Scaling Laws for Secrecy Capacity in Cooperative Wireless Networks

Mahtab Mirmohseni and Panagiotis Papadimitratos
KTH Royal Institute of Technology, Stockholm, Sweden
Email: {mahtabmi,papadim}@kth.se

***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 and n_e eavesdroppers, and path loss exponent $\alpha \geq 2$. As long as $n_e^2(\log(n_e))^\gamma = o(n_l)$ holds for some positive γ, we show one can obtain unbounded secure aggregate rate. This means zero-cost secure communication, given a fixed total power constraint for the entire network. We achieve this result with (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 $n_e^{\frac{\alpha}{2}+1}(\log(n_e))^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$ holds, for some positive γ, δ.**

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., the increasing with the network size key management complexity, or the assumed limited attacker computational power. Moreover, encrypted data may still provide information to attackers (e.g., traffic analysis). This motivated efforts to complement these techniques and fueled interest in information-theoretic physical layer security [1].

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 [2]; the complex nature of large wireless networks with stochastic node distribution 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 [3]; 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, the achievability of linear scaling was shown by Franceschetti *et al*. [4]. The main characteristic of this line of works is the assumption of point-to-point communication, with each receiver (not necessarily the final destination) 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. Although the broadcast nature of wireless networks decreases the security level, it also makes cooperation easier. 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 [5], [6] and follow-up works).

978-1-4799-3360-0/14$31.00 © 2014 IEEE

Recently, there is a growing interest in considering how secrecy constraints affect scaling laws of large wireless networks [7]–[11]. To best of our knowledge, all these works considered point-to-point interference-limited communications (multihopping) [7]–[11] 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 [5] 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, 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 [12], [13]).

A. Background and Related Work

Physical layer security using information-theoretic tools leverages the channel statistics to overcome 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 [14], 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 [15]; Wyner determined the capacity of the degraded wiretap channel, in which the channel to the eavesdropper is a degraded version of the channel to the legitimate receiver. The wiretap secrecy capacity achieving scheme, known also as *Wyner's wiretap channel coding*, comprises multicoding and randomized encoding [2, Section 22.1.1]. Csiszár and Körner extended the secrecy capacity result to the the general wiretap channel (not necessarily degraded) [16].

There is considerable recent research interest in multi-user wiretap channels [17]–[24]. In these channels, cooperation among legitimate users is possible in two different ways. First, 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 [21] as the relay-eavesdropper channel and the secrecy rates were derived using relaying strategies such as the Decode-and-Forward (DF) scheme [25]; the case of multiple relays was investigated in [23], [26]. Second, passive cooperation, also known as deaf cooperation: the helper nodes transmit independent signals to confuse the eavesdroppers and increase the secure rates [24], [26], [27]. In both cooperation modes, one can try to apply beamforming at the helper nodes to improve secrecy, by constructing the virtual Multiple Input Multiple Output (MIMO) scenarios and/or perform Zero-Forcing (ZF) at eavesdroppers [27]–[33]. It was shown that in the high-SNR regime the ZF transmit scheme is Diversity-Multiplexing Tradeoff (DMT) optimal for the MIMO wiretap channel with three nodes (a source, a destination and an eavesdropper) [31], [32]. In this paper, we concentrate on the *active cooperation* schemes based on information-theoretic secrecy coding schemes. Although there is considerable effort in these works on small networks, consisting of few nodes with deterministic locations, the problem of secure communication in large networks received relatively less attention.

Only under the assumption of an interference-limited channel, scaling laws for the secure aggregate rate were derived for large wireless networks. Koyluoglu *et al.* [7] recently achieved a secure aggregate rate of scaling $\sqrt{n}$ for dense networks, as long as the ratio of the densities of eavesdroppers and legitimate nodes scales as $(\log n)^{-2}$. The authors in [9]–[11] 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 [11]. As the total power scales linearly with the number of nodes, n, in these works, the cost of secure communication goes to ∞.

B. Our Contributions

Our work is the first to allow *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 static path loss physical layer model, path loss exponent $\alpha \geq 2$ and stochastic node placement. n_l legitimate nodes and n_e eavesdroppers are distributed in a square of unit area according to Poisson Point Processes (PPP) with intensities λ_l and λ_e, respectively. We consider the fixed total power constraint and find two scaling results for $\frac{n_e}{n_l}$, for which one can obtain an infinite secure aggregate rate, and thus zero-cost secure communication. Compared to [5], 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's wiretap coding at the source, in order 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 [5], [34] and then extended to such networks with an eavesdropper in [23], with some ZF schemes 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 relay selection among legitimate nodes, the priority and power allocation, and finding the appropriate beamforming parameters. Then, we utilize the derived rates to achieve zero-cost secure communication.

Using the parallel relaying strategy, we show the possibility of achieving unbounded secure aggregate rate as long as $n_e^{\frac{\alpha}{2}+1}(\log(n_e))^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$ holds, for some positive γ, δ. 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 [2] to cooperatively transmit the message to the destination, while using ZF against the eavesdroppers. In fact, the relay nodes can be seen as a distributed virtual multi-antenna; using this diversity combats the eavesdroppers. Transmissions are pipelined and relay nodes operate in a full-duplex mode, a typical assumption (e.g., [5], [35]).

At the expense of additional complexity, with serial relaying, we tolerate even more eavesdroppers. We achieve zero energy cost secure communication as long as $n_e^2(\log(n_e))^\gamma = o(n_l)$ 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.

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 V.

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. 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 legitimate nodes and eavesdroppers are indicated with 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 $\lim_{n\to\infty} \frac{f(n)}{g(n)} \to 0$.

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 [3]–[6] and secrecy capacity scaling [7]. The network is a square of unit area where both legitimate nodes and *eavesdroppers* are placed, according to Poisson Point Processes (PPP) with intensities λ_l and λ_e, respectively. $\mathcal{N}_l$ is the set of legitimate nodes and their number is $n_l = |\mathcal{N}_l|$. Similarly, $\mathcal{N}_e$ is the set of eavesdroppers and $n_e = |\mathcal{N}_e|$ is 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 a message $m_i \in \mathcal{M}_i = [1 : 2^{n_t R_i}]$ and send it to its randomly chosen destination $j \in \mathcal{N}_l \setminus \{i\}$ in n_t 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; 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 eavesdropper Y_j^e, respectively. $X_k(t), k \in \mathcal{T}(t), t \in [1 : n_t]$ is an input signal and we consider the total power constraint in the network:

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

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 $\mathcal{SN}$ throughout the paper.

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

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

where $\mathfrak{M} = \{m_i : i \in \mathcal{N}_l\}$; (v) The information leakage rate for eavesdropper $j \in \mathcal{N}_e$ is defined as

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

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

$$\mathcal{R}_s = \sup_{\mathbf{R}\in\mathcal{C}_s} \|\mathbf{R}\|_1. \tag{7}$$

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 $|\mathfrak{M}| = 1$. We also assume that node 1 is the source node, i.e., $\mathfrak{M} = \{m_1\}$, transmitting $X_1(t)$. Thus, we set $Y_1^l(t) = \emptyset$. Without loss of generality, we denote the destination of m_1 by n_l-th node, i.e., $Y_{n_l}^l(t)$, and we set $X_{n_l}(t) = \emptyset$. This means that the transmitter X_1 wishes to send a message $m_1 \in \mathcal{M}_1 = [1 : 2^{n_t R_1}]$ 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 $\mathcal{N}_e$. Therefore, $\mathcal{R}_s = R_1$.

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 aggregate rate of $n \times \frac{1}{n} = 1$ bit/sec. Any other rate allocation with unit aggregate 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 which can be tolerated in a zero-cost secure communication. In fact, Theorem 2, our main result of this section, shows that we achieve an unbounded secure aggregate rate for a fixed total power as long as $n_e^{\frac{\alpha}{2}+1}(\log(n_e))^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$ holds for some positive γ, δ. Our proof is stated 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.
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.
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; we derive the maximum number of the eavesdroppers that can be tolerated in Theorem 2.

Step 1: As mentioned in Section II, the achievability relies on a single unicast scenario. Here, n_r relays (out of n_l legitimate nodes) are used as specified in the following theorem.

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

$$\mathcal{T} = \Big\{1, \Big\{i \,\Big|\, |h^l_{1,i}|^2 \ge \max\{\frac{N^l}{N^e}|h^e_{1,j}|^2, |h^l_{1,n_l}|^2\}\Big\}\Big\} \quad (8)$$

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

$$\mathcal{R}_s^{DF,ZF,par} = \max_{\mathbf{B},\tilde{P}_1,\tilde{P}_u} \min_{j\in\mathcal{N}_e} \min\{\log(\frac{N^e}{N^l}\frac{N^l+|h^l_{1,i^*}|^2\tilde{P}_1}{N^e+|h^e_{1,j}|^2\tilde{P}_1}),$$
$$\log(\frac{N^e}{N^l}\frac{N^l+|h^l_{1,n_l}|^2\tilde{P}_1+|\sum_{k\in\mathcal{T}} h^l_{k,n_l}\beta_k|^2\tilde{P}_u}{N^e+|h^e_{1,j}|^2\tilde{P}_1})\} \quad (9)$$

where

$$i^* = \operatorname*{argmin}_{i\in\mathcal{T}\setminus\{1\}} |h_{1,i}| \quad (10)$$
$$\beta_k = \mathbf{B}(k) \qquad \text{where} \quad \mathbf{B} \in \mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}) \quad (11)$$

$$\tilde{P}_1 + \|\mathbf{B}\|_2^2\tilde{P}_u \le \overline{P}_{tot} \quad (12)$$

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

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's 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

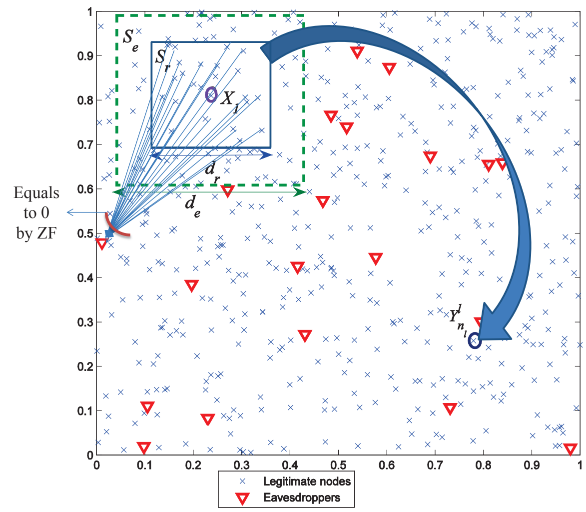

Fig. 1. Parallel relaying illustrated for a typical network model, a square of unit area; with 500 legitimate nodes and 20 eavesdroppers, placed according to PPP. The relaying square S_r of side d_r is shown with solid line and the eavesdropper-free square S_e of side d_e is shown with dashed line. The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

the message of the previous block by coherently transmitting the related codewords. 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's wiretap coding is needed at the relays.

Next, to apply this coding strategy, first we provide the achievable rate $\mathcal{R}_s^{DM,par}$ based on two-stage block Markov coding (parallel DF relaying) and Wyner's wiretap coding for the general discrete memoryless channel in Lemma 1 (proof provided in [36]). Then, we extend $\mathcal{R}_s^{DM,par}$ to our Gaussian channel model ((1) and (2)) in Lemma 2 and derive $\mathcal{R}_s^{DF,par}$ (proof in Appendix). 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:

$$\mathcal{R}_s^{DM,par} = \sup \min_{j\in\mathcal{N}_e}\{\min\{\min_{i\in\mathcal{T}\setminus\{1\}} I(U_1;Y^l_i|U), I(U,U_1;Y^l_{n_l})\}$$
$$-I(U,U_1;Y^e_j)\} \quad (13)$$

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

$$p(u,u_1)p(x_1,\ldots,x_{n_r+1}|u,u_1). \quad (14)$$

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 (14)) is an open problem [23]. 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 $\mathcal{SN}$:

$$\mathcal{R}_s^{DF,par} = \max_{\mathbf{B},\tilde{P}_1,\tilde{P}_u} \min_{j\in\mathcal{N}_e} \Big\{ \min\{ \min_{i\in[2:n_r+1]} \log(1+\frac{|h_{1,i}^l|^2\tilde{P}_1}{N^l}), \log(1+\frac{|h_{1,n_l}^l|^2\tilde{P}_1 + |\sum_{k=1}^{n_r+1} h_{k,n_l}^l \beta_k|^2 \tilde{P}_u}{N^l})\} - \log(1+\frac{|h_{1,j}^e|^2\tilde{P}_1 + |\sum_{k=1}^{n_r+1} h_{k,j}^e \beta_k|^2 \tilde{P}_u}{N^e})\Big\} \quad (15)$$

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

It can easily be seen from (15) 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 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 (8). Moreover, the condition in (10) is obtained by considering the inner $\min$ in (15).

Returning to (15), one should determine the beamforming coefficient vector $\mathbf{B}$. Finding the closed form solution is an open problem [26]. Thus, we consider a suboptimal strategy by applying ZF at all eavesdroppers and we obtain

$$\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}\mathbf{B} = \mathbf{0} \quad (16)$$

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 (11). By applying (16) to (15), we achieve (9).

In order to ensure that there exists a non-trivial solution $\mathbf{B}$ for (16), the dimension of $\mathcal{N}(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}})$ should be greater than zero, i.e., $rank(\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}) \le n_r$. Considering the worst-case scenario when $\mathbf{H}_{\mathcal{N}_e,\mathcal{T}}$ is a full rank matrix, the ZF strategy requires $n_e \le n_r$. This condition is implied by the cardinality of the set of transmitters in (8). This means that to combat eavesdroppers, one needs at least the same number of nodes as relays. Observing that the total power constraint (12) 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 $n_l, n_e \to \infty$. By applying Lemma 7, 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:

$$d_r = \sqrt{\frac{n_r}{n_l}}, d_e = \sqrt{\frac{n_r}{n_l}}(\log n_e)^{\frac{\gamma}{2}} \text{ for some } \gamma > 0. \quad (17)$$

Lemma 3: As long as $n_l \ge n_e n_r (\log n_e)^{\gamma+\delta}$ 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: The number of nodes in S_r is a two-dimensional Poisson RV with parameter $\lambda_l d_r^2$, because a Poisson process has Poisson increments. This number at least equals to n_r w.h.p (by applying (17) and (34)) as long as $\lambda_l d_r^2 \simeq n_r \to \infty$. This always holds because $n_r \ge n_e$. 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 $n_e^{\frac{\alpha}{2}+1}(\log(n_e))^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$ 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 (17) 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 model reduces to a wiretap channel with many eavesdroppers; the following rate, using Wyner coding at the source, is achievable:

$$\mathcal{R}_s^{WT} = \min_{j\in\mathcal{N}_e} \log(\frac{N^e}{N^l}\frac{N^l + |h_{1,n_l}^l|^2\tilde{P}_1}{N^e + |h_{1,j}^e|^2\tilde{P}_1}) \quad (18)$$

$$\overset{(a)}{\ge} \log(\frac{N^e}{N^l}\frac{N^l + d_r^{-\alpha}\overline{P}_{tot}}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_{tot}}) \to \log(\frac{d_e}{d_r})^\alpha \overset{(b)}{\to} \infty \text{ as } n_l \to \infty$$

where (a) is obtained by considering (3), the S_r and S_e definition and by applying (4), and (b) holds due to (17). 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 (8). Now, to make ZF possible we must show that $n_r = |\mathcal{T}| - 1 \ge n_e$. By applying the constraint of Lemma 3 with equality, we have

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

(a) is due to the scaling condition stated in this theorem and (b) is obtained because $\alpha \ge 2$. Now, we can use the strategy of Theorem 1 to achieve (9). To apply the total power constraint (12), 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 (9), known as broadcast term (the secure rate from the source to n_r relay nodes in S_r), and derive its asymptotic behavior as

$$\log(\frac{N^e}{N^l}\frac{N^l + |h_{1,i^*}^l|^2\tilde{P}_1}{N^e + |h_{1,j}^e|^2\tilde{P}_1}) \overset{(a)}{\ge} \log(\frac{N^e}{N^l}\frac{N^l + d_r^{-\alpha}\overline{P}_1}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}) \to \log(\frac{d_e}{d_r})^\alpha \overset{(b)}{\to} \infty \quad \text{as} \quad n_l \to \infty \quad (19)$$

where (a) is obtained by considering (3) and the defined squares, and (b) is due to (17). 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 (9), 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 constraint in (12). Now, we consider the second term of (9), known as the multi-access term. This corresponds to the cooperative secure rate from the source and the n_r relays toward the destination.

$$\max_{\mathbf{B}} \log\left(\frac{N^e}{N^l}\frac{N^l + |h^l_{1,n_l}|^2\tilde{P}_1 + |\sum_{k\in\mathcal{T}} h^l_{k,n_l}\beta_k|^2\tilde{P}_u}{N^e + |h^e_{1,j}|^2\tilde{P}_1}\right) \quad (20)$$

$$\begin{aligned}
&\overset{(a)}{\geq} \max_{\mathbf{B}} \log\left(\frac{2^{\alpha/4}N^e}{N^l}\frac{|\mathbf{1}^\dagger\mathbf{B}|^2\cdot\frac{\overline{P}_{tot}-\overline{P}_1}{\|\mathbf{B}\|_2^2}}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\right)\\
&= \max_{\mathbf{\Phi}^\dagger\mathbf{\Phi}\leq\|\mathbf{B}\|_2^2} \log\left(\frac{2^{\alpha/4}N^e}{N^l}\frac{\mathbf{\Phi}^\dagger\mathbf{V}^\dagger\mathbf{1}\mathbf{1}^\dagger\mathbf{V}\mathbf{\Phi}\cdot\frac{\overline{P}_{tot}-\overline{P}_1}{\|\mathbf{B}\|_2^2}}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\right)\\
&= \log\left(\frac{2^{\alpha/4}N^e}{N^l}\frac{\lambda_{max}(\mathbf{V}^\dagger\mathbf{1}\mathbf{1}^\dagger\mathbf{V})\cdot(\overline{P}_{tot}-\overline{P}_1)}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\right)\\
&= \log\left(\frac{2^{\alpha/4}N^e}{N^l}\frac{\|\mathbf{1}^\dagger\mathbf{V}\|_2^2\cdot(\overline{P}_{tot}-\overline{P}_1)}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\right)\\
&\overset{(b)}{=} \log\left(\frac{2^{\alpha/4}N^e}{N^l}\frac{(n_r+1)\frac{1+\cos 2\theta}{2}\cdot(\overline{P}_{tot}-\overline{P}_1)}{N^e + (\frac{d_e}{2})^{-\alpha}\overline{P}_1}\right)\\
&\underset{n_l\to\infty}{\overset{(c)}{=}} \log\left(\kappa\frac{(n_r+1)}{d_e^{-\alpha}}\right) \overset{(d)}{\to} \infty \quad \text{as} \quad n_l\to\infty
\end{aligned} \quad (21)$$

(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 that 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 (17) 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. ■

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

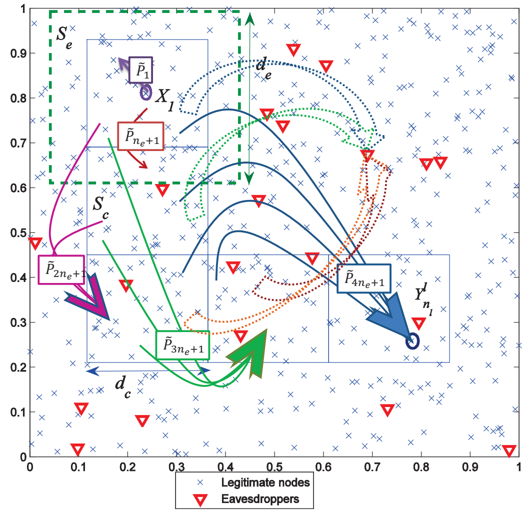

Fig. 2. Clusters (squares S_c, thin solid line) of side d_c used for serial relaying. The nodes in each cluster, c, coherently with nodes in all previous clusters and $i-c$ subsequent clusters send $\tilde{P}_{in_e+1}$ to the nodes in cluster $i+1$ for $i \geq c$. Each dotted arrow shows the received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

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:

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

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 relaying 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 [35]. To apply ZF at the eavesdroppers, we show it is necessary to have clusters of relays with the same stage compared to the source. Wyner's wiretap coding is also utilized at the source. First, we use the multi-stage block Markov coding (serial DF relaying) and Wyner's wiretap coding to obtain $\mathcal{R}_s^{DM,ser}$ in Lemma 4 (proof provided in [36]) and extend it to $\mathcal{R}_s^{DF,ser}$ for our Gaussian channel model ((1) and (2)) in Lemma 5 (proof in Appendix). 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 $\mathcal{N}_l = \{1, \ldots, n_l\}$, where $\pi(1) = 1$, $\pi(n_l) = n_l$ and $\pi(m : n) = \{\pi(m), \pi(m+1), \ldots, \pi(n)\}$. The secrecy capacity is lower-bounded by:

$$\mathcal{R}_s^{DM,ser} = \sup \min_{j \in \mathcal{N}_e} \max_{\pi(\cdot)} \min_{i \in [1:n_l-1]} I(U_{\pi(1:i)}; Y^l_{\pi(i+1)} | U_{\pi(i+1:n_l-1)}) - I(U_{\pi(1:n_l-1)}; Y^e_j) \tag{27}$$

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

$$p(u_1, \ldots, u_{n_l-1}) \prod_{k=1}^{n_l-1} p(x_k|u_k). \tag{28}$$

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:

$$\mathcal{R}_s^{DF,ser} = \min_{i \in [1:n_l-1]} \max_{\mathbf{B}_i, \tilde{P}_i} \min_{j \in \mathcal{N}_e} \log\Big(1 + \frac{\sum_{q=1}^{i} |\sum_{k=1}^{q} h^l_{k,i+1} \beta'_{kq}|^2 \tilde{P}_q}{N^l}\Big) - \log\Big(1 + \frac{\sum_{q=1}^{n_l-1} |\sum_{k=1}^{q} h^e_{k,j} \beta'_{kq}|^2 \tilde{P}_q}{N^e}\Big) \tag{29}$$

where (23) and (26) hold.

In 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 $\mathcal{T} = \{1, \ldots, n_l - 1\}$, 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 $E(q,j) = \sum_{k=1}^{q} h^e_{k,j} \beta'_{kq} = 0 \; \forall q \in [2 : n_l - 1]$. Now consider (37) to obtain $X_k = \tilde{U}_k + \beta_k X_{k+1}$ where $\beta'_{kq} = \prod_{m=k}^{q-1} \beta_m$. Therefore, $E(q_0, j)$ and $E(q_0+1, j)$ 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 $E(q,j) = 0$, 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 (29), we achieve (22). This means that to overcome n_e eavesdroppers using the proposed strategy, one node in every n_e legitimate nodes can transmit fresh information. Thus, the n_e legitimate nodes who transmit the same information in each block can apply beamforming to zero-force 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 $\frac{1}{d_c} \le c_{max} \le \frac{2}{d_c}$. 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

$$d_c = \sqrt{\frac{n_c}{n_l}}, d_e = \sqrt{\frac{n_c}{n_l}} (\log n_e)^{\frac{\gamma}{2}} \text{ for some } \gamma > 0 \tag{30}$$

where n_c is determined in Lemma 6.

Lemma 6: As long as $n_e n_c (\log n_e)^\gamma = o(n_l)$ 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: We choose the source and the destination as in the proof of Theorem 2. If the destination is inside the square S_c, the message is sent directly to it using Wyner's wiretap coding at the source. Similar to (18), 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. Setting $n_c = n_e + 1$ to the scaling of Lemma 6 results in scaling of this theorem. As $n_c \ge n_e$, 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 $q \le c_{max} n_e + 1$. Otherwise ($q \bmod n_e \ne 1$), $\tilde{P}_q = 0$. 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 $i \le n_e + 1$ that comprises the nodes in the first cluster:

$$\mathcal{R}_s^{DF,ZF,ser} \overset{(a)}{=} \log\Big(\frac{N^e}{N^l} \frac{N^l + |h^l_{k,i+1}|^2 \overline{P}_1}{N^e + |h^e_{1,j}|^2 \overline{P}_1}\Big) \overset{(b)}{\ge} \log\Big(\frac{N^e}{N^l} \frac{N^l + d_c^{-\alpha} \overline{P}_1}{N^e + d_e^{-\alpha} \overline{P}_1}\Big) \to \infty \quad \text{as} \quad n_l \to \infty \tag{31}$$

where (a) is due to (25) and (b) is obtained by considering (3) and the defined squares in (30). This rate is similar to the one we have in (19). 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 (9) 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 $q = cn_e + 1$:

$$\begin{aligned} \mathcal{R}_s^{DF,ZF,ser} &\geq \log\left(\frac{N^e}{N^l}\frac{N^l + |\sum_{k=1}^{q} h^l_{k,i+1}\beta'_{kq}|^2\tilde{P}_q}{N^e + |h^e_{1,j}|^2\tilde{P}_1}\right) \\ &\overset{(a)}{=} \log\left(\frac{N^e}{N^l}\frac{N^l + |\mathbf{h}_q^T\mathbf{B}_q|^2\overline{P}}{N^e + |h^e_{1,j}|^2\overline{P}}\right) \\ &\underset{n_l\to\infty}{\overset{(b)}{\geq}} \log\left(\frac{d_e}{d_c}\right)^\alpha \overset{(c)}{\to} \infty \quad \text{as} \quad n_l \to \infty \end{aligned} \tag{32}$$

(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 (30). This completes the proof. ■

V. Discussion and Conclusion

Zero-cost secure communication: In general, we can define the cost of secure communication as $\frac{\overline{P}_{tot}}{\mathcal{R}_s}$. In prior works [7]–[11], 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 it tends to ∞ 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 $\overline{P}_{tot}$. Our strategy tolerates n_e eavesdroppers if $n_e^2(\log(n_e))^\gamma = o(n_l)$ holds. Zero cost communication *with no secrecy constraint* was achieved in [5]. Hence, compared to [5], this means that this number of eavesdroppers does not affect the asymptotic behavior of the communication cost.

Parallel vs. serial relaying: In addition to 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 the $\overline{P}_{tot}$ 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 ($\mathcal{SN}$, 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., [23], [24]). DF relaying 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, future work we consider 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 [26] showed that the achievable secrecy rate depends on the estimation error covariance matrix. Moreover, [38] 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 [9]–[11], the achievable rate is of order 1.

Colluding eavesdroppers: By sharing their channel outputs, eavesdroppers can collude and make the attack more destructive [7], [39]. Deriving the scaling laws for *cooperative* schemes in this case is one part of our ongoing work. Our conjecture is that zero-cost secure communication is possible when $n_e^{(2+\frac{2}{\alpha})}(\log(n_e))^\gamma = o(n_l)$ holds for some positive γ.

Appendix

Proof of Lemma 2: The achievable secrecy rate in Lemma 1 can be extended to the Gaussian case with continuous alphabets (and thus to our network model) by standard arguments [37]. 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 (14), 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

$$\tilde{P}_1 + \|\mathbf{B}\|_2^2\tilde{P}_u \leq \overline{P}_{tot} \tag{33}$$

Now, it is sufficient to evaluate the mutual information terms in (13) by using this mapping and the network model in (1) and (2), to reach (15). ■

Lemma 7: Consider a Poisson RV X with parameter λ. For any $\epsilon \in (0, 1)$:

$$\lim_{\lambda\to\infty} Pr(X \leq (1-\epsilon)\lambda) = 0, \tag{34}$$

$$\lim_{\lambda\to\infty} Pr(X \leq (1+\epsilon)\lambda) = 1. \tag{35}$$

Proof: See [7] for proofs based on applying Chernoff bound and Chebyshev's inequality. ■

Proof of Lemma 5: 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 $\mathbf{B}_q = [\beta'_{1q}, \ldots, \beta'_{qq}] \in \mathbb{C}^q$ for $\beta'_{qq} = 1$ and certain $\beta'_{kq}, k \in [1 : q-1]$ and consider the following mapping for the generated codebook in Lemma 4 with respect to the p.m.f (28),

$$\tilde{U}_q \sim \mathcal{CN}(0, \tilde{P}_q) \qquad , q \in [1 : n_l - 1] \quad (36)$$

$$X_k = \sum_{q=k}^{n_l-1} \beta'_{kq}\tilde{U}_q = \tilde{U}_k + \sum_{q=k+1}^{n_l-1} \beta'_{kq}\tilde{U}_q \ , k \in [1 : n_l - 1] \quad (37)$$

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), and applying interchangings in the order of summations similar to above, deriving the mutual information terms in (27) completes the proof. ■

REFERENCES

[1] 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*, pp. 66–74, April 2011.

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

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

[4] 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.

[5] 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.

[6] 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.

[7] O. O. Koyluoglu, C. E. Koksal, and H. A. El Gamal, "On Secrecy Capacity Scaling in Wireless Networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[8] J. Zhang, L. Pu, and X. Wang, "Impact of secrecy on capacity in large-scale wireless networks," in *Proc. International Conference on Computer Communications: Mini-Conference*, 2012, pp. 3051–3055.

[9] 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.

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

[11] 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*, Fl., USA, March 2012, pp. 1179 – 1187.

[12] 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.

[13] 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.

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

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

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

[17] 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.

[18] 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.

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

[20] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE Int. Symp. Info. Theory (ISIT)*, Nice, France, June 2007, pp. 926 – 930.

[21] L. Lai and H. El Gamal, "The relayeavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[22] 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, Sept. 2011.

[23] 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.

[24] R. Bassily and S. Ulukus, "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.

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

[26] 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, Sept. 2008.

[27] R. Negi and S. Goel, "Secret communication using artificial noise," in *in Proc. IEEE VTC*, Sept. 2005, pp. 1906–1910.

[28] 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.

[29] 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, pp. 4033-4039, Sept. 2009.

[30] A. Khisti and G. Wornell, "Secure transmission with multiple antenna: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 3088-3104, July 2010.

[31] 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.

[32] 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.

[33] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, pp. 4961-4972, Aug. 2011.

[34] L.-L. Xie, P. R. Kumar, "An achievable rate for the multiple-level relay channel," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1348-1358, Apr. 2005.

[35] 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.

[36] M. Mirmohseni and P. Papadimitratos, "Scaling laws for secrecy capacity in cooperative wireless networks," Available: arxiv.org/abs/1312.3198.

[37] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley Series in Telecommunications, 2006.

[38] 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.

[39] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: the case of colluding eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 2442-2446.