INVITED PAPER

Broadcast Networks With Layered Decoding and Layered Secrecy: Theory and Applications

This paper explores how ordering of channel quality among multiple users can translate into users having progressively greater access to information or being progressively restricted.

By Shaofeng Zou, *Student Member IEEE*, Yingbin Liang, *Member IEEE*, Lifeng Lai, *Member IEEE*, H. Vincent Poor, *Fellow IEEE*, and Shlomo Shamai, *Fellow IEEE*

ABSTRACT | Recent information-theoretic results on a class of broadcast channels with layered decoding and/or layered secrecy are reviewed. In this class of models, a transmitter sends multiple messages to a set of legitimate receivers in the presence of a set of eavesdroppers, whose channels can be ordered based on the quality of received signals. Receivers with better channel quality are required to decode more messages, and eavesdroppers with worse channel quality are required to be kept ignorant of more messages. The design of achievable schemes and the characterization of the corresponding secrecy capacity regions are presented. Comparison of the designs for different models is discussed. Applications of these information-theoretic models to the study of secure communication over fading wiretap channels and secret sharing are also presented to illustrate potential applications of these models.

KEYWORDS | Broadcast channel; fading wiretap channel; layered decoding; layered secrecy; secrecy capacity region; secret sharing

I. INTRODUCTION

In wireless networks, communication signals are transmitted via open medium of free space, and hence can be easily eavesdropped upon by any receiver within transmission range. This broadcast nature of radio channels is one of the major challenges to the design of secure wireless communications. Some commonly used security approaches employed in current wireless systems may encounter potential problems as wireless networks incorporate more communication patterns and flexible structures. For example, a popular approach to secure wireless communications is to predeploy a secret certificate into mobile devices, based on which devices can establish keys. However, for device-to-device (D2D) communications recently proposed for LTE networks, such an approach cannot adapt easily to allow a mobile device to directly communicate with a large set of devices in a unicast fashion. Furthermore, public-key based

Manuscript received January 28, 2015; revised May 2, 2015 and July 12, 2015; accepted July 13, 2015. Date of publication September 14, 2015; date of current version September 16, 2015. The work of S. Zou and Y. Liang was supported by a National Science Foundation CAREER Award under Grant CCF-10-26565 and by the National Science Foundation under Grant CNS-11-16932. The work of L. Lai was supported by a National Science Foundation CAREER Award under Grant CCF-13-18980 and the National Science Foundation under Grant ECCS-14-08114. The work of H. V. Poor was supported by the National Science Foundation under Grant CMMI-1435778. The work of S. Shamai (Shitz) was supported by the Israel Science Foundation (ISF), and the European Commission in the framework of the Network of Excellence in Wireless COMmunications NEWCOM#.

S. Zou and **Y. Liang** are with the Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY 13244 USA (e-mail: szou02@syr.edu; yliang06@syr.edu).

L. Lai is with the Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609 USA (e-mail: llai@wpi.edu).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

S. Shamai is with the Department of Electrical Engineering, Technion—Israel Institute of Technology, Technion City, Haifa 32000 Israel (e-mail: sshlomo@ee.technion.ac.il).

Digital Object Identifier: 10.1109/JPROC.2015.2458338

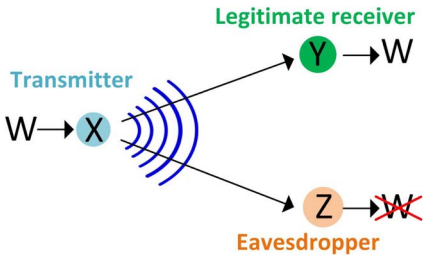


Fig. 1. *Wyner's wiretap model.*

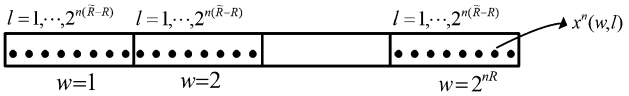


Fig. 2. *Illustration of random binning.*

encryption is also not applicable in many cases, as mobile devices may not be equipped with sufficiently high computational resources for implementing public-key algorithms.

In the seminal work of Wyner [1], a physical-layer approach to secrecy was proposed, which exploits randomness in statistical communication channels as resources to achieve secure communications. Without inherently employing secret keys, such a new security approach, if applied to wireless networks, can significantly reduce requirements on the infrastructure and improve communication flexibility and dynamics. It is therefore instructive to take a more careful look at Wyner's approach and its implications, which we do in the following subsection.

A. Basic Wiretap Channel

In Wyner's model (see Fig. 1), a transmitter wishes to transmit information to a legitimate receiver and to keep the information secure from an eavesdropper.[1] The basic idea of Wyner's scheme is the so-called *stochastic coding* or *random binning* (see Fig. 2). Let w denote the index of the transmitted message with $w \in \{1, 2, \ldots, 2^{nR}\}$, where R denotes the transmission rate. For each w, a bin of codewords $x^n(w, l)$ is constructed, where l denotes the index of codewords within each bin. The codewords for all bins are combined together as a codebook. In order to transmit a message w, the channel input is randomly and uniformly chosen from bin w. In order to guarantee secure communication, the codebook should be constructed to satisfy the condition that the legitimate receiver (based on its received channel output) can always determine which bin the input codeword is from even with channel corruption, and can hence determine which message w was transmitted. However, the eavesdropper can only identify a set of codewords (uniformly distributed over all bins) that may be transmitted based on its received channel output, and is unable to tell which bin the transmitted codeword is likely to be from. Hence, the eavesdropper does not learn any information about the bin number (i.e., the message) w. It can be shown that there exists such a codebook satisfying the above conditions if the transmission rate R satisfies

$$R < \max_{P_X}[I(X;Y) - I(X;Z)] \tag{1}$$

where $I(\cdot,\cdot)$ denotes the mutual information between its arguments. It can be further shown that if the channel is degraded, i.e., the Markov chain condition $X \to Y \to Z$ holds (which implies that the legitimate channel is of better quality than the eavesdropping channel), then the above rate is the largest for which secure communication is guaranteed, which is referred to as the *secrecy capacity*.

It can be observed that the secrecy capacity is in general smaller than or equal to the capacity of the channel. This fact may be misinterpreted as implying that the reliable communication rate is sacrificed in order to achieve secure communication. In fact, this is not the case. In Wyner's binning scheme, the index l within the bin (which is uniformly distributed) was used only for introducing the randomness to confuse the eavesdropper. This index can also be used to carry the transmitter's message,[2] although such information cannot be made secure from the eavesdropper. In this way, the total communication rate can still be equal to the capacity of the channel, and furthermore, part of the transmitted information is made secure from the eavesdropper. From such a perspective, secrecy is provided as an additional benefit rather than sacrificing the communication rate. Of course, the benefit does not come for free, because the codebook should be designed with the binning structure [2]. We refer to a scheme that uses one part of a message to protect another part of the message as the *embedded coding* of messages.

Wyner's result can be further extended to the case in which the legitimate and eavesdropping channels are not degraded. For such a case, in order to achieve the secrecy capacity, random binning is first applied as for Wyner's model. Then the codeword is sent over a virtual prefix channel (chosen by the system designer), and then sent over the actual channel. The prefix channel is useful to provide advantage to the legitimate receiver. Hence, the secrecy capacity is given by

$$C = \max_{P_{UX}}[I(U;Y) - I(U;Z)] \tag{2}$$

[1]The red cross symbol on the message in Fig. 1 represents that the message should be kept secure from the corresponding receiver. This is also applicable to all other figures in the article.

[2]Throughout the article, we assume that all messages are uniformly distributed over their corresponding alphabet sets.

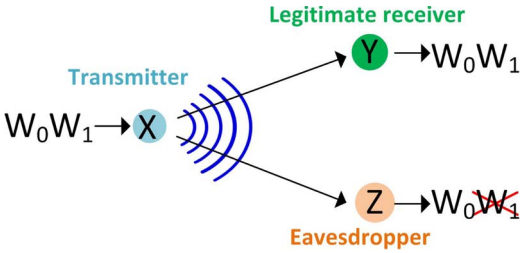


Fig. 3. *Csiszár and Körner's broadcast model.*

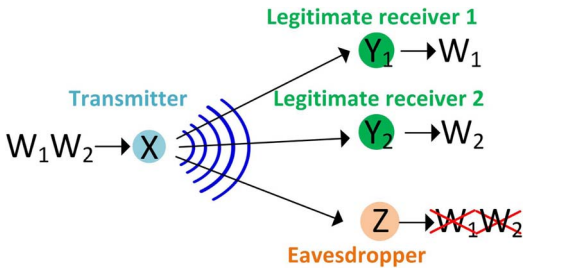


Fig. 4. *Two-user broadcast channel with an additional eavesdropper.*

where U represents the codeword of binning, and the prefix channel is $P_{X|U}$. This result can be specialized from Csiszár and Körner's study in [3] of a more general model (see Fig. 3), in which the transmitter also wants to send a common message to both the legitimate receiver and the eavesdropper in addition to the confidential message intended for the legitimate receiver and required to be kept secure from the eavesdropper.

B. Overview of Broadcast Networks With Secrecy

Following the initial studies in [1] and [3], broadcast channels with various decoding and secrecy constraints have been studied intensively. Due to the upsurge of interest in this topic, it is not possible to address all studies in this article. In the following, we provide an overview of studies that are highly relevant to the topic that this article focuses on here, and refer readers to recent surveys, e.g., [4] and [5], for more comprehensive references.

Wyner's wiretap model was further studied when the legitimate and eavesdropping channels take specific forms. As some key examples, the Gaussian wiretap channel was studied in [6]; the multiple-input–multiple-output (MIMO) wiretap channel with the transmitter, the legitimate receiver, and/or the eavesdropper equipped with multiple antennas was studied in [7]–[12]; and the compound wiretap channel, in which there are multiple legitimate receivers and single/multiple eavesdroppers, was studied in [13]–[17].

Csiszár and Körner's broadcast model was further studied for the Gaussian fading channel in [18], and for the MIMO channel in [19]. This model was generalized in [20] to two compound scenarios, in which the legitimate receiver (i.e., receiver 1) and the eavesdropper (i.e., receiver 2) are respectively replaced by two receivers with the same decoding and secrecy requirements. Furthermore, Csiszár and Körner's model was also generalized in [21] to the compound scenario, in which each receiver is replaced by multiple users.

As further generalizations of the Wyner and Csiszár–Körner models, a class of broadcast channels with an additional eavesdropper (see Fig. 4) were intensively studied. In the model considered in [22] and [23], a transmitter has two independent messages intended for two legitimate receivers, respectively, and wishes to keep the two messages confidential from an (additional) eavesdropper. Such a model was further studied in [24], when the channel is corrupted by additive Gaussian noise. The multiple antenna version of the above model was studied in [25] and [26]. Furthermore, the multiantenna channel was generalized in [27] to the compound scenario with each receiver and the eavesdropper being replaced by a group of colocated users. The model (in Fig. 4) was also generalized and studied in [28] for the case with an arbitrary number of legitimate receivers (and hence with an arbitrary number of independent messages respectively for each receiver), and the fading channel of such a model was studied in [16].

Apart from the above class of broadcast channels, another class of models consisting of receivers that are expected to not only receive certain information from the transmitter but also be kept ignorant of certain other information have also been studied. In the model studied in [29] (see Fig. 5), a transmitter has two independent messages with each intended for one receiver and required to be kept secure from the other receiver. The MIMO version of such a model was studied in [30]–[32]. Furthermore, such a model was generalized in [33] to the case in which the transmitter has one more common message for both receivers, and users are equipped with multiple antennas. The compound scenario of the preceding model with each receiver being replaced by a group of colocated users was studied in [33].

The focus of this article is on a class of broadcast channels with layered decoding and/or layered secrecy, which can be viewed as multiuser (and multimessage)

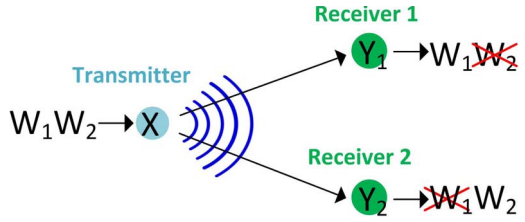


Fig. 5. *Two-user broadcast channel with receivers also treated as eavesdroppers.*

generalizations of the Csiszár–Körner model. More specifically, layered decoding refers to the case in which, as the channel quality gets one level better, one more message is required to be decoded, and layered secrecy refers to the case in which, as the channel quality gets one level worse, one more message is required to be secured. These models are introduced in detail in the next section. In this article, we focus on the degraded broadcast channel, in which the receivers can be ordered in terms of channel quality.

C. The Aim of This Article

Among broadcast models studied so far, a special class of channels have attracted intensive attention, which we refer to as the *degraded broadcast channels with layered decoding and/or layered secrecy*. A common feature that these channels share is that the channels of legitimate receivers and eavesdroppers can be ordered based on the quality of their received signals. Hence, it is natural to require that receivers with better channel quality decode more messages, and eavesdroppers with worse channel quality are kept ignorant of more messages. Here, we focus on degraded channels for two reasons: 1) degraded channels often arise naturally in practical applications such as in the context of Gaussian fading channels that model wireless communication channels; and 2) the performance for degraded channels can often be characterized in simpler forms that can facilitate the illustration of central ideas. However, all achievable schemes designed for degraded channels are applicable to nondegraded channels except that the optimality of the schemes are not easy to prove (due to the difficulty in developing outer bounds that match achievable regions).

Such models often arise in practice. For example, consider the fading wiretap channel, in which the legitimate and eavesdropping channels are corrupted by multiplicative random fading gains. It is typical that the transmitter does not know the fading gains of these channels. In this case, it is desirable that the transmitter can convey as much information as the legitimate channel supports and keep as much information secret as the eavesdropping channel allows. In order for the transmission to adapt to the channel quality without knowing the channel, a broadcast approach is very appealing. The idea is to view the legitimate and eavesdropping channels as having multiple states (i.e., corresponding to the values that fading gains can take), and then design a layered transmission scheme so that more layers can be decoded if the legitimate channel has better quality, and more layers can be made secure if the eavesdropper channel has lower quality. Thus, such an approach naturally yields a degraded broadcast channel with layered decoding and secrecy requirements.

Another example is the secret sharing problem, in which secrets are delivered via a broadcast network from a dealer to a number of participants. The requirements generally include that some groups of users should be able to determine certain secrets by sharing their channel outputs, and some groups of users should be kept ignorant of certain secrets even if they share their outputs. It is of interest to determine at what rates the secrets can be delivered. Such a problem can be naturally viewed as the broadcast channel with secrecy requirements, in which groups that are required to determine secrets should be viewed as legitimate receivers and groups that are required to be ignorant of secrets should be viewed as eavesdroppers. Layers appear when multiple groups are required to determine and/or be ignorant of different sets of secrets.

In this article, we focus on such a class of broadcast models with layered decoding and secrecy, aiming at providing insights into understanding the fundamental limits on secure communication rates for these models and inspiring further applications. We also hope that this article can help to identify new and interesting models in this class, and can motivate new applications of information-theoretic results developed for this class of models. For such a purpose, we provide an overview of the state-of-the-art information-theoretic studies of this class of models as well as presenting our new results on an extended model. More specifically, we present the design of achievable schemes for the models in this class, comparison of designs for different models, and the performance of the designed schemes (i.e., the secrecy capacity region). We also describe applications of these information-theoretic results to studying the fading wiretap channel and solving the problem of secret sharing in the context of wireless networks as we describe above. These applications demonstrate the broad contexts in which this class of information-theoretic models can be useful.

II. INFORMATION-THEORETIC MODELS

In this section, we provide a review of recent information-theoretic results on a class of degraded broadcast models with layered decoding and/or layered secrecy. In fact, these models can be unified under a more general framework, in which a transmitter sends a number of messages to a set of receivers over a broadcast channel, and the receivers' channel quality can be ordered in a certain way. Each receiver can possibly serve as a legitimate user expecting a certain subset of messages, and/or as an eavesdropper that should be kept ignorant of a certain subset of messages. For each special model we present next, we include both a high-level introduction of the model and the design of communication schemes, and a more technical description for readers who are interested in greater technical depth.

In the following, we list a few major techniques that can be exploited to design the achievable schemes, which accommodate the requirements of layered decoding and layered secrecy. Jointly using these techniques has been shown to yield optimal designs for various models of interest.

1) Superposition Coding: (Introduced in Section II-A) Messages are encoded into a set of layers, which are superposed on one another. This scheme is useful when there are requirements of layered decoding, so that receivers have flexibility to decode various layers of messages.

2) Random Binning: (Introduced in Section I) Within each (superposition) layer, codewords are divided into a number of bins. The messages are indexed by the bin number, and the index within the bin serves as a random source to protect the messages.

3) Embedded Coding: (Introduced in Section I) When a codeword is encoded with multiple message indices, or multiple messages are encoded into different layers, lower layer messages can serve as a random source to protect higher layer messages. Such a scheme is useful when there are requirements of layered secrecy.

4) Rate Sharing: (Introduced in Section II-D) The rate of a message, which satisfies the same decoding and secrecy requirements with other messages can be shared with these messages to enlarge the achievable region.

Throughout this section, we introduce how the above schemes are exploited to design the achievable schemes in each specific model as well as comparing the use of these schemes in different models.

A. Layered Decoding and Non-layered Secrecy

In this subsection, we present the model for the degraded broadcast channel with layered decoding and non-layered secrecy [28] (see Fig. 6). In this model, a transmitter sends K messages $W_1, \ldots, W_K$ to K receivers in the presence of an eavesdropper over a degraded broadcast channel. The channel quality is assumed to gradually degrade from receiver K to receiver 1, and each legitimate receiver has a better channel than the eavesdropper. The system is required to satisfy the layered decoding requirement, i.e., receiver k is required to decode the first k messages $W_1, \ldots, W_k$, and to satisfy the secrecy requirement, i.e., the eavesdropper needs to be kept ignorant of all messages $W_1, \ldots, W_K$.

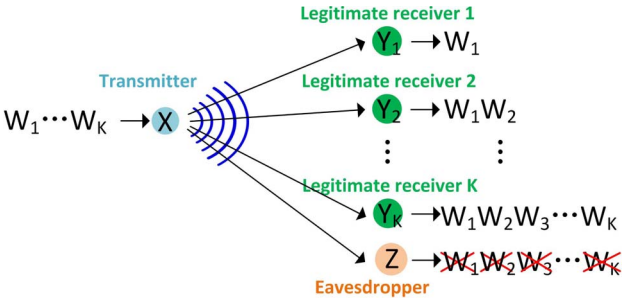


Fig. 6. *Broadcast channel with layered decoding and non-layered secrecy.*

More technically, the broadcast channel is characterized by the probability transition function $P_{ZY_1\cdots Y_K|X}$, in which $X \in \mathcal{X}$ is the channel input, $Y_k \in \mathcal{Y}_k$ is the channel output of receiver k for $k = 1, \ldots, K$, and $Z \in \mathcal{Z}$ is the channel output of the eavesdropper. The channel satisfies the following Markov chain condition (i.e., the degradedness condition):

$$X \to Y_K \to Y_{K-1} \to \cdots \to Y_2 \to Y_1 \to Z \tag{3}$$

where the notation $X \to Y \to Z$ means that X and Z are independent given Y.

Such a model captures practical scenarios, in which legitimate receivers are close to the sender and the eavesdroppers are far away. For example, consider the following location-based applications. A company wishes to share confidential files among its employees within an office building, and wishes to keep these files secure from anybody outside of the building. Another example is when a coffee shop wishes to provide streaming movie services to its customers inside the shop but not to people outside.

The special case with $K = 2$ of the above model was studied in [25, model 1], and the secrecy capacity region was characterized. This two-receiver model was further generalized to a compound model in [27], in which each legitimate receiver and the eavesdropper were replaced respectively by a group of legitimate receivers and eavesdroppers, and the secrecy capacity region was characterized. The general model with K receivers was studied in [28], following which we present the results of this model.

The idea of the achievable scheme exploits the joint design of superposition coding, random binning and rate sharing. More specifically, since multiple messages need to be sent over one input, layers of codewords are designed and *superposed* on one another (see Fig. 7). The lowest layer of codewords carries only message W_1, and each upper layer of codewords carries one more message than its next lower layer. Since all messages are required to be secured from the eavesdropper, each layer employs a *random binning* scheme, i.e., each message in a layer corresponds to a bin of codewords indexed by l. If a message is selected to be transmitted, then one codeword inside the corresponding bin is randomly uniformly selected to be transmitted. An interesting point is that for each layer, say layer k, the index l_k inside the bin serves as a random source to protect not only message W_k in this layer but also all higher layer messages $W_{k+1}, \ldots, W_K$, which reflects a more efficient design. At the receiver side, receiver 1 (with the worst channel quality) decodes only the lowest layer, i.e., W_1, and then receiver 2 first decodes W_1 over layer 1, and then decodes W_2 over the part of layer 2 corresponding

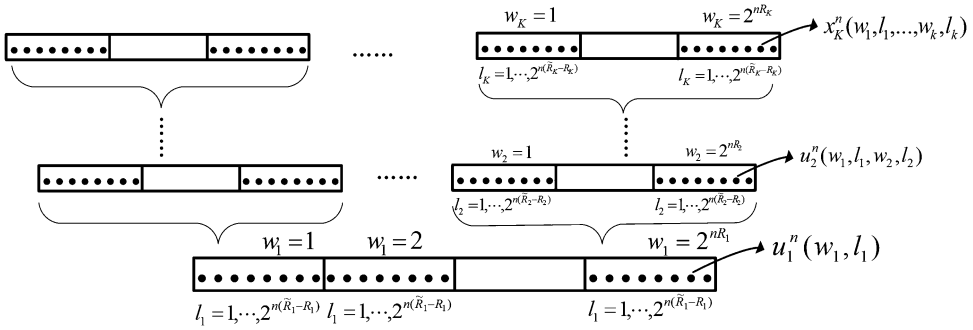


Fig. 7. ***Illustration of joint design of superposition and binning.***

to the correct W_1. This procedure can continue in the same successive fashion until receiver K, which has the best channel quality, decodes all messages successively. Moreover, since each receiver decodes messages intended for receivers with worse channel quality, the rates of receivers with worse channel quality can be *shared* to increase the rates of the receivers with better channel quality, which is reflected in the sum rate bounds in Theorem 1.

More technically, in [28], it is shown that the above achievable scheme is optimal, i.e., achieves the secrecy capacity region characterized in the following theorem.

Theorem 1 [28, Th. 1]: The secrecy capacity region of the degraded broadcast channel with layered decoding and non-layered secrecy contains all rate tuples $(R_1, \ldots, R_K)$ satisfying the following inequalities:

$$R_1 + \cdots + R_l \leq \sum_{k=1}^{l} I(U_k; Y_k|U_{k-1}) - I(U_l; Z), \quad \text{for } l = 1, \ldots, K \tag{4}$$

where $U_0 = \Phi$, $U_K = X$, and for some distribution $P_{U_1 U_2 \ldots U_{K-1} X}$ satisfying the following Markov chain condition:

$$U_1 \to U_2 \to \cdots \to U_{K-1} \to X. \tag{5}$$

In the above theorem, $U_1, \ldots, U_{K-1}$ represent codeword information in layers $1, \ldots, K-1$, respectively, and the channel input X represents codeword information in the highest layer K.

B. Non-Layered Decoding and Layered Secrecy

In this subsection, we present the model of the degraded broadcast channel with non-layered decoding and layered secrecy (see Fig. 8). In this model, a transmitter sends K messages $W_1, \ldots, W_K$ to one legitimate receiver in the presence of K eavesdroppers. It is assumed that the legitimate receiver has the best channel quality, and the channel quality gradually degrades from eavesdropper K to eavesdropper 1. The legitimate receiver is required to decode all messages $W_1, \ldots, W_K$, and the eavesdroppers are required to satisfy the layered secrecy requirements, i.e., the eavesdropper k needs to be kept ignorant of the messages $W_k, \ldots, W_K$, for $k = 1, \ldots, K$. In this case, an eavesdropper with worse channel quality is required to be ignorant of more messages than those eavesdroppers with better channel quality.

More technically, the broadcast channel is characterized by the probability transition function $P_{Z_1, \ldots, Z_K, Y|X}$, in which $X \in \mathcal{X}$ is the channel input, $Y \in \mathcal{Y}$ is the channel output at the legitimate receiver, and $Z_k \in \mathcal{Z}_k$ is the channel output at eavesdropper k for $1 \leq k \leq K$. The channel satisfies the following Markov chain condition (i.e., the degradedness condition):

$$X \to Y \to Z_K \to \cdots \to Z_2 \to Z_1. \tag{6}$$

Such a model captures scenarios in which the eavesdroppers' access to information can be ranked, and it is the system designer's choice to determine how to protect the transmitted information in the best way. Then, it is reasonable to index the information based on the security levels of these messages. The most secret information should be given the highest index so that it is kept secure

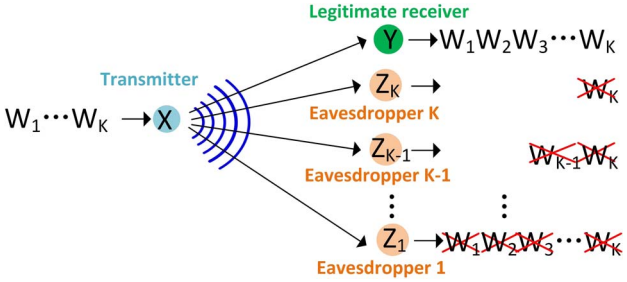


Fig. 8. ***Broadcast channel with layered secrecy.***

from the eavesdropper even with the best channel access, and messages requiring only low security levels can be given lower indices and can be kept secure only from eavesdroppers with worse channel access.

For this model, superposition coding is unnecessary because the decoding is only at one legitimate receiver, and is not done in a layered fashion. In order to achieve the layered secrecy requirement, *embedded coding* [34] is employed jointly with random binning. Such an approach can be intuitively understood as follows: no matter what channel quality an eavesdropper has, sufficient rate of the embedded messages is used to exhaust the decoding capability of the eavesdropper [35] such that the remaining embedded messages are kept confidential from the eavesdropper. More specifically, each codeword is indexed by both a random index and message indices as $x^n(l, W_1, \ldots, W_K)$. The random index l protects messages in the same fashion as for Wyner's model. Each message, say W_k, plays two roles: carrying the message W_k, and protecting higher indexed messages $W_{k+1}, \ldots, W_K$ from being learned by eavesdroppers with better channel quality. On the other hand, the random index l and all message indices $W_1, \ldots, W_{k-1}$ serve as random sources to protect message W_k. Such an approach is more efficient than creating one set of random indices for protecting each message. Moreover, due to the degradedness condition, the messages secured from eavesdroppers with better channel quality is also secured from eavesdroppers with worse channel quality. Hence, the rates of messages secured from eavesdroppers with better channel quality can be *shared* with the rates of messages secured from eavesdroppers with worse channel quality to improve the rate region, which is reflected in the sum rate bounds in Theorem 2.

The above scheme was employed in [36] to study a fading wiretap channel. To be consistent, we present the secrecy capacity region for a discrete memoryless channel in the following theorem.

Theorem 2: For the degraded broadcast channel with non-layered decoding and layered secrecy, the secrecy capacity region contains all rate tuples $(R_1, \ldots, R_K)$ satisfying:

$$\sum_{l=k}^{K} R_l \le \max_{P_X} [I(X;Y) - I(X;Z_k)], \qquad \text{for } k = 1, \ldots, K.$$

We note that for each pair of the legitimate receiver and an eavesdropper (say eavesdropper k), the channel can be viewed as Wyner's wiretap channel with the eavesdropper being ignorant of messages $W_k, \ldots, W_K$. Thus, the sum of secrecy rates $\sum_{l=k}^{K} R_l$ should be bounded by the secrecy capacity of Wyner's wiretap channel given in (1). This implies that the above rate region is optimal.

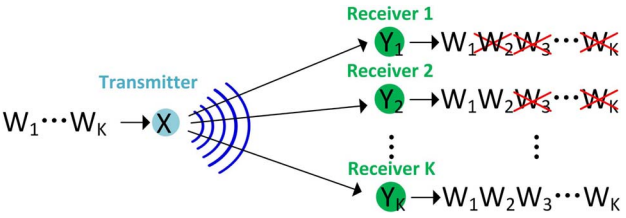


Fig. 9. *Broadcast channel with layered decoding and secrecy.*

C. Layered Decoding and Layered Secrecy

In this subsection, we present the model of the degraded broadcast channel with layered decoding and layered secrecy constraints [37] (see Fig. 9). In this model, a transmitter sends K messages $W_1, W_2, \ldots, W_K$ to K receivers over a degraded broadcast channel. It is assumed that the channel quality gradually degrades from receiver K to receiver 1. Receiver K with the best channel quality is required to decode all messages, and as the channel quality gets worse, each receiver is required to decode fewer messages, i.e., receiver k is required to decode the first k messages $W_1, W_2, \ldots, W_k$. Unlike the previous two models, here each receiver plays two roles: as a legitimate receiver and as an eavesdropper. As the channel quality gets worse, each receiver is required to be kept ignorant of more messages, i.e., receiver k is required to be kept ignorant of messages $W_{k+1}, \ldots, W_K$, for $k = 1, \ldots, K$. Thus, both decoding and secrecy constraints have a layered structure.

More technically, the channel can be characterized by the probability transition function $P_{Y_1 \cdots Y_K|X}$, in which $X \in \mathcal{X}$ is the channel input and $Y_k \in \mathcal{Y}_k$ is the channel output of receiver k for $k = 1, \ldots, K$. The channel outputs $Y_1, \cdots, Y_K$ satisfy the following Markov chain condition (degradedness condition):

$$X \to Y_K \to Y_{K-1} \to \cdots \to Y_2 \to Y_1. \tag{7}$$

Such a model captures practical scenarios in which users are ranked to receive files with different security levels. For example, a WiFi network in a company consists of a number of legitimate users. Users with certain ranks are allowed to receive files up to a certain security level, and should be kept ignorant of files with higher security levels. Hence, users with higher ranks are able to see more files. It is also possible to set the channel quality based on users' ranks by assigning more communication resources to higher ranked users. Another example arises in social networks in which one user wishes to share more resources with close friends and fewer resources with other friends. As we show in the next section, this model is equivalent to a secret sharing problem.

The special case with $K = 3$ and $\mathcal{W}_1 = \Phi$ (i.e., receiver 1 serves as a pure eavesdropper) of the above model was studied in [25, model 2], and the secrecy capacity region was characterized. This two-receiver one-eavesdropper model was further generalized into a compound model in [27], in which each legitimate receiver and the eavesdropper were replaced respectively by a group of legitimate receivers and eavesdroppers, and the secrecy capacity region was also characterized. The general model with K receivers was recently studied in [37], following which we present the results in this subsection.

The idea of the achievable scheme is similar to that introduced in Section II-A, which exploits superposition coding and random binning. For each message, say W_k, one layer is designed and superimposed on the layer designed for W_{k-1}. The codewords within each layer are further divided into a number of bins, and the corresponding message is encoded as the bin number, while the index inside the bin serves as a random source to protect the message. Thus, the receivers that are required to decode this message can tell which bin the codeword is in and hence decode the message, while those receivers with worse channel quality are kept ignorant of the message. Unlike the achievable schemes described in Section II-A, random binning within one layer only protects the message corresponding to the same layer. For example, the index l_k can protect only W_k from being known by receiver $k-1$, but cannot protect W_{k+1}, because W_{k+1} should be kept secure from receiver k which knows l_k due to decoding requirements.

The above scheme was shown to be optimal in [37], which achieves the secrecy capacity region presented below.

Theorem 3 [37, Th. 1]: The secrecy capacity region of the degraded broadcast channel with layered decoding and secrecy constraints contains all rate tuples $(R_1, \ldots, R_K)$ satisfying

$$\begin{aligned} R_1 &\le I(U_1; Y_1) \\ R_k &\le I(U_k; Y_k|U_{k-1}) - I(U_k; Y_{k-1}|U_{k-1}) \\ &\qquad \text{for } k = 2, \ldots, K-1 \\ R_K &\le I(X; Y_K|U_{K-1}) - I(X; Y_{K-1}|U_{K-1}) \end{aligned} \tag{8}$$

for some $P_{U_1U_2\ldots U_{K-1}X}$ such that the following Markov chain condition holds:

$$U_1 \to U_2 \to \cdots \to U_{K-1} \to X. \tag{9}$$

In the above theorem, for $k = 2, \ldots, K-1$, U_k (given U_{k-1}) represents message W_k, which is required to be decoded by receiver k and be kept secure from receiver $k-1$. Thus, the rate R_k given above can be understood intuitively as the secrecy capacity of Wyner's wiretap channel with the channel input U_k, the legitimate output Y_k (given U_{k-1}) and the eavesdropping output Y_{k-1} (given U_{k-1}). We also note that message W_K is represented by the channel input X given U_{K-1}.

The degraded Gaussian MIMO broadcast channel was further studied in [37]. We present the result here which is useful for solving a secret sharing problem presented in Section III-B. For the Gaussian MIMO channel, the received signal at receiver k for one channel use is given by

$$\mathbf{Y}_k = \mathbf{X} + \mathbf{Z}_k, \qquad k = 1, \ldots, K \tag{10}$$

where the channel input $\mathbf{X}$, the channel output $\mathbf{Y}_k$ and the noise $\mathbf{Z}_k$ are r-dimensional vectors. Furthermore, the noise variables $\mathbf{Z}_k$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_k$ for $k = 1, \ldots, K$ that satisfy the following order:

$$\mathbf{0} \prec \mathbf{\Sigma}_K \preceq \mathbf{\Sigma}_{K-1} \preceq \cdots \preceq \mathbf{\Sigma}_1 \tag{11}$$

where $A \preceq B$ denotes that $B - A$ is positive semidefinite. Thus, the quality of channels gradually degrades from receiver K to receiver 1. The channel input $\mathbf{X}$ is subject to a covariance constraint

$$E[\mathbf{X}\mathbf{X}^\top] \preceq \mathbf{S} \tag{12}$$

where $\mathbf{S} \succ \mathbf{0}$. The power constraint on X can further be imposed by requiring $trace(S) \le P$. Since the secrecy capacity region does not depend on the correlation across the channel outputs, the correlation between the noise vectors can be adjusted such that the channel inputs and channel outputs satisfy the following Markov chain condition:

$$\mathbf{X} \to \mathbf{Y}_K \to \mathbf{Y}_{K-1} \to \cdots \to \mathbf{Y}_2 \to \mathbf{Y}_1. \tag{13}$$

For the MIMO channel, the achievability of the secrecy capacity region follows directly from Theorem 3 with a proper choice of the joint Gaussian distribution for auxiliary random variables. The main technical development in the converse (i.e., outer bound) proof lies in the construction of a series of covariance matrices representing input resources for layered messages such that the secrecy rates can be upper bounded as the desired recursive forms in terms of these covariance matrices. We now present the secrecy capacity region in the following theorem.

Theorem 4 [37, Th. 3]: The secrecy capacity region of the degraded Gaussian MIMO broadcast channel with layered decoding and secrecy constraints contains all rate tuples $(R_1, \ldots, R_K)$ satisfying the following inequalities:

$$
\begin{aligned}
R_1 &\le \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1+\mathbf{S}|}{|\mathbf{\Sigma}_1+\mathbf{S}_1|}\\
R_k &\le \frac{1}{2}\log\frac{|\mathbf{\Sigma}_k+\mathbf{S}_{k-1}|}{|\mathbf{\Sigma}_k+\mathbf{S}_k|}-\frac{1}{2}\log\frac{|\mathbf{\Sigma}_{k-1}+\mathbf{S}_{k-1}|}{|\mathbf{\Sigma}_{k-1}+\mathbf{S}_k|}\\
&\quad \text{for } 2\le k\le K-1\\
R_K &\le \frac{1}{2}\log\frac{|\mathbf{\Sigma}_K+\mathbf{S}_{K-1}|}{|\mathbf{\Sigma}_K|}-\frac{1}{2}\log\frac{|\mathbf{\Sigma}_{K-1}+\mathbf{S}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|} \qquad (14)
\end{aligned}
$$

for some $\mathbf{0}\preceq\mathbf{S}_{K-1}\preceq\mathbf{S}_{K-2}\preceq\cdots\preceq\mathbf{S}_2\preceq\mathbf{S}_1\preceq\mathbf{S}$.

The above theorem can be easily understood in the scalar case, in which Σ_k is the variance of noise at receiver k, and $S_{k-1}-S_k$ represents the signal power allocated to transmitted message W_k for $k=1,\ldots,K$. Thus, the rate R_k is given by the difference of the capacities of two Gaussian channels with one having receiver k and one having receiver $k-1$.

D. Layered Decoding and Layered Secrecy With Secrecy Outside a Bounded Range

For the model with layered decoding and secrecy described in Section II-C, the additional message decoded by a better receiver needs to be kept confidential from a receiver with only one level worse channel quality (i.e., layered secrecy and zero secrecy range). Although such a model is feasible for broadcast channels with discrete states (i.e., the quality of receivers can be captured by discrete channel states), it cannot capture scenarios in which the receivers' channel quality varies continuously. For such a case, it is more reasonable to require the message to be secured from receivers with a certain degree of worse channel quality, instead of being secured from the receiver with one level worse channel quality, which is not even well defined for continuous channel quality. To be more explicit, we use an example to illustrate the motivation for such a model. Consider a degraded broadcast channel with infinitely many receivers, in which h denotes the amplitude of the channel gain (the larger the h, the better the channel). In this case, it is impossible to require that the message intended for receivers with $h\ge h_0$ be secured from receivers with $h<h_0$, because no positive secrecy rate can be achieved. Instead, it is more natural to require that the messages intended for receivers with $h\ge h_0$ be secured from receivers with $h\le h_0-\Delta$, where $\Delta>0$. We refer to such a secrecy requirement as *secrecy outside a bounded range*.

In this subsection, we focus on a special case of the above model recently studied in [38], which is a four-receiver degraded broadcast channel model with secrecy outside of a bounded range (see Fig. 10). In this model, a transmitter sends information to four receivers over a broadcast channel. It is assumed that the channel quality gradually degrades from receiver 4 to receiver 1. The transmitter has four messages W_1, W_2, W_3 and W_4 intended for the four receivers with the following decoding and secrecy requirements. For $k=1,2,3,4$, receiver k is required to decode the messages $W_1,\ldots,W_k$. Furthermore, the message W_3 needs to be kept secure from receiver 1, and the message W_4 needs to be kept secure from receivers 1 and 2. It is clear that each message is secured from a receiver with two-level worse channel quality.

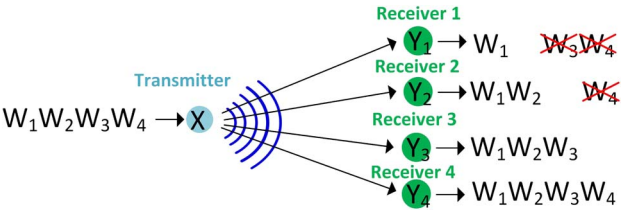


Fig. 10. *Four-receiver degraded broadcast channel with secrecy outside a bounded range.*

More technically, the channel is characterized by the probability transition function $P_{Y_1Y_2Y_3Y_4|X}$, in which $X\in\mathcal{X}$ denotes the channel input, and $Y_k\in\mathcal{Y}_k$ denotes the channel output at receiver k, for $k=1,2,3,4$. The channel is assumed to satisfy the degradedness condition, i.e., the following Markov chain condition holds:

$$X\to Y_4\to Y_3\to Y_2\to Y_1. \qquad (15)$$

The design of an achievable scheme relies on superposition, embedded coding and binning, and rate splitting and sharing. Similarly to previous models, due to the requirement of layered decoding, the messages are encoded using *superposition* coding with each layer corresponding to one message, i.e., layer k corresponds to W_k for $k=1,2,3,4$. Due to secrecy constraints, *joint embedded coding and binning* are applied. Since the messages do not need to be kept secure from their immediate downstream receivers, such a receiver's message can serve as a random source for securing the higher layer message in addition to stochastic binning. In fact, if such a random source is sufficient for securing the message, binning is not necessary. More specifically, W_3 serves as a random source to secure W_4 from receiver 2 jointly with random binning designed at layer 4 (if necessary). Similarly, W_2 at layer 2 serves as a random source to secure W_3 and W_4 from receiver 1 jointly with binning at layers 3 and 4 (if necessary). Furthermore, *rate splitting and sharing* is used, i.e., W_3 is split into two parts, i.e., W_{31} and W_{32}. Such splitting

exploits the fact that W_{31} is sufficient to secure both W_{32} and W_4 from receiver 2 for some cases, and thus the rate of W_{32} can be counted towards the rate of either W_3 or W_4. In this way, the rate region may be enlarged.

We note that joint embedded coding and binning is necessary here to exploit the secrecy requirements only outside the bounded range (i.e., the secrecy is not imposed for the immediate downstream receiver). Thus, messages intended for receivers inside the bounded range can serve as random sources for secrecy purposes. Such a scheme cannot be used for the model with layered decoding and secrecy presented in Section II-C, where the secrecy is imposed for the immediate downstream receiver. We further note that the embedded coding here uses messages across superposition layers as random sources for secrecy, which is different from the original embedded coding [25] as described in Sections I and II-B where the messages serving as random sources are at the same layers as the messages being protected. In other words, the embedded coding technique is realized by the superposition coding in this achievable scheme. But the embedded coding does not have to be realized by superposition coding only, it can also be realized by the random binning with one more message encoded as the bin number.

Based on the scheme described above, an achievable region can be derived, which can be further shown to be tight via a converse argument. The following theorem characterizes the obtained secrecy capacity region.

Theorem 5 [38]: Consider the four-receiver degraded broadcast channel with secrecy outside a bounded range as described above. The secrecy capacity region consists of all rate tuples (R_1, R_2, R_3, R_4) satisfying

$$\begin{aligned}
R_1 &\le I(U_1; Y_1) \\
R_2 &\le I(U_2; Y_2|U_1) \\
R_3 &\le I(U_3; Y_3|U_2) + \min(0, I(U_2; Y_2|U_1) - I(U_3; Y_1|U_1)) \\
R_4 &\le I(X; Y_4|U_3) + I(U_3; Y_3|U_2) - I(X; Y_2|U_2) \\
R_3 + R_4 &\le I(U_3; Y_3|U_2) + I(X; Y_4|U_3) \\
&\quad + \min(0, I(U_2; Y_2|U_1) - I(X; Y_1|U_1)) \qquad (16)
\end{aligned}$$

for some $P_{U_1U_2U_3X}$ such that the following Markov chain condition holds:

$$U_1 \to U_2 \to U_3 \to X. \qquad (17)$$

In fact, using only superposition and joint embedded coding and binning is shown to be optimal (i.e., to achieve the secrecy capacity region) for the three-receiver model in [39]. However, for the four-receiver model, such an achievable scheme is not sufficient. The major novelty of the above scheme lies in developing rating splitting and sharing, which helps to potentially enlarge the achievable region (at least to enlarge the region for a given distribution of auxiliary random variables). Consequently, the proof of the converse can be developed for such an achievable region, and thus the secrecy capacity region is established.

More specifically, without rate splitting and sharing, superposition and joint embedded coding and binning yields an achievable region with rates satisfying

$$\begin{aligned}
R_1 &\le I(U_1; Y_1) \\
R_2 &\le I(U_2; Y_2; U_1) \\
R_3 &\le I(U_3; Y_3|U_2) + \min(0, I(U_2; Y_2|U_1) - I(U_3; Y_1|U_1)) \\
R_4 &\le I(X; Y_4|U_3) + \min(0, I(U_3; Y_3|U_2) - I(X; Y_2|U_2)) \\
R_3 + R_4 &\le I(U_3; Y_3|U_2) + I(X; Y_4|U_3) + I(U_2; Y_2|U_1) \\
&\quad - I(X; Y_1|U_1). \qquad (18)
\end{aligned}$$

It is very difficult to develop the converse proof for the bound $R_4 \le I(X; Y_4|U_3)$ in the above region. However, by using rate splitting and sharing, this bound is replaced by the bound $R_3 + R_4 \le I(U_3; Y_3|U_2) + I(X; Y_4|U_3)$, and the resulting region (16) is larger than the above region (18) (for a given distribution of auxiliary random variables). Furthermore, the converse proof for the new bound on $R_3 + R_4$ in (16) can be derived, and thus establishes the region (16) as the secrecy capacity region.

III. APPLICATIONS OF INFORMATION-THEORETIC MODELS

In this section, we provide two example applications of the broadcast models that we present in Section II. These applications demonstrate that these information-theoretic models and approaches can be very powerful in providing solutions and guidelines to address security issues in wireless networks.

A. Fading Wiretap Channel

In this section, we introduce the application of the results presented in Sections II-A and II-B, respectively, for the broadcast channel with layered decoding and with layered secrecy to studying the following problem arising in the fading wiretap channel.

As physical-layer security exploits physical channel statistics to achieve secure communication, successful implementation of this approach depends crucially on the transmitter's knowledge about the channel state information (CSI), which, however, may not often be

available due to limited feedback resources. Furthermore, eavesdroppers typically do not have incentive to send their channel states to transmitters. Thus, it is desirable to design communication schemes that do not exploit channel state realizations at the transmitter but still adapt to the actual channel state that occurs in order to achieve as good a secrecy performance as possible. Thus, the legitimate receiver decodes more information as its channel gets better, and out of information decoded at the legitimate receiver, more information is kept secure from the eavesdropper as the eavesdropper's channel gets worse. In [36], a (layered) broadcast approach was proposed to achieve such a goal, which we present as follows.

Suppose a transmitter sends a message to one legitimate receiver and one eavesdropper. The channel input-output relationship for one channel use is given by

$$Y = HX + W \quad \text{and} \quad Z = GX + V \tag{19}$$

where X is the input from the transmitter, Y and Z are outputs at the legitimate receiver and the eavesdropper, respectively, H and G are fading gain coefficients, and the noise variables W and V are proper complex Gaussian random variables with zero means and unit variances. The fading gain H and G are assumed to experience block fading, i.e, they are constant within a coding block and change ergodically across blocks. The block length is assumed to be sufficiently large such that one codeword can be successfully transmitted if properly constructed. The channel input is subject to an average power constraint P over each block. The noise variables are assumed to be independent from channel use to channel use within each block. It is assumed that the transmitter does not know the instantaneous CSI, and each receiver knows its own channel state. The goal is to achieve a secrecy rate as high as the legitimate receiver's channel supports, and as the eavesdropper's channel permits, even though the transmitter does not know the CSI.

In [36], three scenarios were studied, i.e., only the legitimate receiver's channel is fading, only the eavesdropper's channel is fading, and both channels are fading. Next, we introduce the results of the first two scenarios, which apply the results in Section II-A and B, respectively. The study of scenario 3 integrates the analysis of the first two scenarios.

In the first scenario, in which only the legitimate receiver's channel is fading and the eavesdropper's channel is constant, suppose there are L fading states, i.e., $|H_1| \leq |H_2| \leq \cdots \leq |H_L|$. In order for the transmitter to adapt its transmission to legitimate receiver's channel without knowing the CSI, a broadcast approach (now known also as variable to fixed coding [59]) was developed in [36], which generalized the broadcast approach in [40] to the fading wiretap channel. More specifically, the entire message is split into L layers so that the legitimate receiver decodes the first l messages if its channel realization is H_l for $l = 1, \ldots, L$ and the eavesdropper is kept ignorant of all messages. Under such an achievable scheme, the channel is the same as the model described in Section II-A, and hence Theorem 1 can be applied to obtain the following result.

Theorem 6 [36, Th. 1]: For the fading wiretap channel with the legitimate receiver having one of the L fading states $H_1, \ldots, H_L$, and with the eavesdropper having a fixed channel state G, where $|G| < |H_1| \leq |H_2| \leq \cdots \leq |H_L|$, the following secrecy rate tuples $(R_1, \ldots, R_L)$ are achievable:

$$R_l = \log\left(1 + \frac{|H_l|^2 P_l}{1 + |H_l|^2 \sum_{k=l+1}^{L} P_k}\right) - \log\left(1 + \frac{|G|^2 P_l}{1 + |G|^2 \sum_{k=l+1}^{L} P_k}\right), \qquad l = 1, \ldots, L \tag{20}$$

where P_l denotes the transmission power assigned for transmitting W_l and satisfies the power constraint $\sum_{l=1}^{L} P_l \leq P$.

The above result was then generalized to the case with continuous fading state to further characterize the average secrecy rate over a large number of blocks in [36].

In the second scenario, in which only the eavesdropper's channel is fading and the legitimate receiver's channel is constant, suppose there are L fading states for the eavesdropper with $|G_1| \leq |G_2| \leq \cdots \leq |G_L|$. In order for the transmitter to adapt its transmission to the eavesdropper's channel without knowing the CSI, an embedded coding technique developed in [34] was employed in [36]. In contrast to the first scenario, in which messages are encoded into layers, here all messages are encoded into one codeword in an embedded fashion. Each message corresponds to one index that identifies the codeword. In particular, lower indexed layers of messages serve as randomization for protecting higher indexed messages from the eavesdropper. Depending on the eavesdropper's channel state, all messages up to a certain index are kept secure from the eavesdropper. All messages are required to be decoded by the legitimate receiver. Under such an achievable scheme, the channel model is the same as the model described in Section II-B, and hence Theorem 2 can be applied to obtain the following result.

Theorem 7 [36, Th. 3]: Consider the fading wiretap channel with the legitimate receiver having a fixed channel state H and the eavesdropper having one of L fading states

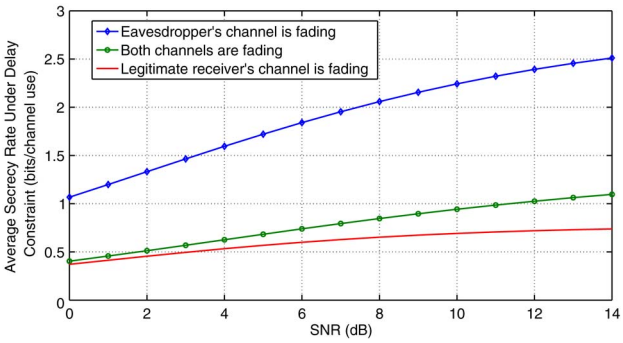


Fig. 11. ***Comparison of rates for the three scenarios.***

$G_1, \ldots, G_L$ with $|G_1|^2 < |G_2|^2 < \cdots < |G_L|^2 < |H|^2$. The following secrecy rate tuples $(R_1, \ldots, R_L)$ are achievable:

$$R_l = \log\left(1 + |G_{l+1}|^2 P\right) - \log\left(1 + |G_l|^2 P\right) \quad \text{for } l = 1, \ldots, L-1$$
$$R_L = \log\left(1 + |H|^2 P\right) - \log\left(1 + |G_L|^2 P\right). \qquad (21)$$

The above result was then generalized to the case with continuous fading state to further characterize the average secrecy rate over a large number of blocks in [36].

For the third scenario, in which the channels to both the legitimate receiver and the eavesdropper undergo fading, an integration of the above two approaches was developed in [36]. We refer the reader to [36] for further details.

We next present an interesting numerical result that compares the average secrecy rates for the three scenarios in Fig. 11. It is clear from the figure that scenario 2 (with only the eavesdropper channel fading) has the best rate, and scenario 3 (with both channels fading) has a better rate than scenario 1 (with only the legitimate channel fading). It is easy to understand that scenario 3 has a worse rate than scenario 2 because the transmitter's power is spread over the states due to no knowledge of the legitimate receiver's CSI. However, it may seem counterintuitive that scenario 3 has a better rate than scenario 1. This is due to the fact that when the eavesdropper's channel is fading, there is a good chance that its state is below the channel average, and such channel fluctuation facilitates achievement of a better secrecy rate and overcomes the effect of no eavesdropper CSI at the transmitter. Therefore, the two major factors that affect the secrecy rate are the knowledge of the legitimate receiver's CSI and the channel fluctuation of the eavesdropper. The knowledge of the eavesdropper's CSI only weakly affects the secrecy rate.

B. Multisecret Sharing Problem

In this section, we introduce the application of the result presented in Section II-C for the MIMO channel to studying the following problem of sharing multiple secrets. Suppose that a dealer wishes to share K secrets $W_1, W_2, \ldots, W_K$ with K participants. It is required that participant 1 decodes W_1, and participants 1 and 2 decode W_1 and W_2 by sharing their information from the dealer, but W_2 should be kept secure from participant 1. Such requirements extend to k participants for $k = 1, \ldots, K$ in the sense that participants 1 to k can recover the first k messages $W_1, \ldots, W_k$ by sharing their information from the dealer, but the new message W_k should be kept secure from the first $k-1$ participants. Hence, as one more participant joins the group, one more secret can be recovered, and this new secret is kept secure from (and hence cannot be recovered by) a smaller group. The goal is to characterize the best tradeoff among the rates of shared messages, i.e., the secret sharing capacity region that contains all possible achievable rate tuples $(R_1, R_2, \ldots, R_K)$ for K secrets.

The above secret sharing problem involves sharing multiple secrets in a layered fashion, and is challenging to solve using the classical approach based on algebraic tools [41]–[44]. Furthermore, existing solutions based on algebraic tools implicitly assume that information delivery from the dealer to the participants is noise free. Such an approach works well for traditional wired networks in which the dealer can distribute each share over dedicated line to each participant. Wireless networks, however, are different from wired networks in that the transmission is noisy and is broadcast in nature. One can address the noise issue by using error correction coding. However, to securely deliver each share to each participant, the dealer has to use secret keys, shared with the intended participant, to encrypt and decrypt each share. Otherwise, even if the secret sharing scheme itself is information-theoretically secure, the system is not secure anymore.

A different approach for secret sharing over wireless networks was proposed in [37]. Instead of converting noisy channels into noiseless bit pipes, the presence of noise inherent in wireless channels is exploited for designing secret sharing schemes. Suppose that a dealer communicates to K participants via a broadcast channel (see Fig. 12). We denote the channel input sent by the dealer by $\mathbf{X}$, and the channel output received at participant k by Y_k for $k = 1, \ldots, K$. Thus, the information that each group of participants share is the outputs that participants in the group receive. The idea in [37] is to construct an equivalent broadcast wiretap model. In particular, suppose that the dealer communicates to the participants via a Gaussian broadcast channel corrupted by additive Gaussian noise variables, in which the dealer has K antennas and each receiver has one antenna. Now for each group of participants 1 to k, for $k = 1, \ldots, K$, design a virtual receiver V_k, such that the channel output

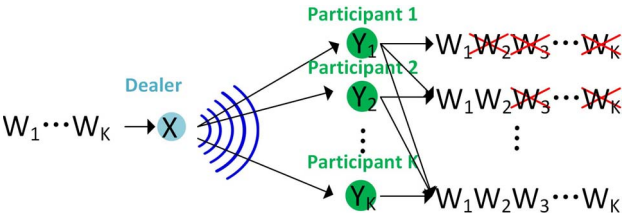


Fig. 12. *Model for secret sharing via a broadcast channel.*

at the virtual receiver k is $(Y_1, \ldots, Y_k)$ representing that receivers $1, \ldots, k$ group their outputs. The decoding and secrecy requirements for the reformulated channel is as follows: virtual receiver k can recover the first k messages $W_1, \ldots, W_k$, and should be kept ignorant of messages $W_{k+1}, \ldots, W_K$. Thus, the secret sharing problem can be reformulated into a communication problem over the degraded Gaussian MIMO broadcast channel with layered decoding and layered secrecy as described in Section II-C. In particular, $\mathbf{\Sigma}'_V(k)$ denotes the covariance matrix of the noise vector at the virtual receiver k, t is a parameter introduced to make the channel output at each virtual receiver having the same dimension, and if $t \to \infty$, the virtual model will reduce to the original model. We refer the readers to [37] for more details. Therefore, the secret sharing capacity region presented below follows from Theorem 4.

Corollary 1 [37, Corollary 1]: The capacity region for the secret sharing problem described above contains all rate tuples $(R_1, R_2, \ldots, R_K)$ satisfying

$$
\begin{aligned}
R_1 &\le \frac{1}{2}\log\frac{\left|\mathbf{\Sigma}'_V(1)+\mathbf{S}\right|}{\left|\mathbf{\Sigma}'_V(1)+\mathbf{S}_1\right|} \\
R_k &\le \lim_{t\to\infty}\frac{1}{2}\log\frac{\left|\mathbf{\Sigma}'_V(k)+\mathbf{S}_{k-1}\right|}{\left|\mathbf{\Sigma}'_V(k)+\mathbf{S}_k\right|}-\frac{1}{2}\log\frac{\left|\mathbf{\Sigma}'_V(k-1)+\mathbf{S}_{k-1}\right|}{\left|\mathbf{\Sigma}'_V(k-1)+\mathbf{S}_k\right|} \\
&\qquad \text{for } 2 \le k \le K-1 \\
R_K &\le \lim_{t\to\infty}\frac{1}{2}\log\frac{\left|\mathbf{\Sigma}'_V(K)+\mathbf{S}_{K-1}\right|}{\left|\mathbf{\Sigma}'_V(K)\right|}-\frac{1}{2}\log\frac{\left|\mathbf{\Sigma}'_V(K-1)+\mathbf{S}_{K-1}\right|}{\left|\mathbf{\Sigma}'_V(K-1)\right|}
\end{aligned}
\tag{22}
$$

for some $\mathbf{0} \preceq \mathbf{S}_{K-1} \preceq \mathbf{S}_{K-2} \preceq \cdots \preceq \mathbf{S}_2 \preceq \mathbf{S}_1 \preceq \mathbf{S}$, where $\mathbf{S}$ is the covariance constraint of the dealer's input and $\mathbf{S}$ should satisfy the power constraint, $trace(\mathbf{S}) \le P$.

We note that the secret sharing problem we describe is only an example problem. The information-theoretic approach proposed in [37] is applicable to more general multisecret sharing problems. The central idea is to reformulate secret sharing problems into secure communication problems with secrecy constraints (i.e., compound wiretap models in general), and then information-theoretic approaches developed for wiretap models can be applied to solving these secret sharing problems.

We further note a technical issue that the secrecy requirement here (and throughout the article) refers to weak secrecy (i.e., per block secrecy). However, the result given in Corollary 1 can be strengthened to satisfy strong secrecy requirements (i.e., per symbol secrecy) without loss of performance by applying the ideas in [45].

IV. DISCUSSION AND CONCLUSION

In this article, we have provided a review of recent studies of a class of broadcast channels with layered decoding and/or layered secrecy. We also have reviewed the applications of such models to the secure communication problem over the fading wiretap channel and the secret sharing problem.

Under the class of broadcast models, there are many open problems that require further exploration. For example, the model with secrecy outside a bounded range was fully explored only for the four-receiver case. Extension of existing results to the case with an arbitrary number of receivers is interesting. It is anticipated that rate splitting and sharing is more involved because one layer message can be split into multiple components in order to be shared by rates corresponding to higher layers. The procedure of Fourier–Motzkin elimination to obtain the resulting achievable region will also become more complex. This suggests that new techniques need to be developed to simplify the mathematical manipulations, as well as capturing the essence of the problem. Extension of such a model can also be applied to study more practical fading wiretap channels with continuous channel states, in which messages decoded at a certain receiver are required to be kept secure from receivers that are outside a bounded range (i.e., with a certain degree of worse channel quality). As another example, it is of interest to study the models with arbitrary numbers of receivers in this class in the context of compound scenarios, in which each receiver and/or eavesdropper can represent a group of nodes in the same fashion as in [13] and [27]. Such scenarios are more flexible for modeling practical networks with clusters of receivers.

The two applications that we have reviewed in this article demonstrate that information-theoretic approaches for security can be advantageous and powerful in various practical scenarios, and can hence serve as useful complements to cryptographic approaches. As we have commented in Section I-A, information-theoretic secrecy provides an additional benefit without sacrificing communication rates. Thus, such an information-theoretic approach at least provides additional security protection even for a system that has been protected via cryptographic approaches. Furthermore, in some wireless systems such as *ad hoc* networks, it is typically challenging to deploy preshared secret keys among the nodes. This key distribution dilemma can be solved by information-theoretic approaches by exploiting randomness resources in physical

layer channels. As we have introduced in this article, broadcast communication channels can be utilized to flexibly distribute keys to satisfy various layered secrecy requirements if we treat messages in broadcast models as secret keys. Hence, we anticipate that information-theoretic security approaches and cryptographic approaches will complement each other in future wireless systems to provide the strongest protection.

This article has focused on studies that characterize information-theoretic performance limits, and hence our review has described only capacity achieving secrecy schemes based on random coding arguments. In recent years, there have been intensive studies on designing practical codes for achieving secrecy capacity for various channel models. In particular, low density parity check (LDPC) codes and polar codes have been designed for achieving secure communications for various wiretap systems; for example, LDPC codes for the basic wiretap channel in [46]–[48], and polar codes for the basic wiretap channel in [49]–[55], for the relay wiretap channel in [49] and [56], and for the broadcast channel with confidential messages in [57] and [58]. Practical code designs for the broadcast models reviewed in this article are much less well understood and require further exploration. ■

REFERENCES

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

[2] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

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

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

[5] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information-theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5. Hanover, MA, USA: Now Publishers, 2008, pp. 355–580.

[6] S. 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.

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

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

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

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

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

[12] 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.

[13] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," *EURASIP J. Wireless Commun. Netw.*, Special Issue on Wireless Physical Layer Security, 2009.

[14] I. Bjelakovic, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channels," *Probl. Inf. Transm.*, vol. 49, no. 1, pp. 73–98, 2013.

[15] A. Khisti, "On the MISO compound wiretap channel," in *Proc. Inf. Theory Appl. Workshop*, Jan. 2010, pp. 1–7.

[16] 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.

[17] R. F. Schaefer and A. Khisti, "Secure broadcasting of a common message with independent secret keys," in *Proc. 48th Annu. Conf. Inf. Sci. Syst.*, Mar. 2014, pp. 1–6.

[18] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, Special Issue on Information Theoretic Security, no. 6, pp. 2470–2492, Jun. 2008.

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

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

[21] R. F. Schaefer and H. Boche, "Robust broadcasting of common and confidential messages over compound channels: Strong secrecy and decoding performance," *IEEE Trans. Inf. Forensic Security*, vol. 9, no. 10, pp. 1720–1732, Oct. 2014.

[22] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secrecy rate region of the broadcast channel with an eavesdropper," 2009. [Online]. Available: http://arxiv.org/abs/0910.3658

[23] M. Benammar and P. Piantanida, "On the secrecy capacity region of the wiretap broadcast channel," in *Proc. IEEE Inf. Theory Workshop*, Nov. 2014, pp. 421–425.

[24] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secrecy capacity region of Gaussian broadcast channel," in *Proc. 43rd Annu. Conf. Inf. Sci. Syst.*, Mar. 2009, pp. 152–157.

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

[26] R. Tandon, P. Piantanida, and S. Shamai, "On multi-user MISO wiretap channels with delayed CSIT," *Proc. IEEE Int. Symp. Inf. Theory*, pp. 211–215, Jun. 2014.

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

[28] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 1:1–1:29, Mar. 2009.

[29] R. Liu, I. Maric, P. Spasojević, 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.

[30] 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.

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

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

[33] M. Kobayashi, Y. Liang, S. Shamai, and M. Debbah, "On the compound MIMO broadcast channels with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 1283–1287.

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

[35] J. L. Massey, "A simplified treatment of Wyner's wire-tap channel," in *Proc. Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, Oct. 1983.

[36] Y. Liang, L. Lai, H. V. Poor, and S. Shamai (Shitz), "A broadcast approach for fading wiretap channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 842–858, Feb. 2014.

[37] S. Zou, Y. Liang, L. Lai, and S. Shamai (Shitz), "An information-theoretic approach to secrecy sharing," *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3121–3136, Jun. 2015.

[38] S. Zou, Y. Liang, L. Lai, and S. Shamai, "Rate splitting and sharing for degraded

broadcast channel with secrecy outside a bounded range," in *Proc. IEEE Int. Symp. Information Theory*, Jun. 2015.

[39] S. Zou, Y. Liang, L. Lai, and S. Shamai (Shitz), "Degraded broadcast channel: Secrecy outside of a bounded range," in *Proc. IEEE Inf. Theory Workshop*, 2015.

[40] S. Shamai (Shitz) and A. Steiner, "A broadcast approach for a single-user slowly fading MIMO channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2617–2635, Oct. 2003.

[41] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[42] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS 1979 Nat. Comput. Conf.*, 1979, IEEE Computer Society.

[43] A. Parakh and S. Kak, "Space efficient secret sharing for implicit data security," *Inf. Sci.*, vol. 181, no. 2, pp. 335–341, 2011.

[44] A. Beimel, "Secret-sharing schemes: A survey," in *Coding and Cryptology*. New York, NY, USA: Springer, 2011, pp. 11–46.

[45] U. M. Maurer and S. Wolf, "From weak to strong information-theoretic key agreement," in *Proc. IEEE Int. Symp. Inf. Theory*, Sorrento, Italy, Jun. 2000, p. 18.

[46] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge-type LDPC codes for the BEC wiretap channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1048–1064, 2013.

[47] R. Liu, Y. Liang, H. V. Poor, and P. Spasojević, "Secure nested codes for type-II wire-tap channels," in *Proc. IEEE Inf. Theory Workshop*, 2007, pp. 337–342.

[48] A. Subramanian, A. Thangaraj, and M. Bloch, "Strong secrecy on the binary erasure wiretap channel using large girth LDPC codes," *IEEE Trans. Inf. Forensic Security*, vol. 6, no. 3, pp. 585–594, Sep. 2011.

[49] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Lett.*, vol. 14, no. 8, pp. 752–754, 2010.

[50] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans. Inf. Forensic Security*, vol. 7, no. 5, pp. 1472–1483, Oct. 2012.

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

[52] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *Proc. IEEE Inf. Theory Workshop*, Aug. 2010.

[53] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of polar codes for the deterministic wiretap channel," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Nov. 2013, pp. 2089–2093.

[54] Y. Wei and S. Ulukus, "Polar coding for the general wiretap channel," in *Proc. IEEE Inf. Theory Workshop*, Apr. 2015.

[55] E. Sasoglu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Proc. IEEE Int. Symp. Inf. Theory*, 2013.

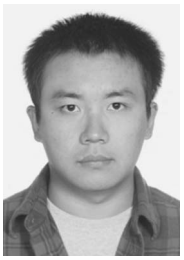
[56] B. Duo, P. Wang, Y. Li, and B. Vucetic, "Secure transmission for relay-eavesdropper channels using polar coding," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2014, pp. 2197–2202.

[57] M. Andersson, R. F. Schaefer, T. J. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1901–1908, 2013.

[58] R. A. Chou and M. Bloch, "Polar coding for the broadcast channel with confidential messages and constrained randomization," *arXiv preprint*, 2014.

[59] S. Verdu and S. Shamai, "Variable-Rate Channel Capacity," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2651–2667, Jun. 2010.

ABOUT THE AUTHORS



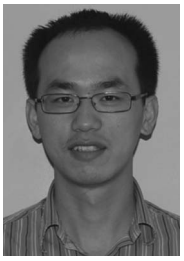
Shaofeng Zou (Student Member, IEEE) received the B.E. degree (with honors) from Shanghai Jiao Tong University, Shanghai, China in 2011. Since September 2011, he has been a Ph.D. student at Syracuse University, Syracuse, NY, USA.

His research interests are on information theory, nonparametric detection, and machine learning. He received the Excellent Student Scholarship from Shanghai Jiaotong University in 2008, 2009 and 2010, and received the National Scholarship from the Ministry of Education of China in 2008. He also received the National Encouragement Scholarship from the Ministry of Education of China in 2009 and 2010.

Yingbin Liang (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Illinois at Urbana-Champaign, Urbana, IL, USA, in 2005.

From 2005 to 2007, she was working as a postdoctoral research associate at Princeton University, Princeton, NJ, USA, and from 2008 to 2009, she was an assistant professor at the Department of Electrical Engineering at the University of Hawaii at Manoa, Honolulu, HI, USA. Since December 2009, she has been on the faculty at Syracuse University, Syracuse, NY, USA, where she is an associate professor. Her research interests include information theory, wireless communications and networks, and machine learning.

Dr. Liang was a Vodafone Fellow at the University of Illinois at Urbana-Champaign during 2003-2005, and received the Vodafone-U.S. Foundation Fellows Initiative Research Merit Award in 2005. She also received the M. E. Van Valkenburg Graduate Research Award from the ECE Department, University of Illinois at Urbana-Champaign, in 2005. In 2009, she received the National Science Foundation CAREER Award, and the State of Hawaii Governor Innovation Award. More recently, her paper received the 2014 EURASIP Best Paper Award for the *EURASIP Journal on Wireless Communications and Networking*. She is currently serving as an Associate Editor for the Shannon Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY.



Lifeng Lai (Member, IEEE) received the B.E. and M.E. degrees from Zhejiang University, Hangzhou, China, in 2001 and 2004, respectively, and the Ph.D. degree from The Ohio State University at Columbus, OH, USA, in 2007.

He was a postdoctoral research associate at Princeton University from 2007 to 2009, and was an assistant professor at the University of Arkansas, Little Rock, AR, USA, from 2009 to 2012. Since August 2012, he has been an assistant professor at Worcester Polytechnic Institute. His research interests include information theory, stochastic signal processing and their applications in wireless communications, security and other related areas.

Dr. Lai was a Distinguished University Fellow of the Ohio State University from 2004 to 2007. He is a corecipient of the Best Paper Award from IEEE Global Communications Conference (Globecom) in 2008, the Best Paper Award from IEEE Conference on Communications (ICC) in 2011, and the Best Paper Award from IEEE Smart Grid Communications (SmartGridComm) in 2012. He received the National Science Foundation CAREER Award in 2011, and Northrop Young Researcher Award in 2012. He served as a Guest Editor for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Special Issue on Signal Processing Techniques for Wireless Physical Layer Security. He is currently serving as an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and an Associate Editor for IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.

H. Vincent Poor (Fellow, IEEE) received the Ph.D. degree in electrical engineering and computer science from Princeton University, Princeton, NJ, USA, in 1977.

From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990, he has been on the faculty at Princeton University, where he is the Dean of Engineering and Applied Science, and the Michael Henry Strater University Professor of Electrical Engineering. He has also held visiting appointments at several other institutions, most recently at Imperial College, London, U.K., and Stanford University, CA, USA. His research interests are in the areas of information theory, stochastic analysis and statistical signal processing, and their applications in wireless networks and related fields. Among his publications in these areas is the recent book *Mechanisms and Games for Dynamic Spectrum Allocation* (Cambridge, U.K., Cambridge University Press, 2014).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a foreign member of Academia Europaea and the Royal Society. He is also a fellow of the American Academy of Arts and Sciences, the Royal Academy of Engineering (U.K.), and the Royal Society of Edinburgh. In 1990, he served as President of the IEEE Information Theory Society, and from 2004–2007, as the Editor-in-Chief of the IEEE Transactions on Information Theory. He received a Guggenheim Fellowship in 2002 and the IEEE Education Medal in 2005. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, and honorary doctorates from Aalborg University, Aalto University, HKUST, and the University of Edinburgh.

Shlomo Shamai (Shitz) (Fellow, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Technion—Israel Institute of Technology, Haifa, Israel, in 1975, 1981, and 1986 respectively.

During 1975–1985, he was with the Communications Research Labs, in the capacity of a Senior Research Engineer. Since 1986, he has been with the Department of Electrical Engineering, Technion—Israel Institute of Technology, where he is now a Technion Distinguished Professor, and holds the William Fondiller Chair of Telecommunications. His research interests encompasses a wide spectrum of topics in information theory and statistical communications.

Dr. Shamai (Shitz) is a member of the Israeli Academy of Sciences and Humanities and a foreign member of the U.S. National Academy of Engineering. He is the recipient of the 2011 Claude E. Shannon Award and the 2014 Rothschild Prize in Mathematics/Computer Sciences and Engineering. He has been awarded the 1999 van der Pol Gold Medal of the Union Radio Scientifique Internationale (URSI), and is a corecipient of the 2000 IEEE Donald G. Fink Prize Paper Award, the 2003, and the 2004 joint IT/COM societies paper award, the 2007 IEEE Information Theory Society Paper Award, the 2009 European Commission FP7, Network of Excellence in Wireless COMmunications (NEWCOM++) Best Paper Award, the 2010 Thomson Reuters Award for International Excellence in Scientific Research, the 2014 EURASIP Best Paper Award (for the *EURASIP Journal on Wireless Communications and Networking*), and the 2015 IEEE Communications Society Best Tutorial Paper Award. He is also the recipient of 1985 Alon Grant for distinguished young scientists and the 2000 Technion Henry Taub Prize for Excellence in Research. He has served as Associate Editor for the Shannon Theory of the IEEE Transactions on Information Theory, and has also served twice on the Board of Governors of the Information Theory Society. He has served on the Executive Editorial Board of the IEEE Transactions on Information Theory.