On information-theoretic secrecy for wireless networks

Etienne Perron, Suhas Diggavi and Emre Telatar
EPFL, Lausanne, Switzerland
Email: {etienne.perron,suhas.diggavi,emre.telatar}@epfl.ch

***Abstract*—In this paper we summarize our recent work on information-theoretically secure wireless relay network communication. In such communication, the goal is to send information between two special nodes ("source" and "destination") in a (memoryless) network with authenticated relays, where the secrecy is with respect to a class of eavesdroppers. We develop achievable secrecy rates when authenticated relays also help increase secrecy rate by inserting noise into the network.**

I. Introduction

The seminal paper of Wyner [20] on the degraded wiretap channel and its generalization in [5] laid the foundations for information-theoretic secrecy in broadcast channels. In the recent past, information-theoretic secrecy has been applied to wireless networks with results on secrecy for MIMO broadcast channels, multiple access channels, interference channels and relay channels (see [10] and references therein). Cooperative strategies in wireless networks has been an active area of research (see [8] and references therein). In [16], [17] cooperative secrecy for *arbitrary* wireless networks was studied[1]. This work was inspired by recent (approximate) characterizations of the wireless relay network [3].

In this paper we summarize the studies in [16], [17], [14]. We will state the results for layered relay networks[2]. The main results are as follows. We first develop a "separable" strategy to provide information-theoretic secrecy for wireless networks, which operates on the principle of providing end-to-end secrecy, while the network operates without presupposing the secrecy requirement. This is developed for (layered) deterministic, Gaussian and discrete memoryless networks. We also develop a noise insertion strategy that allows a subset of the nodes in the network to insert random noise to aid in secure communication. We state the achievable secrecy rates for such active relay strategies, again for deterministic, Gaussian and discrete memoryless networks. We also state a simple outer bound for secrecy of such networks.

The paper is organized as follows. In Section II, we set up the problem and the notation. Some basic results for information flow without secrecy constraints are also established. We summarize the main results in Section III. We end with a short discussion in Section IV.

[1]The case when a *single* relay node present, as an extension of the classical relay channel to the secrecy problem was studied in [13], [9].

[2]A layered network (given more precisely in Definition 1, is loosely that all paths from source to destination are the same length. As in [3], we can extend the results for layered networks to non-layered networks using time-expansion on the network.

II. Preliminaries

We consider transmission over a relay network $\mathcal{G} = (\mathcal{V}, \mathcal{L})$, where $\mathcal{V}$ is the set of vertices representing the communication nodes in the relay network and $\mathcal{L}$ is the set of annotated channels between the nodes, which describe the signal interactions. Note that these channels are not point-to-point links, rather, they model how the transmitted signals are superimposed and received at the receiving nodes (*i.e.,* there is broadcast and interference). We consider a special node $S \in \mathcal{V}$ as the source of the message which wants to securely communicate to another special node $D \in \mathcal{V}$ (the destination) with the help of a set of (authenticated) relay nodes $\mathcal{A} \subset \mathcal{V}$ in the network. We assume that a subset $\mathcal{B} \subseteq \mathcal{A}$ of the relay nodes is allowed to generate and use independent random messages. These special relay nodes are called "noise inserting" nodes. The secrecy is with respect to a set of possible (passive) eavesdropper nodes $\mathcal{E} \subset \mathcal{V}$ where $\mathcal{E}$ is disjoint from $\mathcal{A} \cup \{S, D\}$. We want to keep all or part of the message secret if any one of the possible eavesdropper nodes $E \in \mathcal{E}$ listens to the transmissions in the relay network. Note that the class of eavesdroppers that we define is discrete, *i.e.,* we assume that all possible eavesdroppers and their channels can be enumerated. If there is a continuum of possible eavesdropper channels, our model can approximate this via "quantization" of this continuum.

A. Signal interaction models

The results in this paper are stated for layered networks formally defined as follows.

Definition 1: A relay network is *layered* if for every (i, j) such that $i \in \{S\} \cup \mathcal{B}$ and $j \in \mathcal{V}$, all the paths from i to j have the same length (the same number of hops in $\mathcal{L}$). A *non-layered* network is a network in which at least one node pair (i, j) does not have this property.

Using the time-expanded networks, as used in [3], we can extend the results for layered networks to non-layered networks. The network we consider is constituted by (layered) memoryless channel interactions, which include broadcast and multiple access interference [4] in the following ways.

Wireless interaction model: In this well-accepted model [19], transmitted signals get attenuated by (complex) gains to which independent (Gaussian) receiver noise is added. More formally, the received signal y_j at node $j \in \mathcal{V}$ at time t is given by,

$$y_j[t] = \sum_{i \in \mathcal{N}_j} h_{ij} x_i[t] + z_j[t], \tag{1}$$

where h_{ij} is the complex channel gain between node i and j which is the annotation of the channels in $\mathcal{L}$, x_i is the signal transmitted by node i, and $\mathcal{N}_j$ are the set of nodes that have non-zero channel gains to j. We assume that the average transmit power constraints for all nodes is 1 and the additive receiver Gaussian noise is of unit variance. We use the terminology *Gaussian wireless network* when the signal interaction model is governed by (1).

Deterministic interaction model: In [1], a simpler deterministic model which captures the essence of wireless interaction was developed. The advantage of this model is its simplicity, which gives insight to strategies for the noisy wireless network model in (1). The linear deterministic model of [1] simplifies the wireless interaction model in (1) by eliminating the noise and discretizing the channel gains through a binary expansion of q bits. Therefore, the received signal $y_j^{(d)}$ which is a binary vector of size q is modeled as

$$y_j^{(d)}[t] = \sum_{i \in \mathcal{N}_j} \mathbf{G}_{ij} x_i^{(d)}[t], \tag{2}$$

where $\mathbf{G}_{ij}$ is a $q \times q$ binary matrix representing the (discretized) channel transformation between nodes i and j and $x_i^{(d)}$ is the (discretized) transmitted signal. All operations in (2) are done over the binary field. We use the terminology *linear deterministic network* when the signal interaction model is governed by (2).

Discrete memoryless interaction model: The received signal y_j at node $j \in \mathcal{V}$ in layer l of the network, at time t is related to the inputs at time t through a DMC specified by, $p(y_j[t]|\{x_i[t]\}_{i\in\mathcal{N}_{l-1}})$, where $\mathcal{N}_{l-1}$ are the nodes in layer $l-1$.

To simplify the comparison between different results, we group the most important definitions below.

Definition 2: For $\mathcal{I} \subseteq \mathcal{V}$ and $j \in \mathcal{V}$, define $\Lambda(\mathcal{I}; j)$ to be the set of all cuts (Ω, Ω^c) that separate set $\mathcal{I}$ from j. More precisely, $\Lambda(\mathcal{I}; j)$ is the set of all $\Omega \subset \mathcal{V}$ such that $\mathcal{I} \subseteq \Omega$ and $j \in \Omega^c$.

Definition 3: For a (layered) relay network the transmit distribution $p(\{x_i\}_{i\in\mathcal{V}})$ and quantizers $p(\hat{y}_i|y_i)$, belong to the class $\mathcal{P}$ if for all $p \in \mathcal{P}$, we have

$$p = \left[\prod_{i\in\mathcal{V}} p(x_i)\right] p(\{y_j\}_{j\in\mathcal{V}}|\{x_i\}_{i\in\mathcal{V}}) \prod_{i\in\mathcal{V}} p(\hat{y}_i|y_i). \tag{3}$$

For given $\mathcal{I} \subseteq \mathcal{V}$ and $j \in \mathcal{V}$, we define an achievable rate between between $\mathcal{I}$ and j as

$$\hat{R}_{\mathcal{I};j}(p) \triangleq \min_{\Omega\in\Lambda(\mathcal{I};j)} \left[I(X_\Omega; \hat{Y}_{\Omega^c}|X_{\Omega^c}) - \sum_{i\in\Omega} I(Y_i; \hat{Y}_i|X_{\mathcal{V}}) \right] \tag{4}$$

where $X_{\mathcal{V}}$ are channel inputs, $Y_{\mathcal{V}}$ correspond to the channel outputs, and $\hat{Y}_{\mathcal{V}}$ are the quantized variables, all governed by $p \in \mathcal{P}$.

Definition 4: For a given transmit and quantization distribution $p \in \mathcal{P}$, a subset $\psi \subseteq \mathcal{V}$, a node $j \in \mathcal{E} \cup \{D\}$, define $\mathcal{R}_{\psi;j}(p)$ to be the set of all tuples $B_\psi = (B_i)_{i\in\psi}$ such that the components of the tuple are non-negative and such that for any subset $\mathcal{I} \subseteq \psi$, $\sum_{i\in\mathcal{I}} B_i \leq R_{\mathcal{I};j}(p)$, where the quantity $R_{\mathcal{I};j}(p)$ is the information-theoretic min-cut defined below,

$$R_{\mathcal{I};j}(p) \triangleq \min_{\Omega\in\Lambda(\mathcal{I};j)} I(X_\Omega; Y_{\Omega^c}|X_{\Omega^c}). \tag{5}$$

Note that there is a difference between $\hat{R}_{\mathcal{I};j}(p)$ given in (4) and $R_{\mathcal{I};j}(p)$ given in (5), since $\hat{R}_{\mathcal{I};j}(p)$ is the achievable rate induced by a given (quantize-map-forward) relay strategy, whereas $R_{\mathcal{I};j}(p)$ is related to a cut-value, both evaluated for $p \in \mathcal{P}$.

Definition 5: For a given input and quantization distribution $p \in \mathcal{P}$, a subset $\psi \subseteq \mathcal{V} \setminus \{S\}$, and a node $j \in \mathcal{E} \cup \{D\}$, define $\hat{\mathcal{R}}_{\psi;j}(p)$ to be the set of all tuples $(B', B_\psi) = (B', (B_i)_{i\in\psi})$ such that the components of the tuple are non-negative and such that for any subset $\mathcal{I} \subseteq \psi$,

$$B' + \sum_{i\in\mathcal{I}} B_i \leq \hat{R}_{\mathcal{I}\cup\{S\};j}(p).$$

Note that for a given $\psi \subseteq \mathcal{V} \setminus \{S\}$, $\hat{\mathcal{R}}_{\psi;j}(p)$ differs from $\mathcal{R}_{\psi\cup\{S\};j}(p)$ in two ways. First, $\mathcal{R}_{\psi\cup\{S\};j}(p)$ is related to information-theoretic cut-values, evaluated for a particular $p \in \mathcal{P}$, and $\hat{\mathcal{R}}_{\psi;j}(p)$ is related to the achievable rate for a particular (quantization) relay strategy. Secondly, $\mathcal{R}_{\psi\cup\{S\};j}(p)$ imposes constraints for all subsets of ψ including those that do not contain S, *i.e.*, like a MAC region. In Definition 5 for $\hat{\mathcal{R}}_{\psi;j}(p)$, all the rate-constraints involve S.

Secrecy requirements:: The notion of information-theoretic secrecy is defined through the *equivocation* rate R_e, which is the residual uncertainty about the message when the observation of the strongest eavesdropper is given. More formally, [20], [5], given a (T, ϵ)-code, the equivocation rate is $\frac{1}{T}\min_{E\in\mathcal{E}} H(W|\mathbf{Y}_E)$, where W is the uniformly distributed source message, $\mathbf{Y}_E$ is the sequence of observations at eavesdropper E and $H(\cdot|\cdot)$ denotes the (conditional) entropy [4]. The "perfect" (weak) secrecy capacity is the largest transmitted information rate R, such that $R = R_e$ is achievable. This notion can be strengthened to *strong* perfect secrecy, if the equivocation is defined in bits $\min_{E\in\mathcal{E}} H(W|\mathbf{Y}_E)$, instead of a rate [12]. Using the tools developed in [12], we can convert all the results to strong secrecy, once we have proved it for weak secrecy (see also [14]).

B. Information flow over layered networks

Here we summarize results about communication in layered networks that form an ingredient to our main results on secrecy over relay networks. With no secrecy requirements, the transmission scheme is the same as developed in [3], and is informally described below.

Network operation:: Each node in the network generates codes independently using a distribution $p(x_i)$. The source S chooses a random mapping from messages $w \in \{1, \ldots, 2^{RT}\}$ to its transmit typical set $\mathcal{T}_{x_S}$, and therefore we denote by $\mathbf{x}_S^{(w)}, w \in \{1, \ldots, 2^{TR}\}$ as the possible transmit sequences for each message. Each received sequence $\mathbf{y}_i$ at node i is quantized to $\hat{\mathbf{y}}_i$ and this quantized sequence is randomly

mapped onto a transmit sequence $\mathbf{x}_i$ using a random function $\mathbf{x}_i = f_i(\hat{\mathbf{y}}_i)$, which is chosen such that each quantized sequence is mapped uniformly at random to a transmit sequence. This random mapping can be represented by the following construction. Generate 2^{TR_i} sequences $\mathbf{x}_i$ from the distribution $\prod_j p(\mathbf{x}_i[j])$, and generate 2^{TR_i} sequences $\hat{\mathbf{y}}_i$ using a product distribution $\prod_j p(\hat{\mathbf{y}}_i[j])$. We denote the 2^{TR_i} sequences of $\hat{\mathbf{y}}_i$ as $\hat{\mathbf{y}}_i^{(k_i)}, k_i \in \{1, \ldots, 2^{TR_i}\}$. Note that standard rate-distortion theory tells us that we need $R_i > I(Y_i; \hat{Y}_i)$ for this quantization to be successful. Note that since the uniformly at random mapping produces $\mathbf{x}_i = f_i(\hat{\mathbf{y}}_i)$, for a quantized value of index k_i, we will denote it by $\hat{\mathbf{y}}_i^{(k_i)}$ and the sequence it is mapped to by $\mathbf{x}_i^{(k_i)} = f_i(\hat{\mathbf{y}}_i^{(k_i)})$.

In [3], this scheme was analyzed for deterministic and Gaussian networks. It was established that for deterministic networks, all rates up to $\min_{\Omega \in \Lambda(S:D)} H(Y_{\Omega^c}|X_{\Omega^c})$ for any product distribution of the nodes can be achieved. For linear deterministic networks, (2), this coincides with the cut-set outer bound. For Gaussian networks, an approximate max-flow, min-cut bound was established, which showed that all rates up to $\min_{\Omega \in \Lambda(S:D)} I(X_\Omega; Y_{\Omega^c}|X_{\Omega^c}) - \kappa$, was achievable, where κ was a universal constant, independent of SNR and channel parameters [3].

In the multisource problem, a set of sources $\mathcal{S} \subset \mathcal{V}$ wish to communicate independent messages to the destination D over the network. Each of the relay nodes operate as above, except if it is also a source, then the transmitted sequence is a (uniform random) mapping of both its message and its received (quantized) signal. This scheme, which is a simple extension of the scheme studied in [3], was studied for the deterministic and Gaussian interaction models in [17], [14]. Its simple extension to (layered) memoryless networks is stated below.

Theorem 1: For any memoryless layered network, from a set of sources $\mathcal{S}$ to a destination D, we can achieve any rate vector satisfying

$$\sum_{k \in \mathcal{I} \subseteq \mathcal{S}} R_k \leq \hat{R}_{\mathcal{I};j}(p)$$

for some distribution $p \in \mathcal{P}$ defined in (3), where $\hat{R}_{\mathcal{I};j}(p)$ is defined in (4).

III. Main Results

Broadly there are a sequence of three (increasing generality) ideas to the achievability scheme. (i) *Separable scheme:* The relay network is operated as described in Section II-B, but the secrecy is induced by an end-to-end scheme overlaid on this. (ii) *Noise insertion:* In addition to the above operation, a subset of the authenticated relays insert independent messages (noise) which are intended to disrupt the eavesdropper and are not required to be decoded. (iii) *Auxiliary variables:* In addition to the above, the source prefixes an artificial multiuser channel in order to allow multiple auxiliary variables.

We will state the results in increasing generality in order to clarify and interpret the results. For the simplest case, where relay nodes operate using the quantize-map-forward strategy described in Section II-B, without regard to secrecy requirements, the end-to-end separable scheme achieves the following secrecy region.

Theorem 2: For a given distribution $p \in \mathcal{P}$ defined in (3), the (strong) perfect secrecy rate between the source S and destination D with respect to a class of eavesdroppers $\mathcal{E}$, with $\hat{R}_{S;D}(p)$ given in (4), is lower bounded as

$$\bar{C}_s \quad \geq \quad \hat{R}_{S;D}(p) - \max_{E \in \mathcal{E}} \min_{\Omega \in \Lambda_E} I(X_\Omega; Y_{\Omega^c}|X_{\Omega^c}),$$

where the second term is evaluated for $p \in \mathcal{P}$.

Special cases of this result for deterministic and Gaussian networks was shown in [16]. In the deterministic case, as in [2], the relays do not quantize the inputs, but map-and-forward it. Therefore, for deterministic networks the perfect secrecy rate is $\min_{\Omega \in \Lambda_D} H(Y_{\Omega^c}|X_{\Omega^c}) - \max_{E \in \mathcal{E}} \min_{\Omega \in \Lambda_E} H(Y_{\Omega^c}|X_{\Omega^c})$. In the Gaussian case, by using a quantizer that gets distortion equal to the noise variance (see [3]), $I(Y_i; \hat{Y}_i|X_\mathcal{V})$ is a constant (depending on the noise variance and not the channels), for every relay node i.

We can improve and generalize the result in Theorem 2 by using noise insertion at an arbitrary subset $\mathcal{B} \subset \mathcal{V}$. These independent messages are not needed to be decoded anywhere, but can be used to "jam" the eavesdroppers.

Definition 6: For an input distribution p, we define the following function:

$$F(p) = \max_{B_\mathcal{B} \in \cap_{E \in \mathcal{E}} \mathcal{R}_{\mathcal{B};E}(p)} \Big[\max_x \{x : (x, B_\mathcal{B}) \in \hat{\mathcal{R}}_{\mathcal{B};D}(p)\} - \max_x \{x : (x, B_\mathcal{B}) \in \cup_{E \in \mathcal{E}} \mathcal{R}_{\mathcal{B} \cup \{S\};E}(p)\} \Big].$$

Theorem 3: The (strong) perfect secrecy for any (layered) relay network is lower bounded as

$$\bar{C}_s \geq \max_{p \in \mathcal{P}} F(p),$$

Basically the idea in Theorem 3 is that the noise insertion effectively creates virtual MAC regions (for the eavesdroppers and the legitimate receiver). The projection of the difference of these regions onto the source message rate yields the secrecy rate[3]. That is, the noise insertion "fills" up the eavesdropper rate region with "junk" information, thereby protecting the information. This notion can actually be formalized, as seen in [14]. Also note that this is a way to think of the wiretap channel [20], where all the junk information is at the source. The noise insertion just distributes the origins of the junk all over the network. This strategy was analyzed for deterministic and Gaussian networks in [14], and the above result is its simple generalization for memoryless networks.

In order to introduce auxiliary variables, we prefix an artificial memoryless channel in the sources, thereby modifying the channel law for the networks. Since this does not change the basic arguments for Theorem 3 (or its special case of

[3]A related strategy was developed in [9] for the Gaussian (single) relay channel where the relay forwarded Gaussian noise along with decoded information.

Theorem 2), we do not restate the result. Note that in this case the form of the secrecy rate is the same, except that we can also optimize over the choice of the artificial channels. This essentially would be generalization of the approach taken in [15] for the wiretap channel, to the case of relay networks. Also, following the program of [12] one can focus on showing results for weak secrecy, but (as mentioned earlier), using the techniques of [12] we can obtain it for strong secrecy (see [14] for more details).

The next result is a simple upper bound on the perfect secrecy rate for an arbitrary number of noise-inserting nodes presented in [17].

Theorem 4: For a single eavesdropper E,

$$R_s \leq \max_{p(\{x_i\}_{i\in\mathcal{V}})} \min_{\Omega\in\Lambda(S\mathcal{B},D)} I(X_\Omega; Y_{\Omega^c}|Y_E, X_{\Omega^c}), \quad (6)$$

where, in contrast to Theorems 2 and 3, the maximization is not only over product distributions but over all possible $p(\{x_i\}_{i\in\mathcal{V}})$.

The statement of Theorem 4 is valid for any type of signal interaction, including noisy channels.

IV. Discussion

In this paper we have summarized some of our studies on a communication scenario with secrecy requirement for wireless relay networks. We attempt to model the uncertainty in the eavesdropper's wireless channel, by developing the secrecy rates for a class of eavesdropper channels. It is possible to interpret the secret message generated as secret key generation, and therefore we can use the techniques outlined in this paper to generate an unconditionally (strongly) secure key. One of the important open questions is to develop characterizations of secrecy rates over networks. To obtain such a characterization we need a matching converse stating that no scheme can do better. The outer bound developed in Theorem 4 is quite simple, and we need more sophisticated outer bounding techniques. Another important issue to address is the relevance of these results for wireless networks. In order to make them more applicable, we need to ensure robustness of these results to uncertainties in (network) channel knowledge and eavesdroppers. An interesting approach to addressing this might be the use of feedback. In the seminal paper [11], Maurer showed the surprising result that feedback can allow information-theoretic secrecy, even when the eavesdropper channel dominates that of the legitimate receiver. The use of feedback for network secrecy is a scarcely explored topic and one we believe is worth pursuing. Some preliminary results in this direction were presented in [18]. The recent results of [6], [7] have established strategies also for key-agreement between a set of nodes in a single-hop network. Therefore, we believe that robustness using feedback, is another promising research direction.

References

[1] A. Avestimehr, S. Diggavi, and D. Tse, "A deterministic approach to wireless relay networks," in *Proc. of the Allerton Conf. on Commun., Control and Computing*, Illinois, USA, Sep. 2007, see: http://licos.epfl.ch/index.php?p=research_projWNC.

[2] ——, "Wireless network information flow," in *Proc. of the Allerton Conf. on Commun., Control and Computing*, Illinois, USA, Sep. 2007, see: http://licos.epfl.ch/index.php?p=research_projWNC.

[3] ——, "Wireless network information flow: A deterministic approach," *IEEE Trans. Inform. Theory*, 2009, submitted, http://arxiv.org/abs/0906.5394.

[4] T. Cover and J. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, May 1978.

[6] I. Csiszar and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, pp. 3047–3061, December 2004.

[7] ——, "Secrecy capacities for multiterminal channel models," *IEEE Transactions on Information Theory*, vol. 54, pp. 2437–2452, June 2008.

[8] G. Kramer, I. Maric, and R. Yates, *Cooperative Communications*. Foundations and Trends in Networking, 2006.

[9] L. Lai and H. E. Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[10] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Foundations and Trends in Communications and Information Theory, 2009.

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

[12] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *EUROCRYPT, LNCS 1807*, pp. 351–368, 2000, Springer.

[13] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. Inform. Theory*, Nov. 2006, submitted.

[14] E. Perron, "Information-theoretic secrecy for wireless networks," Ph.D. dissertation, School of Computer and Communication Sciences, EPFL., Lausanne, Switzerland, August 2009, available from http://library.epfl.ch/theses/?nr=4476.

[15] E. Perron, S. Diggavi, and E. Telatar, "A multiple access approach for the compound wiretap channel," in *Proc. of the IEEE Inform. Theory Workshop*, Taormina, Italy, Oct. 2009.

[16] ——, "On cooperative wireless network secrecy," in *Proc. of IEEE Infocom*, Rio de Janeiro, Brazil, Apr. 2009, pp. 1935–1943.

[17] ——, "On noise insertion strategies for wireless network secrecy," in *Proc. of the Information Theory and Applications Workshop*, San Diego, USA, Feb. 2009, pp. 77–84.

[18] E. Perron, S. N. Diggavi, and I. E. Telatar, "Wireless network secrecy with public feedback," in *46th Annual Allerton Conference on Communication, Control, and Computing*, Allerton, Illinois, USA, September 2008, pp. 753–760.

[19] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, May 2005.

[20] A. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.