Colluding Eavesdroppers in Large Cooperative Wireless Networks

Mahtab Mirmohseni
Department of Electrical Engineering,
Sharif University of Technology, Tehran, Iran
Email: mirmohseni@sharif.edu

Panagiotis Papadimitratos
KTH Royal Institute of Technology, Stockholm, Sweden
Email: papadim@kth.se

***Abstract*—Securing communication against non-colluding passive eavesdroppers has been extensively studied. Colluding eavesdroppers were considered for interference-limited large networks. However, collusion was not investigated for *large cooperative* networks. This paper closes this gap: we study the improvement the eavesdroppers achieve due to *collusion* in terms of the information leakage rate in a large *cooperative* network. We consider a dense network with n_l legitimate nodes, n_e eavesdroppers, and path loss exponent $\alpha \geq 2$. We show that if $n_e^{(2+\frac{2}{\alpha})}(\log n_e)^{\gamma} = o(n_l)$ holds, for some positive γ, then zero-cost secure communication is possible; i.e., n_e colluding eavesdroppers can be tolerated. This means that our scheme achieves unbounded secure aggregate rate, given a fixed total power constraint for the entire network.**

I. Introduction

Eavesdroppers can breach confidentiality by *passively* listening to the open wireless medium (channel), independently, or by sharing their observations. Physical-layer solutions to thwart these attackers use information-theoretic tools and channel statistics to achieve a secure positive rate. Wyner [1] modeled the point-to-point noisy communication in the presence of an eavesdropper with the wiretap channel; in which a legitimate transmitter sends a confidential message to a legitimate receiver while keeping it hidden from an eavesdropper. He also derived the capacity of the degraded wiretap channel using *Wyner's wiretap channel coding* [2].

Recently, there has been considerable research interest in finding the fundamental limits of secure communication rates in multi-user wiretap channels, with different legitimate-wiretapper user combinations [3]–[9]. However, even in these simple three- or four-node networks, the problem is open [2]. In large wireless networks, in addition to the large number of nodes, their stochastic distribution motivates the study of scaling laws, or the asymptotic behavior, following the line of works pioneered by Gupta and Kumar in [10]. They showed that, in a network of n randomly located nodes, multi-hopping schemes can achieve at most an aggregate rate that scales like $\sqrt{n}$, under an individual (per node) power constraint. The main assumption in this line of works (based on multi-hopping schemes) is point-to-point communication; in each hop, the receiver (of that hop) only decodes its corresponding transmitter's signal while it treats all other signals, roughly termed interference, as noise. This model is mostly referred to as an interference-limited channel. Without this limitation, *cooperative* schemes increase the aggregate rate to a near-linear scaling under individual power constraints; they even achieve unbounded capacity for fixed total power [11], [12].

Investigating how secrecy constraints affect scaling laws of large wireless networks attracts growing interest in both interference-limited [13]–[15] and cooperative [16] models. Multiple eavesdroppers in these scenarios can either listen individually to the channel (*non-colluding* case) or they can share their observations and make the attack more effective (*colluding* case) [17]. The distinction of the two adversarial models is significant. Collusion implies increased sophistication, thus more powerful adversaries. In practice, it may be feasible for many systems. Thus, a non-colluding eavesdroppers model may underestimate the adversary. In any case, it is an important question: *How does the increase in adversarial power (collusion) affect the secrecy rates and scaling?*

Combating colluding eavesdroppers was investigated ([13], [14], [17], [18]). Scaling results were previously derived only for the interference-limited channel [13], [14]. For non-colluding eavesdroppers, Koyluoglu *et al.*, under the assumption of an interference-limited channel, achieved a secure aggregate rate of scaling $\sqrt{n}$ for dense networks, as long as the ratio of the densities of eavesdroppers and legitimate nodes scales as $(\log n)^{-2}$ [13]. While for *colluding* eavesdroppers, the same rate scaling (i.e., $\sqrt{n}$) is achieved for a lower density of eavesdroppers [13]. These scaling results were achieved assuming that the transmission power for each node is fixed. Thus, the cost of secure communication (defined as the total power over the secure rate) goes to ∞. In contrast, with *arbitrary* (active) cooperation among legitimate nodes allowed, zero-cost secure communication (i.e., unbounded secure rate with fixed total power) against non-colluding eavesdroppers is achieved [16]. Now, the natural question is how a more powerful adversary model (i.e., *colluding* eavesdroppers) degrades the scalings for cooperative networks.

In this paper, we answer this question. We show that, even in the presence of *colluding* eavesdroppers, active cooperation achieves zero-cost secure communication while tolerating less eavesdroppers (compared to the non-colluding case). We consider a dense network with n_l legitimate nodes, n_e eavesdroppers, and path loss exponent $\alpha \geq 2$. We let eavesdroppers exchange their channel outputs (observations), i.e., collude, for free; this is the perfect collusion model

978-1-4799-4877-2/14/$31.00 ©2014 IEEE

considered in literature [13], [17]. Our work is the first to consider collusion in cooperative large networks. Building on the framework proposed in [16], we achieve unbounded secure rate given fixed total power (for the entire network), as long as $n_e^{(2+\frac{2}{\alpha})}(\log n_e)^{\gamma} = o(n_l)$ holds for some $\gamma > 0$. In our achievability scheme, (i) the source uses Wyner coding and a *serial (multi-stage)* relaying scheme, to cooperate with the relays, and (ii) the relays cooperate with the source in a block Markov fashion and, at the same time, act as a virtual multi-antenna to apply beamforming against the eavesdroppers.

II. Network Model and Preliminaries

Notation: Upper-case letters (e.g., X) denote Random Variables (RVs) and lower-case letters (e.g., x) their realizations. The probability mass function (p.m.f) of a RV X with alphabet set $\mathcal{X}$ is denoted by $p_X(x)$. $A_\epsilon^n(X,Y)$ is the set of ϵ-strongly, jointly typical sequences of length n. X_i^j indicates a sequence $(X_i, X_{i+1}, ..., X_j)$; we use X^j instead of X_1^j for brevity. $\mathcal{CN}(0,\sigma^2)$ denotes a zero-mean complex valued Gaussian distribution with variance σ^2. The variables relating to legitimate nodes and eavesdroppers are indicated with sub/superscripts l and e, respectively. $\|\mathbf{X}\|_p$ is the L^p-norm of a vector $\mathbf{X}$; $\mathbf{X}(i)$ is its i-th element. $(\cdot)^T$, $(\cdot)^\dagger$ and $\mathcal{N}(\cdot)$ denote the transpose, conjugate transpose and null space operations, respectively. For stating asymptotic results (Landau notation): $f(n) = o(g(n))$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} \to 0$.

Network and adversary model: The network model is abstracted from [16] and it is consistent with the ones in existing works on capacity scaling laws [10]–[12], [19] and secrecy capacity scaling [13]. For the adversary model, we consider perfect colluding passive eavesdroppers, as per all existing large network analyses to model collusion [13], [17], [18]. For completeness, we briefly describe:

A static path loss physical layer with path loss exponent $\alpha \geq 2$ is considered: channel gains decay exponentially with the distance between the (stochastically distributed) nodes. A set $\mathcal{N}_l$ of legitimate nodes and a set $\mathcal{N}_e$ of eavesdroppers are placed, according to Poisson Point Processes (PPP) with intensities λ_l and λ_e, respectively, in a square of unit area. The number of the legitimate nodes and the eavesdroppers are shown by $n_l = |\mathcal{N}_l|$ and $n_e = |\mathcal{N}_e|$, respectively, which we implicitly assume that $n_l, n_e \to \infty$ in order to investigate the scaling laws. Each legitimate node $i \in \mathcal{N}_l$, operating in a full-duplex mode, at time slot t, transmits $X_i(t)$ and receives $Y_i^l(t)$. In n_t channel uses, a message $m_i \in \mathcal{M}_i = [1 : 2^{n_t R_i}]$ can be sent from each legitimate node $i \in \mathcal{N}_l$ (as the source) to its uniformly randomly chosen destination $j \in \mathcal{N}_l \setminus \{i\}$. $\mathcal{T}(t) \subseteq \mathcal{N}_l$ shows the set of transmitting nodes at time slot t. The eavesdroppers only observe the channel ($Y_j^e(t)$ for $j \in \mathcal{N}_e$ at time slot t), but they can exchange their observations for free (because of the perfect collusion assumption). This means that all eavesdroppers have access to all the observations, shown by the vector $\mathbf{Y}^e(t)$, with $Y_j^e(t)$ its j-th element. Therefore,

$$Y_i^l(t) = \sum_{k\in\mathcal{T}(t)\setminus\{i\}} h_{k,i}^l(t) X_k(t) + Z_i^l(t) \tag{1}$$

$$Y_j^e(t) = \sum_{k\in\mathcal{T}(t)} h_{k,j}^e(t) X_k(t) + Z_j^e(t) \tag{2}$$

where the channel gains are

$$h_{k,i}^l(t) = (d_{k,i}^l)^{-\alpha/2} \quad , \quad h_{k,j}^e(t) = (d_{k,j}^e)^{-\alpha/2} \tag{3}$$

for $i \in \mathcal{N}_l \setminus \{k\}$ and $j \in \mathcal{N}_e$ with $d_{k,i}^l$ and $d_{k,j}^e$ denoting the distances between the transmitter with input signal $X_k, k \in \mathcal{T}(t)$ and the receiver Y_i^l and eavesdropper Y_j^e, respectively. $Z_i^l(t)$ and $Z_i^e(t)$ are independent and identically distributed (i.i.d) and zero mean circularly symmetric complex Gaussian noise components with powers N^l and N^e, i.e., $Z_i^l \sim \mathcal{CN}(0, N^l)$ and $Z_i^e \sim \mathcal{CN}(0, N^e)$, respectively. To apply the total power constraint in the network, we have:

$$\frac{1}{n_t}\sum_{t=1}^{n_t}\sum_{k\in\mathcal{T}(t)} |x_k(t)|^2 \leq \overline{P}_{tot}. \tag{4}$$

We term our network model, defined above, *Secure Network with Perfect Colluding Eavesdroppers ($\mathcal{SN}$-PCE).*

Definition 1: Let $\mathbf{R} = [R_i : i \in \mathcal{N}_l]$ be the rate vector and $2^{n_t\mathbf{R}} \doteq \{2^{n_t R_i} : i \in \mathcal{N}_l\}$. A $(2^{n_t\mathbf{R}}, n_t, P_e^{(n_t)})$ code for $\mathcal{SN}$-PCE consists of: (i) n_l message sets $\mathcal{M}_i = [1 : 2^{n_t R_i}]$ for $i \in \mathcal{N}_l$, where m_i is uniformly distributed over $\mathcal{M}_i$. (ii) $|\mathcal{T}(t)|$ sets of *randomized* encoding functions at the transmitters: $\{f_{i,t}\}_{t=1}^{n_t} : \mathbb{C}^{t-1} \times \mathcal{M}_i \longrightarrow \mathbb{C}$ such that $x_{i,t} = f_{i,t}(m_i, y_{l_i}^{t-1})$, for $i \in \mathcal{T}(t)$, $1 \leq t \leq n_t$ and $m_i \in \mathcal{M}_i$. (iii) Decoding functions, one at each legitimate node $i \in \mathcal{N}_l$, $g_i : (\mathcal{Y}_i^l)^{n_t} \times \mathcal{M}_i \mapsto \mathcal{M}_k$ for some $k \in \mathcal{N}_l \setminus \{i\}$, where it is assumed that node i is the destination for the message of source k. (iv) Probability of error for this code is defined as $P_e^{(n_t)} = \max_{i\in\mathcal{N}_l} P_{e,i}^{(n_t)}$ with: $P_{e,i}^{(n_t)} = \frac{1}{2^{n_t\|\mathbf{R}\|_1}} \sum_{m_k\in\mathfrak{M}} Pr(g_i((Y_i^l)^{n_t}, m_i) \neq m_k | \mathfrak{M} \text{ sent})$, where $\mathfrak{M} = \{m_i : i \in \mathcal{N}_l\}$. (v) The information leakage rate for the perfect colluding eavesdroppers $\mathcal{N}_e$ is defined as

$$R_L^{(n_t)} = \frac{1}{n_t} I(\mathfrak{M}; (\mathbf{Y}^e)^{n_t}). \tag{5}$$

Definition 2: A rate-leakage pair $(\mathbf{R}, R_L)$ is achievable if there exists a sequence of $(2^{n_t\mathbf{R}}, n_t, P_e^{(n_t)})$ codes such that $P_e^{(n_t)} \to 0$ as $n_t \to \infty$ and $\limsup_{n_t\to\infty} R_L^{(n_t)} \leq R_L$. The secrecy capacity region $\mathcal{C}_s$ includes all achievable rate vectors, $\mathbf{R}$, such that perfect secrecy is achieved, i.e., $R_L = 0$. Because of the intractability of dealing with an n_l-dimensional secrecy capacity region, especially in large-scale networks, we concentrate on the secure aggregate rate, defined as $\mathcal{R}_s = \sup_{\mathbf{R}\in\mathcal{C}_s} \|\mathbf{R}\|_1$. Without loss of generality, consider one active source-destination pair, by setting $|\mathfrak{M}| = 1$, while the other nodes help this pair's transmission. The reason follows from using a simple Time Division Multiple Access (TDMA) scheme [16, Remark 1]. Node 1 is assumed to be the source node (with message m_1): it transmits $X_1(t)$; and $Y_1^l(t) = \emptyset$. Thus, $\mathcal{R}_s = R_1$. The destination of m_1 is denoted by the n_l-th node: it receives $Y_{n_l}^l(t)$; and $X_{n_l}(t) = \emptyset$. Hence, the transmitter X_1 sends message $m_1 \in \mathcal{M}_1$ to the receiver $Y_{n_l}^l$ with the help of nodes in $\mathcal{N}_l \setminus \{1, n_l\}$; keeping it secret from the eavesdroppers in $\mathcal{N}_e$ who can freely share their channel outputs.

III. Main Results

Our main result, Theorem 2, states the maximum number of perfect-colluding eavesdroppers that can be tolerated in a zero-cost secure communication using a relaying based scheme. In fact, we show that if $n_e^{(2+\frac{2}{\alpha})}(\log n_e)^{\gamma} = o(n_l)$ holds for some positive γ, we achieve an unbounded secure aggregate rate for a fixed total power. For the proof, we adapt the framework of [16] to the colluding case. This framework consists of three steps, where in each step, the collusion should be taken into consideration.

1) *A lower bound to the secrecy capacity:* We propose an achievability scheme in Theorem 1 for a multiple relay channel in presence of perfect *colluding* eavesdroppers.

2) *Fitting the achievability scheme of Step 1 to $\mathcal{SN}$-PCE:* By choosing appropriate values for the parameters of the first step, the constraints on the number of legitimate nodes and eavesdroppers are derived in Lemma 3, under which the achievability results of Theorem 1 can be applied to $\mathcal{SN}$-PCE.

3) *Infinite secure aggregate rate:* We show that the achievable secure aggregate rate of the first step is unbounded after applying the fixed total power constraint (in Theorem 2). Hence, the maximum number of the tolerable perfect colluding eavesdroppers is obtained.

Step 1: The following theorem presents an achievable secure rate for a multiple relay channel in the presence of *colluding* eavesdroppers. We use serial (multi-stage) active cooperation (relaying), randomized encoding and beamforming through ZF. To make the ZF possible, we divide the network into clusters, where the nodes in each cluster act as a group of relays and, at the same time, collectively apply ZF (essentially as a distributed multi-antenna) on the colluding eavesdroppers. Applying this strategy results in some conditions on the clustering (such as the number of the nodes in each cluster).

Theorem 1: For $\mathcal{SN}$-PCE, the following secure aggregate rate is achievable:

$$\mathcal{R}_s^{ZF}=\min_{i\in[1:n_l-1]}\max_{\mathbf{B}_i,\tilde{P}_i}\log\Big(\frac{N^e}{N^l}\frac{N^l+\sum_{q=1}^{i}\,|\sum_{k=1}^{q}h_{k,i+1}^{l}\beta'_{kq}|^2\tilde{P}_q}{N^e+\sum_{j\in\mathcal{N}_e}|h_{1,j}^{e}|^2\tilde{P}_1}\Big) \quad (6)$$

in which

$$\beta'_{kq}=\mathbf{B}_q(k) \quad \text{and} \quad \beta'_{kq}=1 \quad \text{if} \quad k=q \quad (7)$$

$$\mathbf{B}_q\in\mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}) \quad \text{for} \quad q \bmod n_e=1 \quad (8)$$

$$\tilde{P}_q=\begin{cases}\overline{P}_q & \text{if } q \bmod n_e=1\\ 0 & \text{if } q \bmod n_e\neq 1\end{cases} \quad (9)$$

$$\sum_{q=1}^{n_l-1}\|\mathbf{B}_q\|_2^2\tilde{P}_q\leq\overline{P}_{tot} \quad (10)$$

where $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}\in\mathbb{C}^{n_e\times q}$ is the cluster-eavesdroppers channel matrix; its (j,i)th element is $h_{i,j}^{e}$, for $i\in[1:q], j\in\mathcal{N}_e$.

Proof: First, we consider a Discrete Memoryless version of the $\mathcal{SN}$-PCE and derive an achievable secure aggregate rate $\mathcal{R}_s^{DM}$ in Lemma 1. The proof is based on using (n_l-1)-stage block Markov coding (serial DF relaying) and Wyner's wiretap coding and is given in Appendix. Without loss of generality, let $\mathcal{N}_l=\{1,\ldots,n_l\}$. In the serial relaying scheme, the transmitted signal of each node i can be decoded in all subsequent nodes ($i+1$ to n_l). Hence, it can decode the transmitted signals of nodes 1 to $i-1$ [20]. Next, we extend $\mathcal{R}_s^{DM}$ to $\mathcal{SN}$-PCE in Lemma 2 and call it $\mathcal{R}_s$. Finally, we apply ZF to $\mathcal{R}_s$ and we obtain $\mathcal{R}_s^{ZF}$ Similarly to [16], we need clustering to apply ZF at the eavesdroppers. Each cluster determines the priority of decoding (starting from the source node). This means that the nodes in each cluster form a group of relays with the same priority; this enables them to act as a distributed multi-antenna to collectively apply ZF. Here, our rate expressions show the collusion effect. In Step 2, we adjust the size of the clusters to combat the collusion effect.

Lemma 1: Consider the general discrete memoryless counterpart of $\mathcal{SN}$-PCE, given by some conditional distribution $p(y_2^l,\ldots,y_{n_l}^l,\mathbf{y}^e|x_1,\ldots,x_{n_l})$, and let $\pi(\cdot)$ be a permutation on $\mathcal{N}_l=\{1,\ldots,n_l\}$, where $\pi(1)=1$, $\pi(n_l)=n_l$ and $\pi(m:n)=\{\pi(m),\pi(m+1),\ldots,\pi(n)\}$. The secrecy capacity is lower-bounded by:

$$\mathcal{R}_s^{DM}=\sup\max_{\pi(\cdot)}\min_{i\in[1:n_l-1]}I(U_{\pi(1:i)};Y_{\pi(i+1)}^{l}|U_{\pi(i+1:n_l-1)}) -I(U_{\pi(1:n_l-1)};\mathbf{Y}^e) \quad (11)$$

where the supremum is taken over all joint p.m.fs of the form

$$p(u_1,\ldots,u_{n_l-1})\prod_{k=1}^{n_l-1}p(x_k|u_k). \quad (12)$$

Now, we extend the above lemma to $\mathcal{SN}$-PCE, using an appropriate codebook mapping based on Gaussian RVs in the following lemma (proof is provided in Appendix).

Lemma 2: For $\mathcal{SN}$-PCE, the following secure aggregate rate is achievable.

$$\mathcal{R}_s=\min_{i\in[1:n_l-1]}\max_{\mathbf{B}_i,\tilde{P}_i}\log\Big(1+\frac{\sum_{q=1}^{i}\,|\sum_{k=1}^{q}h_{k,i+1}^{l}\beta'_{kq}|^2\tilde{P}_q}{N^l}\Big) \quad (13)$$
$$-\log\Big(1+\frac{\sum_{j\in\mathcal{N}_e}\sum_{q=1}^{n_l-1}\,|\sum_{k=1}^{q}h_{k,j}^{e}\beta'_{kq}|^2\tilde{P}_q}{N^e}\Big)$$

where (7) and (10) hold.

The serial relaying scheme overcomes the decoding constraint at the farthest relay by ordering the relays. Hence, all nodes in the network (except the source and destination) can be used as the relays; thus, $\mathcal{T}=\{1,\ldots,n_l-1\}$. From (13), we see that the optimal beamforming strategy is the one that results in max over the beamforming coefficient vector $\mathbf{B}$. Finding the closed form solution is an open problem [21]. Hence, we choose to ZF at the colluding eavesdroppers by letting $\sum_{q=2}^{n_l-1}\,|\sum_{k=1}^{q}h_{k,j}^{e}\beta'_{kq}|^2\tilde{P}_q=0,\forall j\in\mathcal{N}_e$. This results in $\tilde{P}_q=0$ or $E(q,j)=\sum_{k=1}^{q}h_{k,j}^{e}\beta'_{kq}=0$, for $\forall q\in[2:n_l-1]$. Now we show that indeed clustering is needed by deriving the power allocation in (9). One can obtain $X_k=\tilde{U}_k+\beta_k X_{k+1}$

from (19), where $\beta'_{kq} = \prod_{m=k}^{q-1} \beta_m$. Therefore, it is seen that $E(q_0, j)$ and $E(q_0+1, j)$ only differ in one variable, i.e., β_{q_0+1}. However, to apply ZF, $E(q, j)$ must be equal to zero for all $j \in \mathcal{N}_e$ if $\tilde{P}_q > 0$, which is clearly not possible. Therefore, we set $\tilde{P}_q = 0$ if $q \bmod n_e \neq 1$ and leave only one equation needing to be satisfied, i.e, $E(q, j) = 0$ if $q \bmod n_e = 1 \forall j \in \mathcal{N}_e$, in every n_e equations. Therefore, power allocation in (9) makes the ZF possible. Thus, the coefficient vector $\mathbf{B}_q$ must lie in the null space of $\mathbf{H}_{\mathcal{N}_e, \mathcal{T}^q}$, i.e, $\mathbf{H}_{\mathcal{N}_e, \mathcal{T}^q} \mathbf{B}_q = \mathbf{0}$, which is given in (8). (6) is resulted from applying (8) on (13). To summarize: in order to overcome n_e eavesdroppers, every n_e nodes form a cluster, where they transmit the same information in each block (equal part of fresh information) and they apply beamforming to ZF all eavesdroppers. To complete the proof, it is enough to derive the total power constraint (10) already given in Lemma 2. ■

Step 2: Now, we specify the details of our strategy and derive the constraints on the number of legitimate nodes and eavesdroppers in Lemma 3 (to apply the scheme of Theorem 1 to $\mathcal{SN}$-PCE). First, we choose randomly the source-destination pair in $\mathcal{N}_l$. Since $n_l, n_e \to \infty$, we can apply [16, Lemma 7] to make n_l and n_e arbitrarily close to λ_l and λ_e, respectively, with high probability (w.h.p). We design c_{max} clusters (squares), S_c, of same side d_c (as shown in Fig. 1); we consider an ordered set of nodes in clusters, with the source in the first cluster and the destination in the last one; any two successive clusters share one side. This results in $\frac{1}{d_c} \leq c_{max} \leq \frac{2}{d_c}$. In fact, the following results show that the asymptotic behavior of $\mathcal{R}_s$ is independent of c_{max}. Adapting the strategy of Step 1, each cluster (S_c) consists of the nodes transmitting the same part of the fresh information: in each cluster, only one node transmits fresh information. We only need one eavesdropper-free square, S_e, of side d_e around the source (the remaining communications are secured through beamforming). We define:

$$d_c = \sqrt{\frac{n_c}{n_l}}, d_e = n_e^{\frac{1}{\alpha}} \sqrt{\frac{n_c}{n_l}} (\log n_e)^{\frac{\gamma}{2}} \text{ for some } \gamma > 0 \quad (14)$$

where n_c is given in the following lemma that shows the feasibility of designing these squares.

Lemma 3: If $n_c n_e^{(1+\frac{2}{\alpha})} (\log n_e)^{\gamma} = o(n_l)$ holds for some $\gamma > 0$, the probability of having at least $n_c \to \infty$ legitimate nodes in S_c goes to 1, and the probability of having no eavesdropper in square S_e approaches 1.

Proof: Using the fact that a Poisson process has Poisson increments, the *number* of nodes in S_c is a two-dimensional Poisson RV with parameter $\lambda_l d_c^2$. As long as $\lambda_l d_c^2 \simeq n_c \to \infty$ holds, we can apply [16, Lemma 7] on (14) to show that this number is greater than n_c w.h.p. Recall that to apply ZF at all eavesdroppers, we need at least n_e nodes in each cluster, i.e., $n_c \geq n_e$. Thus, the above condition already holds ($n_c \geq n_e \to \infty$). The number of eavesdroppers in S_e is also a Poisson RV. Considering (14) and the condition stated in this lemma, we derive the parameter of this RV as: $\lambda_e d_e^2 \simeq \frac{n_c n_e^{(1+\frac{2}{\alpha})}}{n_l} (\log n_e)^{\gamma} \to 0$. Now, the probability of having no eavesdropper in S_e equals to $e^{-\lambda_e d_e^2} \to 1$. This completes the proof. ■

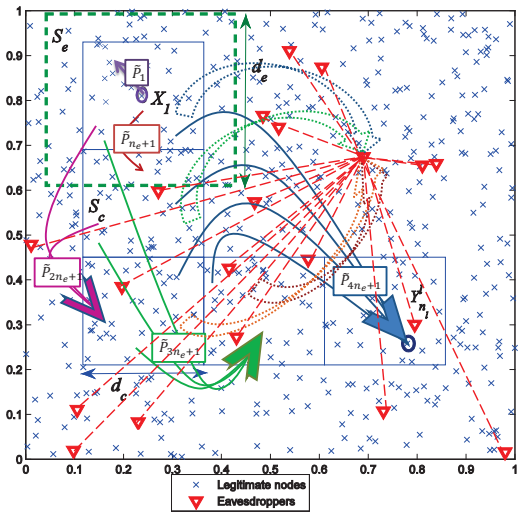

Fig. 1. Clusters (squares, S_c, with thin solid line) of side d_c used for serial relaying. The nodes in cluster c, coherently with nodes in all previous clusters and $i-c$ subsequent clusters send $\tilde{P}_{in_e+1}$ to the nodes in cluster $i+1$ for $i \geq c$. Each dotted arrow shows the received signals at one eavesdropper from all nodes in one cluster; these are equal to zero thanks to ZF. The dashed lines (only shown for one eavesdropper) show the free access of the eavesdroppers to all observations.

Step 3: Now, we state our main result.

Theorem 2: Considering the fixed total power ($\overline{P}_{tot}$) constraint in (4) for $\mathcal{SN}$-PCE, an infinite secure aggregate rate $\mathcal{R}_s$ is achievable (w.h.p.), as long as $n_e^{(2+\frac{2}{\alpha})} (\log n_e)^{\gamma} = o(n_l)$ holds for some positive γ.

Proof: Randomly choose the source-destination pair; term the source as node 1 and the destination as node n_l; design the squares S_c and S_e as (14) (around the source), which exist w.h.p due to Lemma 3. Moreover, design the clusters with an ordered set of legitimate nodes (based on the cluster numbers), which is feasible w.h.p according to Lemma 3. Consider the following cases:

Case 1: the destination is inside the first cluster (S_c). The source directly sends its message to the destination without any cooperation. In fact, all other nodes are silent. Therefore, the network reduces to a wiretap channel with many perfect colluding eavesdroppers. We use Wyner wiretap coding at the source to achieve the following unbounded rate:

$$\mathcal{R}_s^{WT} = \log\left(\frac{N^e}{N^l} \frac{N^l + |h_{1,n_l}^l|^2 \tilde{P}_1}{N^e + \sum_{j \in \mathcal{N}_e} |h_{1,j}^e|^2 \tilde{P}_1}\right) \quad (15)$$

$$\overset{(a)}{\geq} \log\left(\frac{N^e}{N^l} \frac{N^l + d_c^{-\alpha} \overline{P}_{tot}}{N^e + n_e (\frac{d_e}{2})^{-\alpha} \overline{P}_{tot}}\right) \overset{(b)}{\to} \infty \quad \text{as} \quad n_l \to \infty$$

where (a) follows from (3) and (4) (by considering the concepts of S_c and S_e squares); (b) follows from (14).

Case 2: the destination is outside the first cluster (S_c). Now, design the previously described c_{max} clusters each with $n_c = n_e + 1$ nodes. By substituting $n_c = n_e + 1$ into the scaling

TABLE I

	Non-colluding	Colluding
Interference-limited, $\mathfrak{C}_s \to \infty$	[13]: $\frac{n_e}{n_l} = o((\log n_l)^{-2})$	[13]: $\frac{n_e}{n_l} = O((\log n_l)^{-2-\rho}), \rho > 0$
Cooperative, $\mathfrak{C}_s \to 0$	[16]: $n_e^2(\log n_e)^\gamma = o(n_l)$	Theorem 2: $n_e^{(2+\frac{2}{\alpha})}(\log n_e)^\gamma = o(n_l), \gamma > 0$

of Lemma 3, one can obtain $n_e^{(2+\frac{2}{\alpha})}(\log n_e)^\gamma = o(n_l)$, i.e., the scaling of this theorem. As $n_c \geq n_e$, w.h.p, ZF can be applied and we achieve the rate of Theorem 1. Now, we allocate the power equally to the fresh information based on the total power constraint (10). Thus, we have $\tilde{P}_q = \frac{\overline{P}_{tot}}{\sum_{c=0}^{c_{max}} \|\mathbf{B}_{cn_e+1}\|_2^2} = \overline{P}_q = \overline{P}$, if $q \bmod n_e = 1$ and $q \leq c_{max}n_e + 1$. Otherwise, if $q \bmod n_e \neq 1$), we set $\tilde{P}_q = 0$. Thus, we can substitute these allocations into (6) and investigate its asymptotic behavior for all $i \in [1 : n_l - 1]$ and $\mathbf{B}_q$s that satisfy (7) and (8). First, we consider the nodes in the first cluster by letting $i \leq n_e + 1$:

$$\mathcal{R}_s^{ZF} \overset{(a)}{=} \log(\frac{N^e}{N^l} \frac{N^l + |h_{k,i+1}^l|^2 \overline{P}_1}{N^e + \sum_{j \in \mathcal{N}_e} |h_{1,j}^e|^2 \overline{P}_1}) \tag{16}$$
$$\overset{(b)}{\geq} \log(\frac{N^e}{N^l} \frac{N^l + d_c^{-\alpha}\overline{P}_1}{N^e + n_e d_e^{-\alpha}\overline{P}_1}) \to \infty \quad \text{as} \quad n_l \to \infty$$

(a) follows from the power allocation as in (9). (b) follows from the network model in (3) and the clustering (squares) concept with the sizes in (14). The intuition is to make the cluster S_c as small as enough to increase the rate achievable toward the nodes in the first cluster (similar to Case 1). However, by this reduction in the cluster size, one needs larger λ_l to have enough nodes in each cluster to make ZF possible at all eavesdroppers (i.e., $n_c \geq n_e$). This trade-off specifies the scaling.

Now, before continuing to the rate of the other clusters, let us take a closer look at the beamforming vector of each cluster ($\mathbf{B}_q \in \mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q})$ for $q \bmod n_e = 1$). By applying Singular Value Decomposition (SVD), we have $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q} = \mathbf{U}_q \mathbf{\Lambda}_q [\mathbf{\Upsilon}_q \mathbf{V}_q]^T$; $\mathbf{\Upsilon}_q \in \mathbb{C}^{q \times n_e}$ contains the first n_e right singular vectors corresponding to non-zero singular values, and $\mathbf{V}_q \in \mathbb{C}^{q \times (q-n_e)}$ contains the last $q - n_e$ singular vectors corresponding to zero singular values of $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}$. The later forms an orthonormal basis for the null space of $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}$. Hence, $\mathbf{B}_q$ can be expressed as their linear combination, i.e., $\mathbf{B}_q = \mathbf{V}_q \mathbf{\Phi}_q$, where $\mathbf{\Phi}_q \in \mathbb{C}^{(q-n_e)}$ is an arbitrary vector selected by considering the power constraints in (10).

Now, consider the nodes in cluster c, i.e., $cn_e + 1 \leq i \leq (c+1)n_e$, and set $q = cn_e + 1$. We remark that to overcome the fixed, non-decreasing distance between the nodes in the first cluster and the destination, the clusters are designed such that the maximum distance between the nodes in two adjacent clusters is $\sqrt{5}d_c$.

$$\begin{aligned}
\mathcal{R}_s^{ZF} &= \max_{\mathbf{B}_i} \log(\frac{N^e}{N^l} \frac{N^l + |\sum_{k=1}^{q} h_{k,i+1}^l \beta'_{kq}|^2 \tilde{P}_q}{N^e + \sum_{j \in \mathcal{N}_e} |h_{1,j}^e|^2 \tilde{P}_1}) \\
&\overset{(a)}{=} \max_{\mathbf{B}_q} \log(\frac{N^e}{N^l} \frac{N^l + |\mathbf{h}_q^\dagger \mathbf{B}_q|^2 \overline{P}}{N^e + \sum_{j \in \mathcal{N}_e} |h_{1,j}^e|^2 \overline{P}}) \\
&= \max_{\mathbf{\Phi_q}^\dagger \mathbf{\Phi_q} \leq \|\mathbf{B}_q\|_2^2} \log(\frac{N^e}{N^l} \frac{N^l + \mathbf{\Phi}_q^\dagger \mathbf{V}_q^\dagger \mathbf{h}_q \mathbf{h}_q^\dagger \mathbf{V}_q \mathbf{\Phi}_q \overline{P}}{N^e + \sum_{j \in \mathcal{N}_e} |h_{1,j}^e|^2 \overline{P}}) \\
&= \log(\frac{N^e}{N^l} \frac{N^l + \|\mathbf{B}_q\|_2^2 \lambda_{max}(\mathbf{V}_q^\dagger \mathbf{h}_q \mathbf{h}_q^\dagger \mathbf{V}_q)\overline{P}}{N^e + \sum_{j \in \mathcal{N}_e} |h_{1,j}^e|^2 \overline{P}}) \\
&= \log(\frac{N^e}{N^l} \frac{N^l + \|\mathbf{B}_q\|_2^2 \|\mathbf{h}_q^\dagger \mathbf{V}_q\|_2^2 \overline{P}}{N^e + \sum_{j \in \mathcal{N}_e} |h_{1,j}^e|^2 \overline{P}}) \\
&\overset{(b)}{\geq} \log \frac{1}{n_e} (\frac{d_e}{d_c})^\alpha \overset{(c)}{\to} \infty \quad \text{as} \quad n_l \to \infty
\end{aligned} \tag{17}$$

(a) is obtained by defining $\mathbf{h}_q = [h_{1,i+1}^l, \ldots, h_{q,i+1}^l]^T$. (b) follows from $\|\mathbf{B}_q\|_2^2 \geq \mathbf{B}_q(q) = \beta'_{qq} = 1$, $\|\mathbf{h}_q\|_2^2 \geq |h_{q,i+1}^l|^2 \geq d_c^{-\alpha}$, $\|\mathbf{V}_q\|_2^2 = 1$ and the randomness of $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}$ and $\mathbf{h}_q$. (c) is due to (14). This completes the proof. ■

IV. Discussion and Conclusion

Comparison to existing results: The cost of secure communication is defined as $\mathfrak{C}_s = \frac{\overline{P}_{tot}}{\mathcal{R}_s}$ [16]. In prior works with colluding eavesdroppers ([13], [14]), due to their assumption of an individual power constraint (the transmission power for each node is fixed), $\overline{P}_{tot}$ scales linearly with the number of nodes. Therefore, $\mathfrak{C}_s \to \infty$ as $n_l \to \infty$. Here, thanks to cooperation among legitimate nodes, we achieve $\mathfrak{C}_s \to 0$ against the colluding eavesdroppers. Table I compares our scaling result to the existing ones, for both colluding and non-colluding eavesdroppers. It can be seen that in both interference-limited and cooperative network models, the same secure communication cost can be achieved, by tolerating a slightly lower number of eavesdroppers for the colluding case (compared to the non-colluding case). However, in the cooperative model, this degradation depends on the path loss exponent, $\alpha > 2$, and it improves as α increases.

Perfect versus constrained collusion: We assumed *perfect* colluding eavesdroppers, considering that the eavesdroppers share their observations freely. Collusion in *large* wireless networks in all prior works is also assumed to be perfect [13], [14]. Recently, investigating the ramifications of the collusion models, the *Wiretap Channel with Constrained Colluding Eavesdroppers* (WTC-CCE) was proposed [22]: two colluding eavesdroppers communicate over a virtual collusion channel, in addition to the main point-to-point communication channel (one legitimate transmitter-receiver pair). Extending the WTC-CCE to the model at hand can be a natural future work item;

however, this is not trivial due to the complexity of both models.

APPENDIX

Proof of Lemma 1: The proof is similar to the one in [16, Lemma 4]. The difference is in the analysis of the information leakage rate. Therefore, we only provide this analysis for brevity. Consider the mutual information between M_1 and $(\mathbf{Y}^e)^{n_t}$, averaged over the random codebook $\mathcal{C}$.

$$
\begin{aligned}
&I\left(M_1;(\mathbf{Y}^e)^{n_t}|\mathcal{C}\right) = H(M_1|\mathcal{C}) - H(M_1|(\mathbf{Y}^e)^{n_t},\mathcal{C}) \\
&= n_t R_1 - H(M_1,S|(\mathbf{Y}^e)^{n_t},\mathcal{C}) + H(S|M_1,(\mathbf{Y}^e)^{n_t},\mathcal{C}) \\
&= n_t R_1 - H(M_1,S|\mathcal{C}) + I(M_1,S;(\mathbf{Y}^e)^{n_t}|\mathcal{C}) \\
&\quad + H(S|M_1,(\mathbf{Y}^e)^{n_t},\mathcal{C}) \\
&= n_t R_1 - n_t R_w + I(M_1,S,U^{n_t},X_1^{n_t};(\mathbf{Y}^e)^{n_t}|\mathcal{C}) \\
&\quad + H(S|M_1,(\mathbf{Y}^e)^{n_t},\mathcal{C}) \\
&\leq n_t R_1 - n_t R_w + I(M_1,S,U^{n_t},X_1^{n_t},\mathcal{C};(\mathbf{Y}^e)^{n_t}) \\
&\quad + H(S|M_1,(\mathbf{Y}^e)^{n_t},\mathcal{C}) \\
&\overset{(a)}{\leq} n_t R_1 - n_t R_w + n_t I(U,X_1;\mathbf{Y}^e) + H(S|M_1,(\mathbf{Y}^e)^{n_t},\mathcal{C}) \\
&\overset{(b)}{\leq} n_t(R_1 - R_w + I(U,X_1;\mathbf{Y}^e) + R_w - R_1 - I(U,X_1;\mathbf{Y}^e) + \varepsilon) \\
&\leq n_t \varepsilon
\end{aligned}
$$

(a) holds because $M_1,S,\mathcal{C} \rightarrow U^{n_t},X_1^{n_t} \rightarrow (\mathbf{Y}^e)^{n_t}$ forms a Markov chain and thanks to the memoryless property. (b) follows because by using [2, Lemma 22.1], we have: if $R_w - R_1 \geq I(U,X_1;\mathbf{Y}^e)$, then $H(S|M_1,(\mathbf{Y}^e)^{n_t},\mathcal{C}) \leq n_t(R_w - R_1 - I(U,X_1;\mathbf{Y}^e) + \varepsilon)$. ■

Proof of Lemma 2: Using standard arguments, we can extend (11), by computing it for an appropriate choice of the input distribution and constraining all the inputs to be Gaussian [23]. The mapping is same as the one in [16, Lemma 5], which is repeated here for completeness (since it is needed in deriving the beamforming vector).

For each $q \in [1:n_l-1]$, define $\mathbf{B}_q = [\beta'_{1q},\ldots,\beta'_{qq}] \in \mathbb{C}^q$ for $\beta'_{qq}=1$ and certain $\beta'_{kq}, k \in [1:q-1]$ and consider the following mapping for the generated codebook in Lemma 1 with respect to the p.m.f (12),

$$\tilde{U}_q \sim \mathcal{CN}(0,\tilde{P}_q) \qquad , q \in [1:n_l-1] \tag{18}$$

$$X_k = \sum_{q=k}^{n_l-1} \beta'_{kq}\tilde{U}_q = \tilde{U}_k + \sum_{q=k+1}^{n_l-1} \beta'_{kq}\tilde{U}_q \, , k \in [1:n_l-1] \tag{19}$$

Each node k (considering the ordered set of transmitters $k \in [1:n_l-1]$) in each block b transmits a linear combination of the decoded codewords in the n_l-k previous blocks (shown by $\tilde{U}_q(w_{b-q+1}), k \leq q \leq n_l-1$). These codewords make the coherent transmission between this node k and node $i, 1 \leq i < k$ to each node $q, k < q \leq n_l-1$. Beamforming using parameters β'_{kq} is applied by adjusting the power of these codewords. Applying the power constraint in (4) to the above mapping, we obtain

$$\overline{P}_{tot} \geq \sum_{k=1}^{n_l-1}\sum_{q=k}^{n_l-1} |\beta'_{kq}|^2\tilde{P}_q = \sum_{q=1}^{n_l-1}\sum_{k=1}^{q} |\beta'_{kq}|^2\tilde{P}_q = \sum_{q=1}^{n_l-1} \|\mathbf{B}_q\|_2^2\tilde{P}_q$$

Using this mapping, (1) and (2), applying interchangings in the order of summations, and deriving the mutual information terms in (11) completes the proof. ■

REFERENCES

[1] A. D. Wyner, "The Wire-tap Channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] A. E. Gamal and Y.-H. Kim, *Network information theory*. Cambridge Univ. Press, 2011.

[3] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[4] E. Ekrem and S. Ulukus, "Multi-receiver wiretap channel with public and confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2165–2177, April 2013.

[5] Y. K. Chia and A. E. Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2748–2765, May 2012.

[6] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE Int. Symp. Info. Theory (ISIT)*, Nice, France, Jun. 2007.

[7] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[8] R. Bassily and S. Ulukus, "Secure communication in multiple relay networks through decode-and-forward strategies," *Journal of Communications and Networks, special issue on Physical Layer Security*, vol. 14, no. 4, pp. 352–363, Aug. 2012.

[9] ——, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Processing*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.

[10] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 388–404, Mar. 2000.

[11] L.-L. Xie and P. R. Kumar, "A network information theory for wireless communications: Scaling laws and optimal operation," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 748–767, May 2004.

[12] A. Ozgur, O. Leveque, and D. N. C. Tse, "Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3549–3572, Oct. 2007.

[13] O. O. Koyluoglu, C. E. Koksal, and H. A. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[14] J. Zhang, L. Pu, and X. Wang, "Impact of secrecy on capacity in large-scale wireless networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012.

[15] A. Sheikoleslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, "Physical layer security from inter-session interference in large wireless networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012.

[16] M. Mirmohseni and P. Papadimitratos, "Scaling laws for secrecy capacity in cooperative wireless networks," in *Proc. IEEE INFOCOM*, Toronto, Canada, April 27 – May 2, 2014, also online as: arxiv.org/abs/1312.3198.

[17] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: the case of colluding eavesdroppers," in *Proc. IEEE Int. Symp. Info. Theory (ISIT)*, Seoul, Korea, Jun. 2009.

[18] ——, "Secure communication in stochastic wireless networks part ii: maximum rate and collusion," *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 1, pp. 139–147, Feb 2012.

[19] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran, "Closing the gap in the capacity of wireless networks via percolation theory," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1009–1018, Mar. 2007.

[20] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3037–3063, Sep. 2005.

[21] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2008.

[22] M. Mirmohseni and P. Papadimitratos, "Constrained colluding eavesdroppers: an information-theoretic model," in *Proc. International Zurich Seminar on Communications (IZS)*, Zurich, Switzerland, Feb. 2014.

[23] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.