

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.

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

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

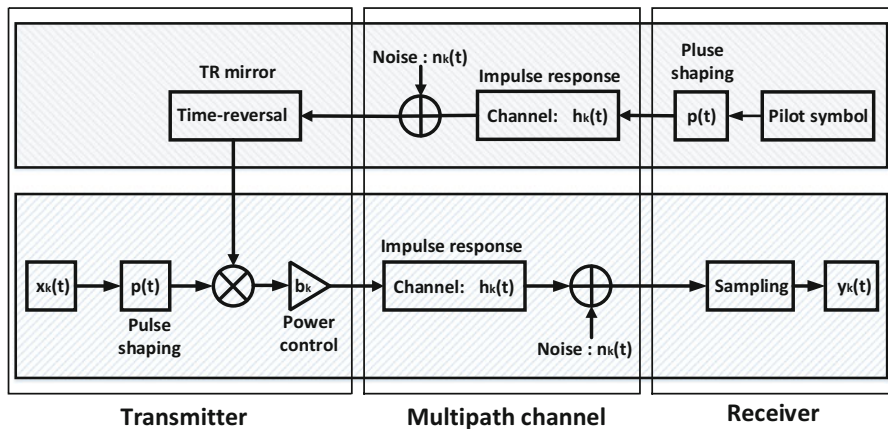


Fig. 2.1 Conventional time reversal communications (k -th antenna) [2]

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

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

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 $\text{Prob}(L_k = \ell) = L^{-1}$, $\ell = 0, 1, \dots, L - 1$.

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, $\tilde{h}_k(t)$, which is the convolution of $h_k(t)$ and $p(t)$, represents as follows:

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

where \otimes denoted the convolution operation, $\tilde{h}_k(t)$ 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 $\tilde{h}_k(t)$. We denote $\tilde{h}_k^*(T_p - t)$ 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]

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

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

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

Therefore the received signal in baseband can be expressed as

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

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

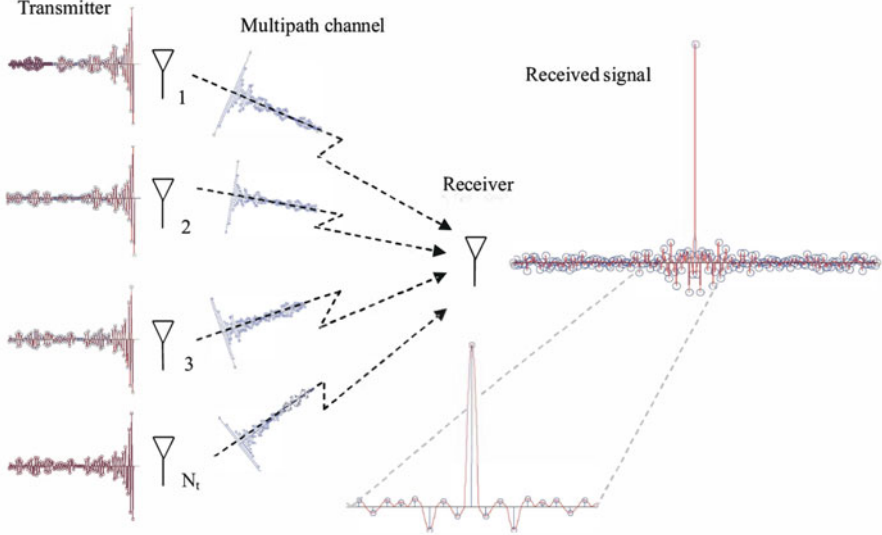


Fig. 2.2 Property of the spatial focusing in TR [5]

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.

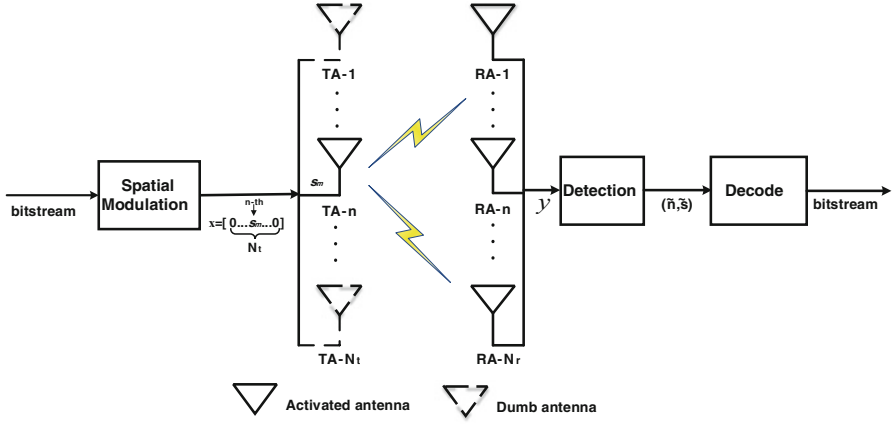


Fig. 2.3 System model of SM

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

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \quad (2.7)$$

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

$$\mathbf{x} = [0 \dots 0 \underbrace{s_m}_{n\text{-th}} 0 \dots 0]^T = \mathbf{e}_n s_m \quad (2.8)$$

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 \mathcal{S} , and $\mathbf{e}_n \in \mathbb{R}^{N_t \times 1}$ is the vector belonging to the spatial-constellation diagram \mathcal{A} as follows:

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

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

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

- **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

$$\mathbf{y} = \mathbf{h}_n s_m + \mathbf{n}, \quad (2.10)$$

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

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,

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

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.

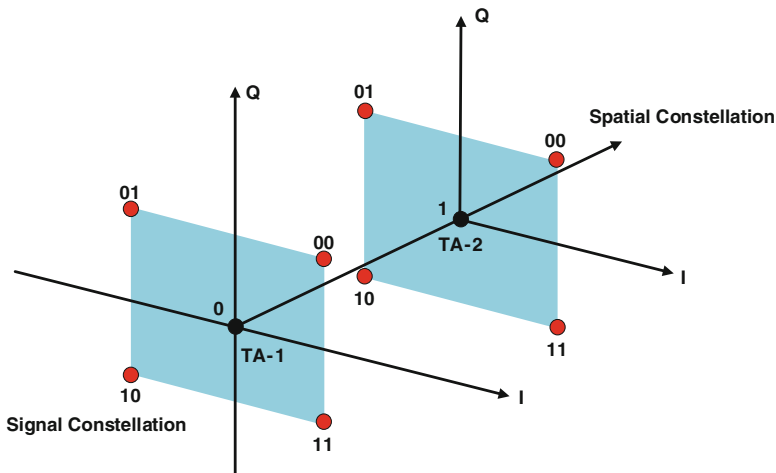


Fig. 2.4 Illustrations of SM mapper (4-QAM)

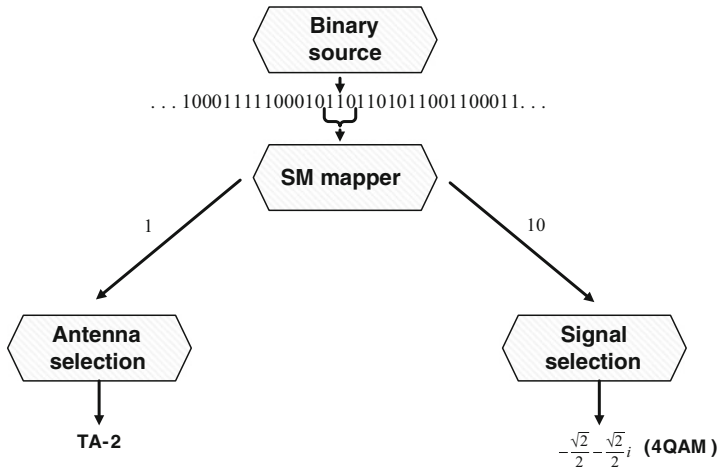


Fig. 2.5 Basic working principle of SM mapper

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-antennas; (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

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

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

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 $n_t(N_t \geq n_t)$ 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.,

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

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

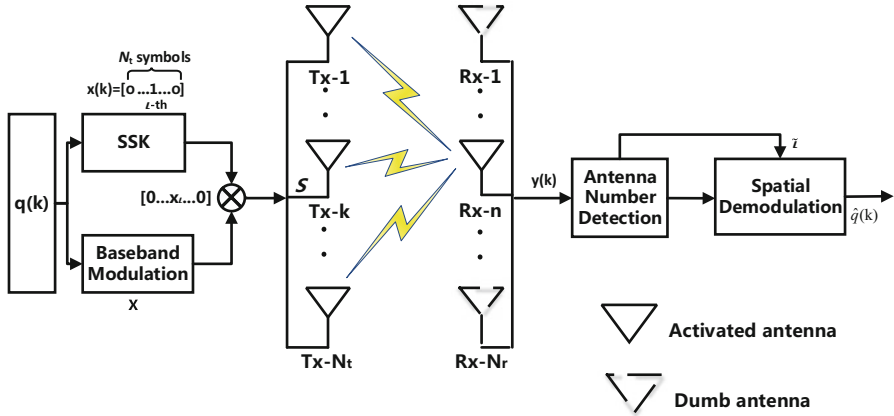


Fig. 2.6 System model of pre-coding aided spatial modulation[26]

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. $\mathbf{q}(k) \in \mathbb{C}^{N_t \times 1}$ is denoted as PSM symbol determined by two components of information, one is $\mathbf{x}(k)$ conveyed by the indices of receive antennas, where $\mathbf{x}(k) = [0 \dots 0 \underbrace{1}_{k\text{-th}} 0 \dots 0]^T$ 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, $\mathbf{q}(k) = \mathbf{x}(k) \cdot x_l = [0 \dots 0 \ x_l \ 0 \dots 0]^T$.

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

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

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 $\mathbf{P} = \boldsymbol{\beta} \mathbf{H}^* (\mathbf{H}^H \mathbf{H}^*)^{-1}$, where $\boldsymbol{\beta} \in \mathbb{C}^{N_r \times N_t}$ 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

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

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 throughput 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 $N_t \geq N_r$. 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 from 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.

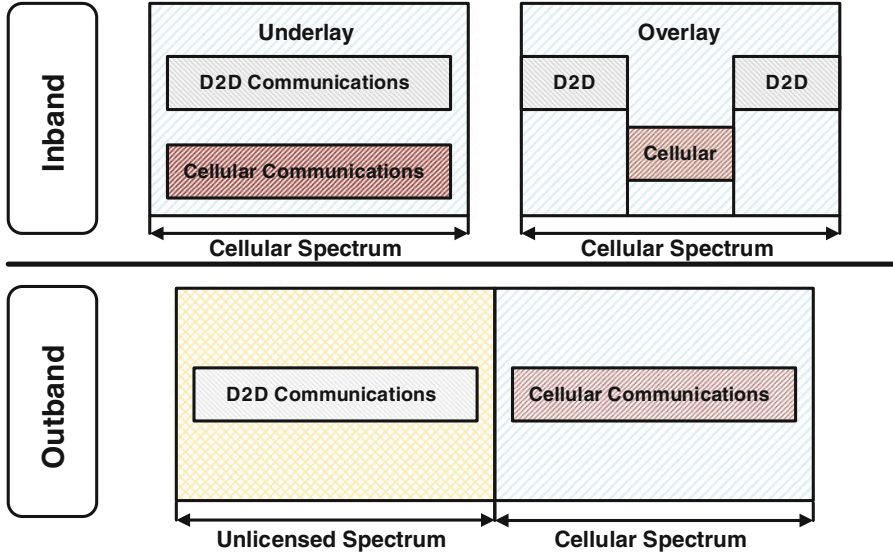


Fig. 2.7 Illustrations of D2D classification [40]

- **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*

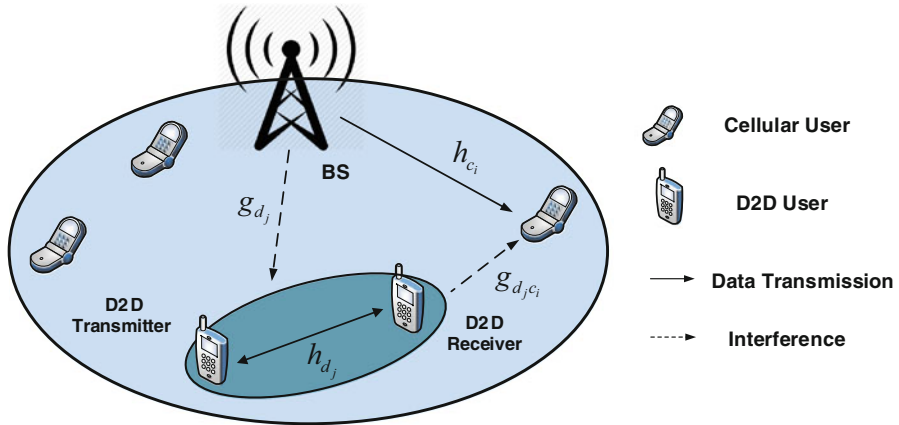


Fig. 2.8 Basic D2D communications in cellular networks

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

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

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

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

$$\gamma_{c_i} = \frac{P_{BS}h_{c_i}}{N_0}, \quad (2.16)$$

$$\gamma_{d_j} = \frac{P_{d_j}h_{d_j}}{N_0}. \quad (2.17)$$

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,

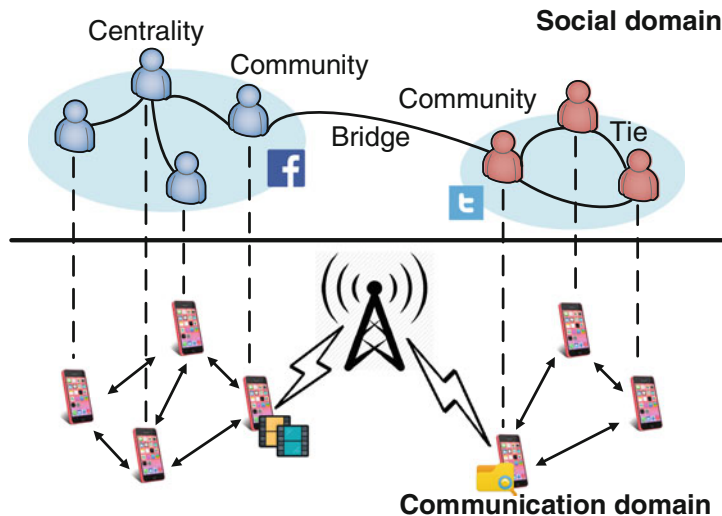


Fig. 2.9 Illustrations of social-aware D2D communications [55]

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

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

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., $\|L_i(t_c^-) - L_j(t_c^-)\| \geq R_{i,j}$ and $\|L_i(t_c) - L_j(t_c)\| = R_{i,j}$, 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.,

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

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]

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

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

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

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. $s_1(i, j) = -\log(p_1(i, j))$ and $s_2(i, j) = -\log(p_2(i, j))$ 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 ($c \in \mathcal{C}$, where \mathcal{C} is the set of community) are contacting with each other and is calculated by averaging the contact rates (is simply defined as $1/E[CI_{ij}]$) of all users [59],

$$f_c = \frac{1}{N_c} \sum_{i=1}^{N_c} \mu_i, \quad (2.22)$$

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

$$S_i = f_c \left(1 - \frac{\sum_{j \in N, j \neq i} \int_0^T (1 - F_{CI_{ij}}(x)) dx}{N - 1} \right) \quad (2.23)$$

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

- **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'Donoghue, "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. Sarrebourg, 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://www.zte.com.cn/endata/magazine/zte technologies/2015/no3/articles/201505/t20150506\\$433771.html](http://www.zte.com.cn/endata/magazine/zte technologies/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 underlying 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.

Physical Layer Security in Wireless Cooperative
Networks

Wang, L.

2018, XVII, 181 p. 10 illus., 3 illus. in color., Hardcover

ISBN: 978-3-319-61862-3