Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey

Amitav Mukherjee, *Member, IEEE,* S. Ali A. Fakoorian, *Student Member, IEEE,* Jing Huang, *Member, IEEE,* and A. Lee Swindlehurst, *Fellow, IEEE*

***Abstract*—This paper provides a comprehensive review of the domain of physical layer security in multiuser wireless networks. The essential premise of physical layer security is to enable the exchange of confidential messages over a wireless medium in the presence of unauthorized eavesdroppers, without relying on higher-layer encryption. This can be achieved primarily in two ways: without the need for a secret key by intelligently designing transmit coding strategies, or by exploiting the wireless communication medium to develop secret keys over public channels. The survey begins with an overview of the foundations dating back to the pioneering work of Shannon and Wyner on information-theoretic security. We then describe the evolution of secure transmission strategies from point-to-point channels to multiple-antenna systems, followed by generalizations to multiuser broadcast, multiple-access, interference, and relay networks. Secret-key generation and establishment protocols based on physical layer mechanisms are subsequently covered. Approaches for secrecy based on channel coding design are then examined, along with a description of inter-disciplinary approaches based on game theory and stochastic geometry. The associated problem of physical layer message authentication is also briefly introduced. The survey concludes with observations on potential research directions in this area.**

***Index Terms*—Physical layer security, Information-theoretic security, wiretap channel, secrecy, artificial noise, cooperative jamming, secret-key agreement**

I. INTRODUCTION

The two fundamental characteristics of the wireless medium, namely *broadcast* and *superposition*, present different challenges in ensuring reliable and/or secure communications in the presence of adversarial users. The broadcast nature of wireless communications makes it difficult to shield transmitted signals from unintended recipients, while superposition can lead to the overlapping of multiple signals at the receiver. As a consequence, adversarial users are commonly modeled either as (1) an unauthorized receiver that tries to extract information from an ongoing transmission without being detected, or (2) a malicious transmitter (*jammer*) that tries to degrade the signal at the intended receiver [1]-[3].

A. Mukherjee is with the Wireless Systems Research Lab of Hitachi America, Ltd., Santa Clara, CA 95050, USA (e-mail: amitav.mukherjee@hal.hitachi.com).

S. A. A. Fakoorian is with Qualcomm Corporate R&D, San Diego, CA 92121, USA (email: afakoori@uci.edu).

J. Huang is with Qualcomm Technologies Inc., Santa Clara, CA 95051, USA (e-mail: jinghuang@qti.qualcomm.com).

A. L. Swindlehurst is with the Center for Pervasive Communications and Computing, University of California, Irvine, CA 92697-2625, USA (e-mail: swindle@uci.edu).

This work was supported by the National Science Foundation under grant CCF-1117983.

While jamming and counter-jamming physical layer strategies have been of long-standing interest especially in military networks, the security of data transmission has traditionally been entrusted to key-based enciphering (cryptographic) techniques at the network layer [4]. However, in dynamic wireless networks this raises issues such as key distribution for symmetric cryptosystems, and high computational complexity of asymmetric cryptosystems. More importantly, all cryptographic measures are based on the premise that it is computationally infeasible for them to be deciphered without knowledge of the secret key, which remains mathematically unproven. Ciphers that were considered virtually unbreakable in the past are continually surmounted due to the relentless growth of computational power. Thus, the vulnerability shown by many implemented cryptographic schemes [5]–[7], the lack of a fundamental proof that establishes the difficulty of the decryption problem faced by adversaries, and the potential for transformative changes in computing motivate security solutions that are provably unbreakable.

After some initial theoretical studies by Wyner and Maurer, aspects of secrecy at the *physical layer* have experienced a resurgence of interest only in the past decade or so. Therefore, the remainder of this paper is devoted to surveying and reviewing the various aspects of physical layer security in modern wireless networks. The fundamental principle behind physical layer security is to exploit the inherent randomness of noise and communication channels to limit the amount of information that can be extracted at the 'bit' level by an unauthorized receiver. More importantly, no limitations are assumed for the eavesdropper in terms of computational resources or network parameter knowledge, and the achieved security can be quantified precisely. With appropriately designed coding and transmit precoding schemes in addition to the exploitation of any available channel state information, physical layer security schemes enable secret communication over a wireless medium without the aid of an encryption key. However, if it is desirable to use a secret key for encryption, then information-theoretic security also describes techniques that allow for the evolution of such a key over wireless channels that are observable by the adversary. Thus, information-theoretic security is now commonly accepted as the strictest form of security. Additionally, since they can operate essentially independently of the higher layers, physical layer techniques can be used to augment already existing security measures. Such a multilayered approach is expected to significantly enhance the security of modern data networks, whether wired or wireless.

Instead of proceeding in a strictly chronological order, we aim to provide a high-level overview of the historical development of the field along with the most pertinent references, juxtaposed with recent and ongoing research efforts. The foundations of single and multi-antenna wiretap channels are treated with some emphasis on the mathematical aspects, in order to facilitate the understanding of advanced multi-user networks. The term physical layer security will be used to encompass both signal processing and information-theoretic treatments of the topic.

The remainder of the article is organized as follows. In the next section, the fundamental mathematical precepts of secrecy are presented, along with a description of the most elementary secrecy problem: the wiretap channel. The state-of-the-art in the burgeoning area of multi-antenna wiretap channels is described in Section III. The extension to more than three terminals for broadcast, multiple-access, and interference channels is described in Section IV. The development of secrecy in relay channels and other cooperative scenarios is carried out in V. The important issue of secret-key generation and agreement in wireless networks is studied in Section VI. Section VII highlights the emerging areas of practical security based on error-correcting codes. The penultimate section covers cross-disciplinary approaches to secrecy based on game theory and stochastic geometry, miscellaneous systems such as sensor and cognitive radio networks, along with physical layer message authentication. Finally, in Section IX we summarize our discussion and provide a broad picture of future research directions. Readers interested in going beyond the treatment of physical layer security offered in this paper are referred to the recent monographs [8]-[12].

II. Fundamentals

The simplest network where problems of secrecy and confidentiality arise is a three-terminal system comprising a transmitter, the intended (legitimate) receiver, and an unauthorized receiver, wherein the transmitter wishes to communicate a private message to the receiver. In the sequel, the unauthorized receiver is referred to interchangeably as an *eavesdropper* or *wiretapper*. The vast majority of physical layer security research reviewed in this survey contains the premise that the eavesdropper is passive, i.e., does not transmit in order to conceal its presence. The knowledge available to the transmitter regarding the eavesdropper's channel state information (CSI) plays a critical role in determining the corresponding optimal transmission scheme. Due to uncertainties regarding the location of eavesdroppers, this knowledge may range from a complete lack of CSI, to partial and statistical CSI, and all the way to complete CSI, as discussed in detail in the current and next section. Furthermore, knowledge of the statistical distributions of the eavesdropper spatial locations may also be beneficial, as discussed further in Sec. VIII-C.

Encryption of messages via a secret key known only to the transmitter and intended receiver has been the traditional route to ensuring confidentiality. In the early 20th century, the design of cryptographic methods was based on the notion of computational security, without a solid mathematical basis for secrecy. A classical example was Vernam's one-time pad cipher [13], where the binary message or plaintext is XOR'ed with a random binary key of the same length.

A. Performance Metrics

Shannon postulated the information-theoretic foundations of modern cryptography in his ground-breaking treatise of 1949 [14]. Shannon's model assumed that a non-reusable private key K is used to encrypt the confidential message M to generate the cryptogram C, which is then transmitted over a noiseless channel. The eavesdropper is assumed to have unbounded computational power, knowledge of the transmit coding scheme, and access to an identical copy of the signal at the intended receiver. The notion of perfect secrecy was introduced, which requires that the *a posteriori* probability of the secret message computed by the eavesdropper based on her received signal be equal to the *a priori* probability of the message. In other words, perfect secrecy implies

$$I(M;C) = 0, \tag{1}$$

where $I(\cdot;\cdot)$ denotes mutual information. A by-product of this analysis was that perfect secrecy [15] can be guaranteed only if the secret key has at least as much entropy as the message to be encrypted (generally equivalent to the key and plaintext being of equal length [16]), i.e., $H(K) \geq H(M)$, which validated Vernam's one-time pad cipher system. In subsequent years, it became common practice to use the nomenclature Alice, Bob, and Eve to refer to the legitimate transmitter, intended receiver, and unauthorized eavesdropper, respectively.

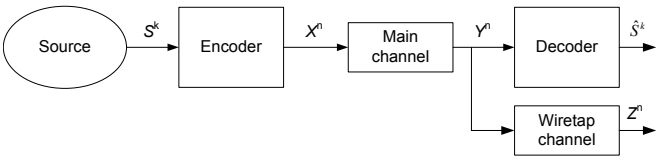


Fig. 1: The wiretap channel of Wyner [17], where the eavesdropper's discrete memoryless channel is degraded relative to the main channel.

Wyner ushered in a new era in information-theoretic security when he introduced the wiretap channel in [17], which considered the imperfections introduced by the channel. Here, the information signal X is transmitted to the intended receiver Bob over the 'main channel' which is modeled as a discrete memoryless channel. The receiver observes Y, which subsequently passes through an additional 'wiretap channel' before being received by the eavesdropper as Z, as shown in Fig. 1.

Under the assumption that the source-wiretapper link is a probabilistically degraded version of the main channel [16], Wyner sought to maximize the transmission rate R in the main channel while making negligible the amount of information leaked to the wiretapper. More specifically, the transmitter has a single message W, which is uniformly distributed over $\{1, ..., 2^{nR}\}$, where R is the *rate* of communication and n is the block length of communication. The goal of the transmitter is to deliver W reliably to the legitimate receiver while keeping

it secure from the eavesdropper. In the classical work of [17], for every $\epsilon > 0$ it is required that

$$R_e - \epsilon \leq \frac{1}{n} H(W \mid Z^n) \tag{2}$$

for sufficiently large n, where R_e represents the uncertainty of message W or the *equivocation* at the eavesdropper [18]. The *capacity-equivocation* region is then the set of rate-equivocation pairs $(R\,,\, R_e)$ that can be achieved by any coding scheme.

It is noted that $R - R_e = \frac{1}{n} I(W; Z^n)$ represents the information that is leaked to the eavesdropper. Thus, when the equivocation rate R_e is arbitrarily close to the information rate R, message W is asymptotically *perfectly* secure from the eavesdropper, i.e., [18]

$$\frac{1}{n} I(W; Z^n) \leq \epsilon\,. \tag{3}$$

Under the asymptotic perfect secrecy constraint (3), the maximum rate of communication R is called the *secrecy capacity* of the wiretap channel. Also, it should be clear that the capacity of the direct link, without secrecy constraints, is the maximum rate R in the capacity-equivocation region regardless of the value of R_e and the secrecy constraint (2). This way, one induces maximal equivocation at the wiretapper, and Wyner was able to show that secure communication was possible *without* the use of a secret key. Strictly speaking, Wyner's definition of "perfect secrecy" as the scenario in which the block-length-normalized mutual information at the eavesdropper vanishes in the limit of long block lengths was weaker than that proposed by Shannon [cf. (1)], which requires that the mutual information be zero regardless of the block length and is also known as strong secrecy [20].

More recently, the study of secrecy in fading channels has led to the use of outage probability performance metrics. Outage metrics for physical layer security are defined analogously to the conventional rate outage metrics, for e.g., the secrecy outage probability is the likelihood that the instantaneous secrecy rate R_s is below a pre-defined threshold ε for a particular fading distribution [19]:

$$P_{out} = \Pr\{R_s < \varepsilon\}\,,\ \varepsilon > 0.$$

Furthermore, security approaches based on signal processing methods often make use of more traditional performance metrics by designing transmission schemes that restrict the bit error rate (BER) or signal-to-interference-plus-noise ratio (SINR) at eavesdroppers to pre-defined thresholds. Note that constraining the BER or SINR at eavesdroppers does not satisfy either weak or strong secrecy requirements, but can often simplify system design.

In 1993, Maurer [21] presented a strategy that allowed a positive rate even when the wiretapper observes a "better" channel than the one used by the legitimate users. The essence of Maurer's scheme was the joint development of a secret key by the transmitter and receiver via communication over a public (insecure) and error-free feedback channel. Thereafter, research in information-theoretic secrecy developed along two main branches: secret key-based secrecy as in the work by Shannon and Maurer, and keyless security as in the work by Wyner. In Section II-B to Section V we trace the evolution of keyless security over the past four decades. We revisit the topic of key-based security for wireless channels in Section VI.

B. Single-Antenna Wiretap Channels Since Wyner

Early work in the field generally assumed non-fading channels, and knowledge of the (fixed) channel state was presumed at the transmitter. In [22], bounds on the equivocation rate for Wyner's wiretap channel model with finite code block lengths are derived. Carleial and Hellman [23] considered a special case of Wyner's model where the main channel is noiseless and the wiretap channel is a binary symmetric channel, and analyzed the applicability of systematic linear codes for preserving the secrecy of an arbitrary portion of the transmitted message. For the degraded wiretap channel [24] with additive Gaussian noise, and C_M and C_W as the Shannon capacities of the main and wiretap channels, the essential result for the secrecy capacity C_S was the following:

$$C_S = C_M - C_W. \tag{4}$$

Ultimately, it was established that a non-zero secrecy capacity can only be obtained if the eavesdropper's channel is of lower quality than that of the intended recipient.

Csiszàr and Körner considered a more general (non-degraded) version of Wyner's wiretap channel in [25], where they obtained a single-letter characterization of the achievable {private message rate, equivocation rate, common message rate}-triple for a two-receiver broadcast channel. For the special case of no common messages, the secrecy capacity was defined as

$$C_S = \max_{V \to X \to YZ} I\,(V;Y) - I\,(V;Z)\,, \tag{5}$$

which is achieved by maximizing over all joint probability distributions such that a Markov chain V, X, YZ is formed, where V is an auxiliary input variable. In [26] it was shown that the availability of non-causal side information at the encoder can enhance the achievable secrecy rate region of (5), based on dirty-paper coding arguments.

In [27], Ozarow and Wyner studied the type-II wiretap channel, where the main communication channel is noiseless but the wiretapper has access to an arbitrary subset μ of the N coded bits, and optimal tradeoffs between code rate k/N and μ that guaranteed secrecy were characterized.

The consideration of channel fading in wiretap channels has recently opened new avenues of research. Works in this area generally assume that at least the statistics of the eavesdropper's fading channel are known to the transmitter. Barros and Rodrigues *et al.* [19]-[28] analyzed the outage probability and outage secrecy capacity of slow fading channels and showed that with fading, information-theoretic security is achievable even when the eavesdropper has a better average SNR than the legitimate receiver.

Li *et al.* [29] examined the achievable secrecy rate for an AWGN main channel and a Rayleigh fading eavesdropper's channel with additive Gaussian noise, assuming that the eavesdropper channel realizations are unknown to legitimate transmitter Alice and receiver Bob. The main result of this

paper was that with Gaussian random codes, artificial noise injection and power bursting, a positive secrecy rate is achievable even when the main channel is arbitrarily worse than the eavesdropper's average channel. A more exotic scenario was studied in [30] where the source has a stochastic power supply based on energy harvesting. Here, the i.i.d. energy arrivals are equated to channel states that are known causally to the source, and the optimal input distribution that attains the boundary of the capacity-equivocation region of the Gaussian wiretap channel was derived. Here, the capacity corresponds to the reliability of the main channel, while the equivocation refers to the normalized conditional entropy at the eavesdropper as described in Sec. II.

Relatively fewer studies consider the case of a complete absence of eavesdropper CSI at the transmitter in fading wiretap channels. In [31], the authors considered a block-fading scalar wiretap channel where the number of channel uses within each coherence interval is large enough to invoke random coding arguments. This assumption is critical for their achievable coding scheme which attempts to "hide" the secure message across different fading states. A recent approach towards understanding the information-theoretic limits of wiretap channels with no eavesdropper CSI has been taken by studying the compound wiretap channel [32]. The compound wiretap channel captures the situation in which there is no or incomplete CSI at the transmitter by assuming the eavesdropper's channel is always drawn from a finite, known set of states, and guarantees secure communication under any state that may occur.

III. Multi-antenna Channels

The explosion of interest in multiple-input multiple-output (MIMO) systems soon led to the realization that exploiting the available spatial dimensions could also enhance the secrecy capabilities of wireless channels. In a fading MIMO channel where the transmitter, receiver, and eavesdropper are equipped with N_T, N_R, N_E antennas respectively as in Fig. 2, a general representation for the signals received by the legitimate receiver and passive eavesdropper are

$$\begin{aligned} \mathbf{y}_b &= \mathbf{H}_b \mathbf{x}_a + \mathbf{n}_b \\ \mathbf{y}_e &= \mathbf{H}_e \mathbf{x}_a + \mathbf{n}_e, \end{aligned} \tag{6}$$

where $\mathbf{x}_a \in \mathbb{C}^{N_T \times 1}$ is the transmit signal with covariance matrix $E\left\{\mathbf{x}_a \mathbf{x}_a^H\right\} = \mathbf{Q}_x$, average power constraint $\mathrm{Tr}\left(\mathbf{Q}_x\right) \leq P$, $\mathbf{H}_b \in \mathbb{C}^{N_R \times N_T}, \mathbf{H}_e \in \mathbb{C}^{N_E \times N_T}$ are the MIMO complex Gaussian channel matrices, and $\mathbf{n}_b, \mathbf{n}_e$ are zero-mean complex white Gaussian additive noise vectors.

The work by Hero [33] was arguably the first to consider secret communication in a MIMO setting, and sparked a concerted effort to apply and extend the single-antenna wiretap theory to this new problem. Hero examined the utility of space-time block coding for covert communications in [33], and designed CSI-informed transmission strategies to achieve either a low probability of intercept (defined in terms of eavesdropper mutual information), or a low probability of detection for various assumptions about the CSI available to the eavesdropper. One of the main results was that if the eavesdropper is completely unaware of its receive CSI, then an equivocation-maximizing strategy is to employ a space-time constellation with a constant spatial inner product.

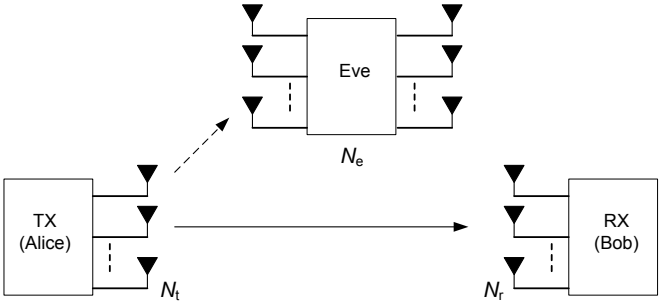


Fig. 2: General MIMO wiretap channel.

Parada and Blahut analyzed a degraded single-input multiple-output (SIMO; $N_T = 1, N_R, N_E > 1$) wiretap channel in [34], and obtained a single-letter characterization of its secrecy capacity by transforming the problem to a scalar Gaussian wiretap channel and then re-applying (4). The authors also proposed a secrecy rate outage metric for the SIMO wiretap channel with slow fading, and observed a secrecy diversity gain of order proportional to the number of receiver antennas. The corresponding multiple-input single-output (MISO) case was studied in [35], [36], where it was noted that the MIMO wiretap channel is not degraded in general. Since this renders a direct computation of (5) difficult, they therefore restricted attention to Gaussian input signals. For the special case of $N_T = 2, N_R = 2, N_E = 1$ analyzed by Shafiee and coworkers in [37], a beamforming transmission strategy was shown to be optimal.

The next steps toward understanding the full-fledged MIMO wiretap channel were taken in [38]-[41], which considered the case of multiple antennas at all nodes and termed it the MIMOME (multiple-input multiple-output multiple-eavesdropper) channel. Khisti *et al*. [38] developed a genie-aided upper bound for the MIMO secrecy capacity for which Gaussian inputs are optimal. When the eavesdropper's instantaneous channel state is known at the transmitter, it was shown that an asymptotically optimal (high SNR) scheme is to apply a transmit precoder based upon the generalized singular value decomposition (GSVD) of the pencil $(\mathbf{H}_b, \mathbf{H}_e)$, which decomposes the system into parallel channels and leads to a closed-form secrecy rate expression. For the so-called MISOME special case where $N_R = 1, N_T, N_E > 1$, the optimal transmit beamformer is obtained as the generalized eigenvector $\boldsymbol{\psi}_m$ corresponding to the largest generalized eigenvalue λ_m of

$$\mathbf{h}_b^H \mathbf{h}_b \boldsymbol{\psi}_m = \lambda_m \mathbf{H}_e^H \mathbf{H}_e \boldsymbol{\psi}_m.$$

If only the statistics of $\mathbf{H}_e$ are known to the transmitter, then the authors proposed an *artificial noise* (AN) injection strategy as first suggested by Goel and Negi [40], [41]. The artificial noise is transmitted in conjunction with the information signal, and is designed to be orthogonal to the intended receiver, such that only the eavesdropper suffers a degradation in channel quality [42], [43]. The transmit signal can be represented in

general as

$$\mathbf{x}_a = \mathbf{T}_a \mathbf{z}_a + \mathbf{T}_n \mathbf{z}_n \tag{7}$$

where precoding matrices $\mathbf{T}_a \in \mathbb{C}^{N_T \times N_T - d}$ and $\mathbf{T}_n \in \mathbb{C}^{N_T \times d}$ correspond to data and AN signal vectors $\mathbf{z}_a \in \mathbb{C}^{N_T - d \times 1}$, $\mathbf{z}_n \in \mathbb{C}^{d \times 1}$, respectively. When $N_T > N_R$, $\mathbf{T}_n$ can be formed from the nullspace of $\mathbf{H}_b$, otherwise $\mathbf{T}_n$ and $\mathbf{T}_a$ can be chosen to guarantee received signals in orthogonal spaces by forming them from the right singular vectors of $\mathbf{H}_b$ [44]. If the eavesdropper's CSIT is partially known, additional gains may be achieved by optimizing the AN transmit covariance [45] or relaxing the orthogonality constraint [46]. As will be seen in the rest of the survey, the use of artificial noise is a recurring theme for secrecy in many different multiuser networks.

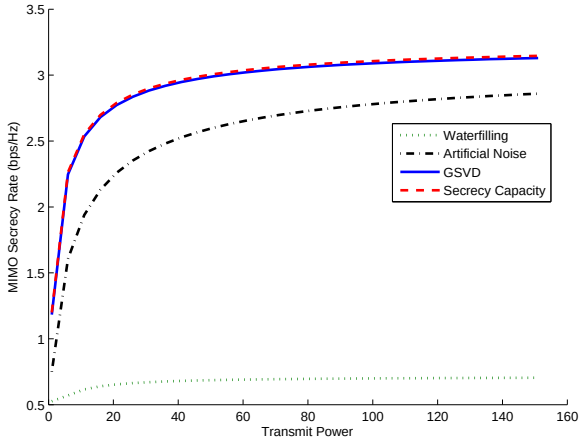


Fig. 3: The MIMO secrecy rates of GSVD-beamforming [42], [61], artificial noise [41], and waterfilling over the main channel, $N_T = N_E = 3, N_R = 2$. Transmit power is in dB, assuming 0dB noise power.

An example of the secrecy rate performance of various transmission strategies for the MIMO wiretap channel is shown in Fig. 3. The GSVD scheme requires instantaneous knowledge of eavesdropper channel $\mathbf{H}_e$, the artificial noise scheme requires the statistics of $\mathbf{H}_e$, and the relatively poor performance of waterfilling on the main channel is also shown when no information is available regarding $\mathbf{H}_e$.

The MIMO wiretap channel was studied independently by Oggier and Hassibi [39], who computed a similar upper bound on the MIMO secrecy capacity, and showed after a matrix optimization analysis that

$$C_S = \max_{\mathbf{Q}_x \succeq 0} \log\det\left(\mathbf{I} + \mathbf{H}_b \mathbf{Q}_x \mathbf{H}_b^H\right) - \log\det\left(\mathbf{I} + \mathbf{H}_e \mathbf{Q}_x \mathbf{H}_e^H\right). \tag{8}$$

In [47], Liu and Shamai reexamine the MIMO wiretap channel with a more general matrix input power-covariance constraint $\mathbf{Q}_x \preceq \mathbf{S}$, and showed that the conjecture of a Gaussian input $U = X$ without prefix coding is indeed an optimal secrecy capacity-achieving choice. Zhang *et al.* attempt to bypass the non-convex optimization of the optimal input covariance matrix by drawing connections to a sequence of convex cognitive radio transmission problems, and obtained upper and lower bounds on the MIMO secrecy capacity [48]. Li and Petropulu [49] computed the optimal input covariance matrix for a MISO wiretap channel, and presented a set of equations characterizing the general MIMO solution.

Bustin and coauthors [50] exploited the fundamental relationship between mean-squared error and mutual information to provide a closed-form expression for the optimal input covariance $\mathbf{Q}_x$ that achieves the MIMO wiretap channel secrecy capacity, again under an input power-covariance constraint. More precisely, it was shown in [50] that, under the matrix power constraint $\mathbf{Q}_x \preceq \mathbf{S}$, the solution of (6) is given by

$$C_{sec}(\mathbf{S}) = \sum_{i=1}^{\lambda} \log \alpha_i \tag{9}$$

where α_i, $i = 1, \ldots, \lambda$, are the generalized eigenvalues of the pencil

$$(\mathbf{S}^{\frac{1}{2}} \mathbf{H}_b^H \mathbf{H}_b \mathbf{S}^{\frac{1}{2}} + \mathbf{I}, \quad \mathbf{S}^{\frac{1}{2}} \mathbf{H}_e^H \mathbf{H}_e \mathbf{S}^{\frac{1}{2}} + \mathbf{I}) \tag{10}$$

that are greater than 1. Note that, since both elements of the pencil (10) are strictly positive definite, all the generalized eigenvalues of the pencil (10) have real positive values [51], [52]. In (9), a total of λ of them are assumed to be greater than 1. Clearly, if there are no such eigenvalues, then the information signal received at the intended receiver is a degraded version of that of the eavesdropper, and in this case the secrecy capacity is zero.

It should be noted that, under the average power constraint $\mathrm{Tr}(\mathbf{Q}_x) \leq P$, there is no computable secrecy capacity expression for the general MIMO case. In fact, for the average power constraint, the secrecy capacity would in principle be found through an exhaustive search over the set $\{\mathbf{S} : \mathbf{S} \succeq 0, \mathrm{Tr}(\mathbf{S}) \leq P\}$. More precisely, we have [51], [83, Lemma 1]

$$C_{sec}(P) = \max_{\mathbf{S} \succeq 0, \mathrm{Tr}(\mathbf{S}) \leq P} C_{sec}(\mathbf{S}) \tag{11}$$

where, for any given semidefinite $\mathbf{S}$, $C_{sec}(\mathbf{S})$ can be computed as given by (9). A closed-form solution is possible in certain special cases, for example when $\mathbf{S}$ is known to be full rank [53], [54], or in the high-SNR regime based on the GSVD [42] as described previously.

Subsequently, numerous research contributions emerged that considered a number of practical issues regarding the MISO/MIMO wiretap channel [56], of which we enumerate a few below:

- Optimal power allocation and beamforming methods for the artificial noise strategy were presented in [57], for the MISO scenario in [58]–[60], and for the GSVD-based precoding scheme in [61].
- If even statistical information regarding the eavesdropper's channel is unavailable, then Swindlehurst *et al.* [44], [55] suggested an approach where just enough power is allocated to meet a target performance criterion (SNR or rate) at the receiver, and any remaining power is used for broadcasting artificial noise, since the secrecy rate cannot be computed at the transmitter. A compound wiretap channel approach and a resultant universal coding scheme that guarantees a positive secrecy rate was presented in [70].

- The effects of imperfect and quantized CSIT of the main (Alice-to-Bob) channel upon the secrecy rate were examined in [62] and [63], respectively, while bounds on secrecy capacity with imperfect CSIT and limited ARQ feedback were given in [64], [65]. MIMOME secrecy rate maximization with imperfect CSIT of all channels was solved using an iterative algorithm in [66] via a Taylor series expansion to convexify the secrecy rate. Discriminatory training methods that include artificial noise for acquisition of main channel CSI while degrading the eavesdropper's estimate of $\mathbf{H}_e$ were analyzed in [67].
- Precoding and receive filter designs to minimize the mean-square error (MSE) at Bob while constraining the MSE at Eve to be above some threshold were given in [68]. Non-linear precoding based on lattices or vector-perturbation ideas with eavesdropper error probability as the metric was examined in [69].
- MIMO secrecy capacity has also been studied for OFDM-based frequency-selective channels [71], [72], Rician fading channels [73], and ergodic [74] channel fading processes. The secrecy outage probability of maximum ratio combining was presented in [75] and of transmit antenna selection in [76]-[78].
- Detection-theoretic methods for discerning the presence of a completely passive eavesdropper based on its local oscillator leakage power were analyzed in [79].
- An evolved full-duplex eavesdropper that can divide its antenna array into sub-arrays for simultaneous eavesdropping and jamming was considered in [80].

A summary of transmission strategies in the MIMO wiretap channel for various assumptions regarding eavesdropper channel state information at the transmitter (ECSIT) is presented in Table I.

TABLE I: Comparison of MIMO wiretap transmission strategies for various ECSIT assumptions

Parameters	**Strategy**	**Criterion**
MIMOME, no ECSIT [44]	Artif. noise	Meet rate target
MIMOME, statistical ECSIT [41]	Artif. noise	Ergodic secrecy rate
MISOME, complete ECSIT [42]	GEVD	Secrecy rate
MIMOME, complete ECSIT [43]	GSVD	Secrecy rate

IV. Broadcast, Multiple-Access, and Interference Channels

A. Broadcast and Multiple-Access Channels

The concept of information-theoretic security is easily extended to larger multi-user networks with more than two receivers and/or transmitters. We begin with one-to-many broadcast channels (BCs), which can be divided into two major categories from a security perspective:

1) BC with confidential messages: each downlink message must be kept confidential from all other unintended receivers, i.e., each receiver is seen as an eavesdropper for messages not intended for it.
2) Wiretap BC: messages do not need to be mutually confidential among the downlink receivers, but must be protected from external eavesdroppers.

The former case is more challenging than the latter, for which the existing transmission techniques of Sec. III can mostly be reused. Therefore, unless stated otherwise the following discussion will assume the first category.

The original wiretap channel as proposed by Wyner [17], is a form of broadcast channel (BC) where the source sends confidential messages to the destination, and attempts to keep the messages as secret as possible from the other receiver(s)/ eavesdropper(s). Csiszàr and Körner extended this work to the case where the source sends common information to both the destination and the eavesdropper, and confidential messages are sent only to the destination [25]. The secrecy capacity region of this scenario, for the case of a BC with parallel independent subchannels, was considered in [81] and the optimal source power allocation that achieves the boundary of the secrecy capacity region was derived. The secrecy capacity region of the MIMO Gaussian broadcast channel with common message to both the destination and the eavesdropper, and confidential message sent only to the destination, was characterized in [82] using a channel enhancement approach [83] and under the matrix input power-covariance constraint $\mathbf{Q}_x \preceq \mathbf{S}$. The notion of an enhanced broadcast channel was first introduced in [83] and was used jointly with the entropy power inequality to characterize the capacity region of the conventional Gaussian MIMO broadcast channel (without secrecy constraint). Most of the current work in the literature on secrecy for the MIMO broadcast channel uses this idea. Moreover, instead of the average total power constraint $\mathrm{Tr}\left(\mathbf{Q}_x\right) \leq P$, they considered the matrix input power-covariance constraint $\mathbf{Q}_x \preceq \mathbf{S}$.

The discrete memoryless broadcast channel with two confidential messages sent to two receivers, where each receiver acts as an eavesdropper for the other, was studied in [84], where inner and outer bounds for the secrecy capacity region were established. This problem was studied in [85] for the MISO Gaussian case and in [51] for the general MIMO Gaussian case. Rather surprisingly, it was shown in [51] that, under the matrix input power-covariance constraint, both confidential messages can be simultaneously communicated at their respected maximum secrecy rates, where the achievability was obtained using dirty-paper coding. To prove this result, Liu *et al*. revisited the MIMO Gaussian wiretap channel and showed that a coding scheme that uses artificial noise and random binning achieves the secrecy capacity of the MIMO Gaussian wiretap channel as well [51].

Consider the broadcast channel represented by (4) and (5), with the addition of independent confidential messages W_1 (intended for receiver 1 but needed to be kept secret from receiver 2) and W_2 (intended for receiver 2 but needed to be kept secret from receiver 1). From [51, Corollary 2], under the matrix constraint $\mathbf{S}$, the secrecy capacity region is given by the set of nonnegative rate pairs (R_1, R_2) such that

$$R_1 \leq \sum_{i=1}^{\lambda} \log \alpha_i; \quad R_2 \leq \sum_{j=1}^{N_T-\lambda} \log \frac{1}{\beta_j} \tag{12}$$

where α_i, $i = 1, \ldots, \lambda$, are the generalized eigenvalues of the pencil (10) that are bigger than 1, and β_j $j = 1, \ldots,(N_T - \lambda)$

are those that are less than or equal to 1.

The secrecy capacity region of MIMO Gaussian broadcast channels with confidential and common messages, where the transmitter has two independent confidential messages and a common message, was characterized in [86]. The achievability was obtained using secret dirty-paper coding, while the converse was proved by using the notion of channel splitting [86]. Secure broadcasting with more than two receivers was considered in [87]–[90] (and references therein). These papers assume one transmitter intends to communicate with several legitimate users in the presence of an external eavesdropper. The secrecy capacity region for the case of two legitimate receivers was characterized by Khandani *et al.* [88] using enhanced channels, and for an arbitrary number of legitimate receivers by Ekrem *et al.* [89]. Ekrem *et al.* use the relationships between minimum-mean-square-error and mutual information, and equivalently, the relationships between Fisher information and differential entropy to provide the converse proof. In [90], Liu *et al.* considered the secrecy capacity regions of the degraded Gaussian MIMO BC with layered confidential messages, where each message must be kept secret from different subsets of receivers. They presented a vector generalization of Costa's Entropy Power Inequality to provide their converse proof. Chia and El Gamal provided inner and outer bounds on the secrecy capacity region of the three-receiver BC with one common and one confidential message in [91], and the extension to additional layered message sets was studied in [92]. The role of artificial noise for jamming eavesdroppers in wiretap broadcast channels was investigated in [93]–[95].

For the average transmit power constraint $\mathrm{Tr}\left(\mathbf{Q}_x\right) \leq P$, a computable secrecy capacity expression is currently unavailable for the general MIMO broadcast channel case. However, optimal solutions based on linear precoding have been found. For example, in [96], a linear precoding scheme was proposed for a general MIMO BC under the matrix covariance constraint. Conditions were derived under which the proposed linear precoding approach is optimal and achieves the same secrecy rate region as S-DPC. This result was then used to derive a closed-form sub-optimal algorithm based on linear precoding for an average power constraint. In [97], GSVD-based beamforming was used for the MIMO Gaussian BC to simultaneously diagonalize the channels. Linear precoding based on regularized channel inversion was studied in [98]–[100] for a multi-antenna downlink where each message must be kept confidential from unintended receivers, and additional external eavesdroppers were assumed present in [101]. User selection in downlink channels with external eavesdroppers was studied in [102]–[107].

Other recent work on secure multi-user communications investigate the multiple-access channel (MAC) with confidential messages [108], [109], the MAC wiretap channel (MAC-WT) [110], [111], and the cognitive MAC with confidential messages [113]. In [108] and [109], two transmitters communicating with a common receiver try to keep their messages secret from each other. For this scenario, the achievable secrecy rate region, and the capacity region for some special cases, are considered.

In [110], the Gaussian multiple access wire-tap channel (GMAC-WT) was considered, where multiple users are transmitting to a base station in the presence an eavesdropper that receives a noisy version of what is received at the base station (degraded wiretapper). In [110], achievable rate regions were found for different secrecy constraints, and it was shown that the secrecy sum capacity can be achieved using Gaussian inputs and stochastic encoders. In [111], [112], a general, not necessarily degraded, Gaussian MAC-WT was considered, and the optimal transmit power allocation that achieves the maximum secrecy sum-rate was obtained. It was shown in [111] that, a user that is prevented from transmitting based on the obtained power allocation can help increase the secrecy rate for other users by transmitting artificial noise to the eavesdropper.

In [113], Liu *et al*. considered the fading cognitive multiple-access channel with confidential messages (CMAC-CM), where two users attempt to transmit common information to a destination while user 1 also has confidential information intended for the destination and tries to keep its confidential messages as secret as possible from user 2. The secrecy capacity region of the parallel CMAC-CM was established and the closed-form power allocation that achieves every boundary point of the secrecy capacity region was derived [113]. It should be noted that all the above work on the MAC with confidential messages assumes single antenna nodes, with little existing work on multiple-antenna scenarios.

B. Interference Channel

The interference channel (IFC) refers to the case where multiple communication links are simultaneously active in the same time and frequency slot, and hence potentially interfere with each other. The IC is generally considered to be the antithesis of a cooperative network, since each transmitter is interested only in selfishly maximizing its own rate, and its message acts as interference to all other links. In conventional IFCs it is generally assumed that each receiver treats the interference from unintended transmitters as noise, but under secrecy constraints this assumption can no longer be made. A special application of the IFC with secrecy constraints is addressed in [114], where the message from only one of the transmitters was considered confidential. The more general case, where each receiver acts as an eavesdropper for the other transmitter, was studied in [84] where, in the absence of a common message, the authors imposed a perfect secrecy constraint and obtained inner and outer bounds for the perfect secrecy capacity region. In [115], the authors analyzed the optimal location of an external eavesdropper so as to drive the secrecy rate of all links to zero, where location is defined logically in terms of channel gains.

Since in most multi-user scenarios it is difficult to obtain the exact secrecy capacity region, there has been recent interest in studying the asymptotic performance of these systems in the high SNR regime. For such networks, a useful metric that captures the scaling behavior of the sum secrecy rate R_Σ as the transmit SNR, ρ, goes to infinity is the number of secure

degrees of freedom (SDoF), which can be defined as

$$\eta \triangleq \lim_{\rho\to\infty} \frac{R_\Sigma(\rho)}{\log(\rho)}.$$

The SDoF of various multiuser networks described in Sections IV-V are summarized in Table II, and generally rely upon the principle of interference alignment (IA) for achievability [116]. For example, the number of secure DoF for K-user Gaussian IFCs ($K \geq 3$) has been addressed in [117], [118], [119], and it was shown that under very strong interference, positive secure DoFs are achievable via IA and channel extension. The $(K \times L)$ X network comprises K transmitters that each wish to communicate with L receivers, and each of the receivers wishes to receive messages from all K transmitters, and the SDoF is achieved via random binning and IA [122].

TABLE II: Secure degrees of freedom in multiuser networks.

Network	Secure DoF
K-user SISO IFC, confidential messages [117]	$\eta = \frac{K-2}{2K-2}$
K-user SISO IFC, external Eve [117]	$\eta = \frac{K-2}{2K}$
K-user SISO MAC, external Eve [120]	$\eta = \frac{K(K-1)}{K(K-1)+1}$
K-helper SISO wiretap, external Eve [121]	$\eta = \frac{K}{K+1}$
$(K \times L)$ X network, confidential messages [122]	$\eta = \frac{L(K-1)}{K+L-1}$

It should be noted that all of the above references [114]-[119] assume single antenna nodes. The more limited set of work that considers the impact of multi-antenna nodes on secrecy in the interference channel include [123]-[125]. In [123], Jorswieck *et al*. studied the achievable secrecy rates of a two-user MISO interference channel, where each receiver has a single antenna. They modeled a non-cooperative game in the MISO interference channel and obtained the Nash equilibrium point using an iterative algorithm. A more unusual formulation was adapted in [126], where a closed-form solution for the NE point was obtained where each multi-antenna transmitter desires to maximize the difference between its secrecy rate and the secrecy rate of the other link.

In [124] and [125], Swindlehurst *et al*. investigated the two-user MIMO Gaussian interference channel with confidential messages, where each node has arbitrary number of antennas. Several cooperative and non-cooperative transmission schemes were described, and their achievable secrecy rate regions were derived. A game-theoretic formulation of the problem was adopted to allow the transmitters to find an operating point that balances network performance and fairness (the so called Kalai-Smorodinsky (K-S) bargaining solution [125]). If the transmitters cooperate by exchanging information about the channels and signal subspaces associated with their link, then a combination of GSVD beamforming and altruistic *artificial noise alignment* by each transmitter to mask the information signal from the other transmitter at its *own* receiver can be used, as seen in Fig. 4. As depicted in the figure, each transmitter intentionally undermines the ability of its receiver to decode the interfering signal; for example, noise $\mathbf{H}_1\mathbf{A}_1$ and interference $\mathbf{G}_2\mathbf{D}_2$ are aligned to lie in the same subspace at receiver 1. Here, the artificial noise can potentially also degrade the confidential message of the transmitter itself, so the transmit signal and power allocated to noise must be carefully designed. It was shown in [125] that, while ordinary jamming is near optimal for the standard wiretap channel [43], its performance is far from optimal for the interference channel. Fig. 4 shows the achievable secrecy rate regions of

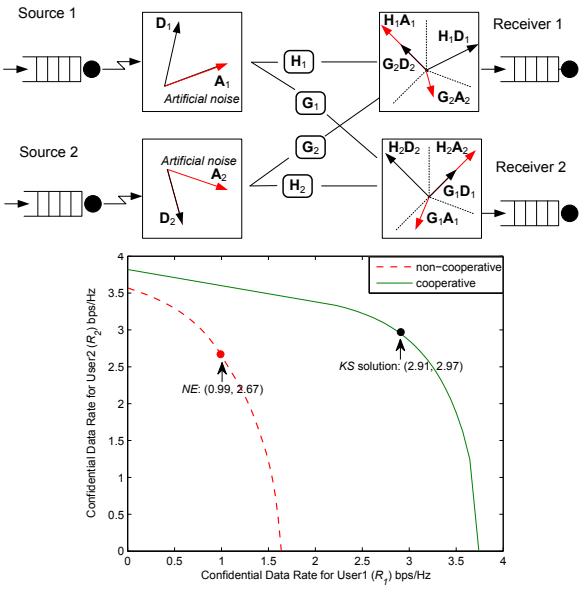


Fig. 4: The cooperative ANA principle in the 2-user MIMO interference channel, and the corresponding secrecy rate region with and without cooperation.

the proposed schemes in [125] with 2 antennas at source 1, 3 antennas at all other nodes, and a transmit SNR of 20 dB, along with the Nash equilibrium (NE) from the non-cooperative GSVD approach, and the clearly superior K-S rate point for the cooperative GSVD and artificial noise alignment method.

V. Relays and Cooperative Methods

The issue of physical layer security in relay and cooperative networks has drawn much attention recently, as a natural extension to the secure transmission problem in non-cooperative networks. The secrecy capacity and achievable secrecy rate bounds have been investigated for various types of relay-eavesdropper channels, and many cooperative strategies stemming from conventional relay systems have been adopted with modifications based on techniques discussed in Sec. III, as shown in Fig. 6. Security issues in relay networks can be divided into two broad categories:

- Relays are untrusted nodes from whom the transmitted messages must be kept confidential even while using them to relay those messages,
- Relays are trusted nodes from whom the transmitted messages need not be kept secret.

A. Untrusted Relays

As a pessimistic assumption, the relay itself can be considered to be an *untrusted* user that acts both as an eavesdropper and a helper, i.e., the eavesdropper is co-located with the relay node as shown in Fig. 5. The source desires to use the relay

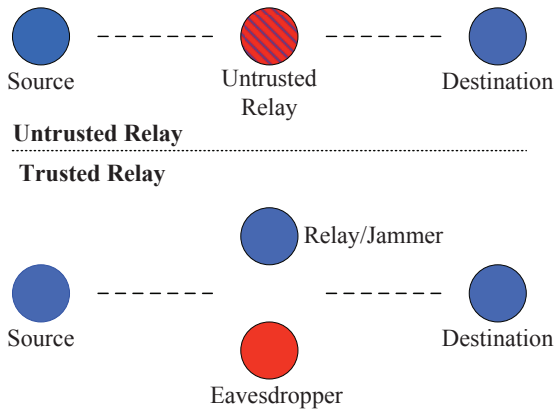
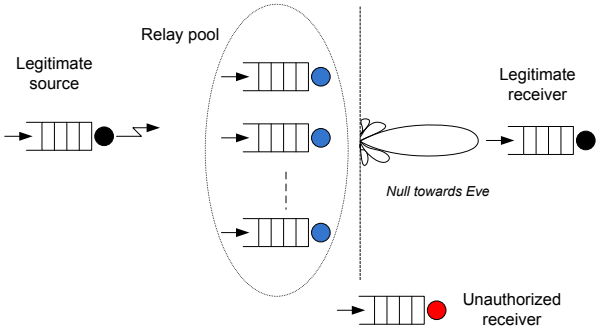
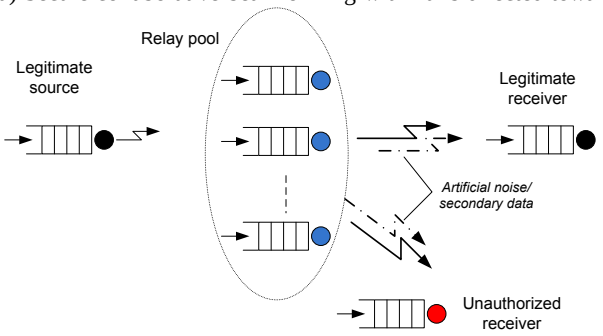


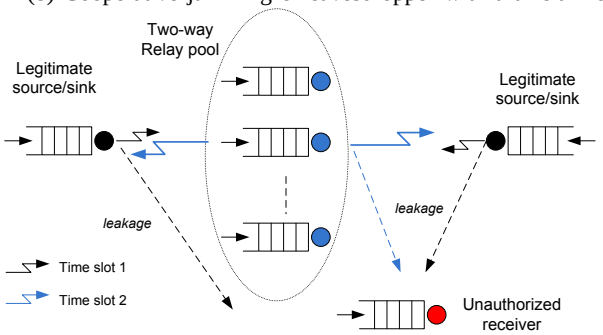
Fig. 5: Representations of trusted (distinct relay and eavesdropper) and untrusted (co-located relay and eavesdropper) relay networks.



(a) Secure collaborative beamforming with nulls directed towards Eve.



(b) Cooperative jamming of eavesdropper with artificial noise.



(c) Two-way relay-aided secret key exchange based on analog network coding.

Fig. 6: Relay-aided cooperative approaches for physical layer security with an external eavesdropper.

to communicate with the destination, but at the same time intends to shield the message from the relay. This type of model was first studied in [128] for the general relay channel. Coding problems associated with the relay-wiretap channel are studied under the assumption that some of transmitted messages are confidential to the relay, and deterministic and stochastic rate regions are explicitly derived in [129]–[131], which showed that cooperation from the untrusted relay is still essential for achieving a non-zero secrecy rate. In [129], an achievable region of rate pairs (R_1, R_e) was derived for the general untrusted relay channel.

Based on this region, the cooperation of an untrusted relay node was found to be beneficial for a specific model where there is an orthogonal link in the second hop. Cooperative relay broadcast channels are discussed in [132], where the users are untrusted but not malicious. In such scenarios, users are willing to help each other, but would not be allowed to decode each other's message. Assuming a half-duplex amplify-and-forward protocol, another effective countermeasure in this case is to have the destination jam the relay while it is receiving data from the source. This intentional interference can then be subtracted out by the destination from the signal it receives via the relay.

In [133], the authors considered the joint source/relay beamforming design problem for secrecy rate maximization, through a one-way untrusted MIMO relay. For the two-way untrusted relay case, [134] proposes an iterative algorithm to solve for the joint beamformer optimization problem, and [135] considers joint optimization for beamformer and untrusted relay node selection. In realistic fading channels, the secrecy outage probability (SOP) is more meaningful compared with the ergodic secrecy rate, which is ill-defined under finite delay constraints. Thus [136] focuses on the secrecy outage probability of the AF relaying protocol, which is chosen due to its increased security vis-à-vis decode-and-forward relaying and its lower complexity compared to compress-and-forward approaches. As in Secs. II-B and III, the SOP indicates the fraction of fading realizations where a secrecy rate R can be supported, and provides a security metric when the source and destination have no CSI for the eavesdropper. The secrecy rate performance of untrusted relay selection was examined in [137]. In [138], a constant BER of 0.5 is maintained at the untrusted relay by revealing to it only the real or imaginary components of the confidential M-ary symbols.

B. Trusted Relays and Helpers

Unlike the aforementioned case, in a *trusted* relay scenario the eavesdroppers and relays are separate network entities. Some of the most commonly encountered relay-based wiretap scenarios and corresponding solutions are depicted in Fig. 6. The relays can play various roles to counteract external eavesdroppers. They may act purely as traditional relays while utilizing help from other nodes to ensure security; they may also act as both relaying components as well as cooperative jamming partners to enhance the secure transmission; or they can assume the role of stand-alone *helpers* to facilitate the jamming of unintended receivers.

A typical model of a relay channel with an external eavesdropper was investigated by Lai *et al.* in [139], where outer-bounds on the optimal rate-equivocation region are derived assuming a classical decode-and-forward protocol. The authors of [139] also propose a novel noise-forwarding strategy where the full-duplex relay sends dummy codewords independent of the secret message in order to confuse the eavesdropper. Such a strategy is also referred to as 'deaf cooperation' in [140], [141].

In [143], [144], several cooperative schemes are proposed for a two-hop multiple-relay network, and the corresponding relay weights are derived to maximize the achievable secrecy rate, under the constraint that the link between the source and the relay is not protected from eavesdropping. The secrecy scaling laws in the limit of a large number of nodes for such a scenario are analyzed in [145]. The extension to a scenario with multiple eavesdroppers and maximum secrecy rate beamforming was pursued in [146]. It was shown in [147] that the decode-and-forward strategy is always outperformed by randomize-and-forward relaying (source and relay use different codebooks) in terms of secrecy outage probability. [147] also discusses where to ideally place the relay. In [148], optimal precoding matrices based on artificial noise alignment are designed for a MIMO relay channel where the source, relay, and destination cooperatively jam an external eavesdropper, while robust relay beamforming was considered in [149]. A combination of source GSVD precoding and relay SVD precoding was adopted in [150] for the MIMO relay wiretap channel. A relay-assisted OFDMA downlink was considered in [151], where the base station and relays jointly optimize the resource allocation for artificial noise versus data. Secrecy rate regions for a generalized relay network with parallel channels between all four terminals are derived in [152]. In [153], the set of relays is optimally divided into actual AF or DF relays and cooperative jammers, under an imperfect CSI assumption. Relay selection is another important issue when multiple relays are available; the optimal selection policy assuming the DF protocol was provided in [154] and shown to be superior to conventional max-min relay selection, while an opportunistic relay selection scheme was shown to have vanishing secrecy outage probability as the number of DF relays grew in [155]. A more general scenario was considered in [156] for AF and DF relays, with single and multiple relay selection schemes and corresponding diversity orders being presented. [157] considered utilizing a buffer-aided relay to enhance both transmission efficiency and security for two-hop relay networks.

Helpers serve as friendly jammers that do not have any information of their own to transmit, but instead cooperate with authorized nodes to degrade the signals intercepted by eavesdroppers. Namely, a helper can send a random codeword at a rate that ensures that it can be decoded and subtracted from the received signal by the intended receiver, but cannot be decoded by the eavesdropper. Alternatively, a helper can transmit a jamming signal that interferes with the ability of the eavesdropper to intercept and decode the desired signal. For example, in a single-antenna wiretap channel with external helpers, an interesting approach is to split the transmission

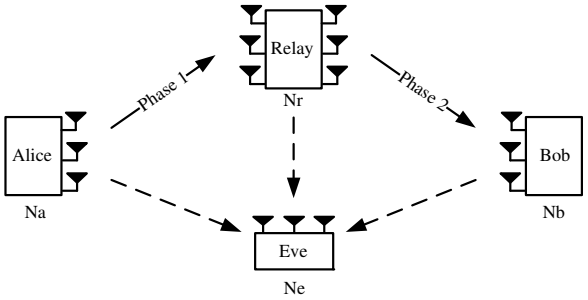


Fig. 7: Two-hop MIMO network with trusted relay and external eavesdropper.

time into two phases. In the first phase, the transmitter and the intended receiver both transmit independent artificial noise signals to the helper nodes. The helper nodes and the eavesdropper receive different weighted versions of these two signals. In the second stage, the helper nodes simply replay a weighted version of the received signal, using a publicly available sequence of weights. At the same time, the transmitter transmits its secret message, while also canceling the artificial noise at the intended receiver [41].

In [158], a wiretap channel with an independent helping jammer was considered. The interferer can send a random codeword at a rate that ensures that it can be decoded and subtracted from the received signal by the intended receiver but cannot be decoded by the eavesdropper. The optimal helper power allocation over parallel OFDM subchannels is derived in [159]. Optimal jamming weights and positions for helpers with mobility are presented in [160]. The effect of CSI feedback delay on relay and helper selection was quantified in [161]. In [162], a MISO scenario with constrained limited feedback of CSI from the receiver was considered, and an adaptive bit-allocation policy was proposed to optimally divide feedback bits between the transmitter and helper channels. The full MIMO scenario with artificial noise jamming by a single multi-antenna helper was analyzed in [163]. The jamming strategy of a multi-antenna helper powered by energy harvesting instead of a regular battery was optimized in [164].

For the proposed coordinated cooperative jamming scheme for MIMO ad hoc networks in [165], when one pair of nodes are communicating with each other, all the nodes surrounding the legitimate receiver cooperate to interfere with the eavesdropper by sending jamming signals. Orthogonal information subspaces and jamming subspaces are broadcast across the network, and artificial noise is chosen to lie in the publicized jamming subspace such that there will be no interference at the destination when an appropriate receive beamformer is used. An uncoordinated cooperative jamming strategy is also proposed for the case where the public jamming subspace is unavailable. In this case, the AN is simply the right singular vector of the main channel corresponding to the smallest singular value. Both schemes have been shown to efficiently increase the secrecy capacity, even if the eavesdropper has knowledge of the associated subspaces. The authors of [166] considered a MISO channel with and without an external helper, and obtained robust beamforming/jamming solutions

via numerical methods for imperfect CSI scenarios.

A more general case where cooperative jamming strategies guarantee secure communication in both hops without the need for external helpers was studied in [167]. In these approaches, the normally inactive nodes in the relay network can be used as cooperative jamming sources to confuse the eavesdropper and provide better performance in terms of secrecy rate. In the proposed cooperative jamming strategies, the source and the destination nodes act as *temporary helpers* to transmit jamming signals during transmission phases in which they are normally inactive. In [168], the source transmits artificial noise along with data in the first hop, in addition to jamming by the destination. Jamming by the destination for the special case of a single-hop system was examined in [169], [170], which is feasible only when the destination has full-duplex capabilities, i.e., it can transmit and receive simultaneously on the same frequency with the aid of self-interference cancelation methods. Returning to [167], two types of cooperative jamming schemes may be defined, *full cooperative jamming* (FCJ) and *partial cooperative jamming* (PCJ), depending on whether or not both the transmitter and the temporary helper transmit jamming signals at the same time. A comparison of these schemes is shown in Fig. 8.

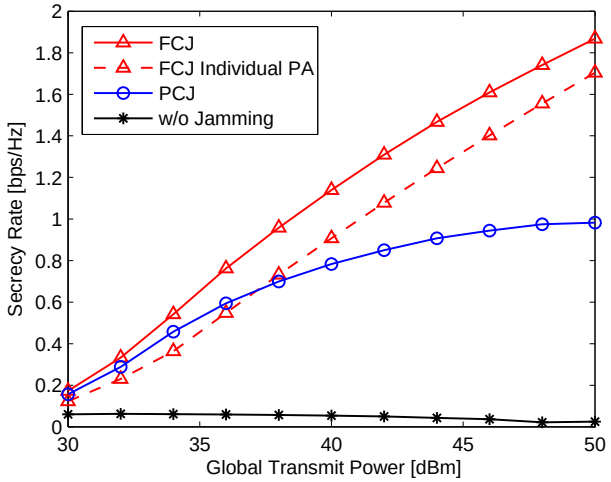


Fig. 8: Secrecy rate versus transmit power in two-hop channel with cooperative jamming, ECSIT unknown, four antennas at all nodes.

In [111], [112], a two-way wiretap channel was considered, in which both the source and receiver transmit information over the channel to each other in the presence of a wiretapper. Achievable rates for the two-way Gaussian channel are derived. In addition, a cooperative jamming scheme that utilizes the potential jammers was shown to be able to further increase the secrecy sum rate. [171] showed that using feedback for encoding is essential in Gaussian full-duplex two-way wiretap channels, while feedback can be ignored in the Gaussian half-duplex two-way relay channel with untrusted relays. More recently, secure transmission strategies are studied for the multi-antenna two-way relay channel with network coding in the presence of eavesdroppers [172]-[175]. By applying the analog network-coded relaying protocol, the end nodes exchange messages in two time slots. In this scenario, the eavesdropper has a significant advantage since it obtains two observations of the transmitted data compared to a single observation at each of the end nodes. As a countermeasure, in each of the two communication phases the transmitting nodes jam the eavesdropper, either by optimally using any available spatial degrees of freedom, or with the aid of external helpers.

VI. Wireless Secret Key Agreement

We recall that the original secure communication system studied by Shannon was based on secret-key encryption. Shannon's result that perfect secrecy required encryption with a random one-time pad cipher at least as long as the message was widely regarded as a pessimistic result, until it was reexamined in the context of noisy channels by Maurer [21]. In his seminal work, Maurer decried Wyner's degraded wiretap channel as being too unrealistic, and instead proposed a secret-key agreement protocol that could be implemented over a noiseless but authenticated and publicly observable two-way channel in the presence of a passive eavesdropper.

The key elements of Maurer's strategy are the *information reconciliation* and *privacy amplification* procedures. The information reconciliation phase is aimed at generating an identical random sequence between Alice and Bob by exploiting a public discussion channel (sometimes split into a separate *randomness sharing* step). The privacy amplification stage extracts a secret key from the identical random sequence agreed to by two terminals in the preceding information reconciliation phase. In other words, after public discussion based on *correlated randomness* in the first stage, privacy amplification reduces an initial piece of random nature into a smaller entity (e.g., by linear mapping and universal hashing) which is known only by the legitimate users, even if the eavesdropper has a less noisy channel in certain cases.

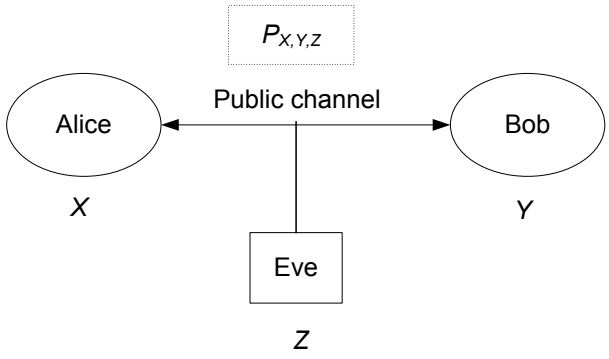


Fig. 9: Secret key agreement by t rounds of public discussion between Alice and Bob. X and Y comprise the source of common randomness; Eve has access to Z and joint distribution $P_{X,Y,Z}$.

More precisely, it was assumed that the transmitter, receiver and adversary have access to repeated independent realizations of random variables $X, Y,$ and Z, respectively, with some globally-known joint probability distribution $P_{X,Y,Z}$ as in Fig. 9. The eavesdropper is completely ignorant of X and Y. Alice and Bob undergo multiple rounds of two-way communication over the public channel, followed by generation of a shared key based on their individual information and

observed messages. The secret-key rate $S(X;Y||Z)$ between X and Y with respect to Z is then defined as the maximal rate at which Alice and Bob can generate a secret key over the noiseless public channel in such a way that the adversary obtains information about this key only at an arbitrarily small rate (cf. (5)). The following upper and lower bounds on the secret key rate were presented in [21]:

$$S\left(X;Y||Z\right) \leq \min\left[I\left(X;Y\right), I\left(X;Y|Z\right)\right], \tag{13}$$

$$S\left(X;Y||Z\right) \geq \max\left[I\left(X;Y\right) - I\left(X;Z\right), I\left(Y;X\right) - I\left(Y;Z\right)\right].$$

Closely related results were offered in the concurrent work by Ahlswede and Csizár [176]. Csiszár and Narayan studied the augmentation of key-based secrecy capacity with the aid of a helper which supplies additional correlated information in [177], and obtained a single-letter characterization of the key-based secrecy capacities with an arbitrary number of terminals in [178]. Maurer and Wolf subsequently extended the secret-key sharing analysis of [21] to account for the presence of an active eavesdropper in [179]-[181], and showed that either a secret key can be generated at the same rate as in the passive-adversary case, or such secret-key agreement is infeasible. Refinements to their model that yield larger key rates are shown in [182]. A two-user interference channel with a noiseless, shared feedback channel from the receivers and corresponding bounds on the secret-key capacity region are studied in [183], while the multiple-access channel was examined in [184].

The next evolution in secret-key sharing was the exploitation of the common randomness inherent in reciprocal wireless communication channels. Koorapaty *et al.* relied on the independence of the channels between transmitter/receiver and transmitter/eavesdropper to use the phase of the fading coefficients as a secret key [185]. Other techniques include key generation via

- discretizing extracted coefficients of the multipath components [186],
- quantizing the channel phases for a multitone communication system such that multiple independent phases are used to generate longer keys [187],
- directly quantizing the complex channel coefficients [188],
- a purposely constructed random variable whose realizations are communicated between the legitimate nodes, with secrecy achieved when the eavesdropper lacks channel state information [189],
- exploiting the level crossing rates of the fading processes at the legitimate terminals [190],
- inducing more rapid fluctuations in channels from which keys are to be extracted via transmit array optimization [191],
- utilization of channel estimates as correlated random variables for information reconciliation [192],
- utilizing appropriately timed one-bit feedback available in practical networks due to Automatic Repeat reQuest (ARQ) protocols [193],
- using unknown deterministic parameters such as wideband multipath channel parameters that are estimated by both Alice and Bob [194]. This is a departure from the common randomness framework of Maurer, and a new notion of intrinsic information is defined accordingly to quantify achievable secret-key lengths.

Not surprisingly, multiple-antenna channels have attracted considerable attention for their capabilities of increasing common randomness at the legitimate users. The MIMO secret-key capacity for Gaussian inputs and system model identical to that of (6) is [195]

$$\begin{aligned} C_{SK} = \max_{\mathbf{Q}_x \succeq 0} & \log\det\left(\mathbf{I} + \mathbf{H}_x\mathbf{Q}_x\mathbf{H}_x^H\right) \\ & - \log\det\left(\mathbf{I} + \mathbf{H}_e\mathbf{Q}_x\mathbf{H}_e^H\right). \end{aligned} \tag{14}$$

where $\mathbf{H}_x^H\mathbf{H}_x = \mathbf{H}_b^H\mathbf{H}_b + \mathbf{H}_e^H\mathbf{H}_e$ is an equivalent channel. Note the similarity to (8), based on which a similar GSVD-based transmission scheme was adopted in [195]. Li and Ratazzi [196] designed a randomized beamforming scheme based on knowledge of the main channel that makes blind channel estimation by the eavesdropper more difficult; the keyless secrecy rate of this method was examined in [197]. Chen and Jensen developed practical key generation protocols for MIMO systems with temporally and spatially correlated channel coefficients in [198], [199]. Some of the first experimental measurement campaigns on secret key generation in reciprocal MIMO channels are presented in [200], [201].

Previously discussed techniques for keyless security can be reutilized to enhance secret-key rates. The cooperative jamming method of [111] was used in [202] as a precursor to secret key establishment over a two-way wiretap channel, and artificial noise was used to enhance secret key rates in a two-way relay network in [203]. From the adversary's perspective, the optimality of Gaussian jamming against secret key establishment in two-way wireless channels was given in [204]. The role of a feedback channel in improving the secrecy rate of a wiretap channel has also been revisited in recent work. For a modulo-additive channel [205], the authors showed that a noisy feedback channel that is observable by all parties can still be utilized to generate a secrecy rate equal to the main channel capacity, since the feedback from the (either full- or half-duplex) receiver acts as a private key that jams the eavesdropper. Ardestanizadeh *et al.* [206] considered a secure but rate-limited feedback channel, and proved that it is optimal for the receiver to feedback a random secret key that is independent of its received channel output symbols.

VII. Code Design for Secrecy

A. Channel Coding

Much like conventional networks, error correction codes play an integral role in building "real-world" secure systems. The McEliece cryptosystem [207], [208] devised in 1978 can now be seen to be a bridge between channel coding-based physical layer security and classical cryptography. In this setup, the size-$(k \times n)$ generator matrix of a (n, k) Goppa (linear) code capable of correcting t errors is multiplied from the left and right by a randomly generated non-singular matrix and permutation matrix respectively, and the size-$(k \times n)$ product is made available as a public key. Messages sent

to this entity are generated using the public key and then perturbed by a random vector of Hamming weight t. The ciphertext is decoded by multiplications with the inverses of the permutation and non-singular matrices interspersed with the code decoding algorithm.

Once the groundwork had been laid for the foundations of information-theoretic security [cf. Sec. II-B], several researchers turned their attention to the development of practical secrecy-preserving channel codes. Wyner [17] and Csiszàr and Körner [25] had used a stochastic coding argument to provide a non-constructive proof of the existence of channel codes that guarantee both robustness to transmission errors and a prescribed degree of data confidentiality as the block length tends to infinity.

In Wyner's stochastic encoding scheme, a mother codebook $C_0(n)$ of length n is randomly partitioned into "secret bins" or subcodes $\{C_1(n), C_2(n), \ldots, C_M(n)\}$. A message w is associated with a sub-code $C_w(n)$ and the transmitted codeword is randomly selected within the sub-code. The mother code $C_0(n)$ provides enough redundancy so that the legitimate receiver can decode the message reliably, whereas each sub-code is sufficiently large and, hence, introduces enough randomness so that the eavesdropper's uncertainty about the transmitted message can be guaranteed. However, the development of practical wiretap codes for general wiretap channels was not as rapid as that of classical error-correction codes in the two decades following Wyner's work.

Therefore, it was natural to turn to known capacity-achieving channel codes and examine their applications for secrecy [209]. In [210], Thangaraj *et al.* advanced the idea of using graph-based codes such as low density parity check (LDPC) codes for binary erasure wiretap channels (noiseless main channel), and showed that both reliability and Wyner's weak secrecy criterion could be satisfied simultaneously. Bloch and coauthors [189] adopted LDPC codes and multi-level coding for the information reconciliation phase of a practical secret key agreement protocol. For Gaussian wiretap channels, appropriately punctured LDPC codes were employed with the relative bit error rate at the receiver and eavesdropper as a proxy security metric in [211], where the authors showed that a 'security gap' was achievable. A turbo code-based scheme with the puncturing pattern determined by a pre-shared secret key was presented in [212], while the achievability of high equivocation rates (cf. (2)) with random puncturing was shown in [213].

Graph-based unstructured codes are not the only viable approach for wiretap coding. He and Yener [214] showed that an arbitrarily large secrecy rate is achievable for Gaussian wiretap channels with an external helper using structured integer and nested lattice codes. Nested lattice codes were also deployed over the binary symmetric wiretap channel in [215]. Arora and Sang presented the notion of dialog codes wherein the receiver aids the transmitter by jamming the eavesdropper while still being able to recover the transmitted symbol [216]. If the receiver is half-duplex, then this can be achieved using a rate-1/2 code with memory where the receiver jams either of the code bits but is able to recover the message from the remaining bit, whereas the equivocation at the eavesdropper is unity. The recently proposed polar coding scheme has been shown to achieve the secrecy capacity for binary symmetric and deterministic wiretap channels [217], [218]. Polar coding was subsequently extended to secret-key generation in [219], and shown to be secret-key capacity-achieving for a binary symmetric channel.

B. Distributed Storage Coding

A recent avenue for coding theory research is the design of resilient codes for distributed data and cloud storage systems. The essence of such systems is that chunks of data files are scattered across various storage nodes, and it is desired that an end-user or data collector be able to accurately reconstruct the original files by retrieving data from a subset of k such storage nodes. However, the storage nodes are assumed to be unreliable and prone to failure (equivalent to data erasures), and thus fault-tolerance to such failures under bandwidth constraints is the primary code design criterion. These considerations lead to the introduction of a new class of 'regenerating codes' which are efficient with respect to both storage space utilization and the amount of data downloaded for repair (termed repair-bandwidth) [224]. In addition to reliability, it is also critical to protect data from being reconstructed by eavesdroppers. A passive eavesdropper that can access the data on up to ℓ storage nodes is denoted a Type-I adversary in [221], and as a Type-II adversary if it can also observe the repair data of ℓ nodes. A typical security scenario is shown in Fig. 10, where $\ell = 2$ out of $k = 4$ storage nodes have been compromised by an eavesdropper that seeks to reconstruct the original file F.

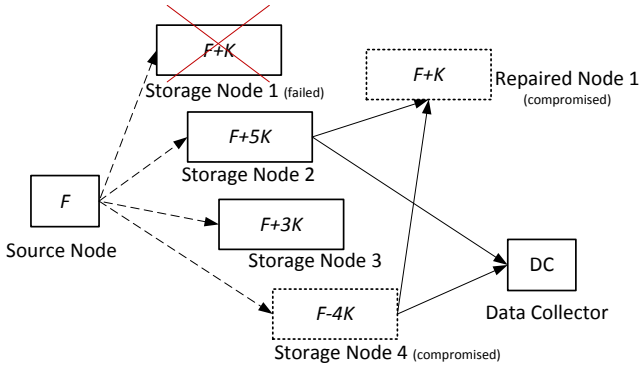


Fig. 10: Security problem in distributed storage network with an eavesdropper that can observe data in compromised nodes.

Pawar *et al.* studied the problem of securing distributed storage systems against eavesdroppers and malicious adversaries in [222], and defined the secrecy capacity $C_s(\alpha, \gamma)$ as the maximum amount of data that can be stored in the system such that the data can be reconstructed reliably while remaining perfectly secret from Eve, for all possible data collectors and eavesdroppers. Their upper bound on the system secrecy capacity for a Type-I adversary turned out to be

$$C_s(\alpha, \gamma) \leq \sum_{i=\ell+1}^{k} \min\left\{(d-i+1)\frac{\gamma}{d}, \alpha\right\}$$

where α is the storage capacity in symbols of each of the k total nodes, and γ is the total amount of data downloaded

for repair by the replacement node from d unaffected storage nodes. The bound verifies the intuition that only the $k-l$ non-compromised nodes can yield secure and reliable information to the data collector. Shah *et al.* constructed secure exact repair codes based on the product-matrix framework in [223], which ensures that the information contained in the symbols downloaded by the replacement node is independent of the identities of the helper nodes. Dikaliotis *et al*. studied the security of distributed storage systems in the presence of a trusted verifier [224]. The maximum file size that can be stored securely was determined for systems in which all the available nodes help with repair in [225]. The single node repair setting was generalized to multiple node failures and secrecy capacity bounds provided for the same in [226]. The characterization of the secure storage-vs-exact-repair-bandwidth tradeoff region under both Type-I and Type-II attacks was given in [221]. For a heterogeneous system with nodes having different storage capacities and different repair bandwidths, lower and upper bounds on the system capacity were given in [227].

C. Network Coding

While the emerging area of network coding is not directly related to traditional channel coding design *per se*, we briefly mention physical layer security issues encountered in this field. Network coding is a paradigm for multi-hop wireline and wireless networks that allows intermediate nodes to 'mix' packets or signals received from multiple paths, with the objective of improving throughput [228]. Therefore, such networks are vulnerable to eavesdropping, akin to other networks discussed thus far in this work.

The secure network coding problem was introduced in [229] for multicast wireline networks where each link has equal capacity, and a wiretapper can observe an unknown set of up to k network links. For this scenario, the secrecy capacity is given by the cut-set bound, and is achieved by injecting k random keys at the source which are decoded at the sink along with the message [229], [230]. Silva and Kschischang [231] among others have drawn connections between the multicast problem and the type-II wiretap channel studied by Ozarow and Wyner, as described in Section II-B. Eavesdropping countermeasures for wireless network coding systems are described in [172], [232], among others. In [173], a distributed version of the randomized transmission scheme of [196] was adopted for a cooperative network coding system with external eavesdroppers, with bit error rate as the performance metric.

VIII. Related Topics

A. Game Theory and Security

The interactions between various agents (transmitters, receivers, helpers, and attackers) in multiuser wireless networks are accurately captured by inter-disciplinary analyses based on game theory and microeconomics, and this holds true for problems of secrecy as well. The central tenet of game theory is to model agents or players as rational entities whose sole focus is to maximize their individual gains or payoff functions. A non-cooperative game model assumes agents eschew coordination with one another (e.g., in a 2-player zero-sum game the payoffs add up to zero), while in a cooperative game players may choose to cooperate to achieve some mutual benefit (e.g., players may offer monetary payments via an auction, or form a coalition). Stable outcomes from which no player has an incentive to deviate are known as Nash Equilibria.

A zero-sum game between a multi-channel transmitter and an adversarial nature in the presence of an eavesdropper was treated in [233], with the difference of Alice and Eve's SINR as the payoff. Utilizing secrecy rate as the payoff in a game-theoretic formulation is a relatively new concept. Yuksel, Liu, and Erkip studied a SISO wiretap network with an adversarial jammer helping the eavesdropper as a zero-sum game, and presented the Nash Equilibrium input and jammer cumulative distribution functions [234]. In [235], [236], the authors considered a MIMO wiretap channel with an active eavesdropper that can either listen or jam, and pose its interactions with the transmitter as a zero-sum game with the MIMO secrecy rate as the payoff function. The SISO one-sided interference channel was studied in [237], and the corresponding Nash equilibrium secrecy rate region was derived. A zero-sum power allocation game between a multi-channel transmitter and a hostile jammer that is distinct from the eavesdropper was formulated in [238], with the secrecy rate as the payoff function.

Cooperative game theory was applied in [239] to demonstrate the improvement in secrecy capacity of an ad hoc network, when users form coalitions to null the signals overheard by eavesdroppers via collaborative beamforming. For a hierarchical multi-hop system with different potential paths to the base station, a distributed tree formation game was postulated in [240]. Han *et al.* [241] developed a two-stage Stackelberg game where a transmitter 'pays' a number of external helpers to jam an eavesdropper, and computed the corresponding equilibrium prices and convergence properties. The same authors examined a similar scenario in [242], where an auction game was used instead to model the transactions between transmitters and helping jammers. Anand and Chandramouli studied an M-user non-cooperative power control game with secrecy considerations in [243], and applied pricing functions to improve the energy efficiency and sum secrecy capacity of the network. For the 2-user IC with confidential messages, we have discussed in Sec. IV-B how Kalai-Smorodinsky bargaining solutions and zero-sum games are adopted to allow the transmitters to find an operating point that balances network performance and fairness [124], [126]. In [244], game theory is used by multiple eavesdroppers to decide whether to collude or not in a MISO wiretap channel.

B. Cognitive Radio and Sensor Networks

As a promising technique to alleviate spectrum scarcity, cognitive radio (CR) [245] is capable of dynamically sensing and locating unused spectrum segments in a target spectrum pool and communicating using the unused spectrum segments in ways that cause no harmful interference to the primary users of the spectrum. Due to the vulnerability of CR physical layer spectrum sensing, research attention on physical

layer security issues, though limited, has emerged recently. In [246], [247], several classes of physical layer attacks for dynamic spectrum access and adaptive radio scenarios are described, and corresponding techniques to mitigate these attacks are proposed. Denial-of-service vulnerabilities from the perspectives of the network architecture employed, the spectrum access technique used and the spectrum awareness model assumed, are examined in [248] and possible remedies are provided. Achievable secrecy rates in CR networks with external eavesdroppers have been studied in [249], [250].

Network spectral efficiencies can be further improved if the cooperative jamming signals are data signals instead of indiscriminate artificial noise. An elegant example of such a system is a CR network where the primary user wishes to conceal its message from an external eavesdropper [251], [252]. Here, the role of helpers is played by secondary or unlicensed users that seek to opportunistically transmit their data in the frequency band occupied by the primary user. Since the eavesdropper is interested only in the primary message, the secondary user signals act as jamming signals at the eavesdropper (as well as the primary receiver). The primary signal in turn is perceived as interference at the secondary receivers. Therefore, it is critical to judiciously select the primary and secondary signal powers in tandem so as to maximize the joint rate region of the cooperating users. In [251], [252], this was achieved via a Stackelberg power-control game formulation for the primary-secondary interactions, where the primary user allows secondary transmissions only if its secrecy rate is improved by doing so. In the multi-channel scenario of [253], the primary users are oblivious to the presence of CRs, while a game-theoretic formulation was constructed for optimal channel selection by the CRs and external eavesdroppers.

While not directly related to information security, a so-called *primary user emulation* (PUE) threat to spectrum sensing was identified in [254]. In PUE, a malicious node mimics the signal characteristics of licensed users in order to mislead cognitive radios into vacating the spectrum. As a countermeasure, [254] proposed a transmitter verification scheme to verify whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics. Another major physical-layer vulnerability in cooperative spectrum-sensing CR systems is the deliberate feedback of false sensing information. In [255], this problem is solved by designing fusion center (FC) counting rules so as to minimize the overall false alarm probability. Details of security challenges peculiar to cognitive radio networks can be found in [247].

Wireless sensor networks and corresponding distributed estimation algorithms have been at the forefront of signal processing research in the past decade. The downlink and uplink phases of communication between the sensors and the FC are inherently vulnerable to eavesdropping. Li, Chen, and Ratazzi [256] tackled downlink secrecy when the FC has multiple antennas by deliberately inducing rapid time-varying fluctuations in the eavesdropper's channel. [257] proposed the use of artificial noise-like schemes on the uplink to 'confuse' eavesdroppers about the aggregate sensor observations sent to the FC. In [258], the sensor observations are randomly mapped to a set of discrete quantization levels, with the corresponding mapping probabilities known only to the intended FC and not the eavesdropper. The optimal mapping probabilities and FC decision rule that jointly minimize its error probability subject to a constraint on the eavesdropper error probability are then derived. Marano *et al.* [259] examined optimal sensor censoring strategies in an energy-constrained sensor network infiltrated by an eavesdropper. Kundur *et al.* examined cross-layer secrecy-preserving design methodologies for multimedia sensor networks in [260].

C. Secrecy in Large-Scale Networks

Unlike point-to-point scenarios, the communication between nodes in large-scale networks strongly depends on the location and the interactions between nodes. In an early work on eavesdropping in cellular CDMA networks with multi-user detection capabilities, the outage probability of the eavesdropper signal-to-interference ratio was adopted as the performance metric [261]. Based on the assumption that legitimate nodes and eavesdroppers are distributed randomly in space, studies on secure communications for large-scale wireless networks have been carried out recently, utilizing tools from stochastic geometry and graph theory. Analyses based on stochastic geometry typically assume a spatial point process model (e.g., Poisson) for the locations of transmitters and receivers.

Secrecy communication graphs describing secure connectivity over a large-scale network with eavesdroppers present were investigated in [262]-[264]. In particular, the statistical characterizations of in-degree and out-degree under the security constraints were considered by Haenggi [262], Pinto *et al*. [263] and Goel *et al*. [265]. By using tools from percolation theory, the existence of a secrecy graph was analyzed in [262], [265]. The results in [264] showed improvements in secure connectivity by introducing directional antenna elements and eigen-beamforming. In order to derive the network throughput, these works on connectivity were further extended to incorporate secrecy capacity analysis. Specifically, the maximum achievable secrecy rate under the worst-case scenario with colluding eavesdroppers was given in [267]. Scaling laws for secrecy capacity in large networks have been investigated in [268]-[270]. Focusing on the transmission capacity of secure communications (defined as the number of successful transmissions taking place in the network per unit area, subject to a constraint on secrecy outage probability), the throughput cost of achieving a certain level of security in an interference-limited network was analyzed in [271], and the impact of uncertainties in node positions and CSI was examined in [272]. The probability of secure connectivity was given in [273] for multi-antenna nodes, and in [274] for a scenario with randomize-and-forward relays and a PPP for eavesdropper locations. A hierarchical multi-level sensor network was considered in [275], which introduced the concept of distributed network secrecy throughput to quantify inter-level network secrecy of all levels, i.e., data transmitted without collision are received successfully without being successfully eavesdropped in all levels.

D. Physical Layer Authentication

The most critical aspect of physical layer security is to ensure that confidential messages are decoded only by their intended receivers. A less well-studied but necessary component is that of message authentication, namely, to enable the receiver of a message to detect whether it was forged or illegitimately modified by someone other than its claimed source. Much like secure encoding, these operations are usually performed at the network and higher layers, with recent interest in devising physical layer counterparts.

In [276] an information-theoretic analysis of authentication is provided assuming both that the legitimate transmitter and receiver share a secret key and that transmission among all parties (including the attacker) are noiseless. In [277] both legitimate distortions of the message and joint typicality decoding are introduced in this framework. The impact of both noise and errors in the channel was taken into account for the first time in [278]. There, information theoretic bounds on the probability of a successful attack were derived for an arbitrarily low false alarm rate and infinitely long codewords.

Current attempts at using physical layer characteristics as authentication keys for the message source follow various approaches. One possibility is to assume a pre-shared secret key hidden in the modulation scheme, which is detected by the receiver [279], [280]. In other keyless transmitter-based methods (referred to as wireless fingerprinting), device-specific non-ideal transmission parameters are extracted from the received signal. They are identified as characteristics of the claimed source and then compared with those from previous authenticated messages [281]. Channel-based authentication algorithms compare the channel response estimated from the current message with that estimated from the previous transmissions by the ostensibly verified source, in effect authenticating the position of the transmitter rather than its identity. In order to reliably distinguish channels from different locations, some source of diversity must be exploited, either in the spatial domain by measurements of the received power levels at many receivers [282]-[284] or in the frequency domain via wideband channel estimates [285]-[288]. Instead of explicitly using channel responses for authentication, Tugnait [289] distinguishes between message sources based on their power spectral densities. A summary of a wide range of possible methods is available in [290].

For the case of a multi-antenna channel, [291] considers an approach where the test is performed in two phases. In the first phase, the receiver gets an authenticated noisy estimate x of the channel with respect to the legitimate transmitter. In the second phase, upon reception of a message, the receiver gets a new estimate u of the channel and compares it with x. A hypothesis test is subsequently performed to determine whether u is an estimate of the legitimate channel or the channel forged by an eavesdropper.

IX. CONCLUSIONS AND DIRECTIONS

This paper has provided a comprehensive survey of the field of physical layer security in wireless networks based on information-theoretic principles. We commenced with an overview of the foundations dating back to the pioneering work of Shannon, Wyner, and Maurer on information-theoretic security. We then described the evolution of secure transmission strategies from point-to-point channels to multiple-antenna systems, followed by generalizations to larger multiuser networks. We also reviewed secret-key establishment protocols based on physical layer mechanisms, along with an overview of practical secrecy-preserving code design and interdisciplinary approaches for security. The associated problem of physical layer message authentication is also introduced. Broadly speaking, it was observed that physical layer security is achieved by either exploiting the independence of wireless channels and background noise conditions observed by different nodes, or by judiciously directing interference (exogenous or intentional) towards unintended receivers.

The scope for future work in this field is extensive and only a few select directions are discussed next. As an example, the application of physical layer security techniques to commercially deployed wireless systems is largely unexplored. The majority of the techniques discussed in this survey, such as artificial noise for eavesdropper jamming and CSI-based precoding to optimize secrecy rates, are agnostic to the underlying air interface (time/code/orthogonal frequency-division multiple access). For example, an OFDMA-based base station may choose to transmit artificial noise along with data symbols in certain subcarriers as long as spectral emission masks are not violated. A CDMA transmitter may do the same after spreading the data with a pseudo-noise sequence. Furthermore, in 3GPP LTE, the introduction of Demodulation Reference Symbols (DMRS) has enabled the use of arbitrary MIMO precoders by the base station, therefore the secure GSVD precoder of [42] or its variants can be implemented without change in the current LTE standard. The secret-key generation scheme in [292] that makes use of LTE precoding matrix indicator (PMI) feedback is therefore a starting point for this direction. Arbitrary MIMO precoding is also allowed in IEEE 802.11ac and other forthcoming WLAN standards. The introduction of relay nodes, machine-type communications, and device-to-device communications in LTE raise new security challenges [293], and conceivably heighten the need for combining physical layer security with existing key-based ciphers.

Indeed, since physical layer security issues arise in multiuser systems of any kind, it is expected that new network scenarios and corresponding security schemes will continue to be developed. For instance, massive MIMO systems, overlay cognitive radio networks, smart grid systems [294], networks with simultaneous wireless information and power transfer [295], and heterogeneous networks [296] are untapped case studies from a secrecy perspective, to name just a few. Holistic approaches spanning the application and physical layer, in addition to exploitation of reconfigurable antennas [297], are expected to become more prominent. It is evident that the use cases of physical layer security extend well beyond cellular systems as seen in this survey.

Another untapped area is cross-layer analysis of secrecy combined with considerations of data queueing delay and rate control. In conventional network control problems, data pack-

ets that need to be served arrive in a queue(s) following some stochastic process, and the system is considered stable if the queue lengths are confined to some finite length. Initial steps to incorporate secrecy constraints into such problems were taken in [298] for a broadcast channel with confidential messages, where a secrecy throughput-optimal scheduling scheme was provided under a network utility maximization framework. More recently, for a single-user scenario the authors of [299] maximized the long-term data admission rate, subject to the stability of the data queue as well as a bound on the rate of secrecy outage. Evidently, many additional network scenarios await further analysis.

Finally, a deeper understanding of the interplay between physical layer security and classic cryptographic security is another rich but unexplored resource for further study [300], [301]. Also of current interest are secure transmission schemes where the confidential message also remains covert, i.e., potential eavesdroppers are uncertain if transmissions are ongoing [302], [303].

REFERENCES

[1] W. E. Stark and R. J. McEliece, "On the capacity of channels with block memory," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 322-324, Mar. 1988.

[2] M. Medard, "Capacity of correlated jamming channels," in *Proc. 35th Allerton Conf.*, pp. 1043-1052, 1997.

[3] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119-2123, Sep. 2004.

[4] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533-549, May 1988.

[5] B. Schneier, "Cryptographic design vulnerabilities," *IEEE Computer*, vol. 31, no. 9, pp. 26-33, Sep. 1998.

[6] G. Kapoor and S. Piramithu, "Vulnerabilities in some recently proposed RFID ownership transfer protocols," *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 260-262, Mar. 2010.

[7] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proc. IEEE*, vol. 100, no. 11, pp. 3056-3076, Nov. 2012.

[8] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Foundations and Trends in Communications and Information Theory, vol. 5, nos. 4-5, pp. 355-580, Now Publishers, 2008.

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

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

[11] X. Zhou, L. Song, and Y. Zhang (Eds.), *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[12] E. Jorswieck, A. Wolf, and S. Gerbracht, *Secrecy on the Physical Layer in Wireless Networks*. Telecommunications, In-Tech Publishers, 2010.

[13] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Trans. American Institute Electrical Engineers*, vol. XLV, pp. 295-301, 1926.

[14] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. Journ.*, vol. 28, pp. 656-715, 1949.

[15] P. R. Geffe, "Secrecy systems approximating perfect and ideal secrecy," *Proc. of the IEEE*, vol. 53, no. 9, pp. 1229-1230, 1965.

[16] M. E. Hellman, "An extension of the Shannon theory approach to cryptography," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 2, pp. 289294, Mar. 1977.

[17] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journ.*, vol. 54, pp. 1355-1387, 1975.

[18] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346-1359, Mar. 2013.

[19] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Seattle, July 2006.

[20] I. Csiszàr, "Almost independence and secrecy capacity," *Prob. Inf. Trans.*, vol. 32, no. 1, pp. 40-47, Jan.-Mar. 1996.

[21] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733-742, May 1993.

[22] V. I. Korzhik and V. A. Yakovlev, "Nonasymptotic estimates for efficiency of code jamming in a wire-tap channel," *Problemy Peredachi Informatsii (USSR)*, vol. 17, no. 4, pp. 11-18, 1981.

[23] A. B. Carleial and M. Hellman, "A note on Wyner's wiretap channel," *IEEE Trans. Inf. Theory*, vol. 23, no. 5, pp. 625-627, May 1977.

[24] S. L. Y. Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[25] I. Csiszàr and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[26] C. Mitrpant, A. J. Vinck,and L. Yuan, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181-2190, May 2006.

[27] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Proc. Eurocrypt, Workshop on Advances in Cryptology*, pp. 33-51, Paris, 1985.

[28] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "An opportunistic physical-layer approach to secure wireless communications," *Proc. Allerton Conf.*, Monticello, Sep. 2006.

[29] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE ISIT*, Nice, July 2007.

[30] O. Ozel, E. Ekrem and S. Ulukus, "Gaussian wiretap channel with a batteryless energy harvesting transmitter," in *Proc. IEEE Inf. Theory Workshop*, Lausanne, Switzerland, Sep. 2012.

[31] P. 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.

[32] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP Journ. Wireless Commun. Network.*, 2009.

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

[34] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE ISIT*, Adelaide, 2005.

[35] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. CISS*, Mar. 2007.

[36] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT*, Nice, France, June 2007.

[37] 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.

[38] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Intl Symp. on Inf. Theory*, pp. 2471-2475, June 2007.

[39] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Intl Symp. on Inf. Theory*, pp. 524-528, July 2008.

[40] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Tech. Conf.*, vol. 3, pp. 1906-1910, Dallas, Sept. 2005.

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

[42] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, July 2010.

[43] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: the MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[44] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. IEEE SPAWC*, pp. 344-348, Perugia, June 2009.

[45] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-Eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704-2717, May 2013.

[46] 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 J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728-1740, Sep. 2013.

[47] 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, June 2009.

[48] L. Zhang, R. Zhang, Y. 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, June 2010.

[49] J. Li and A. Petropulu, "Transmitter optimization for achieving secrecy capacity in Gaussian MIMO wiretap channels," submitted to *IEEE Trans. Inf. Theory*, 2010 [Online]. Available: http://arxiv.org/abs/0909.2622v1.

[50] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP Journ. Wireless Commun. Network.*, 2009.

[51] 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.

[52] R. A. Horn and C. R. Johnson, *Matrix Analysis*, University Press, Cambridge, UK, 1985.

[53] S. A. 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.

[54] S. Loyka and C. D. Charalambous, "On optimal signaling over secure MIMO channels," in *Proc. IEEE ISIT*, Boston, 2012.

[55] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP*, pp. 2437-2440, Taipei, Apr. 2009.

[56] Y.-W .P. Hong, L. Pang-Chang, 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.

[57] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation", in *Proc. Int. Conf. on Sig. Proc. and Commun. Syst*., Omaha, NE, Sept. 2009.

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

[59] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487-490, May 2013.

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

[61] S. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO wiretap channel," in *Proc. IEEE ISIT*, pp. 2321-2325, Boston, MA, 2012.

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

[63] Y.-L. Liang, Y. Wang, T. Chang, Y.-W. P. Hong, and C. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise ," in *Proc. IEEE ISIT*, pp. 2351-2355, Seoul, 2009.

[64] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation," in *Proc. 45th Asilomar Conf.*, pp. 952-957, Pacific Grove, CA, Nov. 2011.

[65] ——, "On the ergodic secret message capacity of the wiretap channel with finite rate feedback," in *Proc. IEEE ISIT*, Boston, 2012.

[66] 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," to appear, *IEEE Trans. Veh. Technol*., 2014. Available: *Early Access*.

[67] C.-W. Huang, T.-H. Chang, X. Zhou, and Y.-W. Peter Hong, "Two-way training for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2724-2738, May 2013.

[68] 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.

[69] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483-1486, July 2013.

[70] X. He and A. Yener, "MIMO wiretap channels with arbitrarily varying eavesdropper channel states," 2010 [Online]. Available: http://arxiv.org/abs/1007.4801

[71] M Kobayashi and M. Debbah, "On the secrecy capacity of frequency-selective fading channels: A practical Vandermonde precoding," in *Proc. IEEE 19th PIMRC*, 2008.

[72] 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.

[73] J. Li and A. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Inf Forensics Security*, vol. 6, no. 3, Part 1, pp. 861 - 867, Sep. 2011.

[74] Z. Rezki, F. Gagnon, and V. Bhargava, "The ergodic capacity of the MIMO wire-tap channel," [Online]. Available: http://arxiv.org/abs/0902.0189v1, Feb. 2009.

[75] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509-511, May 2011.

[76] 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.

[77] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372-375, June 2012.

[78] 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 Commun. Lett.*, vol. 17, no. 5, pp. 864-867, May 2013.

[79] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE ICASSP*, pp. 2809-2812, Kyoto, Japan, Mar. 2012.

[80] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. 45th Asilomar Conf.*, Pacific Grove, CA, 2011.

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

[82] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477-5487, Nov. 2010.

[83] H.Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936-3964, Sep. 2006.

[84] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493-2512, June 2008.

[85] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235-1249, Mar. 2009.

[86] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," in *Proc. IEEE Int. Symp. Information Theory*, Texas, U.S.A., June 2010, pp. 2578-2582.

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

[88] 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.

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

[90] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "A vector generalization of Costa's entropy-power inequality with applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1865-1879, Apr. 2010.

[91] Y. K. Chia and A. El Gamal, Three-receiver broadcast channels with common and confidential messages, *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2748-2765, May 2012.

[92] S. Salehkalaibar, M. Mirmohseni, and M. R. Aref, "One-receiver two-eavesdropper broadcast channel with degraded message sets," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1162-1172, July 2013.

[93] A. Mukherjee and A. L. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. of Forty-Seventh Allerton Conf.*, Oct. 2009.

[94] W. Liao, T. Chang, W. Ma, and C. Chi, "Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink," in *Proc. IEEE ICASSP*, pp. 256-2565, Dallas, TX, Mar. 2010.

[95] D. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Trans. Veh. Technol*., vol. 61, no. 6, pp. 2572-2584, July 2012.

[96] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE J. Selected Areas Commun.*, vol. 31, no. 9, pp. 1701-1713, Sep. 2013.

[97] 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*, 2011.

[98] 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.

[99] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, " Large system analysis of linear precoding in MISO broadcast channels with confidential messages," 2013, [Online]. Available: http://arxiv.org/abs/1304.5850

[100] G. Geraci, A. Y. Al-nahari, J. Yuan, and I. B. Collings, "Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1164-1167, June 2013.

[101] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in the broadcast channel with confidential messages and external eavesdroppers," 2013, [Online]. Available: http://arxiv.org/abs/1306.2101v1

[102] A. Mukherjee and A. L. Swindlehurst, "User selection in multiuser MIMO systems with secrecy considerations," in *Proc. Asilomar Conf.*, Pacific Grove, CA, Nov. 2009.

[103] M. Yanase and T. Ohtsuki, "user selection with secrecy capacity in multiuser MIMO downlink system," in *Proc. Int. Symposium Wireless Personal Multimedia Commun. (WPMC)*, Sendai, Japan, Sep. 2009.

[104] M. Yanase and T. Ohtsuki, "User selection scheme with secrecy capacity between other users in MIMO downlink systems," in *Proc. IEEE International Conference on Wireless Information Technology and Systems*, Honolulu, USA, Aug.-Sep. 2010.

[105] M. Yanase and T. Ohtsuki, "User selection scheme with secrecy capacity in MIMO downlink systems," *Procedia Social and Behavioral Sciences*, Elsevier, vol. 2, issue 1, pp. 161-170, 2010.

[106] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Process. Lett.*, vol. 20, no. 2, pp. 141-144, Feb. 2013.

[107] M. Pei, A. L. Swindlehurst, D. Ma, and J. Wei, "On ergodic secrecy rate for MISO wiretap broadcast channels with opportunistic scheduling," to appear, *IEEE Commmun. Lett.*, 2014, [Online]. Available: *Early Access*.

[108] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, Jul. 9-14, 2006.

[109] 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.

[110] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747-5755, Dec. 2008.

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

[112] –, "Correction to: The Gaussian multiple access wire-tap channel and "The general Gaussian multiple access and two-way wire- tap channels: Achievable rates and cooperative jamming"," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4762-4763, Sep. 2010.

[113] R. Liu, Y. Liang and H. V. Poor, "Fading cognitive multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4992-5005, Aug. 2011.

[114] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604-619, Feb. 2009.

[115] S. Anand and R. Chandramouli, "On the location of an eavesdropper in multiterminal networks," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 148-157, Mar. 2010.

[116] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-User interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425-3441, Aug. 2008.

[117] O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the K-user Gaussian interference channel," in *Proc. IEEE ISIT*, pp. 384-388, July 2008.

[118] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323-3332, 2011.

[119] X. He and A. Yener, "K-user interference channels: Achievable secrecy rate and degrees of freedom," in *Proc. ITW*, Greece, June 2009.

[120] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian multiple access wiretap channel," in *Proc. IEEE ISIT*, pp. 1337-1341, Istanbul, Turkey, 2013.

[121] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wire-tap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Proc. 47th CISS*, Baltimore, MD, 2013.

[122] T. Gou and S. A. Jafar, "On the secure degrees of freedom of wireless X networks," in *Proc. Allerton Conf.*, Monticello, IL, 2008.

[123] E. A. Jorswieck and R. Mochaourab, "Secrecy rate region of MISO interference channel: Pareto boundary and non-cooperative games," in *Proc. WSA*, 2009.

[124] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: game theoretic beamforming designs," in *Proc. Asilomar Conf. on Signals, Systems, and Computers*, Nov. 2010.

[125] ——, "MIMO interference channel with confidential messages: achievable secrecy rates and beamforming design," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 640-649, Sep. 2011.

[126] ——, "Competing for secrecy in the MISO interference channel," *IEEE Trans. Signal. Process.*, vol. 61, no. 1, pp. 170-181, Jan. 2013.

[127] R. Bassily, E. Ekrem, H. Xiang, E. Tekin, X. Jianwei, M. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp.16-28, Sep. 2013.

[128] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE ISIT*, pp. 926-930, Jun. 2007.

[129] 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.

[130] ——, "Two-hop secure communication using an untrusted relay," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1-13, Nov. 2009.

[131] ——, "The role of an untrusted relay in secret communication," in *Proc. IEEE ISIT*, pp. 2212-2216, Jul. 2008.

[132] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in *Proc. IEEE ISIT*, pp. 2217-2221, Jul. 2008.

[133] 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.

[134] 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 WCNC*, Shanghai, China, Apr. 2013.

[135] J. Huang and A. L. Swindlehurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," in *Proc. 47th Asilomar Conf.*, Pacific Grove, CA, Nov. 2013.

[136] 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.

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

[138] A. Mukherjee, "Imbalanced beamforming by a multi-antenna source for secure utilization of an untrusted relay," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1309-1312, July 2013.

[139] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[140] 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.

[141] 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. 1855-1863, Dec. 2012.

[142] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," in *Proc. 50th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, Oct. 2012.

[143] 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.

[144] J. Li, A. P. Petropulu, and S. Weber, "Optimal cooperative relaying schemes for improving wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.

[145] 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 J. Selected Areas Commun.*, vol. 29, no. 10, pp. 2067-2078, Dec. 2011.

[146] 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.

[147] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878-881, June 2012.

[148] 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.

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

[150] M. Jilani and T. Ohtsuki, "Joint SVD-GSVD precoding technique and secrecy capacity lower bound for the MIMO relay wire-tap channel," *EURASIP Journ. Wireless Commun. Networking*, 2012 2012:361.

[151] K. Ng 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.

[152] Z. 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.

[153] S. Vishwakarma and A. Chockalingam, "Amplify-and-forward relay beamforming for secrecy with cooperative jamming and imperfect CSI," in *Proc. IEEE ICC*, Budapest, Hungary, 2013.

[154] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *Proc. IEEE ICC*, Budapest, Hungary, 2013.

[155] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," to appear, *IEEE Trans. Veh. Technol.*, 2014, [Online]. Available: *Early Access*.

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

[157] J. Huang and A. L. Swindlehurst, "Wireless physical layer security enhancement with buffer-aided relaying," in *Proc. 47th Asilomar Conf.*, Pacific Grove, CA, Nov. 2013.

[158] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secret communication," in *Proc. IEEE ITW*, pp. 164-168, May 2008.

[159] M. Ara, H. Reboredo, F. Renna, and M. Rodrigues, "Power allocation strategies for OFDM gaussian wiretap channels with a friendly jammer: The degraded case," in *Proc. IEEE ICC*, Budapest, Hungary, 2013.

[160] D. S. Kalogerias, N. Chatzipanagiotis, M. M. Zavlanos, and A. P. Petropulu, "Mobile jammers for secrecy rate maximization in cooperative networks," in *Proc. IEEE ICASSP*, Vancouver, Canada, May 2013.

[161] N. Wu and H. Li, "Effect of feedback delay on secure cooperative networks with joint relay and jammer selection," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 415-418, Aug. 2013.

[162] M. Pei, A. L. Swindlehurst, D. Ma, and J. Wei, "Adaptive limited feedback for MISO wiretap channels with cooperative jamming," to appear, *IEEE Trans. Signal Process.*, 2014, [Online]. Available: *Early Access*.

[163] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013-5022, Oct. 2011.

[164] A. Mukherjee and J. Huang, "Deploying energy-harvesting cooperative jammers for security in the MIMO wiretap channel," in *Proc. ASILOMAR Conf.*, Pacific Grove, CA, Nov. 2012.

[165] J. Wang and A. L. Swindlehurst, "Cooperative jamming in MIMO ad-hoc networks," in *Proc. Forty-Third Asilomar Conf.*, pp. 1719-1723, Nov. 2009.

[166] 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.

[167] J. Huang and A. Lee Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[168] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682-694, Apr. 2013.

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

[170] G. Zheng, I. Krikidis, L. Jiangyuan, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962-4974 , Oct. 2013.

[171] X. He and A. Yener, "On the role of feedback in two-way secure communication," in *Proc. 42nd Asilomar Conf. Signals, Systems and Computers*, pp. 1093-1097, Oct. 2008.

[172] A. Mukherjee and A. L. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. 11th IEEE SPAWC*, Jun. 2010.

[173] Z. Z. Gao, Y. H. Yang, and K. J. R. Liu, "Anti-eavesdropping space-time network coding for cooperative communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3898-3908, Nov. 2011.

[174] S. Al-Sayed and A. Sezgin, "Secrecy in Gaussian MIMO bidirectional broadcast wiretap channels: Transmit strategies," in *Proc. 44th Asilomar Conf.*, Pacific Grove, CA, Nov. 2010.

[175] R. Zhang, L. Song, Z. Han, B. Jiaa, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. IEEE GLOBECOM*, Miami, FL, 2010.

[176] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121-1132, July 1993.

[177] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 344-366, Mar. 2000.

[178] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047-3061, Dec. 2004.

[179] U. M. Maurer and S. Wolf, "Secret key agreement over a nonauthenticated channel-Part I: Definitions and bounds," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822-831, Apr. 2003.

[180] U. M. Maurer and S. Wolf, "Secret key agreement over a nonauthenticated channel-Part II: The simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832-838, Apr. 2003.

[181] U. M. Maurer and S. Wolf, "Secret key agreement over a nonauthenticated channel-Part III: Privacy amplification," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839-851, Apr. 2003.

[182] V. Yakovlev, V. Korzhik, and G. Morales-Luna, "Key distribution protocols based on noisy channels in presence of an active adversary: Conventional and new versions with parameter optimization," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2535-2549, June 2008.

[183] S. Salimi, E. Jorswieck, and M. Skoglund, "Secret key agreement over an interference channel using noiseless feedback," in *Proc. IEEE ISIT*, 2013.

[184] S. Salimi, M. Salmasizadeh, M. R. Aref, and J. Golic, "Key Agreement over Multiple Access Channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 775-790, Sep. 2011.

[185] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, pp. 52-55, Feb. 2000.

[186] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, "On the secrecy capabilities of ITU channels," in *Proc. IEEE 66th Veh. Tech. Conf.*, pp. 2030-2034, Baltimore, MD, Oct. 2007.

[187] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE ICASSP*, Las Vegas, pp. 3013-3016, Apr. 2008.

[188] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE ISIT*, pp. 2593-2597, Seattle, July 2006.

[189] 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, June 2008.

[190] Y. Chunxuan, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N.B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol.5, no.2, pp. 240-254, June 2010.

[191] 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.

[192] T. Shimizu, H. Iwai, and H. Sasaoka, "Reliability-based sliced error correction in secret key agreement from fading channel," in *Proc. IEEE WCNC*, 2010.

[193] Y. Abdallah, M. A. Latif, M. Youssef, A. Sultan, and H. El Gamal, "Keys through ARQ: Theory and practice," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 737-751, Sep. 2011.

[194] Y. Shen and M. Z. Win, "Intrinsic information of wideband channels," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1875-1888, Sep. 2013.

[195] F. Renna, M. R. Bloch, and N. Laurenti, "Semi blind key agreement over MIMO fading channels," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 620-627, Feb. 2013.

[196] X. Li and E. P. Ratazzi, "MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks," in *Proc. IEEE MILCOM*, Atlantic City, NJ, 2005.

[197] Q. Li, H. Song, and K. Huang, "Achieving secure transmission with equivalent multiplicative noise in MISO wiretap channels," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 892-895, May 2013.

[198] C. Chen and M. A. Jensen, "Secrecy extraction from increased randomness in a time-varying MIMO channel," in *Proc. IEEE GLOBECOM*, Honolulu, Dec. 2009.

[199] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205-215, Feb. 2011.

[200] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17-30, Jan. 2010.

[201] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381-392, Sep. 2010.

[202] A. J. Pierrot and M. R. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 595-605, Sep. 2011.

[203] 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.

[204] H. Zhou, L. Hui, and L. Lai, "Key generation under active attacks," in *Proc. 47th Asilomar Conf.*, Pacific Grove, CA, 2013.

[205] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059-5067, Nov. 2008.

[206] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353-5361, Dec. 2009.

[207] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *DSN Progress Report*, pp. 114-116, 1978.

[208] C. Monico, J. Rosenthal, and A. Shokrollahi, "Using low density parity check codes in the McEliece cryptosystem," in *Proc. IEEE ISIT*, p. 215, Sorrento, Italy, June 2000.

[209] 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.

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

[211] D. Klinc, J. Ha, S. 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.

[212] A. Payandeh, M. Ahmadian, and M. Reza Aref, "Adaptive secure channel coding based on punctured turbo codes," *IEE Proc.-Commun.*, vol. 153, no. 2, pp. 313-316, Apr. 2006.

[213] J. Almeida and J. Barros, "Random puncturing for secrecy," in *Proc. 47th Asilomar Conf.*, Pacific Grove, CA, 2013.

[214] X. He and A. Yener, "Providing secrecy with structured codes: Tools and applications to Gaussian two-user channels," submitted to *IEEE Trans. Inf. Theory*, 2009 [Online]. Available: http://arxiv.org/abs/0907.5388.

[215] R. Liu, H. V. Poor, P. Spasojevic, and Y. Liang, "Nested codes for secure transmission," in *Proc. IEEE PIMRC*, pp. 15, Sep. 2008.

[216] A. Arora and L. Sang, "Dialog codes for secure wireless communications," in *Proc. IPSN*, 2009.

[217] 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, 2011.

[218] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of polar codes for the deterministic wiretap channel," in *Proc. 47th Asilomar Conf.*, Pacific Grove, CA, 2013.

[219] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," 2013, [Online]. Available: http://arxiv.org/abs/1305.4746

[220] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4539-4551, Sep. 2010.

[221] R. Tandon, S. Amuru, T. C. Clancy and R. M. Buehrer, "Towards optimal secure distributed storage systems with exact repair," 2013, [Online]. Available: arXiv:1310.0054v1.

[222] S. Pawar, S. El Rouayheb, and K. Ramchandran, "Securing dynamic distributed storage systems against eavesdropping and adversarial attacks," *IEEE Tran. Inf. Theory*, vol. 57, no. 10, pp. 6734-6753, Oct. 2011.

[223] N. B. Shah, K. V. Rashmi, and P. V. Kumar, "Information-theoretically secure regenerating codes for distributed storage," in *Proc. IEEE GLOBECOM*, Houston, TX, Dec. 2011.

[224] T. K. Dikaliotis, A. G. Dimakis, and T. Ho, "Security in distributed storage systems by communicating a logarithmic number of bits," in *Proc. IEEE ISIT*, Austin, TX, 2010.

[225] S. Goparaju, S. E. Rouayheb, R. Calderbank, and H. V. Poor, "Data secrecy in distributed storage systems under exact repair," in *Proc. IEEE NETCOD*, Calgary, Canada, Jun. 2013.

[226] O. O. Koyluoglu, A. S. Rawat, and S. Vishwanath, "Secure cooperative regenerating codes for distributed storage systems," 2012, [Online]. Available: arXiv:1210.3664.

[227] T. Ernvall, S. E. Rouayheb, C. Hollanti, and H. V. Poor, "Capacity and security of heterogeneous distributed storage systems," in *Proc. IEEE ISIT*, pp. 1247-1251, Istanbul, Turkey, 2013.

[228] R. W. Yeung, *Information Theory and Network Coding*. Springer, August 2008.

[229] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424-435, Jan. 2011.

[230] J. Feldman, T. Malkin, R. Servedio, and C. Stein, "On the capacity of secure network coding," in *Proc. Allerton Conf.*, Sept. 2004.

[231] D. Silva and F. R. Kschischang, "Security for wiretap networks via rank-metric codes," in *Proc. IEEE ISIT*, Toronto, 2008.

[232] K. Lu, S. Fu, Y. Qian, Y., and T. Zhang, "On the security performance of physical-layer network coding," in *Proc. IEEE ICC*, Dresden, Germany, June 2009.

[233] A. Garnaev and W. Trappe, "An eavesdropping game with SINR as an objective function," in *Proc. SECURECOMM*, pp.142-162, 2009.

[234] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," in *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818-830, Sep. 2011.

[235] A. Mukherjee and A. L. Swindlehurst, "Equilibrium outcomes of dynamic games in MIMO channels with active eavesdroppers," in *Proc. IEEE ICC*, Cape Town, South Africa, May 2010.

[236] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pg. 82-91, Jan. 2013.

[237] J. Xie and S. Ulukus, "Secrecy games on the one-sided interference channel," in *Proc. IEEE ISIT*, July 2011.

[238] M. Ara, H. Reboredo, S. Ghanem and M. R. D. Rodrigues, "A zero-sum power allocation game in the parallel Gaussian wiretap channel with an unfriendly jammer," in *Proc. IEEE ICCS*, Singapore, Nov. 2012.

[239] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, and T. Başar, "Physical layer security: Coalitional games for distributed cooperation," in *Proc. 7th WiOpt*, 2009.

[240] W. Saad, X. Zhou, B. Maham, T. Başar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980-3991, Nov. 2012.

[241] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer", *Eurasip Journ. Wireless Commun. and Network.*, 2009.

[242] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Improved wireless secrecy capacity using distributed auction theory", in *Proc. 5th ICMAS*, China, 2009.

[243] S. Anand and R. Chandramouli, "Secrecy capacity of multi-terminal networks with pricing," [Online]. Available: http://koala.ece.stevens-tech.edu/∼mouli/IT02.pdf.

[244] J. Cho, Y.-W. P. Hong, and C.-C. J. Kuo, "A game theoretic approach to eavesdropper cooperation in MISO wireless networks," in *Proc. IEEE ICASSP*, 2011.

[245] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," in *Proc. IEEE Int Mobile Multimedia Commun. Work.*, pp. 3-10, Nov. 1999.

[246] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. CrownCom*, pp. 1-8, May 2008.

[247] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tutorials*, vol. 15, no. 1, pp. 428-445, 2013.

[248] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerailities and protection countermeasures: a multi-dimensional

analysis and assessment," in *Proc. IEEE CrownCom*, pp. 456-464, Aug. 2007.

[249] S. Anand and R. Chandramouli, "On the secrecy capacity of fading cognitive wireless networks," in *Proc. IEEE CrownCom*, May 2008.

[250] Y. Pei, Y. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494-1592 , Apr. 2010.

[251] Y. Wu and K. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 831-842, Sep. 2011.

[252] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134-145, Jan. 2013.

[253] A. Hojeij, W. Saad, and T. Başar, "A game-theoretic view on the physical layer security of cognitive radio networks," in *Proc. IEEE ICC*, Budapest, Hungary, June 2013.

[254] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[255] H. Wang, L. Lightfoot, and T. Li, "On PHY-layer security of cognitive radio: Collaborative sensing under malicious attacks," in *Proc. CISS*, pp. 1-6, Mar. 2010.

[256] X. Li, M. Chen, and E. P. Ratazzi, "Array-transmission based physical-layer security techniques for wireless sensor networks," in *Proc. IEEE ICMA*, pp. 1618-1623, 2005.

[257] M. Anand, Z. Ives, and I. Lee, "Quantifying eavesdropping vulnerability in sensor networks," in *Proc. 2nd International Workshop on Data Management For Sensor Networks*, pp. 3-9, Aug. 2005.

[258] R. Soosahabi and M. Naraghi-Pour, "Scalable PHY-layer security for distributed detection in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1118-1126, Aug. 2012.

[259] S. Marano, V. Matta, and P. K. Willett, "Distributed detection with censoring sensors under physical layer secrecy," *IEEE Trans. Signal Process.*, vol. 57, no. 5, pp. 1976-1986, 2009.

[260] D. Kundur, W. Luh, U. N. Okorafor, and T. Zourntos, "Security and privacy for distributed multimedia sensor networks," *Proc. of the IEEE*, vol. 96, no. 1, pp. 112-130, Jan. 2008.

[261] A. McKellips and S. Verdú, "Eavesdropper performance in cellular CDMA," *European Trans. Telecommun.*, vol. 9, no. 4, pp. 379-390, July-Aug. 1998.

[262] M. Haenggi, "The secrecy graph and some of its properties, in *Proc. IEEE ISIT*, Toronto, Canada, July 2008, pp. 539-543.

[263] P. C. Pinto and M. Z. Win, "Percolation and connectivity in the intrinsically secure communications graph, [Online]. Available on arXiv:1008.4161.

[264] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125-138, Feb. 2012.

[265] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *Proc. IEEE ISIT*, Austin, USA, June 2010, pp. 2627-2631.

[266] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks - Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139-147, Feb. 2012.

[267] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000-3015, May 2012.

[268] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE ISIT*, pp. 1189-1193, Seoul, Korea, June 2009.

[269] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. IEEE INFOCOM*, Orlando, USA, Mar. 2012, pp. 1152-1160.

[270] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764-2775, Aug. 2011.

[271] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776-2787, June 2013.

[272] S. Vuppala and G. Abreu, "Secrecy transmission capacity of random networks," in *Proc. 47th Asilomar Conf.*, Pacific Grove, CA, 2013.

[273] X. Zhou, R. Ganti, and J. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425-430, Feb. 2011.

[274] C. Cai, Y. Cai, W. Yang, and W. Yang, "Secure connectivity using randomize-and-forward strategy in cooperative wireless networks," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1340-1343, July 2013.

[275] J. Lee, A. Conti, A. Rabbachin, and M. Z. Win, "Distributed network secrecy," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1889-1900, Sep. 2013.

[276] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1350-1356, July 2000.

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

[278] 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.

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

[280] P. L. Yu, J. Baras, and B. Sadler, "Power allocation tradeoffs in multicarrier authentication systems, in *Proc. IEEE Sarnoff Symp.*, 2009.

[281] T. Daniels, M. Mina, and S. F. Russell, "Short paper: a signal fingerprinting paradigm for general physical layer and sensor network security and assurance," in *Proc. IEEE First Int. Conf. on Security and Privacy for Emerging Areas in Commun. Networks*, pp. 219-221, 2005.

[282] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proc. ACM Workshop on Wireless Security*, pp. 43-52, 2006.

[283] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in *Proc. IEEE Int. Symp. on a World of Wireless, Mobile and Multimedia Networks*, 2006.

[284] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *Proc. IEEE Conf. on Sensor, Mesh and Ad Hoc Commun. and Networks*, 2007.

[285] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Fingerprints in the ether: using the physical layer for wireless authentication," in *Proc. IEEE ICC*, 2007.

[286] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "A physical layer technique to enhance authentication for mobile terminals," in *Proc. IEEE ICC*, 2008.

[287] 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.

[288] L. Xiao, A. Reznik, W. Trappe, C. Ye, Y. Shah, L. J. Greenstein, and N. B. Mandayam, "PHY-authentication protocol for spoofing detection in wireless networks," in *Proc. IEEE GLOBECOM*, 2010.

[289] 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.

[290] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56-62, Oct. 2010.

[291] 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, July 2012.

[292] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687-1700, Sep. 2013.

[293] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," to appear, *IEEE Commun. Surveys and Tutorials*. Available on *Early Access*.

[294] L. Eun-Kyu, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 46-52, Aug. 2012.

[295] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," 2013, [Online]. Available: http://arxiv.org/abs/1307.6110v1

[296] M. Zhang, R. Xue, H. Yu, H. Luo, and W. Chen, "Secrecy capacity optimization in coordinated multi-point processing," in *Proc. IEEE ICC*, Budapest, Hungary, 2013.

[297] O. Malyuskin and V. Fusco, "Spatial data encryption using phase conjugating lenses," *IEEE Trans. Antennas Propag.*, vol. 60, no. 6, pp. 2913-2920, June 2012.

[298] Y. Liang, H. V. Poor, and L. Ying, "Secure communications over wireless broadcast networks: Stability and utility maximization," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 682-782, Sep. 2011.

[299] Z. Mao, C. E. Koksal, and N. B. Shroff, “Achieving full secrecy rate with low packet delays: An optimal control approach,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1944-1956, Sep. 2013.
[300] M. Bellare, S. Tessaro, and A. Vardy, “A cryptographic treatment of the wiretap channel,” [Online]. Available: http://arxiv.org/abs/1201.2205v1
[301] T. Dean and A. Goldsmith, “Physical-layer cryptography through massive MIMO,” [Online]. Available: http://arxiv.org/abs/1310.1861
[302] P. H. Che, M. Bakshi, and S. Jaggi, “Reliable deniable communication: Hiding messages in noise,” 2013. Available: http://arxiv.org/abs/1304.6693.
[303] J. Hou and G. Kramer, “Effective secrecy: Reliability, confusion and stealth,” [Online]. Available: http://arxiv.org/abs/1311.1411v1.