On cooperative secrecy for discrete memoryless relay 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 consider information-theoretically secure communication 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 [15] on the degraded wiretap channel and its generalization in [3] 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 [7] and references therein). Cooperative strategies in wireless networks has been an active area of research (see [4] and references therein). In [13], [14] cooperative secrecy for *arbitrary* wireless networks was studied[1]. This work was inspired by recent (approximate) characterizations of the wireless relay network [1].

In this paper we extend the studies in [13], [14] in two distinct ways. First we provide an achievable secrecy rate for arbitrary (layered) discrete memoryless networks and thereby generalizing the results in [13] which were presented for deterministic networks and its Gaussian counterpart[2]. Second we generalize the noise insertion strategy studied in [11], [14], [5] to arbitrary memoryless networks. This would also enable a multiple-access approach for the compound wiretap channel [12] to the case of arbitrary networks[3].

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. The proof outlines are provided in Section IV.

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.

Signal interaction model: 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 [1], we can extend the results for layered networks to non-layered networks. The network we consider is constituted by (layered) discrete memoryless channel interactions, which include broadcast and multiple access interference [2]. 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,

$$p(y_j[t] | \{x_i[t]\}_{i \in \mathcal{N}_{l-1}}), \tag{1}$$

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

[1] The case when a *single* relay node present, as an extension of the classical relay channel to the secrecy problem was studied in [10], [5].

[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 [1], we can extend the results for layered networks to non-layered networks using time-expansion on the network.

[3] This in part is motivated by interesting new coding scheme developed in [8] for the compound parallel Gaussian wiretap channel, which was studied in [6]. A way to interpret this is that we introduce multiple auxiliary random variables into the achievable scheme in [13], [14] and give structure to it.

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: Consider a (layered) relay network with discrete signal alphabets. 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

$$p = \left[\prod_{i\in\mathcal{V}} p(x_i)\right] p(\{y_j\}_{j\in\mathcal{V}}|\{x_i\}_{i\in\mathcal{V}}) \prod_{i\in\mathcal{V}} p(\hat{y}_i|y_i). \qquad (2)$$

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

$$\hat{R}_{\mathcal{I};j}(p) \triangleq \min_{\Omega\in\Lambda(\mathcal{I};j)} \left[I(X_\Omega;\hat{Y}_{\Omega^c}|X_{\Omega^c}) - \sum_{i\in\Omega} I(Y_i;\hat{Y}_i|X_\mathcal{V}) \right] \qquad (3)$$

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,

$$R_{\mathcal{I};j}(p) \triangleq \min_{\Omega\in\Lambda(\mathcal{I};j)} I(X_\Omega;Y_{\Omega^c}|X_{\Omega^c}). \qquad (4)$$

Note that there is a difference between $\hat{R}_{\mathcal{I};j}(p)$ given in (3) and $R_{\mathcal{I};j}(p)$ given in (4), 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, [15], [3], 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 [2]. 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 [9]. Using the tools developed in [9], we can convert all the results to strong secrecy, once we have proved it for weak secrecy (see also [11]).

A. Information flow over layered networks

Here we present a result about communication in a layered DMC network that is needed for the proof of our main results on cooperative secrecy. With no secrecy requirements, the transmission scheme is the same as developed in [1], 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 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 was studied for the deterministic and Gaussian interaction models in [14], [11]. 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 (2), where $\hat{R}_{\mathcal{I};j}(p)$ is defined in (3).

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-A, 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-A, 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 (2), 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 (3), 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 $p \in \mathcal{P}$.

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 with discrete memoryless signal interaction 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[4]. 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 the proof outline. Also note that this is a way to think of the wiretap channel [15], where all the junk information is at the source. The noise insertion just distributes the origins of the junk all over the network.

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 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. Also, in the proof outlines, we will focus on weak secrecy, but as mentioned earlier, using the techniques of [9] we can obtain it for strong secrecy (see [11] for more details).

IV. Proof outlines

We first give a proof outline for Theorem 2 for a single eavesdropper, to illustrate the basic techniques. We also give a proof outline for Theorem 3, for the special case of a single eavesdropper and a single noise inserting node. These ideas can then be generalized to give the results stated.

A. Proof outline for Theorem 2

In the separable scheme, the relay network operates as described in Section II-A, without secrecy requirements. The secrecy is induced by an end-to-end "coloring" scheme overlaid on the message list induced at the eavesdropper. In particular, the source transmits a sequence $\mathbf{X}_S$ based on the information message W and a "junk" message J, which have rates R_s and B respectively. For a given choice of relay strategy determined by $p \in \mathcal{P}$, the equivocation R_e at the eavesdropper E can be lower bounded as,

$$\frac{1}{T} H(W|\mathbf{Y}_E) \geq \frac{1}{T} H(\mathbf{X}_S) - \frac{1}{T} H(\mathbf{X}_S | W, \mathbf{Y}_E) - \frac{1}{T} I(\mathbf{X}_S; \mathbf{Y}_E), \qquad (5)$$

where $\mathbf{Y}_E$ is the received sequence at the eavesdropper. Since the message needs to be decoded at the destination, by choosing a total rate $R_s + J$ such that $\frac{1}{T} H(\mathbf{X}_S) = \hat{R}_{S;D}(p) - \epsilon_1$, we guarantee using Theorem 1, for large enough T, that we can do so with vanishing error probability. Now, let us fix a information message $W = w$, and define A_w is the event that E makes a decoding error when trying to decode J, using $\mathbf{Y}_E$, assuming that $W = w$ is available (through a genie) to E. Note that for a fixed $W = w$, the codewords generated at S has the same distribution as a randomly generated code of rates B. Now, we choose junk rate B such that $B \leq \hat{R}_{S;E}(p)$, and this ensures (again due to Theorem 1) that $\mathbb{E}[\mathbf{P}(A_w)] \leq \epsilon_0$. Here the expectation is over the randomly generated code (over source and relays). Therefore by using Fano's inequality [2], we can bound $\frac{1}{T} H(\mathbf{X}_S | W, \mathbf{Y}_E) \leq \epsilon'$, again for large enough T, and arbitrary $\epsilon' > 0$. Hence, the only remaining term to bound in (5), is the term $\frac{1}{T} I(\mathbf{X}_S; \mathbf{Y}_E)$. We bound this by using the following (more general) result proved in [11], which is a form of "local" converse[5].

Lemma 1: Consider a (layered) discrete memoryless network, with finite transmit alphabets. Let $\mathcal{I} \subseteq \mathcal{B}$ be a subset of the noise-inserting nodes and let $E \in \mathcal{V}$ be any node. Let $\prod_{i \in \mathcal{V}} p(x_i)$ be given and let $(\mathbf{X}_\mathcal{V}, \mathbf{Y}_\mathcal{V})$ be the corresponding random transmit and received sequences. The randomness of these sequences comes from the randomness of the code, as well as from the random messages and the channel noise. We assume that the code is a block code of typical sequences (with

[4] A related strategy was developed in [5] for the Gaussian (single) relay channel where the relay forwarded Gaussian noise along with decoded information.

[5] We term this local converse, because it applies to a *given* product distribution on the relay maps and forms a cut-set like outer bound on the mutual information.

respect to $p \in \mathcal{P}$). We have that for any $\epsilon > 0$, there is a large enough value of T such that

$$\mathbf{P}\big(I(\mathbf{X}_S, \mathbf{X}_\mathcal{I}; \mathbf{Y}_E | J_{\mathcal{B}\setminus\mathcal{I}}) > TR_{\mathcal{I}\cup\{S\};E}(p)\big) \leq \epsilon.$$

Here, the probability is over all randomly generated codes, and $R_{\mathcal{I};j}(p)$ is defined in (4).

Therefore, by setting $\mathcal{B} = \phi$, we get from Lemma 1 that for large enough T and any $\epsilon'' > 0$, $\mathbf{P}\big(I(\mathbf{X}_S; \mathbf{Y}_E) > TR_{S;E}(p)\big) \leq \epsilon''$. By putting all these together in (5), we see that for a choice of junk rate $B \leq \hat{R}_{S;E}(p)$ and $R_s + B = \hat{R}_{S;D}(p) - \epsilon_1$, we obtain the result given in Theorem 2, for the single eavesdropper[6].

Now, we illustrate the technique for multiple eavesdroppers. The basic idea is to have multiple "junk" messages at the source. For example, if we have two eavesdroppers E_1, E_2. then the source transmits a sequence $\mathbf{X}_S$ based on the information message W and two "junk" messages (J_1, J_2), which have rates R_s and (B_1, B_2) respectively. For a particular choice of $p \in \mathcal{P}$, let $R_{S;E_1}(p) \geq R_{S;E_2}(p)$, with no loss of generality. In this case, we can lower bound the equivocations at each of the eavesdroppers as,

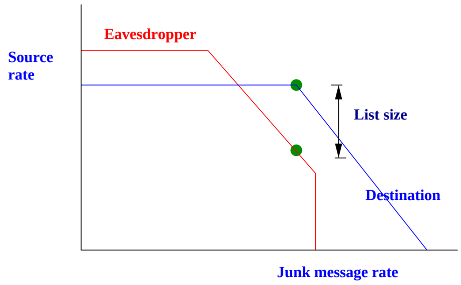
$$\begin{aligned}
\frac{1}{T}H(W|\mathbf{Y}_{E_1}) &\geq \frac{1}{T}H(\mathbf{X}_S) - \frac{1}{T}H(\mathbf{X}_S|W, \mathbf{Y}_{E_1}) - \frac{1}{T}I(\mathbf{X}_S; \mathbf{Y}_{E_1}),\\
\frac{1}{T}H(W|\mathbf{Y}_{E_2}) &\geq \frac{1}{T}H(\mathbf{X}_S|J_1) - \frac{1}{T}H(\mathbf{X}_S|W, J_1, \mathbf{Y}_{E_2})\\
&- \frac{1}{T}I(\mathbf{X}_S; \mathbf{Y}_{E_2}|J_1).
\end{aligned}$$

Now, the argument is similar to the case with the single eavesdropper. We choose a total rate $R_s + B_1 + B_2$ such that (W, B_1, B_2) is decodable at D. For eavesdropper E_2, we choose a junk rate J_2, such that it is able to decode it, given access to (W, J_1), *i.e.*, $B_2 \leq \hat{R}_{S;E_2}(p)$. Then we choose rate B_1, so that (J_1, J_2) is decodable at E_1 given access to W, *i.e.*, $B_1 + B_2 \leq \hat{R}_{S;E_1}(p)$. By doing this, as before we can use Fano's inequality to bound the second terms in each of the above equivocation terms. The last term in each of the above equivocation inequalities are again bounded by using the local converse Lemma 1. Using this argument we therefore lower bound the minimum of the two equivocation rates as $\hat{R}_{S;D}(p) - \max_{i\in\{1,2\}}\{\min_{\Omega\in\Lambda_{E_i}} I(X_\Omega; Y_{\Omega^c}|X_{\Omega^c})\}$, where the mutual information is also evaluated for $p \in \mathcal{P}$. Now, by using a similar argument as in the single eavesdropper case, we can ensure perfect secrecy for this information rate. This argument can be extended to an arbitrary number of eavesdroppers.

B. Proof outline for Theorem 3

The idea in Theorem 3 is that a set of nodes $\mathcal{B}$ insert independent messages that need not be decoded, but could help secrecy. We will illustrate the proof idea using a single noise inserter, but the idea for multiple inserters is extended using techniques similar to that developed in [11], in the case of deterministic and Gaussian networks.

Assume that a single relay node $A \in \mathcal{V}$ inserts a noise message J_A at rate B_A *i.e.*, its transmit sequence $\mathbf{X}_A$ is a function of $(J_A, \hat{\mathbf{Y}}_A)$, where $\hat{\mathbf{Y}}_A$ is its (quantized) received sequence. In addition, as in Section IV-A the source transmits $\mathbf{X}_S$ which is a function of (W, J), its information and "junk" message. As in (5), we can write the equivocation at the eavesdropper E for any $\mathcal{I} \subseteq \mathcal{B} = A$ as,



$$\frac{1}{T}H(W|\mathbf{Y}_E) \geq H(\mathbf{X}_S, \mathbf{X}_\mathcal{I}|J_{\mathcal{B}\setminus\mathcal{I}}) - H(\mathbf{X}_S, \mathbf{X}_\mathcal{I}|W, \mathbf{Y}_{E_1}, J_{\mathcal{B}\setminus\mathcal{I}}) \tag{6}$$
$$- I(\mathbf{X}_S, \mathbf{X}_\mathcal{I}; \mathbf{Y}_E|J_{\mathcal{B}\setminus\mathcal{I}}).$$

Now, the proof proceeds in a manner similar to Section IV-A, with the multisource regions replacing the rates used earlier. Due to Theorem 1 by choosing $R_s + B + B_\mathcal{I} \leq \hat{R}_{\mathcal{I}\cup\{S\}:D}(p)$, with equality for some $\mathcal{I} \subseteq \mathcal{B}$, we can ensure that (W, J) are decoded at D with high probability. Now, if E is given access to $W = w$, we can decode the junk messages (J, J_A) at E, if $B + B_\mathcal{I} \leq \hat{R}_{\mathcal{I}\cup\{S\}:E}(p)$ and $B_\mathcal{I} \leq \hat{R}_{\mathcal{I}:E}(p)$, *i.e.*, the rates (J, J_A) lie in the MAC region. Such a choice allows us to use Fano's inequality and show that $H(\mathbf{X}_S, \mathbf{X}_\mathcal{I}|W, \mathbf{Y}_{E_1}, J_{\mathcal{B}\setminus\mathcal{I}})$, the second term in (6) is small. Finally, by using the local converse Lemma 1, we upperbound the third term. Putting these together, we get the result stated in Theorem 3. This is illustrated in Figure IV-B, where the pentagon represents the MAC region associated with the eavesdropper ($\mathcal{R}_{\psi\cup\{S\};j}(p)$), and the trapezoid represents the region for the destination involving the source ($\hat{\mathcal{R}}_{\mathcal{I};j}(p)$). By creating uncertainty at the eavesdropper, we can obtain perfect secrecy.

C. Proof outline for Theorem 1

We will illustrate this for a single source, in a layered network. The encoding and decoding strategies are as in [1] as described in Section II-A. To summarize, the decoder D checks the set $\hat{\mathcal{W}}$ of messages $\hat{w}$ for which there exists some indices $\{k_j\}$ for all the relay nodes such that

$$(\mathbf{x}_S^{(\hat{w})}, \mathbf{y}_D, \{\hat{\mathbf{y}}_i^{(k_i)}, \mathbf{x}_i^{(k_i)}\}_i) \in \mathcal{A}_\epsilon, \tag{7}$$

where $\mathcal{A}_\epsilon$ is joint typicality. That is we have a set of plausible transmit sequences and associated quantized values for which w' is possible. With high probability the correct message w is in this list, *i.e.*, $\mathbf{P}(w \in \hat{\mathcal{W}}) \to 1$, as block-length T becomes large. Let us denote that for the message w, the quantization indices are $\{k_i\}$ at the relays. We have an error if $w' \neq w$ is also in the list. This probability that $w' \in \hat{\mathcal{W}}$), when $w \neq w'$ was transmitted can be written as follows.

$$\Pr\left\{w \to w'\right\} = \mathbf{P}\left\{\exists\{k_i'\}_i, \forall i, \text{ such that } (\mathbf{x}_S^{(w')}, \mathbf{y}_D, \{\hat{\mathbf{y}}_i^{(k_i')}, \mathbf{x}_i^{(k_i')}\}_i) \in \mathcal{A}_\epsilon\right\} \tag{8}$$

[6] Note the equivocation rate R_e is smaller than R_s, and therefore to get perfect secrecy we need to use a further argument to keep the part of the information with rate equal to $R_e = \hat{R}_{S;D}(p) - \min_{\Omega\in\Lambda_E} I(X_\Omega; Y_{\Omega^c}|X_{\Omega^c})$ perfectly secure.

Distinguishability:: A node i can distinguish between w and w' if $\hat{\mathbf{y}}_i \neq \hat{\mathbf{y}}'_i$, where the "primed" system denotes that under w'. We can condition on the event that the correct message produces indices $\{k_i\}$, and since this is a generic index, we can carry out the entire calculation conditioned on this and then average over it. Of course, we need to take into account all possible outcomes due to the incorrect message, and so we can rewrite (8) as,

$$\Pr\{w \to w'\} \leq \sum_{\Omega} \sum_{i} \sum_{k'_i=1}^{2^{TR_i}} \mathbf{P}\Big\{\{k'_i\}_i, \text{ such that } k'_i = k_i, \forall i \in \Omega^c, \tag{9}$$
$$k'_i \neq k_i, \forall i \in \Omega, (\mathbf{x}_S^{(w')}, \mathbf{y}_D, \{\hat{\mathbf{y}}_i^{(k'_i)}, \mathbf{x}_i^{(k'_i)}\}_i) \in \mathcal{A}_\epsilon\Big\}$$

Given (9), we can focus on a particular cut Ω. note that we can reduce the summation over all i to that in $i \in \Omega$, since for these the quantization index is fixed, *i.e.*, $k'_i = k_i, i \in \Omega^c$. For a particular cut, we can write the cut-probability expression as

$$\Pr\{w \to w'\} \leq \sum_{i \in \Omega} \sum_{k'_i=1}^{2^{TR_i}} \mathcal{P} \tag{10}$$

where

$$\mathcal{P} = \mathbf{P}\Big\{\{k'_i\}_i, \text{ such that } k'_i = k_i, \forall i \in \Omega^c,\ k'_i \neq k_i, \forall i \in \Omega, \tag{11}$$
$$(\mathbf{x}_S^{(w')}, \mathbf{y}_D, \{\hat{\mathbf{y}}_i^{(k'_i)}, \mathbf{x}_i^{(k'_i)}\}_i) \in \mathcal{A}_\epsilon\Big\}$$

Now, let us examine $\mathcal{P}$ by defining the event (which is a "consistency" check),

$$\mathcal{F}_l = \Big\{\{k'_i\}_i, \text{ s.t } k'_i = k_i, \forall i \in \Omega_l^c,\ k'_i \neq k_i, \forall i \in \Omega_l, \tag{12}$$
$$(\{\hat{\mathbf{y}}^{(k'_i)}\}_{i \in \mathcal{N}_l}, \{\mathbf{x}_j^{(k'_j)}\}_{j \in \mathcal{N}_{l-1}}) \in \mathcal{A}_\epsilon\Big\},$$

where for convenience of notation we have denoted $\mathbf{y}_D = \hat{\mathbf{y}}_i^{(k'_i)}, i \in \mathcal{N}_{L_D}$, and $\mathbf{x}_S = \mathbf{x}_j^{(k'_j)}, j \in \mathcal{N}_0, L_S = 0$. As before we have also used $\Omega_l = \Omega \cap \mathcal{N}_l$. Therefore, we can write

$$\mathcal{P} = \Pr\{\mathcal{F}_l, l = 1, \ldots, L_D\} \tag{13}$$

The calculation of $\mathcal{P}$ asks the probability that sequences generated like

$$\left[\prod_{j \in \Omega} p(\mathbf{x}_j)\right] \left[\prod_{i \in \Omega} p(\hat{\mathbf{y}}_i)\right] [p(\{\hat{\mathbf{y}}_i\}_{i \in \Omega^c}, \{\mathbf{x}_j\}_{j \in \Omega^c})], \tag{14}$$

behaves as if they were generated jointly, *i.e.*, like $p(\{\hat{\mathbf{y}}_i\}_{i \in \mathcal{V}}, \{\mathbf{x}_j\}_{j \in \mathcal{V}})$.

Lemma 2: $\mathcal{P} \leq 2^{-T[\Gamma - 4\epsilon]}$, where

$$\Gamma = \sum_{j \in \Omega} H(X_j) + \sum_{i \in \Omega} H(\hat{Y}_i) + H(\{\hat{Y}_i\}_{i \in \Omega^c}, \{X_j\}_{j \in \Omega^c}) \tag{15}$$
$$- H(\{\hat{Y}_i\}_{i \in \mathcal{V}}, \{X_j\}_{j \in \mathcal{V}})$$

We can simplify Γ as,

$$\begin{aligned} \Gamma &= I(\{\hat{Y}_i\}_{i \in \Omega^c}; \{X_j\}_{j \in \Omega} | \{X_j\}_{j \in \Omega}^c) \\ &- H(\{\hat{Y}_i\}_{i \in \Omega} | \{X_j\}_{j \in \mathcal{V}}, \{\hat{Y}_i\}_{i \in \Omega^c}) + \sum_{i \in \Omega} H(\hat{Y}_i) \end{aligned} \tag{16}$$

Now if we use (16) and Lemma 2 in (10), we get

$$\sum_{i \in \Omega} \sum_{k'_i=1}^{2^{TR_i}} 2^{-T[\Gamma - 4\epsilon]} = 2^{-T[[\Gamma - \sum_{i \in \Omega} R_i] - 4\epsilon]}, \tag{17}$$

where Γ is given in (16). Also since we will choose $R_i = I(\hat{Y}_i; Y_i) + \epsilon'$ to ensure the existence of the appropriate quantizer, we can write the exponent in (17) after some algebra as,

$$\min_{\Omega \in \Lambda(\mathcal{I};j)} \left[I(X_\Omega; \hat{Y}_{\Omega^c} | X_{\Omega^c}) - \sum_{i \in \Omega} I(Y_i; \hat{Y}_i | X_\mathcal{V}) \right] \tag{18}$$

which yields the result for a single source. The multi-source extension is quite similar to this (see also [11] for a similar proof for the deterministic and Gaussian cases).

References

[1] A. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow: A deterministic approach," *IEEE Trans. Inform. Theory*, 2009, submitted, http://arxiv.org/abs/0906.5394.

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

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

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

[5] 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.

[6] Y. Liang, G. Kramer, H. Poor, and S. Shamai, "Compound wire-tap channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, Dec. 2008, to appear.

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

[8] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of parallel gaussian compound wiretap channels," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Toronto, Canada, Jul. 2008.

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

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

[11] 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.

[12] 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.

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

[14] ——, "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.

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