Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges

Yiliang Liu, Hsiao-Hwa Chen, *Fellow, IEEE*, and Liangmin Wang, *Member, IEEE*

***Abstract*—Physical layer security (PHY-security) takes the advantages of channel randomness nature of transmission media to achieve communication confidentiality and authentication. Wiretap coding and signal processing technologies are expected to play vital roles in this new security mechanism. PHY-security has attracted a lot of attention due to its unique features and the fact that our daily life relies heavily on wireless communications for sensitive and private information transmissions. Compared to conventional cryptography that works to ensure all involved entities to load proper and authenticated cryptographic information, PHY-security technologies perform security functions without considering about how those security protocols are executed. In other words, it does not require to implement any extra security schemes or algorithms on other layers above the physical layer. This survey introduces the fundamental theories of PHY-security, covering confidentiality and authentication, and provides an overview on the state-of-the-art works on PHY-security technologies that can provide secure communications in wireless systems, along with the discussions on challenges and their proposed solutions. Furthermore, at the end of this paper, the open issues are identified as our future research directions.**

***Index Terms*—Physical layer security, wiretap channel, key generation, authentication, multi-antenna systems, relay.**

I. Introduction

WIRELESS communication networks are particularly vulnerable to eavesdropping and impersonation attacks due to the broadcasting nature of wireless channels. Two basic security requirements are presented in wireless communication networks against these threats, including confidentiality and authentication. Confidentiality makes sure that eavesdroppers cannot read confidential messages. Authentication assures that message receivers can ascertain a transmission origin, and any attacker will not be able to impersonate as the message source.

Traditional security approaches employed symmetric and asymmetrical cryptographic algorithms to achieve communication confidentiality and authentication, respectively. This survey paper focuses on an alternative security mechanism, namely PHY-security, which is implemented on physical layer by exploring the randomness nature of physical layer transmission media to achieve both confidentiality and authentication.

Compared to cryptographic technologies implemented at upper layers, PHY-security has a number of advantages. PHY-security is more secure in some ways. For instance, physical characteristics of wireless channels are exploited to guarantee message confidentiality with the help of proper coding and signal processing, where confidential messages are guaranteed to be decoded only by their intended receivers. While there are numerous risks in cryptographic methods due to the rapid advancement of computing technologies, eavesdroppers may have the access to infinite computing capabilities to launch brute force attacks or analytical attacks [1], which can be disastrous for any cryptosystems. Additionally, PHY-security can be implemented in several convenient ways. Rather than consuming massive communication resources or infrastructures to share cryptographic materials amongst legitimate entities [2], PHY-security does not need to consider how security protocols are executed, and it does not require to implement any extra security mechanisms on other layers above the physical layer. Moreover, PHY-authentication can authenticate legitimate nodes quickly before demodulating and decoding signals so that wasteful signal processing for unintended transmissions is avoided.

The origin of PHY-security research can be traced back to Shannon's information theoretic secrecy analysis [3], which defined that security level depends on the amount of information known by eavesdroppers. A perfect secrecy can be achieved when the eavesdroppers ignore the transmitted information completely, except for just randomly guessing the original information bit by bit. This description on security is related closely to the communications in the presence of noise, so that the concepts of entropy and equivocation developed for communication problems have a direct inspiration in the early investigations on PHY-security [4]–[8]. The confidential communications can achieve a maximum message transmission rate using wiretap channel coding, whose rate is defined as the secrecy capacity by Wyner [4]. Actually, Wyner only showed that it is possible to implement secure communications in degraded broadcast channels. PHY-security concepts have become more popular with the introduction of non-degraded

Manuscript received January 12, 2016; revised June 22, 2016; accepted July 30, 2016. Date of publication August 10, 2016; date of current version February 22, 2017. *(Corresponding author: Hsiao-Hwa Chen.)*

Y. Liu is with the Communications Research Center, Harbin Institute of Technology, Harbin 150001, China (e-mail: alanliuyiliang@gmail.com).

H.-H. Chen is with the Department of Engineering Science, National Cheng Kung University, Tainan 70101, Taiwan (e-mail: hshwchen@mail.ncku.edu.tw).

L. Wang is with the Department of Internet of Things Engineering, Jiangsu University, Zhenjiang 212000, China (e-mail: jasonwanglm@gmail.com).

Digital Object Identifier 10.1109/COMST.2016.2598968

channels [9], Gaussian channels [7], [10], small scale fading channels [11]–[20], multi-antenna channels [21]–[61], and relay channels [62]–[105]. Moreover, physical layer key (PHY-key) generation is emerging as a promising confidential technique, which exploits physical layer random characteristics to share secret keys. These random characteristics, such as channel state information (CSI) [106]–[112], received signal strength (RSS) or phase information [113]–[116], and secrecy wiretap channel codes [117]–[121], are raw materials to generate secret keys for two terminals. Recently, the research has been extended to authentication [122]–[151], which can resist against impersonation attacks. From the perspective of security theory, confidentiality and authentication in physical layer constitute a prototype of PHY-security.

In last two decades, researchers have developed a significant amount of mathematical theories, technologies, algorithms, and solutions for tackling PHY-security challenges. Even though the focus varies depending on each scenario, the main challenges on PHY-security research remain unchanged, such as quantification of secrecy capacities, code designs, imperfect or partial CSI issues, fading influence, etc. Specifically, the secrecy capacity outage will occur when an eavesdropper channel becomes better. Thus, how to strengthen secrecy capacities in adverse conditions is still an open issue. These challenges can be generalized in a simple point-to-point channel, and can be further complicated in modern wireless systems.

The advancement in wireless technologies has improved communication service quality significantly, by exploring spatial diversities and multiplexing gains with the help of multi-antennas technologies [152] or using cooperative strategies with the help of relays [153]. As a result, we are facing a large number of signal processing and precoding technologies, which make us to believe that these technologies could continue to promote PHY-security. Because of security constraints, these emerging technologies will not be applied directly to security applications without needed modifications. For instance, the maximization of secrecy capacity of a multi-input-multi-output (MIMO) system is non-convex with multi-variables [33]. Relay transmissions may be more vulnerable to eavesdropping because confidential information is broadcasted twice, i.e., by a source and a relay, respectively. More than that, some relays may be regarded as eavesdroppers. Wireless technologies also provide potential platforms for the implementation of PHY-key generation and PHY-authentication. In PHY-key generation schemes, many researchers are working hard to find ways to deal with low key generation rates, overhead, and group key issues. Moreover, many PHY-authentication schemes utilize pilot signals and hypothesis testing to determine whether current and prior communication attempts are made by the same transmit terminal, where a serious issue is pilot spoofing attacks. In order to address these challenges, a large number of designs and solutions have been introduced and they will be discussed in detail in this survey.

Several excellent survey papers [154]–[164] appeared in the literature on PHY-security, as illustrated in Table I, and we will briefly introduce them in the sequel. Reference [154] provided an overview on signal processing in multi-antenna systems used to guarantee confidentiality on physical layer, focusing on secrecy signal processing in both data transmissions and channel estimation. Reference [155] presented a summary of PHY-security that guarantees confidentiality using cooperative technologies unique to wireless medium, consisting of cooperative jamming by artificial noise/structured codes and by helping nodes. Reference [156] focused on signal processing in combination with channel coding to guarantee confidentiality, introducing a nested code structure and stochastic encoding allowed for both data reliability and confidentiality. Reference [157] listed most commonly used attacks and security requirements, and then introduced five major research topics, covering secrecy capacity, channel precoding, coding, power, and signal detection approaches. The survey in [158] divided PHY-security issues into two categories: i.e., designing transmit strategies without secret keys, and exploiting wireless communication medium to develop secret keys. It is a very comprehensive survey, covering various topics ranging from the fundamentals to signal processing technologies, from cooperative signals technologies to secrecy channel coding and secret key agreements. Zou *et al.* [159] gave a survey, which summarized the security requirements and security attacks of wireless networks, followed by security protocols and algorithms in existing wireless network standards. It also discussed the state-of-the-art PHY-security schemes and the future trends in wireless communication security. References [160] and [161] focused on very specific areas of security researches. Reference [160] discussed both physical layer and upper layer security issues in cognitive radio networks by introducing security threats and their countermeasures. Reference [161] categorized adversarial models against orthogonal frequency division multiplexing (OFDM) systems, and then discussed jamming attacks and possible countermeasures in synchronization, channel estimation, and equalization procedures in detail. Reference [162] surveyed impersonation attacks and some detection methods. Kapetanovic *et al.* [163] believed that jamming attacks are serious threats in MIMO beamforming designs because these attacks influence beamforming matrices in channel estimation processes. It is worth mentioning that [163] made a conclusion that massive MIMO systems have a great potential to boost up secrecy capacities. Recently, PHY-security issues attract more attentions in body area networks. Reference [164] showed some PHY-security methods to maintain security and

TABLE I
EXISTING SURVEY PAPERS AND THEIR FOCUSED ISSUES

Surveys	Focused issues
[156]	Multi-antenna systems
[157]	Cooperative strategies, relay systems
[158]	Error-control coding
[159]–[161]	Comprehensive surveys
[161]	Jamming attacks, detection methods
[162]	Cognitive radio networks
[163]	OFDM systems
[164]	Impersonation attacks, detection methods
[165]	Massive MIMO, jamming attacks, detection methods
[166]	Medical devices

reliability of medical devices when they have less security softwares and limited energy to implement cryptographic technologies.

This work distinguishes itself from the existing literature surveys in four aspects. First, most of the surveys took into account a limited number of authentication schemes. However, from the security viewpoint, authentication is an important requirement for any wireless system, even more important than confidential communications, because two terminals usually need to verify with each other before starting communications. Second, we summarize general challenges in this area from a more methodological viewpoint if compared to the previous surveys. Third, the organization on PHY-security in this paper is different with the survey in [158]. Rather than going through the fundamentals to signal processing technologies of PHY-security, we devise a new structure to follow a fundamentals-challenges-solutions path, in which the fundamentals of wiretap coding, PHY-key generation, and PHY-authentication are introduced first, followed by coding and signal processing technologies that create proper environments for these theories to work effectively. We believe this descriptive approach allows us to highlight the priorities that researchers have to focus on. Finally and most importantly, different from the survey in [158], we discuss the newest precoding techniques in signal processing areas, such as transmit precoding and cooperation schemes in MIMO and relay systems, which are emerging technologies in next generation wireless communications. In addition, we also identify several topics ignored in the literature, such as the issues on antenna limitations, relay locations and power control. This survey paper embraces more than 200 most relevant literatures and books [165]–[167] on the PHY-security of wireless communication networks.

In summary, this paper provides a comprehensive overview on the fundamentals and technologies of PHY-security, followed by the discussions on their challenges and solutions. The areas of technologies, challenges, and solutions are categorized into wiretap code designs, secure multi-antenna and relay technologies, PHY-key generation technologies, and PHY-authentication technologies. The objectives in revisiting those important topics are summarized as follows. 1) Showcase the latest PHY-security concepts, theories, and technologies; 2) Point out the challenges in PHY-security researches; 3) Identifying the ways to apply the state of the art techniques to tackle these challenges; 4) Highlight the future research directions.

The rest of the paper can be outlined as follows. Section II describes the fundamentals and technologies of PHY-security. Section III discusses the challenges in implementing these technologies. Section IV is to present wiretap coding design solutions through the investigation on wireless fading channels, partial/imperfect CSIs, and compound wiretap channels. Section V introduces some practical secure multi-antenna technologies. Section VI focuses on cooperative relays. Section VII provides the newest PHY-key generation methods. Section VIII illustrates the results in PHY-authentication. The open research issues and conclusions are given in Sections IX and X, respectively. A structural diagram of this survey is shown in Fig. 1, and the abbreviations used in this paper are listed in Table II.

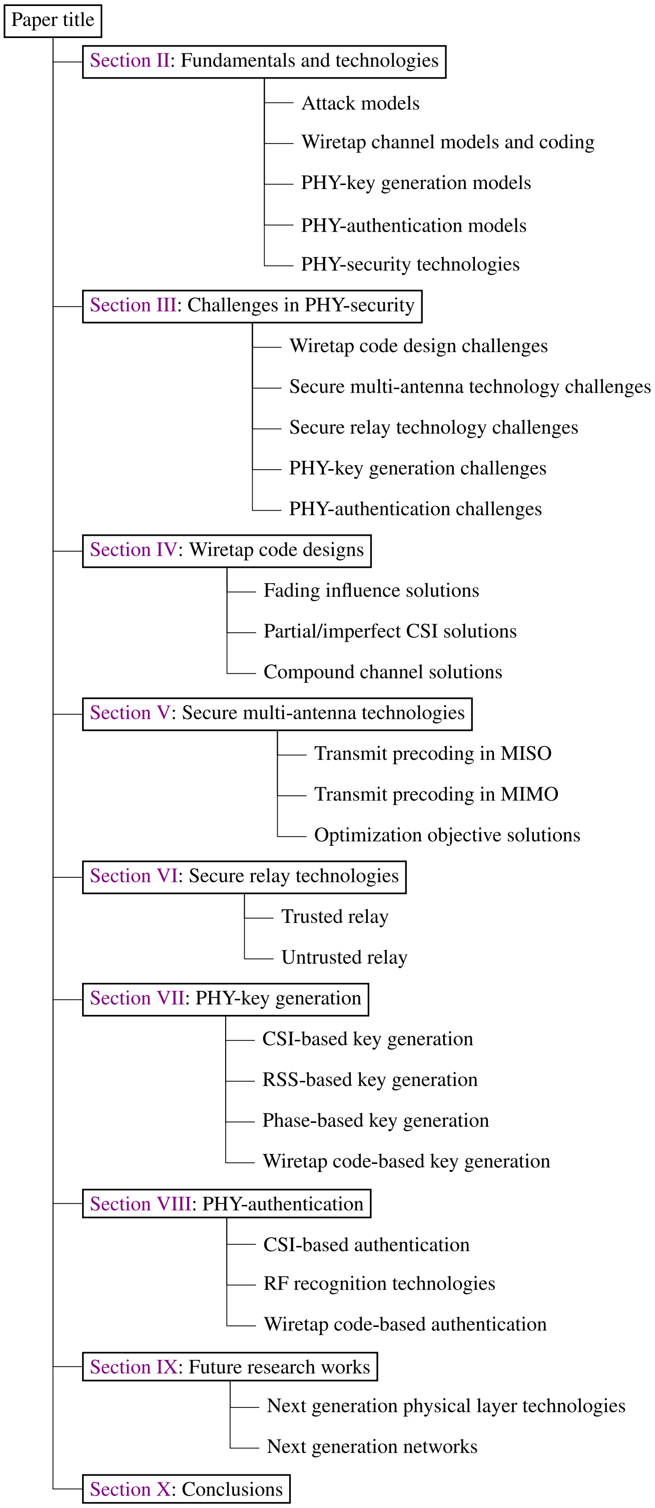

Paper title
Section II: Fundamentals and technologies
Attack models
Wiretap channel models and coding
PHY-key generation models
PHY-authentication models
PHY-security technologies
Section III: Challenges in PHY-security
Wiretap code design challenges
Secure multi-antenna technology challenges
Secure relay technology challenges
PHY-key generation challenges
PHY-authentication challenges
Section IV: Wiretap code designs
Fading influence solutions
Partial/imperfect CSI solutions
Compound channel solutions
Section V: Secure multi-antenna technologies
Transmit precoding in MISO
Transmit precoding in MIMO
Optimization objective solutions
Section VI: Secure relay technologies
Trusted relay
Untrusted relay
Section VII: PHY-key generation
CSI-based key generation
RSS-based key generation
Phase-based key generation
Wiretap code-based key generation
Section VIII: PHY-authentication
CSI-based authentication
RF recognition technologies
Wiretap code-based authentication
Section IX: Future research works
Next generation physical layer technologies
Next generation networks
Section X: Conclusions

Fig. 1. A structural diagram of this survey.

II. Physical Layer Security Fundamentals and Technologies

PHY-confidentiality was introduced first in a wiretap channel model, which uses non-structured random codes. The core

TABLE II
ABBREVIATIONS AND THEIR DEFINITIONS

Abbreviation	Definition
AF	Amplify and forward
AN	Artificial noise
AWGN	Additive white Gaussian noise
BER	Bit error rate
BSC	Binary symmetric channel
CDMA	Code division multiple access
CF	Compress and forward
CSI	Channel state information
CTF	Compute and forward
DCMRWC	Degraded compound multi-receiver wiretap channel
DF	Decode and forward
D2D	Device to device communication
GSVD	Generalized singular value decomposition
IC	Integrated circuit
LDPC	Low-density parity-check
LMS	Least mean square
LTE-A	Long term evolution-advanced
MANET	Mobile ad-hoc network
MTC	Machine type communication
MIMO	Multi-input-multiple-output
MISO	Multi-input-single-output
ML	Maximum likelihood
MPSRM	Minimum per-user secrecy rate maximization
MSE	Mean-squared error
NF	Noise and forward
NLMS	Normalized least mean square
OFDM	Orthogonal frequency division multiplexing
PHY-authentication	Physical layer authentication
PHY-key	Physical layer key
PHY-security	Physical layer security
QoS	Quality of service
QPSK	Quadrature phase shift keyin
RF	Radio frequency
SCM	Secrecy capacity maximization
SDP	Semidefinite programming
SIMO	Single-input-multiple-output
SINR	Signal-to-interference-plus-noise ratio
SISO	Single-input-single-output
SQM	Signal quality maximization
SNR	Signal to noise ratio
SSRM	Secrecy sum rate maximization
SVD	Singular value decomposition
TDD	Time-division duplex
TTPM	Total transmit power minimization
TA	Trusted authority
VANET	Vehicular ad hoc network
ZF	Zero forcing

is to maximize a data transmission rate with a secrecy constraint on the information attainability to an eavesdropper. The wiretap coding must also provide a reliable link between a legitimate sender and a legitimate receiver, where information can be transmitted with an arbitrarily small amount of errors, even though this channel is subject to uncontrollable ambient noises. Shannon [3] proved that proper channel coding achieves reliability. The remaining task is to achieve an optimal secrecy capacity using efficient channel coding or signal processing to ensure both reliability and security. A popular approach for this purpose is to design secure non-structured random codes or structured codes, and use signal processing technologies of multi-antenna and relay systems to create a proper environment for these codes to work effectively. PHY-key generation methods were proposed as alternative solutions for confidentiality. The main task of PHY-key generation is to improve the entropy of randomness in shared channels between two terminals. Latest methods mainly include CSI-based, RSS-based, phase-based, and wiretap code-based key generations. On the other hand, PHY-authentication utilizes pilot signals and channel characteristics to determine the identities of terminals. The task of PHY-authentication is to resist against pilot spoofing attacks. Novel authentication schemes were designed based on CSIs, wiretap codes, radio frequency (RF) recognition, etc.

A. Attack Models

First, let us discuss about attacker models, including eavesdropping, jamming assisted eavesdropping, impersonation, and messages falsification.

- Eavesdropping: Eavesdropping attackers can be classified as active eavesdroppers and silent eavesdroppers. The difference between the two is that active eavesdroppers working as communication parties send some messages to transmitters by accident, whose CSIs can be obtained via CSI estimation. Silent eavesdroppers eavesdrop messages while keeping silent, so their CSIs are not available for transmitters.
- Jamming assisted eavesdropping: Jamming assisted attackers aim to find ways to improve eavesdropping abilities. This attack was investigated in [163] and [168], which wants to send jamming signals to minimize secrecy capacities. Recently, [169] and [170] discussed the issue in a different perspective such that the proactive eavesdroppers can be seen as legitimate monitors. Instead of minimizing secrecy capacities, the proactive eavesdroppers are interested in transmitting jamming signals to maximize wiretap channel capacities.
- Impersonation: Identity impersonators destroy identity-centric trust. These attackers may forge massive fake identities, or embezzle other legitimate nodes' identities, such as Sybil attacks [171]. Especially on the physical layer, without medium access control and IP/IPv6 protocols, broadcasting nature of wireless channels makes it more vulnerable to this type of attacks.
- Messages falsification: Messages falsification destroys data-centric trust. Internal or external attackers have their abilities to modify a part of messages in transmission processes, then affecting receivers' trusts on the messages.

The basic countermeasures are confidential communications and authentication with proper physical layer technologies or cryptography. Here, our discussions focus mainly on their physical layer fundamentals and technologies.

B. Wiretap Channel Models and Coding

In 1975, Wyner [4] introduced a discrete memoryless wiretap channel model. As seen in Fig. 2, messages are reliably

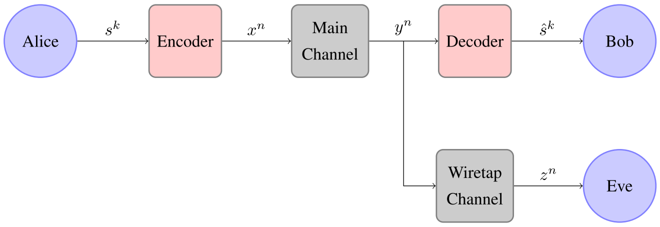


Fig. 2. A general wiretap channel model. The messages $\mathcal{M}$ are mapped to binary sequences by Alice. Each sequence consists of k bits, where $s^k = (s_1, \ldots s_k)$ and $s \in \{0, 1\}$. s^k is encoded into a binary vector $x^n = (x_1, \ldots x_n)$, which is sent via the main channel and the channel outputs are $y^n = (y_1, \ldots y_n)$ with the main channel transition probability p. Meanwhile, Eve observes y^n with a wiretap channel transition probability p_e. The corresponding output is z^n.

transmitted to Bob[1] via the main channel, while the messages are kept confidential to Eve in a wiretap channel. Wyner [4] implied that the intrinsic elements of physical channels, such as noises and interferences, play central roles in secure communications.

Let the source entropy of the message s^k be $d = H(s^k)$. Eve's residual equivocation with regard to s^k is given by a conditional entropy, i.e., $H(s^k|z^n)$. The rate of the coding $(2^n, R)$ must be lower than the residual entropy ratio, i.e., $Rd \leq H(s^k|z^n)/n$, which ensures total confidentiality against eavesdroppers. Wyner provided the characterization of a family of achievable pairs (R, d), and implied that there exists a randomized codebook maximizing R. The maximizing secrecy rate is defined as a secrecy capacity C_s as

$$C_s = \max_{V \to X \to YZ} I(V; Y) - I(V; Z), \tag{1}$$

where $I(\cdot; \cdot)$ denotes mutual information, and V is an auxiliary input variable with a joint auxiliary input distribution $p(s)p(v|s)p(x|v)$. Given a discrete memoryless channel $P_{YZ|X}$, wiretap codes achieve the secrecy capacity via maximization over the choices of the joint distribution $P_{YZ|X}$, such that the Markov chain $V \to X \to YZ$ holds [9]. Furthermore, the difference maximization between two mutual information values is taken over all possible input distributions $p(x)$. For given inputs, the transition probabilities of the main and wiretap channels can quantify their mutual information values, respectively. Hence, transition probabilities, no matter which are fixed or quasi-static random (which obey Rayleigh, Rician, and Nakagami-m distributions, but are constant within the coherent time), are essential to wiretap code designs.

The aforementioned discussions focused on non-structured random codes, [172]–[175] presented structured wiretap codes and advocated that, similar to non-structured random codes, the structured random code generation is useful for providing secrecy. Structured wiretap codes are also mapped to the codewords by random wiretap coding, combined with rate splitting, nested dimension, and channel prefixing technologies. The procedures to generate secure structured wiretap coding consist of three phases, namely codebook generation, encoding, and decoding phases, which are summarized as follows.

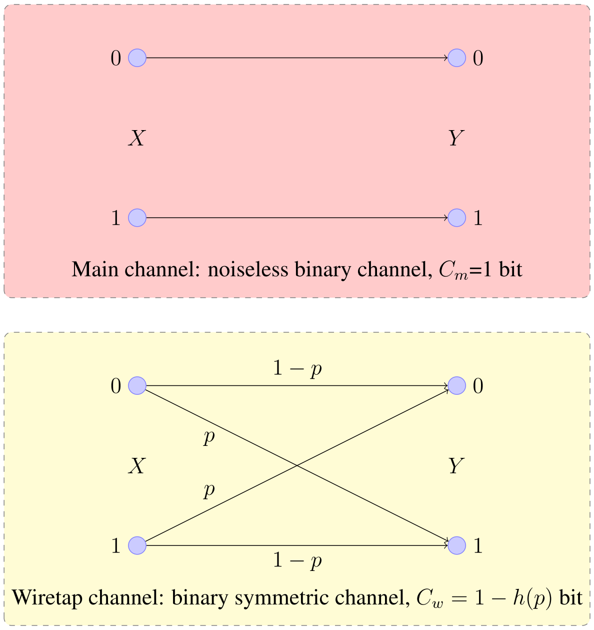

0
0
X
Y
1
1
Main channel: noiseless binary channel, C_m=1 bit
$1-p$
0
0
p
X
Y
p
1
1
$1-p$
Wiretap channel: binary symmetric channel, $C_w = 1 - h(p)$ bit

Fig. 3. An extreme example wiretap channel model, where the main channel is a noiseless binary channel and the wiretap channel is a BSC with its bit error rate p. Any transmitted bit in the main channel is received without error, while the capacity of the wiretap channel depends on p. In the case of $p = 0.5$, the wiretap capacity is zero and the wiretap channel model is in an ideal condition with $C_s = 1$ bit. In the case of $p = 0.1100278$, the wiretap capacity is more than 0.5, and the secrecy capacity drops to lower than 0.5.

- Codebook generation: First, a predefined encoder generates $2^{nI(V;Y)}$ independently and identically distributed sequences v^n according to each v_i^n distribution probability. These sequences are randomly distributed in 2^{nC_s} dimensions, and each dimension represents a codeword, such that a code x^n has $2^{nI(V;Z)}$ codewords, each of which has index w_i. In each w_i, the first sub-codeword is used to convey message, and the rest sub-codewords are used to confuse the eavesdroppers.
- Encoding: When a transmitter wants to send v^i, it will check if $v^i \in \mathbf{w}$. If yes, it encodes by $f\{V \to X^n\}$ according to $P(x^n|v^n) = \prod_{i=1}^{n} P(x_i|v_i)$; otherwise it takes a codebook generation process.
- Decoding: Messages are transmitted over the main channel $P(y^n|x^n) = \prod_{i=1}^{n} P(y_i|x_i)$. An intended receiver checks for the unique sequence v^n through $g\{Y^n \to X^n\}$, such that a pair of (x^n, v^n) are contained in a set of two dimensions.

Reference [175] showed that, although the structured wiretap codes look like randomly generated codes, it is not completely random as every component of each codeword has to be a lattice point.

The wiretap code rate can go too low when the security constraint is taken into account. Fig. 3 gives an extreme example of wiretap channel model to show its low secrecy capacity. First, we provide an ideal case where the main channel is a noiseless binary channel, and the wiretap channel is a binary symmetric channel (BSC) with its bit error rate (BER)

[1] In this security architecture, the nomenclatures, Alice, Bob, and Eve, usually refer to a legitimate transmitter, an intended receiver, and an unauthorized eavesdropper, respectively.

$p = 0.5$. This scenario means that the wiretap channel is in the worst condition, while the main channel is in the best condition. It is seen that as long as the wiretap code rate is $R = 1$, the equivocation can be equal to total binary source information entropy because $h(0.5) = 1$. However, when the wiretap channel becomes better as $h(p) = 0.5$, which corresponds to $p = 0.1100278$ [5], in order to be consistent with the binary source information entropy, the wiretap code rate must drop to less than 0.5. Reference [8] provided a special class of broadcast channels, where both the main and wiretap channels are symmetric. It gave the difference between the conditions "a little noisy" and "more capable", and the results also showed that the wiretap code rate equals to the difference between the capacities of the two channels, which is very small.

The investigations on memoryless discrete-time additive white Gaussian noise (AWGN) channels [7], [10] also indicated that the wiretap code rate is inefficient and not fault-tolerant. AWGN channels are defined as a complete characterization of an independent additive noise and a power constraint. Moreover, a Gaussian channel matches to many practical channels, including radio and satellite links. Reference [10] utilized Wyner's framework to characterize an achievable (R, d) region for AWGN wiretap channels, letting $C_m = (1/2)\log(1+\mathrm{SNR}_m)$ be the capacity of the main channel and $C_w = (1/2)\log(1+\mathrm{SNR}_w)$ be the capacity of the wiretap channel. SNR_m and SNR_w are the signal to noise ratios (SNR) of the main channel and wiretap channel, respectively. The secrecy capacity of the AWGN wiretap channel is given by

$$\begin{aligned} C_s = \max_{x} \ & \{C_m - C_w\}, \\ \text{s.t.} \ & \mathrm{E}\left\{x^2\right\} \le P, \end{aligned} \tag{2}$$

where the channel input signal x must satisfy an average total power constraint P. Eqns. (1) and (2) show that the secrecy capacity is a relative measure, involving the difference of data rates to Bob and Eve. Obviously, when SNR_m is less than SNR_w, the secrecy capacity is zero. When SNR_m is greater than SNR_w, it is feasible for a wiretap coding scheme of a transmitter to yield a secrecy capacity. The secrecy capacity is limited and upper bounded by $1/2\log(N_e/N_b)$ (bits per transmission), where N_b and N_e are the main channel Gaussian noise power and the wiretap channel Gaussian noise power, respectively. No matter how large we allocate the power, the capacity is still too low to be useful in practice. We already see the demands for advanced schemes and signal processing technologies, such as PHY-key generation, multi-antenna and relay methods, to enhance secrecy capacities.

C. PHY-Key Generation Models

The fundamental idea of the PHY-key generation model is to accumulate a small amount of secrecy information of channels in key generation, which relies on the randomness of transmit-receive channels, such as CSI, RSS or phase information. An alternative but more practical method presented in [176] is the cumulate key generation from wiretap codes transmitted via wiretap channels, although wiretap coding schemes are difficult to achieve sufficient secrecy capacities in bad main channel scenarios. Fig. 4 shows a general PHY-key generation process based on channel randomness and wiretap channel models, including randomness (channel randomness and wiretap code randomness) extraction, quantization, information reconciliation, and privacy amplification sub-processes.

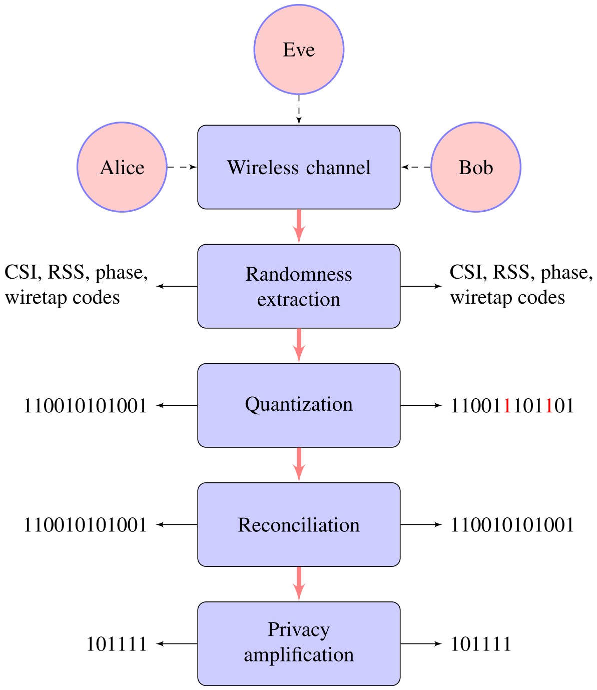


Fig. 4. A general PHY-key generation model, where two terminals are located at the ends of the same time division duplex (TDD) wireless channel experiencing theoretical identical fading. Eve is located one-half wavelength away from Bob, and experiences channel fading uncorrelated with Bob. The generation process includes randomness extraction, quantization, information reconciliation, and privacy amplification sub-processes.

In the randomness extraction sub-process, Alice and Bob measure CSIs, RSS, or phase information. Each measured parameter is theoretically identical when Alice and Bob are connected in the same wireless channel, and can be different when Eve lies one-half wavelength away from Bob. Alternatively, Alice and Bob share opportunistic randomness by wiretap codes when secrecy capacities are positive. The quantization sub-process is used to quantize the extracted randomness into bits. The reconciliation sub-process is carried out synchronously between Alice and Bob in order to ensure that the keys generated separately on both sides are identical. The privacy amplification sub-process is a method for eliminating Eve's partial information about the key, or directly uses wiretap codes because they are invisible to Eve.

D. PHY-Authentication Models

The essence of the PHY-authentication model is to recognize identity information, which relies on the uniqueness of CSIs of the medium in all transmit-receive channels [123]. It performs channel estimation by pilot signals[2] and hypothesis

[2] Standard techniques to probe the channels include pulse-style probing and multi-tonal probing.

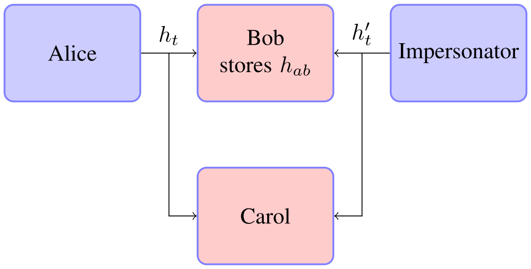


Fig. 5. A general PHY-authentication model. Bob who stores the CSI between Alice and Bob can verify signal transmitted from Alice by channel estimation and hypothesis testing. Bob and an unaware receiver Carol can decode the information without errors, but only Bob can authenticate the signals. The impersonator is an attacker that wants to impersonate Alice.

testing to determine whether the current and prior communication attempts are made by the same transmit terminal.

In Fig. 5, a PHY-authentication model with Gaussian channels assumes that Bob first stores Alice's CSI h_{ab}. Bob can decide whether a transmitting terminal is still Alice when receiving subsequent signals. The decision is made based on a noisy measured version of h_t by channel estimation. Bob uses a simple hypothesis test to decide if the transmitting terminal is Alice or a would-be intruder, as given by

$$\begin{cases} \mathcal{H}_0 : h_t = h_{ab}, \\ \mathcal{H}_1 : h_t \neq h_{ab}, \end{cases} \tag{3}$$

where the null hypothesis $\mathcal{H}_0$ means that the terminal is not an intruder, and Bob accepts this hypothesis if the test statistic he computed is $h_t = h_{ab}$. Otherwise, he accepts the alternative hypothesis, $\mathcal{H}_1$, indicating that the claimant terminal is an intruder. Reference [129] simulated spatially variable CSIs in real environments and proved that the CSI is location-specific, which means, each channel has intrinsic characteristics, such as unique scattering environments, spatial variability or multipath delay characteristics [139], and two channels are considered independent when the distance between the transmit antennas is larger than one-half wavelengths. On the other hand, within the coherent time, the CSI is essentially invariant, which gives us the opportunities to emulate the correlation characteristics of the parties involved.

E. PHY-Security Technologies

In order to ease the implementation of PHY-security by improving transmission rate and verifying the identities of terminals, several technologies have been proposed in the literature. They can be categorized as wiretap code designs, secure multi-antenna technologies, secure relay technologies, PHY-key generation technologies, and PHY-authentication technologies.

1) Wiretap Code Designs: According to the information theory on PHY-security, the key to implement coding is to understand the characteristics of known coding schemes and then integrate codes in more complex scenarios. In addition to the non-structured wiretap coding schemes, practical wiretap coding schemes based on low-density parity-check (LDPC) coding [177], [178], and polar coding [179] were proposed to achieve the confidentiality. These coding schemes belong to structured codes. Reference [177] considered noiseless main channels, binary erasure channels, and binary symmetric channels as the special cases for wiretap channels, then proposed specific LDPC codes to achieve secrecy. The coding scheme in [178] was also proposed based on LDPC coding, but used in Gaussian channel scenarios, yielding a BER close to 0.5 for Eve. Both [177] and [178] can be encoded in linear time, and applicable with finite block lengths. Reference [179] used polar codes as an instantiation of wiretap channel models, where both the main channel and wiretap channel are binary symmetric. Note that the polar coding schemes were derived from a phenomenon called polarization, which is different from other structured wiretap coding schemes. The wiretap coding based on polar codes is illustrated in Fig. 6.

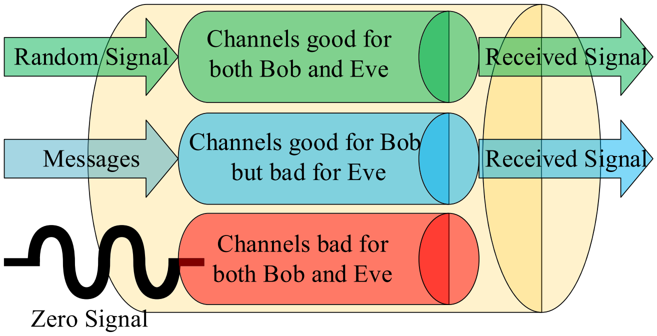
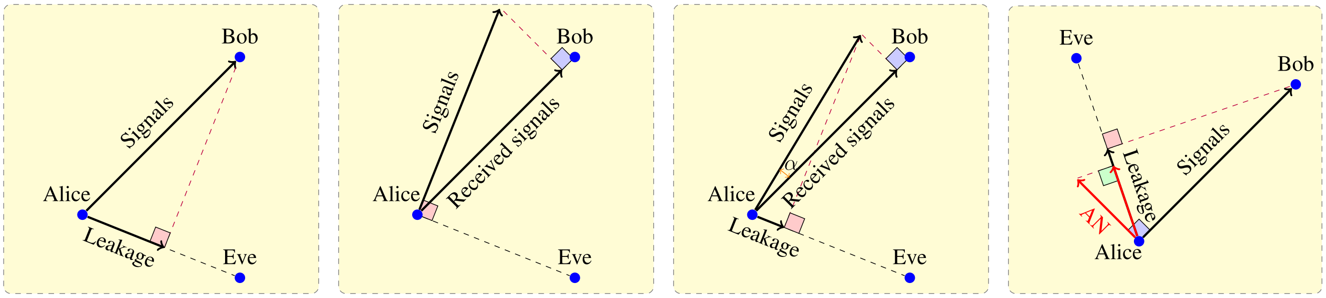

Random Signal
Channels good for both Bob and Eve
Received Signal
Messages
Channels good for Bob but bad for Eve
Received Signal
Channels bad for both Bob and Eve
Zero Signal

Fig. 6. Wiretap channel coding based on polar codes. Given a set of polarized channels, Alice transmits random bits over those channels that are good for both Eve and Bob, the information bits over those channels that are good for Bob but bad for Eve, and zeros over those channels that are bad for both Bob and Eve.

Fig. 6 shows intuitively the channel polarization phenomenon, where the channel is divided into noiseless sub-channels and pure-noise sub-channels. The information bits reach to Bob via good (almost noiseless) channels. Thus, Bob should be able to reconstruct them with a very low error probability. On the other hand, the same bits pass through bad (almost useless) channels to Eve. Thus, Eve will not be able to deduce much information from her observations.

2) Secure Multi-Antenna Technologies: In multi-antenna systems, transmitters as well as receivers are equipped with multiple antennas, which use space-time signal processing to improve wireless transmission rates. Secure multi-antenna technologies serve for the same purpose with normal multi-antenna systems to achieve an upper bound on the secrecy capacity of multi-antenna wiretap channels. The key of the secure multi-antenna research is to enlarge the signal strength difference between Bob and Eve. We briefly summarize these techniques in four categories, covering beamforming, ZF precoding, convex (CVX)-based precoding, and AN precoding in Fig. 7. Reference [24] used multi-input-single-output (MISO) techniques to beamform same information in different antennas to make it as close to the main channel direction as possible. When Bob is also equipped with multiple antennas, Alice uses a beamforming technique based on GSVD [32] to decompose both the main channel and the wiretap channel into a set of parallel independent sub-channels, which can be



(a) Beamforming. (b) ZF precoding. (c) CVX-based precoding. (d) AN precoding.

Fig. 7. Illustrative diagrams of basic secure multi-antenna technologies, including beamforming, ZF precoding, CVX-based precoding, and AN precoding. For simplicity, we set two-dimensional diagrams and a single signal transmit direction, i.e., assume that a 2×2 MIMO system has the same space directions.

selected freely and then be encoded separately. Reference [56] used another secure signal processing technologies based on ZF precoding, where the messages are transmitted to Bob via a shifted beamforming direction, which is as orthogonal to Eve's channel as possible. When the number of Alice's antennas is larger than Eve's, ZF precoding is superior to beamforming because it is tractable to find the null spaces of Eve. References [27] and [58] addressed the transmit covariance matrix optimization based on CVX tools for secrecy capacity maximization in MISO and MIMO, respectively. Only CVX-based methods can provide an optimal secrecy capacity but use a very complex procedure due to the fact that the objectives are matrices. Reference [43] utilized antennas to create AN symbols, which lie in the null spaces of the main channels, so that they do not affect Bob, while Eve's channel is degraded with a high probability.

3) Secure Relay Technologies: Relay systems play an important role in multi-hop wireless networks when transmitters have limited power to send messages. Through the exploitation of relay cooperative strategies [62], such as decode and forward (DF), amplify and forward (AF), noise and forward (NF), and compress and forward (CF), relays can enhance the secrecy capacities of wireless networks. In DF strategies, a relay cooperating with Alice first decodes messages when receiving them, and then re-encodes the messages before sending to Bob. The secrecy capacity of DF is zero when the channel of Alice to the relay is noisier than the channel from Alice to Bob. In AF strategies, Alice encodes its messages and sends them to a relay in the first interval. Then, the relay sends a weighted version of the received noisy signals in the second interval, while Alice sends the combination of recent and previous signals if there is a direct channel between Alice and Bob. In this way, the transmitted signals are enhanced such that the secrecy capacity is improved. NF strategies transform the relay-aided channels into two compound channels. In the first Alice/relay to Bob channel, the relay sends messages for Bob. In the second Alice/relay to Eve channel, the relay only sends artificial signals to confuse Eve. In particular, NF strategies introduce a deaf helper [75], [76], where the relay does not need to listen to Alice, but can still enable a secrecy transmission via generating AN signals. CF can be viewed as a generalization of NF. The relay is not required to decode data, and just sends a quantized version of the relay's noisy observations to Bob. This noisy version of its observations helps Bob in decoding Alice's messages, while its independent codewords from AN signals are used to confuse Eve.

4) PHY-Key Generation: Physical layer randomness plays an significant role in PHY-key generation. According to different randomness properties, there are four categories presented in past two decades to discuss PHY-key generation, including CSI-based [109], RSS-based [113], phase-based [114], and wiretap code-based key generation technologies [117]. In CSI-based technologies, Alice and Bob use pilot signals to obtain Bob-to-Alice CSI h_{ba} and Alice-to-Bob CSI h_{ab}, respectively. In TDD communications, Alice and Bob experience same multi-path fading of a wireless link so that h_{ba} and h_{ab} are theoretically identical. Alice and Bob agree on a secret key based on h_{ba} and h_{ab} using a source coding scheme [180]. RSS-based and phase-based key generation technologies are similar to CSI-based methods, which also use pilot signals and channel estimation methods to recover distorted RSS and phase information. However, RSS-based and phase-based technologies are more practical, which exploit channel reciprocity on RSS or phase information. As the measurements of RSS and phase can be easily read from oscilloscopes and analog-to-digital converters (ADC) [114], RSS-based and phase-based technologies may be applied to next generation secure communications. Wiretap code-based technologies rely on wiretap channel models in our previous discussions in Section II-B. The basic idea of this method is that, even if Bob has a noisy channel, fading gives the opportunity of having positive secrecy capacities to transmit a small amount of confidential bits, which can be collected to form a longer secret sequence for follow-up secure communications.

5) PHY-Authentication Technologies: PHY-authentication should not be ignored because it works as a digital signature to verify the validity of a transmitter's identity. The key of PHY-authentication is to recognize the identities of wireless terminals on physical layer as soon as possible. There are three technologies devoted to PHY-authentication, including CSI-based authentication, RF recognition approaches, and wiretap code-based authentication. References [124] and [125] designed CSI-based authentication, which follows a paradigm of embedded signalling in CSIs to resist against CSI impersonation attacks. The additional embedded signals are sneakers and identification that only can be detected by aware receivers. The RF recognition system [132] determines a device's identity by comparing a captured emission signal from an unintentional device, such as its instantaneous amplitudes, phases, and frequencies, with the reference templates of all known devices. The wiretap coding scheme [133] selects a part of its codebook materials before sharing them between a transmitter and a receiver, where the sender is authenticated if a receiver can successfully demodulate and decode the transmission.

III. Challenges in PHY-Security

Different technologies, ranging from wiretap coding, secure signal processing, PHY-key generation, to PHY-authentication, create diverse issues in wireless networks. These issues lead to a number of research topics, which will be discussed in the sub-sections below. In particular, partial CSI issues should be considered in all aforementioned technologies, because Eve's CSI is not available in case that Eve is a non-cooperator or a silent eavesdropper. On the other hand, fading influence is more specific in wiretap code designs because it reduces secrecy capacities. However, channel fading is not regarded as a challenge but as a benefit in MIMO systems, as signal fluctuations in the channels creates more degrees of freedom.

A. Challenges in Wiretap Code Designs

The aforementioned discussions identified the technologies to achieve secrecy capacity with the help of coding techniques. However, various challenges exist when they are used in different wireless networks.

1) Fading Influence: A secrecy capacity is a preset variable, and it is infeasible to keep it constant because signals are usually propagated by means of reflection, diffraction, and scattering. The fading channels are induced by multiple delayed versions of a transmitted signal such that they carry both time- and location-related properties. The researches on wiretap fading channels include Rayleigh fading channels [11], Rician fading channels [54], Nakagami-*m* fading channels [17], slow fading channels [21], fast fading channels [18], [19], flat fading channels [14], and frequency selective fading channels [20], [181]. Note that frequency selective fading channels [181] are more complex when we need to consider (OFDM) systems. The influence of fading does not allow us to use a simple AWGN channel model as mentioned above to analyze a secrecy capacity and design a PHY-security system. As to channel coding, it seems that we need to investigate fading channels using average (ergodic) secrecy capacities, instead of the AWGN secrecy capacities.

2) Partial/Imperfect CSI: Wiretap coding requires the CSI from both Bob and Eve, including their transmission probabilities and channel gains. With perfect CSI, encoders can obtain optimal inputs via calculating secrecy capacities. In practice, estimation error, feedback quantization error/delay, or channel mobilities are the challenges for the CSI estimation. On the other hand, the CSI of an intended receiver is easy to obtain by handshakes in advance between Alice and the corresponding receiver. However, as a non-cooperator or a silent eavesdropper, Eve is infeasible to collaborate with Alice. Hence, partial CSI makes it extremely challenging to optimize and calculate secrecy capacities.

3) Compound Channels: In many practical scenarios, Alice desires to use a broadcast channel to send confidential messages available to multiple intended receivers, while keeping them confidential to all eavesdroppers. Since each pair of Eve and Bob's channels carry different CSI values, it is more challenging for Alice to design a wiretap broadcast coding scheme, especially in the presence of multiple eavesdroppers [182]. Moreover, researchers begin to study multi-access channels for transmissions of multiple confidential messages [183], [184]. In contrast to broadcast channels, a multi-access channel is a scenario with multiple transmitters and receivers. The problem is more difficult in the presence of multiple eavesdroppers and eavesdroppers' CSIs[3] are usually unknown to Alice [185].

B. Challenges in Secure Multi-Antenna Technologies

Here, the major challenge is to maximize the achievable secrecy rates by optimizing transmit precoding schemes, especially in partial CSI conditions. In addition, the optimization problem, as a special case in secure MIMO systems, should not be ignored.

1) Transmit Precoding: The core issue on multi-antenna wiretap channels is to design an optimal transmit covariance matrix to achieve a good secrecy capacity. The first issue is to propose a computable secrecy capacity expression for Gaussian multi-antenna wiretap channel under an average power constraint. In [33] assumed that all CSIs are known to Alice, and then provided an expression for the secrecy capacity of the Gaussian multi-antenna wiretap channel model ([33] focused on MIMO) under a covariance matrix power constraint, which is given as

$$\begin{aligned} C_s = \max\ & \left[\log\det\left(\mathbf{I}_b + \mathbf{H}_b\mathbf{Q}\mathbf{H}_b^H\right) - \log\det\left(\mathbf{I}_e + \mathbf{H}_e\mathbf{Q}\mathbf{H}_e^H\right)\right], \\ \text{s.t.}\ & \operatorname{Tr}(\mathbf{Q}) \leq P,\ \mathbf{Q} \succeq \mathbf{0}, \end{aligned} \tag{4}$$

where $\mathbf{I}_b$ and $\mathbf{I}_e$ are the identity matrices of additive Gaussian noise vectors, $\mathbf{H}_b$ and $\mathbf{H}_e$ are CSI matrices of the main and wiretap channels, respectively, $\mathbf{H}_b \in \mathbb{C}^{r\times t}$, $\mathbf{H}_e \in \mathbb{C}^{e\times t}$. r, t, and e are the numbers of antennas of an intended receiver, a transmitter, and an eavesdropper, respectively. $\mathbf{Q}$ is a transmit covariance matrix characterized by $\mathbf{Q} = \mathrm{E}[\mathbf{x}\mathbf{x}^H]$, where $\mathbf{x}$ is a transmit input with or without precoding. The average total power constraint can be modelled as Tr($\mathbf{Q}$)$\leq P$. In order to obtain the optimal transmit covariance, the transmit input must be designed alone with optimal precoding. The partial CSI problems become more serious in multi-antenna wireless scenarios. For instance, [45], [47], [52] raised up a question on how to deal with precoding and power allocation issues when Eve's CSI is uncertain. Reference [51] focused on the question on how to measure secrecy capacities without Eve's CSI.

2) Optimization Objectives: The MIMO transmit precoding scheme relies heavily on its secrecy capacity. Thus, transmit covariance optimization is usually transformed to a secrecy capacity maximization (SCM) problem. Reference [23] pointed out that mathematical problem is more complex in

[3] "Alice to Eve CSI" is usually denoted as "eavesdropper's CSI" or "Eve's CSI". This term can be extended to other links.

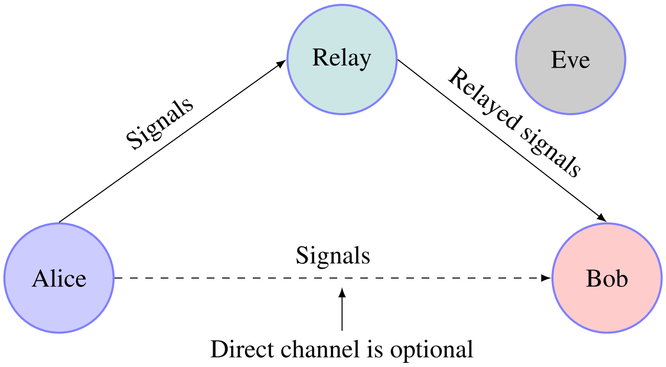


Fig. 8. A general trusted relay wiretap model, where a relay can choose various strategies according to actual circumstances.

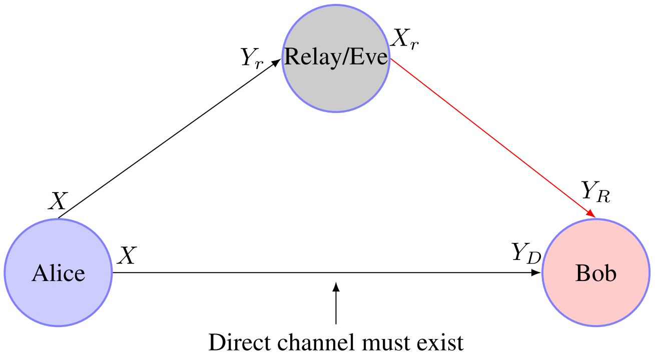


Fig. 9. A general untrusted relay model. Alice communicates with a relay and Bob via a broadcast channel, and the relay communicates with Bob via a link which is separate (orthogonal) from the broadcast channel from Alice. Here, it is assumed that the relay is co-located with an eavesdropper.

MIMO scenarios because both $\{\log\det(\mathbf{I}_b + \mathbf{H}_b\mathbf{Q}\mathbf{H}_b^H)\}$ and $\{\log\det(\mathbf{I}_e + \mathbf{H}_e\mathbf{Q}\mathbf{H}_e^H)\}$ are concave functions of a matrix $\mathbf{Q}$. The objective function is a difference of these two concave functions. Thus, the problem of SCM is not convex. In addition, SCM objective is hard to implement in practical communication systems because the variables of objective functions in SCM are associated with CSIs of both Alice and Bob.

C. Challenges in Secure Relays

There are two categories of relays involved security issues. The first one to be concerned is the issue on trusted relays, which are authorized to facilitate secrecy communications between transmitters and intended receivers. The other one is the issue on untrusted relays.[4] Confidential information should be kept away from the untrusted relays even though we still need to utilize them.

1) Trusted Relays: Fig. 8 shows a typical network topology of a trusted relay wiretap channel. In the investigations done in [62], the secrecy capacity expression of a trusted relay channel is generally defined as

$$\begin{aligned} C_s = \max_{x,w} \ & \{C_d - C_e\}, \\ \text{s.t.} \ & \mathrm{E}\left(x^2\right) \le P_1, \mathrm{E}\left(w^2\right) \le P_2, \end{aligned} \tag{5}$$

where x and w are variables of source signals and relayed signals, respectively. P_1 and P_2 are average power constraints of a transmitter and a relay, respectively. The maximum is pursued over all transmit power covariances. The first term C_d is the rate required to guarantee successful decoding in the channel between Alice and Bob. The second term C_e is the achievable rate in the channel between Alice and Eve. Here, we assume that there is an optional direct channel from the transmitter to an intended receiver. In fact, [62] and [63] found that the distances from Alice to relay imposes a significant challenge for calculating the secrecy capacities. Hence, finding an optimal relay location according to different cooperative strategies is a special requirement in trusted relay researches. The investigations on compound relay wiretap channels, two-way relay wiretap channels, and relays with multiple antennas also attract much attention.

2) Untrusted Relays: The investigations in [91] and [92] revealed that the secrecy capacity of an untrusted relay channel is not always positive. Reference [94] further showed that a positive secrecy capacity is achievable when Alice communicates with a relay and Bob via a broadcast channel, and when the relay communicates with Bob via a separate link, which is an orthogonal link with respect to the broadcast channel. The orthogonal model is shown in Fig. 9. Because the relay to Bob channel output is independent of the outputs of Alice to Bob and to the relay channels, Alice can conceal information against the untrusted relay by secure cooperative strategies in the relay. In conclusion, the property of the positive secrecy capacity depends on the stochastic properties of the relay channels with orthogonal components.

As shown in [94], the secrecy capacity expression of an untrusted relay channel is defined as

$$C_s = [I(X; Y_R, Y_D) - I(X; Y_r)]^+, \tag{6}$$

where $[x]^+ \triangleq \max\{0, x\}$, a transmitter sends X to a relay and Bob, and its outputs are Y_r and Y_D, respectively. Then, the relay forwards the received signal (defined as X_r) to Bob, whose outputs is Y_R. Here, we assume that the relay is co-located with an eavesdropper. Hence, the first term $I(X; Y_R, Y_D)$ is the rate required to guarantee successful decoding when receiving the combined signals from the relay and Alice. The second term $I(X; Y_r)$ is the relay's residual equivocation about signal X when obtaining Y_r. Since the relay is untrusted, it would be a strong eavesdropper when it is allocated with many resources. Therefore, the main challenge to use an untrusted relay is resource control. Specifically, when considering a multi-antenna system as given in [97], power and the number of antennas should be assigned to determine whether these untrusted relays should still participate in cooperative communications, or whether the cooperation with the untrusted relays can bring us any benefit. Even though an untrusted relay is not used, it can participate in communications as a deaf helper with cooperative relay jammer technologies [75], [76]. Thus, the investigation on deaf

[4] This model corresponds to several practical scenarios. For example, in public ad hoc networks, the relays may be unauthenticated, despite the fact that they are operating with known protocols.

helpers of untrusted relays is another open issue, in addition to the issues associated with trusted relays, such as compound untrusted relay, two-way untrusted relay, and untrusted relays with multiple antennas, which are also the focus of attention in the literature.

D. Challenges in PHY-Key Generation

Various challenges exist in PHY-key generation when we actually use these technologies in wireless networks. In particular, PHY-key generation must deal with extra issues such as the combination of signal processing and cryptography technologies.

1) Generation Overhead: It is claimed that the keys must be identical in two parities. Hence, the reconciliation subprocess is essential, which is a key error-correction process between Alice and Bob. Existing approaches focus mainly on error-control coding, such as polar codes and LDPC. It has been shown that the error-control coding needs a large number of extra bits to reconcile the bit mismatch, which consumes a significant amount of time and space overhead [114].

2) Low Key Generation Rates: Existing PHY-key generation technologies offer very low key generation rates. The reasons can be summarized as follows. First, to correct error keys, a larger number of extra bits have to be used in transmissions. Second, wireless channels can not afford to provide abundant secrecy capacities to extract secret messages. This problem also exists in wiretap coding schemes.

3) Group Key Issues: In wireless networks with multiple nodes, group key generation schemes are more efficient compared to one-by-one generation methods. The group secure communications include two scenarios: 1) an identical key is shared in all nodes; 2) each pair maintain a different key with other pairs. Obviously, in the second scenario, key generation suffers from a high complexity because each node needs to maintain a large number of keys.

E. Challenges in PHY-Authentication

1) Impersonation Attacks: PHY-authentication relies on the uniqueness of CSIs over any transmitter-receiver channels. From the analysis in [127] and [128], PHY-authentication is sensitive to impersonation attacks, where an attacker can obtain the legitimate channel information, especially, when it is located close to the legitimate devices. An attacker may also alter the channel estimation at a receiver by pre-processing the transmitted signal. Reference [135] provided a fingerprinting counterfeit strategy in MIMO systems that minimizes the average time required to break in the authentication system, where attackers can maximize the probability of successful attacking using maximum likelihood estimate of Alice to Bob CSI based on the observations of other channels' CSIs.

2) CSI Estimation Errors: PHY-authentication assumes that a correct reference CSI is always available. From the analysis in [129], the assumption does not hold in general, since the channel response changes with channel coherent time. Hence, it requires that channel estimation works fast enough in relative to channel coherent time, or the number of channel response samples is large enough to overcome the time-varying effect.

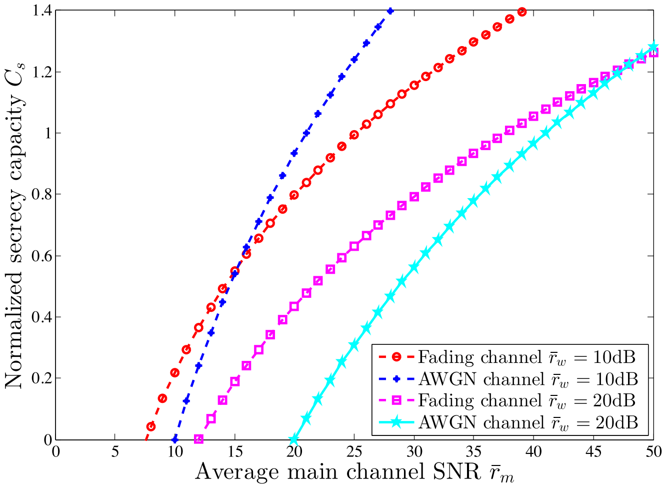


Fig. 10. Comparison between average secrecy capacities and normal Gaussian secrecy capacities. Red and mauve lines represent average secrecy capacities, where both main and wiretap channels are standard AWGN channels with Rayleigh fading coefficients, while blue and cyan lines represent normal Gaussian secrecy capacities, where both main and wiretap channels are standard AWGN channels. In both scenarios, the average SNR of a main channel is denoted as $\bar{r_m}$. The average SNR of a wiretap channel is represented by $\bar{r_w}$.

In addition, [140] showed that authentication under a binary hypothesis testing can not guarantee a robust performance at a low SNR due to a large overlapped portion of CSIs from different sources, because the overlapping parts are induced due to noises and terminal movements, as well as channel variations in channel coefficient amplitude and path delay.

IV. Solutions on Wiretap Code Designs

This section describes the ways to tackle the challenges on wiretap code designs.

A. Fading Influence Solutions

In PHY-security research, fading is no longer a burden for communications, and it facilitates PHY-security if we can deal with it carefully. When an eavesdropper has a better channel, the properties in fading give us the opportunity to exploit the time instants when the main channel is better than the eavesdropper channel to exchange confidential messages. For the secrecy capacity evaluation over the fading channels, [11] introduced an average secrecy capacity metric instead of normal secrecy capacities.

Fig. 10 shows a visual comparison between average secrecy capacities and normal Gaussian secrecy capacities. We adopt the same assumptions in [117], such that the blue and cyan lines represent normal Gaussian secrecy capacities where both the main and wiretap channels are AWGN channels, and the red and mauve lines represent ergodic secrecy capacities where both the main and wiretap channels are standard AWGN channels with Rayleigh fading. The average SNR of the main channel is $\bar{r_m}$. The average SNR of the wiretap channel is $\bar{r_w}$. In Fig. 10, the average secrecy capacities of the fading channel are indeed lower than that of the AWGN channel, because fading reduces more main channel capacities than wiretap channel capacities when average SNR of the main channel is far better than that of the wiretap channel. However, when main SNR becomes lower (even lower than the wiretap SNR), the secrecy capacities of the fading channel are better than the AWGN channel, because in this case, fading influence is large enough such that Alice must design proper wiretap codes based on the main channel fading features, while this codes are mismatched to the wiretap channel with a high probability.

The above investigation focused on the intuitional properties of point-to-point Rayleigh fading wiretap channels. Afterwards, [12] further investigated the secrecy capacity in slow fading broadcast channels, in which fading broadcast wiretap channel is regarded as a general model of parallel independent sub-channels. It provided a graphical approach to evaluate the secrecy capacity. Reference [14] generalized the multiple eavesdroppers case over flat channels. Reference [16] investigated the ways measuring secrecy capacity when the main and wiretap channels are correlated. The level of the correlation depends largely on antenna deployments. For example, antenna deployments at a high altitude in rural or suburban areas generate dominant line-of-sight paths, which result in a high correlation between the received signals at two receivers. It is also possible that the eavesdropper actively induces the correlation by approaching the legitimate receiver. Reference [54] considered a Rician fading channel from Alice to Eve and realized an ergodic secrecy capacity in the presence of multiple antennas at Eve. Reference [17] presented the ergodic secrecy capacity expression of a Nakagami-*m* fading channel in the presence of multiple eavesdroppers. The Nakagami-*m* fading is a generalized distribution, which models different fading environments and matches to practical environments better than Rayleigh or Rician distributions. In the fast fading channels, it is difficult to estimate CSIs because of channel estimation delay. Reference [18] used statistical main and wiretap CSIs only to characterize the secrecy capacity on the condition that the number of Bob's antennas is more than (or equal to) Eve's. Reference [19] considered the channel estimation error derived from fast fading, and characterized the secrecy capacity by providing upper and lower bounds. Frequency selective fading gives more degrees of freedom for security rather than bringing in problems, although the ways to utilize frequency selective fading seem to be rather complex. Reference [20] proposed an AN-based scheme in frequency selective fading channels to degrade Eve's signal reception quality. The scheme divides the main channel into multiple sub-channels in frequency domain, and transmits AN signals in deep-faded sub-channels to confuse Eve, while these AN signals null out Bob. With this method, the received signal quality difference between Bob and Eve is enlarged so as to improve secrecy capacities.

B. Partial/Imperfect CSI Solutions

1) Statistical CSI Approaches: The knowledge of Eve's CSI plays a critical role in determining the corresponding optimal wiretap codes. References [46] and [52] presented a channel statistical approach, which used an appropriate model where the uncertainty of practical CSI was taken into account. It was assumed that Eve's CSI H_{ae} is modelled in two parts as

$$H_{ae} = \sqrt{\kappa} d + \sqrt{1-\kappa} \bar{H_{ae}}, \tag{7}$$

where d is the determined component of the channel between Alice and Eve, which is often referred to as CSI statistics, and $\bar{H_{ae}}$ is an indeterminate component. The scalar κ indicates the confidence level of the available CSI knowledge. If $\kappa = 1$, Alice has perfect CSI. If $0 \le \kappa \le 1$, Alice has imperfect CSI. And if $\kappa = 0$, Alice has no CSI about Eve. Consider a time-varying channel, where the channel stays constant in a time slot and changes from one slot to another according to a stationary correlation model. Reference [45] showed that the classical Clarke's isotropic scattering could be used in the correlation model.

2) Secrecy Outage Metric Approaches: In case that Eve's CSI is not available, [22] used a secrecy outage probability of an ergodic secrecy capacity as a primary security performance metric instead of the secrecy capacity. The secrecy outage probability metric indicates that there is a likelihood that the instantaneous secrecy capacity C_s' goes below a target value C_s. The outage probability metric is defined as

$$P_{out}(C_s) = P\left(C_s' < C_s\right). \tag{8}$$

The outage probability in PHY-security was investigated first for Gaussian Rayleigh channels [11], including a conventional outage metric in fading channels, which occurs when decoding errors appear at an intended receiver at its source transmission capacity, whose capacity without secrecy constraints is assumed to be R ($R > C_s$). In addition, an outage event occurs when the ergodic secrecy capacity is not achieved, which is caused mainly by a) the fact that the main channel offers no advantage over the wiretap channel; b) estimation errors or lack of Eve's CSI.

Reference [117] showed that the distance between transmitters and receivers is the main factor determining outage probabilities because SNR corresponding to fading channel is mainly affected by the distances. And [12] proposed a low-complexity on/off power allocation strategy, which decides if it should transmit messages or not based on CSI conditions. Reference [186] evaluated the lower and upper bounds of the secrecy capacities over all possible fading states, and derived an approximation of the bounds. In general, CSI uncertainty issues can be more serious in MIMO channels.

C. Compound Channel Solutions

A compound wiretap channel generalizes the Wyner's wiretap channel model by taking into account the number of possible states of the channels to the legitimate receivers and those to the eavesdroppers. Compound wiretap channels can be divided into two broad categories, i.e., wiretap broadcast channels and wiretap multi-access channels.

1) Broadcast Channels: Reference [6] proposed a secret broadcast system with two noisy wiretap channels, which was regarded as one of the original researches on the capacity region of parallel channels. It was assumed that any two of eavesdroppers in the broadcast channels can not cooperate with each other. Reference [14] also investigated the secrecy capacities of wireless fading channels in the presence of multiple

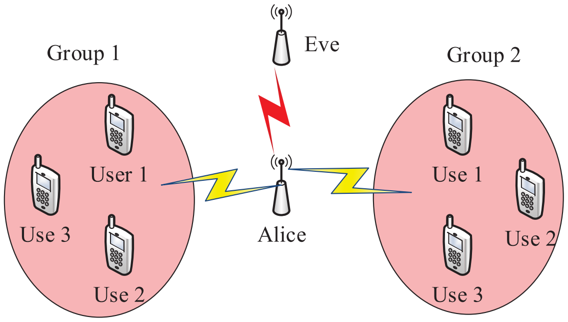


Fig. 11. DCMRWC1, where Alice sends a confidential message to the users in Group 1, and a different confidential message to the users in Group 2, and both messages should be kept confidential from Eve.

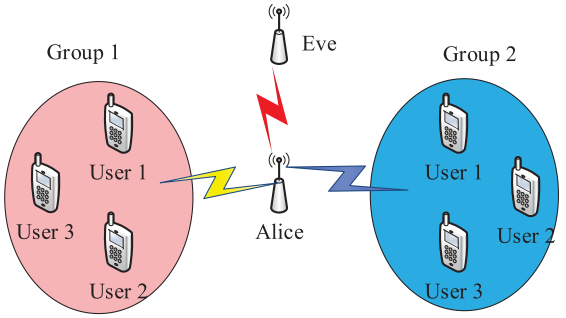


Fig. 12. DCMRWC2, where Alice sends a confidential message to the users in Group 1, which needs to be kept confidential from the users in Group 2 and Eve. Moreover, the transmitter sends a different confidential message to the users in Group 2, which should be kept confidential from the users in Group 1 and Eve.

eavesdroppers. It was assumed that all eavesdroppers are mutually independent. It derived analytical results of the secrecy capacities in terms of outage metrics and ergodic metrics. Reference [31] extended wiretap channels to general broadcast MIMO scenarios, in which there are multiple receivers, and the messages are delivered to each individual receiver, invisible to the other intended users. Reference [182] summarized previous investigations on the secrecy capacity region of wiretap broadcast channels, and then proposed a compound channel model called degraded compound multiple receiver wiretap channel (DCMRWC). Two different communication scenarios were studied for each version of DCMRWC, as shown in Figs. 11 and 12.

In these cases of independent compound channels, security mechanisms use independent wiretap codebooks for each channel to achieve its capacity. This conclusion plays an important role in modern multi-antenna or multi-channel technologies [30], because these technologies can use SVD or GSVD to convert their channels into equivalent parallel channels.

2) Multi-Access Channels: Reference [187] studied the secrecy capacity region of discrete memoryless multi-access channels by equivocation rates, where two users attempt to transmit information to a destination and each user also has confidential information intended for the destination. In this scenario, each user views the other one as an eavesdropper. Reference [68] considered multi-access channels over a common Gaussian relay channel, and used AN to enhance the secrecy capacity. Reference [188] considered an intelligent eavesdropper that can select carefully a group of sub-channels. Thus, the feature was characterized by new constraints that we have never met before. The imperfect CSI issue was investigated in [185], covering both Gaussian MIMO multi-access wiretap channels and two-user Gaussian MIMO broadcast wiretap channels. Reference [189] studied multi-access channels where two users were permitted to maintain communication links with finite secrecy capacities.

V. Secure Multi-Antenna Technologies

To further enhance the transmission rates with the constraints of PHY-security, many investigators developed multi-antenna technologies [152], [190] to increase secrecy capacities, because they can use multiple antennas to achieve more degrees of freedom. This section will investigate the PHY-security problems of MISO and MIMO scenarios, where various optimal and sub-optimal transmit precoding approaches are usually combined for achieving secrecy capacity maximization. Alternatively, signal quality difference maximization between main and wiretap channels also attract our attention, in addition to traditional secrecy capacity maximization schemes.

A. Transmit Precoding in MISO

The signal processing methods can be simplified in the special cases when each intended receiver has only one antenna (i.e., a MISO scenario). A summary of the investigations on the MISO wiretap channels was presented in Table III.

1) GSVD-Based and SVD-Based Beamforming: In GSVD-based beamforming, a geometrical interpretation shows that a main channel and a wiretap channel can be divided into several parallel channels by performing GSVD and precoding $\mathbf{x} = \mathbf{v}s$, where $s \sim \mathcal{CN}(0, 1)$, and $\mathbf{v}$ is the eigenvector corresponding to the largest generalized eigenvalue of the pencil $(\mathbf{I} + P\mathbf{h}_b^H\mathbf{h}_b, \mathbf{I} + P\mathbf{H}_e^H\mathbf{H}_e)$, as proved in [25] and [32]. The obtained beamforming is sub-optimal at any SNR. In a high SNR region, the optimal direction approaches to a zero-forcing scheme, where the beams are tuned toward the direction of an intended receiver, but orthogonal to the eavesdropper. In a low SNR region, it beams to the main channel directly. Without Eve's CSI, [24] proposed a sub-optimal SVD beamforming, whose direction can be adjusted as orthogonal to the wiretap channel direction as possible, and as close to the main channel direction as possible.

2) Cooperative Jammer: Reference [23] proposed a cooperative jammer technique for security purposes. The technique uses a fraction of power P_2 to send a jamming signal $\mathbf{x}_2$ and uses the remaining power P_1 to send a secrecy message x_1. Hence, the received signal y_e at an eavesdropper is $y_e = \mathbf{h}_e(\boldsymbol{\alpha}x_1 + \sqrt{1 - \boldsymbol{\alpha}^T\boldsymbol{\alpha}}\mathbf{x}_2) + n_e$, while the received signal at an intended receiver is $y = \mathbf{h}_b\boldsymbol{\alpha}x_1 + n_b$. The conclusion is that with an optimally chosen constant of $P_2 = \boldsymbol{\alpha}^T\boldsymbol{\alpha}/(1 - \boldsymbol{\alpha}^T\boldsymbol{\alpha})P_1$, a wiretap coding can be used for secrecy communications. $\mathbf{x}_2$ should be linearly correlated to the beam

TABLE III
COMPARISON OF PRECODING STRATEGIES IN SECURE MISO SYSTEMS

Scenario	CSI condition	Strategy	Explanation
MISOME [32]	Perfect CSI	GSVD	In a high SNR region, use ZF detection. In a low SNR region, use eigenvector approaches corresponding to the largest eigenvalue of $(\mathbf{I} + P\mathbf{h}_b^H\mathbf{h}_b, \mathbf{I} + P\mathbf{H}_e^H\mathbf{H}_e)$.
MISOME [25], [32]	Main CSI & Statistical wiretap CSI	AN; SVD	Beamform information in Bob's direction, and generate AN symbols orthogonal to the main channels (requiring $t > \frac{1}{2}e$).
MISOSE	Main CSI & Statistical wiretap CSI [24]; CSI with errors [40]	Beamforming	Beamform information to the main channel direction.
MISOSE	CSI with errors [27], [46]; Perfect CSI [26];	SDP; AN [46]	Transform a nonconvex secrecy capacity optimization problem to a convex one, and find optimal transmit matrices by SDP.
MISOSE [23]	CSI with errors	Cooperative jamming	Create a cooperative signal which is correlated linearly to secret messages, and transmit it along Eve's direction to cancel the secret messages.
MISOSE	CSI with errors [40]; Statistical wiretap CSI [48]	AN; ZF; CVX	Use CVX tools in ZF and AN schemes to find an optimal transmit direction.

of x_1 in such a way that they can cancel each other at Eve as $\boldsymbol{\alpha} x_1 + \sqrt{1 - \boldsymbol{\alpha}^T\boldsymbol{\alpha}}\mathbf{x}_2 = \mathbf{0}$.

3) AN Precoding: Reference [25] proposed a simple scheme that uses only the knowledge of $\mathbf{h}_b$ in choosing transmit directions, where a near-optimal performance is achieved in a high SNR region. The scheme transmits AN in all orthogonal subspaces of the intended directions. The messages are sent in a dimension visible to the intended receiver, while potential eavesdroppers always receive a mixture of AN and signals. Even if eavesdroppers have more than one antenna, AN signals are not fully orthogonal to any of them with a high probability. In a simple intuitive explanation in [32], the number of transmit antennas still should be determined to satisfy the requirement $t > \frac{1}{2}e$. This is because a transmitter in the AN-aided schemes uses additional $t - 1$ dimensions to transmit AN to the null-space of an intended receiver's channel. An eavesdropper needs at least $t - 1$ antennas to cancel the AN, and an additional t antennas to search for secrecy messages. Hence, the eavesdropper requires at least $2t - 1$ antennas. Moreover, the transmitter has an ability to use more antennas and sends noise into more orthogonal channels via additional antennas, so that the probability that an eavesdropper recovers original messages can be further reduced.

The CSI estimation error for the main channel is a big problem in AN precoding. It is actually possible to yield a stronger interference at the main direction, causing a significant secrecy rate loss, when AN signals leak into the main channel with false CSI. As indicated in [51], when the main channel is good enough, the power should be allocated uniformly between data signals and AN, because AN leakage will be negligible. On the other hand, when the main channel is bad, the power allocated to the AN must be more conservative in order to limit the effect of AN leakage.

4) CVX-Based Precoding: CVX-based precoding technologies in MISO scenarios are relatively simple if compared to MIMO scenarios, but more complex than the above three precoding schemes. Reference [26] suggested an optimized power allocation strategy by referencing to other similar investigations that achieved a cognitive radio spectrum sharing capacity with interference power constraints. Li and Ma [27] used a semi-definite program (SDP) to form a non-convex optimization problem. Reference [46] investigated the secrecy capacity based on joint channel error bounds and AN schemes. All of them in principle are sub-gradient methods via an exhaustive search over the set $\{\mathbf{Q} : \mathbf{Q} \succeq \mathbf{0}, \mathrm{Tr}(\mathbf{Q}) \leq P\}$ to find an optimal transmit covariance matrix $\mathbf{Q}$ that can maximize the secrecy capacity.

5) Joint Precoding: References [40] and [48] investigated joint precoding with ZF and AN precoding, where AN direction and ZF direction can be found using an exhaustive search algorithm that is similar to the sub-gradient method. As shown by the simulation results in [48], AN signals are not necessary in one-eavesdropper scenarios when the main channels are better than wiretap channels with perfect CSI. However, an AN-aided transmission will be very effective in improving the secrecy capacity in a multi-eavesdroppers scenario without the knowledge of Bob's CSI.

B. Transmit Precoding in MIMO

The signal processing solutions in MISO systems can be extended to MIMO scenarios. A summary of the works on the MIMO wiretap channels is presented in Table IV.

1) GSVD-Based Precoding: Reference [33] gave a practical design that uses GSVD-based precoding to establish a transmit matrix to separate the sub-channels of a MIMO system into two different subspace groups, S_1 and S_2, where S_1 is for intended receivers only, and S_2 is for intended receivers and eavesdroppers. Most of transmission power will be allocated to the subspace S_1, and only a small fraction for S_2. The available power is distributed uniformly over each dimension of these two subspaces. With this power allocation scheme, in a high SNR region, the scheme achieves its optimal secrecy capacity. However, in a low SNR region, the power is limited, and the secrecy rate with the former power allocation can not approach to the optimal secrecy capacity. In order to make a good use of limited power, [35] used only the sub-channels, in which the output at an eavesdropper is a degraded version of the output at the intended receiver. With the help of GSVD of the pencil $(\mathbf{H}_b, \mathbf{H}_e)$, the main and wiretap channels can be represented by two non-negative diagonal matrices, $\mathbf{M}$ and $\mathbf{W}$, where m_i and w_i are the ith diagonal elements of these matrices. The proposed GSVD-based power allocation strategy chooses these sub-channels corresponding to the condition $m_i > w_i$ as available channels and allocated power to

TABLE IV
COMPARISON OF PRECODING STRATEGIES IN SECURE MIMO SYSTEMS

CSI Condition	Strategy	Explanation
Perfect CSI	GSVD-based precoding [33], [35]	Select secrecy subspace to send messages by GSVD-based precoding, and the best antenna allocation such that the number of antennas satisfies $t : r = 2 : 1$ and $e < 3t$.
Perfect CSI	ZF precoding [38], [56]	Select secrecy subspace to send messages by ZF precoding with QoS-based (MSE [38], SINR [56]) power allocation with $t > e$. When $t \geq r + e$, ZF is better than GSVD-based precoding.
Imperfect main and wiretap CSI	AN precoding [43], [44]	Generate noise to interfere Eve, but not to interfere Bob with QoS-based (MSE [45], SINR [47], [52], [53]) and equal power allocation [50].
Perfect main CSI & Statistical wiretap CSI	Orthogonal blinding [37], [41]	Send AN signals into an orthogonal space of Bob by Gram-Schmidt algorithm. Transmit messages by ZF, requiring $t \geq e$.
Perfect CSI	CVX-based [39], [48], [57], [60]	Generate $\mathbf{Q}$ using CVX tools, where an optimal secrecy capacity is achieved. Generate $\mathbf{Q}$ using CVX tools with QoS-based (SINR [39]) or transmit power minimization [60], where an sub-optimal secrecy capacity is achieved.
Perfect CSI	CVX-based [59]	Generate $\mathbf{Q}$ using CVX tools in each sub-channel. An sub-optimal secrecy capacity is achieved.

them. Clearly, if there are no such sub-channels, the achievable secrecy rate of this transmission would be zero.

In the GSVD-based precoding technologies, even when Alice and Bob could fully exploit the knowledge of $\mathbf{H}_e$, a fraction of secrecy messages are still leaked into the wiretap channel and decoded by eavesdropper if the number of transmit antennas is not large enough. To investigate the message leaking, [33], [35] also studied the numbers of antennas at both Alice and Bob. The results showed that the best antenna allocation between the transmitter and the intended receiver is $t : r = 2 : 1$. In this case, Eve is required to use three times more antennas than Bob to eavesdrop secure communications.

2) ZF Precoding: References [38] and [56] used another secure signal processing technologies based on ZF precoding. Messages are separated by different beamforming directions and then transmitted by multiple antennas, where the transmitter can use a ZF precoding matrix $\mathbf{F}_Z$ that cancels the gain of the wiretap channel by imposing an additional constraint $\mathbf{H}_e\mathbf{F}_Z = \mathbf{0}$. In addition, ZF precoding was so designed such that no interference exists between different antennas. These properties guarantee both security and reliability. It was assumed that a transmitter has full channel knowledge of an intended receiver and an eavesdropper. Otherwise, there is a message leakage. To satisfy the security and transmit power constraints, the message $\mathbf{x}$ is separated by different beamforming directions by ZF precoding matrix $\mathbf{F}_Z$, defined as

$$\begin{pmatrix} \mathbf{y} \\ \mathbf{y}_e \end{pmatrix} = \begin{pmatrix} \mathbf{H}_b \\ \mathbf{H}_e \end{pmatrix} \mathbf{F}_Z \mathbf{x}, \tag{9}$$

where $\mathbf{H}_e\mathbf{F}_Z = \mathbf{0}$, defined as a secrecy constraint, and $\mathbf{F}_Z^{-1}\binom{\mathbf{H}_b}{\mathbf{H}_e}\mathbf{F}_Z = \mathbf{I}$, defined as a QoS constraint. With a pre-assumed QoS constraint, the optimal procedure searches for a transmit matrix $\mathbf{F}_Z$ and the corresponding decoding matrix $\mathbf{F}_Z^{-1}$ such that all multiuser interferences are zero. The secure precoding based on ZF beamforming requires that the number of Alice's antennas is larger than Eve's. In addition, it has its own advantages if compared to GSVD-based precoding. As indicated in [56], the simulation results showed that when $r + e \leq t$, ZF precoding has a higher secrecy capacity than GSVD-based precoding.

3) AN Precoding: The GSVD or ZF secrecy beamforming is usually used in the scenarios when Eve's CSI is known. In partial CSI conditions, the concept of utilizing AN or jamming signals to enhance secrecy was first proposed independently in [43] and [44], where the AN signals can be transmitted to the null spaces of desired directions. These AN-aided schemes exploit a fraction of the transmit power, which is then allocated to send artificially generated noise signals. This type of techniques carry two advantages. First, transmitters are not required to obtain the CSI of Eve. Certainly, the statistical CSI of Eve should be known by Alice to calculate the average secrecy capacity, which is achievable because Alice can assume the channel environments of Eve. Second, there are no strict limitation on the condition of better main channels. AN-aided beamforming achieves an inherent trade-off between the transmission rate and the ability to impair Eve. It should be noted that, if perfect CSI of the Eve's channel is available, the AN precoding technologies are not required.

References [37] and [41] proposed another AN precoding technologies, called orthogonal blinding, to achieve $\mathbf{Q}$ for secrecy MIMO communications, where a transmitter needs at least two antennas in order to send noise into an orthogonal channel of the main channel by precoding. First, Alice uses a Gram-Schmidt algorithm to compute a channel $\mathbf{H}'_b$ orthonormal to Bob' channel $\mathbf{H}_b$, and each row in $\mathbf{H}'_b$ is orthogonal to any other rows in $\mathbf{H}'_b$. Then, Alice combines them into a single channel matrix $H = \binom{\mathbf{H}_b}{\mathbf{H}'_b}$. Under a given power constraint, Alice builds up a zero-forcing filter on the combined matrix $\binom{\mathbf{H}_b}{\mathbf{H}'_b}$ to cancel the interference of different channels and output $\mathbf{Q} = (\mathbf{B}, \mathbf{Z})$, so that $\mathbf{q}_i^T\mathbf{h}_j = 0$ when i and j are in different rows, where $\mathbf{q}_i$ and $\mathbf{h}_j$ are the ith and jth eigenvectors of the matrices $\mathbf{Q}$ and $\mathbf{H}$, respectively. The transmission of a superposition of data signals and AN is mathematically modelled as

$$\begin{pmatrix} \mathbf{y} \\ \mathbf{y}_e \end{pmatrix} = \begin{pmatrix} \mathbf{H}_b \\ \mathbf{H}_e \end{pmatrix} (\mathbf{B}, \mathbf{Z}) \begin{pmatrix} \mathbf{w} \\ \mathbf{v} \end{pmatrix}, \tag{10}$$

where $\mathbf{H}_b\mathbf{Z} = \mathbf{0}$, which ensures that the intended receiver can receive its intended signal only. And $\mathbf{w}$ is the transmitted signal of the desired user, and $\mathbf{v}$ is a random AN signal. Reference [50] proposed another algorithm based on SVD to generate orthogonal interferences to the main channel.

Schulz *et al.* [42] and Zheng *et al.* [191] discussed the known-plaintext attacks in AN precoding methods, where Eve

TABLE V
SUB-OPTIMAL TRANSMIT COVARIANCE MATRICES UNDER DIFFERENT MIMO CHANNEL CONDITIONS

Channel condition	Corresponding CSI	Sub-optimal $\mathbf{Q}$
The main channel dominates the wiretap channel in all sub-channels	$\mathbf{H}_b^T\mathbf{H}_b \succ \mathbf{H}_e^T\mathbf{H}_e$	Full rank
The main channel is the worst in all sub-channels	$\mathbf{H}_b^T\mathbf{H}_b \prec \mathbf{H}_e^T\mathbf{H}_e$	$C_s(\mathbf{Q}) = 0$
Some sub-channels of the main channel are worse than wiretap channel	Eig$(\mathbf{H}_b^T\mathbf{H}_b - \mathbf{H}_e^T\mathbf{H}_e) = m$	Rank$(\mathbf{Q}) \le m$

* Eig(.) is to calculate the number of positive eigenvalues of a matrix

can calculate its corresponding decoded matrix from training the CSI value by least mean square (LMS) and normalized least mean square (NLMS) algorithms, and used the CSI to eliminate AN signals. Note that the known-plaintext attacks require adequate degrees of freedom at Eve, i.e., Eve has more antennas than Alice. In order to enhance security, most of the PHY-security schemes assumes that transmitters have more antennas than Eve.

4) CVX-Based Precoding: The optimization problem can be reformulated and solved easily when the main channel dominates the wiretap channel, at least in some sub-channels. The secrecy capacity is zero if none of users' sub-channels are better than the wiretap channel. There is still no direct optimal secrecy capacity expressions available for MIMO wiretap channels with CVX-based methods. However, when the channel satisfies the condition that intended receivers' channels are more capable than those of eavesdroppers, even in SIMO [21], [22] scenarios, the optimization problem is solvable and the secrecy capacity is achievable.

Next, we discuss the mathematical property of a sub-optimal transmit covariance first, which is required in the optimization of each sub-channel [59]. For a given power constraint, Table V shows the sub-optimal transmit covariance solutions under different main and wiretap channel conditions. $\mathbf{H}_b^T\mathbf{H}_b \succ \mathbf{H}_e^T\mathbf{H}_e$ means that the main channel dominates the wiretap channel in all sub-channels. In this case, Alice uses all sub-channels such that transmit precoding matrix $\mathbf{V}$ is a full rank matrix, and optimizes a transmit precoding vector $\mathbf{v}$ at each sub-channel by CVX tool independently, where $\mathbf{v}$ is a column vector of $\mathbf{V}$. Then, Alice transmits a message $\mathbf{s}$ by precoding $\mathbf{Vs}$. Hence, the optimization problem can be convex and the transmit covariance $\mathbf{Q}$ of the vector $\mathbf{Vs}$ is a full rank matrix. If $\mathbf{H}_b^T\mathbf{H}_b - \mathbf{H}_e^T\mathbf{H}_e$ is not positive definite, the optimal transmit covariance solution $\mathbf{Q}$ is not a full rank matrix, meaning that there are some sub-channels of the main channel are worse than the wiretap channel. In this case, there exist some algorithms to find an equivalent channel $(\mathbf{H}_b', \mathbf{H}_e')$ and a full rank matrix $\mathbf{Q}'$ to achieve the same secrecy capacity as the original channel model.

The same process continues to find optimal algorithms for solving maximized secrecy rate under the average total power constraint. Reference [29] showed a special case of $r = 2$, $t = 2$, and $e = 1$ using this approach. References [57] and [60] developed a novel iterative algorithm to achieve Lagrangian multipliers results with a secrecy rate constraint. The dual problem was solved iteratively by updating the Lagrangian variable using the sub-gradient method, as illustrated in Fig. 13, where the initialization of $\mathbf{Q}$ is an all-zero element matrix, or is a water-filling solution of $\mathbf{Q}_{WF}$. λ is the Lagrangian multiplier.

```
1) Initialize: $\lambda$ and $\mathbf{Q} = \mathbf{0}$ or $\mathbf{Q} = \mathbf{Q}_{WF}$.
2) Repeat
3)    Repeat
          a) Solve the SCM problem with $\mathbf{Q}$ and $\lambda$.
                Obtain the optimal transmit covariance matrix $\mathbf{Q}^*$.
          b) Update $\lambda$ based on the subgardient method.
4)    Until the required accuracy
5)    Update $\mathbf{Q} \leftarrow \mathbf{Q}^*$
6) Until the required accuracy
```

Fig. 13. The universal Lagrangian variable update algorithm for solving an optimal transmit covariance matrix.

C. Optimization Objective Solutions

Since the objective function of a SCM problem is the difference between two concave functions, the maximization problem is a non-convex problem and hard to solve. Instead of directly investigating on the ways to maximize the secrecy capacity, the objective functions are measured by quality of service (QoS), such as SNR [27], [46], mean-squared error (MSE) [38], [45], [173], and signal-to-interference-plus-noise ratio (SINR) [47], [53]. Based on these metrics, the power allocation used by Alice ensures the signal quality of desired receivers above a given level (rather than a perfect secrecy capacity), and further impairs the performance of Eve by setting a threshold on its signal quality level.

Compared to SCM problems, these signal quality maximization (SQM) problems do not guarantee perfect information-theoretic security, but the investigation in [48] proved that it can achieve a secrecy transmission, and can be easily implemented in practical systems. The approaches based on SQM problems can be generally summarized as

$$\begin{aligned} \text{SQM}: \ & \max_{Q} \ \{\text{SNR or MSE or SINR}\}_b \\ & \text{s.t.} \ \{\text{SNR or MSE or SINR}\}_e, \quad C_s, P_a, \end{aligned} \tag{11}$$

where $\{\text{SNR or MSE or SINR}\}_b$ and $\{\text{SNR or SINR or MSE}\}_e$ specify the target signal quality levels for Bob and Eve, respectively. C_s is a target secrecy capacity. P_a is a transmit power constraint. Based on SQM problems, [57] designed transmit and receive filters to guarantee C_s by allocating a fraction of available transmit power to minimize the difference between the secrecy capacities of the input vector and the true input vector, while guaranteeing that Eve's SINR level is kept below a given value, subject to a total power constraint P_a.

In addition, signal processing is used to combine wiretap coding with AN precoding to enlarge signal quality difference between Bob and Eve. In particular, without Eve's CSI, to guarantee a higher signal quality at Bob, a promising approach is to use a part of power resources to transmit AN signals in null spaces of the main channels, but these signals will jam Eve. Searching for null spaces of the main channels requires Bob's CSI only, and the SQM metric or average secrecy capacities can be measured by Bob's CSI and Eve's statistical CSI. The AN-MSE approach [45] and AN-SINR approach [47] were proposed for MIMO scenarios. Reference [192] derived the optimal solutions of AN-SNR by SDP relaxation in the presence of a full duplex base station. These approaches based on AN-SQM problems can be summarized as

$$\begin{aligned}\text{AN-SQM}: \max_{\mathbf{Q}_s,\mathbf{Q}_n}\ & \{\text{SNR or SINR or MSE}\}_b,\\ \text{s.t.}\ & \{\text{SNR or SINR or MSE}\}_e,\\ & C_s(\mathbf{Q}_s,\mathbf{Q}_n),\\ & \text{Tr}(\mathbf{Q}_s+\mathbf{Q}_n)\le P_a, \end{aligned} \tag{12}$$

where $\mathbf{Q}_s$ is allocated for transmitting information, while $\mathbf{Q}_n$ is allocated for transmitting AN symbols. From Eve's perspective, all "undecodable" signals may serve as jamming signals, including one half of simultaneous signals in full duplex channels [192]. Some eavesdroppers may cooperate jointly to receive signals to improve their interception probability for secrecy messages. The worst case is that all eavesdroppers are colluding. Reference [47] considered this case and provided a joint SINR using all eavesdroppers' SINRs as QoS constraints.

1) ZF Precoding With SQM: ZF schemes are near optimal based on the SQM metric and easy to implement. In [38], Alice's ZF precoding optimizes a beamforming design to minimize MSE between itself and the intended receiver, while assuring that MSE of an eavesdropper remains to be above a given threshold to achieve a target secrecy capacity. Reference [56] used SINR as an alternative objective to derive transmit precoding.

2) AN Precoding With SQM: The core of AN precoding is to find an optimal power allocation scheme. The allocation strategies used in [47], [52], and [53] work based on a SINR metric. In [52], a transmitter allocates a minimum possible fraction ρ of the available transmit power P to achieve a desired SINR between the transmitter and the intended receiver, and allocates all of transmitter's remaining power to send artificial interference signals that are uniformly distributed in space. The scheme can work under the condition that the instantaneous CSI of Eve is unknown. Here, $\rho = \sigma_b^2 S/\lambda P$, where λ is the largest singular value of $\mathbf{H}_b$, σ_b^2 is the noise power in the main channel, S is the target SINR given by the intended receiver, and P is the transmit power. Similarly, the other allocation strategies based on MSE metric were proposed in [45].

3) CVX-Based Precoding With SQM: Reference [39] provided an alternative precoding design based on QoS metrics. The scheme includes an optimal regularization parameter and an power allocation scheme, both of which also achieve a tradeoff between maximizing SINR_b and minimizing SINR_e. Reference [60] used a more universal approach to minimize the transmission power to achieve a predefined secrecy rate. These optimization problems were converted to two equivalence Lagrangian dual problems, in which the Lagrangian multipliers representing the secrecy rate or signal quality constraints are solved.

VI. Secure Relay Communications

There are two issues about secure relay communications, namely trusted relay and untrusted relay issues.

A. Trusted Relay

This sub-section will introduce the challenges of the distance problems of a trusted relay, and the corresponding cooperation strategies to the problems, followed by the compound channels, two-way channel, MIMO precoding, and cooperative jamming precoding of a trusted relay.

1) Secrecy Capacity of Trusted Relay in DF, AF, CF, and NF: The secrecy capacity can be kept nonzero with trusted relay nodes. Relay nodes can also be used for increasing the secrecy capacity of a system when a transmitter has a "nonzero" but "limited" secrecy capacity. References [62] and [63] studied the secrecy capacities for DF, AF, and NF schemes in terms of distance optimization. Reference [62] showed that when the distance between Alice and Bob is equal to that between Alice and Eve, the secrecy capacity is zero without relay. On the contrary, it can achieve a positive secrecy rate with a relay. In addition, the results in [62] show that, 1) when the relay is near to Alice, a DF scheme can achieve the highest secrecy capacity. With the distance between the relay and Alice increases, the secrecy rate is approaching to zero, while NF and AF still achieve a higher secrecy rate; 2) when the relay moves away from Alice, the secrecy rate increases first for all schemes, because the channel gain between the relay and Bob increases. However, the secrecy rate then deceases, because received signal power at the relay decreases. In conclusion, there exists an optimal relay location somewhere between Alice and Bob during the construction of a specific relay network. Reference [67] proposed an achievable secrecy region that uses a Cover and El Gamal's CF scheme [193] for relay broadcast channels.

These relay-aided schemes also require some extra time slots to ensure that both Alice and Bob can obtain CSIs. Certainly, the Eve's CSI is usually absent. Reference [79] showed that each relay only needs to know its own channel to the destination if AF is designed to lie in the null space of the relay's channel to the destination. In addition, [80] derived the worst-case secrecy capacity using a statistical fading channel model.

2) Compound Trust Relay Wiretap Channels: The basic secrecy capacity for the compound relay wiretap channels was identified in [81], in which each of the transmitter to relay, transmitter-to-destination, transmitter-to-eavesdropper, relay-to-destination, and relay-to-eavesdropper links is composed of several parallel channels as sub-channels.

However, whether we still need to use the relay when there is already a direct link between the source and destination is still a question in the presence of randomly distributed relays and eavesdroppers, especially when they can collude with each other. References [82] and [83] showed that whether or not to employ a relay wiretap channel for security purposes depends on the relay density and the distances between the transmitter and the receivers. The distance problem has been solved as we have discussed in the simplified relay wiretap channel model before. Reference [66] investigated mainly the upper bound of the number of eavesdroppers, and found that the number of eavesdroppers should satisfy the condition that it is sub-linear to the number of relay nodes if we want to achieve positive secrecy capacities. Reference [69] extended the investigation to multi-receivers scenarios in order to mitigate the interferences of parallel relay wiretap channels.

3) Two-Way Trusted Relay Wiretap Channels: Two-way relays have a potential to significantly improve the overall performance and coverage in wireless networks. In [64] and [65], the communication processes in the scenarios include two phases. In the initial phase, two transmitters (nodes 1 and 2) send their messages to the relay, and then the relay decodes them. In the succeeding broadcast phase, the relay has successfully decoded both private messages m_1 and m_2 in nodes 1 and 2. In addition to m_1 and m_2, the relay generates a common message m_0 for both nodes and a confidential message m_c for node 1, which should be kept secret from node 2. The nodes can not transmit and receive simultaneously because the scenario adopts a time-division duplex (TDD) mode. The different property from the classical broadcast scenario is that, the communication proceeds in two phases and the receiving nodes can use their own messages obtained from the previous phase for decoding the data in the second phase.

4) Trusted Relay With MIMO Precoding: The relay MIMO precoding technologies utilize MIMO and relay jointly, which aim to design the weight coefficients and allocate proper transmission power to enhance the security of wireless networks. The first priority of MIMO precoding technologies for relay wiretap channels is to maximize the secrecy capacity by designing a transmit covariance solution. References [61] and [87] used a SDP relaxation method to transform it to a sub-optimal solvable problem, and adopted a sub-optimal criteria of the precoding scheme named as null space beamforming (similar to ZF precoding). In these schemes, if relays choose a beamforming vector aiming to the null space of Eve's equivalent channel vectors, the information leakage will be less likely so that Eve gets nothing about messages. Reference [87] proposed an optimal power allocation via iterative algorithms such as Vickrey auction and sequential first-price auction games. As an alternative scheme, [88] used space-division multiplexing to allocate the maximal allowable power.

However, in many applications, it may be not practical to acquire Eve's CSI. The AN precoding is adopted to minimize the power allocated to information transmissions at relays. AN precoding technologies can be used in another scheme as shown in [70]. AN precoding is adopted with relay selection schemes, to improve the channel quality of the legitimate receiver but have no impact on Eve's mutual information.

The MIMO precoding in two-way relay wiretap channels was first proposed in [89], whose scenario includes two terminals that expect to exchange information in the presence of an eavesdropper. Reference [90] summarized three general approaches to find an optimal null space beamforming and transmit power for secure communications in two-way MIMO relay networks, namely total transmit power minimization (TTPM), secrecy sum rate maximization (SSRM), and minimum per-user secrecy rate maximization (MPSRM), respectively.

5) Trusted Relay With Cooperative Jamming: Different from AN precoding or NF schemes we talked about before, the AN signals in a cooperative jamming scheme, which was first proposed in [70], were generated not only by relays, but also by cooperative transmitters and receivers. By carefully designing the precoding matrices, the interferences from different transmitters can be aligned within the same subspace at the destination. These interferences at Eve will not be coherently aligned due to the randomness of wireless channels.

Moreover, opportunistic relay selection can enhance the cooperative jamming with an increasing number of relays. To take full advantage of multiple relays, [84], [85] proposed a joint relay and jammer selection scheme to select two or three intermediate nodes to enhance security against Eve. The first selected relay operates in a conventional relay wiretap channel and assists Alice to deliver their messages to the corresponding destinations using an AF protocol or a DF protocol. The other relays are used in different communication phases as jammers to create intentional interferences to Eve. Reference [86] extended cooperative jamming strategies to the scenarios where multiple relays are assigned to multiple source-destination pairs. The smart jamming algorithm was proposed therein, where any relay that is not assigned to any pairs can be selected to act as a friendly cooperative jammer.

B. Untrusted Relay

This sub-section will introduce the challenges in power optimization of a untrusted relay, followed by the compound channels, two-way channels, MIMO precoding, and cooperative jamming precoding of a untrusted relay.

1) Secrecy Capacity of Untrusted Relay in CF, AF, and CTF: In untrusted relay channels, it is assumed that there exists an alternative link for secrecy transmissions, i.e., the transmitter-relay-receiver link, except for the direct link between the transmitters and intended receivers. The relay is regarded as an eavesdropper. Reference [91] first investigated the relay channel in the situation that some of transmitted messages are confidential to the relay, and security of such confidential messages was measured by conditional entropy. The core question of untrusted relay wiretap channels is whether an untrusted relay should still participate in the cooperative communication networks, or whether the cooperation with the untrusted relay can bring in any benefit to us.

TABLE VI
STRATEGIES IN ONE-WAY MIMO RELAY CHANNELS

Transmit power condition		Antenna condition		Alice's optimal strategy
Relay power	Alice power	Relay antenna	Alice antenna	
0	N/A	N/A	N/A	Use direct communication between Alice and Bob
Infinity	0	N/A	N/A	Use relay-aided communication
Infinity	Infinity	Larger	Smaller	Use relay-aided communication
Infinity	Infinity	Smaller	Larger	Use direct communication between Alice and Bob

TABLE VII
STRATEGIES IN TWO-WAY MIMO RELAY CHANNELS

Transmit power condition		Antenna condition			Alice's optimal strategy
Relay power	Alice power	Relay antenna	Alice antenna	Bob antenna	
0	N/A	N/A	N/A	N/A	Use direct communication between Alice and Bob
Infinity	0	N/A	N/A	N/A	Use direct communication between Alice and Bob
Infinity	Infinity	$t_A \leq t_R$	$t_B \leq t_R$	$t_R < t_A + t_B$	Use relay-aided communication
Infinity	Infinity	$t_A > t_R$	$t_B > t_R$	N/A	Use direct communication between Alice and Bob
$P_R/P_S \to$ Infinity	Infinity	$t_A \leq t_R$	$t_B \leq t_R$	$t_R < t_A + t_B$	Use relay-aided communication.

The works in [93] and [94] showed a higher secrecy capacity using CF and AF strategies.[5] The results in [93] showed that, for CF strategies, when the channel gain from the Alice to relay is large enough, it is not required to transmit messages at a maximum power, because increasing power will yield a positive effect to the untrusted relay's capacity if compared to the benefit brought in by the secrecy capacity. On the contrary, as the gain from relay to Bob channel increases, we observe that the upper bounds of theoretical and simulation results become tight.

Apart from these traditional cooperative strategies, [95], [98] developed a novel compute-and-forward (CTF) strategy by decoding linear combinations of incoming symbols at a relay instead of decoding them individually. CTF works well based on lattice codes [194], which have been shown to achieve the secrecy capacity instead of using traditional wiretap codes. Reference [98] extended the CTF strategy to multi-path relay channels with half-duplex nodes in SIMO, SISO, and MISO scenarios.

2) Compound Untrusted Relay Wiretap Channels: In a system with multiple relays, [99] proposed a relay selection scheme using the extreme-value theory of the secrecy capacity in different proposed scenarios. The investigation pointed out that, a relay, no matter whether it is chosen as a helper or not, acts as an eavesdropper because of the broadcast nature of the wireless medium. Hence, it revealed that when the relays are untrustworthy, The performance of communication systems is worse off when the number of relays increases.

3) Two-Way Untrusted Relay Wiretap Channels: References [65] and [68] investigated PHY-security issues in a two-way untrusted relay network. Two terminals (nodes 1 and 2) exchange information through an untrusted relay, as there is no direct communication link between them. Reference [68] found that the two-way channel can be decomposed into two parallel channels, and the relay needs to perform double-user decoding, while each terminal only needs to decode a single user message. To maximize the secrecy capacity of the two-way relay channel, the best way is to force the untrusted relay to use multi-user decoding. Reference [102] utilized untrusted AF relays to establish a communication link, where there is no direct link between the end users. In this investigation, an one-way relay network with AF strategies in general achieves a higher secrecy capacity than two-way model. However, when facing the problem of the unbalanced transmit power between two terminals, i.e., one node's transmit power is much lower than the other, two-way relaying with AF strategies become the best choice.

4) Untrusted Relay With MIMO Precoding: Reference [96] utilized MIMO precoding technologies in a scenario where exists a transmitter, a untrusted relay, and an intended receiver with an analogous AF strategy. In order to improve the secrecy capacity substantially, the transmitter sends messages by a covariance matrix $\mathbf{Q}_S$, and the relay sends messages by a covariance matrix $\mathbf{Q}_R$. These two covariance matrices must be designed jointly to maximize the secrecy capacity. It is very difficult to find the optimal solution because the optimization problem is also in general nonconvex. However, if one of these two covariance matrices is fixed, the problem that optimizes the other one becomes solvable by CVX tools. Although optimized transmit covariance matrices can be built up by CVX methods, it is hard to see clearly that a untrusted relay-aided communication scheme is better than direct communications without relays. Table VI provides an alternative scheme that includes the relay-aided communications and the direct communications, depending on the number of antennas and the transmit power of the transmitter and the relay. Reference [97] extended this two-way relay model to MIMO scenarios, and proposed secure precoding

[5] DF strategies can not be used when a relay is untrusted, since the DF strategies work well only if the signals received from a source are fully decoded at a relay.

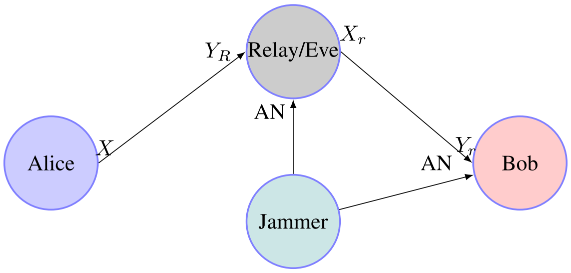


Fig. 14. A secure untrusted relay channel with a cooperative jammer, where there is no direct channel between Alice and Bob, so that Alice transmits the message X to Bob only through a relay. Meanwhile, a jammer (usually close to the destination) transmits AN to the relay to confuse it. The received signal by the relay is $Y_R = H_aX + N_e + AN$, which is relayed by X_r. Bob receives the jamming signal $Y_r = H_bX_r + N_r + AN$ over a noisy channel and then removes the AN signal.

for MIMO two-way untrusted relays. This is the same problem as one-way model, for which Table VII also provides an alternative scheme that includes the relay-aided communications and direct communications. Here, P_R and P_S denote the transmit power of the relay and total terminals (the total power of Alice and Bob), respectively. t_R, t_A, and t_B denote the numbers of antennas at the relay, Alice, and Bob, respectively.

5) Untrusted Relay With Cooperative Jamming: For untrusted relays, [103] proposed a scheme with the aid of an intended receiver or an external node that jams the relay, by which a positive secrecy capacity is achievable. The scheme is illustrated in Fig. 14. Reference [103] derived an upper bound for the secrecy capacity for this cooperative jammer scheme. Reference [99] extended the closed-form expression for the lower bound of the ergodic secrecy capacity to evaluate the performance of a secure communication system in fading environments.

Note that Bob has perfect knowledge of the jamming signal *AN* and perfect CSIs, but Eve does not have those information. So, only Bob can decode received signal Y_r. In particular, cooperative jammers are often co-located with Bob so that Bob can dispel AN signals easily. Reference [68] performed the investigation on friendly jammers in two-way untrusted relay communications. Reference [104] proposed a Stackelberg game between the terminals and friendly jammers as an optimal power control scheme. In the scheme, the secrecy capacity was defined as $(C_s^1 + C_s^2 - M)$, where C_s^1 and C_s^2 represent the capacities of the transmitter and the intended receiver, respectively. M is an extra source as the cost to pay for the friendly jammers. Hence, the secrecy capacity can be represented by the capacities of two parallel channels, minus the capacity which needs to be forfeited by the jammers. The problem becomes how to optimize equilibrium between the equivocation and the forfeited capacity. For multiple jammers and multiple source-destination nodes to combat a single eavesdropper, [105] proposed a distributed match algorithm to select a particular jammer for each source-destination pair.

VII. PHY-Key Generation

This section discusses the existing solutions to tackle the challenges of PHY-key generation. We will introduce the latest proposed PHY-key generation schemes, including CSI-based, RSS-based, phase-based, and wiretap code-based PHY-key generation technologies.

A. CSI-Based Key Generation

In CSI-based PHY-key generation, keys are generated from CSIs between Alice and Bob in TDD modes, where the CSIs are obtained by classic channel estimation methods [195], [196]. In general, CSI-based key generation process can be divided into three steps. In the first step, Alice sends a pilot signal to Bob over a wireless channel. Similarly, Bob transmits a pilot signal to Alice over the same wireless channel. In the second step, Alice and Bob estimate CSIs h_{ab} and h_{ba}, respectively. At last, Alice and Bob agree on a secret key by quantization, reconciliation, and privacy amplification subprocesses. To improve key generation rates, [109] proposed a scheme that exploited the frequency diversity based on OFDM technologies in wireless multipath fading channels, which can extract key bits separately from the real and the imaginary parts of each channel coefficient. This scheme uses LDPC codes to complete both reconciliation and privacy amplification sub-processes. Moreover, an excellent LDPC structure was proposed in [112] through density evolution for a multi-edge-type description. Reference [107] extended this scheme into MIMO networks, and focused on power allocation methods via maximizing a key rate objective function $I(h_{ab}; h_{ba})$. The result showed that the power allocation scheme increases a 15%-30% key generation rate compared to equal power allocation schemes at a low power region. Reference [119] extended the CSI-based key generation scheme to a two-way trusted relay scenario, which presented four secret key agreement schemes, including 1) a conventional AF two-way relaying method; 2) a signal-combining AF method, where the relay transmits combined signals of the received signals from Alice and Bob, and then Alice and Bob extract CSIs from their received signals; 3) a multi-access AF method that utilizes inherently combined signals provided by simultaneous transmissions over a multiple-access channel, and an AN-AF method that the relay transmits AN to confuse Eve.

CSI-based key generation schemes rely heavily on channel estimation. Eve can catch up with the channel estimation for Alice and Bob, and waits for injection opportunities when it detects a similar CSI between Alice and Bob. Existing countermeasures are usually passively defensive. For example, [106] used a two-way estimation process in key generation schemes. The two-way estimation scheme is especially beneficial in fast-fading environments because Alice and Bob can accurately estimate CSIs with the assistance of the two-way pilot signals, while Eve's estimation ability is reduced over a shorter coherent time, because Eve has a low probability of obtaining all pilot signals of the two-way transmission. Reference [108] used an active defensive approach and integrated user-generated randomness into pilot signals, so that the key is a combination of user-generated randomness and channel randomness. In this case, even if the pilot signals are destroyed by Eve, it can not obtain the CSI because received signals consist of user-generated random signals.

Reference [111] proposed a group key generation method for an arbitrary number of legitimate nodes in the presence of a passive eavesdropper. In detail, after pilot signal transmission at all legitimate nodes, each node broadcasts a weighted combination of its received signals with optimized coefficients, so that the legitimate nodes can obtain the CSIs of their channels used for key generation, while an eavesdropper cannot.

B. RSS-Based and Phase-Based Key Generation

1) RSS-Based: Reference [114] introduced a general framework of the key generation schemes based on RSS and phase information. In the RSS-based scheme, Alice transmits a known signal to Bob. Upon receiving the signal, Bob measures and records its RSS values. In the same channel coherent time, Bob transmits the same known signal to Alice. Alice measures and records its RSS values as well. Then, both Alice and Bob convert their RSS measurements into bits using a quantizer. The quantizer sets up the thresholds $(q+\sigma)+$ and $(q+\sigma)-$, where σ is a standard deviation of the RSS sequences. The scheme quantizes successive RSS points above $(q+\sigma)+$ and below $(q+\sigma)-$ to 1 and 0, respectively. Finally, Alice and Bob reconcile the bit discrepancies between their generated keys by message authentication codes (MAC) [197]. MAC is usually used for message integrity verification in the past, and now it can be viewed as new reconciliation codes, where Bob compares MACs from Alice with the corresponding bits to correct erroneous bits.

The secret bits based on RSS are easy to flip over with a small fluctuation of channel characteristics. In order to solve this problem, [113] used beamforming technologies to fluctuate the channel characteristics artificially, which reduce unpredictable fluctuations. The scheme uses parity check matrices to correct erroneous bits in their keys. Nowadays, this scheme has been extended to underwater environments [116].

2) Phase-Based: Phase-based key generation has a lot of advantages compared to RSS-based key generation schemes. First, RSS values usually undergo great changes in high speed mobile wireless systems due to Doppler spread, but the changes of phase values are predictable. For instance, when a node moves across a $1/4$ wavelength, the deviation of phase values is $\pi/2$. Second, with the development of high phase resolution devices, higher key generation rates are achievable because multiple secret bits can be extracted from a received signal. For example, in a quadrature phase shift keying (QPSK) system, each phase of a received signal represents four secret bits. However, [114] pointed out that key generation rates are still unsatisfactory because the keys should be updated continuously to resist against brute force attacks. To enhancing key generation rates, [115] proposed a scheme with a MIMO-OFDM transmission system to increase phase information. The scheme requires a set of pre-shared but public phase randomizing sequences, and uses a maximum likelihood (ML) algorithm to compare the Euclidean distance of each symbol's phase with the pre-shared phase information in each subcarrier. Note that the key reconciliation and privacy amplification techniques used in RSS-based methods are all applicable to phase-based methods.

C. Wiretap Code-Based PHY-Key Generation

A positive secrecy capacity of wiretap coding can not be guaranteed when the main channels are bad. In order to keep a stable secrecy channel, [117], [118] used a channel coding scheme proposed in [176] to generate private key bits. These bits are used to generate private keys that are shared opportunistically between the legitimate nodes when the main channel is better than the wiretap channel. Then, these keys are used later to encrypt delay sensitive messages. In particular, [118] focused on the scenarios where only Bob's CSI is known at Alice. The proposed channel code-based PHY-key generation can be generally outlined as follows:

- Secrecy transmission: Alice calculates an average secrecy capacity for a given scenario, and opportunistically exploits the fluctuations of channels to transmit secure data.
- Reconciliation and privacy amplification: Alice and Bob generate secret keys from synchronized random values, and store them in the form of secret keys.
- Secure communication: Alice and Bob finally use their secret key to transmit messages, where the secret key is seen as a one-time key or a random seed of session key generators.

Reference [120] extended wiretap code-based key generation to correlated MIMO channels with a Kronecker model. However, we must point out that they assumed the eavesdropper has no access to the correlated matrices of the channel model, so that the key generation rate looks higher than other schemes. Reference [121] proposed an approach based on polar codes that deal with reconciliation and privacy amplification jointly. The model consists of degraded binary memoryless source, broadcast channel, and a Markov tree model with uniform marginals. This scheme gives higher key generation rates but has a defect because it must be built up on pre-shared secret messages.

VIII. Physical Layer Authentication

This section describes the technical solutions to implement PHY-authentication. We will introduce the latest proposed PHY-authentication schemes, such as CSI-based authentication, RF recognition, and wiretap code-based authentication in the sequel.

A. CSI-Based Authentication

The main challenges in PHY-authentication include CSI impersonation attacks and channel estimation errors. Embedded watermarking codes and encrypted CSI schemes are proposed to solve impersonation attacks. Robust hypothesis testing technologies can be used to effectively mitigate channel estimation errors, but do not help to resist against CSI impersonation attacks.

1) Embedded Watermarking Codes: Embedded watermarking code technologies use pilot signals to find CSIs, where

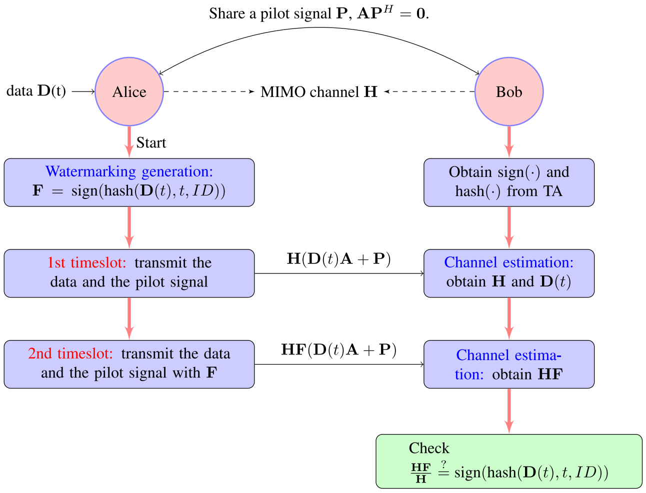

Share a pilot signal $\mathbf{P}$, $\mathbf{AP}^H = \mathbf{0}$.
data $\mathbf{D}$(t)
Alice
MIMO channel $\mathbf{H}$
Bob
Start
Watermarking generation: $\mathbf{F}$ = sign(hash($\mathbf{D}(t), t, ID$))
Obtain sign(·) and hash(·) from TA
1st timeslot: transmit the data and the pilot signal
$\mathbf{H}(\mathbf{D}(t)\mathbf{A} + \mathbf{P})$
Channel estimation: obtain $\mathbf{H}$ and $\mathbf{D}(t)$
2nd timeslot: transmit the data and the pilot signal with $\mathbf{F}$
$\mathbf{HF}(\mathbf{D}(t)\mathbf{A} + \mathbf{P})$
Channel estimation: obtain $\mathbf{HF}$
Check
$\frac{\mathbf{HF}}{\mathbf{H}} \overset{?}{=}$ sign(hash($\mathbf{D}(t), t, ID$))

Fig. 15. An embedded watermarking scheme. Alice conceals the watermarking code $\mathbf{F}$ along with primary information $\mathbf{D}(t)$. Bob processes it using channel estimation to obtain $\mathbf{H}$ and $\mathbf{HF}$, and further recovers the data $\mathbf{D}(t)$. Then, Bob calculates $\mathbf{F}$ via signing $\mathbf{D}(t)$, timestamp t, and Alice's identity information ID to decide if the transmitter is Alice.

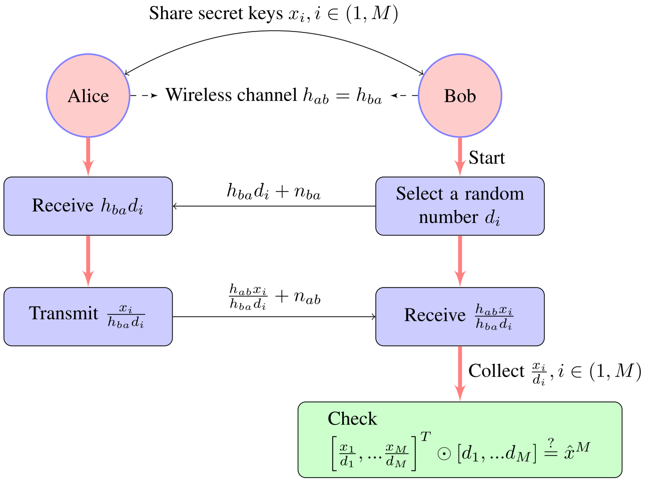

Share secret keys $x_i, i \in (1, M)$
Alice
Wireless channel $h_{ab} = h_{ba}$
Bob
Start
Select a random number d_i
$h_{ba}d_i + n_{ba}$
Receive $h_{ba}d_i$
Transmit $\frac{x_i}{h_{ba}d_i}$
$\frac{h_{ab}x_i}{h_{ba}d_i} + n_{ab}$
Receive $\frac{h_{ab}x_i}{h_{ba}d_i}$
Collect $\frac{x_i}{d_i}, i \in (1, M)$
Check
$\left[\frac{x_1}{d_1}, \dots \frac{x_M}{d_M}\right]^T \odot [d_1, \dots d_M] \overset{?}{=} \hat{x}^M$

Fig. 16. An encrypted CSI mechanism, where Alice and Bob share secret keys $x_i, i \in (1, M)$ in advance. Alice and Bob divide the channel into M subcarriers. Bob selects a random number d_i in a subcarrier and sends it to Alice. Alice receives $h_{ba}d_i$ and sends $x_i/(h_{ba}d_i)$ to Bob. Bob receives it and performs channel inverse operation to obtain x_i/d_i to check Alice's identity. Here, $\odot$ denotes element-wise multiplication.

pilot signals are generated with a watermarking code conveying the credentials of a data source. With the pilot signals, an authenticator (Bob) analyzes current watermarking codes in hearing messages in conjunction with received watermarking codes from a trusted authority (TA) [124], [125], inferring whether these watermarking codes are coherent. Reference [124] provided an approach to protect the pilot signals in MIMO channels, as shown in Fig. 15.

The embedded watermarking scheme is a combination of CSI estimation and cryptographic technologies [122], [137], where watermarking codes are generated by signing a transmitted message $\mathbf{D}(t)$, the transmitter's identity ID, and time information t. A pre-shared pilot signal $\mathbf{P}$ is used for a channel estimator to achieve the CSI at the first time slot, and mixes data with the CSI and watermarking codes at the second time slot. Alice eliminates watermarking codes from the mixed data after the second time slot, and determines if the watermarking codes are authenticated. By channel estimation, unaware receivers can still extract and estimate the CSI in received signals and further recover the original transmission data. In order to obtain $\mathbf{F}$ in the presence of noises, [124], [126] designed detection schemes based on amplitude differences or Hadamard products between even and odd time slots. Reference [130] designed pseudo random sequences whose fundamental idea is similar to watermarking, and used a Kronecker delta function to detect pseudo random sequences in time-varying channels. Watermarking codes keep the orthogonality between data and pilot signals in spaces. When the information signals and the pseudo random sequences are orthogonal to each other using Kasami codes, the impact on the receiver is negligible.

2) Encrypted CSI: Reference [131] provided a PHY-authentication mechanism, which utilizes the randomness, reciprocity, and location decorrelation features of a wireless fading channel to hide/encrypt CSI to resist against impersonation attacks. The detail of the scheme is illustrated in Fig. 16.

In this scheme, the shared secret key x_i and the random number d_i are exploited to "encrypt" the CSI. The scheme performs an inverse operation instead of sounding channel explicitly or reconciling the key disagreement. Reference [136] extended these schemes to two-hop communication links with a trusted relay. However, another case that we must consider is that a relay is an adversary, because all messages for authentication are relayed by the relay. Reference [136] enhanced the scheme using two shared keys to defend against inside attacks from an untrusted relay.

3) Robust Hypothesis Testing: Reference [134] proposed a hybrid authentication protocol to integrate hypothesis testing algorithms with the existing higher-layer security mechanism. In particular, Bob uses signature algorithms or message authentication codes to double-check the message. Reference [139] proposed a search algorithm in hypothesis testing based on a missed detection rate, which was formulated as a joint probability of Alice's CSI and Eve's CSI. The use of a quantization interval can minimize the variation between two adjacent quantized CSI data from the same transmitter, but still have a difference from disparate transmitters. Reference [140] investigated excessive noise in hypothesis testing algorithms, where an adaptive threshold was derived for hypothesis testing based on the statistical properties of the CSI variation and used for distinguishing the legitimate transmitter from intruders.

B. RF Recognition

RF recognition mechanism considered only RF emissions produced by unintentional emitters, such as environment-sensitive features, or environment-invariant features [132], [198], which is different from watermarking codes based on ingenious signals. The identities of transmitters are recognized passively based on discriminating

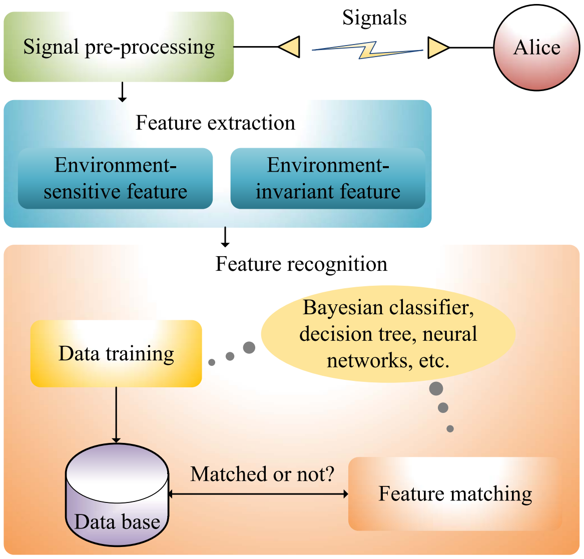


Fig. 17. A general RF recognition scheme based on machine learning, which consists of three components, i.e., signal preprocessing, feature extraction, and feature recognition. Feature recognition includes feature matching and data training, both of which use existing machine learning methods.

features extracted from their intrinsic physical properties. The core of RF recognition is to select a suitable classifier to train the extracted features by dimensionality reduction and probability density estimation techniques. Reference [132] used a Bayesian classifier to complete amplitude, phase, and frequency feature recognition. Reference [150] used a multi-discriminant classifier to perform both one-to-many device classifications and one-to-one device verification processes. Reference [151] used a support vector machine and a linear Fisher discriminant analysis to train the hypothesis test of amplitude or cyclic feature vectors of CSIs. Reference [198] used covariance-based distribution features of environmental noise and power spectrum density as internal similarity features, which can also be differentiated effectively by various classifiers. A system database module stores a training fingerprint of each enrolled device. As each device is associated with a particular digital identity, the records in the database are updated to reflect the pairing-up relationship between a device and its digital identity. The general RF recognition based on machine learning is showed in Fig. 17.

RF recognition has an advantage that it does not require any physical device modification because this technique exploits emissions generated by intrinsic device features. However, it requires high-speed digital sampling oscilloscopes, big databases, high complexity dimensionality reduction, and probability density estimation algorithms, which will increase the cost of the authentication systems.

C. Wiretap Code-Based Authentication

Reference [133] showed that PHY-authentication can be implemented by choosing proper wiretap channel codes $\mathcal{C}$. The elements of a randomly chosen subset of these codewords $\mathcal{A} \subset \mathcal{C}$ are marked as authentication-admissible codes. The subset is secret information shared between Alice and Bob. An encoder maps the source S^n to the nearest admissible codeword U^n and then generates the channel input X^n from U^n. The output of the channel is Y^n. A decoder maps the received signal Y^n to the nearest codeword $C^{'n} \in \mathcal{C}$. If $C^{'n} \in \mathcal{A}$, i.e., $C^{'n}$ is the authentication-admissible code, and the decoder produces reconstruction $\hat{S}^n$ from $C^{'n}$. If $C^{'n} \notin \mathcal{A}$, i.e., $C^{'n}$ is not the authentication-admissible code, and the decoder declares authentication failure. The set of authentication-admissible codewords should be dense enough to allow the encoder to find an X^n near to S^n to avoid a large distortion in the presence of noise. And the number of bits in admissible codewords must be appropriately large enough to avoid a force attack. From the investigation made in [133], an attacker may tamper the signal in order to make it an authentication-admissible code. The probability of the successful attacks is defined as

$$\Pr\left[C_t \subset \mathcal{A} | C_t \neq U^n\right] = \frac{|\mathcal{A}|}{C} = 2^{-n\gamma}, \tag{13}$$

where $\gamma = 1/\sqrt{n}$.

The above theory of channel codes for authentication has been explored in practical systems. For instance, spread spectrum coding [145] and code division multiple access (CDMA) techniques [149] have simple authentication capabilities due to the fact that the intercepters do not know the spreading codes and can not decode the information.

IX. Future Works and Challenges

As we mentioned earlier, one of our goals in this survey is to understand how PHY-security can be applied to various wireless scenarios based on the theories and technologies proposed in the literature. Specifically, we have illustrated wiretap code designs, secure multi-antenna and relay technologies, PHY-key generation technologies, and PHY-authentication technologies. We have also highlighted their challenges and possible solutions. In this section, our objective is to discuss some unique challenges in the future research directions in next generation wireless communications, where novel physical layer technologies and next generation networks may need to be developed.

A. Next Generation Physical Layer Technologies

1) Massive MIMO: Massive MIMO systems have an enormous number of antennas, which offer more degrees of freedom for wireless channels, and a better performance in terms of channel capacities or link reliability [199]. For security purposes, massive MIMO gives narrower beam patterns to Bob's direction so that the message leakage is reduced to unintended directions significantly. In addition, Alice has an adequate number of antennas in massive MIMO systems to generate AN signals to confuse eavesdroppers. As massive MIMO is brought into emerging wireless broadband standards in LTE, researchers begin to utilize massive MIMO to serve for PHY-security. Reference [200] derived an asymptotic secrecy capacities using ZF and AN precoding jointly in massive MIMO systems. Reference [201] analyzed uplink and downlink secrecy capacities in massive MIMO-aided cellular networks, which use ZF and MMSE-based precoding with AN generation. The secrecy outage metric of massive MIMO systems and massive MIMO relays were examined in [202] and [203], respectively. Compared to traditional MIMO systems, massive MIMO brings in more challenges. First, the CSI estimation process is a high complex procedure with the growth of the number of antennas in terminals. Second, channel models are very correlated as the distances of antennas are shorter than an half of the wavelength, so that theoretical secrecy capacity of a massive MIMO system should be re-defined with correlated antennas. Moreover, an application scenario where all communication terminals are equipped with massive antennas is still an open research topic. The secrecy capacity of this scenario is a critical metric for the massive MIMO to be used in PHY-security research.

2) mm-Wave: Currently, almost all wireless communications use spectrum in 300 MHz to 3 GHz band, which is extremely crowded. One of the key solutions of next generation wireless networks is to explore unused high frequency mm-wave band, ranging from 3∼300 GHz [204]. In addition, a short wavelength gives us the chance to use more antennas in a small space to obtain more degrees of freedom. In the mm-wave bands, [205], [206] designed a practice PHY-security scheme, where transmitted messages are beamformed to Bob in mm-wave communications. These schemes, like AN schemes, transmit scrambling constellation points in both amplitude and phase to undesired directions, which means that the transmitted AN signal is a complex random variable from information theory viewpoint. The PHY-security of mm-wave communications is a new research area, where the influence of multipath delay spread, small scale fading on security performance, and wiretap channel models should be characterized. In addition, mm-wave communications provide much uncertainty in signal penetration and propagation loss. This remains to be a problem to address for secure communications.

3) Small Cells: A large number of low-power small cells are deployed to increase system capacities and enhance the coverage of wireless communications, which are expected to be used in next generation wireless systems [207]. 3GPP standard R10 has proposed to deploy heterogeneous networks with various small stations, such as Femto and Pico cells. The small call base stations can be used to provide basic relay-aided secrecy capacities via secure relay technologies. However, an emerging challenge is radio resource management of these base stations because inter-cell interferences could be intolerable if we only consider security purposes. In order to increase the secrecy capacity per cell without affecting any other cell, power allocation and interference alignment with security considerations should be investigated in the heterogeneous networks. The density of small cell base stations [208] has especially become an important issue, where its parameter should be carefully designed to balance communication quality and secrecy.

4) Full Duplex: Full duplex communications provide double spectral efficiency by receiving and transmitting on the same frequency channel simultaneously. Full duplex base stations should consider both self-interference mitigation and PHY-security. References [192] and [209] worked on the design of transmit strategies and the derivation of secrecy capacity expressions of a full duplex base station based networks with traditional self-interference mitigation methods. There are two advantages when using full duplex base stations. First, Eve usually does not have the same self-interference mitigation capability, so that the messages heard at Eve are mixed with the messages from both users and base stations. Second, a full duplex base station can transmit AN signals to confuse eavesdroppers, and receive user information at the same time. The self-interference mitigation of a full duplex base station relies on space division and precoding technologies, such that hardware complexity of the system can be a great challenge.

5) Precoding and Detection Technologies: In PHY-security, precoding technologies are implemented at transmit devices while detection technologies are carried out at receive devices, both of which devote to enhance security performances. A great amount of existing schemes focus on precoding technologies with main CSIs. As the design of massive MIMO and mm-wave communications are integral to emerging next generation wireless networks, and directional beams also seem to be essential. The challenge of precoding technologies is relying on CSIs heavily. Massive links and mm-wave communications increase the difficulty in CSI estimation, thus inevitably bring confidential message leakage problems because of error CSIs. In addition, CVX-based precoding requires a lot of computing resources, and space-based precoding is a sub-optimal choice. How to trade-off complexity and secrecy performances by designing superior precoding schemes is ongoing. Alternatively, detection technologies work at receive terminals and do not require CSIs. Reference [210] first gave that a positive secrecy capacity without any CSI is existent when a coherence interval is large enough. However, efficient detection technologies considering detection and security performances is still an untapped area.

B. Next Generation Networks

1) Cognitive Radio Networks: Cognitive radio can solve the spectrum under-utilization problem by allowing secondary users to opportunistically access the licensed channels without causing interferences to communications of primary users. The characteristics of cognitive radio networks have created new challenges to security applications. For instance, malicious nodes may imitate the primary users, or may modify and interfere the cooperative spectrum sensing information. In order to resist against these attacks, the primary users should be authenticated and the sensing information should be protected. References [211] and [212] used cryptography schemes to protect the spectrum sensing messages and authenticate cognitive users. Recent investigations [213]–[215] presented a security mechanism at physical layer, which has less requirements on computing resources and can save a lot of spectrum resources with advanced physical layer technologies. However, the primary user's QoS constraints should be considered in security objectives to minimize the interferences to the primary user.

2) MTC: Machine type communication (MTC) can exchange and share data without any requirement on any form of human interventions. The MTC carries a lot of unique features, such as a massive number of devices, small and infrequent data transmissions, distinct service scenarios, and fewer opportunities for recharging devices, all of which bring in unprecedented challenges for the MTC, especially in its security issues. Recent developments, such as authentication and key managements [216] in body area networks, adopted PHY-authentication. References [217] and [218] showed several future directions to carry out the research in this area. The next step will focus on minimization of power consumption under the PHY-security constraints and the coexistence problems with various physical layer standards.

3) D2D Communications: The long term evolution-advanced (LTE-A) system supports device to device (D2D) communications, which is defined as the direct communications between two mobile users without traversing base stations or core networks. Without unifying the core networks, a confidential or authenticated transmission between mobile users becomes more difficult. References [219]–[221] showed future directions to carry out the research works in this topic. The core idea is to use D2D interference as an interference jammer to the illegitimate eavesdropper. An open issue is how to optimize radio resource allocation under the PHY-security constraint.

4) Mobile Networks: There are two main issues in PHY-security research in mobile networks. (1) In high speed mobile networks, such as vehicular ad hoc networks (VANETs) and high speed railway communication systems [222]–[224], the channel coefficients will change quickly. (2) The positions of two parties involved in the communications are always changing in mobile networks. In particular, mobility increases the difficulty in authentication of mobile nodes. In order to answer the question (1), fast CSI evaluation schemes in mobile networks need to be proposed, because CSI is the basic information needed for building up PHY-security communications. In order to address the issue (2), dynamic authentication frameworks need to be defined and employed, where channel discovery and resource allocation should be adapted to mobile networks working together with upper layer protocols.

X. Conclusion

PHY-security is a relatively new area in security research. With the advances in communication technologies, such as 5G wireless networks and MTC technologies, it is expected that all devices around us will be connected. These developments have created many new research topics in PHY-security, which is the focus of this survey paper.

This survey began with the security theories to achieve confidentiality and authentication at physical layer. Then, wiretap code designs, secure multi-antenna technologies, secure relay technologies, PHY-key generation technologies, and PHY-authentication technologies were discussed. We reviewed PHY-security research efforts to understand the major challenges associated with fading effects, partial/imperfect CSI, compound channels, MIMO transmit precoding, relay systems, PHY-key generation, and impersonation authentication attacks. Numerous solutions were suggested in the literature to tackle different challenges with the help of coding, precoding, signal processing, and channel estimation technologies, etc.

One of the major issues in PHY-security is the partial CSI problem. In proposed PHY-security schemes, transmitters need to know both Bob's and Eve's CSIs. However, in practice, the eavesdroppers can be silent and their CSIs are not available. This problem exists in wiretap coding designs, multi-antenna systems, relay systems, etc. In this survey paper, we defined the partial CSI problem in Section III first. Then, we identified corresponding solutions in Section IV, where statistical CSI methods were presented to measure secrecy capacities, and secrecy outage was used as an alternative metric. In secure multi-antenna systems, a commonly used solution to address partial CSI issues is to beamform messages to the main channel spaces. The spaces suitable for Bob do not give equally good gains for Eve. To enlarge the difference between the main channel and wiretap channel, Alice sends AN signals at null spaces of desired receivers, where the AN signals can confuse Eve with a high probability. Obviously, the beamforming and AN-aided methods only need Bob's CSI. For measuring secrecy capabilities, Alice can use SQM objectives of main channels to replace SCM objectives, or use average secrecy capacity metrics based on statistical Eve's CSI. The proposed methods to mitigate partial CSI issues in secure multi-antenna systems can also be applied to relay systems.

References

[1] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (blowfish)," in *Proc. Fast Softw. Encryption Cambridge Security Workshop*, Cambridge, U.K., Dec. 1993, pp. 191–204.

[2] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Indianapolis, IN, USA: Wiley, 1996.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[5] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[6] H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Trans. Inf. Theory*, vol. 35, no. 3, pp. 572–578, May 1989.

[7] H. Yamamoto, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 634–638, May 1991.

[8] M. V. Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 43, no. 2, pp. 712–714, Mar. 1997.

[9] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[10] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[11] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[12] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[13] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[14] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 1301–1305.

[15] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[16] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.

[17] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *Proc. Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2009, pp. 829–833.

[18] S.-C. Lin, "On ergodic secrecy capacity of fast fading MIMOME wiretap channel with statistical CSIT," in *Proc. Asia Pac. Conf. Signal Inf. Process. Assoc.*, Kaohsiung, Taiwan, Oct. 2013, pp. 1–4.

[19] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3652–3664, Oct. 2014.

[20] E. Güvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *Proc. IEEE ICC*, Sydney, NSW, Australia, Jun. 2014, pp. 813–818.

[21] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, SA, Australia, Sep. 2005, pp. 2152–2155.

[22] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[23] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2007, pp. 905–910.

[24] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2466–2470.

[25] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[26] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.

[27] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[28] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[29] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[30] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[31] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[32] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2471–2475.

[33] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[34] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 640–649, Sep. 2011.

[35] S. A. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, MA, USA, Jul. 2012, pp. 2321–2325.

[36] S. A. A. Fakoorian and A. L. Swindlehurst, "Dirty paper coding versus linear GSVD-based precoding in MIMO broadcast channel with confidential messages," in *Proc. IEEE GLOBECOM*, Houston, TX, USA, Dec. 2011, pp. 1–5.

[37] A. Wiesel, Y. C. Eldar, and S. Shamai, "Zero-forcing precoding and generalized inverses," *IEEE Trans. Signal Process.*, vol. 56, no. 9, pp. 4409–4418, Sep. 2008.

[38] H. Reboredo, J. Xavier, and M. R. D. Rodrigues, "Filter design with secrecy constraints: The MIMO Gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, Aug. 2013.

[39] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[40] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[41] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively securing wireless communications using zero-forcing beamforming," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 720–728.

[42] M. Schulz, A. Loch, and M. Hollick, "Practical known-plaintext attacks against physical layer security in wireless MIMO systems," in *Proc. Symp. NDSS*, San Diego, CA, USA, 2014, p. 13. [Online]. Available: http://www.internetsociety.org/doc/practical-known-plaintext-attacks-against-physical-layer-security-wireless-mimo-systems

[43] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. 62nd IEEE Conf. Veh. Tech.*, vol. 3. Dallas, TX, USA, Sep. 2005, pp. 1906–1910.

[44] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[45] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[46] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

[47] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[48] Q. Li *et al.*, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 1714–1727, Sep. 2013.

[49] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[50] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3901–3911, Jul. 2015.

[51] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.

[52] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[53] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[54] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

[55] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[56] K. Wang, X. Wang, and X. Zhang, "SLNR-based transmit beamforming for MIMO wiretap channel," *Wireless Pers. Commun.*, vol. 71, no. 1, pp. 109–121, 2013.

[57] A. Khabbazibasmenj, M. A. Girnyk, S. A. Vorobyov, M. Vehkaperae, and L. K. Rasmussen, "On the optimal precoding for MIMO Gaussian wire-tap channels," in *Proc. 10th Int. Symp. Wireless Commun. Syst.*, Ilmenau, Germany, Aug. 2013, pp. 1–4.

[58] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2673–2682, May 2013.

[59] S. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, May 2013.

[60] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[61] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[62] L. Lai and H. E. Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[63] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[64] R. F. Wyrembelski and H. Boche, "Physical layer integration of private, common, and confidential messages in bidirectional relay networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3170–3179, Sep. 2012.

[65] R. H. Y. Louie, Y. Li, and B. Vucetic, "Practical physical layer network coding for two-way relay channels: Performance analysis and comparison," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 764–777, Feb. 2010.

[66] D. Goeckel *et al.*, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.

[67] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

[68] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[69] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[70] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842–2848, Jul. 2012.

[71] T. Yang, I. Land, T. Huang, J. Yuan, and Z. Chen, "Distance spectrum and performance of channel-coded physical-layer network coding for binary-input Gaussian two-way relay channels," *IEEE Trans. Commun.*, vol. 60, no. 6, pp. 1499–1510, Jun. 2012.

[72] C.-L. Wang, T.-N. Cho, and K.-J. Yang, "A new cooperative transmission strategy for physical-layer security with multiple eavesdroppers," in *Proc. 75th IEEE Conf. Veh. Tech.*, Yokohama, Japan, May 2012, pp. 1–5.

[73] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[74] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.

[75] R. Bassily and S. Ulukus, "Deaf cooperation for secrecy with multiple antennas at the helper," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1855–1864, Dec. 2012.

[76] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.

[77] T. Huang, T. Yang, J. Yuan, and I. Land, "Design of irregular repeat-accumulate coded physical-layer network coding for Gaussian two-way relay channels," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 897–909, Mar. 2013.

[78] J. Huang and A. L. Swindlehurst, "Wireless physical layer security enhancement with buffer-aided relaying," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2013, pp. 1560–1564.

[79] S. Luo, J. Li, and A. Petropulu, "Physical layer security with uncoordinated helpers implementing cooperative jamming," in *Proc. 7th IEEE Sensor Array Multichannel Signal Process. Workshop*, Hoboken, NJ, USA, Jun. 2012, pp. 97–100.

[80] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.

[81] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 359–371, Apr. 2012.

[82] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 624–632, Apr. 2014.

[83] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[84] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[85] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[86] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, "Secrecy capacity optimization via cooperative relaying and jamming for WANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 1117–1128, Apr. 2015.

[87] T. Wang, L. Song, Z. Han, X. Cheng, and B. Jiao, "Power allocation using Vickrey auction and sequential first-price auction games for physical layer security in cognitive relay networks," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, ON, Canada, Jun. 2012, pp. 1683–1687.

[88] K. Guan, E. C. Song, E. Soljanin, P. J. Winzer, and A. M. Tulino, "Physical layer security in space-division multiplexed fiber optic communications," in *Proc. 46th IEEE Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2012, pp. 654–658.

[89] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[90] Y. Yang, C. Sun, H. Zhao, H. Long, and W. Wang, "Algorithms for secrecy guarantee with null space beamforming in two-way relay networks," *IEEE Trans. Signal Process.*, vol. 62, no. 8, pp. 2111–2126, Apr. 2014.

[91] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Cairns, QLD, Australia, 2001, pp. 87–89.

[92] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 926–930.

[93] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, Mar. 2009.

[94] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[95] X. He and A. Yener, "Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 177–192, Jan. 2013.

[96] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[97] J. Mo, M. Tao, Y. Liu, B. Xia, and X. Ma, "Secure beamforming for MIMO two-way transmission with an untrusted relay," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Shanghai, China, Apr. 2013, pp. 4180–4185.

[98] J. Richter, C. Scheunert, S. Engelmann, and E. A. Jorswieck, "Weak secrecy in the multiway untrusted relay channel with compute-and-forward," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1262–1273, Jun. 2015.

[99] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[100] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[101] Y. Zhang *et al.*, "Near-optimal joint antenna selection for amplify-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2401–2407, Aug. 2010.

[102] J. Huang and A. L. Swindlehurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2013, pp. 1555–1559.

[103] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE GLOBECOM*, New Orleans, LA, USA, Nov. 2008, pp. 1–5.

[104] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[105] S. Bayat, R. H. Y. Louie, Z. Han, B. Vucetic, and Y. Li, "Physical-layer security in distributed wireless networks using matching theory," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 5, pp. 717–732, May 2013.

[106] S. Im, J. Choi, and J. Ha, "Secret key agreement for massive MIMO systems with two-way training under pilot contamination attack," in *Proc. IEEE GLOBECOM*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[107] K. Chen, B. B. Natarajan, and S. Shattil, "Secret key generation rate with power allocation in relay-based LTE-A networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2424–2434, Nov. 2015.

[108] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[109] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[110] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[111] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Secret group key generation in physical layer for mesh topology," in *Proc. IEEE GLOBECOM*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[112] N. Islam, O. Graur, A. Filip, and W. Henkel, "LDPC code design aspects for physical-layer key reconciliation," in *Proc. IEEE GLOBECOM*, San Diego, CA, USA, Dec. 2015, pp. 1–7.

[113] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[114] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[115] H. Taha and E. Alsusa, "Physical layer secret key exchange using phase randomization in MIMO-OFDM," in *Proc. IEEE GLOBECOM*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[116] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: Advantages, challenges, and performance improvements," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 32–38, Feb. 2016.

[117] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[118] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," in *Proc. 46th Annu. Conf. Inf. Sci. Syst.*, Princeton, NJ, USA, Mar. 2012, pp. 1–6.

[119] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 650–660, Sep. 2011.

[120] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in *Proc. IEEE GLOBECOM*, Atlanta, GA, USA, Dec. 2013, pp. 1245–1250.

[121] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, Nov. 2015.

[122] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[123] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. IEEE Int. Conf. Commun.*, Glasgow, U.K., Jun. 2007, pp. 4646–4651.

[124] N. Goergen, W. S. Lin, K. J. R. Liu, and T. C. Clancy, "Extrinsic channel-like fingerprint embedding for authenticating MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 12, pp. 4270–4281, Dec. 2011.

[125] N. Goergen, T. C. Clancy, and T. R. Newman, "Physical layer authentication watermarks through synthetic channel emulation," in *Proc. IEEE Symp. New Front. Dyn. Spectr.*, Singapore, Apr. 2010, pp. 1–7.

[126] N. Goergen, W. S. Lin, K. J. Liu, and T. C. Clancy, "Authenticating MIMO transmissions using channel-like fingerprinting," in *Proc. IEEE GLOBECOM*, Miami, FL, USA, Dec. 2010, pp. 1–6.

[127] B. Danev, H. Luecken, S. Capkun, and K. E. Defrawy, "Attacks on physical-layer identification," in *Proc. ACM Conf. Inf. Wireless Netw. Security*, Hoboken, NJ, USA, 2010, pp. 89–98.

[128] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[129] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[130] X. Wang, Y. Wu, and B. Caron, "Transmitter identification using embedded pseudo random sequences," *IEEE Trans. Broadcast.*, vol. 50, no. 3, pp. 244–252, Sep. 2004.

[131] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, Sep. 2013.

[132] W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple, and Y. C. Kim, "Intrinsic physical-layer authentication of integrated circuits," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 14–24, Feb. 2012.

[133] E. Martinian, G. W. Wornell, and B. Chen, "Authentication with distortion criteria," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2523–2542, Jul. 2005.

[134] L. Xiao *et al.*, "PHY-authentication protocol for spoofing detection in wireless networks," in *Proc. IEEE GLOBECOM*, Miami, FL, USA, Dec. 2010, pp. 1–6.

[135] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.

[136] X. Du, D. Shan, K. Zeng, and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, Apr. 2014, pp. 1276–1284.

[137] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[138] S. Jain and J. S. Baras, "Preventing wormhole attacks using physical layer authentication," in *Proc. IEEE Conf. Wireless Commun. Netw.*, Shanghai, China, Apr. 2012, pp. 2712–2717.

[139] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE Int. Conf. Commun.*, Budapest, Hungary, Jun. 2013, pp. 4724–4728.

[140] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. Mil. Commun. Conf.*, Baltimore, MD, USA, Nov. 2011, pp. 538–542.

[141] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 74–77, Jan. 2015.

[142] P. L. Yu, J. S. Baras, and B. M. Sadler, "Power allocation tradeoffs in multicarrier authentication systems," in *Proc. IEEE Symp. Sarnoff*, Princeton, NJ, USA, Mar. 2009, pp. 1–5.

[143] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[144] R. M. Gerdes, M. Mina, S. F. Russell, and T. E. Daniels, "Physical-layer identification of wired Ethernet devices," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1339–1353, Aug. 2012.

[145] A. Martin, Y. Hasan, and R. M. Buehrer, "Physical layer security of hybrid spread spectrum systems," in *Proc. IEEE Symp. Radio Wireless*, Austin, TX, USA, Jan. 2013, pp. 370–372.

[146] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906–916, Feb. 2009.

[147] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948–5956, Dec. 2009.

[148] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: Analysis and design," *IEEE Trans. Signal Process.*, vol. 52, no. 9, pp. 2637–2649, Sep. 2004.

[149] T. Li, J. Ren, Q. Ling, and A. Jain, "Physical layer built-in security analysis and enhancement of CDMA systems," in *Proc. IEEE Mil. Commun. Conf.*, vol. 2. Atlantic City, NJ, USA, Oct. 2005, pp. 956–962.

[150] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1180–1192, Jun. 2015.

[151] C. Pei, N. Zhang, X. S. Shen, and J. W. Mark, "Channel-based physical layer authentication," in *Proc. IEEE GLOBECOM*, Austin, TX, USA, Dec. 2014, pp. 4114–4119.

[152] D. Gesbert, M. Shafi, D.-S. Shiu, P. J. Smith, and A. Naguib, "From theory to practice: An overview of MIMO space-time coded wireless systems," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 3, pp. 281–302, Apr. 2003.

[153] Y.-W. Hong, W.-J. Huang, F.-H. Chiu, and C.-C. J. Kuo, "Cooperative communications in resource-constrained wireless networks," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 47–57, May 2007.

[154] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[155] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[156] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[157] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[158] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart. 2014.

[159] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," *Proc. IEEE*, to be published.

[160] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2nd Quart. 2015.

[161] C. Shahriar *et al.*, "PHY-layer resiliency in OFDM communications: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 292–314, 1st Quart. 2015.

[162] M. H. Yilmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *Proc. IEEE Local Comput. Netw. Conf. Workshops*, Clearwater Beach, FL, USA, Oct. 2015, pp. 812–817.

[163] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[164] Z. E. Ankarali *et al.*, "A comparative review on the wireless implantable medical devices privacy and security," in *Proc. Conf. Wireless Mobile Commun. Healthcare*, Athens, Greece, Nov. 2014, pp. 246–249.

[165] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. New York, NY, USA: Springer, 2010.

[166] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[167] X. S. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

[168] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. 45th Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2011, pp. 265–269.

[169] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Inf. Theory*, submitted.

[170] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80–83, Feb. 2016.

[171] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 492–503, Sep. 2009.

[172] H. D. Ly, T. Liu, and Y. Blankenship, "Security embedding codes," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 148–159, Feb. 2012.

[173] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.

[174] F. Lin and F. Oggier, "A classification of unimodular lattice wiretap codes in small dimensions," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3295–3303, Jun. 2013.

[175] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.

[176] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[177] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[178] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sep. 2011.

[179] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[180] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[181] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

[182] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5681–5698, Sep. 2012.

[183] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 976–1002, Dec. 2009.

[184] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of parallel Gaussian compound wiretap channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 116–120.

[185] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.

[186] A. J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1986–1992, Nov. 1997.

[187] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[188] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.

[189] P. Xu, Z. Ding, and X. Dai, "Rate regions for multiple access channel with conference and secrecy constraints," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1961–1974, Dec. 2013.

[190] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[191] Y. Zheng, M. Schulz, W. Lou, Y. T. Hou, and M. Hollick, "Highly efficient known-plaintext attacks against orthogonal blinding based physical layer security," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 34–37, Feb. 2015.

[192] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[193] T. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 5, pp. 572–584, Sep. 1979.

[194] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct. 2014.

[195] A. G. Orozco-Lugo, M. M. Lara, and D. C. McLernon, "Channel estimation using implicit training," *IEEE Trans. Signal Process.*, vol. 52, no. 1, pp. 240–254, Jan. 2004.

[196] M. Morelli and U. Mengali, "A comparison of pilot-aided channel estimation methods for OFDM systems," *IEEE Trans. Signal Process.*, vol. 49, no. 12, pp. 3065–3073, Dec. 2001.

[197] B. Kanukurthi and L. Reyzin, "Key agreement from close secrets over unsecured channels," in *Advances in Cryptology—EUROCRYPT 2009*. Heidelberg, Germany: Springer, 2009, pp. 206–223.

[198] J. Han *et al.*, "GenePrint: Generic and accurate physical-layer identification for UHF RFID tags," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 846–858, Apr. 2016.

[199] F. Rusek *et al.*, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, Jan. 2013.

[200] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[201] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[202] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[203] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.

[204] T. S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.

[205] N. N. Alotaibi and K. A. Hamdi, "Switched phased-array transmission architecture for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1303–1312, Mar. 2016.

[206] N. N. Alotaibi and K. A. Hamdi, "Silent antenna hopping transmission technique for secure millimeter-wave wireless communication," in *Proc. IEEE GLOBECOM*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[207] A. Khandekar, N. Bhushan, J. Tingfang, and V. Vanghi, "LTE-advanced: Heterogeneous networks," in *Proc. Eur. Wireless Conf.*, Lucca, Italy, Apr. 2010, pp. 978–982.

[208] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[209] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[210] T.-Y. Liu, P. Mukherjee, S. Ulukus, S.-C. Lin, and Y.-W. P. Hong, "Secure degrees of freedom of MIMO rayleigh block fading wiretap channels with no CSI anywhere," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2655–2669, May 2015.

[211] S. Althunibat *et al.*, "On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1564–1567, Aug. 2013.

[212] V. Sucasas *et al.*, "Lightweight security against combined IE and SSDF attacks in cooperative spectrum sensing for cognitive radio networks," *Security Commun. Netw.*, vol. 8, no. 18, pp. 3978–3994, 2015.

[213] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, May/Jun. 2013.

[214] A. Alvarado, G. Scutari, and J.-S. Pang, "A new decomposition method for multiuser DC-programming and its applications," *IEEE Trans. Signal Process.*, vol. 62, no. 11, pp. 2984–2998, Jun. 2014.

[215] N. Mokari, S. Parsaeefard, H. Saeedi, P. Azmi, and E. Hossain, "Secure robust ergodic uplink resource allocation in relay-assisted cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 63, no. 2, pp. 291–304, Jan. 2015.

[216] L. Shi, J. Yuan, S. Yu, and M. Li, "MASK-BAN: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 52–62, Feb. 2015.

[217] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1803–1816, Sep. 2013.

[218] S. T. Ali, V. Sivaraman, D. Ostry, G. Tsudik, and S. Jha, "Securing first-hop data provenance for bodyworn devices using wireless link fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12, pp. 2193–2204, Dec. 2014.

[219] N. Yang *et al.*, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[220] C. Ma *et al.*, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.

[221] Y. Wang, Z. Chen, Y. Yao, M. Shen, and B. Xia, "Secure communications of cellular users in device-to-device communication underlaying cellular networks," in *Proc. 6th Int. Conf. Wireless Commun. Signal Process.*, Hefei, China, Oct. 2014, pp. 1–6.

[222] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart. 2011.

[223] Q. Guan, F. R. Yu, S. Jiang, and V. C. M. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2674–2685, Jul. 2012.

[224] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 2014.

Yiliang Liu received the B.E. and M.Sc. degrees in computer science and communication engineering from Jiangsu University, Zhenjiang, China, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree with the Communication Research Centre, Harbin Institute of Technology, China. He was also a Visiting Research Student with the Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan, from 2014 to 2015. His research interests include security for wireless networks and vehicular ad hoc networks.

Hsiao-Hwa Chen (S'89–M'91–SM'00–F'10) received the B.Sc. and M.Sc. degrees from Zhejiang University, China, and the Ph.D. degree from the University of Oulu, Finland, in 1982, 1985, and 1991, respectively. He is currently a Distinguished Professor with the Department of Engineering Science, National Cheng Kung University, Taiwan. He has authored or co-authored over 400 technical papers in major international journals and conferences, six books, and over ten book chapters in the areas of communications. He was a recipient of the Best Paper Award in the IEEE WCNC 2008 and the IEEE 2016 Jack Neubauer Memorial Award. He served as the General Chair, the TPC Chair, and the Symposium Chair for many international conferences. He served or is serving as an Editor or/and Guest Editor for numerous technical journals. He is the Founding Editor-in-Chief of Security and Communication Networks (Wiley). He served as an Editor-in-Chief for the IEEE Wireless Communications from 2012 to 2015. He is a fellow of IET, and an elected member at large of IEEE ComSoc.

Liangmin Wang (M'13) received the B.S. degree in computational mathematics in Jilin University, Changchun, China, in 1999, and the Ph.D degree in cryptology from Xidian University, Xi'an, China, in 2007. He is a Full Professor in the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China. He has been honored as a "Wan-Jiang Scholar" of Anhui Province since November 2013. Now his research interests include security protocols and Internet of Things. Dr. Wang has published over 60 technical papers at premium international journals and conferences. He has served as the TPC of many IEEE conferences, such as IEEE ICC, IEEE HPCC, IEEE TrustCOM. Now, he is an Associate Editor of *Security and Communication Networks*, a member of IEEE, ACM, and a senior member of Chinese Computer Federation.