INVITED PAPER

Wireless Physical-Layer Security: Lessons Learned From Information Theory

Secrecy in multiterminal wireless settings may be enhanced by judiciously introducing interference and structured signaling schemes. This paper reviews recent findings in this area, along with strategies for cooperating with unauthenticated entities rather than treating them as eavesdroppers.

By Aylin Yener, *Fellow IEEE* and Sennur Ulukus, *Member IEEE*

ABSTRACT | Physical-layer security utilizes resources of the transmission medium to guarantee secure communication against an adversary with unlimited computational power. Rooted in information theory, physical-layer security advocates for a foundational approach by requiring security of communicated information as well as its reliability at the outset. The past decade has seen an unprecedented effort in physical-layer security research resulting in promising new design insights. The majority of these advances has been in wireless communications security, well-motivated by the fact that most data at large, including those of sensitive nature, flow over wireless links that are more vulnerable to security breaches, e.g., eavesdropping. At the same time, the open broadcast nature of wireless brings possibilities of cooperation by the network entities for improving security, e.g., resistance to eavesdropping. This article aims to provide an overview of research results in information-theoretic security with multiple wireless transmitters, and focuses on distilling insights for designing wireless systems with confidentiality guarantees.

KEYWORDS | Cooperative jamming; information-theoretic secrecy; physical-layer security; structured signaling; untrusted relays

I. INTRODUCTION

In recent years, the world at large has become increasingly online and connected, more often than not via wireless links, with an unprecedented amount of sensitive data being communicated in the wireless medium. While this transition has been quick thanks to the goal of designing reliable wireless communication networks being realized to a large extent, security of communicated information has not been the focus of wireless system designers. Rather, security of information is handled by the application layer via computation-based mechanisms, i.e., methods that rely on the computational complexity of an underlying mathematical problem which needs to be solved in order to have a successful security attack.

Computational security approaches, e.g., [1], [2] have worked well in practice although there is continuing effort to test their limits in terms of the computation power needed to break them [3], [4]. Successful attacks have been reported on various such security mechanisms, e.g., [5]–[7] over the years. Security being an add-on feature is the result of a layered approach to network design, in particular, separating the physical layer from upper layers as a reliable bit pipe.

By contrast, information-theoretic security relies on the characteristics of the physical layer, i.e., the *channel*, and possibly of the information source. Information-theoretic security provides guarantees by requiring security to be a design constraint just like reliability. As a result, the design possibilities offered by an information-theoretic approach are invariant to the increase in the computational power of an adversary.

While powerful, the framework does come with its caveats. In particular, the guarantees provided are of information-theoretic nature, namely those that are asymptotic, and

Manuscript received February 1, 2015; revised May 16, 2015 and July 13, 2015; accepted July 19, 2015. Date of current version September 16, 2015. This work was supported in part by the National Science Foundation (NSF) under Grants CCF 09-64362, CCF 09-64645, CCF 13-19338, CNS 13-14719, and CNS 13-14733.

A. Yener is with the Wireless Communications and Networking Laboratory (WCAN), Electrical Engineering Department, The Pennsylvania State University, University Park, PA 16802 USA (e-mail: yener@engr.psu.edu).

S. Ulukus is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: ulukus@umd.edu).

Digital Object Identifier: 10.1109/JPROC.2015.2459592

0018-9219 © 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

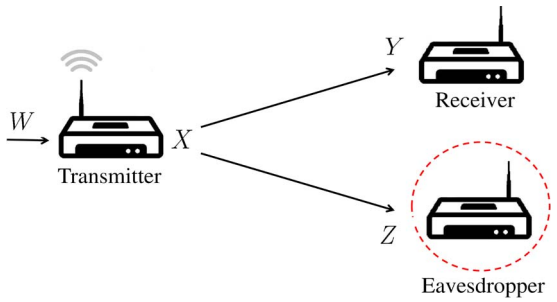

Fig. 1. ***Wiretap channel.***

are existence results. They often rely on assumptions on relative quality of channels and thus special caution is needed when those qualities are unknown or partially known. The resulting secure rates are reduced compared to those that are provided for reliability only. Still, the possibility of an unbreakably secure system is intriguing and has sparked a tremendous research effort, in particular in the last decade. Specifically, research in information-theoretic secrecy, which provides guarantees against eavesdropping by unauthorized parties, has been prominent.

In this overview article, we will summarize some of the results in information-theoretic secrecy obtained in the past decade, focusing on providing confidentiality guarantees based on and aided by the physical medium in which the communication takes place, i.e., the channel. We will consider wireless communication channels only. Further, we will focus on communication scenarios with multiple transmitting terminals and consider the impact of their interactions on secrecy. The goal of this article is to highlight a few lessons learned from these information-theoretic studies as system design insights.

II. BACKGROUND AND BASIC MODEL: SECRECY AS A DESIGN METRIC

Information-theoretic secrecy models often build upon the model called the wiretap channel studied in [8]. This model given in Fig. 1 consists of a transmitter (Alice) who wishes to communicate to a receiver (Bob) while keeping the messages confidential from an unauthorized second receiver (the wiretapper: Eve).

In his landmark paper in 1975, Wyner demonstrated that reliable *and* secure communication between Alice and Bob can be made possible by exploiting the relative qualities of the channels between Alice and Bob and Alice and Eve. Wyner defined the discrete memoryless wiretap channel, where the wiretapper Eve obtains a degraded version of Bob's signal via a cascaded discrete memoryless channel and characterized the rate-equivocation region, where the rate refers to the rate of *reliable communication between Alice and Bob*, and the equivocation refers to the *uncertainty of Eve about the message given her observation*. Reference [9] in 1978 generalized Wyner's framework to a large class of (not necessarily degraded) channels and found the complete characterization of the rate-equivocation region.

One important point on the rate-equivocation region of the wire-tap channel is the point where the reliable rate of communication

$$R = \lim_{n\to\infty} \frac{1}{n} H(W) \tag{1}$$

equals the equivocation rate

$$R_e = \lim_{n\to\infty} \frac{1}{n} H(W|Z^n) \tag{2}$$

with W denoting the secret message, Z^n denoting the observation of Eve after the n-length codeword X^n gets through the channel between Alice and Eve (respectively Y^n in Fig. 1 denotes the observation at Bob's receiver based upon which reliable communication is required), and $H(S)$ is the entropy of S. This is the largest rate at which Eve gains no information about the message after observing Z^n, i.e.,

$$\lim_{n\to\infty} \frac{1}{n} I(W; Z^n) = 0 \tag{3}$$

and is called the *secrecy capacity*. Equation (3) is the so-called *secrecy constraint*. It is also referred to as the *weak* secrecy constraint for the reason that it requires the vanishing only of the rate of the information Eve's observation gets about the message. This constraint can be strengthened to one that vanishes the mutual information

$$\lim_{n\to\infty} I(W; Z^n) = 0 \tag{4}$$

i.e., the *strong* secrecy constraint, for a variety of channels. Examples include [10]–[13], and see, for example, other recent work in strong secrecy relying on a resolvability view of secrecy [14]–[17].

The secrecy capacity of the general wiretap channel is given by the single letter expression [9]

$$C_s = \max_{p(u,x)} I(U; Y) - I(U; Z) \tag{5}$$

where X is the channel input of Alice to communicate W, Y is the channel output at Bob and Z is the channel output at Eve. U is an auxiliary random variable that facilitates the two virtual channels from Alice to Bob and Eve, i.e., even

though the actual physical channels from Alice to Bob and Eve are the channels from X to Y and from X to Z, respectively, using the auxiliary random variable U, we can create two virtual channels from U to Y and from U to Z, respectively. Here, U must satisfy the Markov relation $U \rightarrow X \rightarrow (Y,Z)$. The use of U decreases the rate from Alice to Bob from $I(X;Y)$ to $I(U;Y)$, per data processing inequality [18], but the same is true for the *leakage rate* from Alice to Eve from $I(X;Z)$ to $I(U;Z)$. Thus, by choosing a good U, the overall effect of these two reductions may lead to an overall increase in C_s. This is called *channel prefixing*, as it pre-fixes the actual channel from $p(y|x)$ and $p(z|x)$ to effectively, $p(y|u)$ and $p(z|u)$. For a given channel model, $p(y|x)$ and $p(z|x)$, finding the secrecy capacity is tantamount to finding the joint distribution of U and X, $p(u,x)$, that maximizes the difference in (5).

The familiar Gaussian channel model has also been studied in the presence of Eve in 1978. The secrecy capacity of the Gaussian wiretap channel was found in [19]. This channel model is defined by

$$Y = X + N_Y \tag{6}$$

$$Z = X + N_Z \tag{7}$$

where N_Y and N_Z are independent zero-mean Gaussian random variables with variance σ_Y^2 and σ_Z^2, respectively. Reference [19] showed that, for the single user Gaussian wiretap channel, $U = X$ is optimal, and that a Gaussian X maximizes the difference in (5), yielding the secrecy capacity, for an average power constraint of P, as

$$C_s = (C_Y - C_Z)^+ = \left(C\left(\frac{P}{\sigma_Y^2}\right) - C\left(\frac{P}{\sigma_Z^2}\right)\right)^+ \tag{8}$$

where $C(x) = (1/2)\log_2(1+x)$, and thus, in the above notation, C_Y denotes the capacity of the Alice to Bob link, and C_Z denotes the capacity of the Alice to Eve link. The notation $(x)^+$ denotes $\max(0,x)$. That is, if $C_Y > C_Z$, i.e., $\sigma_Y^2 < \sigma_Z^2$, then, we can provide a positive secure and reliable communication rate for Alice and Bob in the presence of Eve. This is accomplished by stochastic encoding, i.e., by means of assigning multiple codewords for each possible message and sending one at random in a manner that Bob can reliably decode while Eve's best guess for the message remains one that is uniformly random [8]. This rate is guaranteed irrespective of how much processing power or system knowledge including codebooks Eve has.

This is an extremely powerful result. It also concisely quantifies the price of confidentiality: by backing off from capacity by an appropriate amount, namely, by exactly the channel capacity to Eve, we can guarantee secure communications. However, the result does come with the limitation that Bob's channel must be better. In the case where $C_Y < C_Z$, i.e., $\sigma_Y^2 > \sigma_Z^2$, that is, when the channel from Alice to Bob is worse than from Alice to Eve, secure communication is not possible, even if the reliable communication rate C_Y is large. In essence, for secure communication, legitimate users of the system require a *channel advantage* over those of the adversary, even though a computational advantage as in cryptography is not at all needed.

The vehicle with which the above limitation has been overcome is the wireless medium. More specifically, wireless, being an open broadcast medium that can accommodate multiple simultaneous transmissions overheard by all, provides avenues to *create* the needed channel advantage for secure communications. This notion is one that rejuvenated the field of information-theoretic security, or, physical-layer security. In the remainder of the paper, we will focus on a few lessons learned over the past decade from studies and models starting with [20] that consider multiple signal transmissions. We will describe the relevant system model in the corresponding section. We note that there is a large body of research work on utilizing various properties and features of wireless communication channels. These include the medium's time varying nature, where, just as in nonsecret communications, exploiting channel variations is imperative. Additionally, secrecy rates are very much dependent on these variations, their statistical models, how fast channels change, as well as which parties have access to the realizations of the channels between the legitimate entities and the eavesdropper channels, see for example [21]–[29]. There has also been extensive work on utilizing multiple antennas, as well as on identifying secure communication rates for various network information-theoretic channel models, for these, the reader is referred to [30]–[44] and references therein.

III. LESSON 1: INTERFERENCE CAN BE BENEFICIAL: COOPERATIVE JAMMING

Consider a Gaussian wiretap channel with two transmitters and a common legitimate receiver as shown in Fig. 2. The two transmitters Alice and Charles wish to

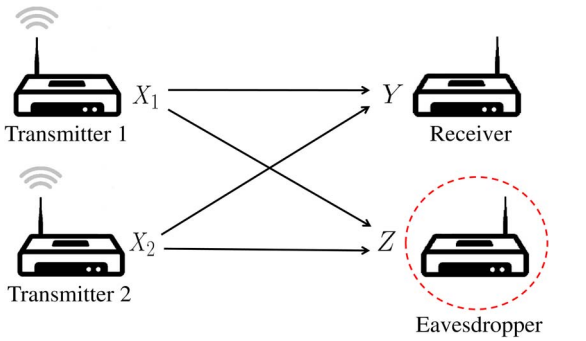

Fig. 2. ***Multiple access wiretap channel.***

communicate to Bob in the presence of an eavesdropper Eve. Further, consider the Gaussian channel where we now have

$$Y = h_1 X_1 + h_2 X_2 + N_Y \tag{9}$$
$$Z = g_1 X_1 + g_2 X_2 + N_Z. \tag{10}$$

Here X_1 and X_2 are sent by Alice and Charles for their secret messages W_1 and W_2, h_1 and h_2 are their channel coefficients to Bob, and g_1 and g_2 are their channel coefficients to Eve. This model was considered in [20] and [45] with the secrecy constraint as one that requires confidentiality of both messages from Eve

$$\lim_{n\to\infty} \frac{1}{n} I(W_1 W_2; Z^n) = 0. \tag{11}$$

This channel, termed the multiple access wiretap channel (MAC-WT) is the simplest network primitive where a channel advantage over Eve can be created via simultaneous signalling by multiple terminals. The model resembles the interference channel at first glance since there are two receivers and two transmitters. However, the goal is to ensure that one of the receivers (Bob) decodes both messages reliably, whereas the other receiver (Eve) is necessarily prevented from decoding either. In this set up, one can consider the secure sum rate of the two users and show that a secrecy sum rate of

$$R_s = \left(C\left(\frac{P_1 h_1 + P_2 h_2}{\sigma_Y^2}\right) - C\left(\frac{P_1 g_1 + P_2 g_2}{\sigma_Z^2}\right)\right)^+ \tag{12}$$

is achievable using Gaussian inputs [46]. Comparing with (8) one can already see that (12) having both users signals "mix" in the air induces a form of implicit cooperation, the effective channel from Alice to Bob in the presence of Charles can have a better quality than that of Alice to Bob alone. For some channels, the rates in [46] are shown to be very close to the secrecy capacity region [47].

The secrecy rate can be improved further by power control [48]. Indeed, it can be shown that, it is possible for the optimal power of one of the users to be zero. This essentially says that for the total achievable secure rate of this system, it may be better for one of the users, Charles, to forego sending any (secure) information. Not surprisingly, this user is one who has a better channel to Eve and thus his sending confidential data hurts the sum rate. This observation then naturally extends to the notion that this otherwise unused power of Charles may be further useful in improving the secrecy rate of Alice (and the sum secrecy rate because Charles is no longer transmitting W_2). Termed *cooperative jamming*, the strategy then calls for Charles to transmit a signal which does not carry his secret message, but has the sole intention of facilitating a more favorable channel for Alice to Bob by way of interfering [46]. This is indeed a form of channel pre-fixing introduced in Section II, namely, Charles, by sending his cooperative jamming signal, prefixes his input in a manner to help Alice improve her secrecy rate.

The simplest form of cooperative jamming is by Charles transmitting Gaussian noise in the set up of (9) and (10), i.e., X_2 is zero-mean Gaussian noise with variance P_2. The signal sent by Charles interferes with Bob and Eve both, and leads to the achievable secrecy rate

$$R_{cj} = \left(C\left(\frac{P_1 h_1}{\sigma_Y^2 + P_2 h_2}\right) - C\left(\frac{P_1 g_1}{\sigma_Z^2 + P_2 g_2}\right)\right)^+. \tag{13}$$

Under channel conditions that can be readily determined [46], R_{cj} can exceed that of the secrecy capacity of the wiretap channel which is the set up if Charles remains silent, i.e.,

$$C_s = \left(C\left(\frac{P_1 h_1}{\sigma_Y^2}\right) - C\left(\frac{P_1 g_1}{\sigma_Z^2}\right)\right)^+. \tag{14}$$

That is, while the transmission from Charles reduces both terms, it does increase the difference, which increases the secrecy rate.

This is the first lesson learned that is surprising: Interference in wireless communications is typically detrimental for the rate, and needs to be managed with design strategies. For secrecy however, interference created by a terminal can in fact be beneficial to increase the rate.

The notion of introducing judicial interference by some (or all) terminals in various multi-transmitter secrecy models has been widely used in subsequent studies. Such cooperative jamming can be with noise [46], or codewords from a codebook (Gaussian or not), see for example, [39], [49]. Additionally, cooperative jamming is utilized in a variety of practical models in communications and signal processing, see for example, [50] and others. We will revisit this notion in Section V applied to a whole different set of communication models as well.

We conclude this section by stating that the achievable rate in (13) can be improved upon, and recent results have obtained precise secure degrees of freedom, i.e., the behaviour of secrecy capacity in the high signal-to-noise ratio (SNR) regime for the MAC-WT channel [51]. The secrecy sum capacity (as well as the secrecy capacity region) of the Gaussian MAC-WT channel for any SNR remains open except for the degraded channel where time sharing between the two users is shown to be optimal [52].

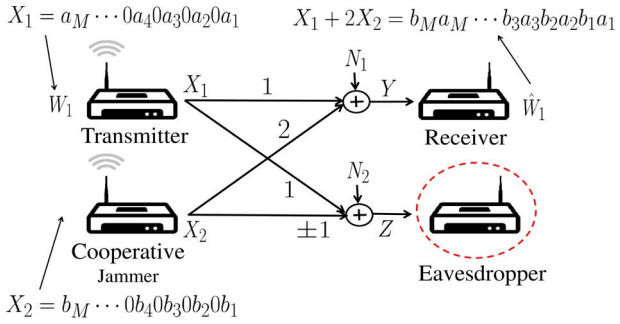

Fig. 3. *Structured signalling: a simple example.*

IV. LESSON 2: STRUCTURE PROVIDES BETTER SECRECY: LATTICES AND ALIGNMENT

So far, we have seen that introducing external interference in a manner that is more detrimental to Eve than to Bob can be helpful to increase secure communication rate for Alice. One can then surmise a construct where the interfering signal and the codewords sent can be chosen in a manner to be most detrimental to Eve while being least harmful to the legitimate receiver Bob. Thus, the notion of alignment [53] comes into picture with structured signalling.

To motivate why structure is good for secrecy, let us focus on the simplest model. Consider the Gaussian wiretap channel. It is easy to see that the secrecy capacity given in (14) does not scale with transmit power. That is, as $P_1 \to \infty$, the secrecy capacity converges to a constant and thus the high SNR slope of the secrecy rate, i.e., the secure degrees of freedom, in this case is zero. Further, consider the Gaussian wiretap channel with the cooperative jammer. The achievable secrecy rate given by (13) suffers from the same fate, even if the cooperative jammer power $P_2 \to \infty$. Therefore with Gaussian signaling and Gaussian cooperative jamming the achievable secrecy rate given by (13) does not scale with power.

Let us further focus on the specific channel configuration as shown in Fig. 3 as an example of the Gaussian channel with a cooperative jammer. Consider that the binary codeword and the jamming signals $a_M a_{M-1}, \ldots, a_1$ and $b_M b_{M-1}, \ldots, b_1$ are modified by inserting a "0" in between each digit so that we have $X_1 = a_M 0 a_{M-1} 0, \ldots, 0a_1$ and $X_2 = b_M 0 b_{M-1} 0, \ldots, 0b_1$. The received signal at Bob is given by $Y = X_1 + 2X_2 + N_1$ and Bob can reliably receive $b_M a_M b_{M-1} a_{M-1}, \ldots, b_1 a_1$ and hence $a_M a_{M-1}, \ldots, a_1$ whereas Eve having received $Z = X_1 + X_2 + N_2$ can only see $(b_M + a_M)0(b_{M-1} + b_{M-1})0, \ldots, (b_1 + a_1)$. This simple structure in the transmitted and jamming codewords allows covering of the legitimate communication by the cooperative jammer, enabling a positive scaling of the secrecy rate. Specifically, seeing the sum of digits, Eve can recover a_i only when $b_i = a_i$, leading to a secrecy rate of 0.5 as transmit and jamming signal power constraints tend to infinity.

There have been ample information-theoretic results which have shown that structured codes including nested lattice codes can be used to construct good channel codes, source codes and physical-layer network codes for Gaussian channels [54]–[57] without secrecy concerns. This approach is useful in multi-terminal problems: the structure of these codes makes it possible to align unwanted interference and also can be useful to analyze multihop scenarios. We shall get back to this latter model in Section V.

Recent work has demonstrated that structured signaling is beneficial for secrecy as well. In particular, [49] has shown that structured signaling (and jamming) in a two terminal setting where one of the terminals employs cooperative jamming improves secrecy in that it yields achievable secrecy rates that are scalable with power for almost all channel coefficients. The reference showed that with nested lattice codes one can lower bound the equivocation rate and quantify the achievable secrecy rate. Further, in [49], integer lattices have been used to show that secure degrees of freedom as high as 1/2 is achievable. A similar structure can be obtained by repetition in time [58].

More recently, [51] has shown that the secure degrees of freedom result of 1/2 is tight. This converse result quantifies the cost of secrecy precisely: even with infinite power at the disposal of the transmitter and the cooperative jammer, the slope with which the secrecy capacity grows in high SNR is half of that of the capacity without secrecy constraints. The achievability results are also insightful from a design perspective: whether nested lattice codes or discrete constellations are used, the structure allows the signals to be aligned favorably at Bob's receiver, while completely covering with an unfavorable alignment at Eve's receiver. This allows for a secrecy rate that grows with power. Hence, the second lesson is that structure is beneficial for secrecy.

V. LESSON 3: EVEN UNAUTHENTICATED NODES CAN BE USEFUL: UNTRUSTED COOPERATIVE COMMUNICATIONS

So far, the models we considered are of communication in the presence of an external eavesdropper from whom the information between legitimate parties need to be kept secret. Consider now a different communication scenario where the so-called eavesdropper, i.e., the terminal that is to be prevented from decoding what is being sent is an internal part of the network. Specifically, consider the communication scenario where a source-destination pair wishes to keep the information secret from a relay node despite wanting to enlist its help. Such a scenario is more practical than one first might think. In many networks, not all nodes have the same rights to access to

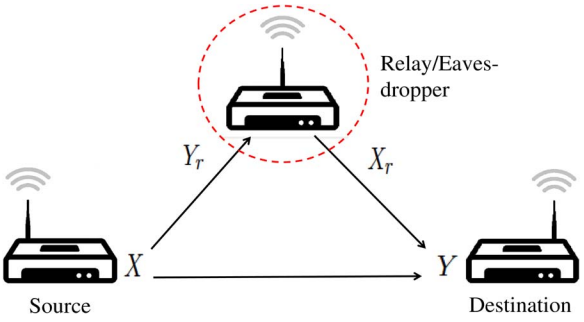

Fig. 4. *Wiretap channel with an untrusted relay.*

information despite operating with agreed protocols and serving as relay nodes in the network. For this scenario, an interesting question is whether the relay node should be deployed at all. That is, whether cooperation with an *untrusted* relay node[1] can ever be beneficial. Reference [59] answered this question positively by showing the existence of situations under which the cooperation with the untrusted relay increases an otherwise zero secrecy rate, while satisfying the condition of leaking no information rate to the relay.

Cooperative communications between a source and a destination in the presence of an untrusted relay was first studied in [60] and [61] for specific channel conditions. Indeed, it was shown in [61] that the secrecy capacity of this model is zero if the relay channel is degraded [62], and is equal to the wiretap channel secrecy capacity if the channel is reversely degraded [62]. Under these conditions, deploying such a relay is altogether unnecessary, as the secrecy capacity is either zero or equal to what is obtained by treating the relay as an external eavesdropper. Further studies with models using untrusted relays, however, have revealed that there are scenarios where cooperation from an untrusted relay is useful, and even imperative for communication. These are explained next.

A. Untrusted Relay Channel

Consider first the classical three node relay channel as shown in Fig. 4. This channel without secrecy constraints has been studied in [62] providing the best known achievable strategies to date for the general relay channel. For clarity of exposition of the strategy, we will consider the same discrete memoryless channel model first, which we will specialize to the Gaussian channel example to demonstrate the role of the untrusted relay. The channel is thus described by the probability distribution $p(Y, Y_r|X, X_r)$; X, X_r are the transmitted signals at the source and the relay, and Y, Y_r are the received signals at the destination and the relay, respectively. The source wishes to reliably send a message W to the destination. The difference from the model in [62] is that the relay is untrusted, and therefore the message needs to be kept secret from the relay node. Thus, we have the secrecy constraint

$$\lim_{n\to\infty} \frac{1}{n} I\left(W; X_r^n, Y_r^n\right) = 0 \tag{15}$$

where the signals are over the n-channel uses. References [59] and [63] have identified the following secrecy rate to be achievable for this channel:

$$R_s = \max_{p(X,X_r)} \left[I(X; Y, \hat{Y}_r|X_r) - I(X; Y_r|X_r) \right]^+ \tag{16}$$

where $\hat{Y}_r$ represents a quantized version of Y_r, which satisfies the condition $I(X_r; Y) > I(\hat{Y}_r; Y_r|Y, X_r)$. The achievability of (16) is established by using stochastic encoding at the source, and compress-and-forward [62] at the relay.

Reference [59] has further studied two special cases of this model in Gaussian channels. The first special case is when the source-to-relay channel, with input X_R and output Y_r, is orthogonal to the multiple access channel from the source and relay to the destination. In this set up, it was found that the secrecy capacity is achieved by restricting the confidential transmission to the direct link from the source to destination, and discarding the relay altogether, contributing to the scenarios where an untrusted relay is not useful.

The second case considered in [59] has provided the first instance where enlisting relay's cooperation improves the achievable secure communication rate. This is when the relay to destination link, with input X_r and output Y_R, is orthogonal to the channel from the source to the relay and destination with input X and outputs Y_r, Y_D. Such a scenario is exceedingly practical in the era of heterogenous networks where nodes can operate with multiple technologies in different bands, e.g., cellular and Wi-Fi. The received signal at the destination is $Y = \{Y_R, Y_D\}$. This channel is expressed as $p(Y_R, Y_D, Y_r|X, X_r) = p(Y_D|X)p(Y_R|X_r)p(Y_r|X, X_r, Y_D)$. By specializing the secrecy rate in (16) to this channel, an achievable secrecy rate for this model is [59]

$$R_s = \max_{p(X,X_r)} \left[I(X; Y_D, \hat{Y}_r|X_r, Y_R) - I(X; Y_r|X_r) \right]^+ \tag{17}$$

where $\hat{Y}_r$ satisfies $I(X_r; Y_R) > I(\hat{Y}_r; Y_r|Y_D, Y_R, X_r)$.

The Gaussian case of this model can be described by the following received signals:

$$Y_r = aX_R + N_r, \tag{18}$$

$$Y = bX_r + X_D + N_Y \tag{19}$$

[1]Such a node is sometimes also called "honest, but curious."

where N_r and N_Y are independent Gaussian noise signals with zero mean and unit variance, at the relay and the destination, respectively. Coefficients a and b are the channel gains of the source-to-relay and relay-to-destination links, respectively. The average power constraints at the source and the relay are P and P_r, respectively. Substituting in (17) $X \sim \mathcal{N}(0,p)$, $X_r \sim \mathcal{N}(0,P_r)$, $\hat{Y}_r = Y_r + Z_Q$, $N_Q \sim \mathcal{N}(0,\sigma_Q^2)$, where N_Q is independent of all other random variables, results in the following secrecy rate [59]:

$$R_s = \max_{0\le p\le P}\left\{C\left(p+\frac{a^2p}{1+\sigma_Q^2}\right) - C(a^2p)\right\} \qquad (20)$$

where σ_Q^2, the variance of the quantization noise N_Q, is

$$\sigma_Q^2 = \frac{(a^2+1)p+1}{b^2P_r(p+1)} \qquad (21)$$

in order, for $\hat{Y}_r$, to satisfy $I(X_r;Y_R) > I(\hat{Y}_r;Y_r|\,Y_D,Y_R,X_r)$.

When $a>1$, and in the absence of the relay-to-destination link, the model is equivalent to a Gaussian wiretap channel with a better eavesdropper channel than the legitimate channel. Since the eavesdropper channel is better, the secrecy capacity is clearly zero as shown in (8) and (14). However, with a sufficiently large relay-to-destination channel gain, b, the secrecy rate in (20), which is achieved by a compress-and-forward scheme at the relay, is larger than zero. Thus cooperation with the untrusted relay increases the achievable secrecy rate of the system. In other words, cooperating with this honest but curious unauthenticated node is better than simply treating it as an eavesdropper.

A design comment is that unlike the model when there are no secrecy constraints on the relay, where the source node should always transmit with maximum power, the secrecy rate in (20) is not necessarily maximized at $p=P$. This is clearer when the relay-to-destination channel gain, b, is small, where σ_Q^2 in (21) increases more rapidly with increasing p, which can result in a faster increase of the term $C(a^2p)$, with increasing p, than that of the term $C(p+(a^2p/(1+\sigma_Q^2)))$ in (20). Thus, one needs to employ careful power control at the source in order to get the most out of the untrusted relay. Furthermore, in order to assess the performance of the achievable scheme above, [59] has also derived an upper bound for this model which is shown to be tight for special cases [59]. Finally, we note that, [63] has generalized this model where the source sends an additional message to the relay which is to be kept secret from the destination. In this case, securing both messages is possible by a combination of compress and forward and cooperative jamming by the relay.

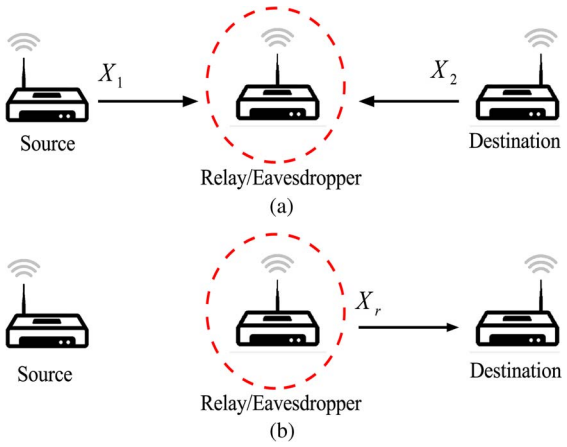

Fig. 5. *Two-hop network with an untrusted relay: (a) in the first phase; (b) in the second phase.*

B. Untrusted Two-Hop Channel

In the preceding model with the untrusted relay, a direct link is present between the source and destination. Thus, the source-destination pair may choose not to cooperate with the untrusted relay node and simply treat it as an eavesdropper; yet can achieve a positive secrecy rate, under certain channel configurations. On the other hand, for many wireless communication scenarios of interest, it is possible that relay nodes are the only way to communicate between the source(s) and destination(s). The distance between the source and destination can be large enough that the rate that could be provided by the direct link is negligible. In this case, all signals sent by the source have to go through the relay and one might wonder if reliable and secure communication between the source and destination can ever be possible if the relay in the middle is untrusted. This question is addressed in [64], and answered in the positive. While surprising at first, the result builds upon the notion introduced in Section III, i.e., introducing interference by legitimate parties into the medium, so that the secure rate between them is improved.

More specifically, [64] considered a Gaussian two-hop single-source single-destination network with an untrusted relay as shown in Fig. 5. All nodes are assumed to operate in half-duplex mode, i.e., they cannot receive and transmit at the same time. This requires the communication to be done over two phases. In the first phase, the achievable scheme in [64] applies stochastic encoding at the source node and requires the destination to participate in communication by (cooperative) jamming the untrusted relay with a random Gaussian signal. Here, cooperative jamming is in fact the main enabler of secure communication, this time utilizing the fact that the receiver (destination) can expend some of its power to ensure the security of the information it receives.

During the first phase, the relay remains silent and receives the following signal:

$$Y_r = X_1 + X_2 + N_r \tag{22}$$

where X_1, X_2 are the transmitted signals by the source and destination, respectively. N_r is a zero mean unit variance Gaussian noise. Then, the relay does compress-and-forward [62], [65] and transmits its signal to the destination, which receives

$$Y = X_r + N_Y, \tag{23}$$

where X_r is the transmitted signal by the relay, and N_Y is a zero mean unit variance Gaussian noise. Using this received signal along with the cooperative jamming signal, which it knows, the destination is able to decode a secure message with a rate given by

$$R_s \leq \max_{\alpha\in(0,1]} \alpha \left[C\left(\frac{P_1}{1+\sigma_Q^2}\right) - C\left(\frac{P_1}{1+P_2}\right)\right]^+ \tag{24}$$

where P_1, P_2 are the powers of the transmitted signal at the source and destination, and α is the time sharing factor of the first phase. σ_Q^2 is the variance of the quantization noise that is calculated from

$$\alpha C\left(\frac{P_1}{1+\sigma_Q^2}\right) = (1-\alpha)C(P_r) \tag{25}$$

where P_r is the power of the transmitted signal at the relay.

One can observe that this strategy achieves a non-zero secrecy rate whenever the jamming power is higher than the variance of the quantization noise resulting from the compress-and-forward scheme applied at the relay. Regarding the power allocations at the different nodes, one can readily see that the relay should always transmit with its maximum power in order to increase the time sharing factor α, and the destination also should jam with its maximum available power for this purpose, in order to reduce the negative term in (24). However, one can also observe that the achievable secrecy rate, in general, is not a monotonically increasing function in the source transmitting power. Therefore, in order to maximize the achievable secrecy rate, once again, a power control policy should be implemented at the source node [64]. Reference [64] also derived a genie aided bound in order to assess how far the proposed achievable rates are from the secrecy capacity and showed that the resulting upper bound was tight for several cases of interest for this two-hop model.

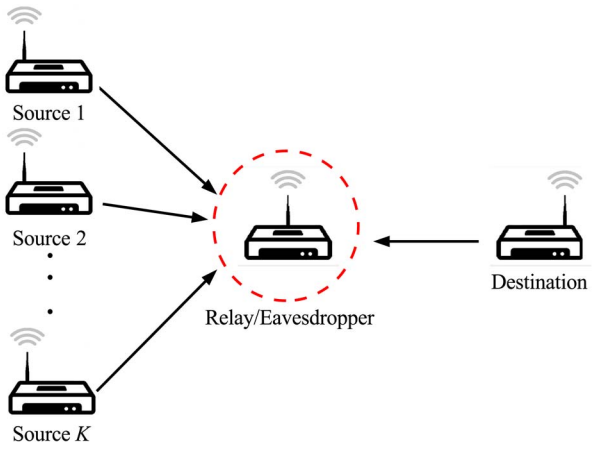

Fig. 6. *Multiple access channel with an untrusted relay.*

The model in this section is compelling in that it provides an avenue for providing (secure) communication using an untrusted entity exclusively. Recent work has extended this model to scenarios where the untrusted relay is shared between multiple transmitters as shown in Fig. 6. This shared relay model once again can be useful for example for relaying information of cellular customers over an unauthenticated Wi-Fi access point. Reference [66] has studied this Gaussian multiple access untrusted relay channel (MARC), where K transmitters aim to communicate securely with a single destination via an untrusted relay and derived an achievable rate region using compress-and-forward at the relay with the help of cooperative jamming from the destination. To maximize the achievable secrecy sum rate, here again, one needs a power allocation policy similar to the aforementioned one for the single-source single-destination two-hop network. It is also worth mentioning that in this achievable scheme for the MARC channel with an untrusted relay, while cooperative jamming by the destination is essential, cooperative jamming by the transmitters is not useful (in contrast to the MAC-WT channel). Once again, the upper bound derived in this work shows that the secrecy sum rate obtained is tight in some cases of interest. Lastly, another recent extension considers multiple terminals at both transmit and receive sides [67]. In particular, achievable rates with Gaussian signaling in a two-source two-destination network with an untrusted relay where all receivers are interested in decoding messages, but some are prevented from doing so, are derived. Such multiple terminal extensions deserve further study, in particular towards understanding the impact of structured signaling strategies.

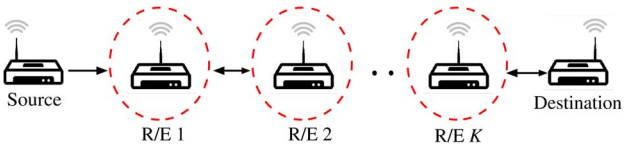

Fig. 7. *Line network with K untrusted relays.*

C. Untrusted Multi-Hop Channel

An extension of the model studied in [64] is a multi-hop relay network where many relay nodes on a line operating in tandem facilitate communication between a source and a destination, as shown in Fig. 7. In such a network, one can again ask the question whether secure communication between the source and the relay is possible. Reference [68] considered this multi-hop line network, where a source node aims to communicate securely with a destination via a chain of untrusted relays, and found a secrecy rate that is *independent* of the number of untrusted relays in the network. This result is surprising in that it states that enlisting the cooperation from many untrusted nodes does not penalize the system from the perspective of secure communication. The enabler in this case is introducing judicial interference by the appropriate node at the appropriate time, as well as, introducing structure to the signaling and communication schemes. This model in essence combines all the lessons learned so far in order to provide a scalable end-to-end secure communication rate by untrusted cooperative communication.

In the following, we provide some details on this model and the achievable secrecy scheme. Again, all nodes are assumed to operate in half-duplex mode. Each node is able to receive the signals transmitted by its immediate neighbors, i.e., the nearest nodes on its left and right (Fig. 7). The channel gain between any two neighbors is normalized to unity and an equal average power constraint, P, is assumed at all network nodes. The need for a new achievable scheme, different from the one in [64], follows from the fact that applying a scheme based on compress-and-forward in the line network leads to accumulation of the quantization noise over the hops, and one would end up with an achievable secrecy rate that decreases dramatically as the number of hops increases, eventually with vanishing end-to-end secrecy rate. To overcome this limitation, [68] proposes an achievable secrecy scheme based on the compute-and-forward strategy [56], [57].

In order to illustrate this scheme, let us first consider the simplest case, where the number of relays is equal to 1, i.e., the two-hop network in Fig. 5. First, the source generates a nested lattice codebook that is used as an inner code for the secure message. An outer code, based on stochastic encoding, is also applied at the source. In other words, the nested lattice codebook is divided into bins, with each bin representing one possible realization of the message. The size of each bin is designed to ensure the secrecy of the transmitted message at the relay node. In the first phase, the source chooses a codeword uniformly from the bin indexed by the message and transmits it to the relay, while the destination cooperatively jams the relay with a lattice codeword chosen uniformly from the same nested lattice codebook. The relay decodes the linear combination formed by these two lattice points and then forwards this combination to the destination. Because the destination knows its transmitted lattice point, it can recover the secure message from the received combination. The achievable secrecy rate of this scheme is given by

$$R_s \leq 0.5[C(2P - 0.5) - 1]^+ \tag{26}$$

where the factor 0.5 appears due to the half-duplex nature of the network and $C(2P - 0.5)$ is the rate without secrecy constraints [56]. The one-bit cost of secrecy follows from quantifying the leakage to the eavesdropper precisely with nested lattice codes [49].

At this point, it is instructive to highlight the differences between this scheme and the one proposed in [64]. Here, the source and destination use nested lattice codebooks, while in [64] the source uses Gaussian codebook and the destination jams with a random Gaussian signal. That is to say that, here we use structured signalling on both message transmission and cooperative jamming. In addition, here, the relay node decodes a linear combination of the received codewords and forwards it to the destination (compute-and-forward), while in [64] the relay compresses its received signal and transmits a quantized version of it to the destination (compress-and-forward). The advantage of both of these will be apparent next in the multi-hop set up.

Now, consider extending this scheme to the line network. The extension entails careful scheduling of transmissions. In the first phase, while the source node transmits its secure message to the first relay (its immediate neighbor to the right) using a lattice codeword, simultaneously, the second relay cooperatively jams the first relay with a random lattice codeword. Then, the first relay decodes the linear combination of these two lattice points reliably, thereby, removing the channel noise in this hop and preventing it from propagating through subsequent hops. The first relay then forwards what it decoded using a lattice codeword to the second relay during the second phase. Simultaneous to the first relay's transmission to the second, the third relay jams the second with a random lattice point. Now, the second relay has received a combination of three lattice points, one of which is known to it, i.e., its cooperative jamming signal it sent during the previous phase. Hence, a combination of two lattice points is obtained by the second relay by removing the known

point. In the next phase, the second relay forwards this combination to the third, while the forth relay is jamming the third, and so on and so forth, until the destination is reached. In other words, each of the relays, except the first one, receives a combination of three lattice points, one represents the secure message, one represents its jamming signal, and the last one is the jamming signal of the node on its right. After removing its own jamming lattice point, the relay forwards the linear combination of the two remaining lattice points to the node on its right, until the destination. The last relay on the left of the destination forwards a combination of the secure message and the jamming signal sent by the destination in the previous phase, thus, from this combination, the destination is able to recover the secure message, and achieve the secrecy rate given in (26). It is worth noting that all intermediate untrusted relays are prevented from decoding the message by way of covering them with a lattice jamming signal and that the rate obtained by each hop is identical, making the end-to-end secrecy rate independent of the number of untrusted relays. Comparing the achievable secrecy rate with that of the achievable rate of the compute-and-forward without secrecy constraints, one can readily quantify the cost of secrecy as at most 0.5 bit per channel use, irrespective of the number of hops.

VI. DISCUSSION AND FUTURE DIRECTIONS

In this paper, we have summarized lessons learned from information-theoretic secrecy studies on multi-transmitter wireless communication scenarios. Our focus has been distilling design insights leading to three main findings that are beneficial from the perspective of providing reliable communication rates with information-theoretic security guarantees. They are 1) carefully and judiciously introducing interference to the communication medium; 2) using structure in signalling schemes; and 3) cooperating with unauthenticated entities rather than treating them as mere eavesdroppers. Such design insights can be helpful in clean slate approaches that are yet to materialize but will likely to be in the future, in particular with a very large number of wireless devices of various capabilities coexisting and connecting in the internet-of-things era.

The studies we summarized are those that were conducted in the first decade of wireless physical-layer security. As such, they stem from a fundamental information-theoretic capacity approach, which relies on a number of idealized assumptions. These include altruistic nodes that are willing to expend their power for improving secure communication rates for others, a potentially losing proposition for energy limited mobile wireless nodes; as well as knowing channel qualities of various nodes including those of external eavesdroppers, again a potentially impractical assumption. Furthermore, the secrecy guarantees provided ensure only vanishing *rate* of information leakage.

It should be noted, however, that none of these are show stoppers for information-theoretic security principles to be brought to reality in the future. For example, via appropriate game-theoretic mechanisms, even selfish nodes can be incentivized to participate as cooperative jammers [69]. Various studies have been conducted in recent years, and are currently being conducted that find mechanisms for providing secrecy in the absence of complete or perfect channel knowledge of the parties. Of those, studies that provide secrecy without the channels of external (adversarial) eavesdroppers are especially significant in that a passive adversary that does not transmit any signal is difficult to obtain any channel information from. Such studies bring further insights, for example with respect to coding strategies in fading channels with statistical knowledge of Eve's CSI only [23], or providing secrecy in the high SNR regime without Eve's CSI for *almost all* channel gain values, except for a set with Lebesgue measure zero [70]. There are further stronger results that prove the existence of a universal coding scheme and provide secrecy for *all* channel conditions by means of using multiple antennas [35]. Such studies point to the potential of information-theoretic security to be able to counter stronger models by means of physical resources, i.e., antennas. The concerns on weak secrecy guarantees can often be alleviated by proving strong secrecy by either extending the weak secrecy proofs or proving strong secrecy directly [35], including for multi-terminal models [71]. Further progress in each of these directions will be helpful for realizing the vision of keyless unbreakable security for wireless communications.

In conclusion, information-theoretic security approaches continue to inspire wireless communications system design that considers security as a quality of service requirement just as reliability. While the first decade has made significant progress with theoretical insights and existence results, there is still much to do before an information-theoretically secure communication system is deployed. Practical communication and coding mechanisms with realistic system deployment assumptions are of current interest of the research community. ■

Acknowledgment

A. Yener would like to thank Mohamed Nafea and Ahmed Zewail for their help with figures.

Dedication

A. Yener dedicates this paper to the loving memory of Henna (04.01.2003–01.03.2015) whose lifespan coincided with the author's research in this subject area, and the joy that she brought to the author's life has certainly inspired the research ideas.

REFERENCES

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[3] "RSA factoring challenge." [Online]. Available: http://en.wikipedia.org/wiki/RSA-Factoring-Challenge

[4] T. Kleinjung *et al.*, "Factorization of a 768-Bit RSA modulus," in *Advances in Cryptology—CRYPTO 2010*, ser. Lecture Notes in Computer Science, Berlin, Germany: Springer, 2010, pp. 333–350.

[5] A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of A5/1 on a PC." [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/gsm.html

[7] D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the cellular message encryption algorithm." [Online]. Available: http://www.schneier.com/paper-cmea.html

[8] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

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

[10] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology—EUROCRYPT 2000*. Berlin, Germany: Springer-Verlag, 2000, pp. 351–368.

[11] J. Barros and M. Bloch, "Strong secrecy for wireless channels," in *Information-Theoretic Security*, ser. Lecture Notes in Computer Science, vol. 5155. Berlin, Germany: Springer, 2008, pp. 40–53.

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

[13] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Advances in Cryptology—CRYPTO 2012*, ser. Lecture Notes in Computer Science, vol. 7417. Berlin, Germany: Springer, 2012, pp. 294–311.

[14] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.

[15] M. Bloch and J. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

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

[17] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *Proc. 2014 IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2014, pp. 601–605.

[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, USA: Wiley-Interscience, 2006.

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

[20] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proc. 39th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2005.

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

[22] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 1296–1300.

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

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

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

[26] Y. Liang, G. Kramer, H. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, Oct. 2009, Art. ID. 142374.

[27] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fast rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792–2799, Sep. 2010.

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

[29] P. Mukherjee and S. Ulukus, "Fading wiretap channel with no CSI anywhere," in *Proc. 2013 IEEE Int. Symp. Inf. Theory Proc.*, July 2013, pp. 1347–1351.

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

[31] 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.

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

[33] 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. 2493–2507, Jun. 2008.

[34] 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, 2011.

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

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

[37] X. He, A. Khisti, and A. Yener, "MIMO broadcast channel with an unknown eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 246–255, Jan. 2014.

[38] 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.

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

[40] 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.

[41] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2730–2745, May 2011.

[42] X. He and A. Yener, "The interference wiretap channel with an arbitrarily varying eavesdropper: Aligning interference with artificial noise," in *Proc. 50th Annu. Allerton Conf. Commun. Control Comput.*, Oct. 2012.

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

[44] M. Bloch and J. Barros, *Physical-Layer Security From Information Theory to Security Engineering*. New York, USA: Cambridge Univ. Press, 2011.

[45] E. Tekin and A. Yener, "The Gaussian multiple-access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006.

[46] 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, 2008.

[47] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. 46th Annu. Allerton Conf. Commun. Control Comput.*, Sep. 2008, pp. 1014–1021.

[48] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proc. 44th Annu. Allerton Conf. Commun. Control Comput.*, Sep. 2006.

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

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

[51] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[52] 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.

[53] V. Cadambe, S. Jafar, and S. Shamai, "Interference alignment on the deterministic channel and application to fully connected Gaussian interference networks," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 269–274, Jan. 2009.

[54] U. Erez and R. Zamir, "Achieving 1/2 log (1+SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.

[55] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3401–3416, Oct. 2005.

[56] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.

[57] M. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641–5654, Nov. 2010.

[58] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, Mar. 2012.

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

[60] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2001.

[61] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007.

[62] T. M. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 9, pp. 572–584, 1979.

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

[64] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wireless Commun. Netw.*, Nov. 2009, Art. ID. 305146.

[65] H. Yamamoto and K. Itoh, "Source coding theory for multiterminal communication systems with a remote source," *Trans. IECE Jpn.*, vol. E-63, pp. 700–706, Oct. 1980.

[66] A. Zewail and A. Yener, "The multiple access channel with an untrusted relay," presented at the *IEEE Inf. Theory Workshop*, Nov. 2014.

[67] A. A. Zewail, M. Nafea, and A. Yener, "Multi-terminal networks with an untrusted relay," in *Proc. 52nd Annu. Allerton Conf. Commun. Control Comput.*, Sep. 2014.

[68] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 1–11, 2013.

[69] 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, 2013.

[70] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Proc. Conf. Inf. Sci. Syst.*, Mar. 2013.

[71] M. Yassaee and M. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. IEEE Inf. Theory Workshop*, Aug. 2010, pp. 1–5.

ABOUT THE AUTHORS

Aylin Yener (Fellow, IEEE) received the B.Sc. degree in electrical and electronics engineering, and the B.Sc. degree in physics, from Bogazici University, Istanbul, Turkey and the M.S. and Ph.D. degrees in electrical and computer engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, New Brunswick, NJ, USA.

She has been a Professor of Electrical Engineering at The Pennsylvania State University, University Park, PA, USA, since 2010, where she joined the faculty as an Assistant Professor in 2002. During the academic year 2008–2009, she was a Visiting Associate Professor with the Department of Electrical Engineering, Stanford University, Stanford, CA, USA. Her research interests are in information theory, communication theory, and network science with recent emphasis on green communications and information security.

Dr. Yener received the NSF CAREER award in 2003, the best paper award in Communication Theory in the IEEE International Conference on Communications in 2010, the Penn State Engineering Alumni Society (PSEAS) Outstanding Research Award in 2010, the IEEE Marconi Prize paper award in 2014, the PSEAS Premier Research Award in 2014, and the Leonard A. Doggett Award for Outstanding Writing in Electrical Engineering at Penn State in 2014. She is currently a member of the board of governors of the IEEE Information Theory Society where she was previously the treasurer (2012–2014). She served as the student committee chair for the IEEE Information Theory Society 2007–2011, and was the co-founder of the Annual School of Information Theory in North America co-organizing the school in 2008, 2009, and 2010. She was a technical (co)-chair for various symposia/tracks at IEEE ICC, PIMRC, VTC, WCNC and Asilomar (2005–2014), and served as an editor for IEEE Transactions on Communications (2009–2012), an editor and an editorial advisory board member for IEEE Transactions on Wireless Communications (2001–2012), a guest editor for IEEE Transactions on Information Forensics and Security (2011) and a guest editor for IEEE Journal on Selected Areas in Communications (2015).

Sennur Ulukus (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, New Brunswick, NJ, USA and the B.S. and M.S. degrees in electrical and electronics engineering from Bilkent University, Ankara, Turkey.

She is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, MD, USA, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. Her research interests are in wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, information-theoretic physical-layer security, and energy harvesting communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, an 2005 NSF CAREER Award, the 2010–2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 George Corcoran Education Award. She served as an Associate Editor for the IEEE Transactions on Information Theory (2007–2010) and IEEE Transactions on Communications (2003–2007). She served as a Guest Editor for the IEEE Journal on Selected Areas in Communications for the special issue on wireless communications powered by energy harvesting and wireless energy transfer (2015), *Journal of Communications and Networks* for the special issue on energy harvesting in wireless networks (2012), IEEE Transactions on Information Theory for the special issue on interference networks (2011), IEEE Journal on Selected Areas in Communications for the special issue on multiuser detection for advanced communication systems and networks (2008). She served as the TPC co-chair of the 2014 IEEE PIMRC, Communication Theory Symposium at 2014 IEEE Globecom, Communication Theory Symposium at 2013 IEEE ICC, Physical-Layer Security Workshop at 2011 IEEE Globecom, Physical-Layer Security Workshop at 2011 IEEE ICC, 2011 Communication Theory Workshop (IEEE CTW), Wireless Communications Symposium at 2010 IEEE ICC, Medium Access Control Track at 2008 IEEE WCNC, and Communication Theory Symposium at 2007 IEEE Globecom. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007–2009.