Supporting PHY-layer Security in Multi-link Wireless Networks Using Friendly Jamming

Rashad Eletreby, Hanif Rahbari, and Marwan Krunz
Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ
{reletreby, rahbari, krunz}@email.arizona.edu

***Abstract*—Friendly jamming is a PHY-layer technique used to secure wireless communications. Unlike previous efforts that fix the placement of the friendly jamming devices, in this paper we consider small-scale multi-link wireless networks, e.g., peer-to-peer or multihop, and jointly optimize the powers and locations of the friendly jamming devices so as to minimize the total jamming power while simultaneously achieving a given secrecy constraint. We use distributed MIMO techniques and incorporate the necessary conditions to ensure nullification of the friendly jamming signals at legitimate receivers. Two optimization strategies are explored: per-link and network-wide. Our optimization framework is based on formulating a signomial programming problem using condensation techniques to approximate the problem as a geometric program, which can then be transformed into a convex problem. We also consider the secrecy-aware routing problem for multihop networks and propose a routing metric based on the total jamming power along the path. Simulations show that our proposed schemes outperform previous schemes in terms of energy efficiency (55%–99% power saving). Moreover, our formulation ensures protecting legitimate transmissions by nullifying friendly jamming signals at legitimate receivers.**

***Index Terms*—PHY-layer security, secure routing, friendly jamming, optimal placement, signomial programming.**

I. Introduction

The broadcast nature of the wireless medium exposes communications to eavesdropping and privacy attacks. Although cryptography can be used to protect the information secrecy of a data frame's payload, it is not sufficient to prevent the leakage of side-channel information from unencrypted headers. Moreover, in many wireless standards, such as 802.11, management and control frames are often sent in the clear. Various operations of a wireless protocol, such as establishing session keys, rely on the exchange of these frames. *Information theoretic secrecy* [1], [2] at the physical (PHY) layer is a lightweight approach that aims at preventing an eavesdropper (Eve) from *decoding* a plaintext frame. A transmitter (Alice) and its legitimate receiver (Bob) are guaranteed secret communications if the Alice-Bob channel is better than Alice-Eve channel. In [1], the notion of *secrecy capacity* was introduced as the maximum rate at which Alice can securely transmit information to Bob. This rate is the difference between the mutual information between Alice and Bob, to that between Alice and Eve.

Non-zero secrecy capacity is not always possible. For example, if Eve is closer to Alice than Bob, then the Alice-Eve channel may be better than the Alice-Bob channel, resulting in zero secrecy capacity [1]. Friendly jamming (FJ), proposed in the pioneering work of Goel and Negi [3], can be used to degrade the Alice-Eve channel without harming Bob's reception. Essentially, a FJ signal is a randomly generated artificial noise. To nullify the FJ signal at Bob, the authors in [3] considered the case when Alice has multiple antennas. Alternatively, a bank of relay nodes can be utilized to transmit the artificial noise in the null space of the Alice-Bob channel.

Although FJ-based PHY-layer security has been extensively considered for single-link scenarios, only a few papers studied the problem in multi-link scenarios. Research efforts on secret communications in a multi-link network can be classified into two broad categories: Large-scale [4]–[6] and small-scale wireless networks [7], [8]. Considering a large-scale wireless network consisting of n nodes, the authors in [4] derived the per-node *asymptotic* secrecy capacity. They also proposed to use "Rx-based FJ", whereby legitimate full-duplex receivers are able to cancel the self-interference resulting from their generation of FJ signals. For the case of independent eavesdroppers, it was shown that a per-node secrecy capacity of $\Theta(\frac{1}{\sqrt{n}})$ is achievable, which is the same per-node capacity without secrecy considerations. These results imply that the per-node secrecy capacity is not affected by the presence of eavesdroppers. However, placing the FJ devices at the same locations of the communicating nodes may not be optimal from an energy consumption perspective. The interference of Rx-based FJ on other receivers was also not considered in [4].

The authors in [6] explored allowing a fraction of transmitters to cooperatively send their signals to their receivers through relay nodes, i.e., two-hop communications. The idea is based on the work in [9]; wherein, for each Alice-Bob pair, a relay node with "good" channels to Alice and Bob is selected. Relay nodes with "bad" channels to the selected relay or to Bob are used to produce FJ signals to confuse passive eavesdroppers. Instead of generating FJ signals, simultaneous transmissions are exploited in [6] to create high interference at the eavesdroppers. In this sense, the messages of other Alice-Bob pairs are utilized as FJ signals. Secrecy is guaranteed only as n tends to infinity. The results of large-scale wireless network, however, may not be always applicable to small-scale networks that can have irregular topologies.

Secure minimum-energy routing with the aid of FJ was investigated in [7], [8] for a small-scale network. The objective is to compute a minimum-energy path subject to constraints on the end-to-end communication secrecy and the throughput over the path. The authors proposed a scheme to assign FJ power

required to secure individual links. Each link was studied independently, assuming that it can be secured by its own set of FJ devices, and there is a discrete set of eavesdropping locations, each with a given probability of eavesdropping in that location. The secure routing problem was reduced to finding a path with the minimum total information and FJ power. These works, although applicable to small-scale networks, do not jointly consider the optimal placement and power allocation of the FJ devices. Moreover, they do not exploit the FJ devices associated with a given link to help in providing secrecy for another link, which can reduce the total jamming power. Finally, they assume that the FJ signals are nullified at legitimate receivers, but the conditions needed to ensure such nullification are not incorporated in the formulation. This undermines the applicability of their designs.

The example in Fig. 1 illustrates the importance of optimizing the placement of the FJ devices. Eve 1 and 2 are the most vulnerable eavesdroppers due to their proximity to Alice. If the FJ devices are placed near Bob (e.g., Rx-based jamming), they would need high power to deafen Eve 1 and 2. The FJ device would consume less power to deafen Eve 1 and 2 if they are moved to the potentially optimal location shown in Fig. 1. Note that if the FJ devices are instead moved to the centroid of the eavesdropping locations or near Alice (e.g., Tx-based jamming), they will have a larger distances to Eve 1 and 2 and consume larger amount of power to deafen them.

In this paper, we consider the problem of placing FJ devices in a small-scale multi-link wireless network, e.g., peer-to-peer (P2P) or multihop, and address the aforementioned limitations of existing PHY-layer solutions. Our contributions are summarized as follows:

- We first consider a per-link strategy and formulate an optimization problem that aims at jointly optimizing the power allocation and placement of the FJ devices for a given link under secrecy constraint. We show that our proposed scheme reduces power consumption by 55%–99% compared to the case in which the optimal placement of the FJ devices is not considered.
- We then consider the joint power allocation and placement of FJ devices under secrecy constraint for all links jointly (network-wide strategy). The exploitation of the FJ devices to simultaneously cover more than one link saves more energy and reduces the number of FJ devices relative to per-link case.
- We use distributed MIMO techniques to create a null region around all the legitimate receivers in network-wide scenario (the given receiver in per-link scenario) and accordingly establish sufficient conditions on the jamming powers and locations of the FJ devices. We incorporate these conditions as constraints in the formulation.
- We propose a novel link weight and a corresponding routing metric for the multihop scenario.

The rest of the paper is organized as follows. In Section II, we explain the underlying distributed MIMO mechanisms for generating FJ signals, and derive sufficient conditions on the powers and locations of FJ devices to ensure FJ nullification at legitimate receivers. In Section III we present the network model, formulate our problem, prove that it is an NP-hard signomial programming problem, and then approximate it by a geometric programming problem, which can further be convexified. In Section IV we propose a novel link weight for the secure routing problem. Section V provides the simulation results. Finally, Section VI concludes the paper.

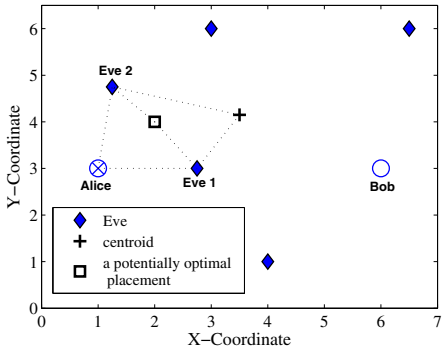

Fig. 1. Possible placements of FJ devices (without nullification constraints.) Jamming power is a function of distances to and received information signals at each Eve.

II. Distributed MIMO for FJ Nullification

If the FJ signals are to be generated by the same MIMO node (e.g., Alice), then the phases of these signals can be easily controlled to provide the desired nullification. A set of FJ signals can add destructively and nullify each other at an intended receiver if these signals, each of which traverses a different channel, are received out-of-phase and sum up to zero. To achieve this, techniques such as zero-forcing beamforming are employed to determine the phase and amplitude of each FJ signal at the transmit antennas. However, in general, FJ signals may be produced by different devices that do not share a reference clock and so are not synchronous. Hence, the signals transmitted from distributed FJ nodes may experience unknown random delays. In this section, we explain how we synchronize FJ devices, each equipped with a single antenna, and establish the sufficient conditions on the jamming signals to ensure nullification of FJ signals at all legitimate receivers.

A. Synchronization of FJ Devices

To enable synchronized FJ devices, we exploit SourceSync's synchronization protocol proposed and empirically demonstrated in [10] for OFDM systems. According to this method, a set of distributed cooperative transmitters choose a leader, who initiates the synchronization process by transmitting an OFDM-based sync header. Using the phase offsets measured across different subcarriers, each cooperating transmitter can accurately estimate the arrival time of the sync header. Based on the estimated RTT between each transmitter and the leader, and the switching time from Rx mode to Tx, each transmitter synchronizes in time with the leader. Finally, considering the propagation delay of the transmitters to the receiver, each transmitter selects a transmission time so as to synchronize the arrival of all the transmissions at the receiver.

B. Nullification of FJ Signals

Assuming that the distributed FJ nodes have been synchronized, the amplitudes/phases of their signals must be adjusted to cancel out at the legitimate receivers. Consider M legitimate receivers and N FJ nodes. The channel is characterized by an $M \times N$ channel matrix $\mathbf{H} = [h_{ij}]$, where h_{ij} is the channel coefficient between receiver i and transmitter j. By setting $N = M + 1$, we can guarantee a nonempty null space for the channel matrix $\mathbf{H}$ [3]. Let $\mathbf{y}$ be an M-by-1 vector that represents only the received FJ signals at the M receivers, let $\mathbf{x}$ be an N-by-1 vector that represents the transmitted signals from the N FJ antennas, and let $\mathbf{F}$ represent the N-by-1 precoding vector (precoder) of the FJ signal.

At any time instant (time index is dropped for simplicity) and ignoring the effect of noise, we have:

$$\mathbf{y} = \mathbf{Hx} = \mathbf{HF}m \tag{1}$$

where m denotes a random complex scalar at the current time and $||m||^2 = 1$. The Singular Value Decomposition (SVD) of $\mathbf{H}$ can be obtained as

$$\mathbf{H} = \mathbf{U}_{\mathbf{M}\times\mathbf{M}}\mathbf{\Sigma}_{\mathbf{M}\times\mathbf{N}}\mathbf{V}^{\dagger}_{\mathbf{N}\times\mathbf{N}}. \tag{2}$$

Thus, $\mathbf{y}$ can be expressed as:

$$\mathbf{y} = \mathbf{U\Sigma V}^{\dagger}\mathbf{x}. \tag{3}$$

If the jamming precoder $\mathbf{F}$ lies in the null space of $\mathbf{H}$, then $\mathbf{y} = \mathbf{Hx} = \mathbf{0}$. In our design, we select $\mathbf{F}$ as the rightmost column of the matrix $\mathbf{V}$, i.e., the kernel of $\mathbf{H}$. For a given total budget on the jamming power and a given m, the precoder $\mathbf{F}$ determines the phase of each of the FJ signals and implies some dependencies between their jamming powers so that they add up destructively at the legitimate receivers. Let $P_j = ||\mathbf{x}_j||^2 = ||\mathbf{F}_j||^2$ be the jamming power of the jth FJ device. We explicitly derive these dependencies by solving $\sum_{j=1}^{N} h_{ij}x_j = 0, \forall i = 1, \ldots, M$. It turns out that each jamming power must be a linear function of P_1 as follows:

$$P_j = \omega_j P_1, \forall j = 2, \ldots, N \tag{4}$$

where ω_j is the scalar ratio between P_j and P_1.

III. PHY-layer Security for Multi-link Networks

A. Network Model and Problem Formulation

We consider a static multi-link network, consisting of an arbitrary number of legitimate nodes, each equipped with an omni-directional antenna. These nodes form a set of links $\mathcal{L}$. Each link l consists of a source (Alice) and a destination (Bob). This general multi-link network model accommodates both P2P and multihop scenarios. For the P2P scenario, $\mathcal{L}$ consists of several independent single-hop links, connecting different Alice-Bob pairs. In the multihop case, $\mathcal{L}$ contains specific links that form several paths between various pairs of nodes. Along with the set $\mathcal{L}$, there is a finite set $\mathcal{E}$ of eavesdropping locations and a set $\mathcal{J}$ of FJ nodes. We adopt a 2-D discrete model for the points in $\mathcal{E}$ [7], [8]. The probability that an eavesdropper is in location $e \in \mathcal{E}$ is denoted by p_e. Even though this model assumes some (probabilistic) knowledge of the eavesdroppers' locations, it can represent numerous scenarios by adjusting the number of locations and the probabilities assigned to them.

The number of FJ devices can be less than or greater than $|\mathcal{E}|$. In this paper, however, we only consider the case when $|\mathcal{E}| > |\mathcal{J}|$, since the solution for the other cases is trivial: Assign a FJ node to each of the possible eavesdropping locations. In contrast to previous research [7], [8], we assume that there can be more than one eavesdropping location per active link, i.e., $\sum_{e\in\mathcal{E}} p_e$ can be greater than one.

We formulate an optimal placement and power allocation problem for the FJ devices such that the *average* SINR at each location e is less than a threshold π. To nullify FJ interference, we consider the case of cooperative FJ whereby FJ devices cooperatively nullify their jamming signals at all $|\mathcal{L}|$ legitimate receivers, even if only a subset of these receivers are active. We employ the SourceSync protocol [10] to synchronize the FJ devices. SourceSync was initially designed to exploit sender diversity by synchronously transmitting the same packet from multiple senders. However, in our design, we leverage it to sync the FJ nodes. The leader will be an active data transmitter (Alice), who sends a sync header together with a random m before its main transmission. The power of the sync-header's transmission must be adjusted to reach all FJ nodes. Following the receipt of this header, FJ nodes calculate and adjust their transmission times to create a null region around all $|\mathcal{L}|$ receivers.

Henceforth, when we say Alice and Bob we mean the transmitter and respective receiver of a specific link $l \in \mathcal{L}$, respectively. Because the FJ signals are nullified at Bob, the transmission power of Alice is only a function of the SINR threshold at Bob and the length of link l, denoted by d_l (assuming a pathloss channel model). Therefore, to maintain the SINR at Bob $\geq$ some threshold β, the minimum transmission power at Alice of link l, denoted by $P_{t,l}$, will be:

$$P_{t,l} = \frac{N_o\beta}{d_l^{-\alpha}}. \tag{5}$$

where N_o is AWGN power and α is the pathloss exponent.

For the case of cooperative jamming, the SINR at Bob (SINR$_b$) is given by:

$$\text{SINR}_b = \frac{P_{t,l}d_l^{-\alpha}}{N_o}. \tag{6}$$

The optimization problem can now be stated as follows:

$$\begin{aligned} \textbf{P1:} \quad & \underset{\{x_j, y_j, P_j\ \forall j\in\mathcal{J}\}}{\text{minimize}} \quad \sum_{j\in\mathcal{J}} P_j \\ & \text{subject to} \quad \textbf{C1: } p_e\text{SINR}_e \leq \pi, \forall e \in \mathcal{E}, \forall l \in \mathcal{L} \\ & \qquad\qquad \textbf{C2: } \sum_{j=1}^{|\mathcal{J}|} h_{ij}x_j = 0, i = 1, \ldots, |\mathcal{L}| \end{aligned} \tag{7}$$

where (x_j, y_j) are the Cartesian coordinates of FJ node j. Constraints **C1** and **C2** represent the secrecy and nullification

constraints, respectively. When link l is active, the SINR at eavesdropper e (SINR$_e$) is given by:

$$\text{SINR}_e = \frac{P_{t,l} d_{ae,l}^{-\alpha}}{N_o + \sum_{j\in\mathcal{J}} P_j d_{je}^{-\alpha}} \tag{8}$$

where $d_{ae,l}$ is the distance between Alice (of link l) and eavesdropping location e, and d_{je} is the distance between the FJ node j and eavesdropper e. Note that j, e, and hence d_{je} are not associated with a specific link l.

We propose two schemes based on formulation **P1**: per-link and network-wide schemes. For the per-link scheme, the problem is solved independently for each link. In this case, we have $|\mathcal{L}|$ independent problems. For each of these problems, the secrecy and nullification constraints are considered only for a specific link l, i.e., $|\mathcal{L}| = 1$. To ensure a nonempty nullspace for the channel matrix $\mathbf{H}$, $|\mathcal{J}|$ has to be greater than $|\mathcal{L}|$. This implies that in the per-link scheme, $\mathcal{J}$ in each problem must contain a minimum of two FJ nodes. Hence, we need at least $2|\mathcal{L}|$ FJ nodes to secure all links. For the network-wide scheme, all links and FJ devices are simultaneously considered in the secrecy and nullification constraints, i.e., we jointly optimize over all links in the set $\mathcal{L}$. One advantage of this scheme is that we only need $|\mathcal{L}| + 1$ FJ nodes to ensure that the jamming signals are nullified at all $|\mathcal{L}|$ legitimate receivers.

Considering the network-wide scheme and assuming that the locations of legitimate nodes and $P_{t,l}$ $\forall l \in \mathcal{L}$ are known, the first constraint can be simplified to:

$$\textbf{C1: } p_e \frac{\max\limits_{l\in\mathcal{L}} P_{t,l} d_{ae,l}^{-\alpha}}{N_o + \sum_{j\in\mathcal{J}} P_j d_{je}^{-\alpha}} \le \pi, \forall e \in \mathcal{E}. \tag{9}$$

B. Solution Based on Condensation Techniques

A function f is said to be *monomial* if $f(x_1, x_2, \cdots, x_n) = \prod_{i=1}^{n} x_i^{a_i}$, where $a_1, a_2, \cdots, a_n \in \mathbb{R}$. A function is said to be *posynomial* if it is a linear combination of monomials. *Signomial* programming is a class of non-convex, non-linear, and NP-hard optimization problems in which the posynomials in the constraints may be lower bounded by monomials [11].

Proposition III.1. *Problem **P1** is a signomial programming problem with $|\mathcal{E}| + |\mathcal{L}|$ signomial constraints.*

Proof. The objective function is a summation of linear variables (i.e., $\sum_{j\in\mathcal{J}} P_j$). As for the secrecy constraint, we have $\forall e \in \mathcal{E}$:

$$p_e \text{SINR}_e \le \pi, \tag{10}$$

$$\frac{p_e P_{t,l} d_{ae,l}^{-\alpha}}{\pi} \overset{(8)}{\le} N_o + \frac{P_1}{d_{1e}^{\alpha}} + \frac{P_2}{d_{2e}^{\alpha}} + \cdots + \frac{P_{|\mathcal{J}|}}{d_{|\mathcal{J}|e}^{\alpha}}, \tag{11}$$

$$\frac{\left(\frac{p_e P_{t,l} d_{ae,l}^{-\alpha}}{\pi}\right) \prod_{j\in\mathcal{J}} d_{je}^{\alpha}}{N_o(\prod_{j\in\mathcal{J}} d_{je}^{\alpha}) + \sum_{j\in\mathcal{J}} P_j \prod_{\substack{i\in\mathcal{J}\\ i\neq j}} d_{ie}^{\alpha}} \le 1 \tag{12}$$

which is in the form of:

$$\frac{Q(\mathbf{x})}{P(\mathbf{x})} \le 1 \tag{13}$$

where $Q(\mathbf{x})$ and $P(\mathbf{x})$ are monomial and posynomial, respectively.

The same analysis can be applied to the nullification constraint to show that it also represents $|\mathcal{L}|$ signomial constraints. It follows that our formulation belongs to the category of signomial programming [11], [12]. ■

Signomial problems cannot be transformed to convex problems. However, by using *condensation techniques* [13], we can approximate any multi-term posynomial $P(\mathbf{x})$ by a monomial and transform **P1** into the standard geometric programming form (i.e., $Q(\mathbf{x}) \le \widetilde{P}(\mathbf{x})$, where $\widetilde{P}(\mathbf{x})$ is the approximated monomial of the posynomial $P(\mathbf{x})$). It can be shown that optimal solution of the condensed problem is a feasible (but not necessarily optimal) solution for **P1** and so upper-bounds its optimal solution.

The original problem can then be heuristically solved by *iteratively* updating the parameters of the condensed problem. For each iteration, we use the optimal solution of the previous condensed problem to update the approximation parameters, and so on until we converge to the optimal solution of **P1**. Because the problem is non-convex, the algorithm may get stuck in a local minima, a case that is left for future work.

IV. Secrecy-aware Routing Problem

Considering the per-link scheme to jointly optimize the transmission powers and locations of the FJ devices in the multihop scenario, we propose to use the total FJ power needed to secure each link as the link weight. Thus, for link $l \in \mathcal{L}$, its weight is:

$$w(l) = \sum_{j\in\mathcal{J}} P_j. \tag{14}$$

By securing each hop, end-to-end secrecy is achieved [5], [6]. At the same time, the quality of service is ensured by having the SINR at each end of a link lower-bounded by β. To find a secure path $\mathcal{P}$ with minimum total FJ power for a given source and destination, we run the shortest path algorithm with respect to the metric w. The cost of the resultant path $c(\mathcal{P})$ is calculated as follows: $c(\mathcal{P}) = \sum_{l\in\mathcal{P}} w(l)$.

V. Performance Evaluation

In this section, we provide the simulation results of the per-link optimization strategy (both P2P and multihop). We also compare the per-link P2P to the network-wide P2P scenarios. We set $\alpha = 2$ and $p_e = 0.5$ for each eavesdropping location, $\beta = 1$ and $\pi = 1$. The number of condensation iterations is set to 100. All power values are normalized with respect to N_o. FJ nodes are initially collocated with the data transmitters, but gradually re-positioned depending on the outcome of the optimization problem. The simulations are performed in MATLAB using the CVX package.

A. Per-link, P2P Simulations

we first study the performance of our proposed per-link scheme for P2P scenarios in terms of power consumption and interference at legitimate receivers. The network consists of 1

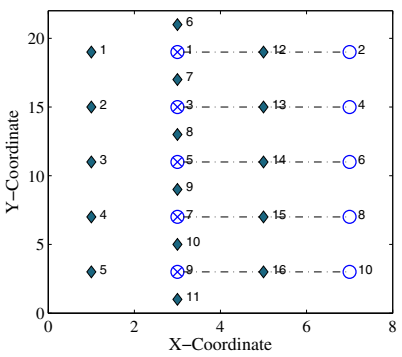

Fig. 2. Network topology for the case of five P2P links. Hollow circles, crossed circles, and diamonds represent receivers, transmitters, and potential eavesdropping locations.

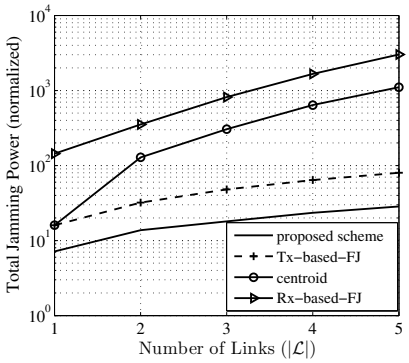

Fig. 3. Total jamming power vs. number of links for the P2P scenario (per-link).

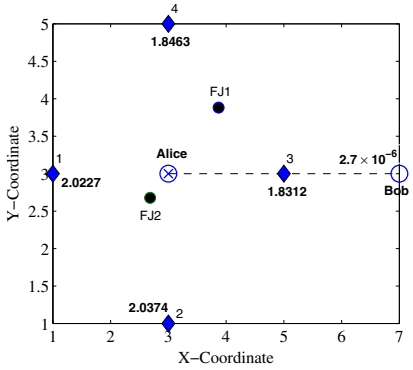

Fig. 4. Outcome of the proposed per-link scheme for the one-link case. The hollow, crossed, and solid circles represent the locations of Bob, Alice, and the FJ nodes, respectively.

to 5 unidirectional links (see Fig. 2). The set of eavesdropping locations is indicated by the diamonds in Fig. 2. The network is deployed on a grid of dimensions $(2|\mathcal{L}|+1)\times 5$ (e.g., when $|\mathcal{L}| = 1$, we simulate a grid of dimension 3×5, with four potential eavesdropping locations).

1) Power Consumption: We compare our proposed per-link P2P scheme with the following schemes in which the locations of the FJ devices are fixed:

- *Tx-based FJ:* The FJ nodes are collocated with the transmitter, which could be a MIMO transmitter with some antennas dedicated to the FJ.
- *Rx-based FJ:* The FJ nodes are placed at full-duplex receivers with perfect self-interference cancellation.
- *Centroid:* The FJ nodes are placed at the centroid of all potential eavesdropping locations.

Collectively, we refer to the above three schemes by *fixed-placement* schemes. As shown in Fig. 3, our proposed per-link P2P scheme outperforms the fixed-placement schemes achieving 55%–99% reduction in power consumption. The centroid scheme is the worst in terms of power consumption because FJ nodes are located far away from data transmitters and need to increase their powers to cover eavesdropping points around data transmitters.

To illustrate the outcome of the proposed per-link P2P case, we consider a network of one link (i.e., $|\mathcal{L}| = 1$), as shown in Fig. 4. Numbers by each node in this figure represent the amount of interference caused by the FJ nodes on that node. In Fig. 5, we show the change in the jamming power for each of the FJ nodes in Fig. 4 along with their total jamming power as a function of the optimization iteration (see Section III-B). The increase of P_{j2} may look counterintuitive because FJ2 is moving towards Eve1 and Eve2. FJ1 moves closer to Bob as it moves towards Eve3 and Eve4 to reduce P_{j1} required to suppress them. According to (4), $P_{j2} = P_{j1}(h_{11}/h_{12})^2$; so as FJ1 moves closer to Bob, P_{j2} increases quadratically with h_{11}/h_{12}. This prevents FJ2 from moving closer to Eve1 and Eve2 because the goal is to minimize the total jamming power.

In Fig. 6, we vary $|\mathcal{E}|$ for the two-link P2P case and study the performance of our proposed per-link scheme in terms of power consumption. Our proposed scheme is shown to reduce power consumption by 54%–96% compared to fixed-placement schemes. It can be noted that the jamming power for the Tx-based FJ scheme does not scale with the number of eavesdroppers. This is because FJ nodes are located very close to data transmitters, thus jamming power will be a function of the transmit power (in **P1** substitute $d_{je} = d_{ae_l}, \forall j \in \mathcal{J}$). Note that the transmit power $P_{t,l}$ does not scale with the number of the eavesdroppers.

2) Interference at Legitimate Receivers: Because FJ nullification is incorporated in our formulation, the SINR at the receiver of any link should not be less than β. Considering the example in Fig. 4, the SINR at Bob in the proposed per-link scheme is maintained at 1 dB with received jamming power of 2.7×10^{-6}. For the Tx-based and centroid schemes, however, FJ is hardly nullified and the SINR goes down to 0.5 dB, which means that Bob is unable to decode Alice's messages.

B. Per-link, Multihop (Routing) Simulations

We simulate a multihop network consisting of three interconnected and bidirectional links, as shown in Fig. 7. We calculate the minimum energy route and its associated jamming power for a packet transmitted from node 1 to node 6 along a multipath route. We also calculate $\mathbb{E}[c(\mathcal{P})]$ for all possible paths $\mathcal{P}$ (i.e., all possible Tx-Rx pairs). A summary of the results is shown in Table I.

TABLE I
COMPARISON OF THE PROPOSED PER-LINK SCHEME AND THE FIXED-PLACEMENT SCHEMES IN TERMS OF THE COST OF THE MINIMUM-ENERGY PATH

	Proposed	Tx-based FJ	Centroid	Rx-based FJ
Best path	1-2-4-6	1-2-4-6	1-3-4-6	1-2-4-6
Cost	7	48	128	304
$\mathbb{E}[c(\mathcal{P})]$	5.5	26.7	75.5	167.5

C. Network-wide Simulation Results

To study the energy efficiency of our network-wide optimization strategy, we compare our proposed per-link P2P and network-wide P2P schemes in terms of the total jamming power required to cover the whole network. As shown in

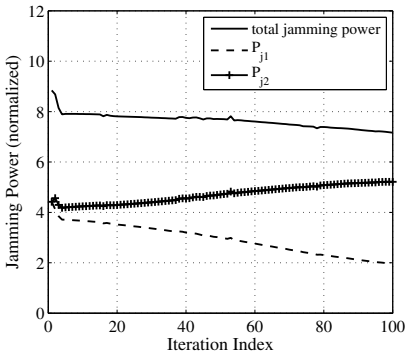

Fig. 5. Jamming power of each FJ node along with total jamming power vs. approximation (iteration) index for the example in Fig. 4.

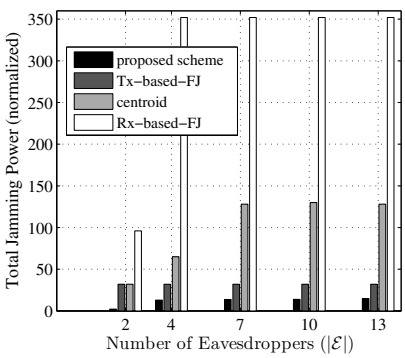

Fig. 6. Power consumption vs. number of potential eavesdropping locations for the case of two P2P links (per-link).

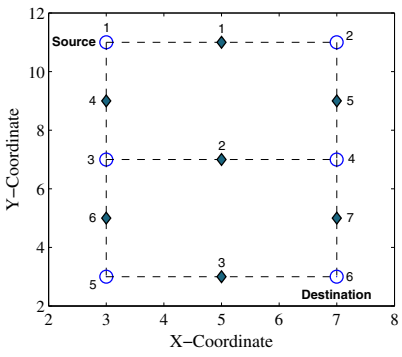

Fig. 7. Network topology for routing simulations. Hollow circles represent the legitimate nodes and diamonds represent potential eavesdropping locations.

Fig. 8, the network-wide scheme reduces power consumption by 29%–39% relative to the per-link scheme. Note also that the network-wide scheme allows for simultaneous operations of different links because it ensures the nullification of the FJ signals at all legitimate receivers.

VI. Conclusion

In this paper, we exploited friendly jamming for PHY-layer security in small-scale multi-link wireless networks in the presence of eavesdroppers. We jointly optimized the powers and locations of the friendly jamming nodes so as to minimize the total jamming power required to secure legitimate transmissions. Distributed MIMO techniques are used to nullify the friendly jamming signals at legitimate receivers. A signomial programming problem was formulated and approximated as a convex geometric programming problem using condensation techniques. We then proposed two optimization strategies: per-link and network-wide (all links jointly). It was shown that our per-link scheme outperforms previous schemes in terms of energy efficiency (55–99 percent power saving). Moreover, the network-wide optimization was shown to be more energy-efficient than per-link scheme (29–39 percent additional power saving) and also requires about half the number of friendly jamming nodes than per-link optimization. For multihop scenarios, we proposed a routing metric that finds a secure path that requires minimal jamming power.

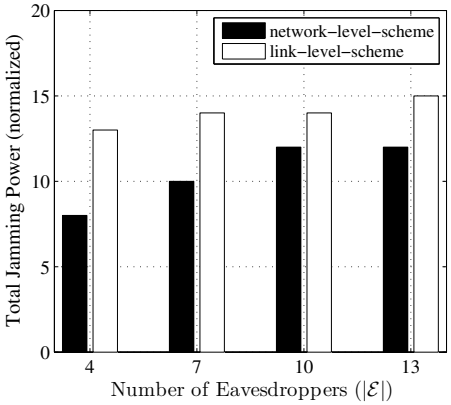

Fig. 8. Power consumption of the network-wide and per-link schemes vs. the number of potential eavesdropping locations for the case of two P2P links.

Acknowledgment

This research was supported in part by the Army Research Office (grant # W911NF-13-1-0302) and in part by the NSF (grants # IIP-1265960 and CNS-1409172). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of ARO or NSF.

References

[1] A. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

[3] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. on Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[4] J. Zhang, L. Fu, and X. Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," *IEEE/ACM Trans. Networking*, vol. 22, no. 1, pp. 66–79, Feb. 2014.

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

[6] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, "Physical layer security from inter-session interference in large wireless networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 1179–1187.

[7] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Efficient wireless security through jamming, coding and routing," in *Proc. 10th IEEE Int. Conf. Sensing, Commun., Netw. (SECON)*, New Orleans, USA, Jun. 2013, pp. 505–513.

[8] ——, "Minimum energy routing and jamming to thwart wireless network eavesdroppers," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1433–1448, Jul. 2015.

[9] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.

[10] H. Rahul, H. Hassanieh, and D. Katabi, "SourceSync: a distributed wireless architecture for exploiting sender diversity," in *Proc. ACM SIGCOMM*, New Delhi, India, Sep. 2010, pp. 171–182.

[11] M. Chiang, C. W. Tan, D. Palomar, D. O'Neill, and D. Julian, "Power control by geometric programming," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2640–2651, Jul. 2007.

[12] T. Shu and M. Krunz, "Coverage-time optimization for clustered wireless sensor networks: A power-balancing approach," *IEEE/ACM Trans. on Netw.*, vol. 18, no. 1, pp. 202–215, Feb. 2010.

[13] C. Beightler and D. Phillips, *Applied Geometric Programming*. Wiley, 1976.