The Gaussian Diamond-Wiretap Channel with Rate-Limited Relay Cooperation

Author 1 and Author 2

***Abstract*—In this letter, we establish the secure degrees-of-freedom (d.o.f.) of the Gaussian diamond-wiretap channel with rate-limited relay cooperation, where the eavesdropper not only observes the relay transmission through another multiple access channel but also wiretaps some of communication links among relays. The legitimate parties do not know the location of wiretapped relay links nor the eavesdropper's channel state information (CSI). As an optimal relay cooperation strategy, a noise-forwarding scheme that does not incorporate secure network coding is adopted. Furthermore, we briefly outline how the scheme can be extended to incorporate the case when the source-relay links are also wiretapped.**

I. Introduction

Multi-cell processing is a promising technique to drastically enhance the data rates for cellular networks [1], [2]. In this technique, the base stations cooperate by rate-limited backbone links connected to a central processor and/or among themselves. This scenario can be modeled as the Gaussian diamond channel with rate-limited relay cooperation where the source is connected with finite-rate links to multiple relays and the relays further set up cooperation through finite-rate links among them for transmission to the destination over the Gaussian multiple access channel.

In this letter, we consider such a model in a secrecy setting [3], where an external eavesdropper wiretaps some of links among relays and also the multiple access part through another multiple access channel. We assume a practical scenario where the legitimate parties do not know the location of wiretapped links among relays nor the eavesdropper's CSI. To study the behavior of secrecy capacity in high signal-to-noise ratio (SNR) regime, we investigate the secure d.o.f. of this Gaussian diamond-wiretap channel with rate-limited relay cooperation. For the optimistic case of full CSIT, the secure d.o.f. was established in [4] when there are only two relays. In the absence of eavesdropper's CSI, however, the optimal scheme and the involved secrecy analysis are in general different, see e.g., [5]. On the other hand, if relay cooperation is not allowed in our model, the secure d.o.f. was established in [6]. Very recently, the work of [6] was generalized in [7] to the scenario where the eavesdropper can wiretap some of source-relay links and the legitimate parties do not know the location. To protect information sent through source-relay links, secure network coding [8]-like technique was incorporated by utilizing the nature of wireless networks. As an extension of these prior works, our setting gives rise to the following interesting questions: (i) whether and how the secure network coding-like technique should be incorporated for the relay cooperation and (ii) whether it would be possible to combine with the result of [7] to characterize the secure d.o.f. when the eavesdropper can wiretap both the source-relay links and the relay-relay links to some extent. We address both questions in this letter.

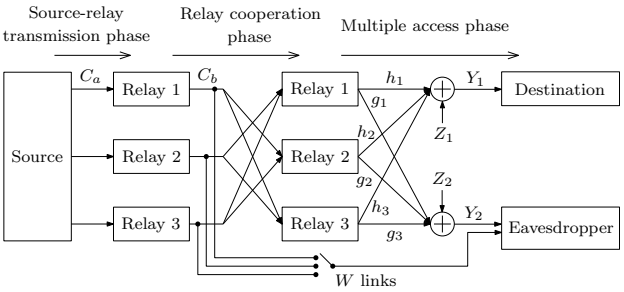

Figure 1. The Gaussian diamond-wiretap channel with rate-limited relay cooperation for $M = 3$.

The following notation is used throughout the paper. For two integers i and j, $[i : j]$ denotes the set $\{i, i+1, \cdots, j\}$. Unif$[S]$ for a set S denotes the uniform distribution over S. When $S = [i : j]$, we use Unif$[i : j]$ instead of Unif$[[i : j]]$. $\lfloor \cdot \rfloor$ denotes the floor function.

II. Model

The Gaussian diamond-wiretap channel with rate-limited relay cooperation consists of a source, M relays, a legitimate destination, and an eavesdropper, which is illustrated in Fig. 1 for $M = 3$. The source can send to M relays through orthogonal links of capacity C_a. Each relay has a broadcast link with capacity C_b connected to all the other relays and the eavesdropper can wiretap up to $W \in [0 : M]$ links among them.[1] For notational convenience, let $L := M - W$. The legitimate parties do not know which links are wiretapped. For the multiple access part, the channel outputs at the legitimate destination and the eavesdropper at time t are given as

$$Y_1(t) = \sum_{k=1}^{M} h_k(t) X_k(t) + Z_1(t) \tag{1}$$

$$Y_2(t) = \sum_{k=1}^{M} g_k(t) X_k(t) + Z_2(t), \tag{2}$$

respectively, where $X_k(t)$ is the channel input from relay k, $h_k(t)$'s and $g_k(t)$'s are the channel fading coefficients, and $Z_1(t)$ and $Z_2(t)$ are additive Gaussian noise with zero mean and unit variance. The average power constraint of P is assumed at each relay. We assume a fast fading scenario where $h_k(t)$'s and $g_k(t)$'s are independent and identically distributed (i.i.d.) over time according to an arbitrary real-valued distribution $f(h_1, \cdots, h_M, g_1, \cdots, g_M)$ satisfying that (i) all joint and conditional distributions are bounded and (ii) there exists a positive finite number J such that $\frac{1}{J} \leq |h_k(t)|, |g_k(t)| \leq J$

[1] In fact, our results hold for a general relay cooperation scenario as described in Remark 2.

for all $k \in [1:M]$. For notational convenience, let $\mathbf{h}(t) = (h_1(t) \ \cdots \ h_M(t))$ and $\mathbf{g}(t) = (g_1(t) \ \cdots \ g_M(t))$ denote the legitimate (user's) CSI and the eavesdropper's CSI at time t, respectively. We assume that the source does not know both the legitimate CSI and the eavesdropper's CSI and the eavesdropper knows both the CSI's. The relays and destination are assumed to know *only* the legitimate CSI.

A $(2^{nR}, n)$ code consists of

- a message $G \sim \text{Unif}[1:2^{nR}]$,
- a stochastic encoder at the source that (randomly) maps $G \in [1:2^{nR}]$ to $(A_1^n, \cdots, A_M^n) \in \mathcal{A}_1^n \times \cdots \times \mathcal{A}_M^n$ such that $\frac{1}{n}H(A_k^n) \le C_a$ for $k \in [1:M]$,
- a stochastic encoder for setting up cooperation at relay $k \in [1:M]$ that (randomly) maps A_k^n to B_k^n such that $\frac{1}{n}H(B_k^n) \le C_b$,
- a stochastic encoder for multiple access part at relay $k \in [1:M]$ at time $t \in [1:n]$ that (randomly) maps $(A_k^n, B_{[1:M]}^n, X_k^{t-1}, \mathbf{h}^t)$ to $X_k(t) \in \mathcal{X}_k$,
- and a decoding function at the destination that (randomly) maps $(Y_1^n, \mathbf{h}^n)$ to $\hat{G} \in [1:2^{nR}]$.

The probability of error is given as $P_e^{(n)} = P(\hat{G} \neq G)$. A secrecy rate of R is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$ and $\lim_{n\to\infty} \frac{1}{n} I(G; B_T^n, Y_2^n | \mathbf{h}^n, \mathbf{g}^n) = 0$ for all $T \subseteq [1:M]$ such that $|T| = W$.

In this letter, we analyze the secure d.o.f. A d.o.f. tuple (α, β, d_s) is said to be achievable if a rate R with $\lim_{P\to\infty} \frac{R}{\frac{1}{2}\log P} = d_s$ is achievable when $\lim_{P\to\infty} \frac{C_a}{\frac{1}{2}\log P} = \alpha$ and $\lim_{P\to\infty} \frac{C_b}{\frac{1}{2}\log P} = \beta$. A secure d.o.f. $d_s(\alpha, \beta)$ is the maximum d_s such that (α, β, d_s) is achievable. According to the context, d_s denotes $d_s(\alpha, \beta)$.

III. Main Result

The following theorem presents the main result of this letter.

Theorem 1. *For the Gaussian diamond-wiretap channel with rate-limited relay cooperation, the secure d.o.f. is equal to*

$$d_s = \min\left\{M\alpha, \frac{M\alpha + L\beta + M - 1}{M+1}, 1\right\}. \tag{3}$$

Proof: The achievability and the converse parts are proved in Sections IV and V, respectively. ∎

Note that the second term in the minimum of (3) corresponds to the penalty term due to secrecy constraint. This term increases as $L\beta$, i.e., the total d.o.f. of securely communicated information among relays, increases and becomes inactive when $L\beta = 1$.

Remark 1. *For channels with constant gains, one can check by closer inspection of our scheme that the RHS of* (3) *is achievable for almost all channel gains. For converse, a key result from [9] used for the upper bound, i.e., the entropy of the channel output at the eavesdropper is at least as large as that at the legitimate destination, does not seem to be immediately generalized to such a channel scenario.*

Remark 2. *Theorem 1 holds when each relay has an orthogonal link with d.o.f. $\frac{\beta}{M-1}$ to each other relay and the eavesdropper wiretaps $(M-1)W$ links among them, illustrated in Fig. 2 for $M = 3$. Converse is obvious because each relay receives less information and there is more freedom for wiretapping. Achievability follows by observing that in our scheme in Section IV, each relay only utilizes $\frac{1}{M-1}$ fraction of information broadcasted from each other relay.*

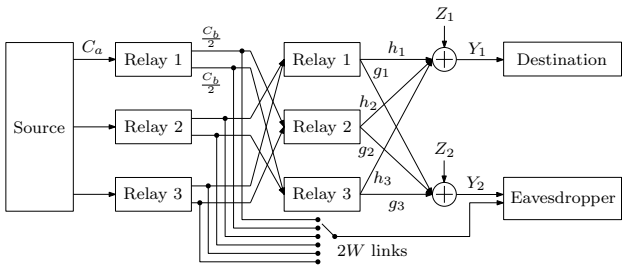

Figure 2. The Gaussian diamond-wiretap channel with pairwise relay cooperation for $M = 3$.

More generally, by closer inspection of our achievability and converse proof, one can show that when there are secure communication links among relays with total d.o.f. μ,[2] the secure d.o.f. is equal to $d_s = \min\left\{M\alpha, \frac{M\alpha+\mu+M-1}{M+1}, 1\right\}$.

Remark 3. *The secure d.o.f. decreases compared to the case of full CSIT studied in [4]. In particular, for $M = L = 2$, while $\beta \ge \frac{1}{4}$ is needed for the case of full CSIT to compensate the decrease in secure d.o.f. due to secrecy constraint, $\beta \ge \frac{1}{2}$ is required for the case of no eavesdropper's CSI.*

Remark 4. *A generalization to the setting where the eavesdropper can also wiretap some of source-relay links is briefly discussed in Section VI.*

IV. Achievability

We note that the works [6], [7] do not consider communication links among relays. Here we present a constituent scheme, called noise-forwarding (NF) scheme, that utilizes the links among relays.

Our achievability proof consists of two parts: (i) we first present the NF scheme that achieves $(\alpha, \beta, d_s) = \left(\frac{1}{M}, \frac{1}{L}, 1\right)$ and then (ii) show that the whole d.o.f. region in Theorem 1 can be achieved by time-sharing the NF scheme with two other previously known schemes.

Let us first describe the NF scheme at a high-level. In Appendix A, we provide a more detailed and rigorous analysis. The NF scheme is illustrated in Fig. 3 for the special case of $M = 3$ and $L = 2$ ($W = 1$). In the NF scheme, the source represents the message of d.o.f. 1 as a vector $(V_1, \cdots, V_M)$ of independent message symbols where V_k has a d.o.f. $\frac{1}{M}$. The source sends V_k to relay k, which requires $\alpha = \frac{1}{M}$. Then, relay k broadcasts to the other relays a vector $(U_{k,j} : j \in [1:M], j \neq k)$ of its own independent noise symbols where $U_{k,j}$ has a d.o.f. $\frac{1}{L(M-1)}$, which requires $\beta = \frac{1}{L}$. Relay k sends the message symbol V_k, a set of noise symbols $(U_{k,j}, U_{i,k} : j \in [1:M], i \in [1:M], j \neq k, i \neq k)$ in a way that (i) each of noise symbols is beam-formed in the

[2] μ only counts *orthogonal* information that are securely communicated among relays. Hence, in both the relay cooperation scenarios described in Section II and in the previous paragraph, $\mu = L\beta$.

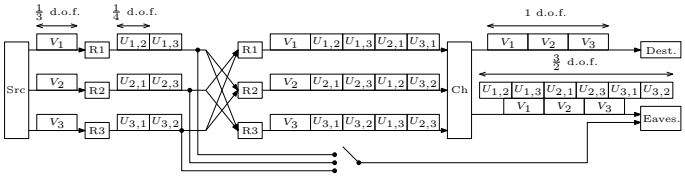

Figure 3. Illustration of the noise-forwarding scheme for $M = 3$ and $L = 2$.

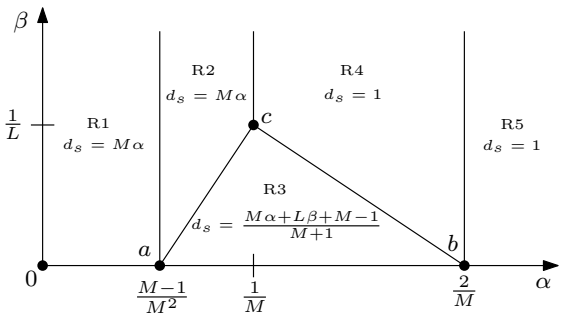

Figure 4. The (α, β, d_s) region of Theorem 1 with three corner points a, b, and c achieved by two schemes in [6], [7] and our NF scheme, respectively.

null space of the destination's channel, (ii) $V_1, \cdots, V_M$ can be distinguished by the destination, and (iii) any two of noise symbols are not aligned at the eavesdropper with high probability. Note that the total d.o.f. of $U_{k,j}$'s is $\frac{M}{L} = 1+\frac{W}{L}$. Hence, although the eavesdropper wiretaps a total of $W(M-1)$ noise symbols each of d.o.f. $\frac{1}{L(M-1)}$, the remaining noise symbols occupy a total of 1 d.o.f at the eavesdropper's signal space and thus the message can be shown to be secure. Readers are referred to Appendix A for a more rigorous analysis.

Now, we prove that the whole d.o.f. region of Theorem 1 is achievable by time-sharing the NF scheme with two other previously known schemes. According to [6], [7], where the relay cooperation was not considered, $(\alpha, \beta, d_s) = \left(\frac{M-1}{M^2}, 0, \frac{M-1}{M}\right)$ and $(\alpha, \beta, d_s) = \left(\frac{2}{M}, 0, 1\right)$ are achievable by a blind cooperative jamming scheme and a computation for jamming scheme. For brevity, let us call the schemes achieving $\left(\frac{M-1}{M^2}, 0, \frac{M-1}{M}\right)$, $\left(\frac{2}{M}, 0, 1\right)$, and $\left(\frac{1}{M}, \frac{1}{L}, 1\right)$ as Schemes a, b, and c, respectively. Fig. 4 illustrates the (α, β, d_s) region of (3) with the corner points achieved by Schemes a, b, and c. Then, the secure d.o.f. in Region 1 (indicated with R1 in Fig. 4) is achieved by using Scheme a for some fraction of time. Next, the secure d.o.f. in Region 2 (R2), Region 3 (R3), and Region 4 (R4) is achieved by time-sharing between Schemes a and c, between Schemes a, b, and c, and between Schemes b and c, respectively. Finally, the secure d.o.f. in Region 5 (R5) can be achieved by Scheme b. ∎

V. Converse

For the Gaussian multiple-access wiretap channel, it is shown in [5, Section 4.2.1] that there is no loss of secure d.o.f. if we consider the following deterministic model with integer-input and integer-output, instead of (1) and (2):

$$Y_1(t) = \sum_{k=1}^{M} \lfloor h_k(t) X_k(t) \rfloor, \; Y_2(t) = \sum_{k=1}^{M} \lfloor g_k(t) X_k(t) \rfloor \quad (4)$$

with the constraint

$$X_k(t) \in \{0, 1, \cdots, \lfloor \sqrt{P} \rfloor\}, k \in [1 : M]. \quad (5)$$

Likewise, it can be shown that there is no loss of secure d.o.f. in considering the deterministic model (4) and (5) for the multiple-access part of our model.[3] Hence, in this section, the multiple-access part is assumed to be given as (4) and (5).

We assume that $\mathbf{g}^n$ in addition to $\mathbf{h}^n$ is available at the destination, which only possibly increases the secure d.o.f. Hence, $\mathbf{h}^n$ and $\mathbf{g}^n$ are conditioned in every entropy and mutual information terms in this section, but are omitted for brevity. In the following, c_i's for $i = 1, 2, 3, \cdots$ are used to denote positive constants independent of n and P.

Fix an arbitrary $T \subseteq [1 : M]$ such that $|T| = W$. We obtain

$$\begin{aligned} nR &\overset{(a)}{\le} I(G; Y_1^n, B_T^n) - I(G; Y_2^n, B_T^n) + nc_1 \quad (6)\\ &\overset{(b)}{=} H(X_{[1:M]}^n | B_T^n) - H(Y_2^n | B_T^n) + nc_1 \\ &\le H(X_{[1:M]}^n, A_{[1:M]}^n, B_{T^c}^n | B_T^n) - H(Y_2^n | B_T^n) + nc_1 \\ &\le H(A_{[1:M]}^n) + H(B_{T^c}^n) + H(X_{[1:M]}^n | A_{[1:M]}^n B_{[1:M]}^n) \\ &\qquad - H(Y_2^n | B_T^n) + nc_1 \\ &\le nMC_a + nLC_b + \sum_{i=1}^{M} H(X_i^n | A_i^n, B_{[1:M]}^n) \\ &\qquad - H(Y_2^n | B_T^n) + nc_1, \quad (7) \end{aligned}$$

where (a) is due to the Fano's inequality and the secrecy constraint and (b) is by applying the similar arguments used to obtain [7, Eq. (15)].

Next, to bound $H(X_i^n | A_i^n, B_{[1:M]}^n)$ for $i \in [1 : M]$, we start from (6) to obtain

$$\begin{aligned} nR &\le I(G; Y_1^n, B_T^n) - I(G; Y_2^n, B_T^n) + nc_1 \\ &\le I(G; Y_1^n | B_T^n) + nc_1 \quad (8)\\ &\overset{(a)}{\le} I(A_{[1:M]}^n, B_{T^c}^n; Y_1^n | B_T^n) + nc_1 \\ &\le H(Y_1^n | B_T^n) - H(Y_1^n | A_{[1:M]}^n, B_{[1:M]}^n) + nc_1 \\ &\overset{(b)}{\le} H(Y_1^n | B_T^n) - H(X_i^n | A_{[1:M]}^n, B_{[1:M]}^n, X_{i^c}^n) + nc_2 \\ &\overset{(c)}{\le} H(Y_1^n | B_T^n) - H(X_i^n | A_i^n, B_{[1:M]}^n) + nc_2, \quad (9) \end{aligned}$$

where $i^c := [1 : M] \setminus \{i\}$, (a) is due to the Markov chain $G - (A_{[1:M]}^n, B_{[1:M]}^n) - Y_1^n$, (b) is from similar arguments used to derive [7, Eq. (31)], and (c) is due to the Markov chain $(X_{i^c}^n, A_{i^c}^n) - (A_i^n, B_{[1:M]}^n) - X_i^n$.

Now, by combining (7) and (9), we have

$$\begin{aligned} &(M+1)nR \\ &\le nMC_a + nLC_b \\ &\qquad + MH(Y_1^n | B_T^n) - H(Y_2^n | B_T^n) + nc_3 \\ &= nMC_a + nLC_b + (M-1)H(Y_1^n | B_T^n) \\ &\qquad + H(Y_1^n | B_T^n) - H(Y_2^n | B_T^n) + nc_3. \quad (10) \end{aligned}$$

Furthermore, from [9, Section 6], it follows that

$$H(Y_1^n | B_T^n) - H(Y_2^n | B_T^n) \le n \cdot o(\log P). \quad (11)$$

By substituting (11) to (10), we obtain $d_s \le \frac{M\alpha+L\beta+M-1}{M+1}$. From the cutset bound, we have $d_s \le M\alpha$. On the other hand, from (8), we have $d_s \le 1$. This completes the proof of the converse part of Theorem 1. ∎

[3] We omit the proof since it is a straightforward extension of [5, Section 4.2.1].

VI. Discussion

As a final remark, we briefly outline the generalization to the scenario where the eavesdropper can also wiretap up to W' source-relay links. Let $N = M - W'$ denote the number of secure source-relay links. In this general model, it can be shown that the secure d.o.f. is given as

$$d_s = \begin{cases} \min\{\alpha, \frac{L\beta+M-1}{M}, 1\}, & N = 1 \\ \min\{N\alpha, \frac{N\alpha+L\beta+M-1}{M+1}, 1\}, & N \geq 2. \end{cases} \quad (12)$$

To achieve (12), we time-share the two constituent schemes in [7][4] with a new constituent scheme achieving $(\alpha, \beta, d_s) = \left(\frac{1}{N}, \frac{1}{L}, 1\right)$ for any $N \geq 1$. This constituent scheme incorporates secure network coding technique used in [7] for the source-relay communication and our noise-forwarding scheme for the relay cooperation. We note that the secure network coding technique is needed for the source-relay links since message has to somehow be forwarded from the source to the relays to be decoded at the legitimate destination. For the relay cooperation part, however, it suffices to send noise symbols that are independent of the message and hence secure network coding is not required.

Appendix A
Detailed analysis of the NF scheme

For the analysis of the NF scheme, we use the following proposition, which can be proved by assuming symbol-by-symbol operation at each relay and regarding our model as the classical wiretap channel [10].

Proposition 1. *For the Gaussian diamond-wiretap channel with rate-limited relay cooperation, a secrecy rate R is achievable if $R \leq I(V;Y_1|\mathbf{h}) - I(V;Y_2,B_T|\mathbf{h},\mathbf{g})$ for all $T \subseteq [1:M]$ such that $|T| = W$ for some $p(v)p(a_{[1:M]}|v)\prod_{k\in[1:M]} p(b_k|a_k)p(x_k|a_k,b_{[1:M]},\mathbf{h})$ such that $H(A_k) \leq C_a$, $H(B_k) \leq C_b$, and $\mathrm{E}[X_k^2] \leq P$ for $k \in [1:M]$.*

Let $\mathcal{C}(\delta, Q)$ for positive real number δ and positive integer Q denote the PAM constellation $\delta\{-Q, -Q+1, \cdots, 0, \cdots, Q-1, Q\}$ of $(2Q+1)$ points with distance δ between consecutive points. We apply Proposition 1 with the following choice of $p(v)p(a_{[1:M]}|v)\prod_{k\in[1:M]} p(b_k|a_k)p(x_k|a_k,b_{[1:M]},\mathbf{h})$:

$$V = (V_1, \cdots, V_M),\ A_k = V_k$$
$$B_k = (U_{k,j} : j \in [1:M], j \neq k)$$
$$X_k = V_k + \sum_{\substack{j\in[1:M]\\ j\neq k}} U_{k,j} - \sum_{\substack{i\in[1:M]\\ i\neq k}} \frac{h_i}{h_k} U_{i,k}$$

for $k \in [1:M]$, where V_k's are independently generated according to Unif$[\mathcal{C}(\delta_a, Q_a)]$ and $U_{k,j}$'s are independently generated according to Unif$[\mathcal{C}(\delta_b, Q_b)]$ for some positive real numbers δ_a and δ_b and positive integers Q_a and Q_b to be specified later. We note that $H(A_k) \leq C_a$, $H(B_k) \leq C_b$, and $\mathrm{E}[X_k^2] \leq P$ for $k \in [1:M]$ are satisfied if

$$\log(2Q_a + 1) \leq C_a,\ (M-1)\log(2Q_b+1) \leq C_b \quad (13)$$
$$\delta_a Q_a + \gamma_b \delta_b Q_b \leq \sqrt{P}, \quad (14)$$

where $\gamma_b = (M-1)(1+J^2)$.[5] Then, the channel outputs are given as $Y_1 = \sum_{k=1}^M h_k V_k + Z_1$ and $Y_2 = \sum_{k=1}^M g_k V_k + \sum_{k\in[1:M]} \sum_{\substack{j\in[1:M]\\ j\neq k}} \left(g_k - \frac{h_k g_j}{h_j}\right) U_{k,j} + Z_2$. Note that the noise symbols $U_{k,j}$'s are canceled at the legitimate destination and the message symbols V_k's are masked by the set of $U_{k,j}$'s at the eavesdropper. From Proposition 1, the following secrecy rate is achievable:

$$R \leq I(V;Y_1|\mathbf{h}) - \max I(V;Y_2,U_T|\mathbf{h},\mathbf{g}), \quad (15)$$

where the maximization is over all $T \subseteq \{(k,j) : k \in [1:M], j \in [1:M], k \neq j\}$ such that $|T| = (M-1)W$. Let us choose $Q_a = P^{\frac{1-\epsilon}{2(M+\epsilon)}}$, $\delta_a = \frac{P^{1/2}}{2Q_a}$, $Q_b = P^{\frac{1-\epsilon}{2((M-1)L+\epsilon)}}$, and $\delta_b = \frac{P^{1/2}}{2\gamma_b Q_b}$ for some $\epsilon > 0$ that satisfies the power constraint (14). Then, by standard real interference alignment arguments [11], it can be shown that for any $T \subseteq \{(k,j) : k \in [1:M], j \in [1:M], k \neq j\}$ such that $|T| = (M-1)W$,

$$I(V;Y_1|\mathbf{h}) \geq \frac{(1-\epsilon)M}{2(M+\epsilon)} \log P - o(\log P) \quad (16)$$
$$I(V;Y_2,U_T|\mathbf{h},\mathbf{g}) \leq \frac{\epsilon((M-1)L+1)}{2((M-1)L+\epsilon)} \log P + o(\log P). \quad (17)$$

By choosing ϵ sufficiently small, it follows from (13), (15), (16), (17) that $(\alpha, \beta, d_s) = (\frac{1}{M}, \frac{1}{L}, 1)$ is achievable. ∎

References

[1] O. Simeone, O. Somekh, H. V. Poor, and S. Shamai (Shitz), "Downlink multicell processing with limited-backhaul capacity," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, no. 1, pp. 1–10, 2009. [Online]. Available: http://dx.doi.org/10.1155/2009/840814

[2] D. Gesbert, S. Hanly, H. Huang, S. S. Shitz, O. Simeone, and W. Yu, "Multi-cell MIMO cooperative networks: A new look at interference," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 9, pp. 1380–1408, December 2010.

[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5g wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, April 2015.

[4] S.-H. Lee and A. Khisti, "The Gaussian diamond-wiretap channel with conferencing relays," *IEEE Communications Letters*, vol. 20, no. 7, pp. 1393–1396, July 2016.

[5] P. Mukherjee, J. Xie, and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT," *IEEE Trans. Inf. Theory*, accepted for publication. [Online]. Available: http://arxiv.org/abs/1506.06114.

[6] S.-H. Lee, W. Zhao, and A. Khisti, "Secure degrees of freedom of the Gaussian diamond-wiretap channel," *IEEE Trans. Inf. Theory*, accepted for publication. [Online]. Available: http://arxiv.org/abs/1512.06291.

[7] S.-H. Lee and A. Khisti, "The wiretapped diamond-relay channel," *IEEE Trans. Inf. Theory*, submitted for publication. [Online]. Available: http://arxiv.org/abs/1606.05954.

[8] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, pp. 424–435, Jan. 2011.

[9] A. G. Davoodi and S. A. Jafar, "Aligned image sets under channel uncertainty: Settling a conjecture by Lapidoth, Shamai and Wigger on the collapse of degrees of freedom under finite precision CSIT," 2014. [Online]. Available: http://arxiv.org/abs/1403.1541.

[10] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[11] A. S. Motahari, S. Oveis-Gharan, M. A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Trans. Inf. Theory*, vol. 60, pp. 4799–4810, Aug. 2014.

[4] The work [7] considers the *wiretapped diamond-relay channel* where there is no cooperation among relays and the eavesdropper can wiretap up to N source-relay links as well as the multiple access part.

[5] We remind that J is a positive finite number such that $\frac{1}{J} \leq |h_k(t)|, |g_k(t)| \leq J$ for all $k \in [1:M]$.