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 $n_l^2 (\log(n_e))^{\gamma} = o(n_l)$ holds for some positive $\gamma$, 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 $n_l^{\frac{\gamma+1}{\alpha}} (\log(n_e))^{\gamma+\delta} = o(n_l)$ holds, for some positive $\gamma, \delta$.

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).

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
achieved a secure rate of order extended networks with unknown eavesdropper locations and large wireless networks. Koyluoglu in large networks received relatively less attention. In these works on small networks, consisting of few nodes with active cooperation (eavesdropper) \[31\], \[32\]. In this paper, we concentrate on Forcing (ZF) at eavesdroppers \[27\]–\[33\]. It was shown that put Multiple Output (MIMO) scenarios and/or perform Zero- Forcing (ZF) at eavesdroppers \[27\]–\[33\]. 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 $\infty$.

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 $\lambda_l$ and $\lambda_e$, 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 $n_e^{\gamma+1}(\log(n_e))^{\gamma+\delta(\frac{2}{3}+1)} = o(n_l)$ holds, for some positive $\gamma, \delta$. Our scheme has two stages. First, the source of the message transmits to $n_e$ 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 $X$ is denoted by $p_X(x)$; occasionally, subscript $X$ is omitted. $X^j$ indicates a sequence of RVs $(X_i, X_{i+1}, \ldots, X_j)$; we use $X^j$ instead of $X^j_i$ for brevity. $CN(0, \sigma^2)$ denotes a zero-mean complex valued Gaussian distribution with variance $\sigma^2$. The variables related to legitimate nodes and eavesdroppers are indicated with superscripts $l$ and $e$, respectively. $|X|^p_l$ is the $L^p$-norm of a vector $X$. $X(i)$ is its $i$th element. $(\cdot)^T$, $(\cdot)^*$ and $N(\cdot)$ denote the transpose, conjugate transpose and null space operators, 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 unit area where all legitimate nodes and eavesdroppers are placed, according to Poisson Point Processes (PPP) with intensities $\lambda_l$ and $\lambda_e$, respectively. $N_l$ is the set of legitimate nodes and their number is $n_l = |N_l|$. Similarly, $N_e$ is the set of eavesdroppers and $n_e = |N_e|$ is their number. As we consider large-scale networks, throughout this paper, we implicitly assume that $n_l$ and $n_e$ go to $\infty$. Each legitimate node $i \in N_l$ can be a source of a message $m_i \in M_i = [1 : 2^{n_e R_l}]$ and send it to its randomly chosen destination $j \in N_l \setminus \{i\}$ in $n_l$ channel uses. Each legitimate node $i \in N_l$ operates in a full-duplex mode; at time slot $t$, it transmits $X_i(t)$ and receives $Y_i^e(t)$. The set of transmitting nodes at time slot $t$ is denoted by $T(t) \subseteq N_l$. As we consider passive attackers, each eavesdropper $j \in N_e$ only observes the channel; at time slot $t$, it receives $Y_j^e(t)$.

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

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

where, for any $i \in N_l \setminus \{k\}$ and $j \in N_e$, the static path loss model channel gains are given by:

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

with $d_{k,i}^l$ and $d_{k,j}^e$ denoting the distances between the transmitter $X_k, k \in T(t)$, and the receiver $Y_i^l$ and eavesdropper $Y_j^e$, respectively. $X_k(t), k \in T(t), t \in [1 : n_l]$ is an input signal and we consider the total power constraint in the network:

$$\frac{1}{n_l} \sum_{t=1}^{n_e} \sum_{k \in T(t)}|X_k(t)|^2 \leq P_{tot}. \quad (4)$$

Moreover, $Z_i^l(t)$ and $Z_j^e(t)$ 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., $Z_i^l \sim CN(0, N^l)$ and $Z_j^e \sim CN(0, N^e)$, respectively. Our **network model**, defined above, is called $SN$ throughout the paper.

**Definition 1:** Let $R = [R_i : i \in N_l]$ be the rate vector and $2^{n_e R} \equiv \{2^{n_e R_i} : i \in N_l\}$. A $(2^{n_e R}, n_e, P_e^{(n_e)}$ code for $SN$ consists of (i) $n_l$ message sets $M_i = [1 : 2^{n_e R_i}]$ for $i \in N_l$, where $m_i$ is uniformly distributed over $M_i$; (ii) $|T(t)|$ sets of randomized encoding functions at the transmitters: $\{f_{i,t}^{(n_l)} : C^{t-1} \times M_i \to C\}$ such that $x_{i,t} = f_{i,t}(m_i, y_{i,t}^{(n_l-1)})$, for $t \in T(t)$, $1 \leq t \leq n_l$ and $m_i \in M_i$; (iii) Decoding functions, one at each legitimate node $i \in N_l$, $g_i : (Q_i^l)^{n_e} \times M_i \to M_k$ for some $k \in N_l \setminus \{i\}$, 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 $P_e^{(n_e)} = \max_{i,t} P_e^{(n_e)}$ with:

$$P_e^{(n_e)} = \sum_{m_k \in M_k} \Pr(g_i(Y_i^l)^{n_e}, m_i) \neq m_k | M_k \text{ sent} \quad (5)$$

where $M_k = \{m_i : i \in N_l\}$; (v) The information leakage rate for eavesdropper $j \in N_e$ is defined as

$$R_{L,j}^{(n_e)} = \frac{1}{n_e} I(M_k; Y_j^e)^{n_e}. \quad (6)$$

**Definition 2:** A rate-leakage vector $(R, R_{L,j})$ is achievable if there exists a sequence of $(2^{n_e R}, n_e, P_e^{(n_e)})$ codes such that $P_e^{(n_e)} \to 0$ as $n_e \to \infty$ and $\limsup_{n_e \to \infty} R_{L,j}^{(n_e)} \leq R_L(j)$. The secrecy capacity region, $C_s$, is the region that includes all achievable rate vectors, $R$, 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:

$$R_s = \sup_{R \in C_s} \|R\|_1. \quad (7)$$

As we are interested in the achievability of $R_s$, without loss of generality, we assume that only one source-destination pair is active and the other nodes assist their transmission. Therefore, we set $\|R\|_1 = 1$. We also assume that node 1 is the source node, i.e., $M_1 = \{m_1\}$, transmitting $X_1(t)$. Thus, we set $Y_1^l(t) = 0$. Without loss of generality, we denote the destination of $m_1$ by $n_l$-th node, i.e., $Y_n^l(t)$, and we set $X_1(t) = 0$. This means that the transmitter $X_1$ wishes to send a message $m_1 \in M_1 = [1 : 2^{n_e R_1}]$ to the receiver $Y_n^l$ with the help of nodes in $N_l \setminus \{1, n_l\}$, while keeping it secret from the eavesdroppers in $N_e$. Therefore, $R_s = R_1$.

**Remark 1:** If a secure aggregate rate $R_s = R_1$ is achievable in the above scenario (with uniformly random matching of the source-destination pairs), any rate vector $R$ with $\|R\|_1 = R_s$ 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 \( n^2 \delta^{\gamma / (\gamma + 1)} = o(n) \) holds for some positive \( \gamma, \delta \). 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 (\( (S,N) \)). 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, \( n_e \) relays (out of \( n_l \) legitimate nodes) are used as specified in the following theorem.

**Theorem 1:** For \( (S,N) \), if there exists a set of transmitters

\[
T = \left\{ i \mid |h_{i,i}|^2 \geq \max\left\{ \frac{N^l}{N^e} |h_{1,i,j}|^2, |h_{1,n_i,j}|^2 \right\} \right\}
\]

(8)

such that \( n_e = |T| - 1 \geq n_e \), the following secure aggregate rate is achievable:

\[
\mathcal{R}_{s}^{DF,ZF,par} = \max_{B,\tilde{P}_1,\tilde{P}_u} \min_{e} \left\{ \log\left( \frac{N^c N^l + |h_{1,i}|^2 \tilde{P}_1}{N^l N^e + |h_{1,j}|^2 \tilde{P}_1} \right) \right\}
\]

\[
= \max_{N^e} \left\{ \log\left( \frac{N^l}{N^e} + \log\left( \frac{N^c N^l + \log(\frac{N^c N^l + |h_{1,i}|^2 \tilde{P}_1}{N^l N^c + |h_{1,j}|^2 \tilde{P}_1})}{N^e + |h_{1,j}|^2 \tilde{P}_1} \right) \right\}
\]

(9)

where

\[
i^* = \arg\min_{i \in T \setminus \{1\}} |h_{1,i}|
\]

(10)

\[
\beta_k = B(k) \quad \text{where} \quad B \in \mathcal{N}(H_{N_e,T})
\]

(11)

\[
\tilde{P}_1 + \|B\|_2^2 \tilde{P}_u \leq \mathcal{P}_{tot}
\]

(12)

in which \( H_{N_e,T} \in \mathbb{C}^{n_e \times (n_e+1)} \) is the transmitters-eavesdroppers channel matrix, with \( h_{i,j}^{*} \) its \((i,j)\)-th element for \( i \in T, j \in N_e \).

**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 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 \( N_l = \{1, \ldots, n_l\} \), \( T = \{1, \ldots, n_r + 1\} \) and \( N_e = \{1, \ldots, n_e\} \).

**Lemma 1:** For the general discrete memoryless counterpart of \( (S,N) \), given by some conditional distribution \( p(y_1, \ldots, y_{n_e}, y_{n_e}^* | x_1, \ldots, x_{n_l}) \), the secrecy capacity is lower-bounded by:

\[
\mathcal{R}_{s}^{DM,par} = \sup_{j \in N_e} \left\{ \min_{i \in T \setminus \{1\}} \min \right\}
\]

\[
\left\{ I(U_1;Y_{i,j}^*) - I(U_1;Y_{i,j}^*) \right\}
\]

(13)

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

\[
p(u, u_1) p(x_1, \ldots, x_{n_r+1} | u, u_1).
\]

(14)

Now, we extend the above lemma to accommodate our model \( (S,N) \). 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 $\mathcal{SN}$:

\[
R_{s}^{DF,par} = \max_{B,T} \min_{P_1, P_u} \left\{ \min_{n_e,N_e} \left\{ \min_{i \in \{2:n_e+1\}} \log \left( 1 + \frac{\|h_{i,1}^T l_{1,i}^2 P_1}{N_i^i} \right) \right\}, \right. \\
\log \left( 1 + \frac{\|h_{1,n_1}^T l_{1,n}^2 P_1 + \sum_{k=1}^{n_e+1} \|h_{k,n_1}^T l_{k,n}^2 P_1}{N_i^i} \right) \right\},
\]

where $\beta_k = B(k)$ and $\hat{P}_1 + \|B\|^2 P_u \leq \hat{P}_{tot}$.

It can easily be seen from (15) that one has 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 $n_e$ relay nodes in the DF strategy and hence the set of transmitters $T(t)$ 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 $B$. 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

\[
H_{N_e,T} B = 0 \tag{16}
\]

where $H_{N_e,T}$ is defined in Theorem 1. Hence, the coefficient vector $B$ must lie in the null space of $H_{N_e,T}$, as stated in (11). By applying (16) to (15), we achieve (9).

In order to ensure that there exists a non-trivial solution $B$ for (16), the dimension of $\mathcal{N}(H_{N_e,T})$ should be greater than zero, i.e., $\text{rank}(H_{N_e,T}) \leq n_e$. Considering the worst-case scenario when $H_{N_e,T}$ 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 (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 $\lambda_l$ and $\lambda_e$, 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:

\[
d_e = \sqrt{n_l n_e/(log(n_e))^2} \quad \text{for some } \gamma > 0. \tag{17}
\]

**Lemma 3**: As long as $n_l \geq n_e (log(n_e))^{\gamma + \delta}$ 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 $\lambda_{d_r^2}$, 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 $\lambda_{d_r^2} \geq n_r \to \infty$. This always holds because $n_r \geq n_e$. Similarly, the number of eavesdroppers in $S_e$ is a Poisson RV with parameter $\lambda_{d_e^2} \approx 2 n_e log(n_e) \gamma$, which converges to 0 by applying the condition stated in this lemma. Hence, the probability of having no eavesdropper in $S_e$, i.e., $e^{-\lambda_{d_e^2}}$, can be made arbitrarily close to 1.

**Step 3**: Note that the number of relays, specified in the above lemma as $\frac{n_l (log(n_e))^\gamma}{\gamma!}$, 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 $\hat{P}_{tot}$ in (4), as long as $n_e^{\frac{\gamma+\delta}{\delta}} (log(n_e))^{\gamma+\delta} = o(n_l)$ holds for some positive $\gamma, \delta$, w.h.p. an infinite secure aggregate rate $R_s$ 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:

\[
R_s^{WT} = \min_{j \in N_e} \log \left( \frac{N^e N_l^i \|h_{1,i}^T l_{1,i}^2 P_1}{N^i N^e + \|h_{1,j}^T l_{1,j}^2 P_1} \right) \tag{18}
\]

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 $n_r = |T| - 1 \geq n_e$. By applying the constraint of Lemma 3 with equality, we have

\[
n_r = \frac{n_l}{n_e (log(n_e))^\gamma + \delta} \tag{19}
\]

(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 (9). To apply the total power constraint (12), in this case, we choose a fixed $\hat{P}_1 = P_1$ and set $P_u = \frac{\hat{P}_1}{\|B\|^2}$. 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

\[
\log \left( \frac{N^e N_l^i \|h_{1,i}^T l_{1,i}^2 P_1}{N^i N^e + \|h_{1,j}^T l_{1,j}^2 P_1} \right) \geq \log \left( \frac{N^e N_l^i \|h_{1,i}^T l_{1,i}^2 P_1}{N^i N^e + (\frac{d_e}{d_r})^\alpha \hat{P}_1} \right) \tag{19}
\]

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 $\lambda_i$ to have $n_c \geq n_e$ 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 $B \in \mathbb{N}(H_{N_r,T})$. By applying Singular Value Decomposition (SVD), we have $H_{N_r,T} = U \Lambda V^T$, $\text{Y} \in \mathbb{C}^{(n_r+1) \times n_e}$ contains the first $n_e$ right singular vectors corresponding to non-zero singular values, and $V \in \mathbb{C}^{(n_r+1) \times (n_r-n_e+1)}$ contains the last $n_r - n_e + 1$ singular vectors corresponding to zero singular values of $H_{N_r,T}$. The later forms an orthonormal basis for the null space of $H_{N_r,T}$. Hence, $B$ can be expressed as their linear combination, i.e., $B = \Phi \text{V}$, where $\Phi \in \mathbb{C}^{(n_r-n_e+1)}$ is an arbitrary vector selected by considering the power constraint in (12). Now, we consider the second term of (9), known as the multiplexing term.

\[
\max_B \log(\frac{N^e l + \|h_{1,n_1}^1\|^2 \tilde{P}_1 + \sum_{k \in \mathbb{P}} h_{1,n_1}^k \beta_k \|\tilde{P}_u\|^2}{\|\Phi\|^2}) \tag{20}
\]

(a) holds since $d_{k,n_1} \leq \sqrt{2}$ and $1 \in \mathbb{C}^{(n_r+1)}$ is the all one vector. In (b), $\theta$ is an RV that denotes the angle between $1$ and $\mathbb{N}(H_{N_r,T})$ and has a continuous distribution on $[0, 2\pi]$ due to the randomness of $H_{N_r,T}$. In (c), $\kappa$ is a constant. (d) is obtained by substituting (17) and $n_r = \frac{\alpha}{\log(n_e)}$ and by applying the scaling $n_e^2 \gamma \log(n_e) \gamma + \delta \frac{\gamma}{2} = o(n_e)$ for some positive $\gamma, \delta$. 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 power can be achieved as long as $n_e^2 \log(n_e) / \gamma = o(n_e)$ holds for some positive $\gamma$.

**Step 1:** Achievability is given in the following theorem.

**Theorem 3:** For $SN$, the following secure aggregate rate is achievable:

\[
R_s^{DF,ZF,ser} = \min_{i \in [1,n_i-1]} \max_B \log(\frac{N^e l + \sum_{k=1}^{q} h_{k,i+1}^q \beta_k \|\tilde{P}_q\|^2}{\|\Phi\|^2}) \tag{22}
\]

in which

\[
\beta_k = B_k(k) \quad \text{and} \quad \beta_k = 1 \quad \text{if} \quad k = q \tag{23}
\]

\[
B_q \in \mathbb{N}(H_{N_q,T}) \quad \text{for} \quad q \mod n_c = 1 \quad \text{and} \quad \tilde{P}_q \text{if} \quad q \mod n_c = 1 \quad \text{and} \quad 0 \quad \text{if} \quad q \mod n_c \neq 1 \tag{24}
\]

\[
\sum_{q=1}^{n_c-1} ||B_q||_2^2 \tilde{P}_q \leq \tilde{P}_tot \tag{25}
\]

where $H_{N_q,T} \in \mathbb{C}^{n_\alpha \times q}$ is the cluster-eavesdroppers channel matrix which its $(j,i)^{th}$ element is $h_{j,i}^i$ for $i \in [1 : q], j \in N_c$.

**Proof:*** We use a $(n_i-1)$-stage block Markov coding by making the nodes relaying the message with ordered priorities. Considering the ordered set for the legitimate nodes, i.e., $N_l = \{1, \ldots, n_i\}$, each node $i$ decodes the transmitted signal of all previous nodes ($1 \text{ to } i-1$) in this order and sends its signal to the subsequent nodes. In order to pipeline communication, $(n_i-1)$-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 $R^D_{s,ser}$ in Lemma 4 (proof provided in [36]) and extend it to $R^D_{s,ser}$ for our Gaussian channel model ((1) and (2)) in Lemma 5 (proof in Appendix). Then, by applying ZF on $R^D_{s,ser}$, we derive $R^D_{s,ZF,ser}$.

Lemma 4: Consider the channel model of Lemma 1 and let $\pi(\cdot)$ be a permutation on $N_1 = \{1, \ldots, n_1\}$, where $\pi(1) = 1$, $\pi(n_1) = n_2$ and $\pi(m : n) = \{\pi(m), \pi(m + 1), \ldots, \pi(n)\}$. The secrecy capacity is lower-bounded by:

$$R^D_{s,ser} = \sup_{\pi(\cdot)} \min_{j \in N_2} \min_{\pi(\cdot)} \left\{ I(U_{\pi(1):1}:Y_{\pi(i+1)}^{l}|U_{\pi(i+1):n_1-1}) - I(U_{\pi(1):n_1-1};Y^e) \right\}$$

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

$$p(u_1, \ldots, u_{n_1-1}) \prod_{k=1}^{n_1-1} p(x_k|u_k).$$

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

Lemma 5: For $SN$, the following is an achievable secure aggregate rate:

$$R^D_{s,ser} = \min_{i \in [1:n_1-1]} \min_{\mathbf{b}_i, \mathbf{b}_j \in \mathcal{N}_e} \left\{ \sum_{q=1}^{i} \sum_{k=1}^{q} h_{k,i+1}^{q} \beta_{q}^{i} 2^{P_q} \right\}$$

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 $T = \{1, \ldots, n_1 - 1\}$, 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

$$\sum_{k=1}^{q} h_{k,j}^{q} \beta_{q}^{i} 2^{P_q} = 0, \forall j \in \mathcal{N}_e.$$ 

This results in $P_q = 0$ or

$$E(q,j) = \sum_{k=1}^{q} h_{k,j}^{e} \beta_{q}^{i} = 0, \forall q = 2 : n_1 - 1.$$ 

Now consider (37) to obtain $X_k = \bar{U} + \beta_k X_{k+1}$ where $\beta_{q+1} = \prod_{m=k}^{q-1} \beta_m$. Therefore, $E(q_0, j)$ and $E(q_0+1, j)$ only differ in one variable, i.e., $\beta_{q_0+1}$. However, we need $E(q, j) = 0, \forall j \in \mathcal{N}_e$ if $P_q > 0$, which is clearly not possible. Therefore, we apply ZF by allocating power as per (25) and $E(q,j) = 0, \forall j \in \mathcal{N}_e$. Thus, we obtain $H_{\mathcal{N}_e,T_r} = 0$ shown in (24) ($H_{\mathcal{N}_e,T_r}$ 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 $\frac{1}{2} \leq c_{max} \leq \frac{1}{2}$. We show $c_{max}$ does not affect the asymptotic behavior of $R_s$. 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 $S_c$ of side $d_c$ around the source. We define

$$d_c = \sqrt{\frac{n_c}{n_1}} d_e = \sqrt{\frac{n_c}{n_1} (\log n_1)^2}$$

for some $\gamma > 0$ (30) where $n_c$ is determined in Lemma 6.

Lemma 6: As long as $n_c n_1 (\log n_1)^\gamma = o(n_1)$ 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 $S_c$ 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 $n_c$.

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

Theorem 4: In $SN$ with fixed total power $P_{tot}$ in (4), as long as $n_c^2 (\log n_1)^\gamma = o(n_1)$ holds for some positive $\gamma$, w.h.p. an infinite secure aggregate rate $R_s$ 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 $\frac{n_c}{n_1} \to \infty$ as $n_1 \to \infty$, 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 $n_c \geq n_e$, 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 $P_q = \frac{P_{tot}}{\sum_{q=0}^{n_1-1} \|\mathbf{b}_{n_e+1}\|^2_2}$ if $q \mod n_c = 1$ and $q \leq c_{max} n_e + 1$. Otherwise (q mod $n_c \neq 1$), $\tilde{P}_q = 0$. 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 $i \in [1 : n_1 - 1], j \in \mathcal{N}_e$ and $\mathbf{b}_q$ that satisfy (23) and (24). First, we consider $i \leq n_e + 1$ that comprises the nodes in the first cluster:

$$R^D_{s,ZF,ser}(a) = \log \left( \frac{n_c N_1^e + |h_{i,i+1}^e|^2 |P_1|}{N_1^e + |h_{i,j}^e|^2 |P_1|} \right)$$

$$\geq \log \left( \frac{n_c N_1^e + d_{e} \alpha |P_1|}{n_c N_1^e + d_{e} \alpha |P_1|} \right) \to \infty$$

as $n_1 \to \infty$. (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 \( q = cn_e + 1 \):

\[
R_{a}^{DF;ZF,ser} \geq \log \left( \frac{N_e N^l + \sum_{k=1}^{q} h_{k,i+1}^{l} \beta_{k}^{q} |\tilde{P}_1|}{N^e + |h_{0}^{l,j}|^2} \right)
\]

(a) is obtained by defining \( h_i = [h_{1,i+1}^{l}, \ldots, h_{q,i+1}^{l}]^T \). (b) follows from the steps similar to (21) and from noting that

\[
|B_{q}(g)|^2 \geq B_{q}(g) = \beta_{q} = 1, \quad |h_{0}^{l,j}|^2 \geq |h_{q,i+1}^{l}|^2 \geq d_{c}^{-a}\text{ and the randomness of } H_{N_e} \text{ is due to (30). This completes the proof.}
\]

V. DISCUSSION AND CONCLUSION

Zero-cost secure communication: In general, we can define the cost of secure communication as \( \bar{P}_{tot} \). In prior works [7]–[11], due to the individual power constraint (the transmission power for each node is fixed), \( \bar{P}_{tot} \) scales linearly with the number of nodes. Therefore, the scaling for the cost of secure communication lies in \( \sqrt{n} \) and it tends to \( \infty \) as \( n \rightarrow \infty \).

Here, we showed that cooperation based schemes can achieve secure communication with cost that goes to 0 as the number of nodes goes to \( \infty \). This is so because we use a fixed \( \bar{P}_{tot} \). 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 \( \bar{P}_{tot} \) 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 (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 \( n_e^2(\log(n_e))^{\gamma} = o(n_l) \) holds for some positive \( \gamma \).

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.

\[
X = \tilde{U}_{1} + \tilde{U}_{1} U \quad \text{and} \quad X = \beta_i U, i \in [2 : n_r + 1]
\]

Parameter \( \beta_1 \) determines the amount of \( \tilde{P}_1 \) dedicated to construct the basis of cooperation, while parameters \( \tilde{\beta}_{i}, i \in [2 : n_r + 1] \) are the beamforming coefficients. Applying the power constraint in (4) to above mapping, we obtain

\[
\tilde{P}_1 + \|B\|^2 \tilde{P}_1 \leq \bar{P}_{tot}
\]

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 \( \lambda \). For any \( \epsilon \in (0, 1) \):

\[
\lim_{\lambda \rightarrow \infty} Pr(X \leq (1 - \epsilon)\lambda) = 0, \quad (34)
\]

\[
\lim_{\lambda \rightarrow \infty} Pr(X \leq (1 + \epsilon)\lambda) = 1. \quad (35)
\]


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 \( q \in \{1: n_t - 1\} \), define \( B_q = [\beta'_{q1}, \ldots, \beta'_{qg}] \in \mathbb{C}^q \) 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),

\[
\hat{U}_q \sim \mathcal{CN}(0, P_q), \quad q \in \{1: n_t - 1\}
\]

\[
X_k = \sum_{q=k}^{n_t-1} \beta'_{kq} \hat{U}_q = \hat{U}_k + \sum_{q=k+1}^{n_t-1} \beta'_{kq} \hat{U}_q, \quad k \in \{1: n_t - 1\}
\]

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

\[
\mathbb{P}_{\text{tot}} \geq \sum_{k=1}^{n_t-1} \sum_{q=k}^{n_t-1} |\beta'_{kq}|^2 \hat{P}_q = \sum_{q=1}^{n_t-1} \sum_{k=1}^{q-1} |\beta'_{kq}|^2 \hat{P}_q = \sum_{q=1}^{n_t-1} ||B_q||_2^2 \hat{P}_q
\]

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

REFERENCES


