On Secure Communication in Large Cooperative Wireless Networks

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

I. Introduction

Naturally, given the shared and open medium in wireless networks, confidentiality is a crucial security requirement. Conventional cryptographic techniques have drawbacks especially in large-scale networks, e.g., the increasing with the network size key management complexity, the assumption of limited attacker computational power and the traffic analysis of encrypted data. This motivated efforts to complement these techniques and fueled interest in information-theoretic physical layer security [1]. Securing the information at the physical layer, based on information-theoretic tools, leverages the channel statistics to overcome attackers; depending on the channel conditions, a secure positive rate can be attainable if suitable coding schemes are employed [2, Section 22.1].

Finding out how overhead due to the secrecy constraints affects the fundamental limits of performance measures (notably the secure rate legitimate nodes can achieve) has attracted considerable research interests, notably in multi-user wiretap channels. 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. Gupta and Kumar in [3] pioneered the problem of finding scaling laws for large wireless networks and showed that multihopping schemes can achieve at most an aggregate rate that scales like $\sqrt{n}$ under an individual (per node) power constraint in a network of n randomly located nodes. The main characteristic of this line of works is a point-to-point communication assumption, where each receiver (not necessarily the final destination) is interested only in decoding the signal of a particular transmitter; all other signals, roughly termed interference, are treated as noise. Therefore, these are mostly referred to as interference-limited channel models. Although the broadcasting 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 capacity for fixed total power (in [4] and follow-up works).

Recently, there is a growing interest in considering how secrecy constraints affect scaling laws of large wireless networks [5]. To best of our knowledge, all existing works considered point-to-point interference-limited communications (multi-hopping) to analyze the *secrecy* capacity scaling; no active cooperative or relaying schemes were considered. 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.* [5] recently achieved a secure aggregate rate of scaling $\sqrt{n}$ for dense networks of n legitimate nodes, as long as the ratio of the densities of eavesdroppers and legitimate nodes scales as $(\log n)^{-2}$. In multi-user wiretap channels, cooperation among legitimate users is possible in two different ways. First, the active cooperation: legitimate nodes act as relays and cooperate with the source of the message in transmitting its message to the destination [6]. Second, the passive one, known as deaf cooperation, in which the helper nodes transmit the independent signals to confuse the eavesdroppers and increase the secure rate [7]. In both cooperation modes, one can try to apply beamforming at the helper nodes to improve the secrecy, by constructing the virtual multi-antenna and possibly perform Zero-Forcing (ZF) at eavesdroppers [7]. In this paper, we concentrate on *active cooperation* schemes based on information-theoretic secrecy coding. 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 less attention.

II. Problem Description and Network Model

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 [4] 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. In general, we can define the cost of secure communication as $\frac{\overline{P}_{tot}}{\mathcal{R}_s}$, where $\overline{P}_{tot}$ is the total power of the legitimate nodes and $\mathcal{R}_s$ is the secure aggregate rate they can achieve. In prior works (e.g., [5]), due to 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 $n \to \infty$. However, addressing secrecy constraints, active cooperation (relaying) is 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. Hence, compared to [4] (zero cost communication *with no secrecy constraint*), this means that this number of eavesdroppers does not affect the scaling of communication cost.

We consider a dense wireless network, with channel gains obeying a static path loss model with path loss exponent $\alpha \geq 2$; decaying exponentially as the distance between the (stochastically distributed) nodes increases. This is consistent with models in prior works [3]–[5]. The network is a square of unit area where n_l legitimate nodes and n_e eavesdroppers are placed, according to Poisson Point Processes (PPP). As we consider large-scale networks, we implicitly assume that n_l and n_e go to ∞. Each legitimate node, operating in a full-duplex mode, can be a source of message and send it to its randomly chosen destination. We allow *arbitrary* cooperation among legitimate nodes in deriving scaling laws for large wireless networks with secrecy constraints. Our **network model**, defined above, is called $\mathcal{SN}$ throughout the paper. For details of the model see [8].

III. Main Results

Without the limitation of point-to-point communication, we show 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 $\overline{P}_{tot}$ and achieve $\mathcal{R}_s \to \infty$. To achieve this result, we make use of (i) block Markov Decode-and-Forward (DF) relaying [2], (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. Our parallel relaying strategy tolerates n_e eavesdroppers if $n_e^{\frac{\alpha}{2}+1}(\log(n_e))^{\gamma+\delta(\frac{\alpha}{2}+1)} = o(n_l)$ for some positive γ, δ holds. This 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, relay nodes can be seen as a distributed virtual multi-antenna; using this diversity to combat the eavesdroppers. Transmissions are pipelined and relay nodes operate in a full-duplex mode, a typical assumption (e.g., [4]).

Theorem 1: In $\mathcal{SN}$ with fixed total power $\overline{P}_{tot}$, 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.

Outline of the proof: Our proof has three steps:

Step 1: First, we provide a lower bound on the secrecy capacity achieved through active cooperation, randomized encoding and beamforming. 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.

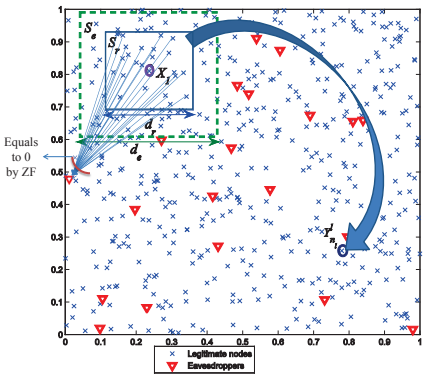

Fig. 1. Parallel relaying for a typical $\mathcal{SN}$; the source has channel input X_1 and the destination has channel output $Y_{n_l}^l$; the relaying and eavesdropper-free squares (S_r and S_e) are shown with the solid and dashed lines, respectively. For brevity, ZF is only shown (solid lines originating S_r) in one eavesdropper.

Step 2: In this step, the main challenge is to find strategies to apply the achievability scheme of the first step to $\mathcal{SN}$. Through defining the *relaying* square S_r and the eavesdropper-free square S_e (see Fig. 1), we obtain the constraints on n_l and n_e under which $\mathcal{SN}$ satisfies the conditions of the first step and the achievability scheme can be applied.

Step 3: In the last step, we apply the fixed total power constraint and show that the achievable secure aggregate rate of the first step can be unbounded and derive the maximum number of the eavesdroppers which can be tolerated.

The detailed proof is provided in [8]. ■

At the expense of additional complexity, we tolerate even more eavesdroppers with serial relaying (in the following theorem). In this scheme, all legitimate nodes can act as relays for the source node. 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 above to obtain our result here. The proof is provided in [8].

Theorem 2: In $\mathcal{SN}$ with fixed total power $\overline{P}_{tot}$, 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.

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*, 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, Mar. 2000.

[4] 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, May 2004.

[5] 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, May 2012.

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

[7] R. Negi and S. Goel, "Secret communication using artificial noise," in *in Proc. IEEE VTC*, Sept. 2005.

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