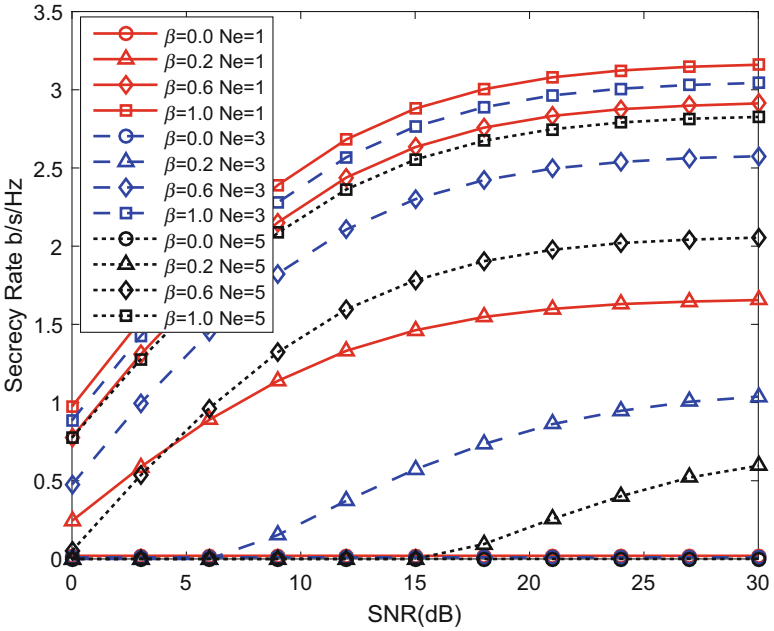


Fig. 4.2 Secrecy rate under QPSK: $N_t = 6$, $N_r = 2$, and $N_e = 1, 3, 5$

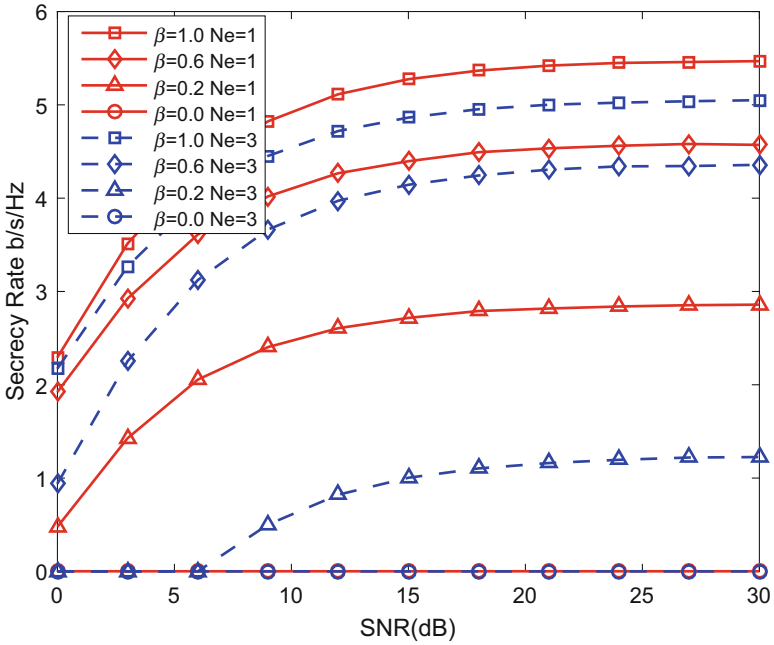


Fig. 4.3 Secrecy rate under 16QAM: $N_t = 4$, $N_r = 2$, and $N_e = 1, 3$

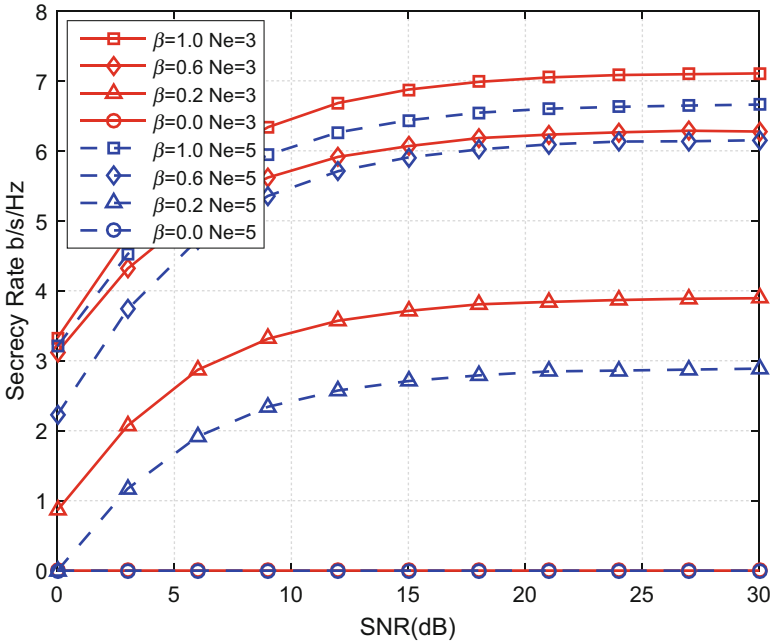


Fig. 4.4 Secrecy rate under 16QAM: $N_t = 8$, $N_r = 4$, and $N_e = 3, 5$

Figure 4.5 presents the simulation results of BER with $N_t = 4$, $N_r = 2$ and $N_e = 2$ or 4. Assume that there are two receivers at Eve. As mentioned before, Eve is unaware of Bob's channel in general, denoted as Eve (U). We also suppose another situation where Eve is aware of Bob's CSI, denoted as Eve (A). We see that when the receiver configuration are the same, the Eve's channel is largely degraded, while the performance of Bob's receivers are still unaffected. Besides, Even if the Eve's diversity is larger than Bob's, its channel can be greatly degraded with enormous jamming power.

Figure 4.6 further shows the receiver performance with $N_t = 8$ and $N_r = 4$. Both Eve (A) and Eve (U) are shown with $N_e = 4$ and $N_e = 8$, respectively. The final results are same with the previous simulation results in Fig. 4.5. These results verify that the channel degradation at Eve's receiver helps improve the secrecy capacity.

4.2 Secrecy Analysis in Space Shift Keying (SSK) and Generalized Space Shift Keying (GSSK) Modulation

In this section, the security issues in physical layer with SSK and GSSK modulations are shown [15]. We aim to show the difference in terms of the performance of physical layer security compared with conventional SM. Specifically, we are interested in the tradeoff between secrecy capacity and transmit power with the variance of the number of activated RF antenna chains in SSK and GSSK.

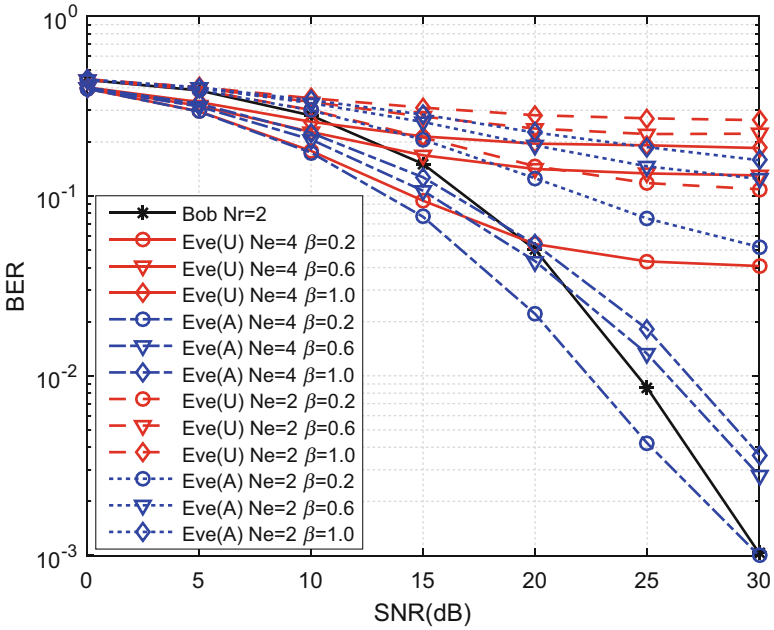


Fig. 4.5 BER of 16QAM for Bob and Eve: $N_t = 4$, $N_r = 2$, and $N_e = 2, 4$ for Eve (U) unaware and Eve (A) aware of Bob's CSI, respectively

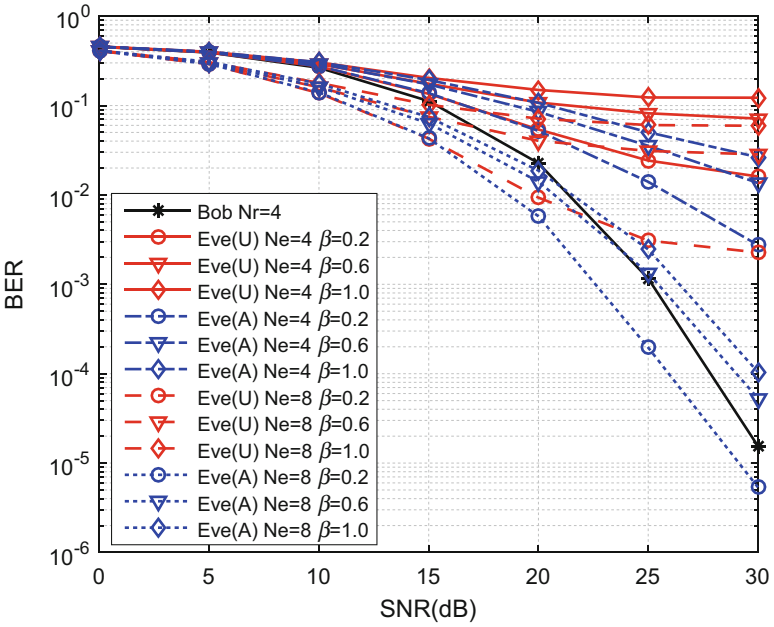


Fig. 4.6 BER of 16QAM for Bob and Eve: $N_t = 8$, $N_r = 4$, and $N_e = 4, 8$ for Eve (U) unaware and Eve (A) aware of Bob's CSI, respectively

4.2.1 System Model and Problem Description

The system model is the same as Sect. 4.1.1. We also assume that the transmitter has prior knowledge of the channel corresponding to Bob, $\mathbf{H}_b$. Now we give some details about the secrecy enhancement design of SSK and GSSK, respectively.

4.2.1.1 SSK

Recall that in each time epoch, the input data vector $\mathbf{x}$ has only a single non-zero entry, i.e., $\mathbf{x} = \mathbf{s} = [0 \ \cdots \ 0 \ \ 1 \ 0 \ \cdots \ 0]^T = \mathbf{e}_n$, where $\mathbf{e}_n$ is the unit vector whose n-th entry is non-zero. The goal of the receiver is only to detect which antenna is active.

We analyze the artificial noise design in SSK, similarly as that in SM. Here we also assume that $\text{rank}(\mathbf{H}_b) = r < N_t$. The SVD of $\mathbf{H}_b$ is obtained as $\mathbf{H}_b = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H$, where the diagonal singular value matrix $\boldsymbol{\Sigma} = \text{Diag}\{\sigma_1, \sigma_2, \ldots, \sigma_r, \ 0 \ \cdots \ 0\}$. Since $\text{rank}(\mathbf{H}_b) = r < N_t$, it is clear that unitary matrix $\mathbf{V} = [\mathbf{v}_1 \ \mathbf{v}_2 \ \ldots \ \mathbf{v}_r \ \mathbf{v}_{r+1} \ \ldots \ \mathbf{v}_{N_t}] \in \mathscr{C}^{N_t \times N_t}$ contains thenull space of $\mathbf{H}_b$, denoted as $\mathbf{V}_\perp = \left[\mathbf{v}_{r+1} \ \ldots \ \mathbf{v}_{N_t}\right]$. Thus, the transmitted signal $\mathbf{x}$ can be rewritten as

$$\mathbf{x} = \mathbf{s} + \underbrace{\left(\sum_{i=r+1}^{N_t} \alpha_i \mathbf{v}_i z_i\right)}_{\text{jamming signal } \mathbf{q}} = \mathbf{e}_n + \mathbf{q}, \tag{4.16}$$

where z_i is independent and identically distributed (i.i.d.) with zero mean and σ_z variance complex Gaussian distribution, and the subspace vector $\mathbf{v}_i$ is weighted by α_i. In order to further improve the secrecy of system, the weighted factor α_i is required to be randomly generated and the weight vector $\boldsymbol{\alpha} = [\alpha_{r+1}, \ \cdots, \ \alpha_{N_t}]$ is on the $(N_t - r)$-D sphere so that $\sum_{i=r+1}^{N_t} \alpha_i^2 = 1$. Thus, the jamming signal $\mathbf{q}$ satisfies $\text{E}\{\|\mathbf{q}\|^2\} = \text{E}\{\sum_{i=r+1}^{N_t} \alpha_i^2 |z_i|^2\} = \text{E}(\sum_{i=r+1}^{N_t} \alpha_i^2)\text{E}\{|z_i|^2\} = \sigma_z^2$.

The secrecy enhancement is realized by activating extra RF antennas and consuming excess transmit power.

Assuming $\text{E}\|s\|^2 = \sigma_s^2$, the total transmit power is expressed as

$$P_x = \text{E}\|\mathbf{x}\|^2 = \sigma_s^2 + \sigma_z^2. \tag{4.17}$$

Because $\mathbf{H}_b \cdot \mathbf{V}_\perp = \mathbf{0}$, we can rewrite $\mathbf{y}_b$ and $\mathbf{y}_e$ as

$$\mathbf{y}_b = \mathbf{H}_b \mathbf{e}_\mathbf{n} + \mathbf{n}_b, \tag{4.18a}$$

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{e}_\mathbf{n} + \mathbf{H}_e\left(\sum_{i=r+1}^{N_t} \alpha_i \mathbf{v}_i z_i\right) + \mathbf{n}_e. \tag{4.18b}$$

4.2.1.2 GSSK

Recall that in each time epoch, the input data vector $\mathbf{x}$ has n_t non-zero entries, i.e., $\mathbf{x} = \mathbf{x}_j$, where $\mathbf{x}_j = [\frac{1}{\sqrt{n_t}}\ 0\ \cdots\ 0\ \frac{1}{\sqrt{n_t}}\ 0\ \cdots\ 0\ \frac{1}{\sqrt{n_t}}\ \cdots\ 0]^T$ is the vector that has n_t non-zero entries [4].

The GSSK detector estimates the antenna indices that are used, and demaps the symbol to its component bits. Similarly, using the SVD of the channel matrix $\mathbf{H}_b$, after generating the jamming signal $\mathbf{q}$, we can rewrite $\mathbf{y}_b$ and $\mathbf{y}_e$ as

$$\mathbf{y}_b = \mathbf{H}_b\mathbf{x}_j + \mathbf{n}_b \quad \text{and} \quad \mathbf{y}_e = \mathbf{H}_e\mathbf{x}_j + \mathbf{H}_e\Big(\sum_{i=r+1}^{N_t} \alpha_i \mathbf{v}_i z_i\Big) + \mathbf{n}_e. \tag{4.19}$$

4.2.2 Secrecy Rate Analysis

4.2.2.1 SSK Modulation

Let $\mathbf{H}_b = [\mathbf{h}_1\ \mathbf{h}_2\ \cdots\ \mathbf{h}_{N_t}]$ and $\mathbf{H}_e = [\mathbf{g}_1\ \mathbf{g}_2\ \cdots\ \mathbf{g}_{N_t}]$. Recall that in each time epoch, Bob receives signal

$$\mathbf{y}_b = \mathbf{H}_b\mathbf{e}_n = \mathbf{h}_n + \mathbf{n}_b. \tag{4.20}$$

Each transmit antenna is selected with probability of $1/N_t$. Thus, the complex signal vector has distribution [14]

$$p\left(\mathbf{y}_b\right) = \frac{1}{N_t}\sum_{n=1}^{N_t}\left[\frac{1}{\pi\sigma^2}\right]^{N_r}\exp\left[-\frac{\|\mathbf{y}_b - \mathbf{h}_n\|^2}{\sigma^2}\right]. \tag{4.21}$$

We now consider the eavesdropper receiver. Because z_i and $\mathbf{n}_e$ are independent, the interference plus noise equals $\mathbf{n}'_e = \mathbf{H}_e \cdot \left(\sum_{i=r+1}^{N_t} \alpha_i \mathbf{v}_i z_i\right) + \mathbf{n}_e$, which has zero mean and covariance matrix

$$\mathbf{R}_e = \sigma_z^2/(N_t - r)\mathbf{H}_e \cdot \left(\sum_{i=r+1}^{N_t} \mathbf{v}_i\mathbf{v}_i^H\right)\mathbf{H}_e^H + \sigma^2\mathbf{I}. \tag{4.22}$$

Thus, without effects on the mutual information $I\left(\mathbf{y}_e; \mathbf{g}_n\right)$, the noise can be whitened as

$$\mathbf{y}_e = \mathbf{g}_n + \mathbf{n}'_e. \tag{4.23}$$

Besides, we adopt a linear whitening transformation matrix $\mathbf{P} = \sigma\mathbf{R}_e^{-1/2}$ to whiten the jamming signal plus noise, resulting in

$$\mathbf{y}'_e = \underbrace{\mathbf{P}\mathbf{g}_n}_{\mathbf{g}'_n} + \underbrace{\mathbf{P}\mathbf{n}'_e}_{\mathbf{n}_\epsilon} = \mathbf{g}'_n + \mathbf{n}_\epsilon, \tag{4.24}$$

such that $\mathbf{n}_\epsilon$ has covariance matrix $\sigma^2\mathbf{I}$. If $\boldsymbol{\alpha}$ is deterministic, then $\mathbf{n}_\epsilon$ is i.i.d. Gaussian. In this case, we have $p\left(\mathbf{y}'_e\right) = \frac{1}{N_t}\sum_{n=1}^{N_t}\left(\frac{1}{\pi\sigma^2}\right)^{N_e}\exp\left[-\frac{\|\mathbf{y}'_e-\mathbf{g}'_n\|^2}{\sigma^2}\right]$. Similar to the derivation of [7], by defining

$$\mathbf{d}_n^{n_2} = \mathbf{h}_n - \mathbf{h}_{n_2}, \tag{4.25}$$

$$\boldsymbol{\delta}_n^{n_2} = \mathbf{P}\left(\mathbf{g}_n - \mathbf{g}_{n_2}\right), \tag{4.26}$$

$$I(\mathbf{y}_b;\mathbf{h}_n) = \int\sum_n p(\mathbf{y}_b,\mathbf{h}_n)\log_2\frac{p(\mathbf{y}_b,\mathbf{h}_n)}{p(\mathbf{y}_b)p(\mathbf{h}_n)}d\mathbf{y}_b \tag{4.27a}$$

$$= \log_2 N_t - \frac{1}{N_t}\sum_{n=1}^{N_t}\mathrm{E}_{\mathbf{n}_b}\left[\log_2\left(\sum_{n_2=1}^{N_t}\exp\left(-\frac{1}{\sigma^2}\left[\left\|\mathbf{d}_n^{n_2}+\mathbf{n}_b\right\|^2-\|\mathbf{n}_b\|^2\right]\right)\right)\right]. \tag{4.27b}$$

$$I\left(\mathbf{y}_e;\mathbf{g}_n\right) = I\left(\mathbf{y}'_e;\mathbf{g}'_n\right) \tag{4.27c}$$

$$= \log_2 N_t - \frac{1}{N_t}\sum_{n=1}^{N_t}\mathrm{E}_{\mathbf{n}_\epsilon}\left[\log_2\left(\sum_{n_2=1}^{N_t}\exp\left(-\frac{1}{\sigma^2}\left(\left\|\boldsymbol{\delta}_n^{n_2}+\mathbf{n}_\epsilon\right\|^2-\|\mathbf{n}_\epsilon\|^2\right)\right)\right)\right]. \tag{4.27d}$$

From Eqs. (4.27a)–(4.27d) as shown above, we can find the secrecy rate as

$$R_s = \max\{0, I\left(\mathbf{y}_b;\mathbf{h}_n\right) - I\left(\mathbf{y}_e;\mathbf{g}_n\right)\}. \tag{4.28}$$

4.2.2.2 GSSK Modulation

In each time epoch of GSSK modulation, Bob receives the signal [16]

$$\mathbf{y}_b = \mathbf{H}_b\mathbf{x}_j = \mathbf{h}_{j,eff} + \mathbf{n}_b, \tag{4.29}$$

where $\mathbf{h}_{j,eff} = \mathbf{h}_{j(1)} + \mathbf{h}_{j(2)} + \ldots + \mathbf{h}_{j(n_t)}$ specifies the column index of $\mathbf{H}_b$. We refer to $\mathbf{h}_{j,eff}$ as an effective column, which represents the sum of n_t distinct columns in $\mathbf{H}_b$. Each antenna combination index in set χ is selected with probability of $1/M$, Thus, the complex signal vector has distribution [14]

$$p\left(\mathbf{y}_b\right) = \frac{1}{M}\sum_{j=1}^{M}\left[\frac{1}{\pi\sigma^2}\right]^{N_r}\exp\left[-\frac{\left\|\mathbf{y}_b-\mathbf{h}_{j,eff}\right\|^2}{\sigma^2}\right]. \tag{4.30}$$

Applying a linear whitening transformation matrix $\mathbf{P}$ on $\mathbf{y}_e$ to whiten the jamming signal plus noise, leads to

$$\mathbf{y}'_e = \underbrace{\mathbf{P}\mathbf{g}_{j,eff}}_{\mathbf{g}'_{j,eff}} + \underbrace{\mathbf{P}\mathbf{n}'_e}_{\mathbf{n}_\epsilon} = \mathbf{g}'_{j,eff} + \mathbf{n}_\epsilon. \tag{4.31}$$

The secrecy rate of GSSK becomes

$$R_s = \max\{0, I\left(\mathbf{y}_b; \mathbf{h}_{j,eff}\right) - I\left(\mathbf{y}_e; \mathbf{g}_{j,eff}\right)\}. \tag{4.32}$$

4.2.3 Simulation and Numerical Results

In this section, we numerically evaluate and compare the performance of these three schemes, i.e., SM, SSK, GSSK, with different configurations, SNR, signal power and jamming power. We perform 5×10^3 independent trials of Monte Carlo experiments to obtain the average results. We also provide some simulation results to demonstrate BER performance with maximum likelihood receivers employed at both Bob and Eve under active jamming.

To begin, we set the modulated signal power as σ_s^2. Without any loss of generality, we assume equal additive complex white Gaussian noise power level at receivers of both Bob and Eve, and the noise power is σ^2 to achieve the required SNR $= \sigma_s^2/\sigma^2$. We also set the jamming power as $\sigma_u^2 = \rho$. Recall that the full transmission power $P_x = \sigma_s^2 + \rho$=1, in which ρ is used to enhance secrecy for Bob. Active jamming power ρ is applied to generate a random signal that lies in the nullspace of Bob's channel, and Bob is immune to this jamming signal. On the other hand, Eve's receiver will suffer from this intentional jamming since its channel is unlikely to coincide with Bob's channel. For this reason, higher ρ is expected to yield higher secrecy rate and also higher BER for Eve.

4.2.3.1 Secrecy Rate

SSK: In Fig. 4.7, [1] we depict statistical evaluation of (4.28), with $N_t = 8$ and $N_r = 4$. We consider Eve with different number of antennas. In particular, we let $N_e = 4, 8$, respectively. We achieve the ergodic secrecy rate over 100 random samples of α. We denote ρ/σ_s^2 as the jamming power and modulated signal power ratio. It can be observed that the secrecy rate steadily grows towards a saturation point as SNR increases. The higher the ratio, the higher the secrecy rate. Larger

[1] Note that all the curves below including 4.7 we obtained in our simulation process are at a given SNR using different amount of transmit power P for different jamming power, and referring the question of the optimal jamming power as future work, as stated in the Conclusions section.

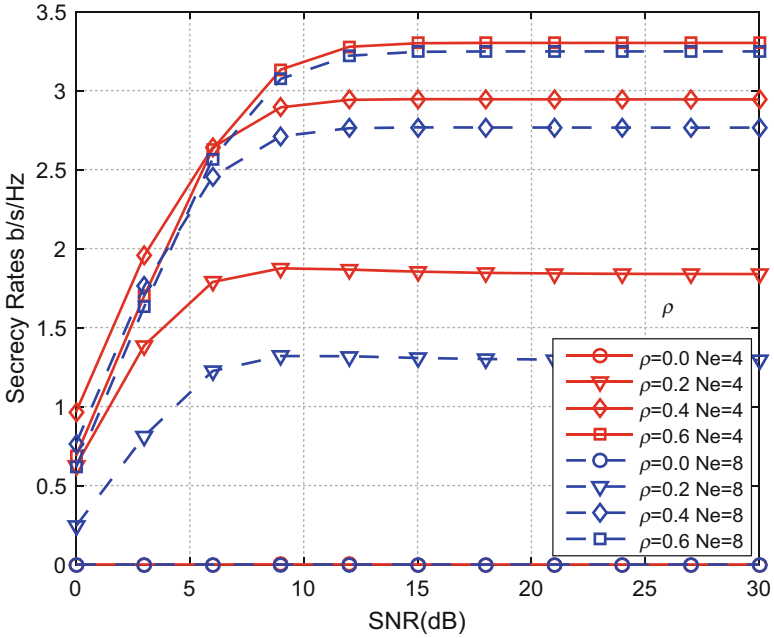


Fig. 4.7 Secrecy rate for SSK: $N_t = 8$, $N_r = 4$, and $N_e = 4, 8$

number of receive antennas by Eve can clearly reduce the secrecy rate since Eve becomes more powerful. Still, with $\rho = 0.5, \rho/\sigma_s^2 = 1$, the secrecy rate when Eve has 8 antennas versus Bob's 4 antennas remains very high. Hence, active jamming is effective in improving the secrecy rate.

SM: The secrecy rate R_s for finite alphabet QPSK signals when $N_t = 8$, $N_r = 4$ and $N_e = 4, 8$ is show in Fig. 4.8. We average the secrecy rate over 100 random samples of α as above. These results are also reaffirmed.

GSSK: In Fig. 4.9, we consider $N_t = 7$, the number of active transmit antennas $n_t = 2$ and Eve with different number of antennas $N_e = 4, 8$. We find that the secrecy rate has similar trend as for the above two schemes.

Finally, we give the secrecy rate of these three modulations under jamming power $\rho = 0.4$ in Fig. 4.10. We note that the secrecy rate of SSK is lower than that of SM under the same antenna configuration. This is because SSK uses only the indices of transmit antennas to convey information while SM convey information through the signal-constellation diagram and the spatial constellation diagram. The secrecy rate of GSSK falls into the range of SSK and SM. The reason is that GSSK only exploits the spatial constellation diagram but is capable of achieving higher data rate as well as higher secrecy rate than SSK by activating more transmit antennas.

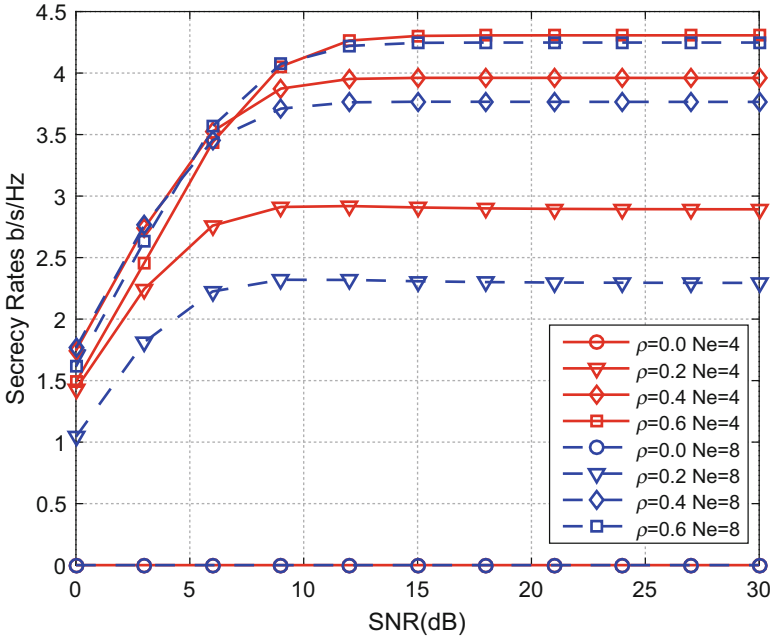


Fig. 4.8 Secrecy rate for SM: QPSK, $N_t = 8$, $N_r = 4$, and $N_e = 4, 8$

4.2.3.2 BER

To illustrate the degradation of Eve's channel by active jamming, we assume that both Bob and Eve employ ML receivers and compare the BER performance of the three schemes in Fig. 4.11. We average the BER over 100 random samples of $\boldsymbol{\delta}$ and 8400 random binary bits.

In Fig. 4.11, all results for Bob and Eve are shown for $N_r = 4$, $N_e = 4$ with $\rho = 0.4$, it can be observed that the BER of SSK is lowest, and SM's BER is lower than GSSK's. This is because SSK only demodulates the index of the transmit antennas so it can obtain higher accuracy rate. Compared to SSK, SM needs to demodulate the index of the transmit antennas and the modulated signals, and GSSK should demodulate the index of antenna combination.

4.3 Secrecy Analysis with Transmitter Precoding Aided Spatial Modulation

Apart from SM mentioned above, which carries information exploiting the transmit spatial constellation diagram [17], there are also cases exploiting the receive spatial constellation diagram, namely precoding aided spatial modulation (PSM).

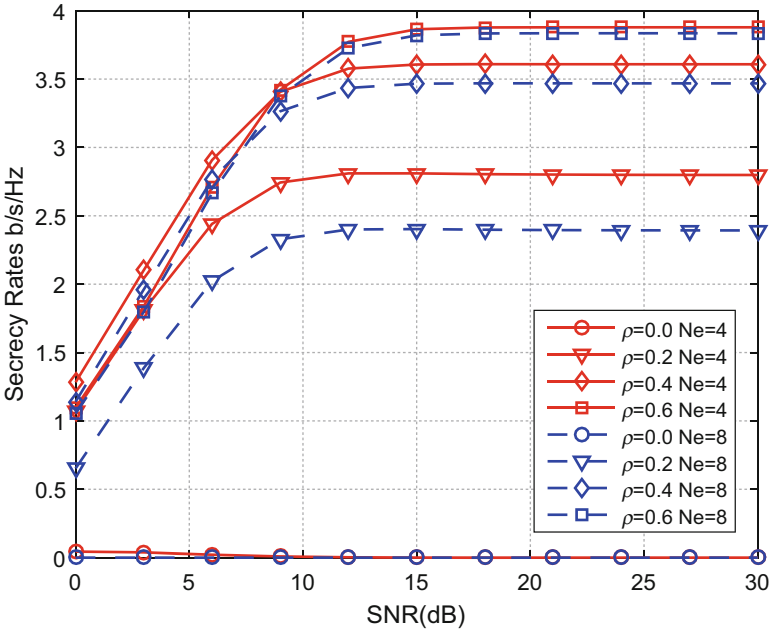


Fig. 4.9 Secrecy rate for GSSK: $N_t = 7$, $n_t = 2$, $N_r = 4$, and $N_e = 4, 8$

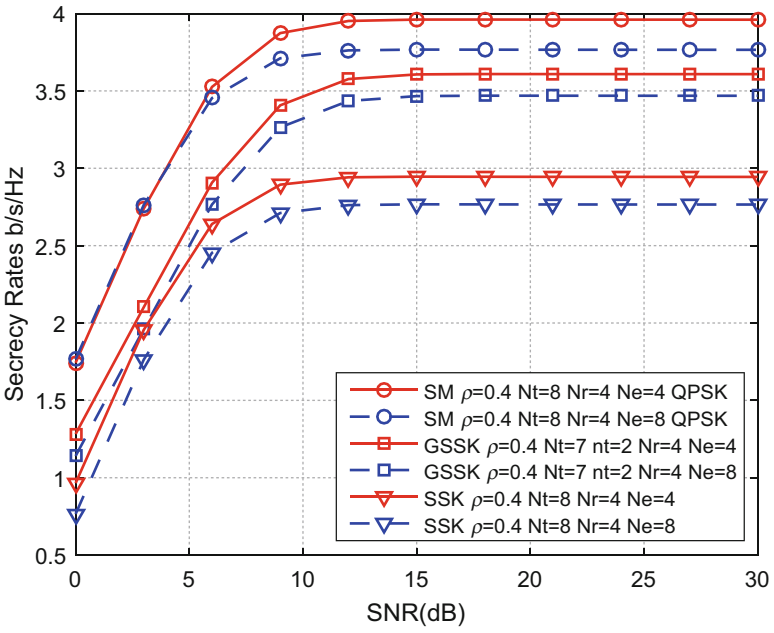


Fig. 4.10 Secrecy rate for SM SSK GSSK: $N_r = 4$, and $N_e = 4, 8$

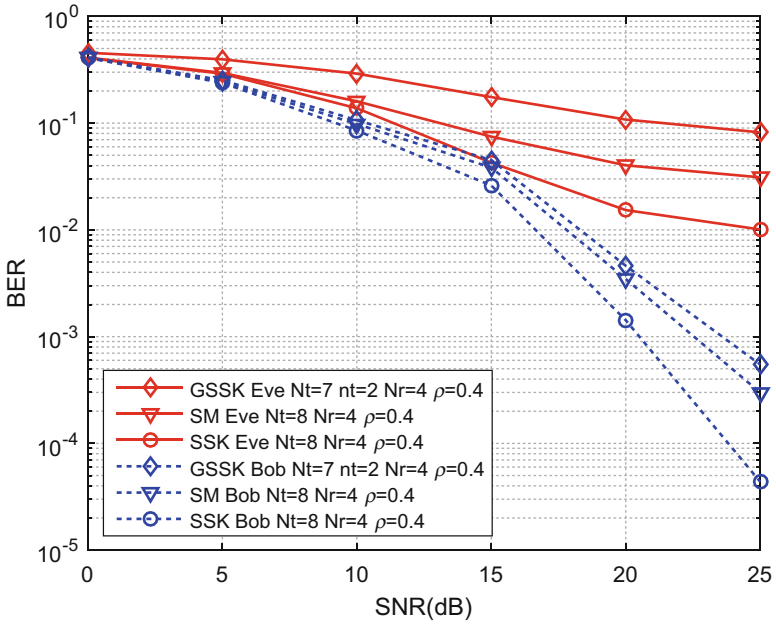


Fig. 4.11 BER of SM, SSK, GSSK for Bob and Eve: $N_r = 4$, and $N_e = 4$

It is also demonstrated that PSM can achieve a good secrecy rate and overall BER performance to combat the eavesdropping if designed properly. Hence it is meaningful to study the achievable performance of PSM communication system. To be more specific, in the following section, we will illustrate the principles, consider the precoding matrix design, as well as study the achievable secrecy rate and bit-error-rate (BER) performance of the PSM [10].

4.3.1 System Model and Problem Description

In this subsection, we study a MIMO downlink scenario with multiuser, where there is one transmitter (Alice) and more than two legitimate receivers (Bobs). Alice is equipped with N_a transmit antennas and every Bob exploits $N_k \geqslant 2$ receive antennas. Besides, there is an authorized passive eavesdropper (Eve) with N_e receive antennas intercepting the data for the k-th Bob, where $k \in \{1, 2, \cdots, K\}$. In the multiuser PSM data transmission scheme, sectional signal bits are carried by the indices of each Bob's receive antennas, while the other bits are made up with M_k-ary amplitude-phase modulation (APM). Consequently, a PSM super symbol consists of one block of $\log_2(N_k M_k)$ bits, where the signal transmitted to the k-th Bob can be written as

$$\mathbf{s}_k = \mathbf{e}_k^i b_k^j, \tag{4.33}$$

where $\mathbf{e}_k^i$ is the i-th column of the identity matrix $\mathbf{I}_{N_k}$, indicating the i-th receive antenna of the k-th Bob is activated. b_k^j is the j-th symbol in the M_k-ary APM, whose power is normalized to unity. All the possible super symbols transmitted to the k-th Bob are from the set $\mathbb{Q}_k$, which satisfy $\|\mathbb{Q}_k\| = N_k M_k$. Here, the total super symbol sent by Alice is denoted by $\mathbf{s} = \left[\mathbf{s}_1^T \cdots \mathbf{s}_k^T \cdots \mathbf{s}_K^T\right]^T$.

We set $\sum_{k=1}^{K} N_k = N_b$ and let $\mathbf{H} \in \mathbb{C}^{N_b \times N_a}$ and $\mathbf{G} \in \mathbb{C}^{N_e \times N_a}$ denote the channel matrices between Alice and Bobs and between Alice and Eve, respectively. Denote $\mathbf{H}$ as

$$\mathbf{H} = \left[\mathbf{H}_1^T \cdots \mathbf{H}_k^T \cdots \mathbf{H}_K^T\right]^T, \tag{4.34}$$

where $\mathbf{H}_k \in \mathbb{C}^{N_k \times N_a}$ is the channel matrix between Alice and the k-th Bob. Assume that CSIT is available and Alice is unaware of Eve's CSI . We assume that channels experience block fading and will not change in one block interval.

4.3.2 Precoding Matrix Design

We need to design the precoding matrix precisely to implement the secure multiuser PSM scheme. At first, different from the point-to-point communication system, partial information bits should be modulated according to some indices of receiver antennas at Bob [18]. Second, the cancellation of co-channel interference is necessary. Besides, a fast-varying scrambling matrix is designed to improve the security of communication system. Therefore, we design the precoding matrix from three parts as follows.

4.3.2.1 Multiuser Interference Cancellation

In the multiuser communication system, the signal to interference plus noise ratio (SINR) of the intended receivers will be much degraded by multiuser interference [19, 20]. Because the locations of receiver are far away from each other, it is impossible for these users to cooperate to cancel multiuser interference. Thus, it is valid to cancel multiuser interference in way of precoding at transmitter. In the multiuser PSM scheme, we adopt block diagonalization (BD) at transmitter to guarantee that each channel between Alice and Bob cannot be interfered by other channels. We let the procedure of determining the total BD matrix be $\mathbf{F} = [\mathbf{F}_1 \cdots \mathbf{F}_k \cdots \mathbf{F}_K]$, where $\mathbf{F}_k \in \mathbb{C}^{N_a \times N_k}$ is the BD matrix for the k-th Bob. To cancel multiuser interference, we suppose that $\mathbf{H}_l \mathbf{F}_k = 0$ if $l \neq k$. The $\tilde{\mathbf{H}}_k \in \mathbb{C}^{(N_b - N_k) \times N_a}$ can be defined as

$$\tilde{\mathbf{H}}_k = \left[\mathbf{H}_1^T \cdots \mathbf{H}_{k-1}^T \; \mathbf{H}_{k+1}^T \cdots \mathbf{H}_K^T\right]^T, \tag{4.35}$$

since $\mathbf{H}_l\mathbf{F}_k = 0$ for $l \neq k$, $\mathbf{F}_k$ will be in the null space of $\tilde{\mathbf{H}}_k$. If the null space of $\tilde{\mathbf{H}}_k$ exists, data can be transmitted to the k-th Bob. when $N_a \geqslant N_b$ and $\mathbf{H}$ has a full row rank, this condition will be satisfied, so the singular value decomposition (SVD) of $\tilde{\mathbf{H}}_k$ can be written as

$$\tilde{\mathbf{H}}_k = \tilde{\mathbf{U}}_k \tilde{\boldsymbol{\Sigma}}_k [\tilde{\mathbf{V}}_k^{(1)} \ \tilde{\mathbf{V}}_k^{(0)}]^H, \tag{4.36}$$

where $\tilde{\mathbf{U}}_k \in \mathbb{C}^{(N_b-N_k)\times(N_b-N_k)}$ is the left singular matrix of $\tilde{\mathbf{H}}_k$ and $\tilde{\boldsymbol{\Sigma}}_k \in \mathbb{C}^{(N_b-N_k)\times N_a}$ is a rectangular matrix with its diagonal consisting of the singular values of $\tilde{\mathbf{H}}_k$. Matrices $\tilde{\mathbf{V}}_k^{(1)} \in \mathbb{C}^{N_a\times(N_b-N_k)}$ and $\tilde{\mathbf{V}}_k^{(0)} \in \mathbb{C}^{N_a\times N_k}$ respectively indicate the right singular matrices corresponding to the nonzero singular values and zero singular values of $\tilde{\mathbf{H}}_k$. Note that $\tilde{\mathbf{V}}_k^{(0)}$ forms the null space of $\tilde{\mathbf{H}}_k$ and its columns are the basis for the BD matrix $\mathbf{F}_k$. Therefore, $\mathbf{F}_k$ can be expressed as

$$\mathbf{F}_k = \tilde{\mathbf{V}}_k^{(0)} \mathbf{W}_k, \tag{4.37}$$

where $\mathbf{W}_k \in \mathbb{C}^{N_k\times N_k}$ is an arbitrary matrix satisfying $\mathbf{W}_k\mathbf{W}_k^H = \mathbf{I}_{N_k}$. To optimize and increase the information rate at Bobs, we weight $\tilde{\mathbf{V}}_k^{(0)}$ by water-filling on the corresponding singular values [21]. Hence, the SVD on $\mathbf{H}_k\tilde{\mathbf{V}}_k^{(0)}$ is written as

$$\mathbf{H}_k\tilde{\mathbf{V}}_k^{(0)} = \bar{\mathbf{U}}_k \bar{\boldsymbol{\Sigma}}_k \bar{\mathbf{V}}_k^H, \tag{4.38}$$

where $\bar{\mathbf{U}}_k \in \mathbb{C}^{N_k\times N_k}$ and $\bar{\mathbf{V}}_k \in \mathbb{C}^{N_k\times N_k}$ are unitary matrices while $\bar{\boldsymbol{\Sigma}}_k \in \mathbb{C}^{N_k\times N_k}$ is a diagonal matrix with the singular values of $\mathbf{H}_k\tilde{\mathbf{V}}_k^{(0)}$. Obviously, the BD matrix $\mathbf{F}_k$ can be obtained as

$$\mathbf{F}_k = \tilde{\mathbf{V}}_k^{(0)} \bar{\mathbf{V}}_k. \tag{4.39}$$

It is easy to notice that the equivalent channel matrices between Alice and each Bob, i.e. $\mathbf{H}_k\mathbf{F}_k$, are both square matrices, whose elements never change during one block interval.

4.3.2.2 Precoding-Aided Spatial Modulation

To make sure that the activated receive antenna can carry partial information, Alice precodes every super symbol $\mathbf{s}_k$ into $\mathbf{A}_k\mathbf{s}_k$ before the procedure of BD. Let $\mathbf{A}_k \in \mathbb{C}^{N_k\times N_k}$ indicate the PSM matrix specially designed for the k-th Bob. Make sure that only one k-th Bob's receive antennas is activated and the other antennas will transmit zero power. This requirement can be met by a zero-forcing precoder

$$\mathbf{A}_k = (\mathbf{H}_k\mathbf{F}_k)^{-1}. \tag{4.40}$$

According to the design of PSM matrices and BD matrices, the signal precoding matrix (SPM) for the k-th Bob rests with $\mathbf{F}_k\mathbf{A}_k$. To guarantee that the power of each column in SPM is normalized to unity, $\mathbf{F}_k\mathbf{A}_k$ needs to be normalized by the matrix $\boldsymbol{\beta}_k \in \mathbb{C}^{N_k \times N_k}$ expressed as

$$\boldsymbol{\beta}_k = \text{Diag}\left\{\left[(\mathbf{F}_k\mathbf{A}_k)_i^H (\mathbf{F}_k\mathbf{A}_k)_i\right]^{-\frac{1}{2}}, i = 1, \cdots, N_k\right\}. \tag{4.41}$$

Hence, from (4.39)–(4.41), the SPM for the k-th Bob can be expressed as $\mathbf{M}_k = \boldsymbol{\beta}_k\mathbf{F}_k\mathbf{A}_k$ and the whole SPM after normalization is denoted by $\mathbf{M} = [\mathbf{M}_1 \cdots \mathbf{M}_k \cdots \mathbf{M}_K]$.

As mentioned above, when Alice communicates with Bob, the equivalent channel matrices will not change during one coherent block duration. Hence, there is only one precoding vectors for Alice to choose when the same receive antenna at the k-th Bob is activated. Despite the transmission in the main links can operate normally, it is still hard to guarantee the security of data since Eve can gather the homologous signals to perform an estimation blindly. If Eve exactly obtains the CSI of main links, it can coherently infer not only the activated antenna number but also the APM symbol. At that time, the secrecy performance of communication system will be degraded largely.

4.3.2.3 Fast-Varying Scrambling on SPMs

According to the foregoing analysis, it is shown that the more knowledge of SPMs Eve collects, the security of multiuser PSM system is more difficult to guarantee. However, it is necessary for Eve to gather the transmitted sequences statistics to perform the blind estimation. In other words, Eve will probably retrieve the data through the blind estimation when the channels stay static during one coherent block interval or plenty symbol durations. Otherwise, Eve is almost impossible to retrieve the original transmitted sequences. In order to further decrease the probability of successful eavesdropping, we come up with a fast-varying scrambling procedure to deteriorate the blind estimation at Eve. Especially, the SVD on $\mathbf{H}$ can be written as

$$\mathbf{H} = \mathbf{U}\boldsymbol{\Sigma}[\mathbf{V}^{(1)} \ \mathbf{V}^{(0)}]^H, \tag{4.42}$$

where $\mathbf{V}^{(0)} \in \mathbb{C}^{N_a \times (N_a - N_b)}$ is the null space of $\mathbf{H}$. Then, a scrambling matrix $\mathbf{T}$ can be designed as $\mathbf{T} = \mathbf{V}^{(0)}\mathbf{R}$ [22], where $\mathbf{R} \in \mathbb{C}^{(N_a - N_b) \times N_b}$ is a matrix whose elements are complex Gaussian random variables with zero mean and unit variance. The symbols in $\mathbf{R}$ keep time-varying and independent. Therefore, compared with $\mathbf{M}$, $\mathbf{T}$ is fast-varying. So the final precoding matrix can be obtained as

$$\mathbf{P} = \alpha_1\mathbf{M} + \alpha_2\mathbf{T}, \tag{4.43}$$

where $\alpha_1 = \sqrt{\theta K}$, $\alpha_2 = \sqrt{(1-\theta)K}$, and θ $(0 < \theta \leqslant 1)$ is a power allocation factor. Let K be the total transmit power. Then the power allocated to Alice-Bob links is θK, while the rest power, $1 - \theta K$, is distributed for scrambling. Let the final transmitted signal at Alice be $\mathbf{x} = \mathbf{Ps}$, where $\mathbf{s}$ is the total super symbol. The received signals at the k-th Bob and Eve can be written as follows, respectively.

$$\mathbf{y}_k = \alpha_1 \mathbf{H}_k \mathbf{M}_k \mathbf{s}_k + \mathbf{n}_k, \tag{4.44}$$

$$\mathbf{z} = \mathbf{GPs} + \mathbf{n}_e, \tag{4.45}$$

where $\mathbf{n}_k \in \mathbb{C}^{N_k \times 1}$ and $\mathbf{n}_e \in \mathbb{C}^{N_e \times 1}$ are complex Gaussian noise vectors distributed with zero mean and covariance matrices $\sigma^2 \mathbf{I}_{N_k}$ and $\sigma^2 \mathbf{I}_{N_e}$, respectively. According to (4.44), it is clear that Bob encounters an equivalent block fading channel without multiuser interference. Besides, the signals received by the k-th Bob seem to be only processed by $\alpha_1 \mathbf{M}_k$. On the contrary, Eve is greatly influenced by the fast-varying precoder $\mathbf{P}$, which largely decreases the precision of blind estimation.

4.3.3 Secrecy Performance with Detection Algorithm

In this subsection, we will respectively introduce the detection algorithms for Bob and Eve in multiuser PSM. Then, we will derive the lower bound of secrecy performance and demonstrate the tradeoff between channel security and reliability.

4.3.3.1 Detection Algorithms

In practical application, a suboptimal detecting method is applied at Bob [23]. Candidate receive antenna index $\hat{i}$ and APM symbol index $\hat{j}$ are respectively determined by [24]

$$\begin{aligned} \hat{i} &= \arg \max_{i \in \{1,2,\cdots,N_k\}} \left| y_k^i \right|, \\ \hat{j} &= \arg \min_{j \in \{1,2,\cdots,M_k\}} \left| y_k^{\hat{i}} - b_k^j \right|, \end{aligned} \tag{4.46}$$

where y_k^i is the i-th element of the column vector $\mathbf{y}_k$. Significantly, there is no need for legitimate receivers to be aware of the precoding matrix at the transmitter.

As for Eve, let $\mathbf{P}_k = \alpha_1 \mathbf{M}_k + \alpha_2 \mathbf{T}_k$ and $\mathbf{T} = [\mathbf{T}_1 \cdots \mathbf{T}_k \cdots \mathbf{T}_K]$, where $\mathbf{T}_k \in \mathbb{C}^{N_a \times N_k}$ for $k \in \{1, 2, \cdots, K\}$. As mentioned previously, the design of $\mathbf{T}_k$ largely prevents Eve from a valid blind estimation. However, we take the worst situation into consideration here, where Eve totally knows the SPM $\mathbf{M}_k$ through blind estimation. Despite this, Eve still never know $\mathbf{P}_k$ because of the existence of $\mathbf{T}_k$. Eve performs the optimal detection called maximum likelihood detection, which is different from the Bob's suboptimal detection. Candidate receive antenna index $\hat{i}$ and APM symbol

index $\hat{j}$ are determined according to

$$\left(\hat{i},\hat{j}\right) = \arg \min_{\substack{i\in\{1,\cdots,N_k\}\\ j\in\{1,\cdots,M_k\}}} \left\| \mathbf{z} - (\mathbf{G}\mathbf{M}_k)_i b_k^j \right\|. \tag{4.47}$$

At last, we will compare the fast-varying scrambling with slow-varying scrambling to further clarify its effects on secrecy. For the design of $\mathbf{T}$, $\mathbf{R}$ is a matrix whose elements are randomly generated per block interval with zero mean and unit variance complex Gaussian distribution. Hence, $\mathbf{P}$ becomes a slow-varying precoder whose elements never change while transmitting one block symbols. It is likely for Eve to know about $\mathbf{P}_k$ through blind estimation to improve the accuracy of detection in slow-scrambling scheme.

4.3.3.2 Secrecy Performance

We take secrecy rate as the standard for the security of communication system here [25]. The k-th Bob's information rate is expressed as [26]

$$R_{b,k}(\theta) = \log_2 N - \frac{1}{N}\sum_{\tau=1}^{N} \mathrm{E}_{\mathbf{Q}_k,\mathbf{n}_k}\left[\log_2\left(\sum_{\varepsilon=1}^{N}\exp \Phi\right)\right], \tag{4.48}$$

where $N \triangleq N_k M_k$ and Φ is given by

$$\Phi = \frac{\|\mathbf{n}_k\|^2 - \left\|\mathbf{Q}_k\left(\mathbf{s}_k^{\tau} - \mathbf{s}_k^{\varepsilon}\right) + \mathbf{n}_k\right\|^2}{\sigma^2}, \tag{4.49}$$

where $\mathbf{Q}_k \triangleq \alpha_1 \mathbf{H}_k \mathbf{M}_k$, while $\mathbf{s}_k^{\tau}$ and $\mathbf{s}_k^{\varepsilon}$ indicate possible super symbols in $\mathbb{Q}_k$. So (4.45) can be written as

$$\mathbf{z} = \alpha_1 \mathbf{G}\mathbf{M}_k \mathbf{s}_k + \underbrace{\alpha_2 \mathbf{G}\mathbf{T}_k \mathbf{s}_k + \mathbf{G}\sum\nolimits_{i\neq k} \mathbf{P}_i \mathbf{s}_i + \mathbf{n}_e}_{\mathbf{w}}, \tag{4.50}$$

in which $\mathbf{w}$ is the sum of the multiuser interference, scrambling interference, and thermal noise, which has zero mean and a covariance matrix $\boldsymbol{\Omega} = \mathrm{E}(\mathbf{w}\mathbf{w}^H)$. By multiplying $\boldsymbol{\Omega}^{-1/2}$ on both sides of (4.50), Eve applies a linear whitening transformation on $\mathbf{z}$, resulting in

$$\underbrace{\boldsymbol{\Omega}^{-1/2}\mathbf{z}}_{\mathbf{z}'} = \underbrace{\boldsymbol{\Omega}^{-1/2}\mathbf{G}\mathbf{M}_k}_{\mathbf{G}'}\mathbf{s}_k + \underbrace{\boldsymbol{\Omega}^{-1/2}\mathbf{w}}_{\mathbf{w}'}, \tag{4.51}$$

where $\mathbf{w}'$ is Gaussian distributed with an unit covariance matrix $\mathbf{I}_{N_e}$. It needs to emphasize that we conduct such whitening procedure because Eve acquires the SPM $\mathbf{M}_k$, which is the worst case. Same as the Bob's information rate as (4.48), the Eve's information rate can be formulated as

$$R_e(\theta) = \log_2 N - \frac{1}{N}\sum_{\tau=1}^{N} \mathrm{E}_{\mathbf{G}',\mathbf{w}'}\left[\log_2\left(\sum_{\varepsilon=1}^{N}\exp \Psi\right)\right], \tag{4.52}$$

where Ψ is given by

$$\Psi = \left\|\mathbf{w}'\right\|^2 - \left\|\mathbf{G}'\left(\mathbf{s}_k^{\tau} - \mathbf{s}_k^{\varepsilon}\right) + \mathbf{w}'\right\|^2. \tag{4.53}$$

Finally, from (4.48) to (4.52), the secrecy rate of the k-th Bob in the multiuser PSM scheme with power allocation factor can be expressed as

$$R_s(\theta) = \max\left\{0, R_{b,k}(\theta) - R_e(\theta)\right\}. \tag{4.54}$$

In a word, when allocating the power of $(1-\theta)K$ for scrambling, its effects are twofold. Considering $\theta \ll 1$, Eve's blind estimation is likely to experience a severer deterioration so that the communication system can achieve a higher secrecy rate. Meanwhile, BER performance of Bobs is degraded. When θ is close to 1, the final results are totally opposite. That is to say, there is a tradeoff between system security and channel reliability.

4.3.4 Simulation and Numerical Results

In the simulation scenario, the multiuser PSM scheme employs one Alice with $N_a = 25$ transmit antennas and $K = 4$ Bobs with $N_k = 4$ receive antennas. We discuss Eve equipped with $N_e = 3,\ 5,\ 7$ receive antennas, respectively. The elements of the channel matrices are independent and identically distributed (i.i.d), and are randomly generated per channel use with zero mean and unit variance complex Gaussian distribution. We assume that 100 symbols are transmitted during one channel realization. If the transmit power of each Alice-Bob link is θ, the SNR is expressed as θ/σ^2. Especially, let the same APM applied to all Bobs for convenience. We make Alice transmit QPSK, 16PSK, and 16QAM symbols, respectively.

Figures 4.12, 4.13, 4.14, 4.15, and 4.16 show the secrecy rate versus SNR with different APMs, N_e and θ values. In all cases, we observe that the secrecy rate grows steadily and then reaches a saturation with SNR increasing. In addition, the larger N_e, the more powerful eavesdropping capacity and the lower secrecy rate. The designed scheme can still guarantee the security of transmission with sufficient SNR values even if Eve has more antennas than Bob. With respect to the influence of θ, for most SNR values, the lower value of θ, the better secrecy performance. It indicates that little transmit power is enough for main links to achieve the upper bound rate in good channel condition. So if we allocate more power for scrambling, the secrecy rate will be greatly increased and the security of communication system will be improved. Instead, when the channel quality is extremely degraded, higher θ leads to higher secrecy rate, because legitimate channels need more power to transmit data. Specially, although there is little power for scrambling, multiuser PSM can still achieve the positive secrecy rate as Eve's observation is greatly interfered by multi-stream transmission.

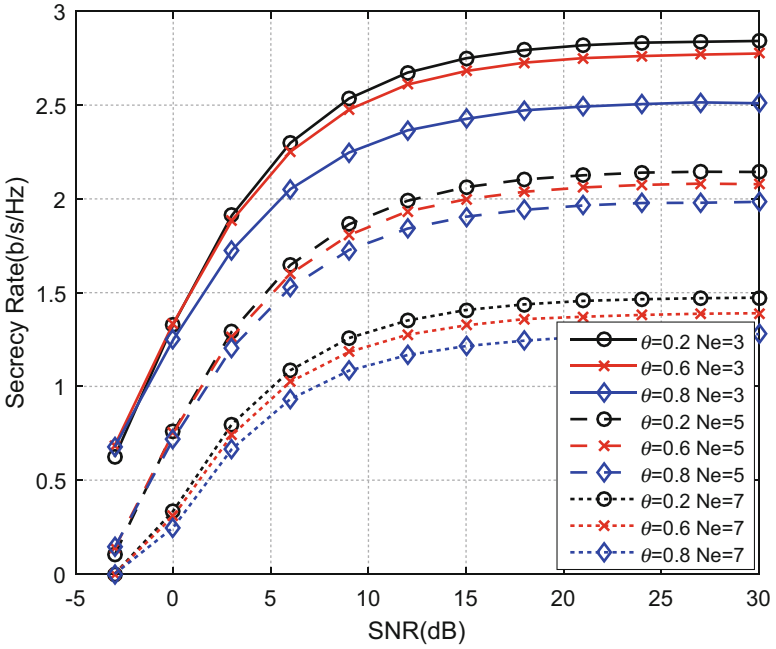


Fig. 4.12 Secrecy rates with different N_e and θ when QPSK is employed

These conclusions can also be confirmed in Figs. 4.12, 4.13, and 4.14, indicating QPSK signal, 16PSK signal and 16QAM signal, respectively. From these figures, we notice that higher dimensional APM achieves higher secrecy rate. Therefore, we can change the order of APM according to different security requirements at Bobs rather than adapt the number of receive antennas.

Figures 4.15 and 4.16 present the BER versus SNR with different APMs, conditions of scrambling and θ values. Clearly, the lower order of APM, the better BER performance for both Bob and Eve. Compared with Eve, Bob always performs much better in BER. The BER of Eve is dramatically high (closing to 1/2), which is helpful to guarantee secure transmission. Besides, the Alice-Bob links and Alice-Eve links both improve their own reliability with θ increasing for the reason that more transmit power is allocated to the main links and Eve's channels are less degraded than before. Furthermore, we also test the BER with different modulation modes. In Fig. 4.16, it is shown that the system employing 16QAM has a better performance than 16PSK because the minimum Euclidean distance of 16QAM is less than 16PSK.

In order to further illustrate the improvement on secrecy created by fast-scrambling, we compare its BER with the BER of a slow-scrambling scheme and show the results in Fig. 4.17. Let (F) and (S) denote fast-scrambling scheme and slow-scrambling scheme, respectively. From Fig. 4.17, we can see that only when $\theta = 1$, which means there is no power allocated for scrambling, these two schemes

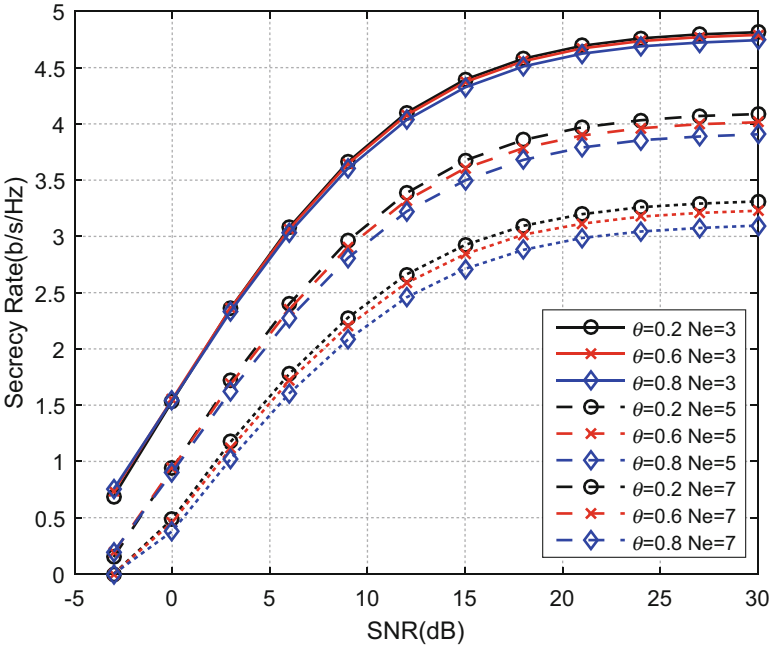


Fig. 4.13 Secrecy rates with different N_e and θ when 16PSK is employed

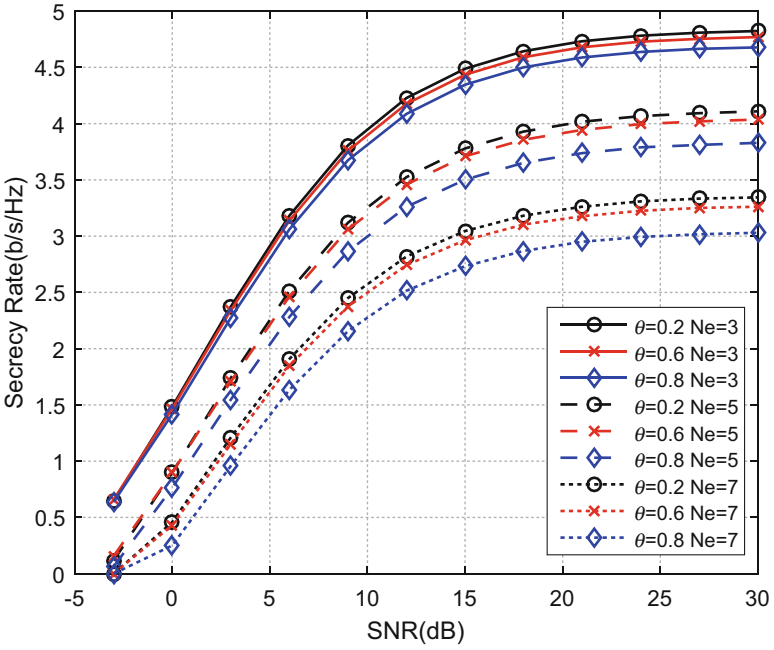


Fig. 4.14 Secrecy rates with different N_e and θ when 16QAM is employed

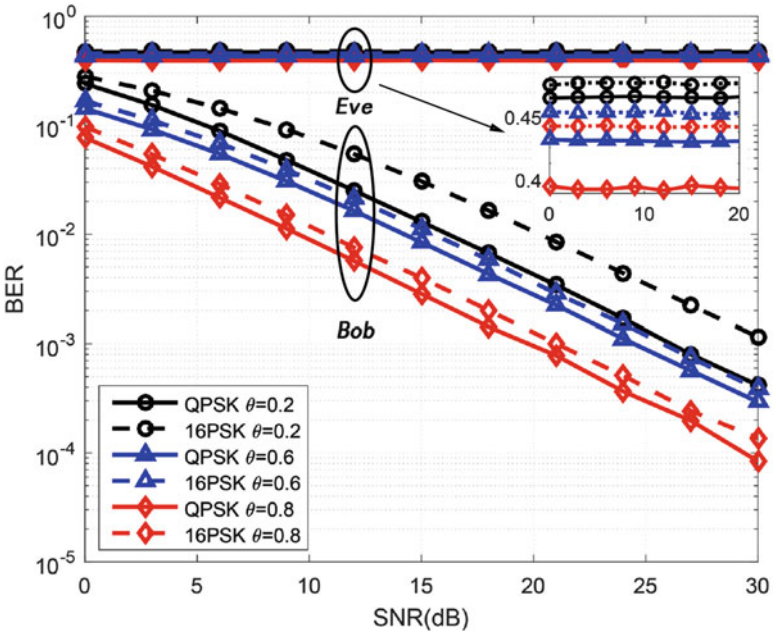


Fig. 4.15 Comparison between Bob and Eve with different θ when QPSK and 16PSK are employed

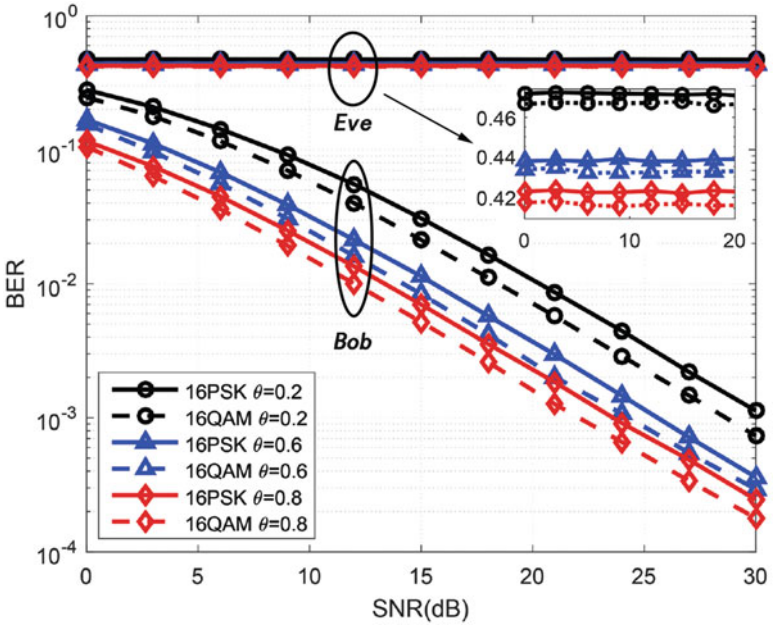


Fig. 4.16 Comparison between Bob and Eve with different θ when 16PSK and 16QAM are employed

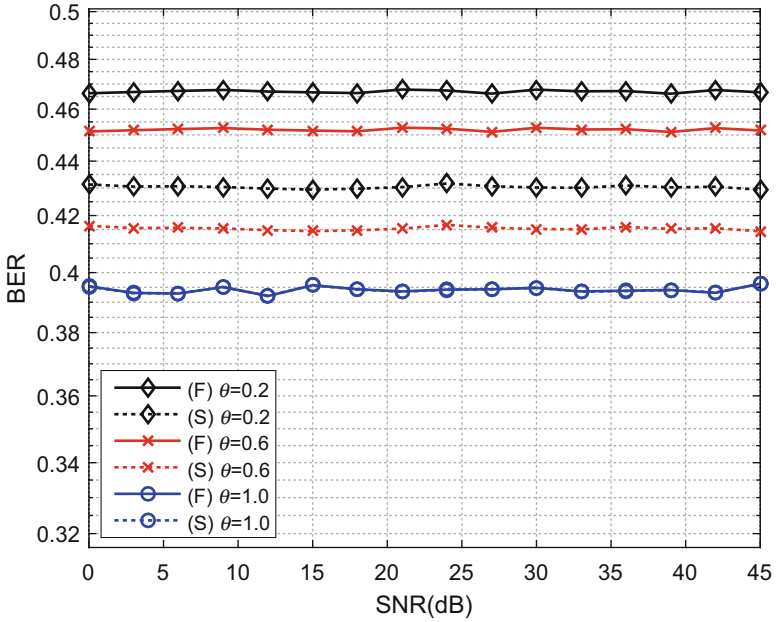


Fig. 4.17 Eve's performance with different θ and scrambling schemes when QPSK is employed

possess the same BER performance. As for other θ values, Eve in (F) possesses the higher BER than that in (S). That is to say, compared with slow-scrambling scheme, fast-scrambling scheme degrades the Eve's accuracy of blind estimation and thus achieves secrecy improvement.

4.4 Chapter Summary

This chapter has studied physical layer security in terms of secrecy rate for SM-MIMO transmissions. We have analyzed the secrecy rate of a simple and practical method for secrecy enhancement by exploiting the spatial diversity of the SM-MIMO system without eavesdropper channel information. We have demonstrated successful improvement of secrecy rate and the improved BER simulation results for multi-antenna users. Future works may target the optimization of power allocation between signal transmission and jamming by freezing the total transmit power.

References

1. J. Mietzner, R. Schober, L. Lampe, W. H. Gerstacker, and P. A. Hoeher, "Multiple-antenna techniques for wireless communications — A comprehensive literature survey," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 2, pp. 87–105, Second Quarter 2009.
2. F. Rusek *et al.*, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 40–60, Jan. 2013.
3. F. Heliot, M. A. Imran, and R. Tafazolli, "On the energy efficiency-spectral efficiency trade-off over the MIMO rayleigh fading channel," *IEEE Transactions on Communications*, vol. 60, no. 5, pp. 1345–1356, May. 2012.
4. R. Y. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2228–2241, Jul. 2008.
5. M. Di Renzo and H. Haas, "Bit error probability of SM-MIMO over generalized fading channels," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 3, pp. 1124–1144, Mar. 2012.
6. M. Di Renzo, H. Haas, A. Ghrayeb, S. Sugiura, and L. Hanzo, "Spatial modulation for generalized MIMO: Challenges, opportunities, and implementation," *Proceedings of the IEEE*, vol. 102, no. 1, pp. 56–103, Jan. 2014
7. R. Mesleh, H. Haas, C. W. Ahn, and S. Yun, "Spatial modulation — A new low complexity spectral efficiency enhancing technique," in *Proc. 2006 1st International Conference on Communications and Networking in China (CHINACOM)*, Beijing, China, Oct. 2006, pp. 1–5.
8. F. Wu, R. Zhang, L. L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 467–471, Jan. 2016.
9. F. Wu, C. Dong, L. L. Yang, and W. Wang, "Secure wireless transmission based on precoding-aided spatial modulation," in *Proc. 2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.
10. L. L. Yang, "Transmitter preprocessing aided spatial modulation for multiple-input multiple-output systems," in *Proc. 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, Budapest, Hungary, May. 2011, pp. 1–5.
11. A. Stavridis, S. Sinanovic, M. D. Renzo, and H. Haas, "Transmit precoding for receive spatial modulation using imperfect channel knowledge," in *Proc. 2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, Yokohama, Japan, May. 2012, pp. 1–5.
12. L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1351–1354, Aug. 2015.
13. O. Cepheli and G. K. Kurt, "Efficient PHY layer security in MIMO-OFDM: Spatiotemporal selective artificial noise," in *Proc. 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Madrid, Spain, Jun. 2013, pp. 1–6.
14. S. Sinanovic, M. Di Renzo, and H. Haas, "Secrecy rate of time switched transmit diversity system," in *Proc. 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, Budapest, Hungary, May. 2011, pp. 1–5.
15. Y. Wei, L. Wang, and T. Svensson, "Analysis of secrecy rate against eavesdroppers in MIMO modulation systems," in *Proc. 2015 International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, Beijing, Oct. 2015, pp. 1–5.
16. J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Generalized space shift keying modulation for MIMO channels," in *Proc. 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Cannes, France, Sept. 2008, pp. 1–5.
17. Z. Chu, H. Xing, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 283–297, Jan. 2016.
18. Y. Chen, L. Wang, Z. Zhao, M. Ma, and B. Jiao, "Secure multiuser MIMO downlink transmission via precoding-aided spatial modulation," *IEEE Communications Letters*, vol. 20, no. 6, pp. 1116–1119, Jun. 2016.

19. T. Lakshmi Narasimhan, P. Raviteja, and A. Chockalingam, "Generalized spatial modulation in large-scale multiuser MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3764–3779, Jul. 2015.
20. F. R. Castillo Soria, J. Sanchez Garcia, V. I. Rodriguez Abdala, and R. Parra Michel, "Multiuser MIMO downlink transmission using spatial modulation," in *Proc. 2014 IEEE Latin-America Conference on Communications (LATINCOM)*, Cartagena de Indias, Spain, Nov. 2014, pp. 1–5.
21. A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2004.
22. F. Wu, L. L. Yang, W. Wang, and Z. Kong, "Secret precoding-aided spatial modulation," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1544–1547, Sept. 2015.
23. Y. Yang and B. Jiao, "Information-guided channel-hopping for high data rate wireless communication," *IEEE Communications Letters*, vol. 12, no. 4, pp. 225–227, Apr. 2008.
24. L. L. Yang, "Signal detection in antenna-hopping space-division multiple-access systems with space-shift keying modulation," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 351–366, Jan. 2012.
25. M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.
26. R. Zhang, L. L. Yang, and L. Hanzo, "Error probability and capacity analysis of generalised pre-coding aided spatial modulation," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 364–375, Jan. 2015.

Chapter 5
Cooperative Security in D2D Communications

Device-to-Device (D2D) communication based storage offers a potential solution for traffic offloading from the cellular infrastructure, and mobile devices themselves can act as caching servers, i.e., content helpers [1]. The content requesters can ask for content items from the helpers among cellular peers without the help of eNodeB. However, the success of such content sharing via D2D links depends on physical conditions of the direct wireless links, which must be weighted against possibly additional security threats in D2D links. To realize the successful content sharing, the selected source node (i.e., content helper) must have the data for which the destination node (i.e., content requester) desires, and the physical link condition and user mobility also cannot be ignored. Thus, the social interaction between content helpers and content requesters is firstly investigated in this chapter. However, the direct transmission among mobile users also increases the risk of eavesdropping. Selecting D2D users (DUEs) to act as friendly jammers or relays can be regarded as an effective way to eliminate the risk of eavesdropping [2, 3]. However, it should be admitted that not all nodes are willing to serve as cooperative jammers or relays due to the different levels of altruistic cooperative behaviors of user nodes. Thus, social trust, which can be quantified by link stability or deduced by the trustiness of cooperative nodes, is also a critical factor for cooperative node selection [4, 5]. To improve link stability and system robustness, this chapter considers both physical links and social characteristics, which includes the social interaction and social trust. It focuses on the mechanism for selecting the best content helper and cooperative jamming partner to enhance the secrecy and transmission reliability of content sharing via D2D links against eavesdropping. Particularly, an optimization problem for joint source and cooperative jammer selection with power allocation is developed to maximize the secrecy rate of D2D links under individual and sum transmit power constraints. In addition to a common scenario in which the CSI of all the links can be accurately acquired, two more practical cases where only statistical CSI is available are also considered in this chapter.

L. Wang, *Physical Layer Security in Wireless Cooperative Networks*, Wireless Networks, DOI 10.1007/978-3-319-61863-0_5

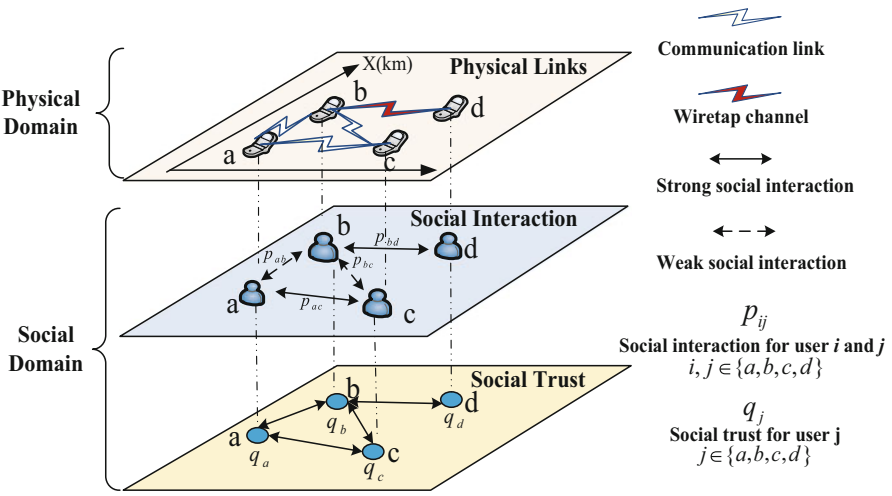


Fig. 5.1 Physical domain and social domain in D2D communications

5.1 Background and Motivations

D2D communications offer a potential solution for traffic offloading from the cellular infrastructure. By storing content items, individual mobile devices themselves can act as caching servers (i.e., content helpers) to help the content requesters to obtain the desired content without going through eNodeB. Thus, the success of such content delivery via D2D links of mobile users depends on physical condition of the direct wireless links. Besides, the social characteristics should also be considered for communication enhancement. So in this chapter, we are going to analyze the secrecy performance by jointly considering the physical link conditions and social relationships among content requesters and content helpers.

Figure 5.1 shows a three-layer structure which describes both physical domain and social domain in D2D communications. The first layer in Fig. 5.1 presents the conventional physical consideration for D2D communications, which would be effected by the quality of wireless physical links. Both the second layer and the third layer describe the social domain of users, and social considerations are made in terms of social interaction and social trust. The social interaction between users presented in the second layer of Fig. 5.1 is effected by the user mobility, which is indicated by the success probabilities between users, e.g., p_{ij}. In the third layer, each user is characterized with a social trust, which indicates user trustworthiness for cooperative communications, e.g., q_j. Though D2D communications improve communication efficiency, there exist some security threats during the signal transmission, such as eavesdropping, which is one of the most common security risk for wireless communications.

Traditionally, security enhancement is considered by assuming static transmission links between the source nodes and the destination nodes. However, this assumption is not always practical due to users' mobility and other specific demands. Moreover, in the multiple-source scenarios, i.e., there are many candidate caching nodes can be chosen as content helpers, which is vital for content requesters to make suitable decisions. Meanwhile, social factors such as contact frequency and duration should also be considered except for the physical factors for content transmission, as shown in Fig. 5.1. Besides, friendly neighbor nodes can be recruited to serve as cooperative relays or jammers to protect the communication links and overcome security vulnerabilities. However, in a mobile environment, one cannot simply rely on arranged jammers for each communication link. Instead, it is important to dynamically select friendly and efficient cooperative jamming partners by considering their physical link conditions, and their willingness for serving as cooperative jammers in the mobile environment.

Based on Fig. 5.1, the social interaction impacted by user mobility and social trust based on the interactive relationship among network nodes can be exploited for efficient and effective cooperative networking. There are a number of existing studies on cooperative jamming for improving secrecy. However, most of them assume a full channel state information (CSI) knowledge between all user nodes, which is not very practical. For the links involving passive and mobile eavesdropper nodes, it is difficult and costly to acquire accurate and real-time CSI. Consequently, the basic system model for content sharing between source nodes and destination nodes via D2D links with the help of jammer nodes in the presentence of eavesdroppers is described and discussed under the consideration of either full CSI case or statistical CSI case. Both the physical domain and the social domain are discussed to improve the communication stability and system robustness.

5.1.1 System Model and Assumptions

The system model considers the problem of reliability and secrecy enhancement for wireless content sharing between content source nodes and content requesters. Scenario used in this chapter comprises of several source nodes (i.e., content helpers) in possession of content required by the destination nodes (i.e., content requesters), and potential social eavesdroppers who may attempt to eavesdrop on the legitimate data transmission. Several intermediate nodes serve as jammers to thwart eavesdropping and to improve security performance.

Figure 5.2 shows a practical D2D wireless system model in D2D overlay, avoiding cross-tier interference between CUEs and D2D links. In other words, neighboring D2D links share the same spectrum is not considered here to avoid the complication of mutual interference. Let $\mathscr{S} = \{1, \ldots, S\}$, $\mathscr{K} = \{1, \ldots, M\}$, and $\mathscr{J} = \{1, \ldots, N\}$ be the index sets of source nodes, eavesdroppers, and jammers, respectively. One source node is chosen for data transmission to the destination node, and a neighboring node is recruited as a cooperative jamming node

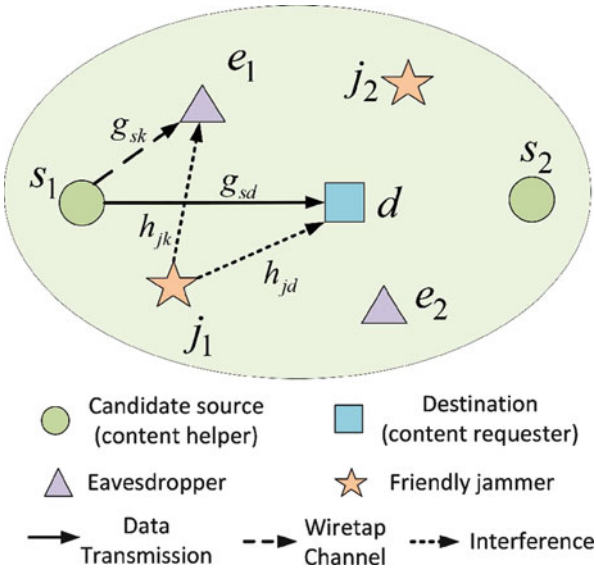


Fig. 5.2 System model

to disrupt passive eavesdropping and improve security. It is assumed that a simple control protocol is used at the destination node to measure the CSI associated with the source-to-destination and jammer-to-destination links. The wireless channels between any pair of mobile nodes are characterized as independent flat Rayleigh fading. The channel power gain between source node s and destination node d is denoted as g_{sd}. Similarly, h_{jd} and h_{jk} denote the channel power gains from the jammer j to destination d and eavesdropper k, respectively. g_{sk} is the channel gain between source node s and eavesdropper k.

5.1.2 Channel State Information

Considering whether the instantaneous information of the channels is available or not, there are three general CSI cases[6] used in research, and we first list them in the following to distinguish.

- **Full CSI case:** as in the typical scenario, the channels between any pair of mobile nodes are assumed to be independent and identically distributed (i.i.d.) with flat fading. In addition, DUEs tend to be with low mobility or even stationary to keep the D2D links stable. In this case, it is usually assumed that the CSI of all the links can be accurately acquired at the BS by means of (blind) channel estimation.
- **Partial CSI case:** practically, it is costly, difficult, and perhaps impossible to acquire accurate and real-time CSI, especially for situations involving passive and mobile eavesdropper nodes [7, 8]. Thus, the model can be expanded to a more general one to accommodate less powerful BS and less accurate

channel information in D2D overlay. In this case, g_{sd} and h_{jd} can be always known at the BS since DUEs and cooperative jammers can feedback the CSI regularly. However, the BS only has statistical information for the CSI of links involving eavesdroppers. Without loss of generality, this chapter focuses on the popular Rayleigh fading channel model, assuming that the channel power gain follows exponential distribution due to fast fading. On the other hand, large-scale shadowing effect is absorbed into the mean of exponential distribution. Therefore, we can acquire the information of $g_{sk} \sim \text{Exp}\ (\lambda_g)$, $h_{jk} \sim \text{Exp}\ (\lambda_h)$, where λ_g and λ_h are the expected channel power gains of g_{sk} and h_{jk}, and $\text{Exp}(\lambda)$ denotes the exponential distribution with mean λ.

- **Statistical CSI case:** compared with the partial CSI case, the statistical CSI case is more practical by assuming that the accurate CSI of channels g_{sd} and h_{jd} is not known either. In other words, only the statistical CSI of all links, i.e., g_{sk}, h_{jk}, g_{sd}, and h_{jd}, is provided, and the expected channel power gains of g_{sd} and h_{jd} are denoted as λ_{sd} and λ_{jd}, respectively.

5.2 Social Characteristics for Cooperative Communications

As mentioned above, both physical links and social factors will impact the successful content sharing between content requesters and content helpers with the assistance of jamming partners. Thus, selecting the source node and the friendly cooperative jamming partner is important to guarantee the communication reliability. In this chapter, social interaction based selection of source node and social trust based selection of jammer are discussed, respectively.

5.2.1 Social Interaction for Content Sharing

When there exist multiple source nodes in the network, it is critical to choose the optimal source node to help the destination node to obtain the desired content. To realize the successful communications, potential D2D links between the content helpers and the content requesters may have good physical channel conditions, and their contact time must be long enough for the desired content transmission. In this part, the social interaction will be exploited to describe the successful transmission of direct content sharing between content requesters and content helpers. Generally, the social interaction is mainly evaluated by two factors: social contact rate and social contact duration. Social contact rate is the number of encounters between two users during a time interval, while social contact duration can be calculated by how long two users remain effective communications within a short distance. Practically, data blocks can be considered successfully delivered if they can be transmitted within a single encountering time or through several encounters [9]. For simplicity, this part focuses on time-sensitive services that require one-time delivery.

As shown in the second layer in Fig. 5.1, p_{sd} is an indicator to demonstrate the social interaction between source node (i.e., content helper) and destination node (i.e., content requester), which is defined as a success probability for the d-th destination node receiving the data block transmitted by the s-th source node. Notice that the success probability of D2D data transmission in a cellular D2D underlay has been studied in [9], by considering spectrum resource sharing between cellular users and D2D users. The scenario in this case focuses on a D2D overlay without spectrum sharing between cellular users and D2D links, which is different from [9], and the D2D links are assigned with dedicated spectrum resources. However, cooperative jamming spans the same spectrum as the desired data transmission.

Referring to the derivation in [9], the success probability p_{sd} can be expressed as

$$\begin{aligned} p_{sd} &= \Pr\left\{T_{sd} \geq \frac{Z}{R_{sd}}\right\} \\ &= \int_0^{\infty} \frac{P_s \lambda_{sd}}{P_s \lambda_{sd} + P_j \lambda_{jd} \left(2^{\frac{Z/t_{sd}}{t}} - 1\right)} \exp\left(-\frac{2^{\frac{Z/t_{sd}}{t}} - 1}{P_s \lambda_{sd}} - t\right) dt, \end{aligned} \tag{5.1}$$

where Z is the size of data blocks. T_{sd} indicates the social contact duration between the s-th source node and the destination node d, which is exponentially distributed with mean t_{sd} [9].

Obviously, narrowing the candidate set of source nodes with the minimum threshold of success probability $\theta_{\min}$ will result in lower complexity without noticeable performance loss. This yields a narrowed candidate source set for d, $\mathscr{S}_T$,

$$\mathscr{S}_T = \{s \in \mathscr{S} : p_{sd} > \theta_{\min}\}. \tag{5.2}$$

5.2.2 *Social Trust for Cooperative Jamming*

In addition to the requirements of the qualified content sharing for selecting the source nodes (i.e., content helpers), selection of potential cooperative jammers should also be considered with their trustworthiness. Recall that in the third layer in Fig. 5.1, each user is characterized with an indicator to demonstrate the trustworthiness for cooperative communications, thus to clarify the trustworthiness degree of jammers, q_j is defined in this subsection to indicate the social trust index of the j-th jammer, and $q_j \in [0, 1]$. It is noted that $q_j = 1$ indicates a fully trusted and dependable node while $q_j = 0$ indicates a node that is totally untrustworthy. Functionally, jammer j will cooperate by sending the requisite jamming signal with probability q_j. Note that $(1 - q_j)$ can also be used to model the selfishness of jammer j to conserve its own energy.

5.2.3 Objective Problem Formulation

As described above, the objective is to select the optimal source node and cooperative jamming partner, with the consideration of social characteristics and power allocation, to hamper reception by the worst-case eavesdropper for secrecy guaranteed transmission. Meanwhile, the source node and the friendly jammer can be selected considering the social interaction and social trust, respectively.

Let P_s and P_j be the transmit powers of source node s and that of jammer j, respectively, which are normalized by the power of noise. Thus, the power of AWGN on each channel will be $\sigma^2 = 1$. Furthermore, given the limited energy of mobile nodes, it is necessary to control interference between jamming nodes and legitimate transceivers when they share the same spectrum. Thus, in our formulation, we consider both individual power constraints for source and jammer, i.e., $P^s_{\max}$ and $P^j_{\max}$, and joint power constraint, i.e., $P_{\max}$. For convenience, the feasible set of the power parameters can be defined as,

$$\mathscr{X} = \left\{ (P_s, P_j) : \begin{array}{c} 0 \le P_s \le P^s_{\max} \\ 0 \le P_j \le P^j_{\max} \\ 0 \le P_s + P_j \le P_{\max} \end{array} \right\}. \tag{5.3}$$

Considering the social trust of jammer j, the security rate of the data transmission from the s-th source node to the d-th destination node against the k-th eavesdropper can be expressed as

$$\begin{aligned} C_{s,j,k}(P_s, P_j) = q_j & \left[\log_2\left(1 + \frac{P_s g_{sd}}{P_j h_{jd} + 1}\right) - \log_2\left(1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}\right) \right]^+ \\ & + (1 - q_j) \left[\log_2(1 + P_s g_{sd}) - \log_2(1 + P_s g_{sk}) \right]^+, \end{aligned} \tag{5.4}$$

where $[x]^+ = \max(0, x)$, and q_j is the social trust for jammer j as aforementioned.

The most damaging eavesdropper is the one that causes the lowest secrecy rate. The worst-case eavesdropper depends only on the physical channel conditions. Here stable and reliable wiretap links are considered to demonstrate worst-case eavesdropping. With the objective to maximize the achievable secrecy rate $C_{s,j,k}(P_s, P_j)$, against the worst-case k-th non-colluding eavesdropper, the controller selects the single best s-th source node and j-th cooperative jammer and optimizes P_s and P_j in the problem formulation of

$$\max_{s \in \mathscr{S}} \max_{j \in \mathscr{J}} \max_{(P_s, P_j) \in \mathscr{X}} \min_{k \in \mathscr{K}} C_{s,j,k}(P_s, P_j) \ . \tag{5.5}$$

As discussed above, the social interaction between the source nodes and the destination nodes plays a role in improving the communication reliability. By considering the social interaction, the previous problem in Eq. (5.5) can be reduced to

$$\max_{s \in \mathscr{S}_T} \max_{j \in \mathscr{J}} \max_{(P_s, P_j) \in \mathscr{X}} \min_{k \in \mathscr{K}} C_{s,j,k}(P_s, P_j) \ . \tag{5.6}$$

Then the set of candidate source nodes can be identified by excluding nodes with poor link stability, in order to improve the stability and robustness of content sharing. Meanwhile, the smaller number of candidate source nodes leads to a lower computational complexity.

Notice that once the solution to Eq. (5.7) is found, the cooperative source and jamming partner selection process in Eq. (5.6) can be addressed more easily.

$$\max_{(P_s,P_j)\in\mathscr{X}} \min_{k\in\mathscr{K}} C_{s,j,k}(P_s, P_j) \ . \tag{5.7}$$

5.3 Optimization for Secrecy Rate Maximization

Recall that the secrecy rate optimization problem of Eq. (5.7) is non-convex and NP-hard. Consequently, both heuristic simulated annealing and approximate solutions will be considered, and bounds on the achievable secrecy rate will be used to simplify the above optimization problem and yield a suboptimal solution with little performance loss.

5.3.1 Secrecy Rate Maximization with Full CSI

In this subsection, the secrecy rate maximization problem is considered in the full CSI case. In other words, the instantaneous information of all the links is known at the controller. Firstly, a direct solution with the simulated annealing algorithm is presented, and then upper and lower bounds on the achievable secrecy rate are discussed to obtain the suboptimal solution with low complexity.

5.3.1.1 Heuristic Simulated Annealing Based Direct Evaluation

In this subsection, a heuristic simulated annealing (SA) approach is presented to solve the optimization problem in full CSI case. SA is a probabilistic method for finding the global minimum of a function that may possess several local minima [10]. It works by emulating the physical process whereby a solid is slowly cooled so that eventually its structure is "frozen" in a minimum energy configuration.

Given a set of source nodes, eavesdroppers, and cooperative jammers, the accurate values of q_j, g_{sd}, g_{sk}, h_{jk}, and h_{jd} are determined when assuming full CSI for all the links. Therefore, the variables of the optimization problem in Eq. (5.4) are P_s and P_j. Below is a brief overview of the steps:

Step 1: Randomly generate an initial solution (P_s, P_j) to be valued by the cost function of Eq. (5.4);

Step 2: Generate a random neighboring solution and compute the new solution's function value;
Step 3: Pick the new solution if its function value is larger. Otherwise, accept the new solution with a certain probability;
Step 4: Repeat Steps 2–3 until an acceptable solution is found or upon reaching a number of iterations.

As proved in [11], after a number of iterations, the SA algorithm will converge to a solution, (P_s^*, P_j^*), which, with high likelihood, represents the optimal or acceptably good suboptimal solution to the optimization problem. However, one limitation of the SA heuristic algorithm is the lack of worst-case performance guarantee. Furthermore, its potential for computational time reduction is limited.

Considering the weaknesses of the SA, a potentially more effective alternative is to design approximation algorithms with higher reliability and lower complexity. Here, upper and lower bounds are firstly derived on the secrecy rate. Notice that many existing relaxation methods optimize either the upper bound or the lower bound of the original problem before taking the optimized parameters as the final result [12, 13]. Thus, in addition to present algorithms based on the exact optimization, both upper and lower bounds are considered in this subsection to simplify the original optimization of transmit powers.

5.3.1.2 Low-Complexity Optimization Leveraging Upper Bound

Applying the well-known inequality $\ln(x) \leq x - 1$ to Eq. (5.4) gives

$$\ln 2 \cdot C_{s,j,k}(P_s, P_j) \leq q_j \left[\frac{1 + \frac{P_s g_{sd}}{P_j h_{jd}+1}}{1 + \frac{P_s g_{sk}}{P_j h_{jk}+1}} - 1 \right]^+ + (1 - q_j) \left[\frac{1 + P_s g_{sd}}{1 + P_s g_{sk}} - 1 \right]^+. \tag{5.8}$$

Reorganizing the formula above, the achievable secrecy rate can be upper bounded as

$$C_{s,j,k}(P_s, P_j) \leq \frac{q_j}{\ln 2} \frac{\left[\frac{P_s g_{sd}}{P_j h_{jd}+1} - \frac{P_s g_{sk}}{P_j h_{jk}+1} \right]^+}{1 + \frac{P_s g_{sk}}{P_j h_{jk}+1}} + \frac{(1-q_j)}{\ln 2} \frac{P_s \left[g_{sd} - g_{sk} \right]^+}{1 + P_s g_{sk}}. \tag{5.9}$$

For simplicity, further define the following:

$$f(P_s, P_j) = \left[\frac{P_s g_{sd}}{P_j h_{jd} + 1} - \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right]^+, \tag{5.10a}$$

$$g(P_s, P_j) = 1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}, \tag{5.10b}$$

$$h(P_s) = P_s \left[g_{sd} - g_{sk}\right]^+, \tag{5.10c}$$

$$w(P_s) = 1 + P_s g_{sk}, \tag{5.10d}$$

$$u_k(P_s, P_j) = g(P_s, P_j) w(P_s), \tag{5.10e}$$

$$v_k(P_s, P_j) = \frac{q_j}{\ln 2} f(P_s, P_j) w(P_s) + \frac{(1-q_j)}{\ln 2} g(P_s, P_j) h(P_s). \tag{5.10f}$$

It follows that the objective function in Eq. (5.7) can use the secrecy rate upper bound in Eq. (5.9) giving

$$\max_{(P_s,P_j)\in\mathscr{X}} \min_k \left\{ \frac{q_j}{\ln 2} \frac{f(P_s,P_j)}{g(P_s,P_j)} + \frac{(1-q_j)}{\ln 2} \frac{h(P_s)}{w(P_s)} \right\} = \max_{(P_s,P_j)\in\mathscr{X}} \min_k \left\{ \frac{v_k(P_s,P_j)}{u_k(P_s,P_j)} \right\}. \tag{5.11}$$

By referring to mathematically equivalent problems in [14], the formula above can be reformulated as follows:

$$\min_{(P_s,P_j)\in\mathscr{X}} \max_k \frac{u_k(P_s,P_j)}{v_k(P_s,P_j)}. \tag{5.12}$$

Therefore, if the optimal solution (P_s^*, P_j^*) and the corresponding optimal objective value $f^* = \frac{u_k(P_s^*,P_j^*)}{v_k(P_s^*,P_j^*)}$ is found for the problem of Eq. (5.12), then (P_s^*, P_j^*) is also the optimal solution to Eq. (5.11).

Notice that $u_k(P_s, P_j)$ and $v_k(P_s, P_j)$ are nonlinear functions of P_s and P_j. Although this optimization problem is still non-convex, fortunately, such a non-convex optimization problem has been studied before by adopting the generalized fractional programming (GFP) algorithms, e.g. in [15]. Particularly, we utilize the Dinkelbach-type algorithm, one of the most popular GFP algorithms [16, 17] to solve our optimization problem.

It should be noted that both $u_k(P_s, P_j)$ and $v_k(P_s, P_j)$ are bounded. Furthermore, $v_k(P_s, P_j) > 0$ for $P_s \in (0, P_{\max}^s)$ and $P_j \in (0, P_{\max}^j)$. Hence the optimization problem in Eq. (5.12) has an optimal solution. Firstly, Eq. (5.12) can be rewritten as follows for simplicity,

$$(P) \qquad \min_{(P_s,P_j)\in\mathscr{X}} \max_k \frac{u_k(P_s,P_j)}{v_k(P_s,P_j)}.$$

To solve problem (P), one considers the following parametric problem:

$$(P_\mu)\ F_k(\mu) = \min_{(P_s,P_j)\in\mathscr{X}} \max_k \{u_k(P_s,P_j) - \mu \cdot v_k(P_s,P_j)\}.$$

Apparently, the optimal objective value μ^* of problem (P) satisfies $F_k(\mu^*) = 0$. In other words, $F_k(\mu) = 0$ implies $\mu = \mu^*$. Therefore, solution of problem (P)

Algorithm 1: Dinkelbach-type Algorithm

$(P_s^{(i)}, P_j^{(i)})$: the i-th iteration of the transmit power for source node s and jammer node j.
$\mathscr{X}$: the feasible set of power parameters.
l: positive integer.
begin
Referring to Eq. (5.10) to Eq. (5.12),
Step 1: Take $(P_s^{(0)}, P_j^{(0)}) \in \mathscr{X}$, compute $\mu_1 = \max_k \left\{u_k(P_s^{(0)}, P_j^{(0)})/v_k(P_s^{(0)}, P_j^{(0)})\right\}$, and let $l = 1$.
Step 2: Determine $(P_s^{(l)}, P_j^{(l)}) = \arg \min_{(P_s,P_j)\in\mathscr{X}} \left\{\max_k\{u_k(P_s, P_j) - \mu_l v_k(P_s, P_j)\}\right\}$.
$F_k(\mu_l) = \min_{(P_s,P_j)\in\mathscr{X}} \max_k \{u_k(P_s, P_j) - \mu_l v_k(P_s, P_j)\}$.
Step 3:
if $F_k(\mu_l) = 0$ **then**
The optimal solution is $(P_s^*, P_j^*) = (P_s^{(l)}, P_j^{(l)})$ with optimal value $\mu^* = \mu_l$ and **Stop**.
else
Let $\mu_{l+1} = \max_k \left\{u_k(P_s^{(l)}, P_j^{(l)})/v_k(P_s^{(l)}, P_j^{(l)})\right\}$, $l = l + 1$, and go to **Step 2**.
end
end

can be achieved by finding a solution to $F_k(\mu) = 0$. Based on this observation, Dinkelbach-type algorithm solves a subproblem (P_μ) in each step, generating a sequence μ_l which converges to the optimal objective value μ^* of problem (P). The detailed process is described in Algorithm 1.

5.3.1.3 Low-Complexity Optimization Leveraging Lower Bound

Similarly, the lower bound of the optimization problem in full CSI case is further discussed in this subsection.

Firstly, Eq. (5.4) is rewritten as

$$C_{s,j,k}(P_s, P_j) = q_j \left[\log_2\left(1 + \frac{\frac{P_s g_{sd}}{P_j h_{jd}+1} - \frac{P_s g_{sk}}{P_j h_{jk}+1}}{1 + \frac{P_s g_{sk}}{P_j h_{jk}+1}}\right)\right]^+ + (1 - q_j)\left[\log_2\left(1 + \frac{P_s g_{sd} - P_s g_{sk}}{1 + P_s g_{sk}}\right)\right]^+.$$

Applying inequality $[\ln(1 + x)]^+ \geq \left[\frac{2x}{2+x}\right]^+$, gives

$$\ln 2 \cdot C_{s,j,k}(P_s, P_j) \geq \frac{2q_j}{2\frac{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}{\left[\frac{P_s g_{sd}}{P_j h_{jd}+1} - \frac{P_s g_{sk}}{P_j h_{jk}+1}\right]^+} + 1} + \frac{2(1 - q_j)}{2\left[\frac{1+P_s g_{sk}}{P_s(g_{sd}-g_{sk})}\right]^+ + 1}.$$

Thus, the achievable secrecy rate from the s-th source node to d-th destination node against the k-th eavesdropper using the j-th cooperative jammer as shown in Eq. (5.4) can be lower bounded as:

$$C_{s,j,k}(P_s,P_j) \geq \frac{2q_j/\ln 2}{2\frac{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}{\left[\frac{P_s g_{sd}}{P_j h_{jd}+1}-\frac{P_s g_{sk}}{P_j h_{jk}+1}\right]^+}+1}+\frac{2(1-q_j)/\ln 2}{2\left[\frac{1+P_s g_{sk}}{P_s(g_{sd}-g_{sk})}\right]^+ +1}. \tag{5.13}$$

Given the lower bound, our optimization problem in Eq. (5.7) can be relaxed as,

$$\max_{(P_s,P_j)\in\mathscr{X}} \min_{k\in\mathscr{K}} \frac{2q_j/\ln 2}{2\frac{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}{\left[\frac{P_s g_{sd}}{P_j h_{jd}+1}-\frac{P_s g_{sk}}{P_j h_{jk}+1}\right]^+}+1}+\frac{2(1-q_j)/\ln 2}{2\left[\frac{1+P_s g_{sk}}{P_s(g_{sd}-g_{sk})}\right]^+ +1}, \tag{5.14}$$

which can also be solved with GFP in terms of the Dinkelbach-type algorithm.

5.3.2 *Secrecy Rate Maximization with Statistical CSI*

This subsection focuses on the joint power optimization and cooperative nodes selection problem when only statistical CSI of all the links is available. Firstly, a direct solution to the optimization problem will be presented. Then, to reduce optimization complexity, an approximate solution will be determined by maximizing the lower bound on the expected secrecy rate.

5.3.2.1 Heuristic Simulated Annealing Based Direct Evaluation

The ergodic sum rate of the system is now maximized under the circumstances that only statistical CSI of g_{sd}, h_{jd}, g_{sk}, and h_{jk} can be acquired. Mathematically, the optimization problem in Eq. (5.7) can be reformulated as,

$$\max_{(P_s,P_j)\in\mathscr{X}} \min_{k\in\mathscr{K}} \mathrm{E}\left\{C_{s,j,k}(P_s,P_j)\right\}, \tag{5.15}$$

where

$$\begin{aligned}\mathrm{E}\left\{C_{s,j,k}(P_s,P_j)\right\} = q_j\left[\mathrm{E}\left\{\log_2\left(1+\frac{P_s g_{sd}}{P_j h_{jd}+1}\right)\right\}-\mathrm{E}\left\{\log_2\left(1+\frac{P_s g_{sk}}{P_j h_{jk}+1}\right)\right\}\right]^+ \\ +(1-q_j)\left[\mathrm{E}\left\{\log_2\left(1+P_s g_{sd}\right)\right\}-\mathrm{E}\left\{\log_2\left(1+P_s g_{sk}\right)\right\}\right]^+.\end{aligned} \tag{5.16}$$

In order to reduce the computation complexity, Eq. (5.16) can be reduced by evaluating the expectations. Specific details can be seen from the following Lemma 5.1, based on some derivations from [18, 19].

Lemma 5.1 *For $X_1 \sim Exp(\alpha_1)$, $X_2 \sim Exp(\alpha_2)$, it holds that*

$$\mathrm{E}\Big[\ln(1+P_1X_1)\Big] = \phi(P_1\alpha_1),$$
$$\mathrm{E}\left[\ln\left(1+\frac{P_2X_2}{1+P_1X_1}\right)\right] = \frac{[\phi(P_2\alpha_2)-\phi(P_1\alpha_1)]}{1-\frac{P_1\alpha_1}{P_2\alpha_2}},$$

where $\phi(x) = e^{1/x}E_1(1/x)$, $E_1(x) = \int_x^\infty \frac{1}{t}e^{-t}dt$, $x \geq 0$.

Proof First, we expand the expectation $\mathrm{E}[\ln(1+P_1X_1)]$,

$$\mathrm{E}[\ln(1+P_1X_1)] = \int_0^\infty \frac{1}{\alpha_1}e^{-\frac{x}{\alpha_1}}\ln(1+P_1x)\,dx.$$

Using Eq. (9) on page 194 of [19], we have

$$\int_0^\infty \frac{1}{\alpha_1}e^{-\frac{x}{\alpha_1}}\ln(1+P_1x)\,dx = e^{\frac{1}{P_1\alpha_1}}E_1\left(\frac{1}{P_1\alpha_1}\right) = \phi(P_1\alpha_1).$$

Similarly, $\mathrm{E}\left[\ln\left(1+\frac{P_1X_1}{1+P_2X_2}\right)\right]$ can be expanded as,

$$\begin{aligned}
&\mathrm{E}\left[\ln\left(1+\frac{P_1X_1}{1+P_2X_2}\right)\right] \\
&= \int_0^\infty \frac{1}{\alpha_2}e^{-\frac{x}{\alpha_2}}\left[\int_0^\infty \ln\left(1+\frac{P_1y}{1+P_2x}\right)\frac{1}{\alpha_1}e^{-\frac{y}{\alpha_1}}dy\right]dx \\
&= \int_0^\infty \frac{1}{\alpha_2}e^{-\frac{x}{\alpha_2}}dx\int_0^\infty \ln\left(1+\frac{y}{(1+P_2x)/(\alpha_1P_1)}\right)e^{-y}dy \\
&= \int_0^\infty \frac{1}{\alpha_2}e^{-\frac{x}{\alpha_2}}e^{(1+P_2x)/(\alpha_1P_1)}E_1\left((1+P_2x)/(\alpha_1P_1)\right)dx \\
&= \int_{\frac{1}{P_1\alpha_1}}^\infty \left(\frac{P_1\alpha_1}{P_2\alpha_2}\right)e^{\frac{1}{P_2\alpha_2}}\exp\left[\left(1-\frac{P_1\alpha_1}{P_2\alpha_2}\right)z\right]E_1(z)dz.
\end{aligned}$$

Defining $\xi = P_1\alpha_1/(P_2\alpha_2)$, and using Eq. (3) on Page 197 of [19], and Eq. (12) on page 308 of [20], we have,

$$\int_{\frac{1}{P_1\alpha_1}}^\infty \left(\frac{P_1\alpha_1}{P_2\alpha_2}\right)e^{\frac{1}{P_2\alpha_2}}\exp\left[\left(1-\frac{P_1\alpha_1}{P_2\alpha_2}\right)z\right]E_1(z)dz$$

$$
\begin{aligned}
&= \xi e^{\frac{1}{P_2\alpha_2}} \int_{\frac{1}{P_1\alpha_1}}^{\infty} e^{(1-\xi)x} E_1(x)dx \\
&= \xi e^{\frac{1}{P_2\alpha_2}} \left(\int_0^{\infty} e^{(1-\xi)x} E_1(x)dx - \int_0^{\frac{1}{P_1\alpha_1}} e^{(1-\xi)x} E_1(x)dx \right) \\
&= \xi e^{\frac{1}{P_2\alpha_2}} \left(\frac{1}{\xi-1} \ln \xi - \frac{1}{\xi-1} \left[-e^{\frac{(1-\xi)}{P_1\alpha_1}} E_1\left(\frac{1}{P_1\alpha_1}\right) + \ln \xi + E_1\left(\frac{\xi}{P_1\alpha_1}\right) \right] \right) \\
&= \frac{\xi}{\xi-1} \left(e^{\frac{1}{P_2\alpha_2}} e^{\frac{(1-\xi)}{P_1\alpha_1}} E_1\left(\frac{1}{P_1\alpha_1}\right) - e^{\frac{1}{P_2\alpha_2}} E_1\left(\frac{\xi}{P_1\alpha_1}\right) \right) \\
&= \frac{\frac{P_1\alpha_1}{P_2\alpha_2}}{\frac{P_1\alpha_1}{P_2\alpha_2} - 1} \left(e^{\frac{1}{P_1\alpha_1}} E_1\left(\frac{1}{P_1\alpha_1}\right) - e^{\frac{1}{P_2\alpha_2}} E_1\left(\frac{1}{P_2\alpha_2}\right) \right) \\
&= \frac{\phi(P_1\alpha_1) - \phi(P_2\alpha_2)}{1 - \frac{P_2\alpha_2}{P_1\alpha_1}}.
\end{aligned}
$$

Applying the Lemma 5.1, the optimization problem in Eq. (5.16) can be expressed as

$$
\begin{aligned}
\max_{(P_s,P_j)\in\mathscr{X}} \min_{k\in\mathscr{K}} \Bigg\{ & \frac{q_j}{\ln 2} \left[\frac{\phi(P_s\lambda_{sd}) - \phi(P_j\lambda_{jd})}{1 - \frac{P_j\lambda_{jd}}{P_s\lambda_{sd}}} - \frac{\phi(P_s\lambda_g) - \phi(P_j\lambda_h)}{1 - \frac{P_j\lambda_h}{P_s\lambda_g}} \right]^+ \\
& + \frac{(1-q_j)}{\ln 2} \left[\phi(P_s\lambda_{sd}) - \phi(P_s\lambda_h) \right]^+ \Bigg\}. \qquad (5.17)
\end{aligned}
$$

5.3.2.2 Ergodic Lower Bound for Complexity Reduction

The achievable ergodic secrecy rate shown in Eq. (5.17) can be lower bounded as

$$
\begin{aligned}
\mathrm{E}\left\{C_{s,j,k}(P_s,P_j)\right\} \geq & q_j \left[\frac{\phi(P_s\lambda_{sd}) - \phi(P_j\lambda_{jd})}{\ln 2 \cdot \left(1 - \frac{P_j\lambda_{jd}}{P_s\lambda_{sd}}\right)} - \log_2\left(1 + \frac{P_s\lambda_{sk}}{P_j\lambda_h}\phi(P_j\lambda_h)\right) \right]^+ \\
& + (1-q_j) \left[\frac{\phi(P_s\lambda_{sd})}{\ln 2} - \log_2(1 + P_s\lambda_g) \right]^+, \qquad (5.18)
\end{aligned}
$$

which can also be proved from the Jensen's inequality as similar with the Eq. (1.15), and the derivations are omitted in this part.

Leveraging the conclusion in Eq. (5.18), a lower bound on the objective function can be maximized, i.e., the following lower bound on the ergodic sum rate can be maximized to achieve optimized transmit powers.

$$\max_{(P_s,P_j)\in\mathscr{X}} \min_{k\in\mathscr{K}} \left\{ q_j \left[\frac{\phi(P_s\lambda_{sd}) - \phi(P_j\lambda_{jd})}{\ln 2 \cdot \left(1 - \frac{P_j\lambda_{jd}}{P_s\lambda_{sd}}\right)} - \log_2\left(1 + \frac{P_s\lambda_{sk}}{P_j\lambda_h}\phi(P_j\lambda_h)\right) \right]^+ \right.$$
$$\left. + (1-q_j)\left[\frac{\phi(P_s\lambda_{sd})}{\ln 2} - \log_2(1+P_s\lambda_g) \right]^+ \right\}. \tag{5.19}$$

Thus far, the sum secrecy rate has been considered under the assumptions of both full CSI and statistical CSI, respectively. The brute force search and SA were both used to solve the optimization problem in Eqs. (5.7) and (5.17). Also, low-complexity optimization problems based on bounds of the secrecy rate were developed. To further reduce the computation complexity, a one dimensional search with low complexity is proposed in the following to solve the optimization problems with little performance loss.

5.3.3 *One-Dimensional Search with Low Complexity*

Recall that the brute-force approach is an available algorithm to solve the optimization problem, which must search over a 2-dimensional (2-D) space of $(P_s,\ P_j)$ for every k. To reduce the computation complexity, a lower complexity algorithm which is suggested by focusing on a one-dimensional (1-D) space is presented in this subsection with little performance loss.

Proposition 5.1 *The optimal solution* (P_s, P_j) *to maximize the sum secrecy rate of Eq.* (5.4)*, Eq.* (5.11)*, Eq.* (5.14) *and the ergodic sum rate of Eq.* (5.17) *and Eq.* (5.19) *must satisfy* $P_s = P_s^{\max}$ *or* $P_s + P_j = P_{\max}$.

Proof Taking the optimization problem in Eq. (5.4) for example, the expression of achievable secrecy rate can be rewritten as

$$C_{s,j,k}(P_s,P_j) \tag{5.20}$$
$$= q_j\left[\log_2\left(\frac{1+\frac{P_s g_{sd}}{P_j h_{jd}+1}}{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}\right)\right]^+ + (1-q_j)\left[\log_2\left(\frac{1+P_s g_{sd}}{1+P_s g_{sk}}\right)\right]^+$$
$$= q_j \log_2\left(1+\left[\frac{\frac{P_s g_{sd}}{P_j h_{jd}+1}-\frac{P_s g_{sk}}{P_j h_{jk}+1}}{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}\right]^+\right) + (1-q_j)\log_2\left(1+\frac{P_s[g_{sd}-g_{sk}]^+}{1+P_s g_{sk}}\right)$$
$$= q_j \log_2\left(1+\left[\frac{\frac{g_{sd}}{P_j h_{jd}+1}-\frac{g_{sk}}{P_j h_{jk}+1}}{\frac{1}{P_s}+\frac{g_{sk}}{P_j h_{jk}+1}}\right]^+\right) + (1-q_j)\log_2\left(1+\frac{[g_{sd}-g_{sk}]^+}{\frac{1}{P_s}+g_{sk}}\right).$$

Table 5.1 Main abbreviations of simulation results

Abbreviations	Explanations
BF	Brute force search is used to optimize the objective function
DE-SA	The optimization problem is solved by direct evaluation by utilizing SA
LB-SA	The optimization problem is solved by leveraging the lower bound solved by SA
UB-D	The optimization problem is solved by leveraging the upper bound solved by Dinkelbach
LB-D	The optimization problem is solved by leveraging the lower bound solved by Dinkelbach
1-D, DE	The optimization problem is solved by direct evaluation leveraging the 1-D search
1-D, UB	The optimization problem is solved by upper bound leveraging the 1-D search
1-D, LB	The optimization problem is solved by lower bound leveraging the 1-D search

Table 5.2 Main simulation parameters

Parameters	Values
Bandwidth	20 MHz
Noise power (σ^2)	-96 dBm
Maximum transmit power of D2D transmitter ($P^s_{\max}$)	23 dBm
Maximum transmit power of jammer nodes ($P^j_{\max}$)	19 dBm
Maximum total sum power ($P_{\max}$)	24 dBm
Number of eavesdroppers (M)	4

Clearly, the secrecy rate increases monotonically with P_s. Without the joint power constraint in Eq. (5.3), the trivial solution $P_s = P_s^{\max}$ applies. With the joint power constraint $P_s + P_j \le P_{\max}$, the optimal solution either reaches the upper limit of P_s or satisfies $P_s + P_j = P_{\max}$ to maximize the target secrecy and its corresponding bounds for both the full CSI case and statistical CSI model.

From Proposition 5.1, the optimization problem with two variables can be transformed into one with only a single variable. Thus, it suffices to implement the 1-D search to maximize the secrecy rate. For notational simplicity, the boundary is denoted as

$$\begin{aligned} &\mathscr{L} = \left\{(P_s, P_j) \middle| P_s = P_s^{\max} \text{ or } P_s + P_j = P_{\max}\right\}, \\ &s.t. \quad 0 \le P_s \le P_s^{\max}, 0 \le P_j \le P_j^{\max}. \end{aligned} \tag{5.21}$$

Instead of the exhaustive 2-D search over the plane $[0, P_s^{\max}] \times [0, P_j^{\max}]$, the proposed 1-D search over $\mathscr{L}$ can significantly reduce the computation complexity.

5.3.4 Simulation and Numerical Results

Different methods have been adopted to optimize P_s and P_j to maximise the secrecy rate of D2D links. The label "1-D" indicates that the power optimization has been simplified into a problem with only one variable, and other methods without "1-D" means that the power optimization is made over the 2-D space of (P_s, P_j). The main related abbreviations of simulation results are listed in Table 5.1. Additionally, large scale path-loss exponents between any two user nodes are assumed to be the same and equal to 4. Other simulation parameters are listed in Table 5.2.

5.3.4.1 Impact of Number of Jammer Nodes and Sum Transmit Power Limitation

- **Full CSI Case**

Figure 5.3 illustrates the achievable secrecy rate and simulation time comparison of the algorithms under the assumption of full CSI. Clearly, by increasing number N of cooperative jammer nodes, both secrecy rate and simulation time grow as shown in Fig. 5.3. More candidate cooperative jammer nodes provide for more choices and possibly better cooperative jammer selection to combat eavesdropping, thereby achieving better performance. Meanwhile, since the power optimization should be executed for every potential cooperative jammer node during the selection step, the computational time grows with more candidate cooperative jammer nodes. It is also natural that a larger $P_{\max}$ achieves better performance for all the optimization problems by comparing the two parts in Fig. 5.3. If a more flexible power allocation is available for the source node and cooperative jamming nodes, then a better power allocation can be found for higher achievable secrecy rate.

Generally, the brute force search and the direct evaluation via simulated annealing achieve nearly the same performance, as expected. The approximation methods via upper-bound and lower-bound optimization lead to somewhat worse performance, although the performance gaps among these methods are rather small. Therefore, our proposed simulated annealing optimization demonstrates little performance loss as seen from Fig. 5.3a. However, it still consumes substantial computation time as shown in Fig. 5.3b. Observe that the upper-bound and lower-bound optimization methods combined with the process of narrowing the candidate source set provides a very good performance-complexity tradeoff. It exhibits very little loss in terms of secrecy rate, while achieving orders of magnitude reduction in complexity.

- **Statistical CSI Case**

Figure 5.4 illustrates the performance comparison of different algorithms under the assumption of statistical CSI. Similar to the full CSI scenario, for all optimization cases, more jammers lead to better performance and higher complexity, and larger secrecy rate can be achieved with a larger $P_{\max}$ as shown in Fig. 5.4. Specifically,

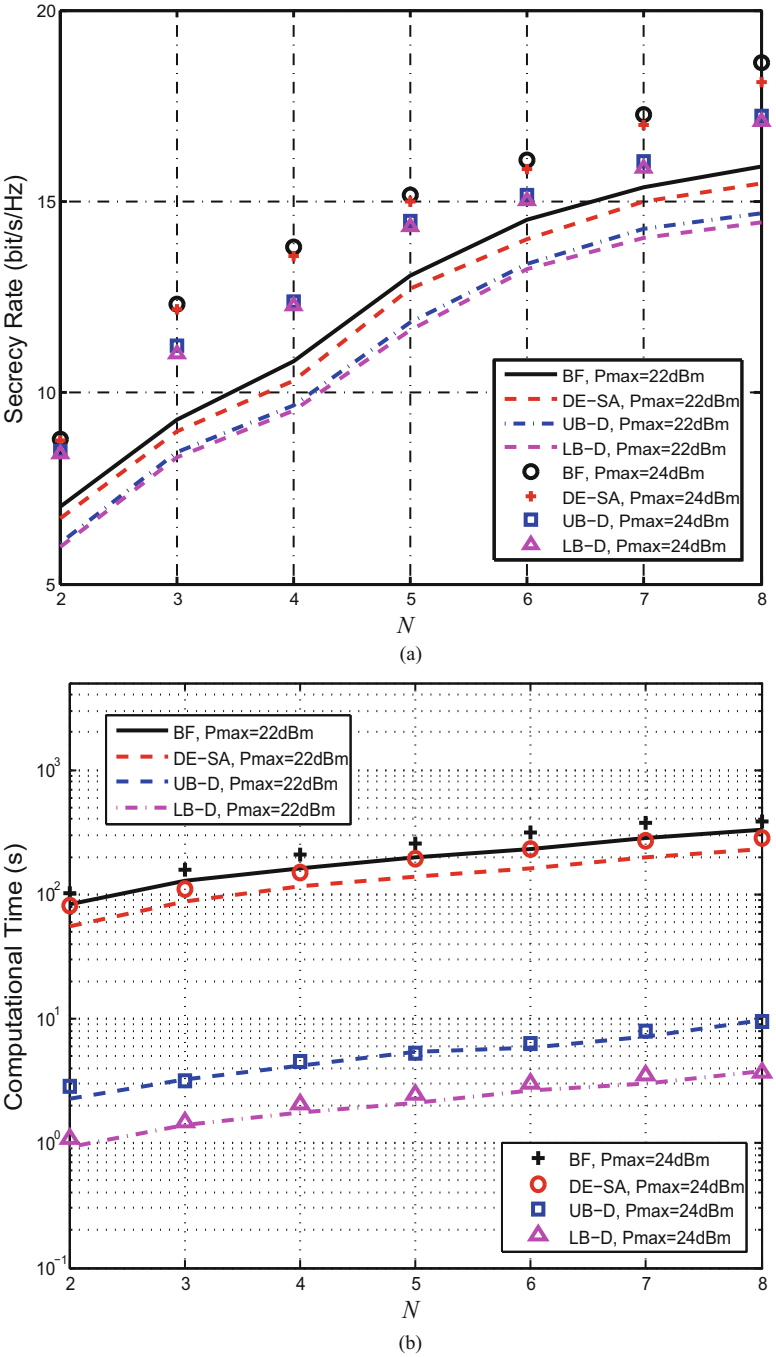


Fig. 5.3 Achievable secrecy rate in full CSI model. $S = 4, q_j = 0.8, \theta_{\min} = 0.5$. (**a**) Achievable secrecy rate. (**b**) Computational time

the brute force search and the SA solution achieve very similar secrecy rate, and the proposed lower bound optimization yields lower secrecy rate, though the performance gaps among different methods remain small as shown in Fig. 5.4a.

Focusing on the simulation time as measure of computation complexity in Fig. 5.4b, similarly, the proposed low-complexity optimization method, by narrowing the candidate source set and optimizing the lower bound of the original secrecy rate, presents a good tradeoff between complexity and performance. Suffering little performance loss, it consumes dramatically less time as seen from Fig. 5.4b.

5.3.4.2 Impact of Searching Dimension over Transmission Power

It should be noted that for the fact that the methods using the procedure of narrowing candidate source set sacrifice little secrecy rate. Thus all the methods involved in this part have narrowed the candidate source set before cooperative jamming node selection and power optimization unless otherwise specified. The label "1-D" indicates that the power optimization has been simplified into a problem with only one variable.

- **Full CSI Case**

Figure 5.5 illustrates the performance and complexity comparison of different optimization algorithms under full CSI case. Naturally, the achievable secrecy rate of the D2D links increases with the number of source nodes, since more source nodes make it more likely for a better option. It can be seen that although the direct evaluation outperforms the proposed upper-bound method and lower-bound method as expected, the performance gap is insignificant, as shown in Fig. 5.5a. While the proposed 1-D search methods achieve identical performance as the 2-D search method, but the computation time difference are very significant as shown in Fig. 5.5b. Observably, a larger number of source nodes leads to higher complexity.

- **Statistical CSI Case**

Figure 5.6 illustrates the performance and complexity comparison of different optimization algorithms under statistical CSI assumption. Similarly, the achievable secrecy rate of the D2D links and the computation time increase with the number of source nodes in statistical CSI case. Meanwhile, the direct evaluation outperforms the proposed lower-bound method as expected. Again, the proposed 1-D search method for statistical CSI case achieves identical performance while consuming much less time than 2-D search, as shown in Fig. 5.6a, b, respectively. Thus, a 1-D search for power is adopted for optimization in the sequel unless specified otherwise.

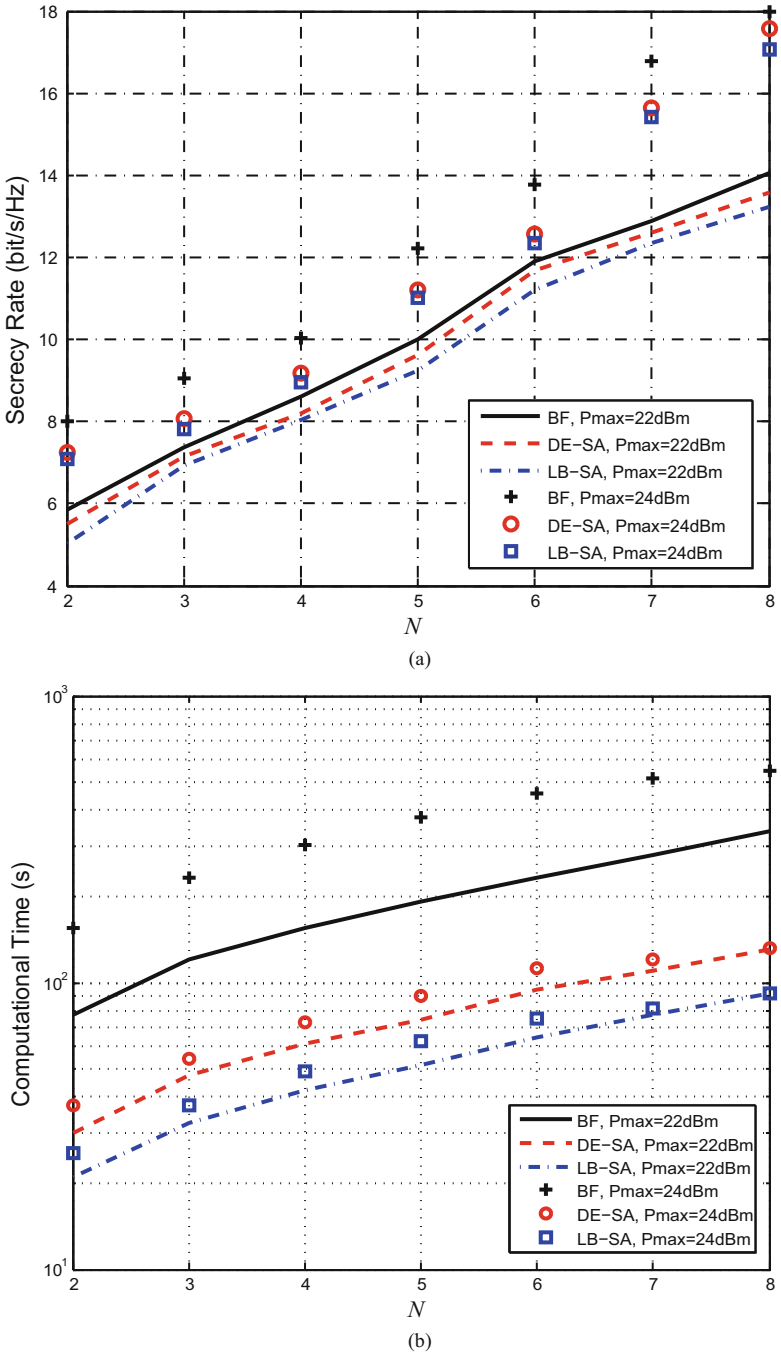


Fig. 5.4 Achievable secrecy rate in statistical CSI model. $S = 4, q_j = 0.8, \theta_{\min} = 0.5$. (**a**) Achievable secrecy rate. (**b**) Computational time

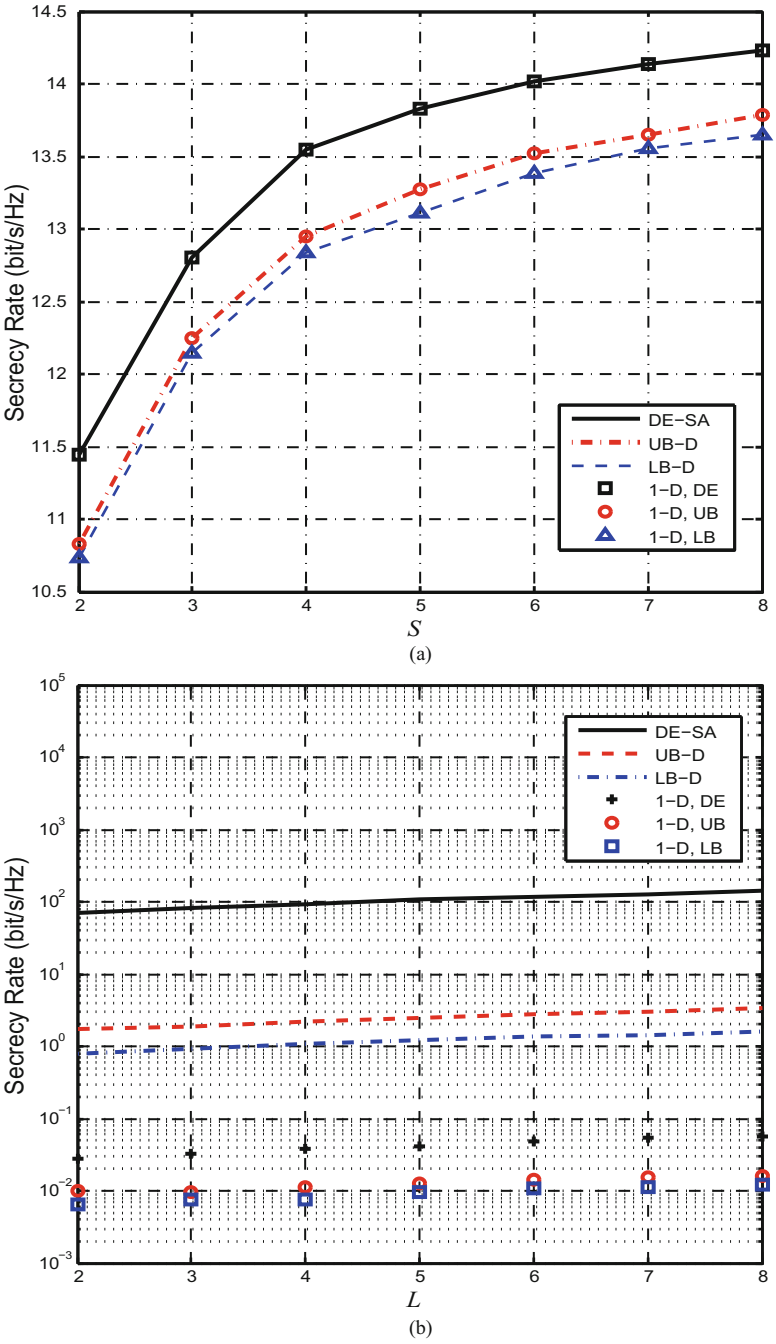
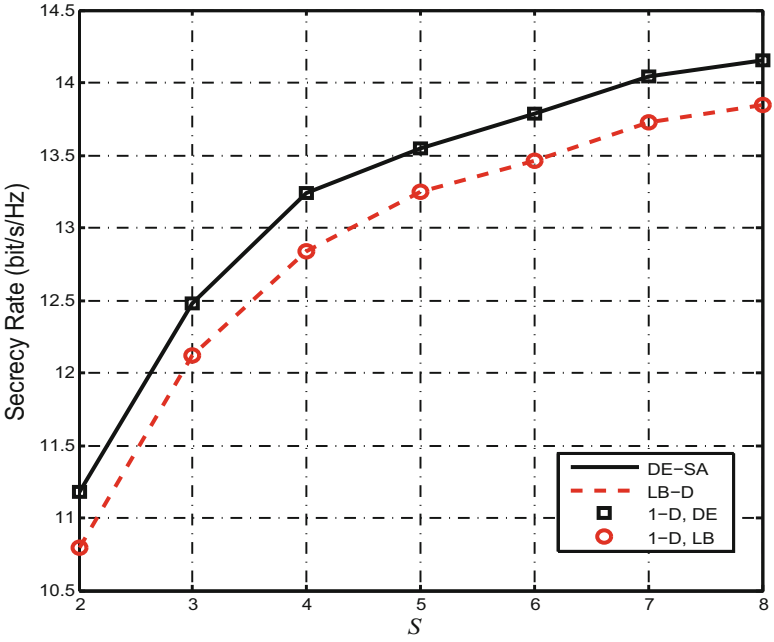
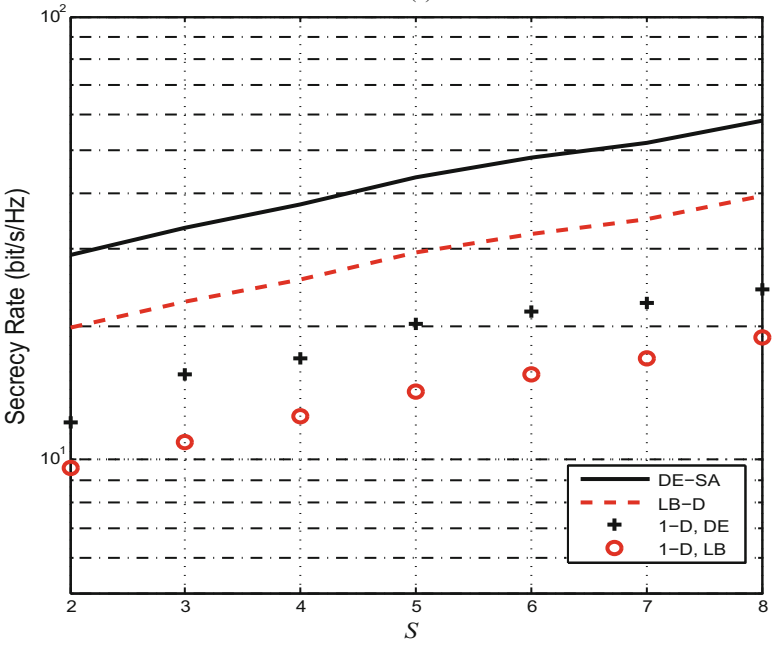


Fig. 5.5 Performance comparison of different optimization methods in full CSI case. $N = 5, q_j = 0.8, \theta_{\min} = 0.5$. (**a**) Achievable secrecy rate. (**b**) Computational time



(a)



(b)

Fig. 5.6 Performance comparison of different optimization methods in statistical CSI case. $N = 5, q_j = 0.8, \theta_{\min} = 0.5$. (**a**) Achievable secrecy rate. (**b**) Computational time

5.3.4.3 Impact of Social Characteristics Consideration

- **Impact of Success Rate Threshold**

Figure 5.7 illustrates the impact of success rate threshold, $\theta_{\min}$, on achievable performance. It can be seen from Fig. 5.7 that both the achievable secrecy rate and the corresponding computational time decline with larger $\theta_{\min}$. With increasing $\theta_{\min}$, more source nodes with success probability lower than $\theta_{\min}$ will be excluded from $\mathscr{S}_T$, leading to faster selection and optimization. However, a higher $\theta_{\min}$ may result in the elimination of source nodes with a prominent physical link but less contact duration, i.e., low success probability. Since such source nodes may potentially have the best resistance capability to eavesdropping due to their physical location, their exclusion may result in poor performance.

On the other hand, when the value of $\theta_{\min}$ is relatively small, the decrease in achievable secrecy rate is negligible, but the reduction of computational time is not satisfying. Generally, the larger $\theta_{\min}$ is, the more the secrecy performance will be sacrificed but more computing time will be saved as well. Therefore, the choice of $\theta_{\min}$ is key to the tradeoff between secrecy performance and computational time.

- **Socially Stable Source Node Selection**

The impact of social interaction on achievable secrecy rate is further investigated as shown in Fig. 5.8. The labels "No Social Interaction" and "With Social Interaction" are used to denote cases when the social interaction is not considered or considered, respectively, for cooperative source and jammer node selection and power allocation. Naturally, a larger $P_{\max}$ allows source and jamming nodes to find a better power allocation and consequently, a higher secrecy rate. Meanwhile, when ignoring social interaction between source and destination nodes, the secrecy rate drops since nodes selected for transmission may have low contact duration with the destination, thereby failing in content delivery. Conversely, consideration of social behavior of candidate source nodes leads to a better performance.

- **Socially Trusted Jammer Node Selection**

In Fig. 5.9, labels "No Social Trust" and "With Social Trust" are used here to denote the cases when the social trust of jammers is not considered versus considered, respectively. Similar to the results in Fig. 5.8, a larger secrecy rate can be achieved with a larger $P_{\max}$ regardless of social trust assumption as shown in Fig. 5.9. Without exploiting knowledge of social trust of cooperative jamming nodes, the secrecy rate will suffer as unreliable jamming partners may be selected. On the other hand, better performance can be achieved by giving consideration to the social trust of candidate cooperative jammers.

- **Social Characteristics Estimation Error**

The social characteristics and social relationship among different nodes (i.e., users) is time varying and the estimation of social interaction and social trust index is prone to errors. To illustrate the robustness of our approach, the impact of estimation errors

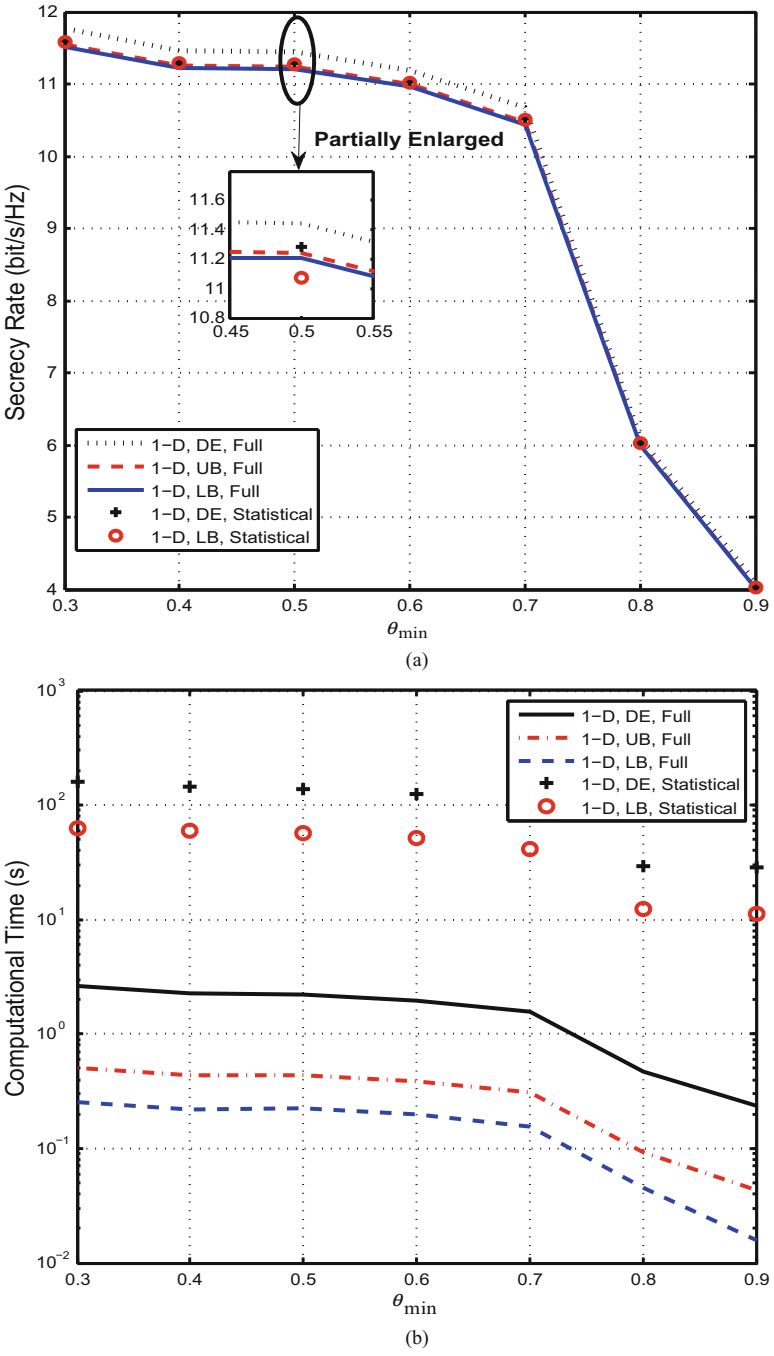


Fig. 5.7 Performance comparison with different success rate threshold. $S = 4, N = 5, q_j = 0.8$. (**a**) Achievable secrecy rate. (**b**) Computational time

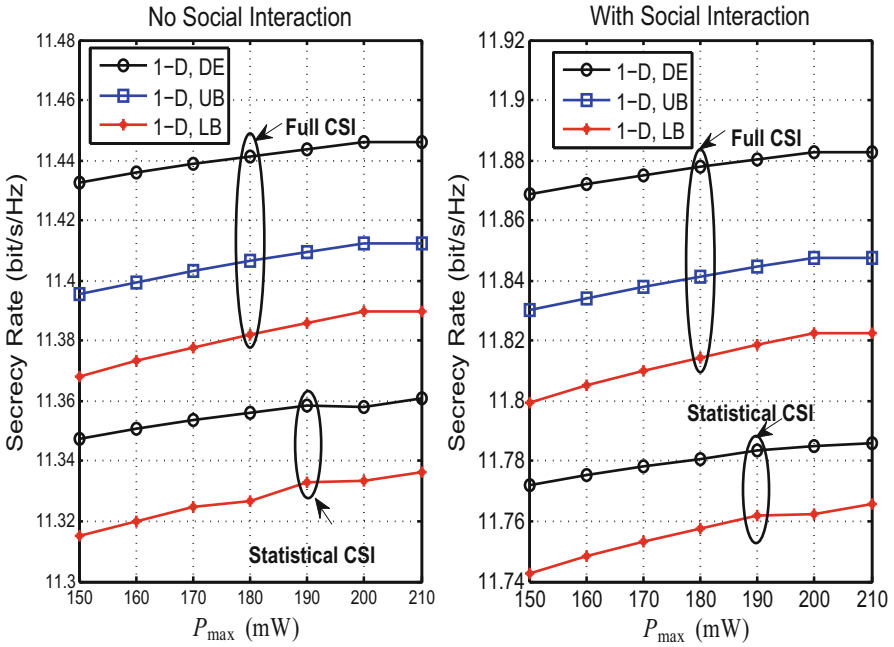


Fig. 5.8 Performance comparison with different social interaction assumptions. $S = 4, N = 5, \theta_{\min} = 0.5$

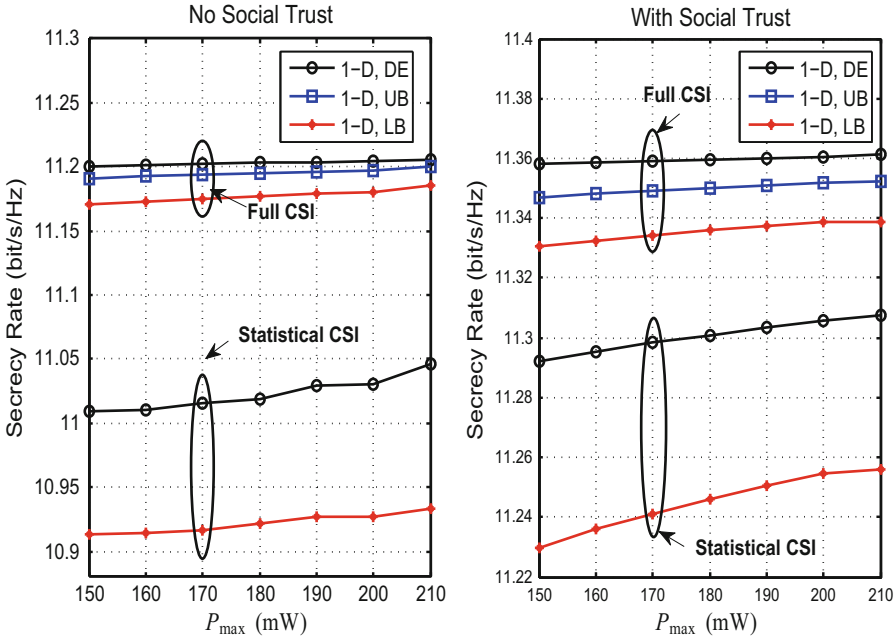


Fig. 5.9 Performance comparison with different social trust assumptions. $S = 4, N = 5, \theta_{\min} = 0.5$

of the social information index (including social interaction of candidate source nodes and social trust index of jammer nodes) on the achievable performance should be considered. In particular, let the estimated social trust index, the true social trust index, and the social trust index estimation error be $\tilde{q}_j$, $\hat{q}_j$, and Δq_j, respectively. They are related as

$$\tilde{q}_j = \hat{q}_j + \Delta q_j. \tag{5.22}$$

The normalized estimation error $\delta_q = |\Delta q_j/\hat{q}_j|$ characterizes the relative uncertainty of the social trust index. The parameter δ_T here characterizes the estimation error of social contact duration between mobile users. By using the estimated social characteristic index in the proposed algorithms, the secrecy rate and the ergodic secrecy rate are both affected and the impact of social characteristic index uncertainty can be assessed accordingly.

To illustrate the robustness of our approach, the impact of inaccurate social information indices with different estimation errors is shown in Fig. 5.10. Normally, the achievable secrecy rate increases with higher $P_{\max}$. However, a larger estimation error of δ_T and δ_q leads to a lower secrecy rate as expected. Nevertheless, the proposed optimization methods remain robust to such errors with graceful performance degradation.

5.4 The Social Interaction Case for Jammer Selection

After the source nodes are firstly selected considering their social interaction, the selection of the cooperative jamming partners are mainly discussed in this subsection. In a special and simple case, we can assume that there only exists one source node, and the social trust for jammer selection is mainly considered under the full CSI case and the partial CSI case, respectively. It should be noted that though there exists interference from the candidate jammers to the destination node, it can be known in advance and suppressed at the destination in a certain way. In addition to the Heuristic Genetic algorithm, the low-complexity approximate algorithms are also presented here to obtain the optimized results.

5.4.1 Optimal Jammer Selection with Full CSI

In this subsection, we focus on how to select the best jamming partner to hamper reception by the smartest social eavesdropper in D2D overlay for secrecy guarantee and high quality transmission, and it is assumed that BS can acquire accurate CSI of all involved links without considering the jamming interference at the destination. Meanwhile, one source node is considered, i.e., $S = 1$, thus the symbol s in the following objective function only stands for the source node, but not a variable.

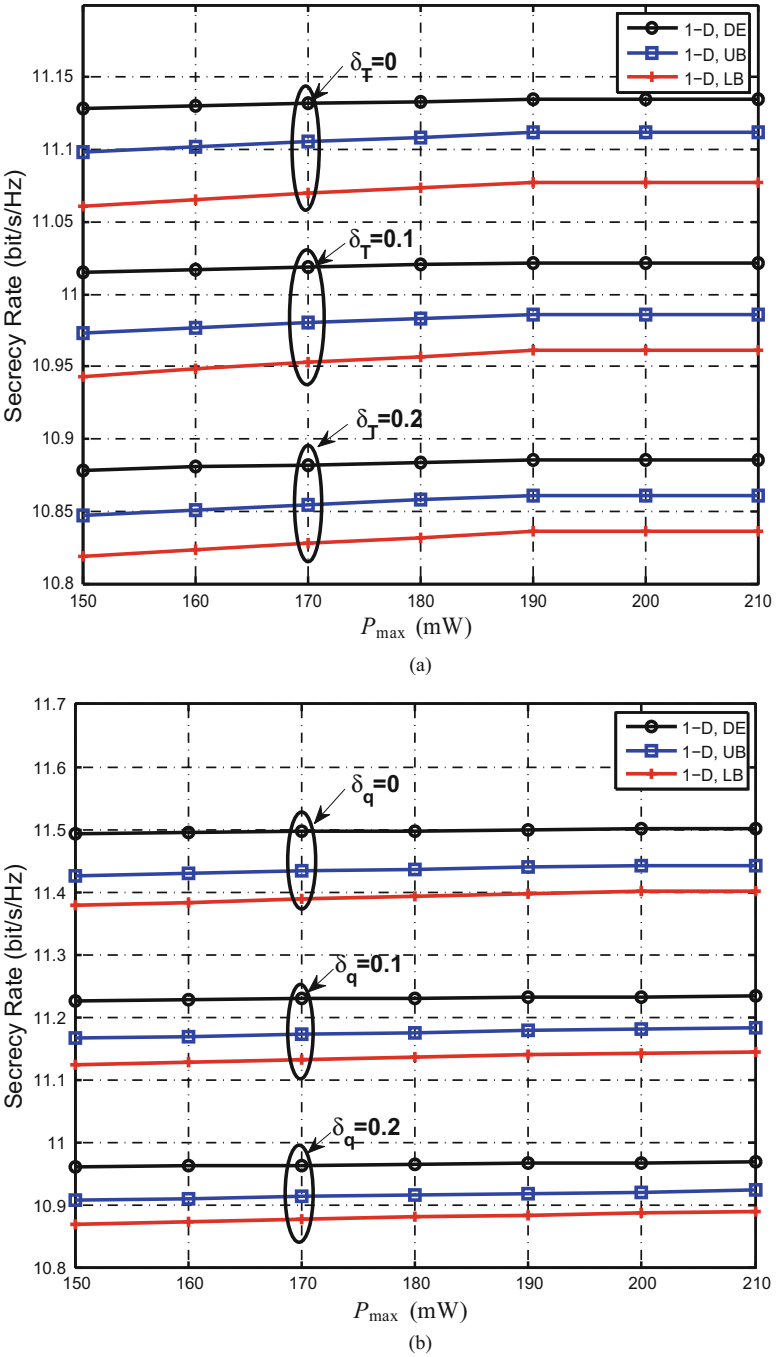


Fig. 5.10 Performance comparison with different social information estimation error in full CSI case. $S = 4, N = 5, \theta_{\min} = 0.5$. (**a**) Impact of social interaction index estimation error. (**b**) Impact of social trust index estimation error

Thus, the problem Eq. (5.4) can be relaxed as

$$C_{j,k}(P_s, P_j) = q_j \left[\log_2 (1 + P_s g_{sd}) - \log_2 \left(1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1} \right) \right]^+ + (1 - q_j) \left[\log_2 (1 + P_s g_{sd}) - \log_2 (1 + P_s g_{sk}) \right]^+ . \tag{5.23}$$

The optimization problem in Eq. (5.23) is non-convex, and its solution can be found by using genetic algorithm (GA) [21].

5.4.1.1 Heuristic Genetic Algorithm Based Direct Evaluation

GA is a well-known heuristic optimization algorithm that imitates some processes in natural evolution. Following the model of evolution, GA establishes a population of individuals, each corresponds to a point in the search space. Using well-conceived operations, the next generation is formed based on the survival of the fittest. Therefore, the evolution from one generation to the next tends to result in potentially better solutions in the search space. Studies have shown that GA can possibly converge to global optima for a large class of non-convex problems [22].

In the situation that optimal jammer selection with full CSI, for a given set of eavesdropper and jammer, the values of q_j, g_{sd}, g_{sk}, and h_{jk} are determined. Therefore, variables of the optimization problem in Eq. (5.23) are P_s and P_j. Detailed, we can use the following four steps to obtain the optimal solution of Eq. (5.23).

Step 1: Randomly create a population of individuals, representing an initial set of P_s and P_j;
Step 2: Every individual in the population is evaluated by fitness values, which are associated with values of $C_{j,k}$;
Step 3: The population is evolved to form a new one by selection, crossover and mutation. New population usually indicates more suitable P_s and P_j which lead to a larger $C_{j,k}$;
Step 4: Go to Step 2 unless the termination condition is satisfied.

After several iterations, GA will converge to the best individual, which hopefully represents the optimal or suboptimal solution to the optimization problem. In other words, the finally generated individuals are the optimal or suboptimal transmit powers for D2D transmitter and the corresponding jamming partner, P_s, P_j, for the optimization problem.

Obviously, the heuristic GA has the potential to converge to a global optimum. However, this heuristic algorithm does not provide a (worst-case) performance guarantee. In order to reduce computation complexity, the upper and lower bounds of the original secrecy rate are utilized for making comparisons.

5.4.1.2 Complexity Reduction Leveraging Upper Bound

Similar to the discussion in Sect. 5.3.1.2, using the well-known inequality $\ln(x) \leq x-1$ for any $x>0$, we have

$$\begin{aligned}\ln 2 \cdot C_{j,k}(P_s,P_j) =& q_j\left[\ln\frac{1+P_s g_{sd}}{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}\right]^+ + (1-q_j)\left[\ln\frac{1+P_s g_{sd}}{1+P_s g_s}\right]^+ \\ \leq& q_j\left[\frac{1+P_s g_{sd}}{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}-1\right]^+ + (1-q_j)\left[\frac{1+P_s g_{sd}}{1+P_s g_{sk}}-1\right]^+ \\ =& q_j\left[\frac{P_s g_{sd}-\frac{P_s g_{sk}}{P_j h_{jk}+1}}{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}\right]^+ + (1-q_j)\frac{P_s\,[g_{sd}-g_{sk}]^+}{1+P_s g_{sk}}, \end{aligned} \tag{5.24}$$

using the j-th jammer to intercept the k-th eavesdropper.

In practical, interference from jammer to eavesdropper is usually dominant over background noise, i.e., $P_j h_{jk} \gg 1$. Thus, $P_j h_{jk}+1 \approx P_j h_{jk}$, which can be used to further simplify Eq. (5.24). Hence the upper bound for the worst case can be approximated as

$$\max_{(P_s,P_j)\in\mathscr{X}} \min_{k\in\mathscr{K}} \left\{ q_j\left[\frac{P_j g_{sd}-\frac{g_{sk}}{h_{jk}}}{\frac{P_j}{P_s}+\frac{g_{sk}}{h_{jk}}}\right]^+ + (1-q_j)\frac{P_s[g_{sd}-g_{sk}]^+}{1+P_s g_{sk}}\right\}, \tag{5.25}$$

which can significantly reduce the complexity of optimization.

5.4.1.3 Complexity Reduction Leveraging Lower Bound

From $[\ln(1+x)]^+ \geq \left[\frac{2x}{2+x}\right]^+$, we have

$$\begin{aligned}\ln 2 \cdot C_k(P_s,P_j,q_j) =& q_j\left[\ln\frac{1+P_s g_{sd}}{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}\right]^+ + (1-q_j)\left[\ln\frac{1+P_s g_{sd}}{1+P_s g_{sk}}\right]^+ \\ \geq& \frac{2q_j\left[\frac{1+P_s g_{sd}}{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}-1\right]^+}{2+\left[\frac{1+P_s g_{sd}}{1+\frac{P_s g_{sk}}{P_j h_{jk}+1}}-1\right]^+} + \frac{2(1-q_j)\left[\frac{1+P_s g_{sd}}{1+P_s g_{sk}}-1\right]^+}{2+\left[\frac{1+P_s g_{sd}}{1+P_s g_{sk}}-1\right]^+}. \end{aligned} \tag{5.26}$$

Similarly, it is supposed that the interference from jammer to eavesdropper is dominant comparing to the background noise, i.e., $P_j h_{jk} \gg 1$, and $P_j h_{jk}+1 \approx P_j h_{jk}$.

Hence optimization problem can be approximated to the following problem,

$$\max_{(P_s,P_j)\in\mathscr{X}} \min_k \left\{ \frac{2q_j}{2\left[\frac{P_j h_{jk}+P_s g_{sk}}{P_s P_j g_{sd} h_{jk}-P_s g_{sk}}\right]^+ + 1} + \frac{2(1-q_j)}{2\left[\frac{1+P_s g_{sk}}{P_s(g_{sd}-g_{sk})^+}\right] + 1} \right\}. \tag{5.27}$$

Let

$$\begin{aligned} f_1(P_s,P_j) &= 2\left[\frac{P_j h_{jk}+P_s g_{sk}}{P_s P_j g_{sd} h_{jk}-P_s g_{sk}}\right]^+ + 1, \\ f_2(P_s,P_j) &= 2\left[\frac{1+P_s g_{sk}}{P_s(g_{sd}-g_{sk})^+}\right] + 1. \end{aligned} \tag{5.28}$$

Equation (5.27) can be rewritten as,

$$\max_{(P_s,P_j)\in\mathscr{X}} \min_k \left\{ \frac{2q_j}{f_1(P_s,P_j)} + \frac{2(1-q_j)}{f_2(P_s,P_j)} \right\}. \tag{5.29}$$

Equivalently, the problem in Eq. (5.29) can be expressed as

$$\min_{(P_s,P_j)\in\mathscr{X}} \max_k \left\{ \frac{f_1(P_s,P_j) f_2(P_s,P_j)}{2q_j f_2(P_s,P_j) + 2(1-q_j) f_1(P_s,P_j)} \right\} = \min_{(P_s,P_j)\in\mathscr{X}} \max_k \left\{ \frac{w_k(P_s,P_j)}{z_k(P_s,P_j)} \right\}. \tag{5.30}$$

Notice that the optimization problem is no-convex, since both $w_k(P_s,P_j)$ and $z_k(P_s,P_j)$ are nonlinear functions of P_s and P_j.

Similar with the Sect. 5.3.1.2, the Dinkelbach-type algorithm is applied here to solve the generalized fractional programming problem, and the details of the optimization using Dinkelbach-type Algorithm are given as Algorithm 2.

5.4.2 *Optimal Jammer Selection with Partial CSI*

In this subsection, joint power allocation with cooperative jammer selection in partial CSI case is considered, where instantaneous CSI of g_{sd} and h_{jd}, and statistical CSI of g_{sk} and h_{jk} are available.

5.4.2.1 Direct Evaluated Ergodic Sum Rate

Since only statistical CSI of g_{sk} and h_{jk} can be acquired by the BS, the maximization of sum rate of the system as shown in Eq. (5.7) can be changed into

$$\max_{(P_s,P_j)\in\mathscr{X}} \min_{k\in\mathscr{K}} \mathrm{E}\left\{C_{j,k}(P_s,P_j)\right\}, \tag{5.31}$$

Algorithm 2: Dinkelbach-type Algorithm

$(P_s^{(i)}, P_j^{(i)})$: the i-th iteration of the transmit power for D2D transmitter and jammer node.
$\mathscr{X}$: the feasible set of power parameters. l: the number of iteration.

begin

Referring to Eq. (5.28) and Eq. (5.30),

Step 1: Take $(P_s^{(0)}, P_j^{(0)}) \in \mathscr{X}$, compute $\mu_1 = \max\limits_k \left\{w_k(P_s^{(0)}, P_j^{(0)})/z_k(P_s^{(0)}, P_j^{(0)})\right\}$, and let $l = 1$.

Step 2: Determine $(P_s^{(l)}, P_j^{(l)}) = \arg \min\limits_{(P_s,P_j)\in\mathscr{X}} \left\{\max\limits_k\{w_k(P_s, P_j) - \mu_l z_k(P_s, P_j)\}\right\}$.

$F_k(\mu_l) = \min\limits_{(P_s,P_j)\in\mathscr{X}} \max\limits_k \{w_k(P_s, P_j) - \mu_l z_k(P_s, P_j)\}$.

Step 3:

if $F_k(\mu_l) = 0$ **then**

The optimal solution is $(P_s^*, P_j^*) = (P_s^{(l)}, P_j^{(l)})$ with optimal objective value $\mu^* = \mu_l$ and **Stop**.

else

Go to **Step 4**;

end

Step 4: Let $\mu_{l+1} = \max\limits_k \left\{w_k(P_s^{(l)}, P_j^{(l)})/z_k(P_s^{(l)}, P_j^{(l)})\right\}$, let $l = l + 1$, and go to **Step 2**.

end

where

$$\begin{aligned}\mathrm{E}\left\{C_{j,k}(P_s, P_j)\right\} =& q_j\left[\log_2(1 + P_s g_{sd}) - \mathrm{E}\left\{\log_2\left(1 + \frac{P_s g_{sk}}{P_j h_{jk} + 1}\right)\right\}\right]^+ \\ &+ \left(1 - q_j\right)\left[\log_2(1 + P_s g_{sd}) - \mathrm{E}\left\{\log_2(1 + P_s g_{sk})\right\}\right]^+. \end{aligned} \tag{5.32}$$

Recall that, the s is only a symbol that stands for the source node as aforementioned.

Applying the Lemma 5.1, the optimization problem in Eq. (5.31) can be expressed as,

$$\begin{aligned}\max_{(P_s,P_j)\in\mathscr{X}} \min_{k\in\mathscr{K}} \Bigg\{ & q_j\left[\log_2(1 + P_s g_{sd}) - \frac{\phi(P_s\lambda_g) - \phi(P_j\lambda_h)}{\ln 2 \cdot (1 - \frac{P_j\lambda_h}{P_s\lambda_g})}\right]^+ \\ & + (1 - q_j)\left[\log_2(1 + P_s g_{sd}) - \frac{\phi(P_s\lambda_g)}{\ln 2}\right]^+ \Bigg\}. \end{aligned} \tag{5.33}$$

5.4.2.2 Complexity Reduction with Ergodic Lower Bound

By leveraging Jensen's inequality, the lower bound of the ergodic sum rate in Eq. (5.33) can be expressed as

$$\begin{aligned}
&q_j\left[\log_2(1+P_s g_{sd})-\mathrm{E}\left\{\log_2\left(1+\frac{P_s g_{sk}}{P_j h_{jk}+1}\right)\right\}\right]^+\\
&+(1-q_j)\left[\log_2(1+P_s g_{sd})-\mathrm{E}\left\{\log_2(1+P_s g_{sk})\right\}\right]^+\\
&\geq q_j\left[\log_2(1+P_s g_{sd})-\log_2\left(1+\mathrm{E}\left[\frac{P_s g_{sk}}{P_j h_{jk}+1}\right]\right)\right]^+\\
&+(1-q_j)\left[\log_2(1+P_s g_{sd})-\log_2(1+\mathrm{E}\left[P_s g_{sk}\right])\right]^+\\
&=q_j\left[\log_2(1+P_s g_{sd})-\log_2\left(1+P_s\lambda_g\mathrm{E}\left[\frac{1}{P_j h_{jk}+1}\right]\right)\right]^+\\
&+(1-q_j)\left[\log_2(1+P_s g_{sd})-\log_2(1+P_s\lambda_g)\right]^+. \qquad (5.34)
\end{aligned}$$

Using Eq. (6) on page 194 of [19], for $X\sim\mathrm{Exp}(\lambda)$, we have,

$$\begin{aligned}
\mathrm{E}\left[\frac{1}{PX+1}\right]&=\int_0^\infty\frac{1}{Px+1}\frac{1}{\lambda}e^{-\frac{x}{\lambda}}dx=\int_0^\infty\frac{1}{P\lambda x+1}e^{-x}dx\\
&=\frac{1}{P\lambda}\int_0^\infty\frac{1}{t+1}e^{-\frac{1}{P\lambda}t}dt=\frac{1}{P\lambda}e^{\frac{1}{P\lambda}}E_1\left(\frac{1}{P\lambda}\right)=\frac{\phi\left(P\lambda\right)}{P\lambda}. \qquad (5.35)
\end{aligned}$$

Using Jensen's inequality in this case, therefore,

$$\mathrm{E}\left\{\log_2\left(1+\frac{P_s g_{sk}}{P_j h_{jk}+1}\right)\right\}\leq\log_2\left(1+\frac{P_s\lambda_g}{P_j\lambda_h}\phi\left(P_j\lambda_h\right)\right), \qquad (5.36)$$

$$\mathrm{E}\left\{\log_2\left(1+P_s g_{sk}\right)\right\}\leq\log_2\left(1+P_s\lambda_g\right). \qquad (5.37)$$

Thus, the problem can be optimized by maximizing the lower bound of the original objective function by considering power allocation, i.e. maximizing the lower bound of the ergodic sum rate:

$$\begin{aligned}
\max_{(P_s,P_j)\in\mathscr{X}}\min_{k\in\mathscr{K}}\Bigg\{&q_j\left[\log_2(1+P_s g_{sd})-\log_2\left(1+\frac{P_s\lambda_g}{P_j\lambda_h}\phi(P_j\lambda_h)\right)\right]^+\\
&+(1-q_j)\left[\log_2(1+P_s g_{sd})-\log_2(1+P_s\lambda_g)\right]^+\Bigg\}. \qquad (5.38)
\end{aligned}$$

Although Eq. (5.38) is much simpler than Eq. (5.33), it is still a non-convex function, and the GA can also be used to accomplish the joint power optimization of P_s and P_j.

5.4.3 One Dimensional Search with Low Complexity

To further reduce the complexity of the proposed algorithm, a one-dimensional search is also presented here under the full CSI case. Considering the total transmission power constraint of P_j and P_s, the following Proposition 5.2 is presented firstly.

Proposition 5.2 *The optimal solution of Eq.* (5.25) *must satisfy* $P_s + P_j = \min(P^s_{\max} + P^j_{\max}, P_{\max})$.

Proof Denoting

$$f(P_s, P_j) = q_j \left[\frac{P_j g_{sd} - \frac{g_{sk}}{h_{jk}}}{\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}}} \right]^+ + (1 - q_j) \frac{P_s [g_{sd} - g_{sk}]^+}{1 + P_s g_{sk}}, \tag{5.39}$$

and the monotonicity of $f(P_s, P_j)$ will be discussed by means of partial derivative as follows.

1. $g_{sd} > g_{sk}$ and $P_j g_{sd} > \frac{g_{sk}}{h_{jk}}$:
   Then we can rewrite $f(P_s, P_j)$ and the corresponding partial derivative as,

$$f(P_s, P_j) = q_j \frac{P_j g_{sd} - \frac{g_{sk}}{h_{jk}}}{\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}}} + (1 - q_j) \frac{P_s (g_{sd} - g_{sk})}{1 + P_s g_{sk}},$$

$$\frac{\partial f(P_s, P_j)}{\partial P_s} = q_j \frac{\left(P_j g_{sd} - \frac{g_{sk}}{h_{jk}} \right) P_j}{\left(P_j + \frac{g_{sk}}{h_{jk}} P_s \right)^2} (1 - q_j) \frac{g_{sd} - g_{sk}}{(1 P_s g_{sk})^2} > 0,$$

$$\frac{\partial f(P_s, P_j)}{\partial P_j} = q_j \frac{\left(g_{sd} + \frac{1}{P_s} \right) \frac{g_{sk}}{h_{jk}}}{\left(\frac{P_j}{P_s} + \frac{g_{sk}}{h_{jk}} \right)^2} > 0.$$

2. $g_{sd} > g_{sk}$ and $P_j g_{sd} \leq \frac{g_{sk}}{h_{jk}}$:
   In this case, $f(P_s, P_j)$ and its partial derivative can be expressed as,

$$f(P_s, P_j) = (1 - q_j) \frac{P_s (g_{sd} - g_{sk})}{1 + P_s g_{sk}},$$

$$\frac{\partial f(P_s,P_j)}{\partial P_s}=(1-q_j)\frac{g_{sd}-g_{sk}}{(1+P_s g_{sk})^2}>0,$$
$$\frac{\partial f(P_s,P_j)}{\partial P_j}=0.$$

3. $g_{sd}\le g_{sk}$ and $P_j g_{sd}>\frac{g_{sk}}{h_{jk}}$:
Then we have,

$$f(P_s,P_j)=q_j\frac{P_j g_{sd}-\frac{g_{sk}}{h_{jk}}}{\frac{P_j}{P_s}+\frac{g_{sk}}{h_{jk}}},$$
$$\frac{\partial f(P_s,P_j)}{\partial P_s}=q_j\frac{\left(P_j g_{sd}-\frac{g_{sk}}{h_{jk}}\right)P_j}{\left(P_j+\frac{g_{sk}}{h_{jk}}P_s\right)^2}>0,$$
$$\frac{\partial f(P_s,P_j)}{\partial P_j}=q_j\frac{\left(g_{sd}+\frac{1}{P_s}\right)\frac{g_{sk}}{h_{jk}}}{\left(\frac{P_j}{P_s}+\frac{g_{sk}}{h_{jk}}\right)^2}>0.$$

4. $g_{sd}\le g_{sk}$ and $P_j g_{sd}\le\frac{g_{sk}}{h_{jk}}$:
Then $f(P_s,P_j)$=0.

To sum up, the partial derivative of $f(P_s,P_j)$ in Eq. (5.39) can be expressed as,

$$\frac{\partial f(P_s,P_j)}{\partial P_s}=q_j\frac{\left[P_j g_{sd}-\frac{g_{sk}}{h_{jk}}\right]^+P_j}{\left(P_j+\frac{g_{sk}}{h_{jk}}P_s\right)^2}+(1-q_j)\frac{[g_{sd}-g_{sk}]^+}{(1+P_s g_{sk})^2}\ge 0,$$
$$\frac{\partial f(P_s,P_j)}{\partial P_j}=q_j\frac{\left(g_{sd}+\frac{1}{P_s}\right)\frac{g_{sk}}{h_{jk}}}{\left(\frac{P_j}{P_s}+\frac{g_{sk}}{h_{jk}}\right)^2}\cdot u\left(P_j g_{sd}-\frac{g_{sk}}{h_{jk}}\right)\ge 0,$$

where $u(\cdot)$ is the unit step function.

Therefore, the problem described in Eq. (5.25) is a nondecreasing function with the increasing of P_s and P_j, respectively. Similarly, without joint power constraint in Eq. (5.3), we have a trivial solution $P_s=P^s_{\max}$ and $P_j=P^j_{\max}$. With the joint power constraint $P_s+P_j\le P_{\max}$, the optimal solution must satisfy $P_s+P_j=\min(P^s_{\max}+P^j_{\max},P_{\max})$.

Furthermore, it can be inferred from Proposition 5.2 that:

(i) For the case when $P^s_{\max}+P^j_{\max}\le P_{\max}$, the optimal solution is $P_s=P^s_{\max}$ and $P_j=P^j_{\max}$.

(ii) For the case when $P^s_{\max} + P^j_{\max} > P_{\max}$, the optimization problem can be rewritten as

$$\max_{P_s} \min_{k} \left\{ q_j \left[\frac{(P_{\max} - P_s) g_{sd} - \frac{g_{sk}}{h_{jk}}}{P_{\max}/P_s - 1 + g_{sk}/h_{jk}} \right]^+ + (1 - q_j) \frac{P_s [g_{sd} - g_{sk}]^+}{1 + P_s g_{sk}} \right\}. \tag{5.40}$$

In other words, there is no need to search for optimal power for the case of $P^s_{\max} + P^j_{\max} \leq P_{\max}$. As a result, power optimization will be executed only in the case of $P^s_{\max} + P^j_{\max} > P_{\max}$, where the optimization problem turns into a 1-dimension searching problem over P_s.

5.4.4 Simulation and Numerical Results

For convenience, in the simulation test, "Full" represents the case when full knowledge of CSI is assumed for all the links, and "Partial" means that full CSI of g_{sd} and h_{jd} and statistical knowledge of CSI of g_{sk} and h_{jk} are available. In this case, different methods have been adopted to optimise P_s and P_j to maximise the secrecy rate of D2D links, and only the optimization solved by upper bound leverages the 1-D search. Table 5.3 shows some related abbreviations in simulation results, and the main simulation parameters are generally in consistent with the general case in Table 5.2.

5.4.4.1 Impact of Number of Jammer Nodes

Figures 5.11 and 5.12 illustrate the effects of number of jammer nodes (N) on the achievable secrecy rate and corresponding computational time. Figure 5.11 shows that the achievable secrecy rate grows with increasing N when the other parameters are fixed, since more jammers result in a higher possibility that a better jammer can be found to combat eavesdropping, thereby lead to better performance.

Generally, the performance of full CSI case exceeds that of partial CSI case as we can imagine, yet the performance gap is negligible. In addition, the brute force algorithm outperforms the direct evaluation by GA with very limited performance

Table 5.3 Main abbreviations in simulation results

Abbreviations	Connotations
DE-GA	The optimization problem is solved by direct evaluation by utilizing GA
LB-GA	The optimization problem is solved by leveraging the lower bound by utilizing GA

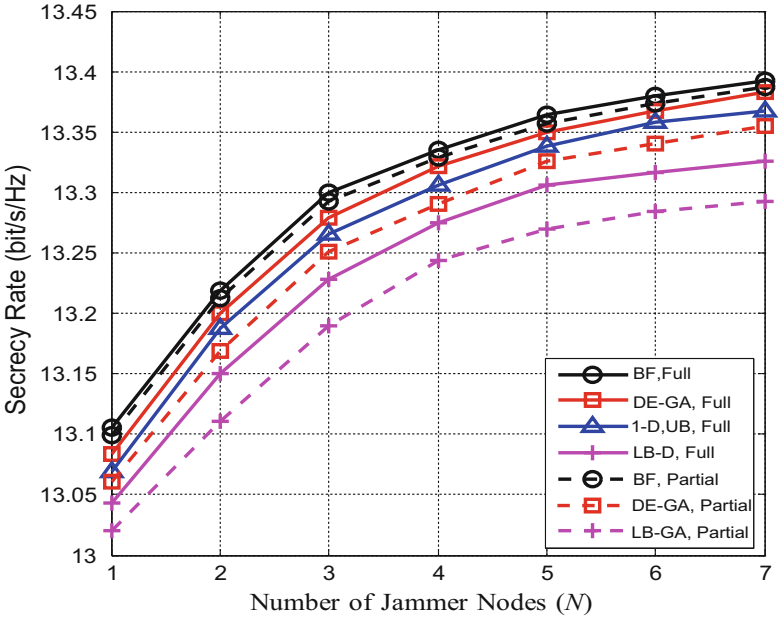


Fig. 5.11 Secrecy rate vs. the number of jammer nodes index, $q_j = 0.5$

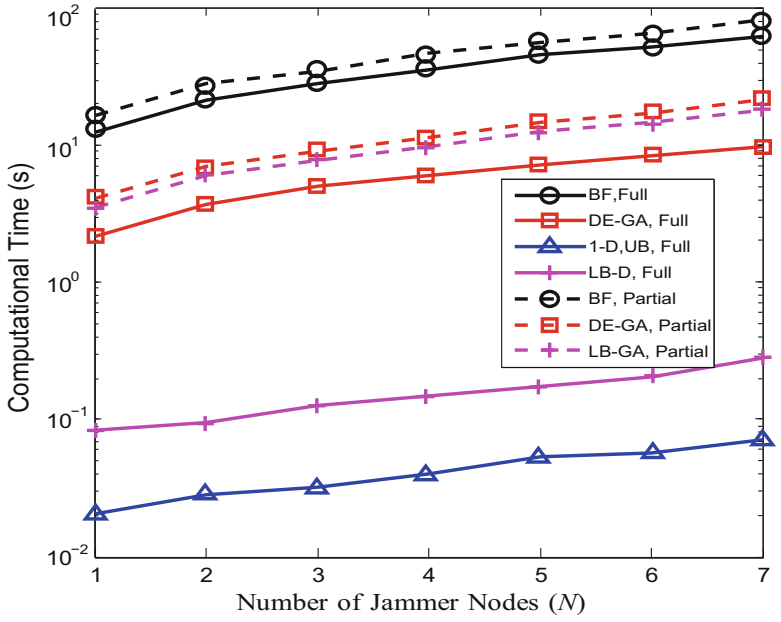


Fig. 5.12 Computational time vs. the number of jammer nodes index, $q_j = 0.5$

gap. Algorithms leveraging upper and lower bounds achieve less satisfying performance when compared to the brute force algorithm and GA, but the performance gap between different algorithms is insignificant.

Figure 5.12 demonstrates the computational time of different methods, which can reflect the complexities of different algorithms. Apparently, the computational time increases significantly with larger number of jammer nodes since power optimization should be executed for every candidate jammer node to select the best one. Methods with partial CSI is generally more time-consuming than that with full CSI, since the calculation of the expectation consumes more time than using accurate channel gains in the expression of achievable secrecy rate. Furthermore, computational time of the brute force algorithm is much higher than the other methods. Direct evaluation, which is taken by using GA, costs less time than brute force but is still more time-consuming compared to the other methods. In partial CSI case, the lower-bound method computes faster since it has less number of integration than direct evaluation. In the assumption of full CSI, the lower-bound method, which is solved by GFP, does have lower complexity. The upper-bound method is the most time-saving since it transforms the joint power optimization into a problem with only one variable.

5.4.4.2 Impact of Sum Transmit Power Limitation

In this part, 5 and 10 jammer nodes are randomly generated respectively, which are uniformly distributed within the network coverage area. The achievable secrecy rate is averaged over 10 random network realizations for each transmit power limitation $P_{\max}$. As shown in Fig. 5.13, the achievable secrecy rate increases with looser power constraint in partial CSI case. Larger $P_{\max}$ indicates that more power is available at D2D transmitter and jammer nodes, which leads to a higher probability that better power allocation can be found to achieve higher secrecy rate. From Fig. 5.11 and 5.13, it is clear that higher secrecy rate can be achieved with increased jammer density, i.e., more jammers in vicinity can lead to better performance.

Comparing the algorithms in both full CSI and partial CSI cases, Fig. 5.14 shows that higher secrecy rate can be achieved with larger $P_{\max}$, which is coincident with the results in Fig. 5.13. Naturally, full CSI case outperforms the partial CSI case. Moreover, the achievable secrecy rate of the brute force algorithm exceeds that of the other methods, among which GA is a close second best. The upper-bound method and lower-bound method exhibit mild performance gap when compared to the high complexity brute force algorithm as well as the GA.

5.4.4.3 Impact of Social Trust Index

The trust level of jammer nodes is crucial for the selection of the best jammer to hamper eavesdropping. In Fig. 5.15, the impact of social trust index of jammer nodes on the performance of secrecy rate is investigated by comparing different

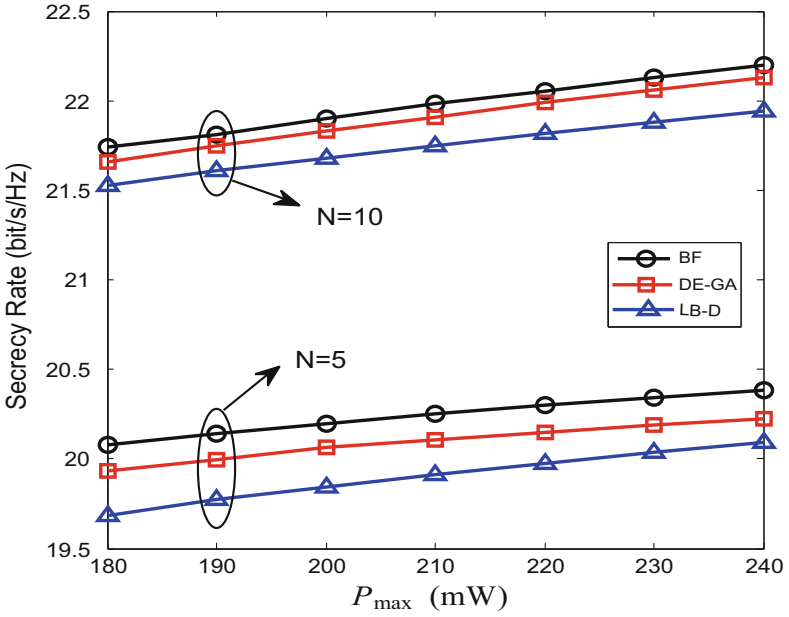


Fig. 5.13 Secrecy rate vs. sum transmit power limitation and number of jammer nodes in partial CSI case, $q_j = 0.5$

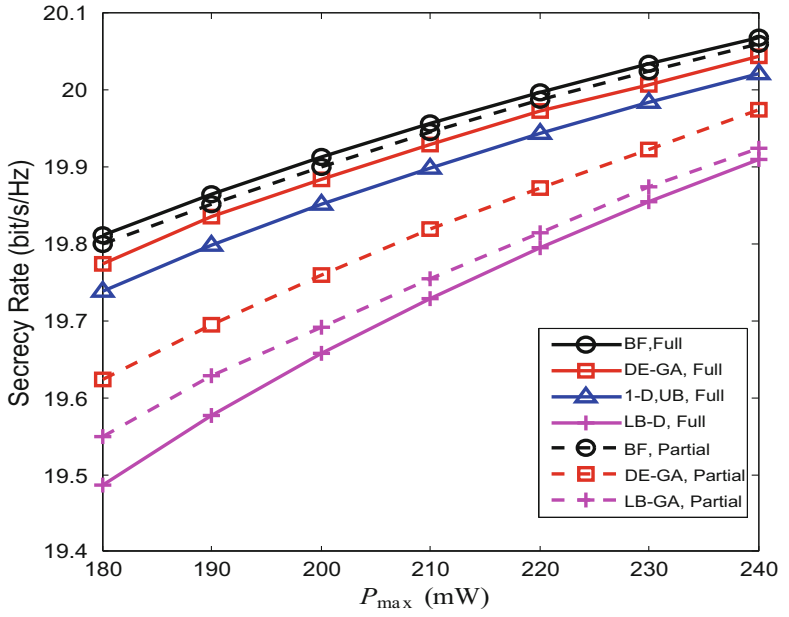


Fig. 5.14 Secrecy rate vs. sum transmit power limitation, $q_j = 0.5$

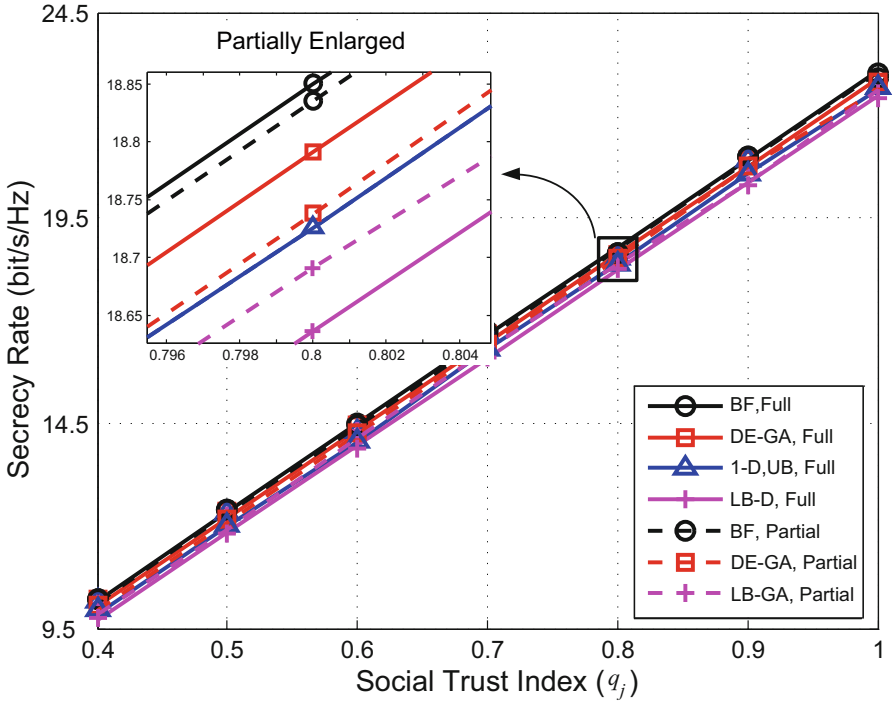


Fig. 5.15 Secrecy rate vs. social trust index of jammer nodes

optimization methods with different CSI assumptions. Recall that, social trust can be represented by link stability or deduced by trustiness of the cooperative jamming nodes, i.e., the probability to utilize the allocated transmit power to support secure transmission of the desired links. When social trust index is higher for the jammer nodes, it is more dependable to act as a jammer when requested. However, a jammer node with low social trust index has a high probability to refuse sending jamming transmission even though it is allocated a certain power. In this case, the allocated jamming power is wasted and the secrecy rate would deteriorate as a result. In other words, the social trust index of the jammer nodes indicates the success probability of acting as desired friendly jammer nodes. Higher social trust index naturally leads to better system performance.

5.5 Chapter Summary

In this chapter, secure transmission for content sharing has been investigated in cellular D2D overlays communication system. The schemes of joint power allocation with the source and jammer selection have been investigated to improve

secrecy and privacy of D2D communications. When there exist multiple source nodes, the social interaction has been exploited for selecting the optimal source node who holds the desired content to share with the destination node by considering both the physical links and social characteristics. Meanwhile, targeting the worst eavesdropping case by the potential smartest eavesdropper, reliable jammer has been selected based on its inherent social trust property. To maximize the achievable secrecy rate of the content sharing between content helper and content requester with the help of jammer partner against eavesdropping, a cooperative security optimization problem has been proposed. To solve the non-convex optimization problem, low complexity solutions have been developed in addition to the brute force search algorithm and heuristic algorithms. Specifically, upper bound and lower bound of the original objective function have also been considered to obtain the optimized solutions with low complexity. Meanwhile, in addition to the ideal case assuming that full CSI of all involved links can be acquired, more practical cases have also been discussed in terms of the partial CSI case and the statistical CSI case when only channel statistics information is available.

References

1. J. Pääkkönen, C. Hollanti, and O. Tirkkonen, "Device-to-device data storage for mobile cellular systems," in *Proc. 2013 IEEE Global Communications Conference Workshops (GLOBECOM Workshops),* Atlanta, Georgia, USA, Dec. 2013, pp. 671–676.
2. L. Wang, C. Cao, and H. Wu, "Secure inter-cluster communications with cooperative jamming against social outcasts," *Computer Communications*, vol. 63, no. 1, pp. 1–10, Jun. 2015.
3. L. Wang and H. Wu, "Jamming partner selection for maximising the worst D2D secrecy rate based on social trust," *IEEE Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 2, Feb. 2017.
4. X. Chen, B. Proulx, X. Gong, and J. Zhang, "Social trust and social reciprocity based cooperative D2D communications," in *Proc. 14th ACM International Symposium on Mobile Ad Hoc NETWORKING and Cumputing*, Bangalore, India, Aug. 2013, pp. 187–196.
5. L. Wang, H. Wu, and G. L. Stüber, "Cooperative jamming aided secrecy enhancement in P2P communications with social interaction constraints," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1144–1158, Feb. 2017.
6. H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.
7. Z. Ding and Y. Li, *Blind Equalization and Identification*, New York: Marcel Dekker, 2001.
8. A. K. Sadek, Z. Han, and K. J. R. Liu, "Distributed relay-assignment protocols for coverage expansion in cooperative wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 4, pp. 505–515, Apr. 2010.
9. L. Wang, H. Tang, and M. Čierny, "Device-to-device link admission policy based on social interaction information," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 9, pp. 4180–4186, Sept. 2015.
10. D. Bertsimas and J. Tsitsiklis, "Simulated Annealing," *Statistical Science*, vol. 8, no. 1, pp. 10–15, Feb. 1993.
11. V. Granville, M. Křivánek, and J.-P. Rasson, "Simulated annealing: A proof of convergence," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 16, no. 6, pp. 652–656, Jun. 1994.

12. T. D. Hoang, L. B. Le, and T. L.-Ngoc, "Energy-efficient resource allocation for D2D communications in cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 6972–6986, Sept. 2015.
13. H. Min, J. Lee, S. Park, and D. Hong, "Capacity enhancement using an interference limited area for device-to-device uplink underlaying cellular networks," *IEEE Transactions on Wireless Communications,* vol. 10, no. 12, pp. 3995–4000, Dec. 2011.
14. S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.
15. A. I. Barros, J. B. G. Frenk, S. Schaible, and S. Zhang, "A new algorithm for generalized fractional programs," *Mathematical Programming*, vol. 72, no. 2, pp. 147–175, Feb. 1996.
16. J. P. Crouzeix, J. A. Ferland, and S. Schaible, "An algorithm for generalized fractional programs," *Journal of Optimization Theory and Applications*, vol. 47, no. 1, pp. 35–49, Sept. 1985.
17. R. G. Ródenas, M. L. López, and D. Verastegui, "Extensions of Dinkelbach's algorithm for solving non-linear fractional programming problems," vol. 7, no. 1, pp. 33–70, Jun. 1999.
18. M.-S. Alouini and A. J. Goldsmith, "Capacity of rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Transactions on Vehicular Technology*, vol. 48, no. 4, pp. 1165–1181, Jul. 1999.
19. M. Geller and E. W. Ng, "A table of integrals of the exponential integral," *Journal of reserach of the national bureau of standards - B. Mathematics and Mathematical Science*, vol. 73, no. 3, pp. 191–210, Jul.-Sept. 1969.
20. A. Erdélyi, W. Magnus, F. Oberhettinger, and F. G. Tricomi, *Tables of Integral Transforms*, McGraw Hill, 1954.
21. P. Guo, X. Wang, and Y. Han, "The enhanced genetic algorithm for the optimization design," in *Proc. 3rd International Conference on Biomedical Engineering and Informatics*, Yantai, China, Oct. 2010, pp. 2990–2994.
22. L. Davis, Ed., *Handbook of Genetic Algorithm*, Van Nostrand Reinhold, 1991.

Chapter 6
Summary

Guaranteeing the confidentiality in wireless communications is always a challenging task, which means we cannot simply regard the issues of security as relying on the cryptographic material in the upper layer. Compared to the wired networks, the wireless networks lack a physical boundary due to the broadcasting nature of wireless medium. So exploiting the feature at the physical layer is also of importance to secrecy performance improvement. Various schemes of physical layer security have been designed to enhance the wireless secrecy, among which the strategy based on the idea of wireless entity cooperation is promising. Motivated by investigating how the wireless cooperative networks play an essential role in the physical layer security, we wrote this book to summarize our corresponding works, from introducing the basic concepts of wireless cooperative networks and physical layer security, to the specific application with respect to certain techniques.

The corresponding contents started with an introduction in Chap. 1, in which some fundamentals about physical layer security and wireless cooperative networks were comprehensively summarized as an overview. Specifically, we mainly focused on the technical and conceptual development and performance metrics to introduce the physical layer security. Furthermore, the wireless cooperative networks was described in terms of principles, classification, and applications, respectively. Furthermore, we reviewed secrecy enhancement by using wireless cooperative techniques. A number of methods have been introduced in terms of their ability to improve security, which consist of intentionally designed coding and signaling schemes that are able to harness the properties of the physical layer. We intentionally divided such methods into two categories: signal-antenna system and multi-antenna system. Meanwhile, a variety of canonical scenarios have been outlined, focusing on providing an intuitive way to illustrate how the wireless nodes cooperate with each other.

In Chap. 2, we have discussed some details about some existing techniques from their basic principles to the issues of physical layer security. Specifically, time reversal (TR) technique, spatial modulation (SM) technique, and D2D communi-

L. Wang, *Physical Layer Security in Wireless Cooperative Networks*, Wireless Networks, DOI 10.1007/978-3-319-61863-0_6

cations were investigated. We not only presented their basic ideas and formulations of signal transmission, but also their characteristics and applications. The issues of physical layer security have been discussed with current state of research, to show a comprehensive insights about the relationship between the security and corresponding techniques.

We have presented characterization of secrecy performance based on TR technique for physical layer security in Chap. 3. Due to the signal focusing property of TR, it naturally can be exploited to reduce signal leakage to unintended mobile users. In particular, a distributed TR (DTR) transmission scheme without knowledge of full CSI at the source was studied, for boosting the source-destination link quality by utilizing both spatial diversity of multiple antennas and the multi-path channel in the temporal domain, while limiting signal leakage to unintended user/passive eavesdropper. With the frequency selective channel information between each distributed antenna and destination, the DTR scheme can focus signal energy on the critical signal detection time samples at the destination receiver. On the other hand, the performance of DTR-based transmission, direct transmission, LoS distributed beamforming, and MGP distributed beamforming were analyzed with respect to signal leakage. We compared the secrecy performance of these schemes by measuring the SNR gap between the destination and unintended receivers. Given multi-path channels, DTR transmission is a much more effective signaling strategy against signal leakage to unintended receivers than traditional beamforming strategies, particularly when the number of multi-path components is large.

Next, in Chap. 4 we have studied physical layer security in SM-MIMO transmissions. First, we analyzed the secrecy rate with basic SM modulation. By exploiting a simple and practical method in which the artificial noise is designed for secrecy enhancement without CSI of eavesdropper, our proposed secrecy enhancement transmission scheme does not influence the security performance at the legitimate receiver while interfering the quality of received signal at the eavesdropper. We demonstrated successful improvement of secrecy rate and the improved BER simulation results for multi-antenna users. Second, in the same system we considered an exhaustive analysis of secrecy rate with SSK and GSSK modulation. We investigated the tradeoff between secrecy capacity and additional transmission power with more than one activated RF antenna chains in these three SM-MIMO modulations. We found that SM, SSK, and GSSK have their own advantages and disadvantages in terms of secrecy performance enhancement. So a system can flexibly choose the suitable modulation scheme under different requirements and configurations. Third, we generalized the precoding-aided spatial modulation (PSM) to a multiuser downlink scenario. Signal precoding matrices were designed to eliminate the MU interference as well as beamform a portion of bit stream on the receivers' antennas, which is distinctive from that in a point-to-point communication system. To gain further security improvement, fast-varying scrambling on SPMs was exploited to degrade the performance of eavesdropper's blind estimation and detection. Compared with no scrambling and slow-varying scrambling, the proposed scheme demonstrated a clear security boost, even the eavesdropper has more antennas than the legitimate receiver.

Finally, the issues of physical layer security in D2D communications have been investigated in Chap. 5. First, we proposed joint power allocation and jammer selection schemes to improve secrecy and privacy of D2D communications, targeting the worst eavesdropping case by the smartest eavesdropper. Two scenarios including the full knowledge of CSI and the partial knowledge of CSI are considered, and the reliable jammer is selected to protect against the interception with the help of social trust among users. Apart from improving the spectrum efficiency, D2D communications also can facilitate the content sharing among content helpers and content requesters. In view of that, we investigated a practical scenario in which the mobile users obtain desired content from their D2D communication partners. For simplicity, we considered the problem of reliability and secrecy enhancement for wireless content sharing between multiple content helpers and a content requester. To further enhance secrecy and privacy, the social interaction was also exploited to guarantee the reliability during the content transmission between the content requester and content helper. Specifically, the impact of mobility for content helper selection for transmission reliability is studied. Considering the communication links and social characteristics simultaneously, the content helper is selected by firstly narrowing the potential link set to provide desired transmission success rate in between. The simulation results demonstrated that the social interactions among D2D users (i.e., content helper and requesters) play a very important role in terms of enhancing the secrecy performance.