Physical Layer Security with Its Applications in 5G Networks: A Review

Li Sun[1,2,*], Qinghe Du[1,3]

[1] Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[2] The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
[3] National Simulation Education Center for Communications and Information Systems, Xi'an 710049, China
* The corresponding author, email: lisun@mail.xjtu.edu.cn

Abstract: 5G network is expected to support massive user connections and exponentially increasing wireless services, which makes network security unprecedentedly important. Unlike traditional security-guaranteeing techniques which rely heavily on cryptographic approaches at upper layers of the protocol stack, physical-layer security (PLS) solutions fully take advantages of the characteristics of wireless channels to degrade the received signal qualities at the malicious users, and realize keyless secure transmission via signal design and signal processing techniques. PLS avoids the difficulties in the distribution and management of secret keys, and provides flexible security levels through adaptive transmission protocol design. Moreover, PLS techniques match the features of 5G networks well. Therefore, the application of PLS to 5G networks is a promising solution to address the security threats. This article presents a comprehensive review of the state-of-the-art PLS techniques, and discusses their applications in 5G networks. We first summarize the principle and advantages of PLS techniques, and point out the reasons why PLS is suitable for 5G networks. Then, we review the existing PLS methods in literature, and highlight several PLS solutions that are expected to be applied in 5G networks. Finally, we conclude this article and figure out some further research directions.

Keywords: 5G; physical layer security; anti-eavesdropping signal design; statistical security guarantee; fountain coding

I. INTRODUCTION

With the continuous growth of the demands for ubiquitous information exchange, the increasing popularity of smart devices, the rapid development of mobile Internet, and the deep integration of information technology into industrial applications, 5G network is expected to support massive user connections and exponentially increasing wireless services, which makes the information security issue unprecedentedly important.

Current network transmission security technologies rely heavily on the cryptographic approaches at the upper layer of the protocol stack, which is not suitable for future 5G networks. The main reasons are threefold. First, 5G is a large-scale heterogeneous network (HetNet) with multiple levels and weakly-structured architectures, which makes it

Editor: Jianwei Zhao
Received: Aug. 6, 2017
Revised: Sep. 4, 2017

This article presents a comprehensive review of the state-of-the-art PLS techniques, and discusses their applications in 5G networks.

extremely difficult to distribute and manage the secret keys. Second, 5G network is expected to support differentiated scenarios and diverse wireless services. Different types of services have totally different security requirements. For example, online payment calls for a much higher security level than the ordinary web browsing service does. However, encryption-based methods can only provide "binary" security levels. That is, information is fully protected if the secret key can be securely exchanged and fully intercepted otherwise. Thus, service-oriented and user-centric security guarantee cannot be achieved. Third, 5G needs to support Internet-of-Things (IoT) applications featured by machine-type communications (MTC), where the massive MTC devices are short of power, storage, and computing capabilities, and complicated encryption/decryption algorithms or protocols cannot be applied.

Unlike the conventional upper-layer security methods, physical layer security (PLS) takes advantages of the intrinsic characteristics of wireless channels, such as noise, interference, and fading, to degrade the received signal qualities at the malicious users, and realize keyless secure transmission via signal design and signal processing approaches. Compared with the cryptographic methods, PLS has the following technical advantages. First, PLS does not depend on encryption/decryption operations, thus avoiding the difficulty of distribution and management of secret keys in HetNets. Second, by using PLS approaches, adaptive signal design and resource allocation can be implemented based on the varying channel conditions, thereby providing flexible security levels. Third, PLS often requires relatively simple signal processing operations, which translates into minor additional overheads. The comparisons between PLS and cryptographic techniques are illustrated in figure 1.

In addition to the aforementioned technical advantages, PLS techniques match the features of 5G networks well. The employment of massive MIMO in 5G greatly enriches the spatial resolution of wireless channels, and offers additional spatial resources to combat eavesdropping. The adoption of high-frequency communications in 5G brings in abundant spectra and provides favorable conditions for wideband secure transmissions. Moreover, the application of multi-cell cooperation techniques makes it possible to implement the

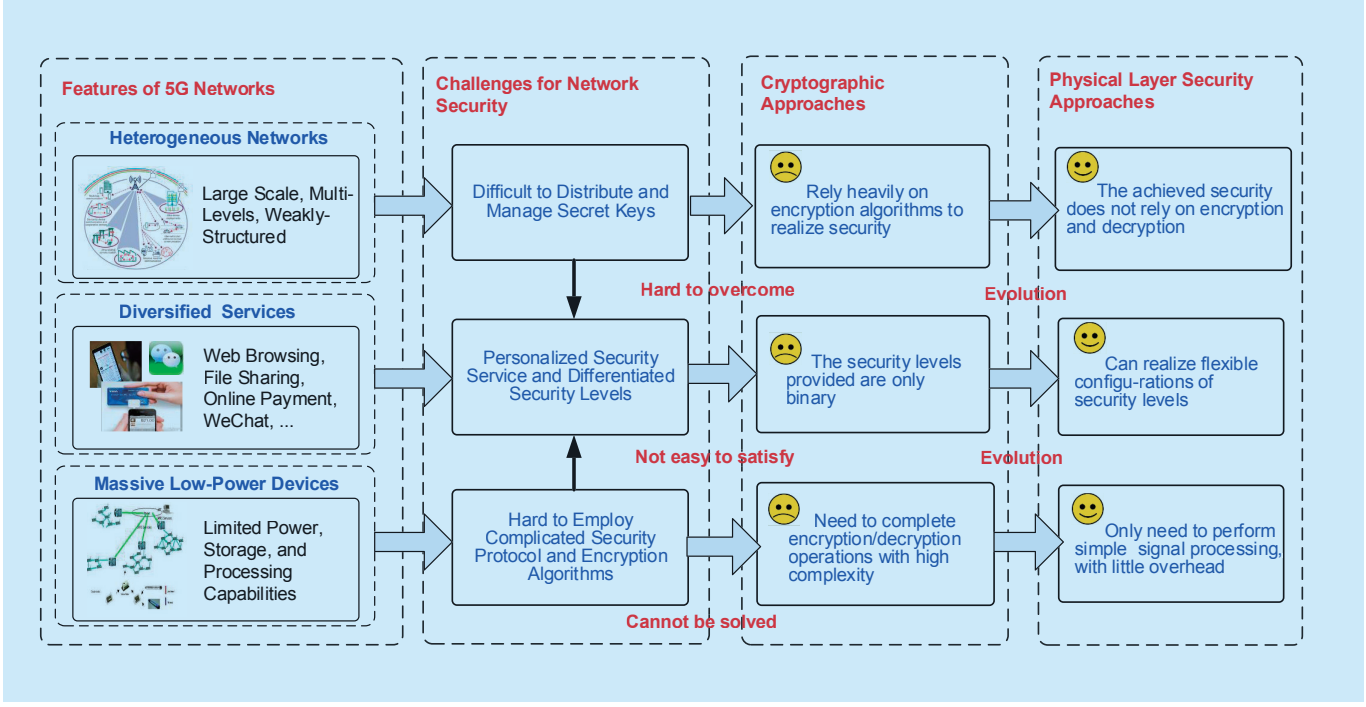

Fig. 1 *The comparison between PLS and cryptographic techniques*

cooperative secrecy ideas. Therefore, PLS is a promising security provisioning solution for 5G networks.

This article presents a comprehensive review of PLS and its applications in 5G networks. Sect. II briefly describes the principle of PLS by referring the main results in information-theoretical security. Sect. III summarizes the recent advances in PLS research. In Sect. IV, we point out the major drawbacks in current PLS studies, and identify the challenges for PLS protocol design toward 5G networks. Sect. V highlights some promising PLS solutions that might be suitable for 5G networks. Finally, Sect. VI concludes this article and figures out several further research directions.

II. Principles of Physical Layer Security

The key idea of PLS is to exploit the intrinsic characteristics of wireless channels, such as noise, fading, and interference, to secure the communications. The research in this area can be traced back to Shannon's pioneering work on secret communications [1], where the concept of perfect secrecy was established. In [1], Shannon considered a system model where the source-destination pair communicates over a noiseless channel, and an eavesdropper overhears the signals sent over the channel. This system is said to be in perfect secrecy if the following condition is satisfied:

$$H\left(M \mid X\right) = H(M) \tag{1}$$

where $H(M)$ and $H(M|X)$ are the entropy of the message M and the conditional entropy of M conditioned on eavesdropper's observation X, respectively. Intuitively, (1) implies that eavesdropper's uncertainty about the message does not decrease after intercepting the transmitted codeword, or equivalently, the information leakage is zero. Perfect secrecy guarantees that eavesdropper's optimal attack is to guess the message M at random and there is no algorithm that can extract any information about M from X. To achieve perfect secrecy, the codeword X should be independent of the messages M. In practice, this can be satisfied by using a one-time pad approach, for which each secret-key bit is XORed with each message bit to produce the transmitted codeword X.

Although the one-time pad scheme can achieve perfect secrecy, the requirement is disappointing that one secret-key bit is needed for one message bit. This result stems from the absence of noise at the physical layer in the model. Unlike Shannon's work, Wyner proposed a degraded wiretap channel model (DWTC) in [2]. The DWTC models a system in which a sender (Alice) tries to communicate with a legitimate receiver (Bob) over a noisy channel, while an eavesdropper (Eve) observes a degraded version of the signal obtained by the legitimate receiver. Alice encodes its confidential message M into an n-length codeword X^n with rate R, while Bob and Eve try to extract the source information by decoding their received codewords Y^n and Z^n, respectively. Rate R, defined as the secrecy rate, is said to be achievable if

$$\lim_{n\to\infty} \Pr\left(\hat{M} \neq M\right) = 0 \tag{2}$$

and

$$\lim_{n\to\infty} I\left(M; Z^n\right) = 0 \tag{3}$$

hold. In (2) and (3), $\hat{M}$ denotes the estimate of M at Bob, and $I\left(M; Z^n\right)$ represents the mutual information between M and Z^n. These two conditions, termed as reliability condition and security condition respectively, guarantee that the decoding error probability at the legitimate receiver can be arbitrarily small while no source information can be obtained by the eavesdropper, as long as the codeword length tends to infinity. The maximum of the achievable secrecy rate is defined as secrecy capacity, which characterizes the rate limit for secure transmission in noisy channels. For DWTC, the secrecy capacity can be expressed as

$$\begin{aligned} C_{\mathrm{s}}^{\mathrm{DWTC}} &= \max_{p_X}\left(I(X;Y) - I(X;Z)\right) \\ &\geq \max_{p_X} I(X;Y) - \max_{p_X} I(X;Z) \end{aligned} \tag{4}$$

where p_X is the probabilistic distribution of the encoder input at Alice. (4) indicates that, the

secrecy capacity is at least as large as the difference between the legitimate channel capacity and the eavesdropper's channel capacity. The inequality in (4) can be strict for Gaussian wiretap channel, yielding the secrecy capacity formula for Gaussian wiretap channel to be

$$C_s^{\mathrm{GWTC}} = \left[\log\left(1+\mathrm{SNR}_B\right) - \log\left(1+\mathrm{SNR}_E\right)\right]^+ \tag{5}$$

where $[x]^+ = \max(x, 0)$, and SNR_B and SNR_E are the received SNRs at Bob and Eve, respectively.

The secrecy capacity expression for Gaussian wiretap channel implies that, secure communication is possible if and only if the legitimate receiver has a better channel quality than the eavesdropper does. Physical layer security techniques harness the intrinsic randomness at the physical layer to create the "physical advantage", i.e., the required better quality, of the legitimate link compared to the eavesdropping link. The intrinsic randomness, mainly includes noise, multipath fading, and interference, is a resource that abounds in the wireless medium. In the next section, we will review the major physical-layer security approaches proposed in literature to show how to exploit these types of "randomness" for enhanced security.

III. Review of Major Physical-Layer Security Approaches

3.1 Artificial noise injection

Based on secrecy capacity theory, a positive secrecy rate can be achieved if the legitimate user has a certain form of physical advantage in terms of the channel quality compared to the malicious users. Artificial noise (AN) injection is an effective means to realize this purpose. The principle of this approach is to simultaneously send the information-bearing signal and the AN using a multi-antenna transmitter. The AN and the information-bearing signal are injected into the null-space and the column space of the legitimate user's channel matrix, respectively. In this manner, the artificial noise only deteriorates the eavesdropper but has little detrimental impact on the legitimate receiver.

Ref. [3] is the seminal work in AN injection scheme design. Afterwards, this method has been applied to various scenarios, taking into account the practical limitations of real-world systems. [4] discussed the optimal power allocation between the artificial noise and the useful signal, where both colluding and non-colluding cases were considered. [5] compared performances of the AN injection method and the artificial fast fading method under different antenna configurations at the eavesdropper, and proposed an improved hybrid scheme. [6] combined the AN injection approach with opportunistic relay selection, and analyzed the security-reliability tradeoff of the system. Common to the works [4]-[6] is that they all assumed perfect channel state information (CSI) is available at the transmitter, which is hard to satisfy in practice. To address this issue, [7] investigated the AN-aided beamforming design with limited feedback, where the coding rate and the power ratio of AN can be adjusted according to the channel feedback. [8] studied the AN-aided secure transmission in multiuser systems, and pointed out that from the secrecy perspective, it is more advantageous to increase the AN power than to increase the information-bearing signal power when the CSI error is large.

3.2 Anti-eavesdropping signal design

Unlike the AN injection approach, the anti-eavesdropping signal design technique attempts to align multiple users' signals at the eavesdropper such that the decoding difficulty is significantly increased and information security can thus be guaranteed [9]. In [10], the authors borrowed the idea of interference alignment (IA) to develop a signal alignment method for Gaussian MAC wiretap channel. By using the proposed approach, the transmitted signals from multiple users align in a low-dimensional subspace of the signal space.

Since all the signals align in the same direction, it is difficult for the eavesdropper to distinguish each user's signal. [11] proposed an ergodic secrecy alignment strategy (ESA) for fading MAC wiretap channel. The key idea of ESA is to repeat data transmission within two slots such that an orthogonal MAC channel is created for legitimate users, while a scalar MAC channel is observed by the eavesdropper.

While the aforementioned works [10] and [11] focused on anti-eavesdropping signal design for MAC channels, there are also some papers dedicating to the secrecy-enhancing signal design in cooperative relay channels. [12] designed the precoder matrix for two-way relay channel, by using which the two sources' signals align in the same subspace at the untrusted relay. In [13], we devised a constellation rotation aided secure transmission scheme for two-way untrusted relay systems. By rotating the signal constellations with an appropriate angle, every complex constellation point can be represented by it real component. Then, each terminal user transmits the information-bearing signal and the artificial noise in two orthogonal dimensions of the signal space. As a result, the artificial noise and the useful signal from different users align to the same direction at the untrusted relay, which significantly degrades the SINR at the relay and prevents information leakage. Meanwhile, the received signal and AN lie in orthogonal dimensions at the terminal users, and hence the signal detection at the legitimate users will not be affected.

3.3 Secure beamforming/precoding

Secure bemforming/precoding belongs to spatial-domain anti-eavesdropping techniques. This approach optimizes the spatial distribution properties of the transmit signals in order to enlarge the difference between the legitimate user's channel quality and the eavesdropper's channel quality. [14] presented the beamforming vector design that can maximize the secrecy rate of MISOME channel. In [15], a linear precoding strategy was proposed for MIMOME channel, and a numerical method was developed as well to solve for the optimal precoder. [16] proposed a channel-inversion precoding method that can maximize the sum secrecy rate under imperfect CSI. In [17], the joint information beamforming and jamming beamforming was devised to guarantee both transmit security and receive security for a full-duplex base station.

All of the works [14]-[17] only exploit the spatial beamforming or precoding to combat eavesdropping. By combining secure beamforming and AN injection, the system secrecy performance can be further enhanced. [18] proposed a transmit beamforming solution that is robust to the channel estimation errors. The proposed method first allocates power to the useful signal component to satisfy the target SINR of the desired user, and then uses the remaining power to send the artificial noise to worsen the detection performance of the eavesdropper. [19] discussed the impact of channel quantization on the secure beamforming design. The authors pointed out that the quantization for the beamforming vector and that for the AN vector should be performed separately to lower the interference to the legitimate receiver. To be more specific, the beamforming vector should be chosen such that the beamforming gain can be maximized; while the objective of the AN vector design is to minimize the information leakage. [20] studied the secure transmission capability for multiuser systems with curious users, where limited feedback is assumed. The major conclusions of [20] are twofold. First, in high SNR regime, if the CSI is quantized to a fixed number of bits, the system secrecy rate will not increase with the transmit power, and may even decrease when the transmit power exceeds a certain threshold. Second, in order to guarantee that the loss in secrecy rate is below a certain given value compared to the perfect CSI case, the number of CSI quantization bits should be an increasing function of the transmit power and the number of transmit antennas. While the aforementioned papers [14]-[20] are merely concerned about the se-

curity aspect of the system, [21] considered simultaneous transfer of secret message and energy using zero-forcing based precoding techniques, and demonstrated the trade-off between the achievable secrecy rate and the transferred energy.

3.4 Cooperation based secure transmission techniques

Wireless network is essentially a multi-user system, for which the network security performance can be greatly enhanced by enlisting the cooperation among nodes. Cooperation based secure transmission techniques can be generally divided into three categories, namely cooperative jamming, relay selection, and cooperative secrecy enhancement.

Cooperative jamming (CJ) utilizes multiple relay nodes to generate artificial noises in a distributed manner to realize information security, which is essentially a distributed beamforming technique. [22] designed CJ schemes for both amplify-and-forward (AF) and decode-and-forward (DF) systems. In the proposed schemes, all relay nodes independently send the weighted artificial noises to degrade the received signal quality at the eavesdropper, while the source transmits its message simultaneously. [23] investigated a nulling based CJ strategy, and devised the optimal structure of the artificial noise signal under global CSI.

Relay selection (RS) techniques enhance transmission secrecy via the selection of relay nodes and (or) friendly jammers. [24] proposed to select two relay nodes to perform message forwarding and artificial-noise injection, respectively, and adaptively switch the cooperation modes to minimize the secrecy outage probability. [25] developed a joint relay-jammer selection policy to maximize the achievable secrecy rate, and presented a low-complexity power allocation strategy. Common to [24] and [25] is that both of them assume the relay nodes are trustworthy, and the eavesdroppers are external nodes in addition to the legitimate entities. However, in some scenarios, the relay nodes, while operating with the designated protocol and offering help to the source-destination pair, are untrusted, from which the source information has to be kept secret. The PLS protocol design for untrusted relaying systems is a hot research topic recently. Yener *et al.* indicated that a positive secrecy rate can be achieved if cooperative jamming technique is applied [26]. [27] proposed a cooperation-mode switching scheme and analyzed the achievable secrecy outage probability. [28] combined the relay assignment and link adaptation, resulting in both secure and spectrally-efficient transmissions. [29] developed an opportunistic relay selection protocol for untrusted relaying systems, and analyzed the scaling law of the secrecy rate. The main drawback of the scheme in [29] is that only the broadcast phase of the two-phase cooperative transmission can be secured. To address this issue, [30] further developed a cooperative mechanism based on alternate jamming and relay selection.

In both CJ and RS, the relay node acts only as a helper, which offers secrecy-embedded relaying services to legitimate transceivers. In contrast, in the cooperative secrecy enhancement (CSE) schemes, several users cooperate with each other to harvest a mutual benefit. In [31], the authors proved that two users that do not trust with each other can enlarge the achievable secrecy rate region by negotiating the signal power and AN power. [32] was concerned about a device-to-device (D2D) communications scenario, for which the authors proposed to utilize the signal generated by the D2D device as interference to degrade the reception performance of the eavesdropper overhearing the cellular user's transmission. As a reward, D2D users can obtain the opportunity to reuse the cellular spectrum, thereby improving its transmission performance. Recently, [33] devised a cooperative privacy preserving scheme for the downlink transmission in multiuser relay systems. The key idea of this scheme is to exploit the cooperation among untrusted users to improve their secrecy rates simultaneously.

3.5 Power control and resource allocation

Security-oriented power control and resource allocation techniques adjust the transmitter parameters based on the instantaneous CSI such that the received SNR at the legitimate user can be improved or kept as a constant, while that at the eavesdropper varies randomly over time. In this manner, the difference in channel qualities between the legitimate link and eavesdropping link can be enlarged. [34] proved that power control based on water filling can achieve the secrecy capacity in wiretap channels. [35] applied the on-off policy to realize power control, which maximizes the system throughput subject the secrecy outage constraint. In [36], the secure transmission issue for OFDMA downlink was investigated, for which it was revealed that, to guarantee the user's data confidentiality, the allocated power does not only depend the channel gain of the served user, but also relies on the maximum of the channel gains among all other users. In practical systems, perfect CSI of the legitimate channel is not available at the transmitter side due to feedback delay or channel estimation error. To address this issue, [37] exploited useful knowledge contained in outdated CSI to decide whether to transmit or not. [38] further developed a versatile strategy to increase the secrecy throughput of on-off secure transmission in the case that only stale CSI is available.

Summary: It is conventionally recognized that noise, fading, and interference are detrimental factors for reliable communications that should be suppressed. However, from the security point of view, these factors are actually the beneficial resources that should be exploited, as state above. For example, the anti-eavesdropping signal design can be viewed as an interference exploitation method for enhanced secrecy, where the inter-user interference is utilized to confuse the eavesdropper. The cooperation based techniques, on the other hand, exploit both noise and fading to create the physical advantage of the legitimate users. In table 1, we summarize the aforementioned PLS approaches, and compare them in terms of the anti-eavesdropping mechanism, required CSI at transmitter, the incurred additional overhead, and implementation complexity.

IV. Drawbacks of the Existing PLS Techniques and Challenges for 5G Transmission Security

From the above discussions we can find that, the research on PLS has generated a large body of literature, with the topics ranging from information-theoretical studies to practical scheme design. However, it is still challenging to develop innovative PLS transmission theory and methods that well match the unique features of 5G networks. The majority of the existing PLS solutions have the following drawbacks that prohibit their applications to 5G networks.

First, most of the existing PLS schemes realize security via the exploitation of noise, fading, and interference. In other words, they

Table I *Summary of the major physical layer security approaches in literature*

PLS Approach	Anti-Eavesdropping Mechanism	Required CSI at Transmitter	Additional Overhead	Implementation Complexity
AN injection	Exploitation of noise	Instantaneous	CSI feedback, additional power	Moderate
Anti-eavesdropping signal design	Exploitation of interference	Instantaneous	CSI exchange	High
Secure beamforming/precoding	Exploitation of fading and noise	Instantaneous	Multi-antenna structure, CSI feedback	Moderate
Cooperative jamming	Exploitation of noise	Not necessary	Additional power, dedicated helper	Moderate
Relay selection	Exploitation of fading	Not necessary	Additional power, dedicated helper	Moderate
Cooperative secrecy enhancement	Exploitation of interference and noise	Instantaneous/Not necessary	Data and (or) CSI exchange	High
Power control and resource allocation	Exploitation of fading	Instantaneous	CSI feedback	Moderate

only take advantages of the characteristics of wireless channels (i.e., link-level properties) but under-appreciate the significance of characteristics of wireless networks (i.e., network-level properties) in security enhancement. 5G is a multi-level multi-user system, for which the network behavior does not only depend on the properties of the individual links, but also highly relates to the interaction among users and sub-networks. To be more specific, feedback, cooperation, competition, and cognition exist widely in the future 5G networks [39]. Yet, it is still unclear how to translate these mechanisms into an anti-eavesdropping resource, and the research on the impact of these network-level features upon PLS protocol design has just started [40].

Second, the PLS techniques developed so far mainly focus on the optimization of the secrecy rate or secrecy outage performance of the system. However, 5G is expected to support various application scenarios and diverse wireless services. Different types of services have totally different quality-of-service (QoS) requirements, which implies that the PLS protocols should jointly consider various aspects of user demands, including reliability, delay, throughput, and secrecy as well. It is impossible to provide a comprehensive QoS guarantee for users by simply optimizing the secrecy rate or secrecy outage performance.

Third, the existing PLS solutions often unilaterally pursue the system performance optimization without taking into account the limitations in the available resources of practical devices. In particular, additional power is consumed to implement the AN injection method; multi-antenna configuration is required at the transmitter for secure beamforming/precoding schemes; dedicated nodes have to be deployed in the networks to send jamming signals for CJ approach. 5G network will support IoT applications featured by MTC communications, for which the devices have very simple functionalities and very limited power, storage, and processing capabilities. Therefore, most of the existing PLS solutions cannot be directly applied in IoT communications.

In summary, the unique features of 5G networks, 5G services, and 5G devices pose significant challenges to PLS protocol design. In the next section, we highlight several newly developed PLS solutions that address the 5G transmission security issue.

V. Promising Physical-Layer Security Solutions Toward 5G Networks

ITU has identified three typical application scenarios for 5G, namely Enhanced Mobile Broadband, Ultra-Reliable and Low-Latency Communications, and Massive Machine Type Communications. In the following, we would like to introduce three PLS solutions that are dedicated to these scenarios, respectively.

5.1 Constellation-rotation based signal design for enhanced secrecy in D2D communications

As a promising paradigm to support the proximity-aware services such as media sharing, online gaming, and social networking, D2D communications has been recognized as a candidate solution for enhanced mobile broadband applications. There are two major transmission modes for D2D communications: 1) Underlay mode where the transmit power of D2D terminals are constrained to cause minimal interference to cellular links; 2) Overlay mode where D2D terminals act as relays to assist the cellular communications in exchange for transmission opportunities. The overlay mode, also known as the cooperative D2D transmission mode, seems to be more appealing because it's a win-win policy that motivates the operators to be willing to accept the deployment of D2D. A typical cooperative D2D system model is shown in figure 2. For this system, each cooperative period is composed of two phases. During the 1st phase, D_2, BS, and CU transmit their signals to D_1, respectively. During the 2nd phase, D_1 transmits the received signals together with its own information-bearing signal to all the other terminals.

There are two technical challenges for the

cooperative D2D communications. First, every terminal has to detect its desired signal while being interfered with by the signals intended for other nodes, which incurs an evitable error floor and deteriorates the detection performance. Second, every node can access the data transmitted from any other node, which yields information leakage among users and violates users' secrecy requirements.

To killing these two birds with one stone, we developed a constellation-rotation aided scheme to realize both interference avoidance and secrecy protection [41]. Our key idea is to rotate the signal constellations. As is exhibited in figure 3, the constellations employed at all terminals are first rotated by an appropriate angle such that a one-to-one mapping is established between the rotated constellation point and its real or imaginary part. Then, every transmitter projects the rotated constellation onto the real or imaginary axis, and transmits the resulting one-dimensional signal. During the 1st phase, BS and CU deliver their information using the real component, while D_2 sends its information with the imaginary component. Similarly, during the 2nd phase, D_1 uses the real and imaginary part of the complex signal as two orthogonal channels to broadcast its received signal and its own information-bearing signal, respectively. With the proposed design, the signal detection for intended messages at all terminals are free of interference, thus perfectly eliminating the error floor in symbol error rate. Meanwhile, the non-intended messages are aligned in the same direction at each node, thereby increasing the difficulty of decoding these messages and preventing information leakage. Moreover, by optimizing the value of the constellation rotation angle, an error floor can be created for the detection of the non-intended messages, and the transmission secrecy is further improved. Readers that are interested in this method can find more details in [41].

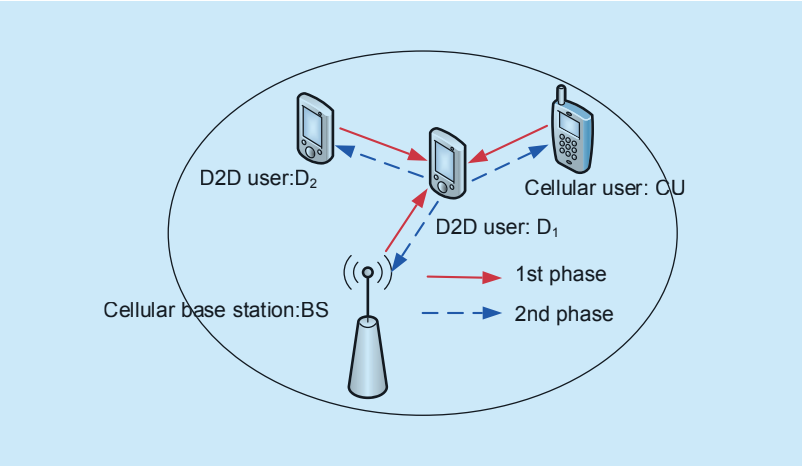

Fig. 2 *Cooperative D2D system model*

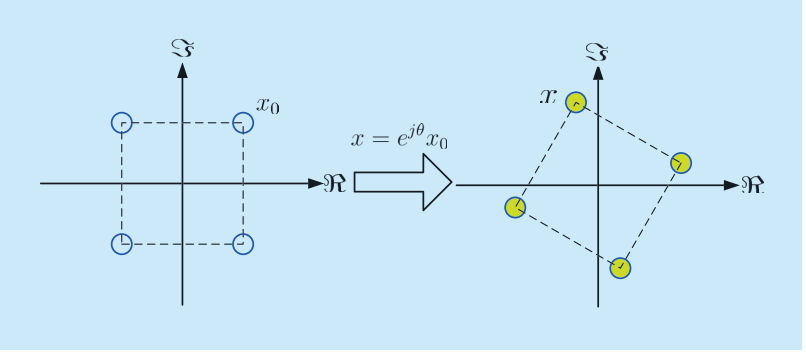

Fig. 3 *The illustration of constellation rotation*

5.2 Fine-grained security level characterization and statistical security guarantee for delay-sensitive services

In ultra-reliable and low-latency communication scenarios such as vehicular networking and industrial automation systems, services are typically delay sensitive, which makes the traditional PLS methodology (targeted at secrecy capacity maximization or secrecy outage minimization) inefficient. First, the secrecy outage probability (SOP) dictates the probability with which the achievable secrecy rate is lower than the target transmission rate. To satisfy a predefined SOP requirement, the transmission rate of the legitimate user has to be kept at a very low level, resulting in an intolerable delay. Second, secrecy capacity (SC) gives the maximum rate below which the legitimate receiver can successfully decode, while the

eavesdropper cannot obtain any information from the received signal. From the practical perspective, however, it is not always necessary to guarantee this "perfect" security. If Eve does not accumulate the sufficient amount of data within the delay bound, it cannot extract useful information, and essential security threat is not really caused. This motivates us to establish a statistical model towards fine-grained security level characterization, and design adaptive resource allocation schemes to realize statistical security guarantee for delay-sensitive services [42].

Our proposed model is depicted in figure 4, where Alice attempts to send data to Bob, and Eve tries to capture Alice's information from its observation. The accumulation and expiration of the eavesdropped data at Eve, which reflects the delay-sensitive characteristics of the transmissions, can be described by the queuing model depicted in the right-lower corner of figure 4. The arrival process of the queue is the amount of eavesdropped data, which is a time-varying process. The departure process (i.e., the dropping process) characterizes the expiration of the data. In practical systems, the timeout threshold is typically set as a constant for all effective data of a service. Therefore, we can assume the departure process of effective data to be constant-rate process. Eve's eavesdropped data which is still effective corresponds to the data staying in the queue. Based on the above model, security requirement can be described by the queue-length bound Q_{th}. If queue length is beyond the bound, the eavesdropper has accumulated sufficient amount of data to decipher users' information, and vice versa. Then, the security level of legitimate users can be characterized by the violation probability of the security requirement. Based on the service nature we require to satisfy $\Pr\{Q > Q_{th}\} \le \delta$, i.e., the probability with which Eve's queue length exceeds the secure threshold Q_{th} needs to be smaller than or equal to a small d. As long as this condition is satisfied, we claim that the user's security is assured. Because this model characterizes security levels based on the statistical features, we term it as statistical security model.

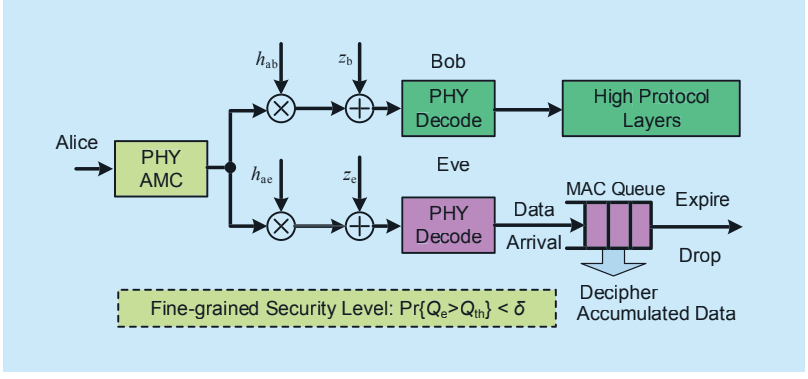

Fig. 4 *Model for fine-grained security level*

Having built the above model, we can design the framework for statistical security based resource allocation and QoS guarantee, which is shown in figure 5. In this figure, security QoS is characterized by the aforementioned statistical security metric, delay QoS is described by delay-bound violation probability, sustainable traffic load is characterized by

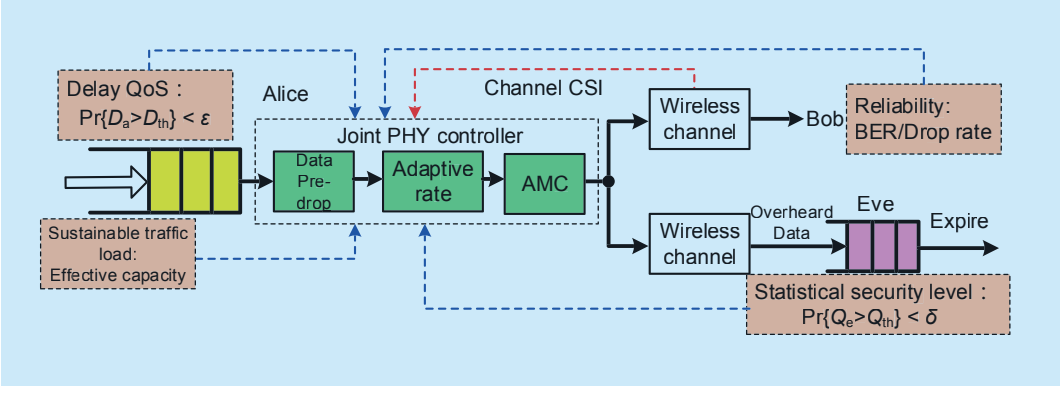

Fig. 5 *Framework for statistical security based resource allocation and QoS guarantee*

effective capacity, and reliability requirement is described by bit error rate (BER) and drop rate. This framework enables the decoupling of diverse QoS functions, whose optimization is conducted by a joint PHY controller including data pre-drop, adaptive rate control, adaptive modulation, and coding.

The above design provides a new architecture for secure transmission toward 5G. On one hand, it can effectively describe fine-grained QoS requirements of terminal users; on the other hand, it comprehensively integrates diversified requirements on security, delay, sustainable traffic load, and reliability, and provides a unified framework for flexible tradeoff.

5.3 Fountain Coding Aided Security Enhancement for IoT Applications

In IoT applications, the low-power machine-type devices often have very stringent constraints on communication resources and processing capabilities. Thus, PLS schemes toward IoT applications should provide the anti-eavesdropping capacity while keeping a very low implementation complexity. Motivated by this, we proposed a security enhancement framework based on fountain coding, which will be elaborated on in detail in what follows:

Fountain code (FC) was first proposed to realize reliable communications without retransmission [43]. In FC-aided data transmissions, the source file is first divided into K packets. Then, a potentially infinite number of FC packets are generated, each of which is the XOR of distinct source packets chosen randomly. The transmitter sprays these coded packets at the destination continuously. Once the receiver has correctly received N packets, where N is slightly larger than K, the source file can be recovered and the transmission terminates. This characteristic of FC can be exploited to realize wireless security. Specifically, by using FCs, the transmission link between legitimate transceivers can be secured if the legitimate receiver successfully accumulates the N coded packets before the eavesdropper does. In other words, the source information is not leaked as long as the destination obtains the required N packets first, even though some packets may be obtained by the eavesdropper.

With the above ideas in mind, we developed a series of FC-aided anti-eavesdropping strategies. In [44], an adaptive power allocation policy was developed based on truncated channel inversion. By using this approach, the received SNR at the legitimate receiver can be kept as a constant, while that at the eavesdropper varies randomly with time. As a result, the equivalent channel condition of the eavesdropping link is severely degraded, which makes it extremely difficult for the eavesdropper to accumulate the required number of FC packets. The scheme in [44] requires the availability of the instantaneous CSI at the transmitter, which is hard to satisfy in practical IoT applications. To combat this barrier, [45] investigated the construction of fountain code for enhanced secrecy. A set called decoding set is maintained at the transmitter, which contains all source packets that have already been decoded by the receiver. Upon the completion of each slot transmission, the legitimate receiver feedbacks a single bit to notify the transmitter about the decoding status of the current FC packet (success or failure). With this feedback information, the transmitter updates the decoding set, and constructs the new FC packet by XORing all source packets in the decoding set with an un-decoded source packet chosen randomly. As long as the current transmission does not fail, the legitimate receiver can recover a new source packet from the received FC packet. However, for the eavesdropper, no source packets can be recovered once any packet in the decoding set is not successfully decoded. Consequently, information leakage is avoided according to the principle of FC-based transmissions.

The FC-aided secure transmission technique can also be extended to cooperative relaying systems where the eavesdropper attempts to extract the source information during both the broadcast phase and the relaying phase. For

this scenario, a cooperative jamming method can be integrated into the FC-aided transmission framework. Interested readers can refer to [46] for more information.

VI. Conclusions and Future Works

This article presented a comprehensive review of the PLS technique with its applications in future 5G networks. We fist briefly introduced the security requirements of 5G, based on which we analyzed the advantages of PLS technique and its suitability to 5G systems. Then, we gave a detailed description of the principles of PLS and the state-of-the-art PLS techniques. Afterwards, the main drawbacks of the existing PLS solutions were discussed and the challenges faced by 5G transmission security were pointed out. Finally, we identified several promising PLS solutions towards the diverse application scenarios of 5G networks.

Although the fundamental research of physical layer security has generated fruitful outcomes, it is still challenging to design PLS schemes to satisfy the 5G security requirements. Some interesting topics that are worthy of further investigations are listed as follows:

1) Cross-layer security techniques. The existing PLS strategies realize transmission secrecy by exploiting the characteristics of wireless channels at the physical layer; on the other hand, the cryptographic approaches use encryption/decryption operations at upper layers to secure communications. By combining these two and introducing the cross-layer optimization techniques, the system secrecy performance can be further enhanced.

2) Content-aware physical-layer security scheme design. The PLS approaches developed so far only focus on the security of the "signals", while ignoring the diverse characteristics of data content carried by the signals. Thus, it is difficult to realize the optimized configuration of the anti-eavesdropping resources. In 5G networks, multimedia services will be the dominant service type. Therefore, it is interesting to develop content-aware PLS solutions to realize unequal secrecy protection.

3) Physical layer security approaches for combating active attacks. Current studies on PLS are primarily concerned about how to combat eavesdropping attacks of the malicious users. Yet, in future 5G networks, there also exist many forms of active attacks in addition to eavesdropping, such as jamming attack or pilot spoofing attack. It would be a non-trivial work to develop PLS solutions to combat active attacks. Some preliminary results on this subject can be found in [47], [48], and references therein.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China under Grants No. 61671369 and 61431011, the National Science and Technology Major Project of China under Grant No. 2016ZX03001012-004, the Open Research Fund of the State Key Laboratory of Integrated Services Networks, Xidian University, under Grant No. ISN18-02, and the Fundamental Research Funds for the Central Universities of China.

References

[1] SHANNON C E. Communication theory of secrecy systems [J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[2] WYNER A D. Wire-tap channel [J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[3] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise [J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.

[4] ZHOU Xiangyun, MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and power allocation [J]. IEEE Transactions on Vehicular Technology, 2010, 59(8): 3831-3842.

[5] WANG Huiming, ZHENG Tongxing, XIA Xianggen. Secure MISO wiretap channels with multiantenna passive eavesdropper: artificial noise vs. artificial fast fading [J]. IEEE Transactions on Wireless Communications, 2015, 14(1): 94-106.

[6] DING Xiaojin, SONG Tiecheng, ZOU Yulong, *et al.* Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection [J]. IEEE Transactions on Vehicular Technology, 2017, 66(5): 3930-3941.

[7] ZHANG Xi, MCKAY M R, ZHOU Xiangyun, *et al.* Artificial-noise-aided secure multi-antenna transmission with limited feedback [J]. IEEE

Transactions on Wireless Communications, 2015, 14(5): 2742-2754.
[8] LI Na, TAO Xiaofeng, WU Huici, *et al*. Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: ergodic secrecy sum rate and optimal power allocation [J]. IEEE Transactions on Vehicular Technology, 2016, 65(9): 7036-7050.
[9] ZHAO Nan, YU F R, LI Ming, *et al*. Physical layer security issues in interference-alignment-based wireless networks [J]. IEEE Communications Magazine, 2016, 54(8): 162-168.
[10] TEKIN E, YENER A. Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading [C]// Proceedings of the 45th Annual Allerton Conference on Communications, Control, and Computing: Sep. 26-28, 2007, Allerton House, Illinois, USA: 856-863.
[11] BASSILY R, ULUKUS S. Ergodic secret alignment [J]. IEEE Transactions on Information Theory, 2012, 58(3): 1594-1611.
[12] MO Jianhua, TAO Meixia, LIU Yuan, *et al*. Secure beamforming for MIMO two-way communications with an untrusted relay [J]. IEEE Transactions on Signal Processing, 2014, 62(9): 2185-2199.
[13] XU Hongbin, SUN Li, REN Pinyi, *et al*. Securing two-way cooperative systems with an untrusted relay: a constellation-rotation aided approach [J]. IEEE Communications Letters, 2015, 19(12): 2270-2273.
[14] KHISTI A, WORNELL G. Secure transmission with multiple antennas – I: The MISOME wiretap channels [J]. IEEE Transactions on Information Theory, 2010, 56(7): 3088-3104.
[15] KHISTI A, WORNELL G. Secure transmission with multiple antennas – II: The MIMOME wiretap channels [J]. IEEE Transactions on Information Theory, 2010, 56(11): 5515-5532.
[16] GERACI G, COUILLET R, YUAN Jinhong, *et al*. Secrecy sum-rates with regularized channel inversion precoding under imperfect CSI at the transmitter [C] // Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP): May 26-31, 2013, Vancouver, Canada: 1-4.
[17] ZHU Fengchao, GAO Feifei, YAO Minli, *et al*. Joint information- and jamming-beamforming for physical layer security with full duplex base station [J]. IEEE Transactions on Signal Processing, 2014, 62(24): 6391-6401.
[18] MUKHERJEE A, SWINDLEHURST A L. Robust beamfoming for security in MIMO wiretap channels with imperfect CSI [J]. IEEE Transactions on Signal Processing, 2011, 59(1): 351-361.
[19] LIN C H, TSAI S H, LIN Y P. On quantization for masked beamforming secrecy systems [J]. IEEE Transactions on Wireless Communications, 2015, 14(10): 5616-5628.
[20] LI Na, TAO Xiaofeng, XU Jin. Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback [J]. IEEE Communications Letters, 2014, 18(6): 969-972.
[21] ZHU Fengchao, GAO Feifei, YAO Minli. Zero-forcing beamforming for physical layer security of energy harvesting wireless communications [J]. EURASIP Journal on Wireless Communications and Networking, 2015, 2015(58): 1-9.
[22] DONG Lun, HAN Zhu, PETROPULU A P, *et al*. Improving wireless physical layer security via cooperative relays [J]. IEEE Transactions on Signal Processing, 2010, 58(3): 1875-1888.
[23] LUO Shuangyu, LI Jiangyuan, PETROPULU A P. Uncoordinated cooperative jamming for secret communications [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(7): 1081-1090.
[24] KRIKIDIS I, THOMPSON J S, MCLAUGHLIN S. Relay selection for secure cooperative networks with jamming [J]. IEEE Transactions on Wireless Communications, 2009, 8(10): 5003-5011.
[25] GUO Haiyan, YANG Zhen, ZHANG Linghua, *et al*. Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks [J]. IEEE Transactions on Communications, 2017, 65(5): 2180-2193.
[26] HE Xiang, YENER A. Cooperation with an untrusted relay: a secrecy perspective [J]. IEEE Transactions on Information Theory, 2010, 56(8): 3807-3827.
[27] JU M, HWANG K S. Opportunistic transmission of nonregenerative network with untrusted relay [J]. IEEE Transactions on Vehicular Technology, 2015, 64(6): 2703-2709.
[28] KHODAKARAMI H, LAHOUTI F. Link adaptation with untrusted relay assignment: design and performance analysis [J]. IEEE Transactions on Communications, 2013, 61(12): 4874-4883.
[29] SUN Li, ZHANG Taiyi, LI Yubo, *et al*. Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes [J]. IEEE Transactions on Vehicular Technology, 2012, 61(8): 3801-3807.
[30] SUN Li, REN Pinyi, DU Qinghe, *et al*. Security-aware relaying scheme for cooperative networks with untrusted relay nodes [J]. IEEE Communications Letters, 2015, 19(3): 463-466.
[31] ZHU Jingge, MO Jianhua, TAO Meixia. Cooperative secret communication with artificial noise in symmetric interference channel [J]. IEEE Communications Letters, 2010, 14(4): 885-887.
[32] MA Chuan, LIU Jiaqi, TIAN Xiaohua, *et al*. Interference exploitation in D2D-enabled cellular networks: a secrecy perspective [J]. IEEE Transactions on Communications, 2015, 63(1): 292-242.
[33] XU Hongbin, SUN Li, REN Pinyi, *et al*. Cooperative privacy preserving scheme for downlink

transmission in multiuser relay networks [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(4): 825-839.
[34] GOPALA P K, LAI Lifeng, GAMAL H E. On the secrecy capacity of fading channels [J]. IEEE Transactions on Information Theory, 2008, 54(10): 4687-4698.
[35] HE Biao, ZHOU Xiangyun. Secure on-off transmission design with channel estimation errors [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 1923-1936.
[36] WANG Xiaowei, TAO Meixia, MO Jianhua, *et al*. Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks [J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 693-702.
[37] HU Jianwei, YANG Weiwei, YANG Nan, *et al*. On-off-based secure transmission design with outdated channel state information [J]. IEEE Transactions on Vehicular Technology, 2016, 65(8): 6075-6088.
[38] HU Jianwei, YANG Nan, ZHOU Xiangyun, *et al*. A versatile secure transmission strategy in the presence of outdated CSI [J]. IEEE Transactions on Vehicular Technology, 2016, 65(12): 10084-10090.
[39] LI Xiangming, JIANG Tao, CUI Shuguang, *et al*. Cooperative communications based on rateless network coding in distributed MIMO systems [J]. IEEE Wireless Communications, 2010, 17(3): 60-67.
[40] TANG Xiao, REN Pinyi, HAN Zhu. Distributed power optimization for security-aware multi-channel full-duplex communications: a variational inequality framework [J]. IEEE Transactions on Communications, 2017, 65(9): 4065-4079
[41] SUN Li, DU Qinghe, REN Pinyi, *et al*. Two birds with one stone: towards secure and interference-free D2D transmissions via constellation rotation [J]. IEEE Transactions on Vehicular Technology, 2016, 65(10): 8767-8774.
[42] DU Qinghe, SUN Li, REN Pinyi, *et al*. Statistical security model and power adaptation over wireless fading channels [C] // Proceedings of the International Conference on Wireless Communications & Signal Processing (WCSP): Oct. 15-17, 2015, Nanjing, China: 1-6.
[43] MACKAY D. Fountain codes. IEE Proceedings: Communications, 2005, 152(6): 1062-1068.
[44] NIU Hao, IWAI M, SEZAKI, K, *et al*. Exploiting fountain codes for secure wireless delivery [J]. IEEE Communications Letters, 2014, 18(5): 777-780.
[45] LI Wanyu, DU Qinghe, SUN Li, *et al*. Security enhanced via dynamic fountain code design for wireless delivery [C] // Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC): Apr. 3-6, 2016, Doha, Qatar: 1-6.
[46] SUN Li, REN Pinyi, DU Qinghe, *et al*. Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks [J]. IEEE Transactions on Industrial Informatics, 2016, 12(1): 291-300.
[47] TANG Xiao, REN Pinyi, WANG Yichen, *et al*. Combating full-duplex active eavesdropper: a hierarchical game perspective [J]. IEEE Transactions on Communications, 2017, 65(3): 1379-1395.
[48] LI Lingxiang, PETROPULU A P, A. CHEN Zhi. MIMO secret communications against an active eavesdropper [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(10): 2387-2401.

Biographies

Li Sun, received the B.S. and Ph.D. degrees in Information and Communications Engineering from Xi'an Jiaotong University, China, in 2006 and 2011, respectively. Since Jan. 2012, he has been with the Department of Information and Communications Engineering, Xi'an Jiaotong University, where he is currently an Associate Professor. His research interests include wireless physical-layer security, cooperative relaying networks, and M2M/D2D communications. Currently he is serving as an Editor of the KSII Transactions on Internet and Information Systems, and the Leading Guest Editor of the Wireless Communications and Mobile Computing, Special Issue on "Safeguarding 5G Networks through Physical Layer Security Technologies".

Qinghe Du, received his B.S. and M.S. degrees both from Xi'an Jiaotong University, China, and his Ph.D. degree from Texas A&M University, USA. He is currently an Associate Professor of Information and Communications Engineering Department, Xi'an Jiaotong University, China. His research interests include wireless communications and networking with emphasis on statistical QoS provisioning, secure wireless transmissions, 5G networks, D2D/M2M networks, cognitive radio networks, mobile multicast, etc. He served as an Associate Editor of IEEE Communications Letters.