Gaussian Fading Channel with Secrecy Outside a Bounded Range

Shaofeng Zou
Coordinated Science Lab
University of Illinois at Urbana Champaign
Email: szou3@illinois.edu

Yingbin Liang
Department of EECS
Syracuse University
Email: yliang06@syr.edu

Shlomo Shamai (Shitz)
Department of EE
Technion-Israel Institute of Technology
Email: sshlomo@ee.technion.ac.il

***Abstract*—The Gaussian fading channel is studied, in which the channel from the transmitter to the receiver is corrupted by a multiplicative fading coefficient H and an additive Gaussian random noise. It is assumed that the channel is experiencing block fading, and the transmitter does not know the channel state information (CSI). The receiver is assumed to have full knowledge of the CSI. If the channel state is better, then more information is required to be decoded by the receiver, and if the channel state is worse, more information is required to be secure from the receiver. Furthermore, the information intended to be decoded by the receiver with a better state (e.g., $|H| \geq |h_0|$) is required to be secure from the receiver if it has a state worse than $|h_0|$ by Δ (i.e., $|H| \leq |h_0| - \Delta$), which is referred to as *secrecy outside a bounded range*. A (layered) broadcast approach is studied for this problem, which views the fading channel as a degraded broadcast channel with a number of receivers each experiencing a different fading coefficient. The achievable scheme designates one superposition layer to each message with binning employed to protect all upper-layer messages from lower-layer receivers. Furthermore, the scheme allows adjacent layers to share rates so that part of the rate of each message can be shared with its upper-layer messages to enlarge the rate region. The achievable secrecy rate region via the broadcast approach is characterized. The developed scheme can adapt the transmission rate to the actual unknown channel state without exploiting the CSI at the transmitter.**

I. Introduction

In wireless networks, signals are transmitted via the open medium of free space, and hence can be easily eavesdropped upon by any receiver within transmission range. The major challenge of secure wireless communication is due to this broadcast nature. To address this challenge, Wyner proposed a physical layer approach [1] which exploits physical channel randomness to achieve secure communication. This approach can significantly reduce requirements on the infrastructure and improve communication flexibility and dynamics without inherent use of secret keys. This approach was first introduced via the wiretap channel [1], in which a transmitter has one message intended for a legitimate receiver and would like to keep this message secure from an eavesdropper. This model was further generalized to a more general broadcast scenario by Csiszár and Köner [2], in which one more common message is required to be decoded by both the legitimate receiver and the eavesdropper. More recently, there has been a surge in interest in applying this approach to wireless networks (see [3]–[5] for overviews of recent works).

Successful implementation of the physical layer method depends crucially on the transmitter's knowledge of the channel state information (CSI) since it exploits the statistical channel randomness to achieve secure communication. Previous studies mostly focused on the scenarios in which the CSI is available to the transmitter with a few exceptions, e.g., [6]–[9]. However, in wireless networks, the CSI might not be available to the transmitter due to lack of feedback resources. More generally, for security reasons, the eavesdroppers do not intend to feed their channel state back to the transmitters.

A reasonable approach to model the channel state uncertainty is through compound wiretap channel [10]–[13], and arbitrary varying channel [14], [15]. These approaches guarantee secure communication under any possible channel states, in particular under the worst channel state. However, in order to guarantee secure communication under the worst channel state, the channel resources are not used efficiently if the actual channel state is good. Thus, it is appealing to design secure transmission schemes that do not exploit the CSI but can still adapt to the actual unknown channel state and achieve a secrecy rate as high as the actual channel state permits.

A broadcast approach was introduced in [16] for wireless communication with channel state uncertainty but without secrecy constraint, and was then generalized to the multiple-input multiple-output (MIMO) case in [17]. This approach facilitates to adapt the transmission rate to the actual unknown channel state without having any feedback link from the receiver to estimate the CSI. The basic idea is to view the fading channel as a degraded Gaussian broadcast channel with a continuum of receivers each experiencing a different fading coefficient. The transmitter then splits the entire message into a number of components with each component being transmitted via one layer of input. These layers of inputs are then combined into one channel input using superposition encoding. The receiver decodes the layers one after another via successive cancellation. The realization of the channel state determines up to which layer the receiver can decode. This broadcast approach was further employed to study the problem of fading wiretap channel in which both the legitimate and the eavesdropping channels are corrupted by multiplicative fading coefficients [18]. The average secrecy rate that can be achieved via the broadcast approach was derived.

In this paper, we consider a Gaussian fading channel, in which a transmitter sends information to a receiver. The channel is corrupted by an additive complex Gaussian noise

and random multiplicative fading gain coefficient. The status of the receiver is determined by its channel state. If the channel state is better, then more information is required to be decoded by the receiver. Meanwhile, if the channel state is worse, more information is required to be kept secure from the receiver. In this model, the receiver plays the role of both legitimate receiver and eavesdropper, and the amount of information it can decode and is kept secure depends on its channel state. Furthermore, the information intended to be decoded by the receiver if it has state h_0 should be kept secure from the receiver if it has state worse than h_0 by Δ, i.e. $|H| < |h_0| - \Delta$, for all $|h_0| \geq \Delta$, which is referred to as secrecy outside of a bounded range [19].

We generalize the broadcast approach in [16] and [17] to the model considered in this paper. We view the fading channel as a degraded broadcast channel with layered decoding and layered secrecy [20], [21] and with secrecy outside a bounded range [19]. We split the entire message into a number of layers with each component being transmitted via one layer of superposition coding. We further employ binning within each layer. These layers are then superposed one on another by superposition coding. Furthermore, the scheme allows adjacent layers to share rates so that part of the rate of each message can be shared with its upper-layer messages to enlarge the achievable region. This transmission strategy can adapt the rate to the actual unknown channel state, i.e., if the channel state is better, more layers of messages can be decoded, and less layers of messages are kept secure.

This paper is organized as follows. In Section II, we introduce the problem model of the fading channel with secrecy outside a bounded range. In Section III, we first present the results for the case with discrete channel states, and then generalize the results to the case with continuous channel states. In Section IV, we conclude the paper.

II. Problem Model

We consider a fading channel, in which a transmitter sends information to a receiver. The channel input-output relationship for one channel use is given by

$$Y = HX + U, \tag{1}$$

where Y is the channel output, X is the channel input, H is random fading gain coefficient, and U is complex Gaussian random noise with zero mean and unit variance.

The fading gain coefficient H is assumed to experience block fading, i.e., it is constant within a coding block and changes 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:

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}[|X_i|^2] \leq P, \tag{2}$$

where i denotes the symbol time (i.e., channel use) index, and n is the block length. The noise variable U is assumed to be independent and identically distributed (i.i.d.) per channel use within each block. The instantaneous CSI is assumed to be unknown to the transmitter, and known to the receiver. The transmitted message is required to be decoded within one block, i.e., satisfies the delay constraint, and coding across blocks is not allowed.

It is required that more information is decoded by the receiver if it has a better channel state, and more information is kept secure from the receiver if it has a worse channel state. It is further required that the secrecy is outside a bounded range [19]. More specifically, the information intended to be decoded by the receiver with channel state h_0 should be kept secure from the receiver with channel state worse than h_0 by Δ, i.e., $|H| < |h_0| - \Delta$, for all $|h_0| \geq \Delta$. Here Δ is the secrecy range.

More specifically, we consider two scenarios. In the first scenario, the receiver has a finite number of channel states, i.e., H can take on one of $H_1, \ldots, H_L$ values, where $|H_1| < \cdots < |H_L|$. It is assumed that the message intended to be decoded by the receiver with channel state H_k should be kept secure from the receiver with channel state worse than H_k by two levels of channel quality, i.e., $|H| \leq |H_{k-2}|$, and Δ is two levels of channel quality. This model is then generalized to the case in which Δ is arbitrary m levels of channel quality, where $m \geq 1$, i.e., the message intended to be decoded by the receiver with channel state H_k should be kept secure from the receiver with channel state worse than H_{k-m}.

In the second scenario, the fading coefficient H can take continuous values. The message at the transmitter is divided into infinite number of layers. It is required that the layers of the messages intended to be decoded by the receiver if it has a better state than h_0 is required to be secure from the receiver if it has a state worse than h_0 by Δ, i.e., $|H| < |h_0| - \Delta$.

A message W is said to be decoded at the receiver if the probability of decoding error is asymptotically small,

$$P_e^n(W) = P(\hat{W} \neq W) \leq n\epsilon_n, \tag{3}$$

where $\hat{W}$ is the decoded message at the receiver, and $\epsilon_n \to 0$ as $n \to \infty$, The measure of security is based on the equivocation rate of message W at the receiver,

$$\frac{1}{n}H(W|Y_k^n),$$

where Y_k^n is the channel output at the receiver with state H_k. The message W is said to be secure from the receiver with state H_k if

$$\frac{1}{n}H(W|Y_k^n) \geq \frac{1}{n}H(W) - \epsilon_n, \tag{4}$$

where $\epsilon_n \to 0$ as $n \to \infty$.

III. Main Results

In this section, we present our main results. We first consider the scenario in which the receiver has a finite number of channel states. We then generalize our results to the general case with continuous channel states.

A. Discrete Channel States

Before we introduce our results for the fading channel, we first review the results for the problem of degraded broadcast channel with secrecy outside a bounded range in [19].

In this problem, a L-receiver degraded broadcast channel is considered. A transmitter sends information to L receivers through a discrete memoryless channel. The channel is assumed to be degraded, i.e., the following Markov chain condition holds:

$$X \to Y_L \to Y_{L-1} \to \cdots \to Y_1. \tag{5}$$

Hence, the channel quality gradually degrades from receiver L to receiver 1. There are in total L messages $W_1, W_2, \ldots, W_L$ intended for L receivers with the following decoding and secrecy requirements. Receiver k is required to decode messages $W_1, W_2, \ldots, W_k$, for $k = 1, 2, \ldots, L$, and to be kept secure of $W_{k+2}, \ldots, W_L$, for $k = 1, \ldots, L-2$. For this problem, the secrecy capacity region is characterized as follows:

Proposition 1. *[19, Theorem 1] Consider the L-receiver degraded broadcast channel with secrecy outside a bounded range. The secrecy capacity region consists of rate tuples $(R_1, R_2, \ldots, R_L)$ satisfying*

$$R_1 \le I(U_1; Y_1), \tag{6a}$$

$$\sum_{j=2}^{k} R_j \le \sum_{j=2}^{k} I(U_j; Y_j|U_{j-1}), \quad \text{for } 2 \le k \le L, \tag{6b}$$

$$\sum_{j=l}^{k} R_j \le \left(\sum_{j=l-1}^{k} I(U_j; Y_j|U_{j-1}) \right) - I(U_k; Y_{l-2}|U_{l-2}), \quad \text{for } 3 \le l \le k \le L, \tag{6c}$$

for some $P_{U_1 \ldots U_K}$ satisfying the following Markov chain condition:

$$U_1 \to U_2 \to \cdots \to U_K \to Y_K \to \cdots \to Y_2 \to Y_1. \tag{7}$$

By the broadcast approach, our problem of fading channel can be viewed as degraded broadcast channel with L receivers, with each receiver k experiencing the fading coefficient H_k, for $1 \le k \le L$. The transmitter splits the entire message into L submessages, $W_1, \ldots, W_L$. By the decoding and secrecy requirements, message k should be decoded by receiver k, and should be kept secure from receiver $k-2$. Due to the degradedness condition, receiver k can decode messages $W_1, \ldots, W_k$ and is kept secure of message $W_{k+2}, \ldots, W_L$. For each message i, the transmitter assigns power P_i, such that $\sum_{i=1}^{L} P_i \le P$.

The rate tuple $(R_1, \ldots, R_L)$ is achievable if there exists a coding scheme that encodes $W_1, \ldots, W_L$ at the rate $(R_1, \ldots, R_L)$ such that for $k = 1, \ldots, L$, the receiver can decode W_k with small probability of error if its channel state is H_k, and $W_{k+2}, \ldots, W_L$ are kept secure from it.

Via the broadcast approach, this fading channel is reformulated into a degraded broadcast channel with layered decoding and layered secrecy and with secrecy outside a bounded range as in [19]. The following theorem characterizes the secrecy rate tuples that can be achieved.

Theorem 1. *For the fading channel with the receiver has L fading states $H_1, \ldots, H_L$, where $H_1 < \cdots < H_L$, the following secrecy rate tuples $(R_1, \ldots, R_L)$ are achievable:*

$$R_1 \le \log\left(1 + \frac{|H_1|^2 P_1}{|H_1|^2 \sum_{i=2}^{L} P_i + 1}\right), \tag{8a}$$

$$\sum_{j=2}^{k} R_j \le \sum_{j=2}^{k} \log\left(1 + \frac{|H_j|^2 P_j}{1 + |H_j|^2 \sum_{i=j+1}^{L} P_i}\right), \quad \text{for } 2 \le k \le L, \tag{8b}$$

$$\sum_{j=\ell}^{k} R_j \le \left[\sum_{j=\ell-1}^{k} \log\left(1 + \frac{|H_j|^2 P_j}{1 + |H_j|^2 \sum_{i=j+1}^{L} P_i}\right) \right] - \log\left(1 + \frac{|H_{\ell-2}|^2 \sum_{i=\ell-1}^{k} P_i}{1 + |H_{\ell-2}|^2 \sum_{i=k+1}^{L} P_i}\right), \quad \text{for } 3 \le \ell \le k \le L. \tag{8c}$$

In the above region, the bounds (8a) and (8b) are due to the decoding requirements, i.e., the receiver with state H_k should decode messages $W_1, \ldots, W_k$, for $1 \le k \le L$. The bounds (8c) are due to the secrecy requirements, i.e., messages $W_\ell, \ldots, W_k$ need to be kept secure from the receiver with state $H_{\ell-2}$ for $3 \le l \le k \le L$. Furthermore, the bounds (8c) can be written as

$$\begin{aligned} \sum_{j=\ell}^{k} R_j &\le \sum_{j=\ell-1}^{k} \left[\log\left(1 + \frac{|H_j|^2 P_j}{1 + |H_j|^2 \sum_{i=j+1}^{L} P_i}\right) - \log\left(1 + \frac{|H_{\ell-2}|^2 P_j}{1 + |H_{\ell-2}|^2 \sum_{i=j+1}^{L} P_i}\right) \right], \\ &\triangleq \sum_{j=\ell-1}^{k} A_j, \end{aligned} \tag{9}$$

which has a clear intuitive interpretation. The term A_j is corresponding to the rate of message W_j that can be secure from the receiver with state $H_{\ell-2}$ given the knowledge of $W_1, \ldots, W_{j-1}$. Those rates A_j for $\ell - 1 \le j \le k$ can all be counted towards $\sum_{j=\ell}^{k} R_j$ in accordance to the secrecy requirement of keeping $W_\ell, \ldots, W_k$ secure from the receiver with state $H_{\ell-2}$.

Due to the degradedness condition, the total rate satisfying the secrecy constraints that is achievable when the receiver is at channel state H_ℓ is $\sum_{j=1}^{\ell} R_j$. Then the average achievable secrecy rate is

$$\sum_{\ell=1}^{L} \left[P(H_\ell) \sum_{j=1}^{\ell} R_j \right].$$

This average secrecy rate can be further optimized with respect to the power allocation P_ℓ subject to a power constraint $\sum_{\ell=1}^{L} P_\ell \le P$.

A very important property of our designed scheme is that it is adaptive to the actual unknown channel state. More specifically, if the channel state is better, then more messages can be decoded, and less messages are kept secure from

the receiver. This adaptive property does not require the transmitter to know the instantaneous CSI.

The achievable scheme follows from the one in [19], which is based on superposition coding, binning and rate splitting and sharing. More specifically, for each message, one layer of codebook is designed, i.e., layer k corresponds to W_k, for $1 \leq k \leq L$. Within each layer, binning is employed, i.e., the codewords in each layer are divided into a number of bins, where the bin number contains the information of the corresponding message.

Furthermore, rate splitting and sharing is employed to enlarge the achievable region. More specifically, within the k-th layer, the message is split into two parts $W_{k,1}, W_{k,2}$. The message $W_{k,1}$ serves as embedded coding which is a random source in addition to the binning to protect $W_{k,2}$ and the higher layer messages from the receiver with state H_{k-1}, i.e., the messages $W_{k,2}, W_{k+1,1}, W_{k+1,2}, \ldots, W_{L,1}, W_{L,2}$ are secured from the receiver with state H_{k-1}. Furthermore, the receiver with state better than H_{k-1} can also decode $W_{k,2}$ because of the degradedness condition. Thus, the message $W_{k,2}$ satisfies both the decoding and secrecy requirements for message W_{k+1}, and hence the rate of $W_{k,2}$ can be counted towards the rate of either W_k or W_{k+1}. By such a rate sharing strategy, the achievable region is enlarged.

The motivation of adding the ingredient of the rate splitting and sharing is due to an important observation that although those layers within the bounded range Δ are not required to be kept secure, partial of their rate is kept secure, and hence can be shared with higher layer messages, which helps to enlarge the achievable rate region. We note that such a rate splitting and sharing strategy is critical to achieve the secrecy capacity region for the degraded broadcast channel with secrecy outside a bounded range in [19].

Based on such an achievable scheme, we obtain an achievable region in terms of $R_{k,1}$ and $R_{k,2}$, i.e., the rate of $W_{k,1}$ and $W_{k,2}$, for $1 \leq k \leq L$. Define $R_k = R_{k-1,2} + R_{k,1}$ for $3 \leq k \leq K-1$, $R_2 = R_{2,1}$ and $R_K = R_{K-1,2} + R_{K,1} + R_{K,2}$. A novel inductive Fourier-Motzkin elimination algorithm is designed which eliminates the rate pairs $R_{k-1,2}$ and $R_{k,1}$ for $3 \leq k \leq K$ one at each step [19]. The region $\mathcal{R}_k$ after eliminating $R_{k-1,2}$ and $R_{k,1}$ possesses a common structure. By doing this recursively, we obtain the region as shown in (8). More details can be found in [19].

To understand how well the broadcast approach performs, we compare its performance to an outer bound, which is derived by considering the case with no secrecy constraints, i.e., Δ is infinite levels of channel quality. It is equivalent to the fading channel without secrecy constraints as in [16], [17], in which the average capacity can serve as an outer bound for our problem with secrecy constraints. We also note that the designed scheme is a variable-to-fixed coding scheme as in [22].

We next present the result for the case in which Δ is arbitrary m levels of channel quality, where $m \geq 1$. The following secrecy rate region can be achieved using similar scheme as Theorem 1. We note that when $m = 1$, rate splitting and sharing is not needed anymore [20].

Theorem 2. *For the fading channel with receiver has L fading states $H_1, \ldots, H_L$, and secrecy outside m levels of channel quality, where $H_1 < \cdots < H_L$, the following secrecy ratre tuples are achievable:*

$$R_1 \leq \log\left(1 + \frac{|H_1|^2 P_1}{|H_1|^2 \sum_{i=2}^{L} P_i + 1}\right),$$

$$\sum_{j=2}^{k} R_j \leq \sum_{j=2}^{k} \log\left(1 + \frac{|H_j|^2 P_j}{1 + |H_j|^2 \sum_{i=j+1}^{L} P_i}\right), \quad \text{for } 2 \leq k \leq L, \tag{10}$$

$$\sum_{j=\ell}^{k} R_j \leq \left[\sum_{j=\ell-m+1}^{k} \log\left(1 + \frac{|H_j|^2 P_j}{1 + |H_j|^2 \sum_{i=j+1}^{L} P_i}\right)\right] - \log\left(1 + \frac{|H_{\ell-m}|^2 \sum_{i=\ell-m+1}^{k} P_i}{1 + |H_{\ell-m}|^2 \sum_{i=k+1}^{L} P_i}\right), \quad \text{for } m+1 \leq \ell \leq k \leq L. \tag{11}$$

B. Continuous Channel States

In this subsection, we consider the case with continuous channel states, i.e., H can take continuous values.

It is required that the messages intended to be decoded by the receiver if it has a better state than h_0 is required to be secure from the receiver if it has state worse than h_0 by Δ, i.e., $|H| < |h_0| - \Delta$, for all $|h_0| \geq \Delta$. For each channel state $H = h$, let $s = |h|^2$.

Motivated by the broadcast approach for the Gaussian fading channel without secrecy constraints as in [16], the message is divided into infinitely many layers of messages indexed by s. For each layer s of message, the transmitter allocates power $\rho(s)ds$, where $\rho(s)$, satisfying

$$\int_0^\infty \rho(s)ds \leq P,$$

is the power allocation function. Denote

$$\Sigma(s) = \int_s^\infty \rho(x)dx,$$

which is the power allocated to the layers of messages intended for receiver with channel state better than s. It is clear that $\rho(s) = -\Sigma'(s)$.

It is assumed that the message indexed by s is required to be decoded by the receiver with state $|h| = \sqrt{s}$ and be kept secure from the receiver with state worse than $\sqrt{s} - \Delta$. We use $R(s)ds$ to denote the incremental differential rate for layer indexed by s. By the broadcast approach, the fading channel with continuous channel states can be viewed as a degraded broadcast channel with infinitely many receivers with a continuum of channel states.

Similar to Theorem 2, we can obtain the following achievable region.

Theorem 3. *Consider the fading channel with continuous channel states, i.e., H can take continuous values. The incremental differential rate $R(s)ds$ satisfying the following*

constraints is achievable:

$$\int_0^t R(s)ds \le \int_0^t \frac{x\rho(x)dx}{1+x\Sigma(x)}, \text{ for } t \ge 0, \tag{12a}$$

$$\int_{t_1}^{t_2} R(s)ds \le \int_{(\sqrt{t_1}-\Delta)^2}^{t_2} \frac{x\rho(x)dx}{1+x\Sigma(x)} - \log\left(1+\frac{(\sqrt{t_1}-\Delta)^2\left(\Sigma((\sqrt{t_1}-\Delta)^2)-\Sigma(t_2)\right)}{1+(\sqrt{t_1}-\Delta)^2\Sigma(t_2)}\right), \text{ for } \Delta^2 \le t_1 \le t_2 \le \infty. \tag{12b}$$

To maximize the average secrecy rate, it suffices to solve the following optimization problem:

$$\max_{\rho(s)} \int_0^\infty p(s)ds\left(\int_0^s R(t)dt\right), \tag{13}$$

subject to the constraints in (12) and $\int_0^\infty \rho(x) \le P$, where $p(s)$ is the probability distribution function of s.

In order to understand how well the broadcast approach performs, we let $\Delta = \infty$. Then the fading channel with secrecy outside a bounded range is equivalent to the fading channel without any secrecy constraint. The average capacity in [22] and [17] can serve as an outer bound.

IV. Conclusion

In this paper, we studied the problem of secure communication over a fading channel with secrecy outside a bounded range, and with no instantaneous CSI at the transmitter. By the broadcast approach in [16], our problem can be viewed as a degraded broadcast channel with layered decoding and layered secrecy and with secrecy outside a bounded range. We designed transmission schemes that are adaptive to the actual channel state without employing the knowledge of the CSI. We note that our designed scheme can be viewed as variable-to-fixed coding as in [22], in which the number of observed channel symbols (blocklength) is prespecified, but the number of reliably recovered information bits depends on channel conditions.

In this paper, we focused on the case with a delay constraint. It is also of interest to study the case with a relaxed delay constraint, i.e., coding across blocks is allowed. Furthermore, we characterized the achievable average secrecy rate via a broadcast approach. Although the average capacity for the case without any secrecy constraints can serve as an outer bound, such a bound in general is not tight since the secrecy constraints are not taken into consideration. Therefore, it is also worth exploiting to provide tighter outer bounds to better understand how well the broadcast approach performs. Moreover, extension to the MIMO setting is interesting, where there are different ways to impose a degraded message set, and guarantee secrecy outside a bounded range.

Acknowledgment

The work of S. Zou was supported in part by NSF Grant CCF-1618658. The work of Y. Liang was supported by NSF Grant CCF-1618127. The work of S. Shamai was supported by the European Union's Horizon 2020 Research And Innovation Programme with grant agreement no. 694630.

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, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, Now Publishers, Hanover, MA, USA, 2008.

[5] M. Baldi and S. Tomasin, *Physical and Data-Link Security Techniques for Future Communication Systems*. Switzerland: Springer, 2016.

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

[7] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*. IEEE, 2007, pp. 1296–1300.

[8] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[9] X. He and A. Yener, "The role of channel states in secret key generation," in *Proc. IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, Istanbul, Turkey, 2010, pp. 2681–2686.

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

[11] A. Khisti, "On the MISO compound wiretap channel," in *Proc. Information Theory and Applications Workshop (ITA)*, Jan 2010, pp. 1–7.

[12] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of parallel Gaussian compound wiretap channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, July 2008, pp. 116–120.

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

[14] X. He and A. Yener, "Providing secrecy when the eavesdropper channel is arbitrarily varying: A case for multiple antennas," in *Proc. Annu. Allerton Conf. Communication, Control and Computing*, 2010, pp. 1228–1235.

[15] ——, "MIMO wiretap channels with arbitrarily varying eavesdropper channel states," *arXiv preprint arXiv:1007.4801*, 2010.

[16] S. Shamai (Shitz), "A broadcast strategy for the Gaussian slowly fading channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, June 1997, p. 150.

[17] 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, October 2003.

[18] Y. Liang, L. Lai, H. 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.

[19] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "Degraded broadcast channel with secrecy outside a bounded range," *arXiv preprint arXiv:1609.06353*, 2016.

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

[21] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "Broadcast networks with layered decoding and layered secrecy: Theory and applications," *Proc. IEEE*, vol. 103, no. 10, pp. 1841–1856, 2015.

[22] S. Verdú and S. Shamai (Shitz), "Variable-rate channel capacity," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2651–2667, June 2010.