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

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

***Abstract*—This paper provides a comprehensive review of the domain of physical layer security for wireless communications. 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. 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. We begin 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. Subsequently, we evaluate secret-key establishment protocols based on physical layer mechanisms, along with an overview of practical secrecy-preserving code design.**

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].

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. The information-theoretic 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 authors are with the Dept. of Electrical Engineering & Computer Science, University of California, Irvine, CA 92697-2625, USA. (e-mail: {amukherj; afakoori; jing.huang; swindle}@uci.edu)

The fundamental principle behind physical-layer security is to limit the amount of information that can be extracted at the 'bit' level by an unauthorized receiver. 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. Alternatively, since they can operate essentially independently of the higher layers, physical layer techniques can be used to augment already existing security measures. The vast majority of information-theoretic 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 survey does not proceed in a strictly chronological order, nor is the list of references intended to be exhaustive. Furthermore, due to inaccessibility we are forced to omit contributions to the field published within the former Soviet Union [5] and other international forums. Instead, we aim to provide a high-level overview of the historical development of the field with references that are easily accessible, juxtaposed with recent and ongoing research efforts.

The remainder of the paper 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 miscellaneous systems such as sensor and cognitive radio networks is carried out in V. The important issue of secret-key agreement in wireless networks is studied in Section VI. Section VII highlights the emerging areas of practical wiretap code design and cross-disciplinary approaches to secrecy. Finally, in Section VIII we summarize our discussion.

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*. Encryption of messages via a secret key known only to the transmitter and intended receiver has been the traditional route to ensuring confidentiality. Up until the 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 [6], 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 [7]. 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 has unbounded computational power, has knowledge of the transmit coding scheme, and has 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,

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

where $I(\cdot;\cdot)$ denotes mutual information. A by-product of this analysis was that perfect secrecy [8] can be guaranteed only if the secret key has at least as much entropy as the message to be encrypted, $H(K) \geq H(M)$, which validated Vernam's one-time pad cipher system.

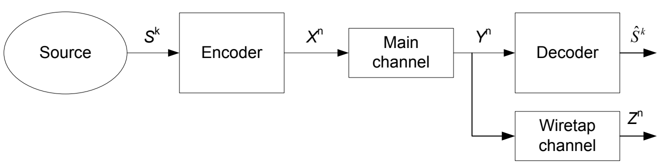

Fig. 1. The degraded wiretap channel [9].

Wyner ushered in a new era in information-theoretic security when he introduced the wiretap channel in [9], which considered the imperfections introduced by the channel. In the wiretap channel, the information signal X is transmitted to the intended receiver 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 channel is a probabilistically degraded version of the main channel [10], Wyner sought to maximize the transmission rate R in the main channel while making negligible the amount of information leaked to the wiretapper channel.

In his development Wyner defined the *equivocation* rate of the wiretapper, where the wiretapper equivocation or 'ambiguity' is the conditional entropy $H(S^k \mid Z^n)$, and therefore the equivocation rate is

$$R_e \leq \frac{H(S^k \mid Z^n)}{n}.$$

If the equivocation rate R_e is arbitrarily close to the information rate R, then R is the *secrecy capacity*[1] of the wiretap channel. He constructed a randomized coding scheme which sought to hide the information stream in the additional noise impairing the wiretapper by mapping each message to many codewords according to an appropriate probability distribution. 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.

In 1993, Maurer [14] 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 is 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 Sections III-V we trace the evolution of keyless security over the past decade. We revisit the topic of key-based security for wireless channels in Section VI.

B. Single-Antenna Wiretap Channels Since Wyner

Carleial and Hellman [10] 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 arbitrarily portion of the transmitted message. For the degraded wiretap channel with additive Gaussian noise [12], the essential result for the secrecy capacity C_S was the following:

$$C_S = C_M - C_W, \tag{2}$$

where C_M and C_W are the Shannon capacities of the main and wiretap channels, respectively. 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.

Csizar and Korner considered a more general (non-degraded) version of Wyner's wiretap channel in [11], 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

$$C_S = \max_{V \to X \to YZ} I\left(V;Y\right) - I\left(V;Z\right), \tag{3}$$

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 [13], 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

[1] 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 the one proposed by Shannon [cf. (1)], which requires that the mutual information be zero regardless of the block length.

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. Barros and Rodrigues *et al* [16]-[17] analyzed the outage secrecy capacity of slow fading channels and have showed that in the presence of fading information-theoretic security is achievable even when the eavesdropper has a better average SNR than the legitimate receiver.

Li *et al*. [18] examined an achievable secrecy rate for an AWGN main channel, while the eavesdropper's channel is Rayleigh fading with additive Gaussian noise, and its realizations are unknown to Alice and Bob. The main result of this paper is that with Gaussian random codes, artificial noise injection and power bursting, positive secrecy rate is achievable even when the main channel is arbitrarily worse than the eavesdropper's average channel.

Relatively fewer studies consider the case of a complete absence of eavesdropper CSI at the transmitter in fading wiretap channels. In [19], the authors consider 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 [20]. The compound wiretap channel captures the situation in which there is no or incomplete CSI at the transmitter by characterizing the eavesdroppers channel with a finite set of states, and guarantees secure communication under any state that may occur. The schemes designed for the compound channel are robust to various communication environments.

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. The work by Hero [21] is 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. In a fading MIMO channel where the transmitter, receiver, and eavesdropper are equipped with N_T, N_R, N_E antennas respectively, a general representation for the signal received by the legitimate receiver is

$$\mathbf{y}_b = \mathbf{H}_b \mathbf{x}_a + \mathbf{n}_b, \tag{4}$$

while the received signal at the eavesdropper is

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{x}_a + \mathbf{n}_e, \tag{5}$$

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

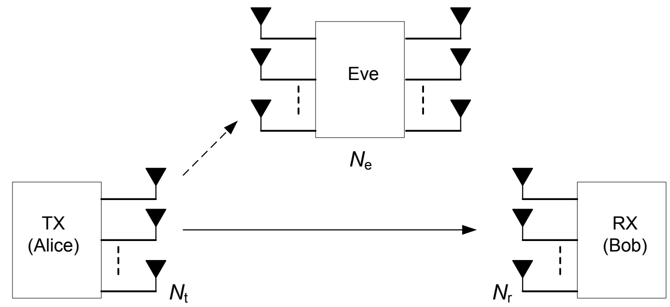

Fig. 2. General MIMO wiretap channel.

Hero examined the utility of space-time block coding for covert communications in [21], and designed CSI-informed transmission strategies to achieve either a low probability of intercept (equivalent to secrecy rate), 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 a secrecy capacity-achieving (i.e., equivocation-maximizing) strategy is to employ a space-time constellation with a constant spatial inner product.

Parada and Blahut analyzed a degraded single-input multiple-output ($N_T = 1, N_R, N_E > 1$) wiretap channel in [22], and obtained a single-letter characterization of its secrecy capacity via transformation into a scalar Gaussian wiretap channel, and then re-applying (2). 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 MISO case was studied in [23], [24], who noted that the MIMO wiretap channel is not degraded in general. Since this renders a direct computation of (3) 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 [25], a beamforming transmission strategy was shown to be optimal.

The next steps toward understanding the full-fledged MIMO wiretap channel were taken in [26]-[29], 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*. [26] 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 eigenvector 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* injection strategy as first suggested by Goel and Negi [28], [29]. 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 [34], [35].

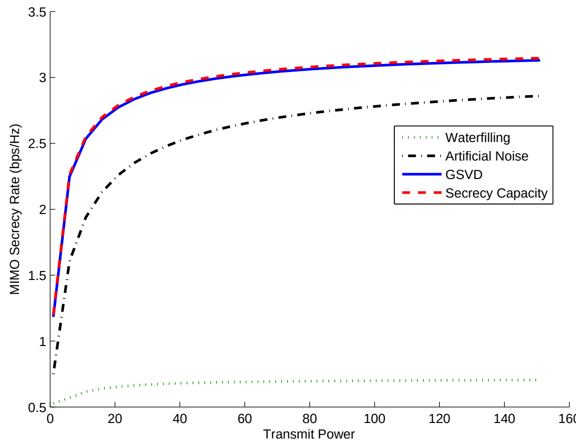

Fig. 3. The MIMO secrecy rates of GSVD-beamforming [34], [40], artificial noise [29], and waterfilling over the main channel, $N_T = N_E = 3, N_R = 2$.

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

The MIMO wiretap channel was studied independently by Oggier and Hassibi [27], who computed a similar upper bound on the MIMO secrecy capacity, and showed after a matrix optimization analysis that

$$C_S = \max_{\mathbf{Q}_x \succeq 0} \log\det\left(\mathbf{I} + \mathbf{H}_b\mathbf{Q}_x\mathbf{H}_b^H\right) - \log\det\left(\mathbf{I} + \mathbf{H}_e\mathbf{Q}_x\mathbf{H}_e^H\right). \quad (6)$$

In [30], Liu and Shamai reexamined 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*. attempted 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. Li and Petropulu [32] 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 [33] 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 [33] that, under the matrix power constraint $\mathbf{Q}_x \preceq \mathbf{S}$, the solution of (6) is given by

$$C_{sec}(\mathbf{S}) = \sum_{i=1}^{\lambda} \log \alpha_i \quad (7)$$

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

$$\left(\mathbf{S}^{\frac{1}{2}}\mathbf{H}_b^H\mathbf{H}_b\mathbf{S}^{\frac{1}{2}} + \mathbf{I}, \quad \mathbf{S}^{\frac{1}{2}}\mathbf{H}_e^H\mathbf{H}_e\mathbf{S}^{\frac{1}{2}} + \mathbf{I}\right) \quad (8)$$

that are greater than 1.

Note that, since both elements of the pencil (8) are strictly positive definite, all the generalized eigenvalues of the pencil (8) have real positive values [51], [137]. In (7), 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 $\mathrm{Tr}\left(\mathbf{Q}_x\right) \leqslant P$, there is not a computable secrecy capacity expression for the general MIMO case. In fact, for the average power constraint, the secrecy capacity is 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], [48, Lemma 1]

$$C_{sec}(P) = \max_{\mathbf{S} \succeq 0, \mathrm{Tr}(\mathbf{S}) \leq P} C_{sec}(\mathbf{S}) \quad (9)$$

where, for any given semidefinite $\mathbf{S}$, $C_{sec}(\mathbf{S})$ can be computed as given by (7).

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

- Optimal power allocation methods for the artificial noise strategy were presented in [39], and for the GSVD-based precoding scheme in [40].
- If even statistical information regarding the eavesdropper's channel is unavailable, then Swindlehurst *et al*. [37], [38] 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 is presented in [43].
- The effects of imperfect and quantized main channel state information at the transmitter upon the secrecy rate were examined in [41] and [42], respectively.
- MIMO secrecy capacity has also been studied for frequency-selective [44] and ergodic [45] channel fading processes.

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.

IV. Broadcast, Multiple-Access, and Interference Channels

The concept of information-theoretic security is easily extended to larger multi-user networks with more than 2 receivers and/or transmitters. The original wiretap channel as proposed by Wyner [9], is a form of broadcast channel (BC) where the source sends confidential messages to the destination while the messages should be kept 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 [11]. The secrecy capacity region of this scenario, for the case of a BC with parallel independent subchannels is considered in [46] and the optimal source power allocation that achieve the boundary of the secrecy capacity region is derived. The secrecy capacity region of the MIMO Gaussian broadcast channel with common and confidential messages, is characterized in [47] using a channel enhancement approach [48] and under matrix input power-covariance constraint $\mathbf{Q}_x \preceq \mathbf{S}$. The notion of an enhanced broadcast channel was firstly introduced in [48] and was used jointly with entropy power inequality to characterize the capacity region of the conventional Gaussian MIMO broadcast channel (without secrecy constraint). But, as we will show, most of the current works in the literature, studying different examples of MIMO broadcast channel with secrecy, use this notion. Moreover, instead of the average total power constraint $\mathrm{Tr}\left(\mathbf{Q}_x\right) \leqslant P$, they consider the more general 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 one, was studied in [49], where inner and outer bounds for the secrecy capacity region were established. This problem was studied in [50] for the multiple-input single-output (MISO) Gaussian case and in [51] for 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 is obtained using the 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 (3) and (4), but this time the transmitter has independent confidential messages W_1 (intended for receiver 1 but needing to be kept secret from receiver 2) and W_2 (intended for receiver 2 but needing 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

$$R_1 \leq \sum_{i=1}^{\lambda} \log \alpha_i \tag{10}$$

$$R_2 \leq \sum_{j=1}^{N_T-\lambda} \log \frac{1}{\beta_j} \tag{11}$$

where α_i, $i = 1, \ldots \lambda$, are the generalized eigenvalues of the pencil (8) that are bigger than 1, and β_j $j = 1, \ldots (N_T - \lambda)$ are the generalized eigenvalues of the pencil (8) that are less than or equal to 1.

The secrecy capacity region of the MIMO Gaussian broadcast channels with confidential and common messages, where the transmitter has two independent confidential messages and a common message, is characterized in [52]. The achievability is obtained using secret dirty-paper coding, while the converse is proved by using the notion of channel splitting [52].

Secure broadcasting with more than two receivers are considered in [53],[54], [55], and [56] (and reference therein). More precisely, there is one transmitter which wants to communicate with several legitimate users in the presence of an external eavesdropper. The secrecy capacity region for the two-legitimate receiver case is characterized by Khandani *et al.* [54] using the enhanced channels, and for an arbitrary number of legitimate receivers by Ekrem et. al [55]. Ekrem et. al. use the relationships between the minimum-mean-square-error and the mutual information, and equivalently, the relationships between the Fisher information and the differential entropy to provide the converse proof.

In [56], Liu *et al.* considered the secrecy capacity regions of the degraded vector Gaussian MIMO broadcast channel with layered confidential messages. They presented a vector generalization of Costa's Entropy Power Inequality to provide their converse proof. The role of artificial noise for jamming unintended receivers in multiuser downlink channels was investigated in [57], [58].

Other recent works on secure multi user communications investigated the multiple-access channel (MAC) with confidential messages [59], [60], the MAC wiretap channel (MAC-WT) [61], [62], and the cognitive MAC with confidential messages [63]. In [59] and [60], 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 [61], the Gaussian multiple access wire-tap channel (GMAC-WT) is considered where multiple users are transmitting to a base station in the presence an eavesdropper which receives a noisy version of the signal received at the base station (degraded wiretapper). In [61], 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, where the secrecy sum capacity is given by: In [62], a general, not necessarily degraded, Gaussian MAC-WT is considered, and the optimal transmit

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

Parameters	Strategy
MIMOME, no ECSIT	Artificial noise
MIMOME, statistical ECSIT	Artificial noise
MISOME, complete ECSIT	GEVD beamforming
MIMOME, complete ECSIT	GSVD precoding

power allocation that achieves the maximum secrecy sum-rate is obtained. It is shown in [62] 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 [63], Liu et al. consider 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 is established and the closed-form power allocation that achieves every boundary point of the secrecy capacity region is derived [63]. It should be noted that, all the above works in the field of MAC with confidential messages, assume single antenna nodes.

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. A special application of the IFC with secrecy constraints is addressed in [64], where the message from only one of the transmitters is considered confidential. The more general case, where each receiver acts as an eavesdropper for the other transmitter, was studied in [49] 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.

For multiuser networks, a useful metric that captures the scaling behavior of sum secrecy rate R_Σ as the transmit SNR, ρ, goes to infinity is the degrees of freedom (DoF), which can be defined as

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

The number of secure DoF for K-user Gaussian IFCs ($K \geq 3$) has been addressed in [65], [66], [67], and it was shown that under very strong interference, positive secure DoFs are achievable for each user in the network. More precisely, for the case of K-user SISO Gaussian interference channel with confidential messages, where each node has 1 antenna and each transmitter needs to ensure the confidentiality of its message from all non-intended receivers, a secure DoF of

$$\eta = \frac{K-2}{2K-2} \quad (12)$$

is almost surely achievable for each user [66]. The achievablity is obtained by interference alignment and channel extension [68]. Moreover, for the case of K-user SISO Gaussian interference channel with an external eavesdropper, each user can achieve

$$\eta = \frac{K-2}{2K} \quad (13)$$

secure DoF in the ergodic setting.

It should be noted that all of the above references [64]-[67] assume single antenna nodes. In fact, to the best of our knowledge, the only works considering the effect of multi-antenna nodes on secrecy in interference channel are [69]-[71]. In [69], Jorswieck *et al*. study the achievable secrecy rates of a two-user MISO interference channel, where each receiver has single antenna. They model a non-cooperative game in MISO interference channel and obtain the Nash equilibrium point using an iterative algorithm.

In [70] and [71], Swindlehurst *et al*. investigate 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 are described, and their achievable secrecy rate regions are derived. A game-theoretic formulation of the problem is adopted to allow the transmitters to find an operating point that balances network performance and fairness (the so called Kalai-Smorodinsky bargaining solution [71]). It is shown in [71] that, while ordinary jamming is near optimal for the standard wiretap channel [35], its performance is far from optimal for the interference channel.

V. Relay Channels and Miscellaneous Networks

A. *Relays and Helpers*

The physical layer security in relay networks has drawn much attention recently, as a natural extension to the secure transmission in MIMO networks. The secrecy capacity and achievable secrecy rate bounds have been investigated for various types of relay-eavesdropper channels, and many cooperative strategies, based on the ones that serve for the conventional relay systems, have been proposed.

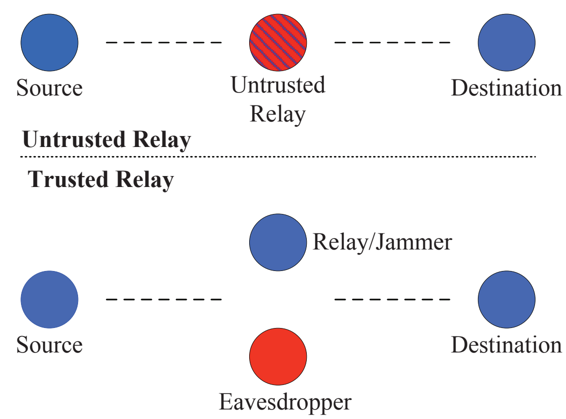

Fig. 4. Models of trusted and untrusted relay networks

As an extreme case study, the relay itself can be considered to be an *untrusted* user, where the relay node acts both as an eavesdropper and a helper, i.e., the eavesdropper is co-located with the relay node. The source desires to use the relay to communicate with the destination, but at the same time intends to shield the message from the relay. This group of model was first studied in [72] for the general relay channel. Coding problems of 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 [73]–[75], which show that the cooperation from the untrusted relay is still essential for achieving a non-zero secrecy rate. In [73], for the general untrusted relay channel which can be described as $p(Y, Y_r|X, X_r)$ with X, X_r being the input from the source and the relay, respectively, and Y, Y_r being the signals received by the relay and destination, respectively, the following achievable region of rate pairs (R_1, R_e) is derived:

$$\bigcup \left\{ \begin{array}{l} R_e \leq R_1 < I(X;Y,\hat{Y}_r|X_r) \\ 0 \leq R_e < [I(X;Y,\hat{Y}_r|X_r) - I(X;Y_r|X_r)]^+ \end{array} \right\}. \quad (14)$$

Based on this region, the cooperation of an untrusted relay node is found to be beneficial for a specific model where there is an orthogonal link in the second hop. A more symmetric case is discussed in [76], where both the source and the relay send their own private messages while keeping them secret from the destination. 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.

However, unlike the aforementioned case, in a *trusted* relay scenario, the eavesdroppers and relays are separate network entities. The relays can play various roles with 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 jamming unintended receivers.

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. For example, from an information-theoretic viewpoint, 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. In both cases, there is either no or minimal impact on the mutual information of the desired link, but that of the eavesdropper's link is reduced, and hence the secrecy rate is improved. For example, in a single-antenna wiretap channel with external helpers, an interesting approach is to split the transmission 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 [29].

A typical model of a relay channel with an external eavesdropper is investigated in [77], where the four-terminal network is introduced and an outer-bound on the optimal rate-equivocation region is derived. Specifically, for the traditional decode-and-forward (DF) relaying strategy, a achievable perfect secrecy rate is derived as

$$R_s^{(DF)} = \sup_{p(u)p(v_1,v_2|u)p(x_1,x_2|v_1,v_2)} [\min\{I(V_1,V_2;Y|U), I(V_1;Y_1|V_2,U)\} - I(V_1,V_2;Y_2|U)]^+ \quad (15)$$

for some random variables $U \rightarrow (V_1, V_2) \rightarrow (X_1, X_2) \rightarrow (Y, Y_1, Y_2)$ where X_1, X_2 are the channel inputs from the source and the relay respectively, while Y, Y_1, Y_2 are the channel outputs at the destination, relay and eavesdropper respectively. Lai et al. also propose a noise-forwarding strategy where the full-duplex relay sends codewords independent with the secrete message to confuse the eavesdropper. In [78], several cooperative schemes are proposed for a two-hop multiple-relay network, and the corresponding relay weights are derived aiming to maximize the achievable secrecy rate, under the constraint that the link between the source and the relay is not protected from eavesdropping.

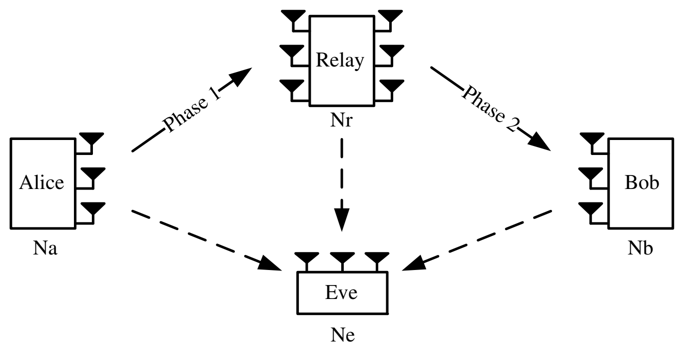

Fig. 5. Two-hop MIMO relay network with external eavesdropper.

In [80], a wiretap channel with an independent helping jammer is 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. [81] consider the cooperative artificial interference approach for MIMO ad hoc networks. The model therein can also be regarded as the external helper category, since 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. A general model is given by

$$\mathbf{y} = \mathbf{H}_{B,0}\mathbf{x} + \Sigma_{i=1}^{N}\mathbf{H}_{B,i}\mathbf{q}_i + \mathbf{n}_B \quad (16)$$

$$\mathbf{z} = \mathbf{H}_{E,0}\mathbf{x} + \Sigma_{i=1}^{N}\mathbf{H}_{E,i}\mathbf{q}_i + \mathbf{n}_E \quad (17)$$

where $\mathbf{H}_{B,0}$ and $\mathbf{H}_{E,0}$ are the channels from the source to the destination and eavesdropper respectively and $\mathbf{H}_{B,i}$ and $\mathbf{H}_{E,i}$ are the channels from jammer i to the destination and eavesdropper respectively. $\mathbf{x}$ is the information signals and $\mathbf{q}_i$ is the artificial interference, and $\mathbf{y}$ and $\mathbf{z}$ are received signals at the destination and eavesdropper respectively. For the proposed coordinated cooperative jamming scheme in [81], orthogonal information subspace and jamming subspace are broadcast across the network and $\mathbf{q}_i$ 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, $\mathbf{q}_i$ is simply the right singular vector of $\mathbf{H}_{B,i}$ 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.

A more general case where cooperative jamming strategies guarantee secure communication in both hops using without the need for external helpers is studied in [82]. In these approaches, the normally inactive node 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. We define two types of cooperative jamming schemes, *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.

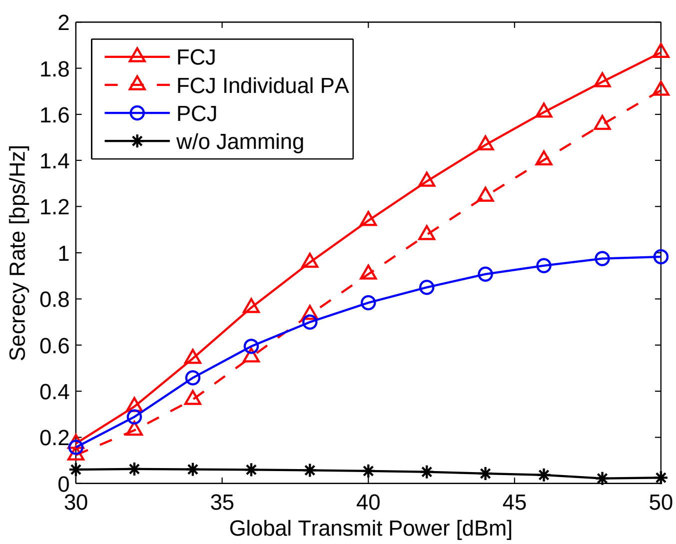

Fig. 6. Secrecy rate vs. transmit power, ECSIT unknown, $N_a = N_b = N_e = N_r = 4, d_{ij} = 800$m, $R_t = 2$bps/Hz.

In [62], a two-way wiretap channel is 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. Besides, a cooperative jamming scheme that utilizing the potential jammers is shown to be able to further increase the secrecy sum rate. [83] shows 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 multi-antenna two-way relay channel with network coding with the presence of eavesdroppers by [84]-[86]. 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.

B. Cognitive Radio and Sensor Networks

As a promising technique to alleviate spectrum scarcity, cognitive radio (CR) [87] 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 physical layer spectrum sensing of CR, research attention on physical layer security issues, though limited, has emerged recently. In [88], several classes of physical layer attacks for dynamic spectrum access and adaptive radio scenarios are described, and corresponding mitigation techniques to these attacks are proposed. In [89], the denial-of-service vulnerabilities, from the perspectives of the network architecture employed, the spectrum access technique used and the spectrum awareness model, are examined and possible remedies are provided.

A so-called *primary user emulation* threat to spectrum sensing is identified in [90], and a transmitter verification scheme is proposed to verifies whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics. In [91], the security problem of collaborative sensing for spectrum occupation is formulated as

$$Q_f = \begin{cases} \sum_{i=q-k}^{n-k} \begin{pmatrix} n-k \\ i \end{pmatrix} P_f^i \left(1-P_f\right)^{(n-k-i)} & \text{if } k < q \\ 1 & \text{if } k \geqslant q \end{cases} \tag{18}$$

where Q_f and P_f are the overall and individual false alarm probabilities respectively. In the sensing network, n users are collaboratively reporting sensing results and k of which are malicious users who deliver false reports. The base station makes the final decision based on certain counting rules related to q. The work provides a numerical algorithm to optimize q such that Q_f is minimized. Thus the issue of improving efficiency of spectrum access on a non-interfering basis is formulated as a constrained parameter optimization problem, which provides a better understanding on the effectiveness of the attacks and their countermeasures.

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 a fusion center (FC) are inherently vulnerable to eavesdropping. Li, Chen, and Ratazzi [94] tackle downlink secrecy where the FC has multiple antennas by deliberately inducing rapid time-varying fluctuations in the eavesdropper's channel. [95] proposed the use of artificial noise-like schemes on the uplink to 'confuse' eavesdroppers about the aggregate sensor observations sent to the FC. Kundur *et al.* examine cross-layer secrecy-preserving design methodologies for multimedia sensor networks in [96].

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 [14]. 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 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 the two terminals by exploiting the public discussion channel. The privacy amplification stage extracts a secret key from the identical random sequence agreed to by two terminals in the preceding information reconciliation phase. Less formally, after public discussion based on *correlated randomness* in the first stage, privacy amplification reduces a 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.

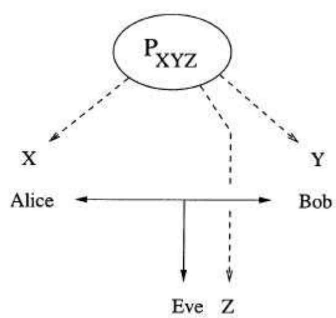

Fig. 7. Secret key agreement by public discussion.

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 joint probability distribution $P_{X,Y,Z}$ as in Fig. 7. The eavesdropper is completely ignorant of X and Y. The secret-key rate $S(X;Y||Z)$ was then defined as the maximal rate at which Alice and Bob can generate a secret key by communication over the noiseless and authentic but otherwise insecure channel in such a way that the opponent obtains information about this key only at an arbitrarily small rate (cf. (3)). The following upper and lower bounds on the secret key rate were presented:

$$S(X;Y||Z) \leqslant \min\left[I(X;Y), I(X;Y|Z)\right], \qquad (19)$$

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

Closely related results were offered in the concurrent work by Ahlswede and Csizar [97]. Csiszar and Narayan studied the augmentation of key-based secrecy capacity with the aid of a helper which supplies additional correlated information in [98], and obtained a single-letter characterization of the key-based secrecy capacities with an arbitrary number of terminals in [99]. Maurer and Wolf subsequently extended the secret-key sharing analysis of [14] to account for the presence of an active eavesdropper in [100]-[102], 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.

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 [103]. Other techniques include key generation via

- discretizing extracted coefficients of the multipath components [104],
- quantizing the channel phases for a multitone communication system such that multiple independent phases are used to generate longer keys [105],
- directly quantizing the complex channel coefficients [106],
- a purposely constructed random variable whose realizations are communicated between the legitimate nodes, with secrecy achieved when the eavesdropper lacks channel state information [107],
- exploiting the level crossing rates of the fading processes at the legitimate terminals [108],
- utilizing appropriately timed one-bit feedback available in practical networks due to Automatic Repeat reQuest (ARQ) protocols [109].

Unsurprisingly, multiple-antenna channels have attracted considerable attention for their capabilities of increasing common randomness at the legitimate users. Li and Ratazzi [110] design a MIMO precoder based on knowledge of the main channel that renders difficult blind channel estimation by the eavesdropper. Chen and Jensen developed practical key generation protocols for MIMO systems with temporally and spatially correlated channel coefficients in [111], [112]. One of the first experimental measurement campaigns on secret key generation in reciprocal MIMO channels was presented by Wallace and Sharma in [113].

The role of a feedback channel in improving the secrecy rate of a wiretap channel has been revisited in recent work. In [114], the authors show 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 can be used to jam the eavesdropper (assuming a modulo-additive channel model). Javidi *et al.* [115] consider a secure but rate-limited feedback channel, and prove that it is optimal for the receiver to feedback a random secret key that is independent of its received channel output symbols.

VII. Related Topics

A. Code Design for Secrecy

Once the groundwork had been laid for the limits of information-theoretic security, several researchers turned their attention to the development of practical channel codes for secrecy. Wyner [9] and Csiszàr and Körner [11] 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, and several open problems remain till date.

Therefore, it was natural to turn to capacity-achieving channel codes and examine their applications for secrecy. In [116], 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 [107] 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 as a proxy security metric in [117], 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 [118].

Graph-based unstructured codes are not the only viable approach for wiretap coding. He and Yener [119] show 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 [120]. 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 [121]. 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 wiretap channels [122].

While the emerging area of network coding is not directly related to traditional channel coding design, we briefly mention physical-layer security issues encountered in this field. Network coding is an paradigm for wireline and wireless networks that allows intermediate nodes to mix signals received from multiple paths, with the objective of improving throughput. Therefore, such networks are vulnerable to eavesdropping, as all other networks discussed thus far in this work.

The secure network coding problem was introduced in [124] 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 [124], [125]. Silva and Kschischang [126] 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 [84], [127], among others.

B. Cross-Disciplinary Tools

The interactions between various agents (transmitters, receivers, helpers, and attackers) in multiuser wireless networks is accurately captured by inter-disciplinary analyses based on game theory and microeconomics, and this holds true for problems of secrecy as well. Cooperative game theory was applied in [128] 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. Han *et al.* [129] 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 [130], where an auction game was used instead to model the transactions between transmitters and helping jammers. Anand and Chandramouli studied a M-user non-cooperative power control game with secrecy considerations in [131], and applied pricing functions to improve the energy efficiency and sum secrecy capacity of the network. For the 2-user MIMO-IC with confidential messages, the so called Kalai-Smorodinsky bargaining solution is adopted to allow the transmitters to find an operating point that balances network performance and fairness [70].

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 [132]. Mukherjee and Swindlehurst posed the MIMO wiretap channel with an active eavesdropper as a zero-sum dynamic (sequential) game, and examined the equilibrium transmit/wiretapper strategies for games with and without perfect information [133].

VIII. CONCLUSION

This paper 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 Shannon's pioneering work 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 networks. We also evaluate secret-key establishment protocols based on physical layer mechanisms, along with an overview of practical secrecy-preserving code design and inter-disciplinary models for security. Several recent monographs that provide a more rigorous and in-depth introduction to the topic of information-theoretic security are [134]–[136].

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] 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.

[6] 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.

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

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

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

[10] 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.

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

[12] 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.

[13] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Proc. Eurocrypt, Workshop on Advances in Cryptology*, pp. 3351, Paris, 1985.

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

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

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

[17] 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.

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

[19] 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.

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

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

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

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

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

[25] 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.

[26] 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.

[27] 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.

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

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

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

[31] 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.

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

[33] 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.

[34] 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.

[35] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: the MIMOME wiretap channel", to appear, *IEEE Trans. Inf. Theory*, 2010. [Online]. Available: http://www.rle.mit.edu/sia/.

[36] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, to appear, 2010.

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

[38] 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.

[39] 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.

[40] S. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO wiretap channel," 2010 [Online]. Available: http://arxiv.org/abs/1006.1890.

[41] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for secrecy in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Proc.*, Oct. 2010.

[42] 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.

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

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

[45] 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.

[46] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 32470-2492, June 2008.

[47] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, submitted July 2009.

[48] 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.

[49] 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.

[50] 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.

[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*, to appear, 2010.

[52] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "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.

[53] 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.

[54] G. Bagherikaram, A. S. Motahari and A. K. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," submitted to *IEEE Trans. Inform. Theory*, March 2009, available at http://arxiv.org/PScache/arxiv/pdf/0903/0903.3261v2.pdf

[55] E. Ekrem and S.Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," submitted to *IEEE Trans. Inform. Theory*, March 2009, available at http://arxiv.org/PS cache/arxiv/pdf/0903/0903.3096v1.pdf.

[56] 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.

[57] 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.

[58] 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, Mar. 2010.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] R. Liu, Y. Liang and H. V. Poor, "Fading cognitive multiple-access channels with confidential messages," submitted to *IEEE Trans. Inform. Theory*, Dec. 2009, available at http://arxiv.org/PS-cache/arxiv/pdf/0910/0910.4613v2.pdf

[64] 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.

[65] 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.

[66] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," submitted to *IEEE Trans. Inf. Theory*, 2008 [Online]. Available: http://arxiv.org/pdf/0810.1187.

[67] X. He and A. Yener, "K-user interference channels: achievable secrecy Rate and degrees of freedom," *ITW*, Greece, June 2009.

[68] 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.

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

[70] 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.

[71] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: achievable secrecy rates and beamforming design," submitted to *IEEE Trans. on Inf. Forensics and Security*, Aug. 2010.

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

[73] 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.

[74] ——, "On the equivocation region of relay channels with orthogonal components," in *Proc. Forty-First Asilomar Conf.*, pp. 883-887, Nov. 2007.

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

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

[77] 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.

[78] 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.

[79] J. Li, A. P. Petropulu, and S. Weber, "Optimal cooperative relaying schemes for improving wireless physical layer security," [Online]. Available: http://arXiv.org/abs/1001.1389.

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

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

[82] J. Huang and A. L. Swindlehurst, "Secure communications via cooperative jamming in two-hop relay systems," in *Proc. IEEE GLOBECOM*, Dec. 2010.

[83] 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.

[84] 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.

[85] S. Al-Sayed and A. Sezgin, "Secrecy in Gaussian MIMO bidirectional broadcast wiretap channels: Transmit strategies," in *Proc. 44th Asilomar Conf. Signals, Systems and Computers*, Nov. 2010.

[86] 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, 2010.

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

[88] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. 3rd Int. Conf. Cognitive Radio Oriented Wireless Networks and Communications CrownCom 2008*, pp. 1-8, May 2008.

[89] 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.

[90] 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.

[91] H. Wang, L. Lightfoot, and T. Li, "On PHY-layer security of cognitive radio: Collaborative sensing under malicious attacks," in *Proc. 44th Annual Conf. Information Sciences and Systems (CISS)*, pp. 1-6, Mar. 2010.

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

[93] 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.

[94] 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.

[95] 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.

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

[97] 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.

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

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

[100] 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.

[101] 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.

[102] 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.

[103] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, “Secure information transmission for mobile radio,” *IEEE Commun. Lett.*, vol. 4, pp. 5255, Feb. 2000.
[104] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, “On the secrecy capabilities of ITU channels,” in *Proc. IEEE 66nd Veh. Tech. Conf.*, pp. 20302034, Baltimore, MD, Oct. 2007.
[105] A. Sayeed and A. Perrig, “Secure wireless communications: Secret keys through multipath,” in *Proc. IEEE ICASSP*, Las Vegas, pp. 3013-3016, Apr. 2008.
[106] C. Ye, A. Reznik, and Y. Shah, “Extracting secrecy from jointly Gaussian random variables,” in *Proc. IEEE ISIT*, pp. 2593-2597, Seattle, July 2006.
[107] 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.
[108] 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. Inform. Forensics and Security*, vol.5, no.2, pp. 240-254, June 2010.
[109] Y. Abdallah, M. A. Latif, M. Youssef, A. Sultan, and H. El Gamal, “Keys through ARQ: Theory and practice,” submitted to *IEEE Trans. Inform. Forensics and Security*, May 2010 [Online]. Available: http://arxiv.org/pdf/1005.5063.
[110] 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.
[111] C. Chen and M. A. Jensen, “Secrecy extraction from increased randomness in a time-varying MIMO channel,” in *Proc. IEEE GLOBECOM*, Honolulu, Dec. 2009.
[112] C. Chen and M. A. Jensen, “Secret key establishment using temporally and spatially correlated wireless channel coefficients,” *IEEE Trans. Mobile Computing*, submitted Oct. 2009.
[113] J. W. Wallace and R. K. Sharma, ”Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis,” *IEEE Trans. Inform. Forensics and Security*, vol. 5, no. 3, pp. 381-392, Sep. 2010.
[114] 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.
[115] 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.
[116] 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.
[117] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, “LDPC codes for physical layer security,” in *Proc. IEEE GLOBECOM*, Honolulu, HI, Nov. 2009.
[118] 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
[119] 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.
[120] R. Liu, H. V. Poor, P. Spasojevic, and Y. Liang, “Nested codes for secure transmission,” in *Proc. IEEE PIMRC*, pp. 15, Sep. 2008.
[121] A. Arora and L. Sang, “Dialog codes for secure wireless communications,” in *Proc. IPSN*, 2009.
[122] H. Mahdavifar and A. Vardy, “Achieving the secrecy capacity of wiretap channels using polar codes,” 2010, [Online]. Available: http://arxiv.org/abs/1001.0210.
[123] R. W. Yeung, *Information Theory and Network Coding*. Springer, August 2008.
[124] N. Cai and R. Yeung, “Secure network coding,” in *Proc. IEEE ISIT*, p. 323, June 2002.
[125] J. Feldman, T. Malkin, R. Servedio, and C. Stein, “On the capacity of secure network coding,” in *Proc. Allerton Conf.*, Sept. 2004.
[126] D. Silva and F. R. Kschischang, “Security for wiretap networks via rank-metric codes,” in *Proc. IEEE ISIT*, Toronto, 2008.
[127] 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.
[128] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, and T. Basar, “Physical layer security: Coalitional games for distributed cooperation,” in *Proc. 7th WiOpt*, 2009.
[129] 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.*, special issue on physical layer security, 2009.
[130] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, “Improved wireless secrecy capacity using distributed auction theory”, in *Proc. 5th ICMAS*, China, 2009.
[131] S. Anand and R. Chandramouli, “Secrecy capacity of multi-terminal networks with pricing,” [Online]. Available: http://koala.ece.stevens-tech.edu/∼mouli/IT02.pdf.
[132] M. Yuksel, X. Liu, and E. Erkip, “A secure communication game with a relay helping the eavesdropper,” in *Proc. IEEE Inf. Theory Workshop*, Taormina, Italy, Oct. 2009.
[133] 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.
[134] 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, Hanover, MA, USA, 2008.
[135] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer, Norwell, MA, USA, 2009.
[136] E. Jorswieck, A. Wolf, and S. Gerbracht, *Secrecy on the Physical Layer in Wireless Networks*. Telecommunications, In-Tech Publishers, 2010.
[137] R. A. Horn and C. R. Johnson, *Matrix Analysis*, University Press, Cambridge, UK, 1985.