Compound Wire-tap Channels

Yingbin Liang, Gerhard Kramer, H. Vincent Poor and Shlomo Shamai (Shitz)

***Abstract*— The compound wire-tap channel is studied, which is based on the classical wire-tap channel with the channel from the source to the destination and the channel from the source to the wire-tapper taking a number of states, respectively. This channel can also be viewed as the wire-tap channel with multiple destinations and multiple wire-tappers, i.e., *multicast with multiple wire-tappers*. The source wishes to transmit information to all destinations and wants to keep the information secret from all wire-tappers. For the discrete memoryless compound wire-tap channel, lower and upper bounds on the secrecy capacity are derived and are shown to match for the degraded channel. The parallel Gaussian compound wire-tap channel is further studied, for which the secrecy capacity and the characterization of an optimal power allocation are obtained. The secrecy degree of freedom ($s.d.o.f.$) is also derived, which connects the secure communication rate in the high SNR regime to secure networking coding for deterministic networks. Finally, the multi-antenna (i.e., MIMO) compound wire-tap channel is studied. The secrecy capacity is established for the degraded MIMO compound wire-tap channel and an achievable $s.d.o.f.$ is given for the general MIMO compound wire-tap channel.**

I. Introduction

The compound channel models transmission over a channel that may take a number of states, and reliable communication needs to be guaranteed no matter which state occurs. For example, this might occur for real-time wireless communications when the source has no knowledge of the channel state, but zero performance outage needs to be guaranteed subject to a stringent delay constraint. In this paper, we are interested in the compound channel with a wire-tapper that receives outputs from a compound channel that may also take a number of states. Now the source not only needs to guarantee reliable communication to the destination, but also needs to prevent the information from being known by the wire-tapper. This is a generalization of Wyner's wire-tap channel [1] to the case of multiple channel states.

The compound wire-tap channel can also be viewed as the wire-tap channel with multiple destinations and multiple wire-tappers with each source-to-destination channel state corresponding to the channel from the source to one destination and each source-to-wire-tapper channel state corresponding to the channel from the source to one wire-tapper. The source wants to transmit information to all the destinations and needs to keep the information secret from all wire-tappers. Such a model is also referred to as the *multicast with multiple wire-tappers*. From this viewpoint, the compound wire-tap channel provides a general framework that includes a number of models studied previously as special cases. These models include the parallel wire-tap channel with two wire-tappers studied in [2], [3], the fading wire-tap channels with multiple wire-tappers studied in [4], and the wire-tap channel with multiple receivers studied in [5].

In this paper, we first study the discrete memoryless compound wire-tap channel, for which we provide lower and upper bounds on the secrecy capacity. We further show that these two bounds match for the degraded compound wire-tap channel and we hence obtain the secrecy capacity for this channel. The lower bound (achievable secrecy rate) has the worst-case interpretation, i.e., it is limited by the secrecy rate of the destination-wire-tapper pair when the destination has the worst channel state and the wire-tapper has the best channel state. However, since the source input scheme needs to balance the rates of all channel states, none of the channel states may achieve its best secrecy rate. We further illustrate these results by using parallel Gaussian wire-tap channels and multi-antenna compound wire-tap channels.

For the parallel Gaussian compound wire-tap channels, we assume there is one destination and there are multiple wire-tappers. The channel from the source to the destination consists of a number of independent subchannels and each wire-tapper may have access to a subset of these subchannels with noisier outputs with respect to the outputs at the destination from the corresponding subchannels. One application of this channel is to wideband wireless communication systems such as FDM communications in which transmission is over a number of frequency bands, and the wire-tappers can tune their receivers to access some of these frequency bands. For the parallel Gaussian compound wire-tap channel, we obtain the secrecy capacity and the characterization of an optimal source power allocation among the subchannels to achieve the secrecy capacity. To further illustrate our results, we study the secrecy degree of freedom ($s.d.o.f.$) which characterizes how the secrecy capacity scales with $\log \mathsf{SNR}$. We show that the $s.d.o.f.$ depends only on the total number of subchannels and the maximal number of subchannels that one wire-tapper can access. It is somewhat interesting that the $s.d.o.f.$ does not depend on the total number of subchannels that all wire-tappers can access, and does not depend on the

The work of Y. Liang and H. V. Poor was supported by the National Science Foundation under Grants ANI-03-38807 and CNS-06-25637. The work of G. Kramer was supported in part by the Board of Trustees of the University of Illinois Subaward no. 04-217 under NSF Grant CCR-0325673 and the Army Research Office under ARO Grant W911NF-06-1-0182. The work of S. Shamai was partly supported by the Israel Science Foundation.

Yingbin Liang and H. Vincent Poor are with the Department of Electrical Engineering, Princeton University, E-Quad, Olden Street, Princeton, NJ 08544, USA {yingbinl,poor}@princeton.edu

Gerhard Kramer is with the Bell Laboratories, Alcatel-Lucent, Murray Hill, NJ 07974, USA gkr@research.bell-labs.com

Shlomo Shamai (Shitz) is with the Department of Electrical Engineering, Technion-Israel Institute of Technology, Technion City, Haifa 32000, Israel sshlomo@ee.technion.ac.il

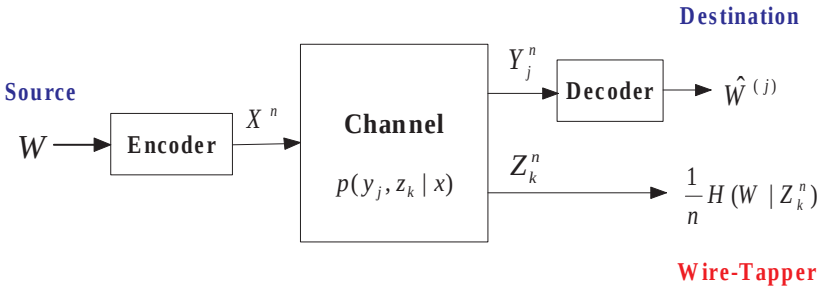

Fig. 1. Compound wire-tap channel

number of wire-tappers either. We observe that there is a connection between the *s.d.o.f.* and secure network coding studied in [6]. However, the *s.d.o.f.* is defined for noisy Gaussian channels while secure network coding addresses deterministic networks.

For the multi-input multi-output (MIMO) compound wire-tap channel, we first provide the secrecy capacity for the degraded MIMO compound wire-tap channel. We then study the general MIMO compound wire-tap channel, for which we propose an input scheme and derive an achievable *s.d.o.f.* based on this scheme. Comparing with the MIMO channel without wire-tappers, the *s.d.o.f.* of the MIMO compound wire-tap channel is reduced by the maximal dimension of the projection of wire-tap channel matrices on the vector space spanned by the eigenvectors corresponding to nonzero eigenvalues of channel matrices to the destination. We further illustrate our result by an example channel which can be changed to an equivalent parallel Gaussian compound channel with a precoding scheme and the *s.d.o.f.* can hence be achieved with the scheme that we provide for the corresponding parallel Gaussian compound channel.

The paper is organized as follows. In Section II, we introduce the model of the compound wire-tap channel. In Section III, we present our results on the discrete memoryless compound wire-tap channel. In Section IV, we provide the results on the secrecy capacity and the *s.d.o.f.* for the parallel Gaussian compound wire-tap channel. In Section V, we provide our results on the MIMO compound wire-tap channel. In the last section, we give concluding remarks.

II. Channel Model

We consider the following compound wire-tap channel model.

***Definition** 1:* A discrete memoryless compound wire-tap channel consists of one finite channel input alphabet $\mathcal{X}$, J finite channel output alphabets $\mathcal{Y}_1, \ldots, \mathcal{Y}_J$, K finite channel output alphabets $\mathcal{Z}_1, \ldots, \mathcal{Z}_K$, and a set of the transition probability distributions

$$p(y_j, z_k|x) \quad \text{for } j = 1, \ldots, J; \text{ and } k = 1, \ldots, K \tag{1}$$

where $x \in \mathcal{X}$ is the channel input from the source, $y_j \in \mathcal{Y}_j$ is one of the possible channel outputs at the destination, and $z_k \in \mathcal{Z}_k$ is one of the possible channel outputs at the wire-tapper.

We note that the channel transition probability distributions are indexed by (j, k) pairs for $j = 1, \ldots, J$ and $k = 1, \ldots, K$, and the channel can be in one of these JK states. We assume that the channel remains in the same state during the entire transmission. We further assume that the channel state is known at the corresponding receivers, but is not known at the transmitter. However, we note that having the channel state information at the receivers comes at no cost in this time-invariant channel model. No matter which state occurs, the source node wants to transmit information at a certain rate to the destination and wishes to keep the information secret from the wire-tapper.

***Definition** 2:* A $\left(2^{nR}, n\right)$ code for the compound wire-tap channel consists of the following:

- A message set: $\mathcal{W} = \{1, 2, \ldots, 2^{nR}\}$ with the message W uniformly distributed over $\mathcal{W}$;
- An encoder: $\mathcal{W} \to \mathcal{X}^n$, which maps each message $w \in \mathcal{W}$ to a codeword $x^n \in \mathcal{X}^n$;
- J decoders, f_j: $\mathcal{Y}_j^n \to \mathcal{W}^{(j)}$, each of which maps a received sequence y_j^n to a message $\hat{w}^{(j)} \in \mathcal{W}$ for $j = 1, \ldots, J$.

The error probability when the channel state to the destination is j and the message w is sent is defined as

$$P_{e,j}(w) = Pr\left\{\hat{w}^{(j)} \neq w\right\} \tag{2}$$

and the average block error probability when the channel state to the destination is j is

$$P_{e,j} = \frac{1}{2^{nR}} \sum_{w=1}^{2^{nR}} P_{e,j}(w). \tag{3}$$

The secrecy level of the message W at the wire-tapper when the channel state to the wire-tapper is k is defined by the following equivocation rate:

$$\frac{1}{n} H(W|Z_k^n). \tag{4}$$

A rate-equivocation pair (R, R_e) is *achievable* if there exists a sequence of $\left(2^{nR}, n\right)$ codes with the average error probabilities

$$P_{e,j}^{(n)} \to 0 \quad \text{for } j = 1, \ldots, J$$

as n goes to infinity and with the equivocation rate satisfying

$$R_e \leq \lim_{n\to\infty} \frac{1}{n} H(W|Z_k^n) \quad \text{for } k = 1, \ldots, K.$$

In this paper, we are interested in the case of perfect secrecy, i.e., $R = R_e$. A secrecy rate R is *achievable* if the rate-equivocation pair (R, R) is achievable. The *secrecy capacity* is defined to be the maximum achievable secrecy rate.

***Remark** 1:* The compound wire-tap channel can also be interpreted as a wire-tap channel with multiple destinations and multiple wire-tappers, where each Y_j corresponds to the output at one destination and each Z_k corresponds to the output at one wire-tapper. The source wants to transmit the same message to all the destinations and needs to keep this message secret from all wire-tappers. We refer to this system as *multicast with multiple wire-tappers*.

III. Discrete Memoryless Compound Wire-tap Channels

In the following, we provide lower and upper bounds on the secrecy capacity of the compound wire-tap channel.

***Theorem** 1:* The following secrecy rate is achievable for the compound wire-tap channel:

$$\begin{aligned} R &= \max \Big[\min_j I(U;Y_j) - \max_k I(U;Z_k) \Big] \\ &= \max \min_{j,k} \Big[I(U;Y_j) - I(U;Z_k) \Big] \end{aligned} \tag{5}$$

where the maximum is over all distributions $p(u, x)$ that satisfy the Markov chain relationships:

$$U \to X \to (Y_j, Z_k) \text{ for } j = 1, \ldots, J \text{ and } k = 1, \ldots, K.$$

Theorem 1 can be interpreted as a worst case result, because the secrecy rate should be achievable no matter which channel state occurs. If we view the system as a multicast with multiple wire-tappers, the worst destination and the best wire-tapper dominate the secrecy rate. The details of the proof are omitted due to the space limitations.

Proof: (outline) We first show that there exists a codebook that consists of a number of subcodebooks (similar to [1]). Each destination can successfully decode over the entire codebook, but all wire-tappers can successfully decode only within each subcodebook. Hence the source maps messages to different subcodebooks to confuse the wire-tapper and achieve perfect secrecy. The encoding scheme and equivocation rate computation are similar to those given in [7]. ■

***Theorem** 2:* An upper bound on the secrecy capacity of the compound wire-tap channel is given by

$$\bar{R} = \min_{j,k} \max_{p(u,x)p(y_j,z_k|x)} \Big[I(U;Y_j) - I(U;Z_k) \Big]. \tag{6}$$

Proof: It can be seen that

$$\max_{p(u,x)p(y_j,z_k|x)} \Big[I(U;Y_j) - I(U;Z_k) \Big]$$

in (6) is the secrecy capacity of the wire-tap channel with the transition probability distribution $p(y_j, z_k|x)$ [8, Corollary 2]. But the secrecy capacity of the compound wire-tap channel is less than the secrecy capacity of any of the possible channel states. ■

We note that it may not be possible to achieve the upper bound given in Theorem 2 in general. This is because the input scheme needs to balance the rates that can be achieved for all channel states, and consequently, none of the channel states can achieve its best rate. This can also be seen from the achievable rate in (5). The input distribution $p(u, x)$ that maximizes the minimum of the secrecy rates of all channel states may not be optimal for any single state.

We next give an example channel in which the lower bound given in Theorem 1 can be shown to be the secrecy capacity. We say that the compound wire-tap channel is *degraded* if the transition probability satisfies the Markov chain relationships:

$$X \to Y_j \to Z_k \tag{7}$$

for all $j = 1, \ldots, J$ and $k = 1, \ldots, K$. For the degraded compound wire-tap channel, we have the following capacity theorem.

***Theorem** 3:* The secrecy capacity of the degraded compound wire-tap channel is given by

$$\begin{aligned} C &= \max_{p(x)} \Big[\min_j I(X;Y_j) - \max_k I(X;Z_k) \Big] \\ &= \max_{p(x)} \min_{j,k} \Big[I(X;Y_j) - I(X;Z_k) \Big]. \end{aligned} \tag{8}$$

Proof: The achievability follows from Theorem 1 by setting $U = X$. The converse follows because for each channel state (j, k) and an input distribution $p(x)$, an upper bound

$$R_e \leq I(X;Y_j) - I(X;Z_k) \tag{9}$$

can be derived as given in [1]. ■

IV. Parallel Gaussian Compound Wire-tap Channels

In this section, we view the compound wire-tap channel as multicast with multiple wire-tappers (see Fig. 2). We focus on the case in which $J = 1$ and $K > 1$, i.e., one destination and K wire-tappers. We further assume that the channel from the source to the destination is the parallel Gaussian channel with N independent subchannels, and the outputs of the subchannels at the destination are given by

$$Y_a = X_a + W_a, \qquad \text{for} \qquad a = 1, \ldots, N, \tag{10}$$

where $W_1, \ldots, W_a$ are independent Gaussian random variables with variances $w_1^2, \ldots, w_a^2$. We note that for this model, $Y_1, \ldots, Y_N$ indicate the outputs at the destination from the N subchannels, and do not indicate the outputs corresponding to different channel states or different destinations. The source input is subject to the average power constraint P, i.e.,

$$\frac{1}{n} \sum_{i=1}^{n} \sum_{a=1}^{N} \mathrm{E}\Big[X_{ai}^2\Big] \leq P, \tag{11}$$

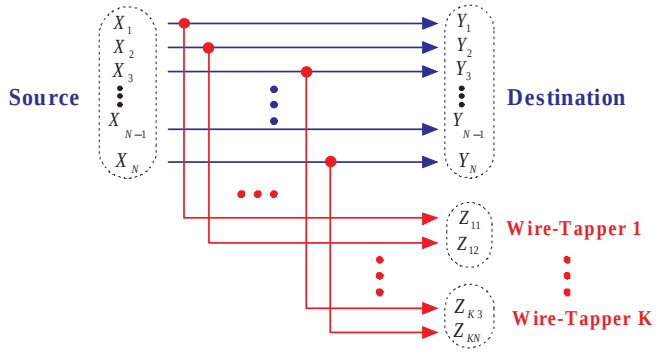

Fig. 2. Parallel compound wire-tap channel with one destination and K wire-tappers

where i is the symbol time index. We assume that each wire-tapper can access some subchannels. On letting $\mathcal{A}_k \subseteq \{1,\ldots,N\}$ include all indices of the subchannels that wire-tapper k can access, the outputs at wire-tapper k are given by

$$Z_{ka} = X_a + V_{ka}, \qquad \text{for} \qquad a \in \mathcal{A}_k \tag{12}$$

where V_{ka} for $a \in \mathcal{A}_k$ are independent Gaussian random variables with variances v_{ka}^2. We further assume that $v_{ka}^2 \geq w_a^2$ for all $a \in \mathcal{A}_k$.

For the parallel Gaussian compound wire-tap channel, we have the following secrecy capacity.

***Theorem** 4:* The secrecy capacity of the parallel Gaussian compound wire-tap channel is given by

$$C = \max_{\sum_{a=1}^N P_a \leq P} \min_k \left[\sum_{a=1}^N \frac{1}{2}\log\left(1+\frac{P_a}{w_a^2}\right) - \sum_{a\in\mathcal{A}_k}\frac{1}{2}\log\left(1+\frac{P_a}{v_{ka}^2}\right)\right]. \tag{13}$$

Proof: The achievability follows from Theorem 1 by choosing independent $X_1,\ldots,X_a$ with each $X_a \in \mathcal{N}(0,P_a)$. The converse follows from [9, Theorem 2] by setting $R_0 = 0$ for each wire-tapper. ■

To obtain the secrecy capacity of the parallel Gaussian compound wire-tap channel, we need to solve the "max-min" optimization problem in (13), i.e., we need to derive the optimal power allocation. We use $\underline{P} = (P_1,\ldots,P_N)$ to indicate a source power allocation among N subchannels where each component indicates the power allocated for the corresponding subchannel. The following theorem characterizes the optimal power allocation.

***Theorem** 5:* The power allocation $\underline{P}^*$ that maximizes (13) and hence achieves the secrecy capacity for the parallel Gaussian compound wire-tap channel satisfies the following necessary and sufficient condition. For some

$$\mathcal{B} = \{b_1,\ldots,b_m\} \subseteq \{1,\ldots,K\},$$

$\underline{P}^*$ maximizes

$$R_{b_1}(\underline{P}) = R_{b_2}(\underline{P}) = \cdots = R_{b_m}(\underline{P})$$

and

$$R_{b_1}(\underline{P}^*) < R_k(\underline{P}^*) \text{ for all } k \in \mathcal{B}^c,$$

where

$$R_k = \sum_{a=1}^N \frac{1}{2}\log\left(1+\frac{P_a}{w_a^2}\right) - \sum_{a\in\mathcal{A}_k}\frac{1}{2}\log\left(1+\frac{P_a}{v_{ka}^2}\right)$$

for $k = 1,\ldots,K$. Hence the optimal power allocation $\underline{P}^*$ can be obtained by searching over all sets $\mathcal{B}$ to find the one that satisfies the above conditions.

Proof: The proof is similar to the argument in [9, Lemma 2]. ■

We note that the parallel Gaussian compound wire-tap channel is a more general model than the model in [3] in that the number of wire-tappers is arbitrary, each wire-tapper may access an arbitrary number of subchannels, and the source is allowed to allocate power among the subchannels to achieve better secrecy rate. We also note that the parallel Gaussian compound wire-tap channel reduces to the Gaussian/fading wire-tap channel with multiple wire-tappers studied in [4] if there is only one subchannel.

To gain more insight into the secrecy capacity, we consider the rate at which the secrecy capacity scales with $\log \mathsf{SNR}$. In particular, we define the secrecy degree of freedom (s.d.o.f.) as

$$s.d.o.f. = \lim_{\mathsf{SNR}\to\infty} \frac{C(\mathsf{SNR})}{\frac{1}{2}\log \mathsf{SNR}} \tag{14}$$

where without loss of generality, we choose w_1^2 as the reference noise level and define $\mathsf{SNR} = \frac{P}{Nw_1^2}$.

***Corollary** 1:* Assume the maximum number of subchannels that one wire-tapper can access is L. The secrecy degree of freedom of the parallel Gaussian compound wire-tap channel is given by

$$s.d.o.f. = N - L. \tag{15}$$

Proof: The achievability follows by applying Theorem 4 and choosing $P_a = P/N$ for $a = 1,\ldots,N$. The converse follows by considering only the wire-tapper k that accesses L subchannels, i.e., $|\mathcal{A}_k| = L$. Then

$$\begin{aligned} C &= \max_{\sum_{a=1}^N P_a \leq P} \left\{ \sum_{a\notin\mathcal{A}_k} \frac{1}{2}\log\left(1+\frac{P_a}{w_a^2}\right) \right. \\ &\qquad \left. + \sum_{a\in\mathcal{A}_k}\left[\frac{1}{2}\log\left(1+\frac{P_a}{w_a^2}\right) - \frac{1}{2}\log\left(1+\frac{P_a}{v_{ka}^2}\right)\right]\right\} \\ &\leq \sum_{a\notin\mathcal{A}_k}\frac{1}{2}\log\left(1+\frac{P}{w_a^2}\right) \\ &\qquad + \sum_{a\in\mathcal{A}_k}\left[\frac{1}{2}\log\left(1+\frac{P}{w_a^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{v_{ka}^2}\right)\right] \\ &= \frac{|\mathcal{A}_k^c|}{2}\log \mathsf{SNR} + o(\log \mathsf{SNR}) \end{aligned} \tag{16}$$

where the last inequality follows because each term in the summand is an increasing function of P_a, and

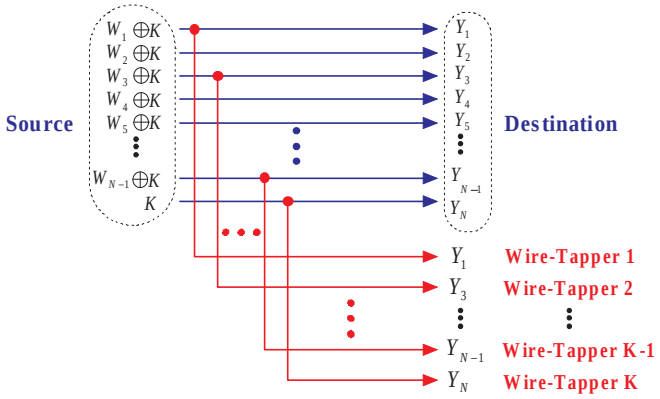

Fig. 3. Example 1

$o(\log \mathsf{SNR})/\log \mathsf{SNR} \to 0$ as $\mathsf{SNR} \to \infty$. Hence we obtain

$$s.d.o.f. = |\mathcal{A}_k^c| = N - L. \tag{17}$$

■

***Remark** 2:* The $s.d.o.f.$ depends only on the maximum number of subchannels that one wire-tapper can access, and does not depend on the total number of subchannels that all wire-tappers access. This is because the wire-tappers do not cooperate with each other. This implies that, even if every subchannel is accessed by some wire-tapper, positive $s.d.o.f.$ is still possible if none of the wire-tappers accesses a full set of the subchannels. This can also be seen from the following examples.

***Remark** 3:* The $s.d.o.f.$ does not depend on the number of wire-tappers.

We note that the $s.d.o.f.$ in Corollary 1 is similar to the secure rate given in [6, Theorem 2] for multicast networks based on network coding. However, we note that Corollary 1 is applicable for noisy Gaussian channels while the secure rate given in [6, Theorem 2] is derived for deterministic networks.

We now illustrate some examples for which simple schemes that achieves $s.d.o.f.$ can be easily constructed. For general parallel Gaussian compound wire-tap channels, the scheme given in [6] may be applied to achieve $s.d.o.f.$ based on linear code multicast over a finite field.

In the following examples, we consider the parallel Gaussian compound wire-tap channel, where the noise terms of all subchannels have the same variance w^2. Hence, $\mathsf{SNR} = P/(Nw^2)$. We assume that if a wire-tapper accesses one subchannel, it receives the same output from this subchannel as the destination. Based on these assumptions, we consider the following examples.

***Example** 1:* Each wire-tapper can access only one subchannel (see Fig. 3).

It follows from Corollary 1 that $s.d.o.f. = N - 1$ for Example 1. We now give a simple scheme to achieve it. We allocate the source power equally for all subchannels. Each subchannel can hence support the following rate

$$R = \frac{1}{2}\log\left(1 + \mathsf{SNR}\right). \tag{18}$$

TABLE I

MESSAGES TRANSMITTED OVER TWO TIME SLOTS FOR EXAMPLE 2

	time 1	time 2
subchannel 1	$X_{11} = W_1 \oplus K_1 \oplus K_2$	$X_{12} = K_3$
subchannel 2	$X_{21} = W_2 \oplus K_2 \oplus K_3$	$X_{22} = K_4$
subchannel 3	$X_{31} = W_3 \oplus K_3 \oplus K_4$	$X_{32} = K_1$
subchannel 4	$X_{41} = W_4 \oplus K_4 \oplus K_1$	$X_{42} = K_2$

We let the source message be $W = (W_1, \ldots, W_{N-1})$, where $W_1, \ldots, W_{N-1}$ are i.i.d. and uniformly distributed over the set $\{0, \ldots, 2^{nR}-1\}$. We also generate a key random variable K that is independent of $W_1, \ldots, W_{N-1}$, and is also uniformly distributed over the set $\{0, \ldots, 2^{nR}-1\}$. Define the operation $\oplus$ to be "addition modulo 2^{nR}". We transmit $W_1 \oplus K, \ldots, W_{N-1} \oplus K$ over the first $N-1$ subchannels, respectively, using a capacity achieving code for each subchannel, and transmit K over the Nth subchannel. It is clear that the destination can decode $W_1 \oplus K, \ldots, W_{N-1} \oplus K$ and K, and hence can decode $W_1, \ldots, W_{N-1}$. For each wire-tapper, if it accesses the Nth channel, it decodes only K and does not know any information about $W_1, \ldots, W_{N-1}$. If the wire-tapper accesses one of the first $N-1$ subchannels, it decodes only $W_i \oplus K$ which is independent of W_i, and does not get any information about $W_1, \ldots, W_{N-1}$. Hence, $W = (W_1, \ldots, W_{N-1})$ can be transmitted to the destination at the rate $(N-1)R$ with perfect secrecy, and $s.d.o.f. = N - 1$.

***Example** 2:* The parallel channel consists of four subchannels, and each wire-tapper can access at most two subchannels.

It follows from Corollary 1 that the $s.d.o.f. = 2$ for Example 2. To achieve the $s.d.o.f.$ in this case, we need to use two time slots. We let $W = (W_1, W_2, W_3, W_4)$ indicate the source message with each component uniformly distributed over the set $\{0, \ldots, 2^{nR}-1\}$, where R is given in (18). We generate four key random variables K_1, K_2, K_3, K_4 that are i.i.d. and uniformly distributed over the set $\{0, \ldots, 2^{nR}-1\}$, and are independent of W. The transmission scheme over two time slots is shown in Table I.

It can be shown that no wire-tapper can get any information about any component of the message W by accessing only two subchannels. Therefore, the message $W = (W_1, W_2, W_3, W_4)$ can be transmitted to the destination at the average rate of $2R$ with perfect secrecy, and the $s.d.o.f. = 2$.

V. MIMO COMPOUND WIRE-TAP CHANNELS

In this section, we view the compound wire-tap channel as a multicast transmission to J destinations with K wire-tappers. Furthermore, we assume that the source, the destinations, and the wire-tappers are equipped with multiple antennas, and study how multiple antennas affect the secrecy capacity.

We let N_s indicate the number of transmit antennas of the source, N_d indicate the number of receive antennas of the destinations, and N_w indicate the number of receive antennas of the wire-tappers. We note that although we assume all destinations have the same number of antennas and all wire-tappers have the same number of antennas, our analysis below is also applicable without this assumption. The channel input-output relationship at one time instant is given by

$$\begin{array}{lll} \underline{Y}_j = H_j \underline{X} + \underline{W}_j & \text{for} & j = 1, \ldots, J; \\ \underline{Z}_k = G_k \underline{X} + \underline{V}_k & \text{for} & k = 1, \ldots, K; \end{array} \tag{19}$$

where H_j for $j = 1, \ldots, J$ and G_k for $k = 1, \ldots, K$ are fixed matrices, and $\underline{W}_1, \ldots, \underline{W}_J$ and $\underline{V}_1, \ldots, \underline{V}_K$ are i.i.d. Gaussian random vectors with identity variance matrices. We assume that the source input is subject to an average power constraint

$$\frac{1}{n} \sum_{i=1}^{n} \mathrm{E}\left[\underline{X}_i^T \underline{X}_i\right] \leq P \tag{20}$$

where i is the symbol time index.

In the following, we first study the degraded MIMO compound wire-tap channel, and then study the general MIMO compound wire-tap channel. We use the following notations associated with matrices. We use $A \succeq 0$ to indicate that A is a positive semidefinite matrix, $A \succ 0$ to indicate A is a positive definite matrix, and $A \succeq B$ to indicate that $A - B$ is a positive semidefinite matrix. The symbols $\preceq$ and $\prec$ indicate the oppositive meanings to those of $\succeq$ and $\succ$, respectively.

A. Degraded MIMO Compound Wire-tap Channels

As in [10], we define the MIMO compound wire-tap channel to be *degraded* if for each (j, k) pair, there exists a matrix D_{jk} such that $D_{jk} H_j = G_k$ and $D_{jk} D_{jk}^T \preceq I$. It is easy to check that for each (j, k) pair, the channel satisfies the Markov chain relationship $\underline{X} \rightarrow \underline{Y}_j \rightarrow \underline{Z}_k$.

***Theorem** 6:* The secrecy capacity of the degraded MIMO compound wire-tap channel is given by:

$$C = \max_{Q:\, Q \succeq 0,\, Tr(Q) \leq P} \min_{j,k} \frac{1}{2} \log \frac{|I + H_j Q H_j^T|}{|I + G_k Q G_k^T|} \tag{21}$$

Proof: (outline) We need only to show that the secrecy capacity is given by

$$\min_{j,k} \frac{1}{2} \log \frac{|I + H_j Q H_j^\intercal|}{|I + G_k Q G_k^\intercal|} \tag{22}$$

if the input is subject to the following covariance matrix constraint

$$\frac{1}{n} \sum_{i=1}^{n} K_{\underline{X}_i} \preceq Q. \tag{23}$$

where $K_{\underline{X}_i}$ indicates the covariance matrix of $\underline{X}_i$ at symbol time i. Theorem 6 then follows by maximizing (22) over all Q that satisfy the power constraint, i.e., $Tr(Q) \leq P$.

The achievability follows from Theorem 3 by choosing $X \sim \mathcal{N}(0, Q)$. To show the converse, we first have the following bound for any (j, k) pair by referring to [11, Sec. III]:

$$R_e \leq \frac{1}{n} \sum_{i=1}^{n} I(\underline{X}_i; \underline{Y}_{j,i} | \underline{Z}_{k,i}). \tag{24}$$

It can be shown that Gaussian $\underline{X}_i$ maximizes the preceding bound if the covariance matrix of $\underline{X}_i$ is fixed to be $K_{\underline{X}_i}$. Therefore, we have the following bound

$$\begin{aligned} R_e &\leq \frac{1}{n} \sum_{i=1}^{n} \frac{1}{2} \log \frac{|I + H K_{\underline{x}_i} H^T|}{|I + G K_{\underline{x}_i} G^T|} \\ &\overset{(a)}{\leq} \frac{1}{2} \log \frac{|I + H \left(\frac{1}{n} \sum_{i=1}^{n} K_{\underline{x}_i}\right) H^T|}{|I + G \left(\frac{1}{n} \sum_{i=1}^{n} K_{\underline{x}_i}\right) G^T|} \\ &\overset{(b)}{\leq} \frac{1}{2} \log \frac{|I + H Q H^T|}{|I + G Q G^T|} \end{aligned} \tag{25}$$

where (a) and (b) follow from the degradedness assumption, the constraint (23), and some matrix properties. ■

B. General MIMO Compound Wire-tap Channels

In this subsection, we study the general MIMO compound wire-tap channel defined in (19), where we do not make the the degradedness assumption.

Based on Theorem 1 by choosing $U = X \sim \mathcal{N}(0, Q)$, it is easy to see that the following secrecy rate is achievable.

***Lemma** 1:* For the general MIMO compound wire-tap channel, an achievable secrecy rate is given by

$$R = \max_{Q:Q \succeq 0, Tr(Q) \leq P} \min_{j,k} \frac{1}{2} \log \frac{|I + H_j Q H_j^T|}{|I + G_k Q G_k^T|}. \tag{26}$$

In general, the maximization problem in (26) is difficult to solve. To gain some insight, we study the $s.d.o.f.$ defined as in (14), but with $\mathsf{SNR} = P/N_s$.

We let $r = \mathrm{Rank}\left(\sum_{j=1}^{J} H_j^T H_j\right)$, and $\{\underline{u}_1, \ldots, \underline{u}_r\}$ be the eigenvectors of $\sum_{j=1}^{J} H_j^T H_j$ that correspond to nonzero eigenvalues. In fact, if we let $\{\underline{u}_{j1}, \ldots, \underline{u}_{jr_j}\}$ be the eigenvectors of $H_j^T H_j$ that correspond to nonzero eigenvalues, then $(\underline{u}_{j1}, \ldots, \underline{u}_{jr_j})$ for $j = 1, \ldots, J$ together span the same vector space as $\{\underline{u}_1, \ldots, \underline{u}_r\}$.

We let $\{\underline{u}_{r+1}, \ldots, \underline{u}_{N_s}\}$ be the eigenvectors of $\sum_{j=1}^{J} H_j^T H_j$ that correspond to zero eigenvalues. We further let

$$U = [\underline{u}_1 \cdots \underline{u}_r] \quad \text{and} \quad U^\perp = \left[\underline{u}_{r+1} \cdots \underline{u}_{N_s}\right]. \tag{27}$$

Then

$$\sum_{j=1}^{J} H_j^T H_j = \begin{bmatrix} U & U^\perp \end{bmatrix} \begin{bmatrix} \Lambda_r & \\ & 0_{N_s - r} \end{bmatrix} \begin{bmatrix} U^T \\ (U^\perp)^T \end{bmatrix} \tag{28}$$

where Λ_r denotes the diagonal matrix with the eigenvalues of $\sum_{j=1}^{J} H_j^T H_j$ as the diagonal components, and $0_{N_s - r}$ denotes the all-zero matrix with dimension $(N_s - r) \times (N_s - r)$.

We now let $\mathcal{L}$ be a subset of $\{1, 2, \ldots, r\}$, and assume $\mathcal{L} = \{l_1, \ldots, l_{|\mathcal{L}|}\}$ where $|\mathcal{L}|$ indicates the number of components in the set $\mathcal{L}$. We then let $\mathcal{L}^c$ denote the complement of

$\mathcal{L}$ with respect to the set $\{1, 2, \ldots, r\}$, and assume $\mathcal{L}^c = \{l'_1, \ldots, l'_{r-|\mathcal{L}|}\}$. Let

$$U_{\mathcal{L}} = \left[\underline{u}_{l_1} \cdots \underline{u}_{l_{|\mathcal{L}|}}\right] \quad \text{and} \quad U_{\mathcal{L}^c} = \left[\underline{u}_{l'_1} \cdots \underline{u}_{l'_{r-|\mathcal{L}|}}\right]. \quad (29)$$

Finally, we let

$$Q_{\mathcal{L}} = \frac{P}{|\mathcal{L}|}\left[U_{\mathcal{L}} \;\; U_{\mathcal{L}^c} \;\; U^{\perp}\right] \begin{bmatrix} I_{|\mathcal{L}|} & & \\ & 0 & \\ & & 0 \end{bmatrix} \begin{bmatrix} U_{\mathcal{L}}^T \\ U_{\mathcal{L}^c}^T \\ (U^{\perp})^T \end{bmatrix} \quad (30)$$

and obtain

$$\begin{aligned} \left|I + H_j Q_{\mathcal{L}} H_j^T\right| &= \left|I + \frac{P}{|\mathcal{L}|}(H_j U_{\mathcal{L}})^T (H_j U_{\mathcal{L}})\right| \\ \left|I + G_k Q_{\mathcal{L}} G_k^T\right| &= \left|I + \frac{P}{|\mathcal{L}|}(G_k U_{\mathcal{L}})^T (G_k U_{\mathcal{L}})\right|. \end{aligned} \quad (31)$$

Hence

$$\lim_{\mathsf{SNR}\to\infty} \frac{\frac{1}{2}\log\frac{|I+H_jQH_j^T|}{|I+G_kQG_k^T|}}{\frac{1}{2}\log \mathsf{SNR}} = \mathrm{Rank}(H_jU_{\mathcal{L}}) - \mathrm{Rank}(G_kU_{\mathcal{L}}) \quad (32)$$

Therefore, we have the following theorem.

***Theorem** 7:* An achievable secrecy degree of freedom of the MIMO compound wire-tap channel is given by

$$s.d.o.f. \geq \max_{\mathcal{L}} \min_{j,k} \left\{\mathrm{Rank}(H_jU_{\mathcal{L}}) - \mathrm{Rank}(G_kU_{\mathcal{L}})\right\} \quad (33)$$

From the choice of the input covariance matrix Q in (30), we note that the beamforming directions of the channel inputs are chosen to be along the eigenvectors of $\sum_{j=1}^{J} H_j^T H_j$ that correspond to nonzero eigenvalues. Each set $\mathcal{L}$ indicates the directions for which the source allocates the power, and hence corresponds to one power allocation strategy. The optimal achievable $s.d.o.f.$ can be obtained by searching over all power allocation strategies. We note that $\mathrm{Rank}(H_jU_{\mathcal{L}})$ and $\mathrm{Rank}(G_kU_{\mathcal{L}})$ in (33) can be interpreted as the dimensions of the projections of H_j and G_k, respectively, onto the vector space spanned by the column vectors of $U_{\mathcal{L}}$. Hence the achievable $s.d.o.f.$ is determined by the geometry of the channel matrices to the destinations and wire-tappers.

For the special case when $J = 1$, i.e., only one destination, and so the channel matrix to the destination is H, r becomes the rank of H^TH and hence the rank of H. We should always choose $\mathcal{L} = \{1, \ldots, r\}$, and the resulting $s.d.o.f.$ is given in the following corollary to Theorem 7.

***Corollary** 2:* For the MIMO compound wire-tap channel with $J = 1$, an achievable secrecy degree of freedom is given by

$$s.d.o.f. \geq \min_{k} \left\{\mathrm{Rank}(H) - \mathrm{Rank}(G_kU)\right\} \quad (34)$$

where U is the matrix whose columns are the eigenvectors of H^TH corresponding to nonzero eigenvalues.

We now consider an example.

***Example** 3:* Consider the MIMO compound wire-tap channel where $J = 1$ and $K > 1$. We assume the source and the destination have M antennas, and each wire-tapper has one antenna. We further assume $K \leq M$. We assume that the channel matrix H to the destination is of full rank, and the channel vectors $\underline{g}_k^T$ for $k = 1, \ldots, K$ to the wire-tappers are linearly independent.

From Corollary 2, it is clear that an achievable $s.d.o.f.$ is equal to M-1, because H is of full rank and $\mathrm{Rank}(\underline{g}_k^T U) = 1$.

We now show how we can achieve this degree of freedom. We first consider the case when $K = M$. Let

$$G = \begin{bmatrix} \underline{g}_1^T \\ \cdots \\ \underline{g}_M^T \end{bmatrix}. \quad (35)$$

Note that G is of full rank due to the assumptions, and is hence invertible.

We first do a precoding for channel input and let $\underline{X} = G^{-1}\underline{U}$. The channel hence becomes

$$\begin{aligned} \underline{Y} &= HG^{-1}\underline{U} + \underline{W} \\ \begin{bmatrix} Z_1 \\ \cdots \\ Z_M \end{bmatrix} &= G\underline{X} + \underline{V} = \underline{U} + \underline{V}. \end{aligned} \quad (36)$$

We now let $\underline{Y}' = GH^{-1}\underline{Y}$ and obtain the following equivalent channel

$$\begin{aligned} \underline{Y}' &= \underline{U} + \underline{W}' \\ \begin{bmatrix} Z_1 \\ \cdots \\ Z_M \end{bmatrix} &= \underline{U} + \underline{V}. \end{aligned} \quad (37)$$

We now have an equivalent channel which is a parallel Gaussian compound wire-tap channel with M subchannels in which each wire-tapper has access to one subchannel. It is easy to see that each subchannel can support one degree of freedom. Hence we can use a scheme similar to that in Example 1 and achieve $s.d.o.f. = M - 1$.

If the number of wire-tappers is $K < M$, we can artificially add $M - K$ wire-tappers such that the resulting G matrix is of full rank. In this way, we may only lose $s.d.o.f.$. However, we can use the same scheme as above and still achieve $s.d.o.f. = M - 1$.

VI. Conclusions

In this paper, we have studied the compound wire-tap channel, which provides a general framework for examining multicast communication with multiple wire-tappers. We have obtained lower and upper bounds on the secrecy capacity for the general compound wire-tap channel and have established the secrecy capacity for the degraded channel. We have further obtained the secrecy capacity for the parallel Gaussian and degraded MIMO compound wire-tap channels. The secrecy rate/capacity in general has a worst-case interpretation.

We have also introduced the notion of the secrecy degree of freedom, which captures the most important factors that affect the scaling behavior of the secrecy rate at high SNR. For the parallel Gaussian compound channel, we have demonstrated that the $s.d.o.f.$ depends only on the maximum number of subchannels that one wire-tapper can access, and does not depend on the number of wire-tappers. For the MIMO compound wire-tap channel, we have shown that the

achievable $s.d.o.f.$ is determined by the geometries of the matrices describing the channels to the destinations and wire-tappers. We have also demonstrated that there are simple schemes to achieve the $s.d.o.f.$ in many cases via a few example channels.

REFERENCES

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

[2] H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Trans. Inform. Theory*, vol. 35, no. 3, pp. 572–578, May 1989.

[3] ——, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 634–638, May 1991.

[4] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 2007.

[5] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting," submitted to *IEEE Trans. Inform. Theory*, Feb. 2007.

[6] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Lausanne, Switzerland, Jun./Jul. 2002, also see the extension of the abstract at http://personal.ie.cuhk.edu.hk/∼ITIP/ISIT02/secure.ps.

[7] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," submitted to *IEEE Trans. Inform. Theory*, April 2006; available at http://www.arxiv.org/PS_cache/cs/pdf/0605/0605014.pdf.

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

[9] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," submitted to *IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, Nov 2006; available at http://arxiv.org/PS_cache/cs/pdf/0701/0701024v1.pdf.

[10] H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, and P. Viswanath, "The capacity region of the degraded MIMO compound broadcast channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 2007.

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