An Overview of Physical Layer Security in Wireless Communication Systems with CSIT Uncertainty

Article *in* IEEE Access · September 2016

DOI: 10.1109/ACCESS.2016.2612585

3 authors, including:

Amal Hyadi
McGill University
17 PUBLICATIONS **129** CITATIONS
SEE PROFILE

Zouheir Rezki
University of Idaho
136 PUBLICATIONS **1,074** CITATIONS
SEE PROFILE

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2612585, IEEE Access

An Overview of Physical Layer Security in Wireless Communication Systems with CSIT Uncertainty

Amal Hyadi, *Student Member, IEEE*, Zouheir Rezki, *Senior Member, IEEE*,
and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—The concept of physical layer security builds on the pivotal idea of turning the channel's imperfections, such as noise and fading, into a source of security. This is established through appropriately designed coding techniques and signal processing strategies. In this vein, it has been shown that fading channels can enhance the transmission of confidential information and that a secure communication can be achieved even when the channel to the eavesdropper is better than the main channel. However, to fully benefit from what fading has to offer, the knowledge of the channel state information at the transmitter (CSIT) is of primordial importance. In practical wireless communication systems, CSIT is usually obtained, prior to data transmission, through CSI feedback sent by the receivers. The channel links over which this feedback information is sent can be either noisy, rate-limited, or delayed, leading to CSIT uncertainty. In this article, we present a comprehensive review of recent and ongoing research works on physical layer security with CSIT uncertainty. We focus on both information theoretic and signal processing approaches to the topic when the uncertainty concerns the channel to the wiretapper or the channel to the legitimate receiver. Moreover, we present a classification of the research works based on the considered channel uncertainty. Mainly, we distinguish between the cases when the uncertainty comes from an estimation error of the CSIT, from a CSI feedback link with limited capacity, or from an outdated CSI.**

***Index Terms*—Physical layer security, fading channels, channel state information, estimation error, rate-limited feedback, outdated CSI.**

I. Introduction

The number of research works on physical layer security has increased exponentially over the last few years. This number is certainly to continue growing with the emergence of decentralized networks and the deployment of 5G and beyond wireless communication systems. What distinguishes physical layer security compared to other high layers cryptographic techniques is that it exploits the randomness and the fluctuations of the wireless channel to achieve security at a remarkably reduced computational complexity. Information theoretic security dates back to Shannon's pioneer work [1], in 1949. Shannon's model, called a cipher system, considers the transmission of confidential information to a legitimate receiver in the presence of a passive eavesdropper intercepting the communication, cf. Figure 1. The model also assumes that a random secret key is shared between the transmitter and the legitimate receiver and that the key is unknown to the eavesdropper. To guarantee perfect secrecy, the entropy of the shared secret key should exceed the entropy of the message. In other words, this requires the key to be at least as long as the confidential message itself. Many years later, Wyner's work [2] came to shed some positive light on information theoretic security. Wyner's model, called a wiretap channel, takes advantage of the channel's imperfections to secure a transmission at the physical layer without the need of a shared secret key. Since then, studies of the wiretap channel have multiplied and have extended to more general communication systems including broadcast channels, fading channels, multiuser networks, and many other wireless communication models.

To capture the enormous growth of research works on physical layer security, multiple surveys, overview papers, and books have been published in recent years. A general detailed review of the theoretical foundations, coding techniques, practical implementations, challenges and opportunities of physical layer security is presented in [3]–[7]. The work in [8] provides a comprehensive survey describing the evolution of information theoretic security from point-to-point communication systems to multiple antenna and multiuser networks. A brief summary of challenges facing physical layer security is presented in [9] and in [10] for next generation networks. An overview of physical layer security is also considered in [11] for cooperative relay systems, in [12] for massive multiple-input-multiple-output (MIMO) systems, and in [13] for cognitive radio networks. The authors, in [14], present an earlier survey on physical layer security under the imperfect channel state information (CSI) assumption, with a particular focus on relay channels, cognitive system, and large-scale decentralized networks. The effect of outdated CSI at the transmitter (CSIT) on information theoretic security is highlighted in [15], and a synopsis of how different levels of CSIT impact the system's security is provided in [16].

The aim of this work is to present a detailed state-of-the-art review of physical layer security with CSIT uncertainty. We consider both cases when the eavesdropper's CSI is available at the transmitter and when it is not. Besides, we categorize the presented references based on the probable cause of CSIT imperfection, namely when an estimation error of the CSIT occurs, when the transmission of the CSI feedback is performed over a finite rate link, or when obtaining a delayed version of the CSIT. The case when only statistical CSI is

A. Hyadi and M.-S. Alouini are with the Division of Computer, Electrical, and Mathematical Sciences & Engineering (CEMSE), King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia. [e-mail: {amal.hyadi, slim.alouini}@kaust.edu.sa].

Z. Rezki is with the Electrical and Computer Engineering Department, University of Idaho, Moscow, ID, US. [e-mail: zrezki@uidaho.edu].

The research reported in this publication was supported by CRG 2 grant from the Office of Sponsored Research at King Abdullah University of Science and Technology (KAUST).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2612585, IEEE Access

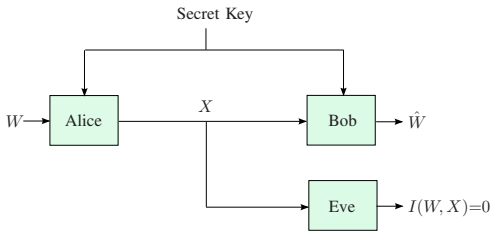


Fig. 1: Shannon's cipher system.

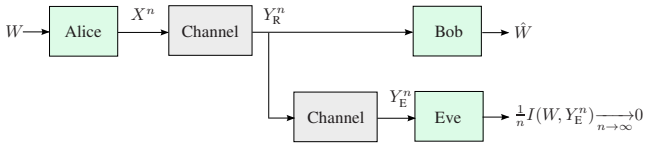


Fig. 2: Wyner's wiretap channel.

available at the transmitter is also examined.

The remainder of this article is organized as follows. Section II presents a concise description of some fundamental concepts of physical layer security, specifically the wiretap channel, the transmission of artificial noise, and secrecy metrics. The case when the transmitter has perfect main CSI is elaborated in Section III with a clear distinction between the cases when the eavesdropper CSI is available at the transmitter and when it is not. Section IV discusses CSIT uncertainty when the imperfection is the result of an estimation error of the CSIT, or when it is the consequence of a rate-limited or a delayed CSI feedback link. The scenario when the transmitter is only aware of statistical CSI is addressed in Section V. Finally, Section VI concludes the paper.

Notations: Throughout the paper, we use the following notational conventions. The entropy of a discrete random variable X is denoted by $H(X)$, and the mutual information between random variables X and Y is denoted by $I(X;Y)$. A sequence of length n is denoted by X^n, i.e., $X^n{=}\{X(1),X(2),\cdots,X(n)\}$. We also use the notation $X{\sim}\mathcal{CN}(0,\sigma^2)$ to indicate that X is a circularly symmetric complex-valued Gaussian random variable with zero-mean and variance σ^2.

II. Fundamentals

This section provides the reader with an objective description of some fundamental concepts associated with physical layer security. First, we present the basic information theoretic model introduced by Wyner in his seminal work [2], which is colloquially known as the *wiretap channel*. We shed light on how Wyner's model take advantage of the channel's noisiness to secure a transmission, and we briefly explain the structure of the wiretap code. Then, we consider and discuss the usefulness of transmitting *artificial noise* to ensure or enhance the security of a wireless transmission. The last part of this section presents two key secrecy metrics used to evaluate and measure the performance of a system under confidentiality constraints, namely the *secrecy capacity* and the *secrecy outage probability*.

A. Wiretap Channel

Wyner's channel model, also known as the wiretap channel, represents a generalization of Shannon's cipher system. The originality of Wyner's work comes straight from his pivotal idea to take advantage of the imperfection of the communication medium to secure a transmission at the physical layer. In Wyner's model, illustrated in Figure 2, the transmitter (Alice) tries to communicate a confidential message W to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve) over a noisy memoryless link. The model assumes that Eve observes a degraded version of the signal obtained by Bob. The channel between Alice and Bob is usually referred to as the main channel while the channel between Alice and Eve is known as the wiretap channel or the eavesdropper's channel. The message W is encoded into a codeword X^n of length n and transmitted at a rate $\mathcal{R}_{\mathrm{s}}$. A $(2^{n\mathcal{R}_{\mathrm{s}}},n)$ code consists of the following elements:

- A message set $\mathcal{W}=\left\{1,2,\cdots,2^{n\mathcal{R}_{\mathrm{s}}}\right\}$ with the messages $W\in\mathcal{W}$ independent and uniformly distributed over $\mathcal{W}$;
- A stochastic encoder $f:\mathcal{W}\rightarrow\mathcal{X}^n$ that maps each message w to a codeword $x^n\in\mathcal{X}^n$;
- A decoder at the legitimate receiver $g:\mathcal{Y}^n\rightarrow\mathcal{W}$ that maps a received sequence $y_{\mathrm{R}}^n\in\mathcal{Y}^n$ to a message $\hat{w}\in\mathcal{W}$.

A rate $\mathcal{R}_{\mathrm{s}}$ is an *achievable secrecy rate* if there exists a sequence of $(2^{n\mathcal{R}_{\mathrm{s}}},n)$ code such that the reliability condition

$$\lim_{n\to\infty}\frac{1}{2^{n\mathcal{R}_{\mathrm{s}}}}\sum_{w=1}^{2^{n\mathcal{R}_{\mathrm{s}}}}\Pr\left[W\neq\hat{W}\middle|W=w\right]=0, \tag{1}$$

and the secrecy condition

$$\lim_{n\to\infty}\frac{1}{n}I\left(W;Y_{\mathrm{E}}^n\right)=0, \tag{2}$$

with Y_{E} representing the received signal at the eavesdropper, are both satisfied.

The secrecy constraint in (2) is called the *weak secrecy* condition. It requires only the information leaked rate to vanish as $n{\rightarrow}\infty$. This condition is weaker than *strong secrecy* which requires the absolute information $I\left(W;Y_{\mathrm{E}}^n\right)$ to vanish as $n{\rightarrow}\infty$ [17], [18], i.e. $\lim_{n\to\infty}I\left(W;Y_{\mathrm{E}}^n\right){=}0$.

The achieving secrecy code that guarantees both the reliability and the security of the transmitted information is called a *wiretap code*. It is a stochastic code having a nested structure. As a matter of fact, instead of fixing the codeword associated with each message W, the codeword is chosen at random according to a local random number generator $W'\in\left\{1,\cdots,2^{n\mathcal{R}_{\mathrm{e}}}\right\}$, with $\mathcal{R}_{\mathrm{e}}$ denoting the *equivocation rate*, i.e., $\mathcal{R}_{\mathrm{e}}{=}I\left(W;Y_{\mathrm{E}}^n\right)$. The set of $2^{n\mathcal{R}_{\mathrm{e}}}$ codewords, corresponding to each secret message, forms what we call a bin or a subcode of the wiretap code. To date, practical constructions of wiretap codes are only possible for some particular channels.

Although Wyner's model builds on the assumption of a degraded wiretap channel where the signal at the eavesdropper

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2612585, IEEE Access

is a degraded version of the legitimate receiver's signal, it provides the essential elements required to understand information theoretic security without the complexity of a more general setup. Ulterior works generalized Wyner's work to the case of non-degraded channels [19], Gaussian channels [20], and fading channels [21]–[25], to cite only few. For more details about the wiretap channel, wiretap coding or alternative coding techniques for secret communications, we invite the reader to consider the following references [3], [5], [6], [26].

B. Artificial Noise Transmission

One of the effective signal processing approaches proposed to provide security at the physical layer is the transmission of *jamming signals*, also known as *artificial noise*. Goel and Negi introduced the artificial noise technique in [27], [28]. The main idea of the work is to exploit part of the available transmission power to send artificially generated noise. The generated noise is designed such that only the wiretap channel is degraded while the main channel is kept intact. Consequently, Bob gets an advantage over Eve, and a secure transmission can be achieved. The transmission of the jamming signals is possible either by using multiple antennas at the transmitter or with the assistance of relaying nodes. The latter case is more challenging since the transmission of all nodes must be synchronized, and Alice can not directly control the jamming signals. However, in either case, the total number of transmit antennas should exceed the number of antennas at the eavesdropper. Also, in order to ensure that the interfering noise will only affect the eavesdropper, the jamming signal must be sent in the null space of the legitimate receiver, hence, requiring the knowledge of the CSIT. Since Goel and Negi's work, research on physical layer security with artificial noise transmission has multiplied. The multiple antenna case is examined, for instance, in [29]–[33] while the jamming relays case is considered in [34]–[36].

C. Secrecy Performance Measures

To evaluate the performance of a communication system with a security constraint, the two most commonly used metrics are the secrecy capacity and the secrecy outage probability.

Secrecy Capacity: The secrecy capacity $\mathcal{C}_{\rm s}$ is defined as the maximum achievable secrecy rate, i.e.,

$$\mathcal{C}_{\rm s} \triangleq \sup \mathcal{R}_{\rm s},$$

where the supremum is over all achievable secrecy rates. It could be seen as the homologue of the traditional channel capacity with a secrecy constraint.

For Wyner's wiretap channel, the secrecy capacity is given as the difference between a rate of reliable communication and a rate of information leaked to the eavesdropper, i.e.,

$$\mathcal{C}_{\rm s} = \max_{U \to X \to Y_{\rm R} \to Y_{\rm E}} \left(I\left(U;Y_{\rm R}\right) - I\left(U;Y_{\rm E}\right)\right), \qquad (3)$$

where U is an auxiliary random variable and $U \to X \to Y_{\rm R} \to Y_{\rm E}$ forms a Markov chain. From (3), it is clear that the secrecy capacity is positive as long as the transmitter and the legitimate receiver have an advantage over the eavesdropper at the physical layer. This is the case for Wyner's model since $Y_{\rm R}$ is a degraded version of $Y_{\rm E}$. For a general fading channel, this could be viewed as transmitting only over the channel instants where the main channel is better than the eavesdropper's channel. This brings us back to the problematic of having CSIT.

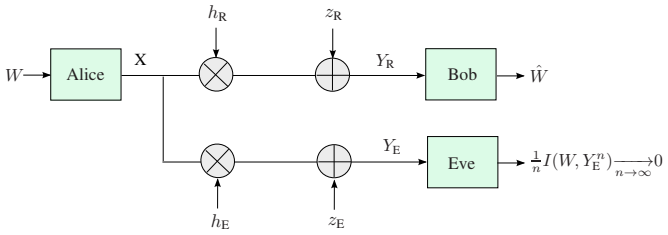


Fig. 3: Fading wiretap channel.

secrecy outage probability: In parallel with the definition of outage probability in a communication system with no confidentiality constraints, the secrecy outage probability is defined as the probability that a target rate is unachievable. In other words, an outage occurs if the secrecy capacity is smaller than a certain fixed value. The expression of the secrecy outage probability can hence be formulated as

$$P_{\rm out} = \Pr\left[\mathcal{C}_{\rm s} \leq \overline{\rm R}_{\rm s}\right], \qquad (4)$$

where $\mathcal{C}_{\rm s}$ is the secrecy capacity and $\overline{\rm R}_{\rm s}$ is the targeted fixed rate. In the case when the secrecy capacity of the system in question is unknown, the achievable secrecy rate is considered instead.

Other Metrics: In a significant number of works on information theoretic security, mainly considering fading channels, other metrics based on signal processing methods are used to study the performance of a wireless system with security constraints. The aim of these works is mainly to design optimal transmission schemes that maintain the bit error rate (BER) or the signal-to-interference-plus-noise-ratio (SINR) at the desired receiver or the eavesdropper to prespecified thresholds. It must be emphasized that even though optimizing the communication system by constraining the BER or the SINR usually simplifies the system design, it satisfies neither the weak nor the strong secrecy constraints.

III. Physical Layer Security with Perfect CSIT

In recent years, the fading wiretap channel has opened new research directions for information theoretic security. What is unique about the fading model is that it takes advantage of the randomness of the channel gain fluctuations to secure the transmission against potential eavesdroppers, at the physical layer itself. As a result, even if the eavesdropper has a better average signal-to-noise ratio (SNR) than the legitimate receiver, physical layer security can still be achieved over fading channels without requiring the sharing of a secret key [21]–[23]. Figure 3 illustrates the fading wiretap channel

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2612585, IEEE Access

where the respective received signals at the legitimate receiver and the eavesdropper, at time instant t, can be represented as

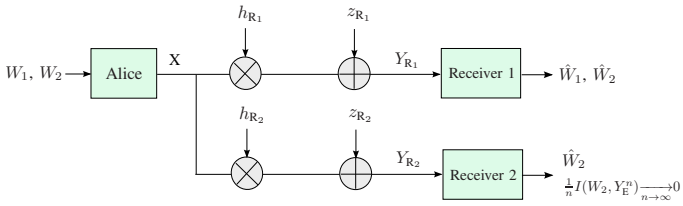
$$\begin{aligned} Y_{\mathrm{R}}(t) &= h_{\mathrm{R}}(t)X(t) + z_{\mathrm{R}}(t) \\ Y_{\mathrm{E}}(t) &= h_{\mathrm{E}}(t)X(t) + z_{\mathrm{E}}(t)' \end{aligned} \tag{5}$$

where $X(t)$ is the transmitted signal, $h_{\mathrm{R}}(t)$ and $h_{\mathrm{E}}(t)$ are the respective channel gains of Bob and Eve's channels, and $z_{\mathrm{R}}(t)$ and $z_{\mathrm{E}}(t)$ represent the additive white Gaussian noises at the respective receivers. The fading coefficients h_{R} and h_{E} are usually assumed mutually independent, and an average transmit power is generally imposed at the transmitter.

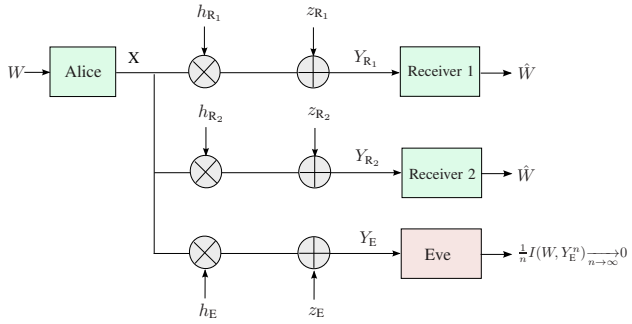
To make the most of what the fading channel has to offer to physical layer security, the knowledge of the CSIT is of primordial importance. A vast majority of works assume that the transmitter has a perfect knowledge of the CSI of both the main and the eavesdropper channels or at least of the main channel. In this section, we are interested in these research works where the perfect CSI assumption is made. We start by considering the case when both the main and the eavesdropper channel gains are revealed to the transmitter. Then, we look at the case when only the main CSI is perfectly known at the transmitter.

Both the main and the eavesdropper CSI are perfectly known at the Transmitter: When the transmitter is perfectly aware of the legitimate receiver's and the eavesdropper's CSI, the optimal transmission scheme is to send the confidential information only when the main CSI is better than the eavesdropper's CSI and adapt the transmitted power according to the instantaneous values of the channel gains. The block-fading wiretap channel is considered in [22], where the ergodic secrecy capacity is established in both cases, when the eavesdropper's CSI is available at the transmitter and when it is not. The effect of correlation between the main and the wiretap block-fading channels is investigated in [37], [38], where the loss engendered by the correlation is quantified in terms of the secrecy capacity. The authors in [39] examine the case of frequency-selective fading channels. The model of interest is a broadcast channel with confidential message (BCC), in which the source has a common message to transmit to two receivers (Receiver 1 and 2) and a confidential message to transmit to only one of the receivers (Receiver 1) while keeping it secret from the other (Receiver 2). Figure 4 highlights the difference between the broadcast channel with confidential information, the broadcast wiretap channel with common message transmission, and the broadcast wiretap channel with independent messages. The work in [39] proposes a practical Vandermonde precoding to exploits the zeros of Receiver 2's channel to hide the secret information in a similar way to spatial beamforming. The ergodic secrecy capacity region of the BCC is established in [25]. Further results on the BCC can be found in [40]–[42]. The frequency-selective fading model is also considered in [43], where the secure degrees of freedom of a K user interference channel are analyzed.

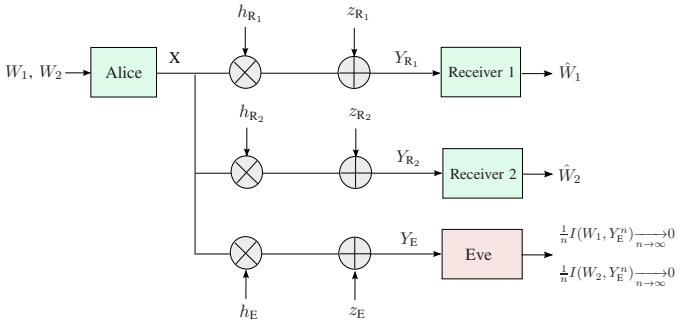
In the last few years, multiple antenna wiretap channels have become a compelling research topic. In [44] and [45], the authors investigate the secrecy capacity of a multi-antenna quasi-static fading wiretap channel and highlight the positive



(a) Two-user broadcast channel with confidential messages.



(b) Two-user broadcast wiretap channel with common message transmission.



(c) Two-user broadcast wiretap channel with independent messages transmission.

Fig. 4: Two-user broadcast channel with secrecy constraints.

impact of deploying multiple antennas on the confidentiality of the system. The work in [46] considers the case of a degraded single-input-multiple-output (SIMO) wiretap channel and shows that the secrecy diversity gain is proportional to the number of receive antennas. The multiple-input-single-output (MISO) case is studied in [47]–[49]. The secrecy capacity of a multiple-input-multiple-output (MIMO) wiretap channel with a single antenna eavesdropper is examined in [50], and the case of MIMO transmission with a multiple-antenna eavesdropper is considered in [51]–[56] when the channel gain matrices are fixed and known to all terminals. Analysis on the secure degrees of freedom, the secrecy diversity gain, and the secrecy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2612585, IEEE Access

multiplexing gain can be found in [57] and references therein.

Other works on physical layer security with full CSIT include [58]–[63] where the security of cooperative systems is investigated, [64]–[68] where cognitive systems with confidentiality constraints are considered, and [69]–[71] for secure massive MIMO systems.

Only the main CSI is perfectly known at the Transmitter: In this case, it is generally assumed that the transmitter is aware of the statistics of the eavesdropper's CSI but not of its instantaneous realizations. Baros and Rodrigues, [21], were one of the first to emphasize the key role fading channels play in enhancing the information theoretical security of wireless communication systems. Their model consists of a quasi-static Rayleigh fading channel where the channel gains remain constant over all channel uses, and only the main CSI is perfectly known to the transmitter. The work characterizes the outage secrecy capacity of the system and interestingly shows that secure transmission is possible even when the average SNR of the eavesdropper is better than that of the legitimate receiver. An extension of their work, considering the case when an imperfect estimation of the eavesdropper's CSI is also available at the transmitter, is presented in [23]. The authors in [72] investigate the achievable secrecy rate of a wiretap channel with a constant AWGN main channel and a time varying Rayleigh fading eavesdropper's channel. The ergodic secrecy capacity and the optimal transmission power for block-fading channels are examined in [22]. Block-fading channels are also considered in [73], where the secrecy outage probability of the system is evaluated under different secure hybrid automatic retransmission request (HARQ) protocols. The work in [74] and [24] analyses the ergodic secrecy capacity of parallel channels and fast fading broadcast channels. Both cases, when a common information is transmitted to all the legitimate receivers, and when each receiver is interested in an independent information, are considered. Research on multiple antenna wiretap channels assuming perfect main CSI and no eavesdropper's CSI at the transmitter may be found in [75]–[79] and in [27]–[29], [31], [80]–[82] for artificial noise transmission. Another work, [83], study the optimal beamforming design for a MISO system with perfect main CSI and a noisy version of the eavesdropper's CSI available at the transmitter. Secure cooperation is tackled in [84]–[86].

Although the assumption of perfect CSIT reduces the complexity of the secrecy analysis and allows the characterization of the full potential of the fading wiretap channel, it does not capture the practicality of the transmission system. On one hand, the knowledge of the eavesdropper's CSIT is far from possible in a real scenario as Eve is a passive node who does not transmit and whose sole interest is to intercept the communication between Alice and Bob. That is, the eavesdropper has no interest in giving Alice its CSI. This assumption is usually justified by considering that Eve belongs to the same communication network as Alice and Bob and that all users provide the transmitter with their CSI prior to data transmission. However, as Eve is a malicious node, nothing guarantees that it will give Alice its actual CSI. On the other hand, in a practical communication system, only partial main CSI can be obtained at the transmitter. We will discuss this latter case in details in the following section.

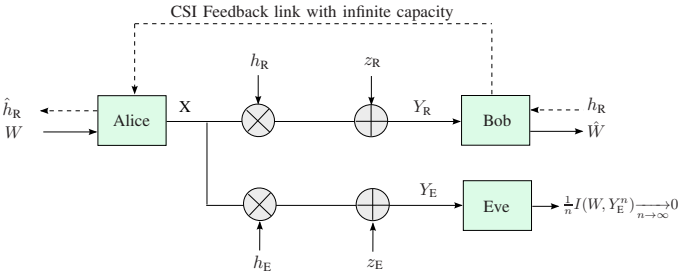


Fig. 5: Fading wiretap channel with perfect CSIR and noisy estimation of the main CSIT.

IV. Physical Layer Security with main CSIT Uncertainty

In a wireless communication system, the knowledge of the CSI at the receiver (CSIR) is usually possible through training signals sent by the transmitter. For wiretap channels, these training signals can also be used by the eavesdropper who gets to estimate its channel gain too. The estimation of the CSI at the receiving nodes is generally very accurate thanks to the receivers' capability to deploy rapid channel tracking. As for acquiring the CSIT, the receiver should feedback its CSI to the transmitter constantly. This feedback process is typically accompanied by the introduction of uncertainty into the CSIT. Different phenomena can cause the CSIT to be imperfect. Most commonly, the uncertainty comes from an error of estimation at the transmitter who ends up with a noisy version of the CSI, or from a feedback link with a limited capacity which requires the transmission of quantized CSI, or also from a delayed feedback causing outdated CSIT. Considering these three main causes of CSI imperfection, we present in what follows an exhaustive list of research works on physical layer security with main channel gain uncertainty.

A. Estimation Error of the main CSIT

Estimation error is one of the most common reasons behind CSIT uncertainty. Research on physical layer security, with an estimation error of the main CSIT, generally assumes that the legitimate receiver sends its CSI to the transmitter through a feedback link with infinite capacity, cf. Figure 5. The main channel gain estimation model can be formulated as

$$h_{\mathrm{R}}(t) = \sqrt{1-\alpha}\,\hat{h}_{\mathrm{R}}(t) + \sqrt{\alpha}\,\tilde{h}_{\mathrm{R}}(t), \tag{6}$$

where $h_{\mathrm{R}}(t)$ is the actual main CSI at time instant t, $\hat{h}_{\mathrm{R}}(t)$ is the noisy version of the CSI available at the transmitter, $\tilde{h}_{\mathrm{R}}(t)$ is the channel estimation error, and α is the estimation error variance ($\alpha \in [0,1]$). The case α=0 corresponds to the perfect main CSIT scenario while α=1 corresponds to the no main CSIT case. It is usually assumed that Bob can perfectly estimate its CSI and that Alice is only aware of the statistics of the wiretap channel. Besides, most research works consider

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2612585, IEEE Access

the worst case scenario where the eavesdropper has a perfect knowledge of all channel gains.

One of the first works in this research area is [87] and its journal version [88], where the ergodic secrecy capacity, of a single-antenna single-user fast fading wiretap channel with a noisy CSIT, is characterized by a lower and an upper bound. The proposed achievable secrecy rate is based on a standard wiretap code with a Gaussian input and a simple on-off power transmission scheme while the upper bound is obtained using an appropriate correlation between the main and the wiretap channels. The authors show that even with a high estimation error, the transmitter can still achieve a positive secrecy rate, and that a simple constant rate on-off power scheme is enough to establish a secure communication at a reduced computational complexity. A concurrent work, presented in [89] and [90], investigates the achievable secrecy rate of ergodic and block-ergodic fading channels in the presence of imperfect CSIT about both the main channel and the eavesdropper's channel. The presented results suggest that CSIT uncertainty does not necessarily preclude security and that relatively little CSIT is required to take advantage of fading. The problem of secure multiuser broadcasting over fast fading channels with noisy CSIT is considered in [91] and [92]. The work derives bounds on the ergodic secrecy capacity when a common message is broadcasted to all legitimate receivers and bounds on the ergodic secrecy sum-capacity when multiple independent messages are broadcasted. In both scenarios, common message and independent messages broadcasting, the transmitted information has to be kept secret from the eavesdropper. The scaling law of the system, when transmitting to a large number of legitimate receivers, is also analyzed.

Multiple antenna wiretap channels with an estimation error of the main CSIT have raised considerable research interset. The performance analyses of a multi-cell MISO downlink system, where a multi-antenna base station transmits confidential messages to its legitimate users with a passive eavesdropper present in each cell, are approached in [93] from a signal processing perspective. It is assumed that the receivers only feedback the channel gain directions, required to cancel out the inter-cell interference, and that an error of estimation occurs at the base station. Closed-form expression for the ergodic secrecy rate, the secrecy outage probability, and the interception probability are presented for Rayleigh fading channels. The ergodic secrecy capacity of MISO wiretap communication systems is characterized in [94] and the achievable secrecy rate is evaluated in [95] and [96] using transmit beamforming. The case when a noisy estimate of the eavesdroppers channel is also available at the transmitter is addressed in [96] and in [97] where different secrecy rate optimization techniques are proposed for MISO channels. An earlier work on MIMO wiretap channels with artificial noise transmission is conducted in [98]. The focus of this study is twofold. First, to maximize the amount of power available to broadcast a jamming signal while maintaining a predefined SINR at the desired receiver. Second, to assess the resulting performance degradation due to the presence of imperfect CSIT. Noisy estimation of the main CSIT is also considered in [99] for massive MIMO system, in [100] for cooperative wiretap channels, and in [101] for cognitive radio networks.

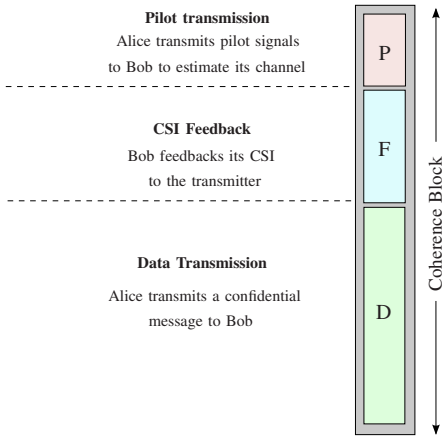


Fig. 6: CSI training and data transmission over one coherence block.

B. Limited main CSI Feedback

Another cause of CSIT uncertainty is the transmission of the feedback information over finite-rate links. As a matter of fact, the process of procuring CSI is resource consuming in time-varying fading channels, and the accuracy of the obtained CSIT is highly correlated with the size of the feedback overhead and the allocated power for feedback transmission. In block-fading channels, the acquisition of the CSIT during each coherence time takes place in three stages: transmission of a pilot signal destined for the receiver to estimates its channel gain, followed by CSI feedback to the transmitter, then data transmission, cf. Figure 6. Clearly, when more time is allocated to training, time for data transfer is reduced and vice versa. The feedbacked information is used to notify the transmitter about the forward link condition. A broad look at the field of limited feedback in wireless communication systems is provided in [102]. For works on information theoretical security with limited feedback, it is usually assumed that the receiver feedbacks the index of a quantized version of the CSI, the index of the channel region in which the CSI lies, or the index of the quantized channel gain direction. It is also assumed, in most works, that the quantization codebook is fixed and known to all terminals, that the feedback link is error-free, and that both Bob and Eve estimate their respective channel gains perfectly.

In [103] and [104], the ergodic secrecy capacity of block-fading wiretap channels with limited-rate feedback is investigated under both a short-term power constraint and a long-term power constraint. The study establishes lower and upper bounds on the secrecy capacity when the feedback information is sent at the beginning of each coherence block over an error-free public channel with finite capacity. The proposed bounds coincide as the capacity of the feedback link goes to infinity, hence, fully characterizing the secrecy capacity in this case. It is also shown that a positive secrecy rate can still

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2612585, IEEE Access

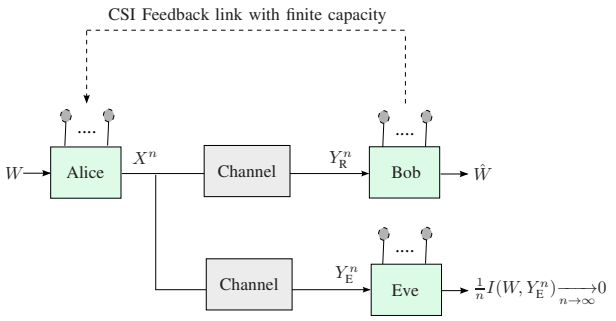


Fig. 7: MIMO wiretap channel with limited CSI feedback.

be achievable even when only 1-bit ARQ feedback is sent to the transmitter at the end of each coherence block. Multiuser block-fading broadcast channels, where the transmission is intended for multiple legitimate receivers in the presence of an eavesdropper, is examined in [105]. Here too, the presented lower and upper bounds on the ergodic secrecy capacity for the common message case and lower and upper bounds on the secrecy sum-rate for the independent messages case are shown to coincide for the particular case of infinite feedback. The ergodic secrecy capacity region of the block-fading BCC in which the transmitter has common information for two receivers and confidential information intended for only one of them is tackled in [106]. Both cases when the feedback link is error-free and when it is a binary erasure channel (BEC) are analyzed. In the latter case, it is demonstrated that as long as the erasure event is not a probability 1 event, Alice can still transmit the confidential information with a positive secrecy rate.

The impact of having imperfect CSIT obtained via a limited rate feedback on the throughput of multiple antenna wiretap channels was elaborated first in [107]–[109]. The work considers both MISO and MIMO communication systems with artificial noise transmission and investigates the optimal power allocation strategy that maximizes the secrecy rate. Assuming the transmitter is only aware of a quantized version of the main channel gain direction, it is shown that sending artificial noise does not only harm the eavesdropper but can also leak into the legitimate receiver's channel and cause a significant rate loss in the secrecy rate. The achievable secrecy rate of MIMO wiretap channels is also addressed in [110], [111], and [112]. In [110], a transmission strategy based on artificial noise and linear precoding is proposed to overcome CSIT imperfection in the presence of an adversarial jammer. The main CSI feedback is quantized using Grassmannian quantization, [113], and sufficient conditions on the feedback bit rate scaling are derived to guarantee the same secure degrees of freedom (SDoF) as for the perfect CSIT case. In [111], artificial noise assisted secure transmission is considered in the context of frequency-division duplexed MIMO wiretap channels. The work defines the achievable effective ergodic secrecy rate (ESR) and evaluates the optimal power allocation and training overhead that maximize it when the channel direction information of the eavesdropper is available at the transmitter. The transmission of artificial noise is also adopted in [112] with random vector quantization (RVQ). The results show that a positive secrecy rate can always be achieved when the number of feedback bits is large, the artificial noise power is high, and a constraint on the number of antennas at the eavesdropper is satisfied. A characterization of the ergodic secrecy capacity in terms of lower and upper bounds is presented in [114]. The work also proposes an optimal framework for feedback and transmission which is based on the iterative Lloyd algorithm [115]. The ergodic secrecy sum-rate of multiuser multi-antenna downlink systems with limited main channel direction feedback is discussed in [116] and [109]. On another note, the authors in [117] assume that in addition to having a limited rate feedback, a CSI estimation error occurs at the legitimate receiver. Under this assumption, an upper bound on the secrecy rate loss is derived and used to design an optimal CSI feedback strategy that maintains a predefined secrecy service quality (QoS).

C. Outdated main CSIT

Delay in feedback transmission is one of the common sources of CSIT uncertainty. It causes the transmitter to base its transmission strategy on a time-delayed channel coefficient version of the current legitimate receiver's CSI. Considering a time-varying wiretap channel, where the main channel remains constant over a time slot and changes from one slot to another, it is generally assumed that the feedback delay is of the length of a time slot, i.e., at time instant t, Alice is aware of $h_{\mathrm{R}}(t-1)$. This particular scenario straightforwardly generalizes to the case when the delay is of multiple time slots length.

The impact of outdated CSIT on the secrecy outage performance of MISO wiretap channels with transmit antenna selection (TAS) is evaluated in [118]. The authors present a closed-form expression for the secrecy outage probability when the transmission is conveyed over Nakagami-m fading channels, and show that a significant diversity loss results from making use of the delayed CSI version to select the optimal transmit antenna. The secrecy outage performance with CSI feedback delay and TAS is also addressed in [119] and [120], for MIMO wiretap channels. The work in [119] proposes a new secure transmission scheme intended to defeat the detrimental effect the outdated CSI have on transmit antenna selection. The presented strategy requires two feedback phases sent in different time slots, take spatial correlation at the legitimate receiver into consideration, and guarantees a better outage performance. The probability of non-zero secrecy capacity is also investigated, and the loss in terms of the secrecy diversity is assessed. In [120], a general order TAS scheme is proposed to enhance the secrecy performance of Nakagami-m MIMO fading wiretap channels with outdated CSI. The work considers both cases when Alice is aware of Eve's instantaneous CSI and when it is not. In the first scenario, the average secrecy capacity of the system is analyzed while in the second scenario, the secrecy outage probability and the probability of non-zero secrecy capacity are derived.

Other research works on physical layer security with outdated main CSI analyze the repercussion of CSIT imperfection

on the system's secure degrees of freedom. In [121], the SDoF of a two-user MIMO broadcast wiretap channel with outdated CSI is characterized. The achieving scheme is based on an aligned transmission of artificial noise along with the confidential information. The case when the transmitter has also access to a delayed version of the eavesdropper's CSI is also studied. Obviously, the secure performances in the latter case are better compared to when Alice is only aware of the outdated main CSI. The authors in [122] investigate the sum SDoF region of a two-user MIMO X-channel under secrecy constraints with a delayed CSIT sent over an asymmetric feedback link. The work highlights the importance of sending an asymmetric output feedback in conjunction with the outdated CSI to improve the secrecy performance of the system. Moreover, it shows that the sum SDoF region of the adopted model is the same as the SDoF region of a two-user MIMO broadcast channel with feedback delay. Another work, presented in [123], examines the SDoF of a single antenna wiretap channel with a friendly jammer and an arbitrary number of eavesdroppers. Assuming that both the transmitter and the jammer have access to outdated main CSI and that linear coding transmission strategies are employed, it is proven that a strictly positive SDoF is achievable irrespective of the number of eavesdroppers.

The effect of delayed feedback coupled with an estimation error of the CSI at the transmitter is discussed in [124]. The work investigates an optimal masked beamforming scheme to enhance the secure performance of a multiuser MIMO downlink wiretap channel with noisy and outdated CSIT. The presented technique aims to maximize the transmission power allocated to artificial noise while meeting individual minimum mean square error (MMSE) constraints of the legitimate users. The obtained results show that the adopted approach can significantly reduce the sensitivity of the system to CSIT imperfections.

In most research works on physical layer security with CSIT uncertainty, the CSIT is obtained through a feedback link sent by the legitimate receiver before data transmission. In such a model, the eavesdropper is perfectly able to track the feedback link and hence recover the feedback information. Furthermore, the secrecy performances of fading wiretap channels are usually investigated for the worst case scenario, where the eavesdropper is perfectly aware of all channel gains. Note though that to avoid leaking the main CSI to the eavesdropper, the legitimate receiver can send a reverse training signal to the transmitter to estimate the CSI. Assuming that the eavesdropper has no other means to obtain the legitimate receiver's CSI, the main channel gain information can be used as a source of secrecy.

V. Physical Layer Security with No CSIT

As explained in the previous section, acquiring CSI at the transmitter requires the receivers to feedback their measured CSI throughout the communication. In certain cases, CSI feedback is not feasible. In particular, this may happen when the channel varies very quickly for the receivers to estimate it and feedback it to the transmitter. Also, this can be the case when the end nodes have no feedback capability as in some sensor and ad-hoc wireless communication networks. In such a situation, the transmitter has to base its transmission strategy only on the knowledge of the statistics of the main and the eavesdropper channels since the actual realizations can not be obtained. However, to achieve some level of information theoretic security, at least the statistics of the channels should be available at the transmitter.

In [125], the authors consider a single antenna single user transmission over a fast fading Rayleigh wiretap channel with no CSI available at neither the transmitter nor the receivers. The work analyses the ergodic secrecy capacity of the system under the no CSI assumption and derives an exact expression for it. Furthermore, the authors show that the considered channel is equivalent to a degraded wiretap channel and that the optimal input distribution has a finite support. The ergodic secrecy capacity of fast fading wiretap channels with no CSIT is also investigated in [126] under different stochastic orders. More specifically, it is proven that even with only statistical CSI, it is still possible to compare the channel orders. The presented numerical results illustrate the case of Nakagami-m fading wiretap channels and show that the proposed achievable scheme outperforms the Gaussian codebook in several cases. The block-fading wiretap channel is considered in [127], where two broadcast schemes are proposed to ensure the confidentiality of the transmitted information without the need of CSIT. The presented schemes are based on superposition coding and embedded coding and guarantees that the legitimate receiver decodes more information when its channel is better than the eavesdropper. The secrecy rate of the system when using each of the broadcast approaches is derived, and the corresponding optimal power allocation over the different layers is characterized. Besides, the work introduces and study a notion of probabilistic secrecy to examine the secrecy rate under stringent delay constraints.

Multiple antenna wiretap channels with only statistical CSIT are addressed in [128] and [129]. In [128], the ergodic secrecy capacity of fast Rayleigh fading MISO wiretap channels is established. The authors derive a new secrecy capacity upper bound and prove that a Gaussian input is secrecy capacity achieving without the use of prefixing. Moreover, the presented results show that with only statistical CSIT, the secrecy capacity can neither scale with the SNR, nor with the number of transmit antennas. The case of block Rayleigh fading MIMO wiretap channels is examined in [129] when no CSI is available at any of the terminals. The work investigates the SDoF of the system when the channel coherence time is of a moderate duration. A positive SDoF is shown to be achievable by a constant norm channel input as long as the eavesdropper has fewer antennas than the legitimate entities. The cooperative multiple antenna wiretap scenario is elaborated in [130], in terms of the secrecy outage probability, when only the index of the selected antenna is available at the transmitter. Another work on physical layer security with no CSIT is addressed in [131], [132] from a stochastic geometry perspective.

It is clear that the knowledge of the CSIT is highly correlated with the secrecy rate that can be achieved. Indeed,

the more the transmitter knows, the better the secrecy rate is. However, what is interesting to notice is that as long as the transmitter has some knowledge of the CSI, a positive secrecy rate can still be achieved. Note thought that at least the statistics of the legitimate and the eavesdropper channels should be known at the transmitter. Otherwise, it is not clear how to achieve a secure transmission, and the secrecy rate is equal to zero in this case.

VI. Conclusion

In the last few years, research on physical layer security tends to consider practical communication scenarios. Indeed, there has been more and more interest is studying the impact of CSIT uncertainty on the secrecy performances of wireless communication systems with security constraints. In this paper, we presented a detailed overview of recent and ongoing research works on physical layer security with CSIT uncertainty. We focused on both information theoretic and signal processing approaches to the topic and classified the related references according to the cause of CSIT imperfection. In particular, we distinguished between the cases when the uncertainty comes from an estimation error of the CSIT, from a CSI feedback link with limited capacity, or from an outdated CSI. The case when only statistical CSI is available at transmitter was also considered. The lessons to learn here is that even with a little knowledge of the CSIT, a secure transmission can still be achieved and that the more the transmitter knows about the CSI, the better the secrecy performances are.

Certainly, there are still open challenges related to physical layer security with CSIT uncertainty. First, we can see that, for most cases, the secrecy capacity of fading wiretap channels with partial CSIT is not perfectly known and is only characterized in terms of bounds. Also, we notice that a certain level of CSI knowledge is required at the transmitter, i.e., at least the statistics of the communicating channels should be known at the transmitter. It would be of interest to consider and study the case when even the statistics of the eavesdropper's channel can not be obtained at the transmitter. The construction of practical wiretap codes is another open issue facing physical layer security either with perfect or partial CSIT.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–719, Oct. 1949.

[2] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] Y. Liang, H. Poor, and S. Shamai, *Information Theoretic Security*. Foundations and Trends in Communications and Information Theory 5 (4-5), 2008.

[4] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Norwell, MA, US: Springer, 2009.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.

[6] E. by X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2014.

[7] E. Jorswieck, A. Wolf, and S. Gerbracht, *Trends in Telecommunications Technologies: Secrecy on the Physical Layer in Wireless Networks*. InTech, 2010.

[8] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[9] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[10] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[11] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

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

[13] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, "Securing physical-layer communications for cognitive radio networks," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48–54, Sep. 2015.

[14] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Communications*, no. 3, Sep. 2013.

[15] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.

[16] T.-Y. Liu, P.-H. Lin, Y.-W. P. Hong, and E. Jorswieck, "To avoid or not to avoid CSI leakage in physical layer secret communication systems," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 19–25, Dec. 2015.

[17] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Advances in Cryptology - EUROCRYPT 2000 (Lecture Notes in Computer Science, vol. 1807), Bruges, Belgium: Springer-Verlag*, pp. 351–368, 2000.

[18] I. Bjelakovic, H. Boche, and J. Sommerfeld, "Strong secrecy in arbitrarily varying wiretap channels," in *Proc. IEEE Information Theory Workshop (ITW'2012)*, Lausanne, Switzerland, Sept. 2012, pp. 617–621.

[19] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[20] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[21] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. International Symposiumon on Information Theory (ISIT'2006)*, Seattle, WA, US, Jul. 2006, pp. 356–360.

[22] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[23] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

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

[25] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[26] 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 Processing Magazine*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[27] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference (VTC-2005-Fall)*, Dallas, US, Sept. 2005, pp. 1906–1910.

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

[29] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels:achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[30] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[31] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communication Letters*, vol. 17, no. 7, pp. 1483–1486, Jul. 2013.

[32] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[33] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas of Communication*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[34] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Journal on Selected Areas of Communication*, vol. 29, no. 10, pp. 2067–2078, Dec. 2011.

[35] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secret communication," in *Proc. IEEE Information Theory Workshop (ITW'2008)*, Porto, Portugal, May 2008, p. 164168.

[36] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[37] H. Jeon, N. Kim, M. Kim, H. Lee, and J. Ha, "Secrecy capacity over correlated ergodic fading channels," in *Proc. IEEE Military Communications Conference*, San Diego, CA, US, Nov. 2008, pp. 1–7.

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

[39] M. Kobayashi, M. Debbah, and S. Shamai, "Secured communication over frequency selective fading channels: A practical Vandermonde precoding," *EURASIP Journal on Wireless Communications and Networkin*, pp. 1–19, article ID 386 547, Aug. 2009.

[40] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[41] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.

[42] S. Zou, Y. Liang, L. Lai, and S. Shamai, "Rate splitting and sharing for degraded broadcast channel with secrecy outside a bounded range," in *Proc. International Symposiumon on Information Theory (ISIT'2015)*, Hong Kong, Jun. 2015, pp. 1357–1361.

[43] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the k-user Gaussian interference channels," in *Proc. IEEE International Symposium on Information Theory (ISIT'2008)*, Toronto, Canada, Jul. 2008, pp. 384–388.

[44] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. International Symposiumon on Information Theory (ISIT'2008)*, Nice, France, Jul. 2008, pp. 524–528.

[45] A. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[46] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. International Symposiumon on Information Theory (ISIT'2005)*, Adelaide, Australia, Sept. 2005, pp. 2152–2155.

[47] A. Khisti and G. Womell, "Secure transmission with multiple antennas Part I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[48] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conference on Information Sciences and Systems (CISS'2007)*, Baltimore, MD, Mar. 2007, pp. 905 –910.

[49] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. International Symposiumon on Information Theory (ISIT'2007)*, Nice, France, Jun. 2007, pp. 2466–2470.

[50] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

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

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

[53] A. Khisti and G. Womell, "Secure transmission with multiple antennas Part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

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

[55] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, no. 3, p. 12351249, Mar. 2009.

[56] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP J. Wireless Communications and Networking*, pp. 1–8, 2009.

[57] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, pp. 762–771, Mar. 2011.

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

[59] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer," *EURASIP Journal on Wireless Communications and Networking (Special Issue on Wireless Physical Layer Security)*, Jun 2009.

[60] I. W. P. L. S. via Cooperating Relays, "L. dong and z. han and a. p. petropulu and h.v. poor," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[61] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical layer security," in *Proc. IEEE Conference on Information Sciences and Systems (CISS'2010)*, Princeton, NJ, US, Mar. 2010, pp. 1–6.

[62] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 818–830, Sep. 2011.

[63] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[64] Y. Pei, Y. Liang, L. Zhang, K. Teh, and K. Li, "Secure communication over MISO cognitive radio channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[65] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[66] J. Zhang and M. C. Gursoy, "Secure relay beamforming over cognitive radio channels," in *Proc. IEEE Conference on Information Sciences and Systems (CISS'2011)*, Baltimore, MD, US, Mar. 2011, pp. 1–5.

[67] K. Lee, O. Simeone, C. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," in *Proc. IEEE International Conference on Communications Workshops (ICC'2011)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[68] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[69] J. Zhu, R. Schober, and V. Bhargava, "Secure transmission in multi-cell massive MIMO systems," in *Proc. IEEE Globecom Workshops (GC Workshps'2013)*, Atlanta, GA, US, Dec. 2013, pp. 1286–1291.

[70] ——, "Secrecy analysis of multi-cell massive MIMO systems with RCI precoding and artificial noise transmission," in *Proc. International Symposium on Communications, Control and Signal Processing (ISCCSP'2014)*, Athens, Greece, May 2014, pp. 101–104.

[71] Y. Long, Z. Chen, L. Li, and J. Fang, "Non-asymptotic analysis of secrecy capacity in massive MIMO system," in *Proc. IEEE International Conference on Communications Workshops (ICC'2015)*, London, UK, Jun. 2015, pp. 4587–4592.

[72] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE International Symposiumon on Information Theory (ISIT'2007)*, Nice, France, Jul. 2007, pp. 1296–1300.

[73] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[74] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting with multiuser diversity," in *Proc. 44th Allerton Conference on Communication, Control, and Computing*, Monticello, IL,US, Sep. 2006.

[75] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[76] J. Li and A. P. Petropulu, "On ergodic secrecy rate for gaussian MISO wiretap channels," *IEEE Transactions on Signal Processing*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

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

[78] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.

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

[80] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[81] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

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

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

[84] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Proc. IEEE Wireless Communications Symposium (ICC'2010)*, Cape Town, South Africa, Jun. 2010, pp. 1–5.

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

[86] K.-S. Hwang and M. Ju, "Secrecy outage probability of amplify-and-forward transmission with multi-antenna relay in presence of eavesdropper," in *Proc. IEEE Wireless Communications Symposium (ICC'2014)*, Sydney, Australia, Jun. 2014, pp. 5408–5412.

[87] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation," in *Proc. Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR'2011)*, Pacific Grove, CA, US, Nov. 2011, pp. 952–957.

[88] ——, "On the secrecy capacity of the wiretap channel under imperfect main channel estimation," *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3652–3664, Sep. 2014.

[89] M. Bloch and J. Laneman, "Information-spectrum methods for information-theoretic security," in *Proc. IEEE Information Theory and Applications Workshop (ITA'2009)*, San Diego, CA,US, Feb. 2009, pp. 23–28.

[90] ——, "Exploiting partial channel state information for secrecy over wireless channels," *IEEE Journal on Selected Areas of Communication*, vol. 31, no. 9, pp. 1840–1849, Sep. 2013.

[91] A. Hyadi, Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the broadcast wiretap channel with imperfect channel state information," in *IEEE Global Communications Conference (GLOBECOM'2014)*, Austin, TX , US, Dec. 2014, pp. 1608–1613.

[92] ——, "Secure broadcasting with imperfect channel state information at the transmitter," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2215–2230, Mar. 2016.

[93] X. Chen and H.-H. Chen, "Physical layer security in multi-cell MISO downlinks with incomplete CSIa unied secrecy performance analysis," *IEEE Transactions on Signal Processing*, vol. 62, no. 23, pp. 6286–6297, Dec. 2014.

[94] Z. Rezki, B. Alomair, and M.-S. Alouini, "On the secrecy capacity of the MISO wiretap channel under imperfect channel estimation," in *Proc. IEEE Global Communications Conference (GLOBECOM2014)*, Austin, TX, USA, Dec. 2014, pp. 1602–1607.

[95] X. Zhou, Z. Rezki, B. Alomair, and M.-S. Alouini, "Achievable rates of secure transmission in gaussian MISO channel with imperfect main channel estimation," in *Proc. IEEE Globecom Workshops (GC Wkshps'2015)*, San Diego, CA, US, Dec. 2015, pp. 1–6.

[96] ——, "Achievable rates of secure transmission in gaussian MISO channel with imperfect main channel estimation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4470–4485, Jun. 2016.

[97] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[98] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–360, Jan. 2011.

[99] A. Al-nahari, "Physical layer security using massive multiple-input and multiple-output: passive and active eavesdroppers," *IET Communications*, vol. 10, no. 1, pp. 50–56, 2016.

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

[101] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Transactions on Signal Processing*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[102] D. Love, R. Heath, V. Lau, D. Gesbert, B. Rao, and M. Andrews, "An overview of limited feedback in wireless communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 8, pp. 1341–1365, Oct. 2008.

[103] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the ergodic secret message capacity of the wiretap channel with finite-rate feedback," in *Proc. IEEE International Symposium on Information Theory (ISIT'2012)*, Cambridge, MA, US, Jul. 2012, pp. 239–243.

[104] ——, "Ergodic secret message capacity of the wiretap channel with finite-rate feedback," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3364–3379, Jun. 2014.

[105] A. Hyadi, Z. Rezki, and M.-S. Alouini, "On the secrecy capacity of the broadcast wiretap channel with limited CSI feedback," in *IEEE Information Theory Workshop (ITW'2016)*, Cambridge, UK, Sep. 2016.

[106] ——, "On the secrecy capacity region of the block-fading BCC with limited CSI feedback," in *IEEE Global Communications Conference (Globecom'2016)*, Washington, DC, US, Dec. 2016.

[107] Y.-L. Liang, Y.-S. Wang, T.-H. Chang, Y.-W. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise," in *Proc. IEEE International Symposiumon on Information Theory (ISIT'2009)*, Seoul, Korea, Jun. 2009, pp. 2351–2355.

[108] S.-C. Lin, T.-H. Chang, Y.-W. Hong, and C.-Y. Chi, "On the impact of quantized channel direction feedback in multiple-antenna wiretap channels," in *Proc. IEEE Wireless Communications Symposium (ICC'2010)*, Cape Town, South Africa, May 2010, pp. 1–5.

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

[110] T. Tsiligkaridis, "Secure MIMO communications under quantized channel feedback in the presence of jamming," *IEEE Transactions on Signal Processing*, vol. 62, no. 23, pp. 6265–6275, Dec. 2014.

[111] H.-M. Wang, C. Wang, and D. W. K. Ng, "Articial noise assisted secure transmission under training and feedback," *IEEE Transactions on Signal Processing*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[112] S. Liu, Y. Hong, and E. Viterbo, "Guaranteeing positive secrecy capacity for MIMOME wiretap channels with finite-rate feedback using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4193–4203, Aug. 2015.

[113] D. J. Love, R. W. Heath, and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

[114] A. Hyadi, Z. Rezki, and M.-S. Alouini, "On the secrecy capacity of the multiple-antenna wiretap channel with limited CSI feedback," in *Proc. IEEE Global Communications Conference (Globecom'2015)*, San Diego, CA, US, Dec. 2015, pp. 1–6.

[115] S. Lloyd, "Least squares quantization in PCM," *IEEE Transactions on Information Theory*, vol. IT-28, no. 2, pp. 129–137, Mar. 1982.

[116] X. Chen and R. Yin, "Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback," *IEEE Wireless Communications Letters*, vol. 2, no. 5, pp. 503–506, Oct. 2013.

[117] Z. Peng, W. Xu, J. Zhu, H. Zhang, and C. Zhao, "On performance and feedback strategy of secure multiuser communications with MMSE channel estimate," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1602–1616, Feb. 2016.

[118] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Communications Letters*, vol. 17, no. 5, pp. 864–867, May 2013.

[119] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Transactions on Forensics and Security*, vol. 10, no. 11, pp. 2435–2446, Nov. 2015.

[120] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Transactions on Communications*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[121] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai, "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5244–5256, Sep. 2013.

[122] A. Zaidi, Z. H. Awan, S. Shamai, and L. Vandendorpe, "Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSIT," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1760–1774, Nov. 2013.

[123] S. Lashgari and A. S. Avestimehr, "Blind wiretap channel with delayed CSIT," in *Proc. IEEE International Symposium on Information Theory (ISIT'2014)*, Honolulu, HI, US, Jul. 2014, pp. 36–40.

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

[125] P. Mukherjee and S. Ulukus, "Fading wiretap channel with no CSI anywhere," in *Proc. IEEE International Symposium on Information Theory (ISIT'2013*, Istanbul, Turkey, Jul. 2013, pp. 1347–1351.

[126] P.-H. Lin and E. Jorswieck, "On the fast fading gaussian wiretap channel with statistical channel state information at the transmitter," *IEEE Transactions on Informtion Forensics and Security*, vol. 11, no. 1, pp. 46–58, Jan. 2016.

[127] Y. Liang, L. Lai, H. Poor, and S. Shamai, "A broadcast approach for fading wiretap channels," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 842–858, Feb. 2014.

[128] S.-C. Lin and P.-H. Lin, "On secrecy capacity of fast fading multiple-input wiretap channels with statistical CSIT," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 414–419, Feb. 2013.

[129] 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 Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2655–2668, May 2015.

[130] G. Brante, H. Alves, R. D. Souza, and M. Latva-aho, "Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter," *IEEE Transactions on Communications*, vol. 63, no. 4, pp. 1330–1342, Apr. 2015.

[131] P. C. Pinto, J. Barros, and M. Z.Win, "Secure communication in stochastic wireless networks - part I: Connectivity," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[132] ——, "Secure communication in stochastic wireless networks - part II: Maximum rate and collusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.