Secrecy Capacity Scaling in Large Cooperative Wireless Networks

Mahtab Mirmohseni and Panagiotis Papadimitratos

***Abstract*—We investigate *large* wireless networks subject to security constraints. In contrast to point-to-point, interference-limited communications considered in prior works, we propose active cooperative relaying based schemes. We consider a network with n_l legitimate nodes, n_e eavesdroppers, and path loss exponent $\alpha \geq 2$. As long as $n_e^2\big(\log(n_e)\big)^\gamma = o(n_l)$, for some positive γ, we show one can obtain unbounded secure aggregate rate. This means zero-cost secure communication, given fixed total power constraint for the entire network. We achieve this result through (i) the source using Wyner randomized encoder and a *serial (multi-stage)* block Markov scheme, to cooperate with the relays and (ii) the relays acting as a virtual multi-antenna to apply beamforming against the eavesdroppers. Our simpler *parallel (two-stage)* relaying scheme can achieve the same unbounded secure aggregate rate when $n_e^{\frac{\alpha}{2}+1}\big(\log(n_e)\big)^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$ holds, for some positive γ, δ. Finally, we study the improvement (to the detriment of legitimate nodes) the eavesdroppers achieve in terms of the information leakage rate in a large *cooperative* network in case of *collusion*. We show that again the zero-cost secure communication is possible, if $n_e^{(2+\frac{2}{\alpha})}\big(\log n_e\big)^\gamma = o(n_l)$ holds, for some positive γ; i.e., in case of collusion slightly fewer eavesdroppers can be tolerated compared to the non-colluding case.**

***Index Terms*—Secrecy capacity; Scaling laws; Cooperative strategies; Relaying; Large wireless networks; Information-theoretic security; Colluding eavesdroppers.**

I. Introduction

The open nature of wireless networks makes them vulnerable to eavesdropping attacks; thus, confidentiality is a crucial security requirement. Conventional, cryptographic techniques have drawbacks, e.g., increasing, with the network size, key management complexity. Moreover, they rely on an assumption of limited attacker computational power, while encrypted data may still provide information to attackers (e.g., through traffic analysis). This motivated efforts to complement cryptographic techniques and fueled interest in information-theoretic physical layer security [3].

The natural problem is to find the fundamental limits of performance measures, notably the secure rate legitimate nodes can achieve, considering the overhead imposed by satisfying the secrecy constraints. However, even in simple three- or four-node networks, the problem is open [4]; the complex nature of large wireless networks with stochastic node distribution in space makes the derivation of exact results intractable. This motivated the investigation of scaling laws, or the asymptotic behavior of the network, to gain useful insights. The problem of finding scaling laws for large wireless networks with n randomly located nodes was first investigated by Gupta and Kumar in [5]; they showed that multihopping schemes can achieve at most an aggregate rate that scales like $\sqrt{n}$ under an individual (per node) power constraint. Using percolation theory, achievability of linear scaling was shown by Franceschetti *et al.* [6]. The main characteristic of this line of works is the assumption of point-to-point communication, where each receiver (not necessarily the final destination) is interested only in decoding the signal of a particular transmitter; all other signals, roughly termed interference, are treated as noise. Therefore, these are mostly referred to as interference-limited channel models. The broadcasting nature of wireless networks makes cooperation easier, though it decreases the security level. Contrary to the interference-limited model, it has been shown that cooperative schemes increase the aggregate rate to a near-linear scaling under individual power constraints and achieve unbounded transport capacity for fixed total power in some cases (in [7], [8] and follow-up works).

Recently, there is a growing interest in considering how secrecy constraints affect scaling laws of large wireless networks [9]–[13]. To best of our knowledge, all these works considered point-to-point interference-limited communications (multi-hopping) [9]–[13] to analyze the *secrecy* capacity scaling; no active cooperative or relaying schemes were considered.

In this paper, contrary to the interference-limited models, we allow for arbitrary cooperation among nodes and concentrate on the information-theoretic relaying schemes. With no secrecy constraint, Xie and Kumar in [7] proposed a strategy of coherent multistage relaying to achieve unbounded transport capacity for fixed total power in low-attenuation networks, i.e., achieving zero energy cost communication. However, when seeking to address secrecy constraints, active cooperation (relaying) is a double-edged sword: it benefits both legitimate receivers and eavesdroppers. Considering this trade-off, the fundamental question is whether zero-cost *secure* communication is possible through active cooperation. We answer this question positively here, filling this theoretical gap. Our result is further motivated by recent technological developments for relaying-based schemes (e.g., massive deployment of relay nodes in LTE-Advanced networks [14], [15]).

M. Mirmohseni is with the Department of Electrical Engineering, Sharif University of Technology, Tehran, IRAN (e-mail: mirmohseni@sharif.edu).

P. Papadimitratos is with the Networked Systems Security Group, KTH Royal Institute of Technology, Stockholm, Sweden (e-mail: papadim@kth.se).

The material in this paper has been presented in part in the IEEE INFOCOM, Toronto, Canada, April-May 2014 [1] and in the Iran Workshop on Communication and Information Theory (IWCIT), Tehran, Iran, May 2014 [2].

A. Background and Related Work

Physical layer security using information-theoretic tools leverages the channel statistics to thwart eavesdroppers (attackers); depending on the channel conditions, a secure positive rate can be possible if suitable coding schemes are employed. The information-theoretic notion of secrecy was introduced by Shannon in [16], where he showed that in order to achieve perfect secrecy, i.e., zero information leakage, one needs a secret key of size at least equal to the message size. This result inspired keyless information-theoretic security in a noisy communication model called the wiretap channel. Wyner determined the capacity of the degraded wiretap channel, with the channel to the eavesdropper being a degraded version of the channel to the legitimate receiver [17]. The wiretap secrecy capacity achieving scheme, known also as *Wyner wiretap channel coding*, comprises multicoding and randomized encoding [4, Section 22.1.1]. Csiszár and Körner extended the secrecy capacity result to the the general wiretap channel (not necessarily degraded) [18].

There has been considerable recent research interest in multi-user wiretap channels [19]–[26]. In these channels, cooperation among legitimate users is possible in two different ways. First, through active cooperation: legitimate nodes act as relays and cooperate with the source of the message in transmitting its message to the destination. This scenario with a single relay was introduced in [23] as the relay-eavesdropper channel where the secrecy rates were derived using relaying strategies such as the Decode-and-Forward (DF) scheme [27]. The case of multiple relays was investigated in [25], [28]. Second, passive cooperation, also known as deaf cooperation: the so called helper nodes transmit signals, which are independent from the transmitted message of the legitimate transmitter, to confuse the eavesdroppers and increase the secure rates [26], [28], [29]. In both cooperation modes, one can try to apply beamforming at the helper nodes to improve the secrecy by constructing the virtual Multiple Input Multiple Output (MIMO) scenarios and/or perform Zero-Forcing (ZF) at eavesdroppers [29]–[36]. It was shown that in a high-SNR regime, the ZF transmit scheme is Diversity-Multiplexing Tradeoff (DMT) optimal in a MIMO wiretap channel, with three nodes, a source, a destination and an eavesdropper [34], [35]. In this paper, we concentrate on the *active cooperation* schemes based on information-theoretic secrecy coding schemes.

The adversarial behavior in the aforementioned scenarios is captured by multiple eavesdroppers that can either listen individually to the channel (*non-colluding* eavesdroppers) or they can share their observations and make the attack more effective (*colluding* eavesdroppers) [37]. 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 some applications. In any case, it is an important question: *How does the increase in adversarial power (collusion) affect the secrecy rates and their scaling?* The mitigation of colluding eavesdroppers was investigated [9], [10], [37], [38].

Although there is considerable effort in these works on small networks (for both non-colluding and colluding eavesdroppers), consisting of few nodes with deterministic locations, the problem of secure communication in large networks received relatively less attention. Scaling laws for the secure aggregate rate were derived for large wireless networks, only under the assumption of *interference-limited channel*. Koyluoglu *et al.* [9] recently achieved a secure aggregate rate of scaling $\sqrt{n}$ for a dense network of n legitimate nodes, as long as the ratio of the densities of eavesdroppers and legitimate nodes scales as $(\log n)^{-2}$, for non-colluding eavesdroppers. While for *colluding* eavesdroppers, the same rate scaling (i.e., $\sqrt{n}$) is achieved for a lower density of eavesdroppers [9]. The authors in [11]–[13] considered extended networks with unknown eavesdropper locations and achieved a secure rate of order 1. This result is achieved through a deaf (passive) cooperative multi-hopping scheme in [13]. These scaling results were achieved assuming that the transmission power for each node is fixed. Thus, the total power scales linearly with the number of nodes, n, and the cost of secure communication (defined as the total power over the secure rate) goes to ∞.

B. Our Contributions

Our work is the first that allows *arbitrary* cooperation among legitimate nodes in deriving scaling laws for large wireless networks with secrecy constraints. Without the limitation of point-to-point communication, we show that cooperation can achieve *unbounded secure rate with fixed total power*, i.e., *zero-cost secure communication*, as long as the number of the eavesdroppers is less than a *derived* threshold. We consider a *dense* network, with a static path loss physical layer model and path loss exponent $\alpha \geq 2$, and stochastic node placement. n_l legitimate nodes and n_e eavesdroppers are distributed according to Poisson Point Processes (PPP) with intensities λ_l and λ_e, respectively, in a square of unit area. We consider the fixed total power constraint and find two scaling results for $\frac{n_e}{n_l}$, where by satisfying these results one can obtain infinite secure aggregate rate and thus zero-cost secure communication. Compared to [7], this means that n_e eavesdroppers can be tolerated asymptotically and do not affect the communication cost.

To achieve this result, we make use of (i) block Markov DF relaying, (ii) Wyner wiretap coding at the source to secure the new part of the message transmitted in each block, and (iii) beamforming, to secure the coherent parts transmitted cooperatively by all the nodes in the network. To apply DF, we propose two types of schemes: parallel (two-stage) relaying and serial (multi-stage) relaying. For beamforming, partial ZF at the eavesdroppers is used. DF based strategies for multiple relay networks were proposed in [7], [39] and then they were extended to such networks with an eavesdropper in [25], where some ZF schemes were applied. Here, we first extend these schemes to our network model with stochastic distribution of legitimate nodes and eavesdroppers by deriving the conditions under which we can apply the schemes. The main challenges we face are: the selection of relays among the legitimate nodes, the priority and power allocation, and the choice of appropriate beamforming parameters. Once these challenges addressed, we utilize the derived rates to achieve zero-cost secure communication.

Using the parallel (two-stage) relaying strategy, we show the possibility of achieving unbounded secure aggregate rate as long as $n_e^{\frac{\alpha}{2}+1}\big(\log(n_e)\big)^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$ for some positive γ, δ holds. Our scheme has two stages. First, the source of the message transmits to n_r relay nodes within some distance. At the second stage, the source and these relay nodes use block Markov coding [4] to cooperatively transmit the message to the destination, while using ZF against the eavesdroppers. In fact, relay nodes can be seen as a distributed virtual multi-antenna; using this diversity to combat the eavesdroppers. Transmissions are pipelined and relay nodes operate in a full-duplex mode, a typical assumption (e.g., [7], [40]).

At the expense of additional complexity, we tolerate even more eavesdroppers with serial (multi-stage) relaying. We achieve zero energy cost secure communication as long as $n_e^2\big(\log(n_e)\big)^{\gamma} = o(n_l)$ holds, for some $\gamma > 0$. In this scheme, all network nodes can act as relays for the source node but they are ordered in clusters and use block Markov coding and coherent transmission. Nodes in each cluster form a virtual multi-antenna to apply ZF at the eavesdroppers.

Finally, we investigate how a more powerful adversary model (i.e., *colluding* eavesdroppers) degrades the scaling of $\frac{n_e}{n_l}$ for cooperative networks. 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 let eavesdroppers exchange their channel outputs (observations), i.e., collude, for free; this is the perfect collusion model considered in literature [9], [37]. We achieve an unbounded secure rate given fixed total power (for the entire network), as long as $n_e^{(2+\frac{2}{\alpha})}\big(\log n_e\big)^{\gamma} = o(n_l)$ holds for some $\gamma > 0$. For the achievability, we propose a *serial (multi-stage)* relaying based scheme.

The rest of the paper is organized as follows. Section II introduces the network model and notation. Section III describes our proposed parallel relaying scheme and its scaling is derived. In Section IV, the results of serial relaying scheme are stated. A number of remarks are provided in Section VI.

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 $p_X(x)$; occasionally subscript X is omitted. $A_\epsilon^n(X,Y)$ is the set of ϵ-strongly, jointly typical sequences of length n. X_i^j indicates a sequence of RVs $(X_i, X_{i+1}, ..., X_j)$; we use X^j instead of X_1^j for brevity. $\mathcal{CN}(0,\sigma^2)$ denotes a zero-mean complex value Gaussian distribution with variance σ^2. The variables related to the 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 ith 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: We consider a dense wireless network, with channel gains obeying a static path loss model, decaying exponentially as the distance between the (stochastically distributed) nodes increases. This is consistent with models in prior works on capacity scaling laws [5]–[8] and secrecy capacity scaling [9]. For the adversary model, we consider two cases: *non-colluding* and *perfect colluding* passive eavesdroppers (as per all existing large network analyses modeling collusion [9], [37], [38]). For brevity, in the rest of the paper, the eavesdroppers are non-colluding, unless it is stated otherwise explicitly.

The network is a square of unit area where both the legitimate nodes and *eavesdroppers* are placed, according to Poisson Point Processes (PPP) with intensities λ_l and λ_e, respectively, which is a suitable assumption when nodes are independently and uniformly distributed in the network area or there is a substantial mobility [41]. There is a set $\mathcal{N}_l$ of legitimate nodes and their number is $n_l = |\mathcal{N}_l|$. Similarly, $\mathcal{N}_e$ and $n_e = |\mathcal{N}_e|$ are the set of eavesdroppers and their number. As we consider large-scale networks, throughout the paper, we implicitly assume that n_l and n_e go to ∞. Each legitimate node $i \in \mathcal{N}_l$ can be a source of message $m_i \in \mathcal{M}_i = [1 : 2^{nR_i}]$ and send it to its randomly chosen destination $j \in \mathcal{N}_l \setminus \{i\}$ in n channel uses. Every legitimate node $i \in \mathcal{N}_l$ operates in a full-duplex mode; at time slot t, it transmits $X_i(t)$ and receives $Y_i^l(t)$. The set of transmitting nodes at time slot t is denoted by $\mathcal{T}(t) \subseteq \mathcal{N}_l$. As we consider passive attackers, each eavesdropper $j \in \mathcal{N}_e$ only observes the channel and at time slot t, it receives $Y_j^e(t)$. 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, for any $i \in \mathcal{N}_l \setminus \{k\}$ and $j \in \mathcal{N}_e$, the static path loss model channel gains are given by:

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

with $d_{k,i}^l$ and $d_{k,j}^e$ denoting the distances between the transmitter $X_k, k \in \mathcal{T}(t)$ and the receiver Y_i^l and Y_j^e, respectively. We assume that the path loss exponent satisfies $\alpha \geq 2$. Though our results based on the parallel relaying scheme in Section III need this assumption, our serial relaying based results hold for any $\alpha > 0$. $X_k(t), k \in \mathcal{T}(t), t \in [1:n]$ is an input signal and we consider the total power constraint in the network:

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

Moreover, $Z_i^l(t)$ 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. Our **network model**, defined above, is called *Secure Network* ($\mathcal{SN}$) throughout the paper.

To model collusion, in addition to observing the channel ($Y_j^e(t)$ for $j \in \mathcal{N}_e$ at time slot t), the eavesdroppers 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. We term our network model in this case, *$\mathcal{SN}$ with Perfect Colluding Eavesdroppers ($\mathcal{SN}$-PCE)* throughout the rest of the paper.

Definition 1: Let $\mathbf{R} = [R_i : i \in \mathcal{N}_l]$ be the rate vector and $2^{n\mathbf{R}} \doteq \{2^{nR_i} : i \in \mathcal{N}_l\}$. A $(2^{n\mathbf{R}}, n, P_e^{(n)})$ code for $\mathcal{SN}$ (or $\mathcal{SN}$-PCE) consists of

(i) n_l message sets $\mathcal{M}_i = [1 : 2^{nR_i}]$ 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: $\{f_{i,t}\}_{t=1}^n : \mathbb{C}^{t-1} \times \mathcal{M}_i \longrightarrow \mathbb{C}$ such that $x_{i,t} = f_{i,t}(m_i, y_{l_i}^{t-1})$, for $i \in \mathcal{T}(t)$, $1 \leq t \leq n$ and $m_i \in \mathcal{M}_i$.

(iii) Decoding functions, one at each legitimate node $i \in \mathcal{N}_l$, $g_i : (\mathcal{Y}_i^l)^n \times \mathcal{M}_i \mapsto \mathcal{M}_k$ 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 $P_e^{(n)} = \max_{i \in \mathcal{N}_l} P_{e,i}^{(n)}$ with:

$$P_{e,i}^{(n)} = \frac{1}{2^{n\|\mathbf{R}\|_1}} \sum_{m_k \in \mathfrak{M}} Pr(g_i((Y_i^l)^n, m_i) \neq m_k | \mathfrak{M} \text{ sent}) \tag{5}$$

where $\mathfrak{M} = \{m_i : i \in \mathcal{N}_l\}$.

(v) For $\mathcal{SN}$: The information leakage rate for eavesdropper $j \in \mathcal{N}_e$ is defined as

$$R_{L,j}^{(n)} = \frac{1}{n} I(\mathfrak{M}; (Y_j^e)^n). \tag{6}$$

For $\mathcal{SN}$-PCE: The information leakage rate for the perfect colluding eavesdroppers set $\mathcal{N}_e$ is defined as

$$R_L^{(n)} = \frac{1}{n} I(\mathfrak{M}; (\mathbf{Y}^e)^n). \tag{7}$$

Definition 2: For $\mathcal{SN}$: A rate-leakage vector $(\mathbf{R}, \mathbf{R_L})$ is achievable if there exists a sequence of $(2^{n\mathbf{R}}, n, P_e^{(n)})$ codes such that $P_e^{(n)} \to 0$ as $n \to \infty$ and $\limsup_{n\to\infty} R_{L,j}^{(n)} \leq \mathbf{R_L}(j)$. The secrecy capacity region, $\mathcal{C}_s$, is the region which includes all achievable rate vectors, $\mathbf{R}$, such that perfect secrecy is achieved, i.e., $\mathbf{R_L} = \mathbf{0}$.

For $\mathcal{SN}$-PCE: A rate vector-leakage pair $(\mathbf{R}, R_L)$ is achievable if there exists a sequence of $(2^{n\mathbf{R}}, n, P_e^{(n)})$ codes such that $P_e^{(n)} \to 0$ as $n \to \infty$ and $\limsup_{n\to\infty} R_L^{(n)} \leq R_L$. The secrecy capacity region $\mathcal{C}_s$ includes all achievable rate vectors, $\mathbf{R}$, such that perfect secrecy is achieved, i.e., $R_L = 0$.

In large-scale networks, it is intractable to consider the n_l-dimensional secrecy capacity region; thus, we focus on the secure aggregate rate, defined as:

$$\mathcal{R}_s = \sup_{\mathbf{R} \in \mathcal{C}_s} \|\mathbf{R}\|_1. \tag{8}$$

The secure rate per legitimate user (uniformly distributed among them) can easily be obtained by calculating $\frac{\mathcal{R}_s}{n_l}$.
As we are interested in the achievability of $\mathcal{R}_s$, without loss of generality, we assume that only one source-destination pair is active and the other nodes assist their transmission. Therefore, we set $|\mathfrak{M}| = 1$. Without loss of generality, we assume that node 1 is the source node, i.e., $\mathfrak{M} = \{m_1\}$: it transmits $X_1(t)$; and $Y_1^l(t) = \emptyset$. Thus, $\mathcal{R}_s = R_1$. We denote the destination of m_1 by n_l-th node: it receives $Y_{n_l}^l(t)$; and $X_{n_l}(t) = \emptyset$. This means that the transmitter X_1 wishes to send message $m_1 \in \mathcal{M}_1 = [1 : 2^{nR_1}]$ to the receiver $Y_{n_l}^l$ with the help of nodes in $\mathcal{N}_l \setminus \{1, n_l\}$, while keeping it secret from the eavesdroppers in $\mathcal{N}_e$.

Remark 1: If a secure aggregate rate $\mathcal{R}_s = R_1$ is achievable in the above scenario (with uniformly random matching of the source-destination pairs), any rate vector $\mathbf{R}$ with $\|\mathbf{R}\|_1 = \mathcal{R}_s$ is also achievable using a time-sharing scheme. For example, consider a network of n nodes with a total rate of 1 bit/sec. If there is only one active source-destination pair, the source can transmit at the rate of 1 bit/sec. Otherwise, a Time Division Multiple Access (TDMA) scheme, with n equal time slots, achieves the rate of $\frac{1}{n}$ for each (source) node in the network, with the total rate of $n \times \frac{1}{n} = 1$ bit/sec. Any other rate allocation with unit total rate is also attainable by using TDMA with non-equal time slots.

III. Parallel Relaying

In this section, we consider a parallel (two-stage) relaying scheme and obtain the maximum number of eavesdroppers that can be tolerated in a zero-cost secure communication. In fact, our main result of this section, Theorem 2 shows that we achieve an unbounded secure aggregate rate for a fixed total power as long as $n_e^{\frac{\alpha}{2}+1}\big(\log(n_e)\big)^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$, for some positive γ, δ.

The idea of our technique is to implement a two-stage transmission scheme: in the first stage, the source transmits the message *securely* to the nodes that are close enough. In the second stage, these nodes (cooperating with their nearby source) send the message to the destination (making a virtual distributed Multi-Input Single-Output (MISO) channel), using ZF against the eavesdroppers to secure their transmission. The challenge here is to to have a sufficiently high number of legitimate nodes located close enough to the source node, while keeping the closest eavesdropper far enough from the source node. The sufficient number of legitimate nodes is determined by the ZF approach, while the distances of the legitimate nodes and the eavesdroppers to the source node are controlled by adjusting their densities.

Our proof is derived in three steps:

1) First, we provide a lower bound on the secrecy capacity achieved through active cooperation, randomized encoding and beamforming in Theorem 1. We propose a two-stage DF relaying and design the appropriate codebook mapping that enables ZF at the eavesdroppers. To apply these strategies, we derive conditions on the number and location of the relay nodes. Thus, this step yields the sufficient number of legitimate nodes (close to the source node).
2) In the second step, the main challenge is to find strategies to apply the achievability scheme of the first step to our network model ($\mathcal{SN}$). In Lemma 3, we obtain

the constraints on the number of legitimate nodes and eavesdroppers under which our network satisfies the conditions of the first step and the achievability scheme can be applied. In fact, we make use of the difference between the densities of the legitimate nodes and the eavesdroppers to ensure the existence of two squares around the source node, free of eavesdroppers, where the legitimate nodes of Step 1 lie in the inner square.

3) In the last step, we apply the fixed total power constraint and show that the achievable secure aggregate rate of the first step can be unbounded and derive the maximum number of the eavesdroppers which can be tolerated in Theorem 2. To make the unbounded rate possible, the sizes of the squares in Step 2 are chosen appropriately.

Step 1: As mentioned in Section II, the achievability relies on a single unicast scenario. Recall that a lower bound on the secrecy capacity of this scenario is an achievable secure aggregate rate for $\mathcal{SN}$. Here, n_r relay nodes (in $\mathcal{N}_l \setminus \{1, n_l\}$) are used as specified in the following theorem.

Theorem 1: For $\mathcal{SN}$, if there exists a set of transmitters

$$\mathcal{T} = \Big\{1, \{i \,\Big|\, |h^l_{1,i}|^2 \geq \max\{\frac{N^l}{N^e}|h^e_{1,j}|^2, |h^l_{1,n_l}|^2\}\}\Big\} \quad (9)$$

such that $n_r = |\mathcal{T}| - 1 \geq n_e$, the following secure aggregate rate is achievable :

$$\mathcal{R}_s^{DF,ZF,par} = \max_{\mathbf{B},\tilde{P}_1,\tilde{P}_u} \min_{j\in\mathcal{N}_e} \min\Big\{ \log\Big(\frac{N^e}{N^l}\frac{N^l + |h^l_{1,i^*}|^2\tilde{P}_1}{N^e + |h^e_{1,j}|^2\tilde{P}_1}\Big), \log\Big(\frac{N^e}{N^l}\frac{N^l + |h^l_{1,n_l}|^2\tilde{P}_1 + |\sum_{k\in\mathcal{T}} h^l_{k,n_l}\beta_k|^2\tilde{P}_u}{N^e + |h^e_{1,j}|^2\tilde{P}_1}\Big)\Big\} \quad (10)$$

where

$$i^* = \operatorname*{argmin}_{i\in\mathcal{T}\setminus\{1\}} |h_{1,i}| \quad (11)$$

$$\beta_k = \mathbf{B}(k) \qquad \text{where} \quad \mathbf{B} \in \mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}) \quad (12)$$

$$\tilde{P}_1 + \|\mathbf{B}\|_2^2\tilde{P}_u \leq \overline{P}_{tot} \quad (13)$$

in which $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}} \in \mathbb{C}^{n_e\times(n_r+1)}$ is the transmitters-eavesdroppers channel matrix whose (j,i)-th element is $h^e_{i,j}$ for $i \in \mathcal{T}, j \in \mathcal{N}_e$.

Remark 2: The first term in the right hand side of (10) shows the first stage of the transmission, where the source transmits the message securely to n_r legitimate nodes close enough to it (i.e., the nodes termed *relays*). These relays are determined in (9). The second term in the right hand side of (10) shows the second stage of the transmission, where the relays, in cooperation with the source, constitute a MISO toward the destination after applying ZF against the eavesdroppers to secure their transmission. Note that ZF can be only applied on the transmitted signals by the relays, while the transmitted signal of the source will be received by the eavesdroppers. This is why the $|h^e_{1,j}|^2\tilde{P}_1$ term appears in the denominator of the rates in (10).

Proof: First, we outline the coding strategy, based on a two-stage block Markov coding, i.e., all relays have the same priority for the source. In each block, the source sends the fresh message to *all* n_r relay nodes and uses Wyner wiretap coding to keep this part of the message secret from the eavesdroppers. At the same time, the source and the relays cooperate in sending the message of the previous block by coherently transmitting the related codeword. This coherent transmission enables them to use ZF against the eavesdroppers, by properly designed beamforming coefficients. As the cooperative codewords of the relays are fully zero-forced at all eavesdroppers, no Wyner wiretap coding is needed at the relays.

Now, to apply this coding strategy, first we provide achievable rate $\mathcal{R}_s^{DM,par}$ based on two-stage block Markov coding (parallel DF relaying) and Wyner wiretap coding for the general discrete memoryless channel in Lemma 1 (proof is provided in Appendix A). Then, we extend $\mathcal{R}_s^{DM,par}$ to the Gaussian channel in Lemma 2 and derive $\mathcal{R}_s^{DF,par}$ (proof in Appendix B). Finally, we apply ZF on $\mathcal{R}_s^{DF,par}$ to achieve the desired result, i.e., $\mathcal{R}_s^{DF,ZF,par}$. For simplicity in notation, let $\mathcal{N}_l = \{1,\ldots,n_l\}$, $\mathcal{T} = \{1,\ldots,n_r+1\}$ and $\mathcal{N}_e = \{1,\ldots,n_e\}$.

Lemma 1: For the general discrete memoryless counterpart of $\mathcal{SN}$, given by some conditional distribution $p(y^l_2,\ldots,y^l_{n_l},y^e_1\ldots,y^e_{n_e}|x_1,\ldots,x_{n_l})$, the secrecy capacity is lower-bounded by:

$$\mathcal{R}_s^{DM,par} = \sup \min_{j\in\mathcal{N}_e} \Big\{\min\{\min_{i\in\mathcal{T}\setminus\{1\}} I(U_1;Y^l_i|U), I(U,U_1;Y^l_{n_l})\} - I(U,U_1;Y^e_j)\Big\} \quad (14)$$

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

$$p(u,u_1)p(x_1,\ldots,x_{n_r+1}|u,u_1). \quad (15)$$

Now, we extend the above lemma to accommodate our model ($\mathcal{SN}$). Even for a simple channel with one relay and one eavesdropper, the optimal selection of the RVs in Lemma 1 (i.e., finding the optimal p.m.f of (15)) is an open problem [25]. Hence, we propose an appropriate suboptimal choice of input distribution, using Gaussian RVs, to achieve the following rate.

Lemma 2: The following secure aggregate rate is achievable for $\mathcal{SN}$:

$$\mathcal{R}_s^{DF,par} = \max_{\mathbf{B},\tilde{P}_1,\tilde{P}_u} \min_{j\in\mathcal{N}_e} \Big\{ \min\{ \min_{i\in[2:n_r+1]} \log\Big(1 + \frac{|h^l_{1,i}|^2\tilde{P}_1}{N^l}\Big), \log\Big(1 + \frac{|h^l_{1,n_l}|^2\tilde{P}_1 + |\sum_{k=1}^{n_r+1} h^l_{k,n_l}\beta_k|^2\tilde{P}_u}{N^l}\Big)\} - \log\Big(1 + \frac{|h^e_{1,j}|^2\tilde{P}_1 + |\sum_{k=1}^{n_r+1} h^e_{k,j}\beta_k|^2\tilde{P}_u}{N^e}\Big)\Big\} \quad (16)$$

where $\beta_k = \mathbf{B}(k)$ and $\tilde{P}_1 + \|\mathbf{B}\|_2^2\tilde{P}_u \leq \overline{P}_{tot}$.

Remark 3: The description of the rate terms is similar to Remark 2, with the difference that here ZF was not applied yet. Thus, the signals of the transmitter and the relays are received by the eavesdroppers.

It can easily be seen from (16) that to have a positive secrecy rate the source-relay links should be stronger than the source-eavesdropper links. Moreover, for the DF strategy to be better than point-to-point transmission the source-relay links should

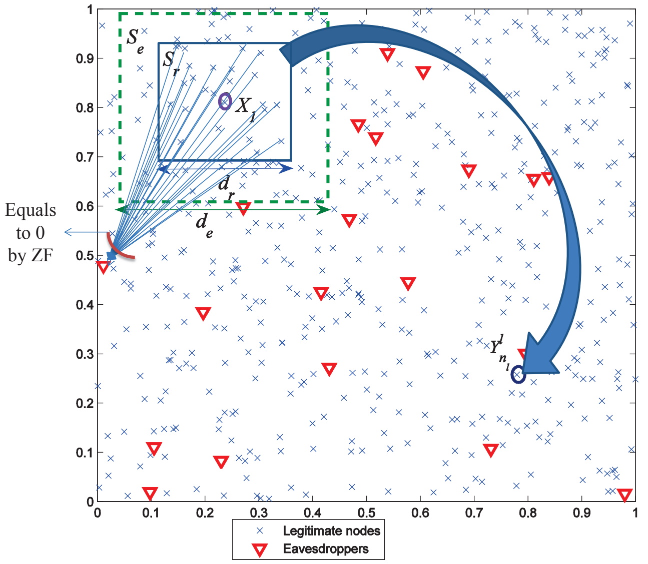

Fig. 1. Parallel relaying illustrated for a typical network model, a square of unit area; with 500 legitimate nodes and 20 eavesdroppers, placed according to PPP. The relaying square S_r of side d_r is shown with solid line and the eavesdropper-free square S_e of side d_e is shown with dashed line. The source (with channel input X_1) is at the center of S_r and S_e. We choose $\mathcal{T}$ as n_r+1 nodes in S_r. The destination node is shown with channel output $Y^l_{n_l}$. For brevity, ZF is only shown (solid lines originating S_r) in one eavesdropper.

be stronger than the direct source-destination link. Therefore, these two conditions "select" the n_r relay nodes in the DF strategy and, hence, the set of transmitters $\mathcal{T}(t)$ given by (9). Moreover, the condition in (11) is obtained by considering the inner $\min$ in (16).

Returning to (16), one should determine the beamforming coefficient vector $\mathbf{B}$. Finding the closed form solution is an open problem [28]. Thus, we consider a suboptimal strategy by applying ZF at all eavesdroppers and obtain

$$\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}\mathbf{B} = \mathbf{0} \tag{17}$$

where $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}$ is defined in Theorem 1. Hence, the coefficient vector $\mathbf{B}$ must lie in the null space of $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}$, as stated in (12). By applying (17) to (16), we achieve (10).

In order to ensure that there exists a non-trivial solution $\mathbf{B}$ for (17), the dimension of $\mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}})$ should be greater than zero or $rank(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}) \leq n_r$. Considering the worst-case scenario when $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}$ is a full rank matrix, the ZF strategy requires $n_e \leq n_r$. This condition is implied by the cardinality of the set of transmitters in (9). This means that to combat eavesdroppers, one needs at least the same number of nodes as relays in this scheme. Observing that the total power constraint (13) is already obtained in Lemma 2 completes the proof. ■

Step 2: We start by choosing two random nodes in the network as our source-destination pair. Recall that $n_l, n_e \rightarrow \infty$. By applying Lemma 9 (stated in Appendix C), n_l and n_e can be made arbitrarily close to λ_l and λ_e, respectively, with high probability (w.h.p). We define the *relaying* square S_r of side d_r, with the source at its center, as well as the *eavesdropper-free* square S_e of side d_e (illustrated in Fig. 1) such that:

$$d_r = \sqrt{\frac{n_r}{n_l}}, d_e = \sqrt{\frac{n_r}{n_l}}(\log n_e)^{\frac{\gamma}{2}} \text{ for some } \gamma > 0. \tag{18}$$

The next lemma shows the feasibility of these squares.

Lemma 3: As long as $n_l \geq n_e n_r \big(\log n_e\big)^{\gamma+\delta}$ for some $\gamma, \delta > 0$, the probability of having at least n_r legitimate nodes in S_r tends to 1, and the probability of having the eavesdropper-free square S_e can be made arbitrarily close to 1.

Proof: Using the fact that a Poisson process has Poisson increments, the number of nodes in S_r is a two-dimensional Poisson RV with parameter $\lambda_l d_r^2$, at least equals to n_r w.h.p (by applying (18) and (47)) as long as $\lambda_l d_r^2 \simeq n_r \rightarrow \infty$. This always holds because $n_r \geq n_e$. Similarly, the number of eavesdroppers in S_e is a Poisson RV with parameter $\lambda_e d_e^2 \simeq \frac{n_e n_r}{n_l}(\log n_e)^{\gamma}$, which converges to 0 by applying the condition stated in this lemma. Hence, the probability of having no eavesdropper in S_e, i.e., $e^{-\lambda_e d_e^2}$, can be made arbitrarily close to 1. ■

Step 3: Note that the number of relays, specified in the above lemma as $\frac{n_l}{n_e(\log n_e)^{\gamma+\delta}}$, should not be less than n_e. Now, we state the main result of this section and prove that the scaling of the nodes satisfies this constraint.

Theorem 2: In $\mathcal{SN}$ with fixed $\overline{P}_{tot}$ in (4), as long as $n_e^{\frac{\alpha}{2}+1}\big(\log(n_e)\big)^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$ holds for some positive γ, δ, w.h.p. an infinite secure aggregate rate $\mathcal{R}_s$ is achievable.

Proof: First, we randomly choose the source of the message and call it node 1. According to Lemma 3, squares S_r and S_e with sides defined in (18) exist w.h.p, with the source at their center. We randomly choose the destination and call it node n_l. If the destination is inside S_r, then the message is sent directly and no cooperation is needed. The reason is that, on the one hand, the distance between the source and the destination approaches zero by increasing the number of legitimate nodes and the eavesdroppers (i.e., the size of S_r in (18)). On the other hand, the eavesdroppers also get closer to the source and the destination (i.e., the size of S_e in (18)). However, the size of S_r decreases much faster than S_e. The model reduces to a wiretap channel with many eavesdroppers; the following rate, using Wyner wiretap coding at the source, is achievable:

$$\begin{aligned}\mathcal{R}_s^{WT} &= \min_{j\in\mathcal{N}_e} \log\Big(\frac{N^e}{N^l}\frac{N^l + |h^l_{1,n_l}|^2\tilde{P}_1}{N^e + |h^e_{1,j}|^2\tilde{P}_1}\Big) \\ &\overset{(a)}{\geq} \log\Big(\frac{N^e}{N^l}\frac{N^l + d_r^{-\alpha}\overline{P}_{tot}}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_{tot}}\Big) \\ &\overset{(b)}{\simeq} \log\Big((\frac{d_e}{d_r})^{\alpha}\Big) \overset{(c)}{\rightarrow} \infty \quad \text{as} \quad n_l \rightarrow \infty\end{aligned} \tag{19}$$

where (a) is obtained by considering (3), the definitions of S_r and S_e and by applying (4), (b) becomes $=$ in limit (when $n_l \rightarrow \infty$) and (c) holds due to (18). Otherwise, if the destination node is not in S_r, Lemma 3 implies that w.h.p. we can construct the set of transmitters in (9). Now, to make ZF possible we must show that $n_r = |\mathcal{T}| - 1 \geq n_e$. By applying the constraint of Lemma 3 with equality, we have

$$n_r = \frac{n_l}{n_e(\log n_e)^{\gamma+\delta}} \overset{(a)}{=} n_e^{\frac{\alpha}{2}}\big(\log n_e\big)^{\frac{\alpha}{2}\delta}\frac{n_l}{o(n_l)} \overset{(b)}{\geq} n_e$$

(a) is due to the scaling condition stated in this theorem and (b) is obtained because $\alpha \geq 2$. Now, we can use the strategy of Theorem 1 to achieve (10). To apply the total power constraint (13), in this case, we choose a fixed $\tilde{P}_1 = \overline{P}_1$ and set $\tilde{P}_u = \frac{\overline{P}_{tot} - \overline{P}_1}{\|\mathbf{B}\|_2^2}$. First, we consider the first term in (10), known as broadcast term (the secure rate from the source to n_r relay nodes in S_r), and derive its asymptotic behavior as

$$\log\Big(\frac{N^e}{N^l}\frac{N^l + |h^l_{1,i^*}|^2\tilde{P}_1}{N^e + |h^e_{1,j}|^2\tilde{P}_1}\Big) \overset{(a)}{\geq} \log\Big(\frac{N^e}{N^l}\frac{N^l + d_r^{-\alpha}\overline{P}_1}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\Big) \quad (20)$$
$$\overset{(b)}{\simeq} \log\Big((\frac{d_e}{d_r})^{\alpha}\Big) \overset{(c)}{\to} \infty \text{ as } n_l \to \infty$$

where (a) is obtained by considering (3) and the defined squares, (b) becomes $=$ in limit (when $n_l \to \infty$) and (c) is due to (18). As expected, the rate to each node in S_r is similar to the case where the destination is also in S_r; it can be made arbitrary large by decreasing the size of S_r as needed. Note that this decrease needs larger λ_l to have $n_r \geq n_e$ legitimate nodes in S_r to employ them as relays. Before continuing to the second term in (10), we take a closer look at the beamforming vector $\mathbf{B} \in \mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}})$. By applying Singular Value Decomposition (SVD), we have

$$\mathbf{H}_{\mathcal{N}_e,\mathcal{T}} = \mathbf{U}\mathbf{\Lambda}[\mathbf{\Upsilon}\mathbf{V}]^T;$$

$\mathbf{\Upsilon} \in \mathbb{C}^{(n_r+1)\times n_e}$ contains the first n_e right singular vectors corresponding to non-zero singular values, and $\mathbf{V} \in \mathbb{C}^{(n_r+1)\times(n_r-n_e+1)}$ contains the last $n_r - n_e + 1$ singular vectors corresponding to zero singular values of $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}$. The later forms an orthonormal basis for the null space of $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}$. Hence, $\mathbf{B}$ can be expressed as their linear combination, i.e.,

$$\mathbf{B} = \mathbf{V}\mathbf{\Phi}$$

where $\mathbf{\Phi} \in \mathbb{C}^{(n_r-n_e+1)}$ is an arbitrary vector selected by considering the power constraints in (13). Now, we consider the second term of (10), known as the multi-access term. This corresponds to the cooperative secure rate from the source and the n_r relays toward the destination.

$$\max_{\mathbf{B}} \log\Big(\frac{N^e}{N^l}\frac{N^l + |h^l_{1,n_l}|^2\tilde{P}_1 + |\sum_{k\in\mathcal{T}} h^l_{k,n_l}\beta_k|^2\tilde{P}_u}{N^e + |h^e_{1,j}|^2\tilde{P}_1}\Big)$$
$$\overset{(a)}{\geq} \max_{\mathbf{B}} \log\Big(\frac{2^{\alpha/4}N^e}{N^l}\frac{|\mathbf{1}^\dagger\mathbf{B}|^2\cdot\frac{\overline{P}_{tot}-\overline{P}_1}{\|\mathbf{B}\|_2^2}}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\Big)$$
$$= \max_{\mathbf{\Phi}^\dagger\mathbf{\Phi}\leq\|\mathbf{B}\|_2^2} \log\Big(\frac{2^{\alpha/4}N^e}{N^l}\frac{\mathbf{\Phi}^\dagger\mathbf{V}^\dagger\mathbf{1}\mathbf{1}^\dagger\mathbf{V}\mathbf{\Phi}\cdot\frac{\overline{P}_{tot}-\overline{P}_1}{\|\mathbf{B}\|_2^2}}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\Big)$$
$$= \log\Big(\frac{2^{\alpha/4}N^e}{N^l}\frac{\lambda_{max}(\mathbf{V}^\dagger\mathbf{1}\mathbf{1}^\dagger\mathbf{V})\cdot(\overline{P}_{tot}-\overline{P}_1)}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\Big)$$
$$= \log\Big(\frac{2^{\alpha/4}N^e}{N^l}\frac{\|\mathbf{1}^\dagger\mathbf{V}\|_2^2\cdot(\overline{P}_{tot}-\overline{P}_1)}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\Big)$$
$$\overset{(b)}{=} \log\Big(\frac{2^{\alpha/4}N^e}{N^l}\frac{(n_r+1)\frac{1+\cos 2\theta}{2}\cdot(\overline{P}_{tot}-\overline{P}_1)}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\Big)$$
$$\underset{n_l\to\infty}{\overset{(c)}{=}} \log\Big(\kappa\frac{(n_r+1)}{d_e^{-\alpha}}\Big) \overset{(d)}{\to} \infty \quad \text{as} \quad n_l \to \infty \quad (21)$$

(a) holds since $d^l_{k,n_l} \leq \sqrt{2}$ and $\mathbf{1} \in \mathbb{C}^{(n_r+1)}$ is the all one vector. In (b), θ is an RV denotes the angle between $\mathbf{1}$ and $\mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}})$ and has a continuous distribution on $[0, 2\pi]$ due to the randomness of $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}$. In (c), κ is a constant. (d) is obtained by substituting (18) and $n_r = \frac{n_l}{n_e(\log n_e)^{\gamma+\delta}}$ and by applying the scaling $n_e^{\frac{\alpha}{2}+1}(\log(n_e))^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$ for some positive γ, δ. This completes the proof. ∎

Remark 4: (21)-(b) implies that the transmitted beamforming vector $\mathbf{B}$ is not orthogonal to the channel vector from the transmitters to the destination. As $\mathbf{B} \in \mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}})$, consider two cases: (i) $\dim(\mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}})) > 1$: the beamforming vector $\mathbf{B}$ can be chosen in a way that is not orthogonal to the to the channel vector from the transmitters to the destination. (ii) $\dim(\mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}})) = 1$: we set $\mathbf{B} = \mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}})$. Here, the channel vector from the transmitters to the destination must not be orthogonal to $\mathbf{B}$, because the legitimate nodes are distributed according to a poisson point process and thus the angles of their channel vectors angles have continuous distributions.

IV. Serial Relaying

In this section, we improve the scaling of the number of eavesdroppers we can defend against at the expense of a more complicated strategy, serial (multi-stage) relaying. The network is divided into clusters, with the nodes in each cluster acting as a group of relays and, at the same time, collectively applying ZF (essentially acting as a distributed multi-antenna). These clusters perform *ordered* DF: the nodes in each cluster decode the transmitted signals of all previous clusters. We use the three-step approach outlined in Section III to obtain our result here. We show that unbounded secure aggregate rate for a fixed total power can be achieved as long as $n_e^2(\log n_e)^\gamma = o(n_l)$ holds for some positive γ.

Step 1: Achievability is given in the following theorem.

Theorem 3: For $\mathcal{SN}$, the following secure aggregate rate is achievable:

$$\mathcal{R}_s^{DF,ZF,ser} = \quad (22)$$
$$\min_{i\in[1:n_l-1]} \max_{\mathbf{B}_i,\tilde{P}_i} \min_{j\in\mathcal{N}_e} \log\Big(\frac{N^e}{N^l}\frac{N^l + \sum_{q=1}^{i}|\sum_{k=1}^{q} h^l_{k,i+1}\beta'_{kq}|^2\tilde{P}_q}{N^e + |h^e_{1,j}|^2\tilde{P}_1}\Big)$$

in which

$$\beta'_{kq} = \mathbf{B}_q(k) \quad \text{and} \quad \beta'_{kq} = 1 \quad \text{if} \quad k = q \quad (23)$$
$$\mathbf{B}_q \in \mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}) \quad \text{for} \quad q \bmod n_e = 1 \quad (24)$$
$$\tilde{P}_q = \begin{cases} \overline{P}_q & \text{if } q \bmod n_e = 1 \\ 0 & \text{if } q \bmod n_e \neq 1 \end{cases} \quad (25)$$
$$\sum_{q=1}^{n_l-1} \|\mathbf{B}_q\|_2^2\tilde{P}_q \leq \overline{P}_{tot} \quad (26)$$

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

Proof: We use a $(n_l - 1)$-stage block Markov coding by making the nodes relay the message with ordered priorities. Considering the ordered set for the legitimate nodes, i.e., $\mathcal{N}_l = \{1, \ldots, n_l\}$, each node i decodes the transmitted signal of all previous nodes (1 to $i-1$) in this order and sends its signal to the subsequent nodes. In order to pipeline communication, (n_l-1)th order block Markov correlated codes are proposed. Therefore, in each block, the received signals at the legitimate nodes are coherent [40]. To apply ZF at the eavesdroppers, we show it is necessary to have clusters of enough relays, where the nodes in each cluster have the same priority compared to the source. Wyner wiretap coding is also utilized at the source. First, we use the multi-stage block Markov coding (serial DF relaying) and Wyner wiretap coding to obtain $\mathcal{R}_s^{DM,ser}$ in Lemma 4 (proof provided in Appendix D) and extend it to $\mathcal{R}_s^{DF,ser}$ for the Gaussian channel in Lemma 5 (proof in Appendix E). Then, by applying ZF on $\mathcal{R}_s^{DF,ser}$ we derive $\mathcal{R}_s^{DF,ZF,ser}$.

Lemma 4: Consider the channel model of Lemma 1 and let $\pi(\cdot)$ be a permutation on $\mathcal{N}_l=\{1,\dots,n_l\}$, where $\pi(1)=1$, $\pi(n_l)=n_l$ and $\pi(m:n)=\{\pi(m),\pi(m+1),\dots,\pi(n)\}$. The secrecy capacity is lower-bounded by:

$$\mathcal{R}_s^{DM,ser}=\sup\min_{j\in\mathcal{N}_e}\max_{\pi(\cdot)}\min_{i\in[1:n_l-1]} I(U_{\pi(1:i)};Y^l_{\pi(i+1)}|U_{\pi(i+1:n_l-1)})-I(U_{\pi(1:n_l-1)};Y^e_j)$$

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

$$p(u_1,\dots,u_{n_l-1})\prod_{k=1}^{n_l-1}p(x_k|u_k). \tag{27}$$

Similar to the parallel relaying case, we choose an appropriate suboptimal input distribution in the following lemma.

Lemma 5: For $\mathcal{SN}$, the following is an achievable secure aggregate rate:

$$\mathcal{R}_s^{DF,ser}=\min_{i\in[1:n_l-1]}\max_{\mathbf{B}_i,\tilde{P}_i}\min_{j\in\mathcal{N}_e}\log\Big(1+\frac{\sum_{q=1}^{i}|\sum_{k=1}^{q}h^l_{k,i+1}\beta'_{kq}|^2\tilde{P}_q}{N^l}\Big)-\log\Big(1+\frac{\sum_{q=1}^{n_l-1}|\sum_{k=1}^{q}h^e_{k,j}\beta'_{kq}|^2\tilde{P}_q}{N^e}\Big) \tag{28}$$

where (23) and (26) hold.

For the serial relaying scheme, as the achievable rate is not limited by the decoding constraint at the farthest relay, all nodes in the network (except the source and destination) can be used as the relay nodes. Therefore, the transmission set can be $\mathcal{T}=\{1,\dots,n_l-1\}$ where the relays are assumed to be in a certain order, e.g., based on their distances to the source node. Similar to Section III, we apply ZF at all eavesdroppers to determine the beamforming coefficient vectors $\mathbf{B}_q$ by setting $\sum_{q=2}^{n_l-1}|\sum_{k=1}^{q}h^e_{k,j}\beta'_{kq}|^2\tilde{P}_q=0,\forall j\in\mathcal{N}_e$. This results in $\tilde{P}_q=0$ or

$$E(q,j)=\sum_{k=1}^{q}h^e_{k,j}\beta'_{kq}=0,$$

for $\forall q\in[2:n_l-1]$. Now consider (50) to obtain $X_k=\tilde{U}_k+\beta_kX_{k+1}$ where $\beta'_{kq}=\prod_{m=k}^{q-1}\beta_m$. Therefore, $E(q_0,j)$ and

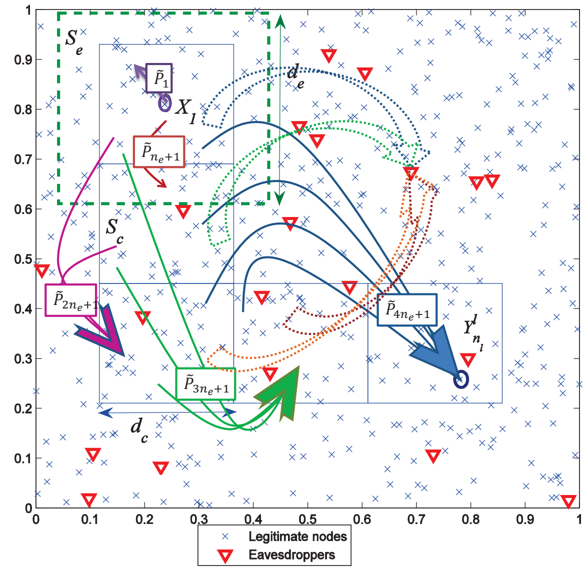

Fig. 2. Clusters (squares S_c, thin solid line) of side d_c used for serial relaying. The nodes in each cluster, c, coherently with nodes in all previous clusters and $i-c$ subsequent clusters send $\tilde{P}_{in_e+1}$ to the nodes in cluster $i+1$ for $i\geq c$. Each dotted arrow shows the received signals at one eavesdropper from all nodes in each cluster; these are equal to zero thanks to ZF.

$E(q_0+1,j)$ only differ in one variable, i.e., β_{q_0+1}. However, we need $E(q,j)=0,\forall j\in\mathcal{N}_e$ if $\tilde{P}_q>0$, which is clearly not possible. Therefore, we apply ZF by allocating power as per (25) and $E(q,j)=0,\text{if } q \bmod n_e=1,\forall j\in\mathcal{N}_e$. Thus, we obtain $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}\mathbf{B}_q=\mathbf{0}$ shown in (24) ($\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}$ is defined in Theorem 3). By applying (24) on (28), we achieve (22). This means that to overcome n_e eavesdroppers using the proposed strategy, one node in every n_e legitimate nodes should transmit fresh information and the n_e nodes who transmit the same information in each block should apply beamforming to ZF at all eavesdroppers. ■

Step 2: Consider Fig. 2 and assume $c_{\max}$ clusters (squares) S_c of same side d_c; the source is located in the first and the destination in the last cluster; any two successive clusters share one side. Hence, we have $c_{\max}\leq\frac{2}{d_c}$. We show $c_{\max}$ does not affect the asymptotic behavior of $\mathcal{R}_s$. Assuming the strategy of Step 1, all the nodes in each cluster S_c transmit the same fresh information. Now, consider an eavesdropper-free square S_e of side d_e around the source. We define

$$d_c=\sqrt{\frac{n_c}{n_l}},d_e=\sqrt{\frac{n_c}{n_l}}(\log n_e)^{\frac{\gamma}{2}}\text{ for some }\gamma>0 \tag{29}$$

where n_c is determined in Lemma 6 which shows the feasibility of these squares and can be proved similar to Lemma 3.

Lemma 6: As long as $n_en_c(\log n_e)^{\gamma}=o(n_l)$ for some $\gamma>0$, the probability of having at least $n_c\to\infty$ legitimate nodes in S_c tends to 1, and the probability of having no eavesdropper in square S_e can be made arbitrarily close to 1.

We remark that to apply ZF at all eavesdroppers, the number of nodes in each cluster, i.e., n_c, should not be less than n_e.

Step 3: Now, we state the main result of this section.

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

Proof: Choosing the source and the destination is same as proof of Theorem 2. If the destination is inside the square S_c, the message is sent directly to it using Wyner wiretap coding at the source. Similar to (19), since $\frac{d_e}{d_c} \to \infty$ as $n_l \to \infty$, in this case an unbounded rate is achievable. Otherwise (the destination is outside S_c), we choose $n_c = n_e+1$ and consider $c_{\max}$ clusters as described in the previous step. Substituting $n_c = n_e + 1$ into the scaling of Lemma 6 results in scaling of this theorem. As $n_c \geq n_e$, w.h.p ZF can be applied and the rate of Theorem 3 is achievable. If we consider equal power allocation for the fresh information in the total power constraint (26), we obtain

$$\tilde{P}_q = \frac{\overline{P}_{tot}}{\sum_{c=0}^{c_{\max}} \|\mathbf{B}_{cn_e+1}\|_2^2} = \overline{P}_q = \overline{P},$$

if $q \bmod n_e = 1$ and $q \leq c_{\max} n_e + 1$. Otherwise ($q \bmod n_e \neq 1$), $\tilde{P}_q = 0$. Note that we consider an ordered set of legitimate nodes based on the cluster numbers, which can be done w.h.p according to Lemma 6. Now, we show that (22) can be unbounded w.h.p for all $i \in [1 : n_l - 1], j \in \mathcal{N}_e$ and $\mathbf{B}_q$s that satisfy (23) and (24). First, we consider $i \leq n_e + 1$ that comprises the nodes in the first cluster:

$$\begin{aligned}\mathcal{R}_s^{DF,ZF,ser} &\overset{(a)}{=} \log\Big(\frac{N^e}{N^l}\frac{N^l + |h^l_{k,i+1}|^2\overline{P}_1}{N^e + |h^e_{1,j}|^2\overline{P}_1}\Big) \\ &\overset{(b)}{\geq} \log\Big(\frac{N^e}{N^l}\frac{N^l + d_c^{-\alpha}\overline{P}_1}{N^e + d_e^{-\alpha}\overline{P}_1}\Big) \to \infty \quad \text{as} \quad n_l \to \infty\end{aligned} \tag{30}$$

where (a) is due to (25) and (b) is obtained by considering (3) and the defined squares in (29). This rate is similar to the one we have in (20). In fact, one expects that this rate can be made arbitrary large if we choose S_c small enough (by increasing the density of nodes). In parallel relaying, the problem with the second term in (10) is the fixed non-decreasing distance between the nodes in S_r and the destination. We here overcome this problem by considering clusters such that the maximum distance between the nodes in two adjacent clusters is $\sqrt{5}d_c$. Therefore, for the nodes in cluster c, i.e., $cn_e + 1 \leq i \leq (c+1)n_e$, we set $q = cn_e + 1$:

$$\begin{aligned}\mathcal{R}_s^{DF,ZF,ser} &\geq \log\Big(\frac{N^e}{N^l}\frac{N^l + |\sum_{k=1}^{q} h^l_{k,i+1}\beta'_{kq}|^2\tilde{P}_q}{N^e + |h^e_{1,j}|^2\tilde{P}_1}\Big) \\ &\overset{(a)}{=} \log\Big(\frac{N^e}{N^l}\frac{N^l + |\mathbf{h}_q^T\mathbf{B}_q|^2\overline{P}}{N^e + |h^e_{1,j}|^2\overline{P}}\Big) \\ &\underset{n_l\to\infty}{\overset{(b)}{\geq}} \log\Big((\frac{d_e}{d_c})^\alpha\Big) \overset{(c)}{\to} \infty \quad \text{as} \quad n_l \to \infty\end{aligned} \tag{31}$$

(a) is obtained by defining $\mathbf{h}_q = [h^l_{1,i+1}, \ldots, h^l_{q,i+1}]^T$. (b) follows from the steps similar to (21) and from noting that $\|\mathbf{B}_q\|_2^2 \geq \mathbf{B}_q(q) = \beta'_{qq} = 1$, $\|\mathbf{h}_q\|_2^2 \geq |h^l_{q,i+1}|^2 \geq d_c^{-\alpha}$ and the randomness of $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}$. (c) is due to (29). This completes the proof. ■

V. Colluding Eavesdroppers

In this section, we focus on the case of perfect-colluding eavesdroppers and propose a relaying-based scheme that achieves zero-cost secure communication provided that the number of eavesdroppers is less than a tolerable limit. In fact, we show that if $n_e^{(2+\frac{2}{\alpha})}\big(\log n_e\big)^\gamma = o(n_l)$ 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 Section IV to the colluding case, 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 5 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 7, under which the achievability results of Theorem 5 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 6). 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). The proof is provided in Appendix F.

Theorem 5: For $\mathcal{SN}$-PCE, the following secure aggregate rate is achievable:

$$\mathcal{R}_s^{ZF} = \min_{i\in[1:n_l-1]} \max_{\mathbf{B}_i,\tilde{P}_i} \log\Big(\frac{N^e}{N^l}\frac{N^l + \sum_{q=1}^{i}|\sum_{k=1}^{q} h^l_{k,i+1}\beta'_{kq}|^2\tilde{P}_q}{N^e + \sum_{j\in\mathcal{N}_e}|h^e_{1,j}|^2\tilde{P}_1}\Big) \tag{32}$$

in which

$$\beta'_{kq} = \mathbf{B}_q(k) \quad \text{and} \quad \beta'_{kq} = 1 \quad \text{if} \quad k = q \tag{33}$$

$$\mathbf{B}_q \in \mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}) \quad \text{for} \quad q \bmod n_e = 1 \tag{34}$$

$$\tilde{P}_q = \begin{cases} \overline{P}_q & \text{if } q \bmod n_e = 1 \\ 0 & \text{if } q \bmod n_e \neq 1 \end{cases} \tag{35}$$

$$\sum_{q=1}^{n_l-1} \|\mathbf{B}_q\|_2^2\tilde{P}_q \leq \overline{P}_{tot} \tag{36}$$

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 $h^e_{i,j}$, for $i \in [1 : q], j \in \mathcal{N}_e$.

Step 2: Now, we specify the details of our strategy and derive the constraints on the number of legitimate nodes and eavesdroppers in Lemma 7 (to apply the scheme of Theorem 5 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

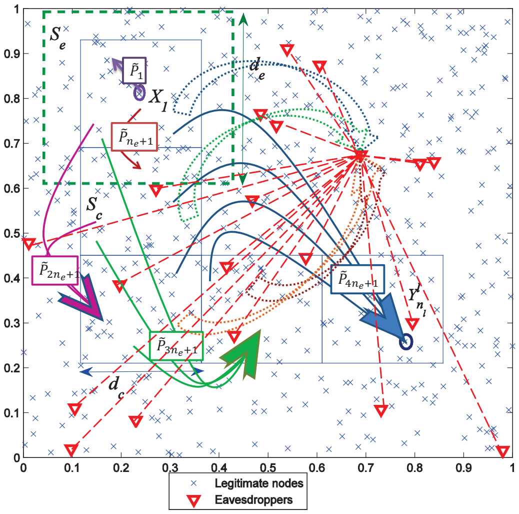

Fig. 3. The squares are same as the ones in Fig. 2. Here, the dashed lines (only shown for one eavesdropper) show the free access of the eavesdroppers to all observations.

Lemma 9 (stated in Appendix C) 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. 3); 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 $c_{\max} \leq \frac{2}{d_c}$. 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:

$$d_c = \sqrt{\frac{n_c}{n_l}}, d_e = n_e^{\frac{1}{\alpha}} \sqrt{\frac{n_c}{n_l}} (\log n_e)^{\frac{\gamma}{2}} \text{ for some } \gamma > 0 \quad (37)$$

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

Lemma 7: 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 Lemma 9 (stated in Appendix C) on (37) 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 (37) 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. ∎

Step 3: Now, we state our main result of this section.

Theorem 6: 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 $n_e^{(2+\frac{2}{\alpha})} \big(\log n_e\big)^{\gamma} = o(n_l)$ holds for some positive γ.

Proof: Randomly choose the source-destination pair; let the source be node 1 and the destination node n_l; design the squares S_c and S_e as per (37) (around the source), which exist w.h.p due to Lemma 7. 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 7. 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:

$$\begin{aligned} \mathcal{R}_s^{WT} &= \log\Big(\frac{N^e}{N^l}\frac{N^l + |h^l_{1,n_l}|^2\tilde{P}_1}{N^e + \sum\limits_{j\in\mathcal{N}_e}|h^e_{1,j}|^2\tilde{P}_1}\Big) \qquad (38)\\ &\overset{(a)}{\geq} \log\Big(\frac{N^e}{N^l}\frac{N^l + d_c^{-\alpha}\overline{P}_{tot}}{N^e + n_e(\frac{d_e}{2})^{-\alpha}\overline{P}_{tot}}\Big) \overset{(b)}{\to} \infty \quad \text{as} \quad n_l \to \infty \end{aligned}$$

where (a) follows from (3) and (4) (by considering the concepts of S_c and S_e squares); (b) follows from (37).

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 of Lemma 7, 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 5. Now, we allocate the power equally to the fresh information based on the total power constraint (36). 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 (32) and investigate its asymptotic behavior for all $i \in [1 : n_l - 1]$ and $\mathbf{B}_q$s that satisfy (33) and (34). First, we consider the nodes in the first cluster by letting $i \leq n_e + 1$:

$$\begin{aligned} \mathcal{R}_s^{ZF} &\overset{(a)}{=} \log\Big(\frac{N^e}{N^l}\frac{N^l + |h^l_{k,i+1}|^2\overline{P}_1}{N^e + \sum\limits_{j\in\mathcal{N}_e}|h^e_{1,j}|^2\overline{P}_1}\Big) \qquad (39)\\ &\overset{(b)}{\geq} \log\Big(\frac{N^e}{N^l}\frac{N^l + d_c^{-\alpha}\overline{P}_1}{N^e + n_e d_e^{-\alpha}\overline{P}_1}\Big) \to \infty \quad \text{as} \quad n_l \to \infty \end{aligned}$$

(a) follows from the power allocation as in (35). (b) follows from the network model in (3) and the clustering (squares) concept with the sizes as per (37). The intuition is to make the cluster S_c small 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 (36).

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 $\sqrt{5}d_c$.

$$\begin{aligned}
\mathcal{R}_s^{ZF} &= \max_{\mathbf{B}_i} \log\Big(\frac{N^e}{N^l}\frac{N^l + |\sum_{k=1}^{q} h^l_{k,i+1}\beta'_{kq}|^2\tilde{P}_q}{N^e + \sum_{j\in\mathcal{N}_e}|h^e_{1,j}|^2\tilde{P}_1}\Big)\\
&\overset{(a)}{=} \max_{\mathbf{B}_q}\log\Big(\frac{N^e}{N^l}\frac{N^l + |\mathbf{h}_q^\dagger\mathbf{B}_q|^2\overline{P}}{N^e + \sum_{j\in\mathcal{N}_e}|h^e_{1,j}|^2\overline{P}}\Big)\\
&= \max_{\mathbf{\Phi_q}^\dagger\mathbf{\Phi_q}\leq\|\mathbf{B}_q\|_2^2}\log\Big(\frac{N^e}{N^l}\frac{N^l + \mathbf{\Phi}_q^\dagger\mathbf{V}_q^\dagger\mathbf{h}_q\mathbf{h}_q^\dagger\mathbf{V}_q\mathbf{\Phi}_q\overline{P}}{N^e + \sum_{j\in\mathcal{N}_e}|h^e_{1,j}|^2\overline{P}}\Big)\\
&= \log\Big(\frac{N^e}{N^l}\frac{N^l + \|\mathbf{B}_q\|_2^2\lambda_{max}(\mathbf{V}_q^\dagger\mathbf{h}_q\mathbf{h}_q^\dagger\mathbf{V}_q)\overline{P}}{N^e + \sum_{j\in\mathcal{N}_e}|h^e_{1,j}|^2\overline{P}}\Big)\\
&= \log\Big(\frac{N^e}{N^l}\frac{N^l + \|\mathbf{B}_q\|_2^2\|\mathbf{h}_q^\dagger\mathbf{V}_q\|_2^2\overline{P}}{N^e + \sum_{j\in\mathcal{N}_e}|h^e_{1,j}|^2\overline{P}}\Big)\\
&\underset{n_l\to\infty}{\overset{(b)}{\geq}} \log\Big(\frac{1}{n_e}(\frac{d_e}{d_c})^\alpha\Big) \overset{(c)}{\to} \infty \quad \text{as} \quad n_l\to\infty
\end{aligned} \tag{40}$$

(a) is obtained by defining $\mathbf{h}_q = [h^l_{1,i+1},\ldots,h^l_{q,i+1}]^T$. (b) follows from $\|\mathbf{B}_q\|_2^2 \geq \mathbf{B}_q(q) = \beta'_{qq} = 1$, $\|\mathbf{h}_q\|_2^2 \geq |h^l_{q,i+1}|^2 \geq d_c^{-\alpha}$, $\|\mathbf{V}_q\|_2^2 = 1$ and the randomness of $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}^q}$ and $\mathbf{h}_q$. (c) is due to (37). This completes the proof. ■

VI. Discussion and Conclusion

Comparison to existing results: In general, we can define the cost of secure communication as $\mathfrak{C}_s = \frac{\overline{P}_{tot}}{\mathcal{R}_s}$. In prior works [9]–[13], due to the individual power constraint (the transmission power for each node is fixed), $\overline{P}_{tot}$ scales linearly with the number of nodes. Therefore, the scaling for the cost of secure communication lies in $[\sqrt{n}, n]$ and $\mathfrak{C}_s \to \infty$ as $n\to\infty$. Here, we showed that cooperation based schemes can achieve secure communication with cost that goes to 0 as the number of nodes goes to ∞. This is so because we use a fixed $\overline{P}_{tot}$. 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. Moreover, the scaling of Theorem 4 can be written as $\frac{n_e}{n_l} = o\Big(\big(n_e(\log n_e)^\gamma\big)^{-1}\Big) \simeq o(n_e^{-1})$. To compare the scalings, one must compare $(\log n_l)^2$ (for result of [9]) with n_e (for our result), which seems to have the same order. For example, $n_e = \log n_l$ satisfies both scalings.

Zero cost communication *with no secrecy constraint* was achieved in [7]. Note that our strategy tolerates n_e eavesdroppers satisfying the constraints in Table I. Hence, compared to [7], this means that this number of eavesdroppers does not affect the scaling of communication cost.

Upper bound: To see how the secrecy constraint affects the achievable aggregate rate as well as to show how our proposed schemes work, we present a cut-set based upper bound by ignoring the secrecy constraint. It is worth noting that the upper bounds of [7] cannot be applied immediately to our case due to the difference in the network model. In fact, a planar regular extended network is considered in [7], compared to our dense network model with nodes distributed according to PPP (same as the one considered in [9]). Also, for simplicity we assume that $N^l = 1$. Note that we consider the multiple-unicast scenario as described in Section II.

Lemma 8: In $\mathcal{SN}$ with fixed $\overline{P}_{tot}$ in (4), when $n_l, n_e \to \infty$, the secure aggregate rate $\mathcal{R}_s$ is upper bounded as:

$$\mathcal{R}_s \leq \log\big(1 + \overline{P}_{tot}n_l^{\alpha+\varepsilon+1}\big) \tag{41}$$

for any $\theta > 0$.

Proof: We first relax the secrecy constraint and assume no eavesdropper presents. As Section II, the transmitter X_1 sends message $m_1 \in \mathcal{M}_1 = [1 : 2^{nR_s}]$ to the receiver $Y^l_{n_l}$ with the help of nodes in $\mathcal{N}_l\setminus\{1, n_l\}$. We consider the cut-set around the receiver node (i.e., the n_l-th legitimate node) and we follow the same lines as in the proof of [7, Lemma 4.1] to obtain the following upper bound:

$$\begin{aligned}
\mathcal{R}_s &\leq \frac{1}{n}\sum_{t=1}^{n}\log\big(1 + E[|\sum_{k\in\mathcal{N}_l\setminus\{n_l\}} h^l_{k,n_l}X_k(t)|^2]\big)\\
&\overset{(a)}{=} \frac{1}{n}\sum_{t=1}^{n}\log\big(1 + E[|\mathbf{1}^\dagger\tilde{\mathbf{X}}(\mathbf{t})|^2]\big)\\
&= \frac{1}{n}\sum_{t=1}^{n}\log\big(1 + E[\tilde{\mathbf{X}}^\dagger(\mathbf{t})\mathbf{1}\mathbf{1}^\dagger\tilde{\mathbf{X}}(\mathbf{t})]\big)
\end{aligned}$$

where in (a) we set $\tilde{\mathbf{X}}(\mathbf{t})(k) = h^l_{k,n_l}X_k(t)$. Now, we further relax the problem and assume that all the transmitters are located at the distance of the closest node to the receiver. Similar to the proof of Lemma 3, it can be shown that the distance of closest node to the receiver almost surely is greater than $n_l^{-(1+\vartheta)}$. Using this distance to lower-bound the distance (and thus to upper-bound the rate), we obtain:

$$\begin{aligned}
\mathcal{R}_s &\overset{(a)}{\leq} \log\big(1 + n_l^{\alpha+\theta}\overline{P}_{tot}\lambda_{\max}(\mathbf{1}\mathbf{1}^\dagger)\big)\\
&\overset{(b)}{\leq} \log\big(1 + \overline{P}_{tot}n_l^{\alpha+\varepsilon+1}\big)
\end{aligned}$$

where (a) follows from the power constraint in (4); the Jensen's inequality using the concavity of log function and setting $\varepsilon = \alpha\vartheta$ and (b) follows since $\lambda_{\max}(\mathbf{1}\mathbf{1}^\dagger) = n_l - 1$. ■

TABLE I

	Non-colluding	Colluding
Interference-limited [9], $\mathfrak{C}_s \to \infty$	$\frac{n_e}{n_l} = o\big((\log n_l)^{-2}\big)$	$\frac{n_e}{n_l} = O\big((\log n_l)^{-2-\rho}\big), \rho > 0$
Cooperative, $\mathfrak{C}_s \to 0$	Theorem 4: $n_e^2(\log n_e)^{\gamma} = o(n_l)$	Theorem 6: $n_e^{(2+\frac{2}{\alpha})}(\log n_e)^{\gamma} = o(n_l), \gamma > 0$

In our coding schemes the achievable secure aggregate rate is lower bounded as either $\log\big((\log n_e)^{\frac{\alpha\gamma}{2}}\big)$ (in (20), (30) and (31)) or $\log\left(\frac{n_l}{n_e^{\frac{\alpha}{2}+1}(\log n_e)^{\gamma+\delta(\frac{\alpha}{2}+1)}}\right)$ (in (21)). Comparing these bounds with the upper bound in (41), the difference is two-fold: (i) The information leakage rate (the minus term) in the secure capacity is ignored to derive (41). (ii) The number of transmitters (and so their distances) are limited due to the eavesdroppers. For instance, we need at least n_e transmitters to transmit the *same* data to be able to zero force successfully at the eavesdroppers.

Now, we focus on the serial relaying scheme for further discussion. Similar arguments can be made for the parallel relaying scheme. To achieve the secure aggregate rate that scales as $\log(n_l^{\alpha+\varepsilon+1})$ (similar to (41)), one must set $d_e = n_c n_l^{\alpha+\varepsilon+\frac{1}{2}}$ in (29). This violates the Lemma 6 for all $\frac{n_l}{n_e}$ and thus the rate of (41) is not achievable. However, in the following corollary we show that by tolerating less eavesdropper (compared with $n_e^2(\log n_e)^{\gamma} = o(n_l)$) a better scaling for the secure aggregate rate can be achieved (compared with $\log\big((\log n_e)^{\frac{\alpha\gamma}{2}}\big)$).We also remark that our the serial relaying scheme can be reduced to the coherent multistage relaying with interference subtraction (CRIS) scheme of [7] in case of no secrecy (and thus achieves a similar scaling behavior but adapted to dense randomly setup).

Corollary 1: In $\mathcal{SN}$ with fixed total power $\overline{P}_{tot}$ in (4), as long as $n_e^{2(2+\alpha+\varepsilon)} = o(n_l)$ holds for some positive ε, w.h.p. $\mathcal{R}_s$ scales as $\log(n_e^{\alpha+\varepsilon+1})$ (i.e., infinite secure aggregate rate).

Proof: The proof is same as the proof of Theorem 4 by setting $d_e = \sqrt{\frac{n_c}{n_l}} n_e^{\alpha+\varepsilon+1}$. ■

Parallel vs. serial relaying: The difference in the derived scaling for the number of tolerated eavesdroppers in two relaying schemes comes from ensuring that the transmitters and receivers in the adjacent clusters are close enough. In fact, in the serial relaying scheme, the nodes in each cluster receive signal from the nodes in all the previous clusters, in particular from their adjacent cluster. Hence, in all transmission stages the distance between (at least one) transmitter and receiver goes to zero (as the size of clusters decreases by increasing the number of nodes). Therefore, the scaling of $\mathcal{R}_s$ is only like $\log\left((\frac{d_e}{d_c})^{\alpha}\right)$ and there is no MISO type rate (like (21)); which appears in the parallel relaying because of fixed (non-decreasing) distance between the transmitter and the receiver. Apart from the difference in the derived scaling for the number of tolerated eavesdroppers, our two schemes differ in terms of the individual power allocation. The parallel relaying scheme uses fewer relay nodes than the serial scheme. Hence, a larger fraction of $\overline{P}_{tot}$ is allocated per node. Therefore, serial relaying may be suitable for power-limited applications, with strict per node power constraints. For both schemes, the per node allocated power vanishes as the number of nodes increases but with different asymptotic behavior.

Channel State Information (CSI): In our network model ($\mathcal{SN}$ and $\mathcal{SN}$-PCE, notably (3)), CSI is equivalent to node location information. CSI for legitimate nodes can be obtained in practice (e.g., pilot symbols, feedback). The challenge is to obtain the eavesdroppers' CSI. We assume global CSI is available, a common assumption in most of the physical layer security schemes (e.g., [25], [26]). DF relaying can be applied without the eavesdroppers' CSI as it only needs the location of the closest eavesdropper. However, to design the beamforming coefficients for ZF, full CSI is necessary. Due to the complexity of the problem, this idealistic assumption allows to gain valuable insights. Obviously, the next step we consider as a future work is to investigate the problem when less or no eavesdroppers' CSI is available. Less CSI means knowledge of the eavesdroppers' channel statistics or imperfect estimates. In practice, these assumptions are appropriate in some scenarios, e.g., public safety, where some areas are less likely to have eavesdroppers. For imperfect CSI estimation, the authors in [28] showed that the achievable secrecy rate depends on the estimation error covariance matrix. Moreover, [42] concludes that to achieve secure rate in wireless networks one needs little CSI. We contrast our result of achieving infinite rate with known eavesdropper CSI/location, to the results for the *interference-limited* channel model: if the location of eavesdroppers is unknown [11]–[13], the achievable rate is of order 1.

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 [9], [10]. Recently, investigating the ramifications of the collusion models, the *Wiretap Channel with Constrained Colluding Eavesdroppers* (WTC-CCE) was proposed [43]: 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 A
Proof of Lemma 1

Proof: The proof is based on the random coding scheme, which combines Csiszar and Korner's scheme [18] and DF strategy (two-stage block Markov superposition coding). For decoding at the receivers we utilize backward decoding [4].[1]

[1]This scheme first proposed for a relay-eavesdropper channel in [23] and extended to multiple relays with an eavesdropper in [25].

We prove the theorem by using the replacement X_1 for U_1 and then the general case can be proved using a memoryless prefix channel as [23]. Also, as mentioned in Remark 1, we assume $\mathcal{R}_s = R_1$. Consider a block Markov encoding scheme with B blocks of transmission, each of n symbols. A sequence of $B-1$ messages, $m_{1,b}, b = 1, 2, \ldots, B-1$, each selected independently and uniformly over $\mathcal{M}_1$ is to be sent over the channel in nB transmissions. Note that as $B \to \infty$, the average rate $R_1(B-1)/B$ is arbitrarily close to R_1.

Codebook Generation: Fix a joint p.m.f as (15). Let $R_w = \min\{\min_{i \in \mathcal{T}\setminus\{1\}} I(X_1; Y_i^l|U), I(U, X_1; Y_{n_l}^l)\}$. Generate 2^{nR_w} i.i.d u^n sequences, each with probability $\prod_{j=1}^{n} p(u_j)$. Index them as $u^n(m_1', s')$ where $m_1' \in [1 : 2^{nR_1}]$ and $s' \in [1 : 2^{n(R_w - R_1)}]$. For each $u^n(m_1', s')$, generate 2^{nR_w} conditionally i.i.d x_1^n sequences, according to probability $\prod_{j=1}^{n} p(x_{1,j}|u_j)$. Index them as $x_1^n(m_1', s', m_1, s)$, where $m_1 \in [1 : 2^{nR_1}]$ and $s \in [1 : 2^{n(R_w - R_1)}]$. s is the randomness index used to protect u based on the Wyner code partitioning method.

Encoding (at the beginning of block b): Let $m_{1,b}$ be the new message to be sent from the source node in block b. The stochastic encoder at the source uniformly randomly chooses s_b and transmits $x_1^n(m_{1,b-1}, s_{b-1}, m_{1,b}, s_b)$. Each relay node $i \in \mathcal{T} \setminus \{1\}$ knows the estimates $m_{1,b-1}, s_{b-1}$ of the messages the source sent in the previous block; hence, it picks $u^n(m_{1,b-1}, s_{b-1})$ and sends $\prod_{j=1}^{n} p(x_{i,j}|u_j)$. We assume that in the first block, cooperative information is $m_{1,b-1} = m_{1,0} = 1$ and in the last block, a previously known message $m_{1,b} = m_{1,B} = 1$ is transmitted.

Decoding (at the end of block b): Each relay node $i \in \mathcal{T} \setminus \{1\}$ wants to correctly recover $m_{1,b}, s_b$. Hence, it seeks a unique pair $(\tilde{m}_{1,b}, \tilde{s}_b)$ such that

$$(x_1^n(m_{1,b-1}, s_{b-1}, \tilde{m}_{1,b}, \tilde{s}_b), u^n(m_{1,b-1}, s_{b-1}), y_i^l(b)) \in A_\epsilon^n(X_1, U, Y_i^l)$$

Considering the first term of R_w and using the covering lemma [4], this can be done with small enough probability of error if n is sufficiently large. Backward decoding is used at the destination node n_l, hence it starts decoding after all B blocks are received. Using its channel output at the end of block b, i.e., $y_{n_l}^l(b)$, the decoder at the destination looks for a unique pair $\tilde{m}_{1,b-1}, \tilde{s}_{b-1}$ and such that

$$(x_1^n(\tilde{m}_{1,b-1}, \tilde{s}_{b-1}, m_{1,b}, s_b), u^n(\tilde{m}_{1,b-1}, \tilde{s}_{b-1}), y_{n_l}^l(b)) \in A_\epsilon^n(X_1, U, Y_{n_l}^l) \tag{42}$$

where $m_{1,b}, s_b$ were decoded in the previous step of backward decoding (i.e., block $b+1$). Similarly, considering the second term in R_w for large enough n, the probability of error can be made sufficiently small.

Analysis of information leakage rate: Let $j^* = \operatorname{argmin}_{j \in \mathcal{N}_e}\{R_w - I(U, U_1; Y_j^e)\}$ and $(Y_{j^*}^e)^n \doteq \mathbf{Y}^e$. Now, to consider the information leakage rate over all B blocks, we analyze the mutual information between all the messages sent in the B blocks (i.e., $M_{1,1}, \ldots, M_{1,B-1}$) and all the received signal in B blocks at the bottleneck eavesdropper (i.e., $\mathbf{Y}^e(1), \ldots, \mathbf{Y}^e(B)$), averaged over the random codebook $\mathcal{C}$.

$$\begin{aligned}
&I(M_{1,1}, \ldots, M_{1,B-1}; \mathbf{Y}^e(1), \ldots, \mathbf{Y}^e(B)|\mathcal{C}) \\
&\overset{(a)}{=} \sum_{b=2}^{B} I(M_{1,b-1}; \mathbf{Y}^e(1), \ldots, \mathbf{Y}^e(B)|M_{1,b}, \ldots, M_{1,B-1}, \mathcal{C}) \\
&\overset{(b)}{=} \sum_{b=2}^{B} I(M_{1,b-1}; \mathbf{Y}^e(b-1), \mathbf{Y}^e(b)|M_{1,b}, \mathcal{C}) \\
&= \sum_{b=2}^{B} I(M_{1,b-1}; \mathbf{Y}^e(b)|M_{1,b}, \mathcal{C}) \\
&\quad + H(\mathbf{Y}^e(b-1)|\mathbf{Y}^e(b), M_{1,b}, \mathcal{C}) \\
&\quad - H(\mathbf{Y}^e(b-1)|\mathbf{Y}^e(b), M_{1,b-1}, M_{1,b}, \mathcal{C}) \\
&\overset{(c)}{\le} \sum_{b=2}^{B} I(M_{1,b-1}; \mathbf{Y}^e(b)|M_{1,b}, \mathcal{C}) + H(\mathbf{Y}^e(b-1)|\mathcal{C}) \\
&\quad - H(\mathbf{Y}^e(b-1)|M_{1,b-1}, \mathcal{C}) \\
&= \sum_{b=2}^{B} I(M_{1,b-1}; \mathbf{Y}^e(b)|M_{1,b}, \mathcal{C}) + I(M_{1,b-1}; \mathbf{Y}^e(b-1)|\mathcal{C})
\end{aligned} \tag{43}$$

(a) follows from the chain rule; (b) follows from the code structure; (c) follows since conditioning does not increase the entropy and $\mathbf{Y}^e(b), M_{1,b} \to M_{1,b-1} \to \mathbf{Y}^e(b-1)$ forms a Markov chain due to code construction and the memoryless property of the channel (see (42)).

Now, we show that each term in (43) is not greater than $n\varepsilon$ if the rate satisfies the (14). For the first term, we have:

$$\begin{aligned}
I(M_{1,b-1}\ ;\ &\mathbf{Y}^e(b)|M_{1,b}, \mathcal{C}) \\
&= H(M_{1,b-1}|M_{1,b}, \mathcal{C}) - H(M_{1,b-1}|\mathbf{Y}^e(b), M_{1,b}, \mathcal{C}) \\
&\overset{(a)}{\le} H(M_{1,b-1}|\mathcal{C}) - H(M_{1,b-1}|\mathbf{Y}^e(b), M_{1,b}, S_b, \mathcal{C}) \\
&= nR_1 - H(M_{1,b-1}, S_{b-1}|\mathbf{Y}^e(b), M_{1,b}, S_b, \mathcal{C}) \\
&\quad + H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b), M_{1,b}, S_b, \mathcal{C}) \\
&= nR_1 - H(M_{1,b-1}, S_{b-1}|M_{1,b}, S_b, \mathcal{C}) \\
&\quad + I(M_{1,b-1}, S_{b-1}; \mathbf{Y}^e(b)|M_{1,b}, S_b, \mathcal{C}) \\
&\quad + H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b), M_{1,b}, S_b, \mathcal{C}) \\
&= nR_1 - H(M_{1,b-1}, S_{b-1}|\mathcal{C}) \\
&\quad + I(M_{1,b-1}, S_{b-1}, U^n(b), X_1^n(b); \mathbf{Y}^e(b)|M_{1,b}, S_b, \mathcal{C}) \\
&\quad + H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b), M_{1,b}, S_b, \mathcal{C}) \\
&\le nR_1 - nR_w \\
&\quad + I(M_{1,b-1}, S_{b-1}, U^n(b), X_1^n(b), M_{1,b}, S_b, \mathcal{C}; \mathbf{Y}^e(b)) \\
&\quad + H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b), M_{1,b}, S_b, \mathcal{C}) \\
&\overset{(b)}{\le} nR_1 - nR_w + nI(U, X_1; Y_{j^*}^e) \\
&\quad + H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b), M_{1,b}, S_b, \mathcal{C}) \\
&\overset{(c)}{\le} n(R_1 - R_w + I(U, X_1; Y_{j^*}^e) \\
&\quad + R_w - R_1 - I(U, X_1; Y_{j^*}^e) + \varepsilon) \\
&\le n\varepsilon
\end{aligned} \tag{44}$$

(a) holds since conditioning does not increase the entropy and the messages are independent; (b) holds because

$M_{1,b-1}, S_{b-1}, M_{1,b}, S_b, \mathcal{C} \rightarrow U^n(b), X_1^n(b) \rightarrow \mathbf{Y}^e(b)$ forms a Markov chain and thanks to the memoryless property; (c) follows because by using [4, Lemma 22.1], we have: if $R_w - R_1 \geq I(U, X_1; Y^e_{j^*})$, then $H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b), M_{1,b}, S_b, \mathcal{C}) \leq n(R_w - R_1 - I(U, X_1; Y^e_{j^*}) + \varepsilon)$ (see (42) for the details of each codeword).

The analysis of the second term in (43) is as follows.

$$\begin{aligned}
&I(M_{1,b-1}; \mathbf{Y}^e(b-1)|\mathcal{C}) \\
&\overset{(a)}{\leq} H(M_{1,b-1}|\mathcal{C}) - H(M_{1,b-1}|\mathbf{Y}^e(b-1), M_{1,b-2}, S_{b-2}, \mathcal{C}) \\
&= nR_1 - H(M_{1,b-1}, S_{b-1}|\mathbf{Y}^e(b-1), M_{1,b-2}, S_{b-2}, \mathcal{C}) \\
&\quad + H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b-1), M_{1,b-2}, S_{b-2}, \mathcal{C}) \\
&= nR_1 - H(M_{1,b-1}, S_{b-1}|M_{1,b-2}, S_{b-2}, \mathcal{C}) \\
&\quad + I(M_{1,b-1}, S_{b-1}; \mathbf{Y}^e(b-1)|M_{1,b-2}, S_{b-2}, \mathcal{C}) \\
&\quad + H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b-1), M_{1,b-2}, S_{b-2}, \mathcal{C}) \\
&= nR_1 - nR_w \\
&\quad + I(M_{1,b-1}, S_{b-1}, X_1^n(b-1); \mathbf{Y}^e(b-1)|M_{1,b-2}, S_{b-2} \\
&\quad , U^n(b-1), \mathcal{C}) \\
&\quad + H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b-1), M_{1,b-2}, S_{b-2}, \mathcal{C}) \\
&\overset{(b)}{\leq} nR_1 - nR_w + nI(X_1; Y^e_{j^*}|U) \\
&\quad + H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b-1), M_{1,b-2}, S_{b-2}, \mathcal{C}) \\
&\overset{(c)}{\leq} n(R_1 - R_w + I(X_1; Y^e_{j^*}|U) \\
&\quad + R_w - R_1 - I(X_1; Y^e_{j^*}|U) + \varepsilon) \\
&\leq n\varepsilon
\end{aligned} \tag{45}$$

(a) holds since conditioning does not increase the entropy; (b) holds because $M_{1,b-1}, S_{b-1}, M_{1,b-2}, S_{b-2}, \mathcal{C} \rightarrow U^n(b-1), X_1^n(b-1) \rightarrow \mathbf{Y}^e(b-1)$ forms a Markov chain and thanks to the memoryless property; (c) follows because by using [4, Lemma 22.1], we have: if $R_w - R_1 \geq I(X_1; Y^e_{j^*}|U)$, then $H(S_{b-1}|M_{1,b-1}, \mathbf{Y}^e(b-1), M_{1,b-2}, S_{b-2}, \mathcal{C}) \leq n(R_w - R_1 - I(X_1; Y^e_{j^*}|U) + \varepsilon)$ (see (42) for the details of each codeword). Therefore, to make both (44) and (45) hold, we must have $R_w - R_1 \geq \max\left\{I(U, X_1; Y^e_{j^*}), I(X_1; Y^e_{j^*}|U)\right\} = I(U, X_1; Y^e_{j^*})$. This condition, after applying prefix channel, gives (14).

Our approach resembles providing side information (the message of the previous and the next blocks) to the eavesdropper to upper-bound the information leakage rate to the eavesdroppers. For the proofs based on backward decoding, see [23, Appendix B] and [44, Section III.B]. ■

APPENDIX B
PROOF OF LEMMA 2

Proof: The achievable secrecy rate in Lemma 1 can be extended to the Gaussian case with continuous alphabets (and so to our network model) by standard arguments [45]. We constrain all the inputs to be Gaussian. For certain $\beta_i, i \in [1 : n_r + 1]$, consider the following mapping for the generated codebook in Lemma 1 with respect to the p.m.f (15), which contains a simple Gaussian version of the block Markov superposition coding where all relay nodes send the same common RV (shown by U). However, they adjust their power and use beamforming.

$$\begin{aligned}
&U \sim \mathcal{CN}(0, \tilde{P}_u) \quad \text{and} \quad \tilde{U}_1 \sim \mathcal{CN}(0, \tilde{P}_1) \\
&X_1 = \tilde{U}_1 + \beta_1 U \quad \text{and} \quad X_i = \beta_i U, i \in [2 : n_r + 1]
\end{aligned}$$

Parameter β_1 determines the amount of $\tilde{P}_1$ dedicated to construct the basis of cooperation, while parameters $\beta_i, i \in [2 : n_r + 1]$ are the beamforming coefficients. Applying the power constraint in (4) to above mapping, we obtain

$$\tilde{P}_1 + \|\mathbf{B}\|_2^2 \tilde{P}_u \leq \overline{P}_{tot}. \tag{46}$$

Now, it is sufficient to evaluate the mutual information terms in (14) by using this mapping and the network model in (1) and (2), to reach (16). ■

APPENDIX C

Lemma 9: Consider a Poisson RV X with parameter λ.

$$Pr(X \geq x) \leq \frac{e^{-\lambda}(e\lambda)^x}{x^x} \quad \text{for} \quad x > \lambda$$

And hence For any $\epsilon \in (0, 1)$:

$$\lim_{\lambda \to \infty} Pr(X \leq (1 - \epsilon)\lambda) = 0, \tag{47}$$

$$\lim_{\lambda \to \infty} Pr(X \leq (1 + \epsilon)\lambda) = 1. \tag{48}$$

Proof: See [9] for proofs based on applying Chernoff bound and Chebyshev's inequality. ■

APPENDIX D
PROOF OF LEMMA 4

Proof: The proof is similar to the proof of Lemma 1. Therefore, we only highlight the differences. Here, a serial $(n_l - 1)$-stage block Markov coding is used.[2] Without loss of generality and for simplicity, we choose the identity permutation and prove the achievability of

$$\min_{j \in \mathcal{N}_e} \min_{i \in [1:n_l-1]} I(U_1^i; Y_{i+1}^l | U_{i+1}^{n_l-1}) - I(U_1^{n_l-1}; Y_j^e)$$

Moreover, we use the replacement X_i for U_i in the proof and then the general case can be proved using a memoryless prefix channel as [23]. A sequence of $B - n_l + 2$ messages, $m_{1,b}, b = 1, 2, \ldots, B - n_l + 2$, each selected independently and uniformly over $\mathcal{M}_1$ is to be sent over the channel in nB transmission. Note that as $B \rightarrow \infty$, the average rate $R_1(B - n_l + 2)/B$ is arbitrarily close to R_1.

Codebook Generation: Fix a joint p.m.f as (27). Define $w_\iota = (m_{1,\iota}, s_\iota)$ where $m_{1,\iota} \in [1 : 2^{nR_1}]$ and $s_\iota \in [1 : 2^{n(R_w - R_1)}]$ and $R_w = \min_{i \in [1:n_l-1]} I(X_1^i; Y_{i+1}^l | X_{i+1}^{n_l-1})$. Generate 2^{nR_w} i.i.d $x^n_{n_l-1}(w_{n_l-1})$ where $w_{n_l-1} \in [1 : 2^{nR_w}]$. For each $x^n_{n_l-1}(w_{n_l-1})$, generate 2^{nR_w} conditionally i.i.d $x^n_{n_l-2}(w_{n_l-1}, w_{n_l-2})$ where $w_{n_l-2} \in [1 : 2^{nR_w}]$. Continuing in this way, at each node $i \in [1 : n_l - 2]$, for each $(x^n_{i+1}(w_{i+1}, \ldots, w_{n_l-1}), \ldots, x^n_{n_l-1}(w_{n_l-1}))$ generate 2^{nR_w} conditionally i.i.d $x_i^n(w_i, \ldots, w_{n_l-1})$ where $w_i \in [1 : 2^{nR_w}]$. Since we use sliding-window decoding, we repeat this process

[2] The scheme for the multiple relay networks is first proposed in [7], [39] and then extended to multiple relays with an eavesdropper in [25].

n_l-1 times and generate n_l-1 random codebooks which in block b we use the $(b \mod n_l-1)$th codebook to make the error events independent.

Encoding (at the beginning of block b): Let $m_{1,b}$ be the new message to be sent from the source node in block b. The stochastic encoder at the source uniformly randomly chooses s_b and setting $w(b)=(m_{1,b},s_b)$ transmits $x_1^n(w(1),\dots,w(n_l-1))$. Each node $i\in[1:n_l-1]$ knows the estimations of $w(b-r+1), r\geq i+1$ (from the decoding part) and transmits $x_i^n(w(b-i),\dots,w(b-n_l+1))$. We assume that $w(b)=1, B-n_l+3\leq b\leq B$.

Decoding (at the end of block b): Each node $i\in[2:n_l]$ wants to correctly recover $w(b-i+1)$. Hence, it looks for a unique index $\tilde{w}(b-i+1)$ such that for all $k=1,\dots,i-1$ satisfy

$$(x_{i-1-k}^n(\tilde{w}(b-i+1),w(b-i),\dots,w(b-k-n_l+1)),\dots,\; x_{n_l-1}^n(w(b-k-n_l+1)),y_i^l(b-k)) \in A_\epsilon^n(X_{i-1-k},\dots,X_{n_l-1},Y_i^l)$$

If n is large enough, it can be shown from R_w, the covering lemma [4] and the independent codebooks over (n_l-1) adjacent block, the probability of error can be made sufficiently small. The analysis of the information leakage rate can be done same as in the proof of Lemma 1, by defining $U=X_2^{n_l-1}$. ■

Appendix E
Proof of Lemma 5

Proof: Similar to the proof of Lemma 2, we compute (27), with an appropriate choice of the input distribution by constraining all the inputs to be Gaussian. For each $q\in[1:n_l-1]$, define $\mathbf{B}_q=[\beta'_{1q},\dots,\beta'_{qq}]\in\mathbb{C}^q$ for $\beta'_{qq}=1$ and certain $\beta'_{kq}, k\in[1:q-1]$ and consider the following mapping for the generated codebook in Lemma 4 with respect to the p.m.f (27),

$$\tilde{U}_q\sim\mathcal{CN}(0,\tilde{P}_q) \qquad ,q\in[1:n_l-1] \tag{49}$$

$$X_k=\sum_{q=k}^{n_l-1}\beta'_{kq}\tilde{U}_q=\tilde{U}_k+\sum_{q=k+1}^{n_l-1}\beta'_{kq}\tilde{U}_q\;, k\in[1:n_l-1] \tag{50}$$

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

$$\overline{P}_{tot}\geq\sum_{k=1}^{n_l-1}\sum_{q=k}^{n_l-1}|\beta'_{kq}|^2\tilde{P}_q=\sum_{q=1}^{n_l-1}\sum_{k=1}^{q}|\beta'_{kq}|^2\tilde{P}_q =\sum_{q=1}^{n_l-1}\|\mathbf{B}_q\|_2^2\tilde{P}_q \tag{51}$$

Using this mapping, (1) and (2), and applying interchangings in the order of summations similar to (51), deriving the mutual information terms in (27) completes the proof. ■

Appendix F
Proof of Theorem 5

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 10. The proof is based on using (n_l-1)-stage block Markov coding (serial DF relaying) and Wyner wiretap coding. The details of the proof is similar to Lemma 4. The difference is only in the analysis of the information leakage rate which again can be derived following the similar steps of the one in the information leakage rate analysis of Lemma 4 by replacing $(Y_{j^*}^e)^n\doteq\mathbf{Y}^e$ of Appendix A with all vector of all the received signal at the eavesdroppers. Thus, we omit the proof for brevity. Without loss of generality, let $\mathcal{N}_l=\{1,\dots,n_l\}$. 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 $i-1$ [40]. Next, we extend $\mathcal{R}_s^{DM}$ to $\mathcal{SN}$-PCE in Lemma 11 and call it $\mathcal{R}_s$. Finally, we apply ZF to $\mathcal{R}_s$ and we obtain $\mathcal{R}_s^{ZF}$. Similar to the non-colluding case, 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 10: Consider the general discrete memoryless counterpart of $\mathcal{SN}$-PCE, given by some conditional distribution $p(y_2^l,\dots,y_{n_l}^l,\mathbf{y}^e|x_1,\dots,x_{n_l})$, and let $\pi(\cdot)$ be a permutation on $\mathcal{N}_l=\{1,\dots,n_l\}$, where $\pi(1)=1$, $\pi(n_l)=n_l$ and $\pi(m:n)=\{\pi(m),\pi(m+1),\dots,\pi(n)\}$. The secrecy capacity is lower-bounded by:

$$\mathcal{R}_s^{DM}=\sup\max_{\pi(\cdot)}\min_{i\in[1:n_l-1]}I(U_{\pi(1:i)};Y_{\pi(i+1)}^l|U_{\pi(i+1:n_l-1)}) -I(U_{\pi(1:n_l-1)};\mathbf{Y}^e) \tag{52}$$

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

$$p(u_1,\dots,u_{n_l-1})\prod_{k=1}^{n_l-1}p(x_k|u_k). \tag{53}$$

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 G).

Lemma 11: For $\mathcal{SN}$-PCE, the following secure aggregate rate is achievable.

$$\mathcal{R}_s=\min_{i\in[1:n_l-1]}\max_{\mathbf{B}_i,\tilde{P}_i}\log\Big(1+\frac{\sum_{q=1}^{i}|\sum_{k=1}^{q}h_{k,i+1}^l\beta'_{kq}|^2\tilde{P}_q}{N^l}\Big) -\log\Big(1+\frac{\sum_{j\in\mathcal{N}_e}\sum_{q=1}^{n_l-1}|\sum_{k=1}^{q}h_{k,j}^e\beta'_{kq}|^2\tilde{P}_q}{N^e}\Big) \tag{54}$$

where (33) and (36) 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, $\mathcal{T}=\{1,\dots,n_l-1\}$. From (54), 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 [28]. Hence, we choose to ZF at the colluding eavesdroppers by letting $\sum_{q=2}^{n_l-1} |\sum_{k=1}^{q} h^e_{k,j}\beta'_{kq}|^2\tilde{P}_q = 0, \forall j \in \mathcal{N}_e$. This results in $\tilde{P}_q = 0$ or $E(q,j) = \sum_{k=1}^{q} h^e_{k,j}\beta'_{kq} = 0$, for $\forall q \in [2:n_l-1]$. Now we show that indeed clustering is needed by deriving the power allocation in (35). One can obtain $X_k = \tilde{U}_k + \beta_k X_{k+1}$ from (56), 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 (35) 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 (34). (32) is resulted from applying (34) on (54). 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 (36) already given in Lemma 11. ■

Appendix G
Proof of Lemma 11

Proof: Using standard arguments, we can extend (52), by computing it for an appropriate choice of the input distribution and constraining all the inputs to be Gaussian [45]. The mapping is same as the one in 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 10 with respect to the p.m.f (53),

$$\tilde{U}_q \sim \mathcal{CN}(0, \tilde{P}_q) \qquad , q \in [1:n_l-1] \quad (55)$$

$$X_k = \sum_{q=k}^{n_l-1} \beta'_{kq}\tilde{U}_q = \tilde{U}_k + \sum_{q=k+1}^{n_l-1} \beta'_{kq}\tilde{U}_q \text{ , } k \in [1:n_l-1] \quad (56)$$

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 (52) completes the proof. ■

References

[1] 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.

[2] ——, "Colluding eavesdroppers in large cooperative wireless networks," in *Proc. Iran Workshop on Communication and Information Theory (IWCIT)*, Tehran, Iran, May 2014.

[3] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. Huang, and H. H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[4] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge Univ. Press, 2011.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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, pp. 3051–3055.

[11] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. eleventh ACM international symposium on Mobile ad hoc networking and computing, MobiHoc '10*, Ill., USA, Sep. 2010, pp. 21–30.

[12] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 1152 – 1160.

[13] 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, pp. 1179 – 1187.

[14] LTE-A, *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (EUTRA)*. 3GPP TR 36.806 V9.0.0, 2010.

[15] M. Sawahashi, Y. Kishiyama, A. Morimoto, D. Nishikawa, and M. Tanno, "Coordinated multipoint transmission/reception techniques for lte-advanced, coordinated and distributed mimo," *IEEE Wireless Communications*, vol. 17, no. 3, pp. 26–34, June 2010.

[16] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

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

[18] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[19] 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.

[20] 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.

[21] 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.

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

[23] 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.

[24] Y. Liang, H. V. Poor, and L. Ying, “Secure communications over wireless broadcast networks: stability and utility maximization,” *IEEE Trans. Inf. Forensics and Security*, vol. 6, no. 3, pp. 682–692, Sep. 2011.

[25] 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.

[26] ——, “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.

[27] T. M. Cover and A. E. Gamal, “Capacity theorems for relay channels,” *IEEE Trans. Inf. Theory*, vol. 25, no. 5, pp. 572–584, Sep. 1979.

[28] 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.

[29] R. Negi and S. Goel, “Secret communication using artificial noise,” in *Proc. IEEE VTC*, Sep. 2005, pp. 1906–1910.

[30] J. N. Laneman and G. W. Wornell, “Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2415–2425, Oct. 2003.

[31] S. Shafiee, N. Liu, and S. Ulukus, “Towards the secrecy capacity of the gaussian MIMO wire-tap channel: The 2-2-1 channel,” *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[32] A. Khisti and G. Wornell, “Secure transmission with multiple antennas I: the MISOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[33] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas - part II: the MIMOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[34] M. Yuksel and E. Erkip, “Diversity-multiplexing trade off for the multiple-antenna wire-tap channel,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, Mar. 2011.

[35] Z. Rezki and M. S. Alouini, “Secure diversity-multiplexing tradeoff of zero-forcing transmit scheme at finite-SNR,” *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 1138–1147, Apr. 2012.

[36] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[37] 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, pp. 2442–2446.

[38] ——, “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.

[39] P. R. K. L.-L. Xie, “An achievable rate for the multiple-level relay channel,” *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1348–1358, Apr. 2005.

[40] 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.

[41] J. A. S. Weber and N. Jindal, “An overview of the transmission capacity of wireless networks,” *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3593–3604, Dec. 2010.

[42] M. Bloch and J. N. Laneman, “Information-spectrum methods for information-theoretic security,” in *Proc. Inf. Theory and App. Workshop*, San Diego, CA, USA, Feb. 2009, pp. 23–28.

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

[44] M. Yuksel and E. Erkip, “The relay channel with a wire-tapper,” in *Proceedings of the 41st Annual Conference on Information Sciences and Systems, CISS 2007, 14-16 March 2007, Johns Hopkins University, Department of Electrical Engineering, Baltimore, MD, USA*, 2007, pp. 13–18.

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

Mahtab Mirmohseni (S′06- M′12) is an assistant professor at Department of Electrical Engineering, Sharif university of Technology (SUT), since Spring 2014. She is also affiliated with the Information Systems and Security Laboratory (ISSL), Sharif University of Technology, Tehran, Iran. She received the B.Sc., M.Sc. and Ph.D. degrees from Department of Electrical Engineering, Sharif University of Technology, Tehran, IRAN in the field of Communication Systems in 2005, 2007 and 2012, respectively. She was a postdoctoral researcher at Royal Institute of Technology (KTH), Stockholm, Sweden, in the School of Electrical Engineering till Feb. 2014. Her current research interests include different aspects of information theory, mostly focusing on molecular communication, secure communication and energy-constrained networks.

Panagiotis (Panos) Papadimitratos earned his Ph.D. degree from Cornell University, Ithaca, NY, in 2005. He then held positions at Virginia Tech, EPFL and Politecnico of Torino. Panos is currently a tenured Associate Professor at KTH, Stockholm, Sweden, where he leads the Networked Systems Security group. His research agenda includes a gamut of security and privacy problems, with emphasis on wireless networks. At KTH, he is affiliated with the ACCESS center, leading its Security, Privacy, and Trust thematic area, as well as the ICES center, leading its Industrial Competence Group on Security. Panos is a Knut and Alice Wallenberg Academy Fellow and he received a Swedish Science Foundation Young Researcher Award. He has delivered numerous invited talks, keynotes, and panel addresses, as well as tutorials in flagship conferences. Panos currently serves as an Associate Editor of the IEEE Transactions on Mobile Computing and the ACM/IEEE Transactions on Networking. He has served in numerous program committees, with leading roles in numerous occasions; notably, in 2016, as the program co-chair for the ACM WiSec and the TRUST conferences. Web: http://www.ee.kth.se/nss