Efficient Wireless Security Through Jamming, Coding and Routing

Majid Ghaderi
University of Calgary

Dennis Goeckel
UMass Amherst

Ariel Orda
Technion

Mostafa Dehghan
UMass Amherst

***Abstract*—There is a rich recent literature on how to assist secure communication between a single transmitter and receiver at the physical layer of wireless networks through techniques such as cooperative jamming. In this paper, we consider how these single-hop physical layer security techniques can be extended to multi-hop wireless networks and show how to augment physical layer security techniques with higher layer network mechanisms such as coding and routing. Specifically, we consider the secure minimum energy routing problem, in which the objective is to compute a minimum energy path between two network nodes subject to constraints on the end-to-end communication secrecy and goodput over the path. This problem is formulated as a constrained optimization of transmission power and link selection, which is proved to be NP-hard. Nevertheless, we show that efficient algorithms exist to compute both exact and approximate solutions for the problem. In particular, we develop an exact solution of pseudo-polynomial complexity, as well as an ϵ-optimal approximation of polynomial complexity. Simulation results are also provided to show the utility of our algorithms and quantify their energy savings compared to a combination of (standard) security-agnostic minimum energy routing and physical layer security. In the simulated scenarios, we observe that, by jointly optimizing link selection at the network layer and cooperative jamming at the physical layer, our algorithms reduce the network energy consumption by half.**

I. Introduction

A. Background and Motivation

Protecting the secrecy of user messages is a major concern in modern communication networks. Due to the propagation properties of the wireless medium, wireless networks can potentially make the problem more challenging by allowing an eavesdropper to have relatively easy access to the transmitted message if countermeasures are not employed. Our goal is to provide everlasting security in this wireless environment; that is, we will consider methods that will prevent an eavesdropper from ever decoding a transmitted message, even if the eavesdropper has the capability to record the signal and attempt decryption over a long period of time. There are two different classes of security techniques of interest here: cryptographic approaches based on computational complexity, and information-theoretic approaches that attempt to obtain perfect secrecy.

The traditional solution to providing security in a wireless environment is the cryptographic approach: assume that the eavesdropper will get the transmitted signal without distortion, but the desired recipient who shares a key with the transmitter is able to decode the message easily, while the eavesdropper lacking the key must solve a hard problem that is beyond her/his computational capabilities.In the information-theoretic approach to perfect secrecy [1], on the other hand, the goal is to guarantee that the eavesdroppers can never extract information from the message, regardless of their computational capability. Wyner [2] and succeeding authors [3], [4] showed that perfect secrecy is possible if the channel conditions between the transmitter and receiver were favorable relative to the channel conditions between the transmitter and eavesdropper. In this so-called *wiretap* channel, perfect secrecy at a positive rate with no pre-shared key is possible. This clearly satisfies the requirement for everlasting secrecy, but it relies on favorable channel conditions that are difficult (if not impossible) to guarantee in a wireless environment. Hence, information-theoretic secrecy requires a network design which inhibits reception at the eavesdropper while supporting reception at the desired recipient.

Our work supports both a cryptographic (computational) approach or information-theoretic approach. Per above, it is advantageous in either case to seek or create conditions so as to inconvenience reception at eavesdropper(s) while facilitating communication of the legitimate system nodes. This has been actively considered in the literature on the physical layer of wireless networks over the last decade, with approaches based on both opportunism [5], [6] and active channel manipulation [7], [8] being employed. Most of these works have arisen in the information-theoretic community and considered small networks consisting of a source, destination, eavesdropper, and perhaps a relay node(s) [6]–[12]. More recently, there has been the active consideration of large networks with the introduction of the secrecy graph to consider secure connectivity [13]–[15] and a number of approaches to throughput scaling versus security tradeoffs [16]–[18]. Hence, whereas there has been a significant consideration of small single- and two-hop networks and asymptotically large multi-hop networks, there has been almost no consideration of the practical multi-hop networks that lie between those two extremes. It is this large and important gap that this paper fills.

B. Our Work

Consider a network where system nodes communicate with each other wirelessly, possibly over multiple hops, such as in wireless mesh networks and ad hoc networks. A set of *eavesdroppers* try to passively listen to communications among legitimate system nodes. To prevent the eavesdroppers from successfully capturing communications between system nodes, mechanisms to thwart such are employed at the physical layer of the network (*i.e.*, physical layer security). Two nodes that wish to communicate securely may need to do so over multiple hops in order to thwart eavesdroppers or simply because the nodes are not within the reach of each other. While we make no argument about the optimality or practicality of any specific physical layer

security mechanism, for the sake of concreteness, we focus on *cooperative jamming*, which has recently received considerable attention [7]–[12]. In cooperative jamming, whenever a node transmits a message, a number of cooperative nodes, called *jammers*, help the node conceal its message by transmitting a carefully chosen signal to raise the background *noise* level and degrade the eavesdropping channels. Because our general philosophy applies to any physical layer approach, the framework can be extended to include other forms of physical layer security. However, some of the attractive features of cooperative jamming that motivated us to consider this technique include:

1) Opportunistic techniques [5], [6] that exploit the time-varying wireless channel may suffer from excessive delays. For applications that require security without an excessive delay, active channel manipulation such as cooperative jamming should be adopted. The price to be paid, in this case, is the increased interference due to jamming.
2) Multi-antenna systems can also be used to jam eavesdroppers. However, the use of multiple antennas on every wireless device may not be feasible due to cost and size (*e.g.*, wireless sensors). Cooperative jamming is a distributed alternative to multi-antenna systems.
3) The implementation of node cooperation, while requiring a more complex physical layer, is advancing rapidly [19], [20] and has been incorporated in commercial wireless technologies such as LTE systems [21]. Indeed, node cooperation at physical layer has been implemented on software-defined [22] as well as commodity radios [23].

In this general case, the main questions are: (1) how to choose the intermediate nodes that form a multi-hop path from the source node to the destination node, and (2) how to configure each hop at the physical layer with respect to the security and throughput constraints of the path. Specifically, the problem we consider in this paper is how to find a *minimum cost* path between a source and destination node in the network, while guaranteeing a pre-specified lower bound on the *end-to-end secrecy* and *goodput* of the path. In a wireless network, transmission power is a critical factor affecting the throughput and lifetime of the network. With cooperative jamming at the physical layer, transmission power is even more important due to the additional interference caused by jamming signals if they need to be employed. Thus, in this work, we consider the amount of end-to-end transmission power as the cost of a path with the objective of finding secure paths that consume the least amount of energy. In turn, such paths, by minimizing interference in the network, result in *higher* throughput. Note that solutions employing power only at the nodes transmitting the messages (and no cooperative jamming) are part of the space over which the optimization will be performed; thus, if it is more efficient to not employ cooperative jamming, such a solution will be revealed by our algorithms.

While it might seem that physical layer security techniques can be extended to multi-hop networks by implementing them on a hop-by-hop basis, in general, such extensions sacrifice performance or are not feasible. The eavesdropping probability on a link is a function of the power allocation on that link. A hop-by-hop implementation is unable to determine the optimal eavesdropping probability and consequently power allocation for each link in order to satisfy the end-to-end constraints (*i.e.*, the chicken-egg problem). Moreover, a hop-by-hop approach overlaid on a shortest path routing algorithm might pay an enormous penalty to mitigate eavesdroppers on some links (*e.g.*, by routing through a node with one or more links, that, because of system geometry, are very vulnerable to nearby eavesdroppers). A routing algorithm that is designed in conjunction with physical layer security can selectively employ links that are easier to secure when it is power-efficient to do so and, in such a way, minimize the impact of the security constraint on end-to-end throughput.

Our main contributions can be summarized as follows:

- We formulate the secure minimum energy routing problem with end-to-end security and goodput constraints as a constrained optimization of transmission power at the physical layer and link selection at the network layer.
- We prove that the secure minimum energy routing problem is NP-hard, and develop exact and ϵ-approximate solutions of, respectively, pseudo-polynomial and fully-polynomial time complexity for the problem.
- We show how cooperative jamming can be used to establish a secure link between two nodes in the presence of multiple eavesdroppers or probabilistic information about potential eavesdropping locations by utilizing random linear coding at the network layer.
- We provide simulation results that demonstrate the significant energy savings of our algorithms compared to the combination of security-agnostic minimum energy routing and physical layer security.

Finally, while there are numerous works on secure routing in wireless networks (see, *e.g.*, [24] and references therein), their focus is on preventing malicious attacks that disrupt the operation of the routing protocol using such mechanisms as authentication and cryptography. The focus of this paper, on the other hand, is on secure transmission of messages via the most cost-effective paths, which is orthogonal to the secure routing problem considered in the existing literature. Also, our approach is complimentary to those security techniques that rely on network topology [25], [26], by providing a mechanism to find a minimum-cost path that is information-theoretically secure, regardless of the diversity of paths in the network.

The rest of the paper is organized as follows. Our system model is described in Section II. The optimal link and path cost are analyzed in Sections III and IV. Our routing algorithms are presented in Section V. Simulation results are discussed in Section VI, while Section VII concludes the paper. **Due to space limitation, some proofs, technical details and simulation results are omitted from this version and can be found (online) in [27].**

II. System Model and Assumptions

Consider a wireless network where each node (legitimate or eavesdropper) is equipped with a single omni-directional antenna. A K-hop route Π between a source and a destination in the network is a sequence of K links connecting the source to

the destination[1]. We use the notation $\Pi = \langle \ell_1, \ldots, \ell_K \rangle$ to refer to a route that is formed by K links ℓ_1 to ℓ_K. A link $\ell_k \in \Pi$ is formed between two nodes S_k and D_k on route Π. We assume that every link ℓ_k is exposed to a set of (potential) eavesdroppers denoted by $\mathcal{E}_k$. Whenever S_k transmits a message to D_k, a set of trusted nodes, called jammers, cooperate with S_k to conceal its message from the eavesdroppers in $\mathcal{E}_k$ by jamming S_k's signal at the eavesdroppers. The set of the jammers cooperating with S_k is denoted by $\mathcal{J}_k = \{J_1 \ldots, J_{|\mathcal{J}_k|}\}$, where $|\mathcal{A}|$ denotes the cardinality of set $\mathcal{A}$. Throughout the paper, we use the notation $\ell_k = (S_k, D_k, \mathcal{E}_k, \mathcal{J}_k)$ to identify link ℓ_k.

In the following subsections, for notational simplicity, we may drop the link index k whenever there is no ambiguity.

A. Wireless Channel Model

Consider the discrete-time equivalent model for a transmission from node S to node D. Let x_S be the normalized (unit-power) symbol stream to be transmitted by S, and let y_D be the received signal at node D. We assume that transmitter S is able to control its power P_S in arbitrarily small steps, up to some maximum power $P_{\max}$. Let n_D denote the receiver noise at D, where n_D is assumed to be a complex Gaussian random variable with $\mathbb{E}\left[|n_D|^2\right] = N_0$. The received signal at D is expressed as

$$y_D = \sqrt{P_S}\, h_{S,D}\, x_S + n_D, \tag{1}$$

where $h_{S,D}$ is the complex channel gain between S and D. The channel gain is modeled as $h_{S,D} = |h_{S,D}|e^{\theta_{S,D}}$, where $|h_{S,D}|$ is the channel gain magnitude and $\theta_{S,D}$ is the uniform phase. We assume a non line-of-sight environment, implying that $|h_{S,D}|$ has a Rayleigh distribution, and that $\mathbb{E}[|h_{S,D}|^2] = 1/d^{\alpha}_{S,D}$, where $d_{S,D}$ is the distance between nodes S and D, and α is the path-loss exponent (typically between 2 and 6). This is the standard narrowband fading channel model employed in the physical layer literature [28].

B. Adversary Model

We limit our attention to non-colluding passive eavesdroppers as in prior work [6]–[12]. Although there are other forms of adversarial behavior, their consideration is beyond the scope of this paper.While the literature on physical layer security often assumes not only eavesdropper locations but also either perfect (*e.g.*, [8]) or imperfect (*e.g.*, [12]) knowledge at the transmitters and jammers of the complex channel gains of the eavesdropping channels (*i.e.*, availability of instantaneous eavesdropper channel state information (CSI)), we consider the more realistic scenario, in which CSI for eavesdropping channels is not available.

Specifically, we assume that each link ℓ_k is subject to potential eavesdropping from a set of locations denoted by $\mathcal{E}_k = \{E_1, \ldots, E_{|\mathcal{E}_k|}\}$, where the probability of eavesdropping from location E_i is given by $p(E_i)$. Although our model cannot be applied to every possible scenario, it is more general compared to the models in the literature on physical layer security (see [7]–[12], and references therein) and can be used to represent a wide range of eavesdropping scenarios. For example, setting all $p(E_i)$'s to 1 for a link models multiple eavesdroppers for that link. Other examples include military scenarios where the locations of enemy installations are known, or wireless networks where a malicious user(s) has been detected. In general, for any given link, there is only a limited region around the link that can be exploited for eavesdropping (due to the attenuation of wireless signals). By dividing the effective eavesdropping region to a few smaller areas (for example, by tessellating the eavesdropping region [29]), one can compute the most effective eavesdropping location within each area, and consequently, construct the set of eavesdropping locations for that link. As the uncertainty about the location of eavesdroppers increases, so does the cost of establishing a secure link as will be shown in the next section.

[1]The terms "path" and "route" are used interchangeably in the paper.

C. Physical Layer Security Model

Consider a secure link formed between source S and receiver D with the help of jammers $\mathcal{J}$. For the moment, we assume that cooperative jamming is implemented at the physical layer to deal with a *single* eavesdropper E located at a *fixed* position. Later, in Section III, we show how this physical layer primitive can be used to provide security against multiple eavesdroppers or unknown eavesdropping locations.

When node S transmits a message, there are multiple ways in which cooperative jamming by system nodes can be exploited, ranging from relatively simple noncoherent techniques to sophisticated beamforming techniques [30]. Since the *implementation* of beamforming in other contexts, with the same challenges of synchronization in the wireless environment, is advancing rapidly [19], [20], we assume that the jammers cooperatively *beamform* a common artificial noise signal z to the receiver in such a way that their signals cancel out at the receiver [31]. The noise signal z is transmitted in the *null space* of the channel vector $\mathbf{h}_D = [h_{J_1,D}, h_{J_2,D}, \ldots, h_{J_{|\mathcal{J}|},D}]^{\mathrm{T}}$ where, $h_{J_i,D}$ denotes the channel gain between jammer J_i and destination D and $\mathbf{A}^{\mathrm{T}}$ denotes the conjugate transpose of vector $\mathbf{A}$. Thus, the signal transmitted by the jammers can be expressed as $\mathbf{s}_J = \mathbf{h}_D^{\perp} z$, where $\mathbf{h}_D^{\perp}$ is a vector chosen in the null space of $\mathbf{h}_D$. It follows that the total transmission power of the jammers is given by $P_J = \| \mathbf{h}_D^{\perp} \|^2$. Then, the signals received at the destination and the eavesdropper are given by

$$\begin{aligned} y_D &= \sqrt{P_S}\, h_{S,D}\, x_S + n_D, \\ y_E &= \sqrt{P_S}\, h_{S,E}\, x_S + \mathbf{h}_E^{\mathrm{T}} \mathbf{h}_D^{\perp} z + n_E, \end{aligned} \tag{2}$$

where, $\mathbf{h}_E = [h_{J_1,E}, h_{J_2,E}, \ldots, h_{J_{|\mathcal{J}|},E}]^{\mathrm{T}}$ is the channel gain vector between the jammers and the eavesdropper, and n_D and n_E denote the complex Gaussian noise at the destination and eavesdropper, respectively, with $\mathbb{E}\left[|n_D|^2\right] = \mathbb{E}\left[|n_E|^2\right] = N_0$.

Although the jammers try to prevent the eavesdropper from successfully receiving the message, there is still some probability that the eavesdropper actually obtains the message due to the fact that the channel to the eavesdropper is *unknown* in our model, *i.e.*, $\mathbf{h}_E$ and $h_{S,E}$ are unknown. Recalling that the signal-to-interference-plus-noise ratio (SINR) at the destination is controlled via power control, let γ_E denote the minimum required SINR at the eavesdropper in order to violate the security constraints of the protocol (*e.g.*, for the cryptographic case, the SINR above which the eavesdropper can record a meaningful version of the transmitted signal; in the information-theoretic case, the SINR above which, for a given wire-tap code,

the equivocation does not equal the entropy of the message). Let SINR_E denote the SINR at the eavesdropper. We have (see [27]):

$$\mathbb{P}\left\{\mathrm{SINR}_E \geq \gamma_E\right\} \leq \frac{e^{-N_0\gamma_E \frac{d_{S,E}^{\alpha}}{P_S}}}{1+\frac{\gamma_E d_{S,E}^{\alpha}}{P_S}\sum_{J_i\in\mathcal{J}}\frac{P_J}{d_{J_i,E}^{\alpha}}}, \tag{3}$$

where $d_{A,B}$ is the distance between nodes A and B. In the remainder of the paper, we use (3) in equality form to compute the eavesdropping probability for a given jamming power P_J. While this results in a (slightly) conservative power allocation, it is sufficient to satisfy the security requirement of each link.

D. Routing Model

Consider a K-hop route $\Pi = \langle \ell_1, \ldots, \ell_K \rangle$ between a source and destination in the network. Let $\mathcal{L}$ denote the set of all possible routes between the source and destination. Let $\mathcal{C}(\Pi)$ denote the cost of route Π, which is defined as the summation of the costs of the links forming the route. With slight abuse of the notation, we use $\mathcal{C}(\ell_k)$ to denote the cost of link ℓ_k as well. The secure routing problem is then defined as follows.

SMER: Secure Minimum Energy Routing Problem
Consider a wireless network and a set of eavesdroppers distributed in the network. Given a source and destination, find a minimum energy path Π^* between the source and destination subject to constraints π and λ on the end-to-end successful eavesdropping probability and goodput of the path respectively.

Let $\lambda(\ell_k)$ denote the goodput of link $\ell_k \in \Pi$. We have,

$$\lambda(\Pi) = \min_{\ell_k\in\Pi} \lambda(\ell_k), \tag{4}$$

where $\lambda(\Pi)$ denotes the goodput of path Π. Since goodput of a link is an increasing function of the transmission power of the transmitter of that link, a necessary condition for minimizing power over the path Π is given by $\lambda(\ell_k) = \lambda$, for all $\ell_k \in \Pi$. Thus, our power allocation scheme (see Section III) establishes links that achieve exactly the minimum required goodput λ. Consequently, the constraint on the end-to-end goodput is satisfied by any path in the network, and hence does not need to be explicitly considered when solving SMER. As such, SMER can be formally described by the following optimization problem:

$$\begin{aligned} \Pi^* = \arg\min_{\Pi\in\mathcal{L}} & \sum_{\ell_k\in\Pi} \mathcal{C}(\ell_k) \\ s.t. \quad & \mathbb{P}\left\{\text{eavesdropping on route } \Pi\right\} \leq \pi, \end{aligned} \tag{5}$$

for some pre-specified π $(0 < \pi < 1)$.

The constraint on the route eavesdropping probability in the above optimization problem can be expressed in terms of the eavesdropping probability on individual links ℓ_k that form the route Π, as $\prod_{\ell_k\in\Pi}(1-\pi_k) \geq 1-\pi$, where π_k $(0 < \pi_k < 1)$ denotes the successful eavesdropping probability on link ℓ_k.

Lemma 1: The cost of route Π is a monotonically increasing function of $\prod_{\ell_k\in\Pi}(1-\pi_k)$.

Proof: See [27]. ∎

Thus, to minimize the cost of the optimal route, the inequality constraint can be substituted by the equality constraint $\prod_{\ell_k\in\Pi}(1-\pi_k) = 1-\pi$. On each link ℓ_k, it is desirable to keep the successful eavesdropping probability π_k close to 0. In this case, the product $\prod_{\ell_k\in\Pi}(1-\pi_k)$ can be approximated by the expression $1-\sum_{\ell_k\in\Pi}\pi_k$. By substituting the approximate linearized constraint in the routing problem, the following optimization problem is obtained

$$\begin{aligned} \Pi^* = \arg\min_{\Pi\in\mathcal{L}} & \sum_{\ell_k\in\Pi} \mathcal{C}(\ell_k) \\ s.t. \quad & \sum_{\ell_k\in\Pi} \pi_k = \pi\,. \end{aligned} \tag{6}$$

In the rest of the paper, we focus on this optimization problem.

III. Secure Link Cost

Let $\mathcal{C}(\ell_k)$ denote the cost of link $\ell_k = (S_k, D_k, \mathcal{E}_k, \mathcal{J}_k)$. The link cost is composed of two components: (1) the source power, and (2) the jammers power. Then, $\mathcal{C}(\ell_k)$ is given by:

$$\mathcal{C}(\ell_k) = P_S^{(k)} + P_J^{(k)}, \tag{7}$$

where $P_S^{(k)}$ and $P_J^{(k)}$ denote, respectively, the average source and jammers power on link ℓ_k. In the following subsections, we will compute the optimal values of $P_S^{(k)}$ and $P_J^{(k)}$ under the constraint of eavesdropping probability π_k.

A. Source Transmission Power

Assume that the (complex) fading channel coefficient h_{S_k,D_k} is known at the source S_k of the given link ℓ_k. Because we are trying to maintain a fixed rate (and, hence, a fixed received power), the source will attempt to invert the channel using power control. However, for a Rayleigh frequency-nonselective fading channel, as assumed here, the expected required power for such an inversion goes to infinity, and, hence *truncated channel inversion* is employed [28, Pg. 112]. In truncated channel inversion, the source maintains the required link quality except for extremely bad fades, where the link goes into outage. When a link is in a bad fade, the source will need to wait until the link improves before transmitting the packet and delay will be incurred. To limit the delay, we maintain a given outage probability ρ per link. Then, for a given packet, we need to transmit at rate $R = \lambda/(1-\rho)$ to maintain the desired goodput λ. Associated with that rate R is the SINR threshold $\gamma_D = 2^R - 1$ required for successful reception at the link destination [28].

Let $P_S^{(k)}$ denote the average transmission power of S_k, and let $P_S^{(k)}(|h_{S_k,D_k}|^2)$ denote the power used for a given packet as a function of the power $|h_{S_k,D_k}|^2$ in the fading channel between S_k and D_k. Per above, below some threshold τ, the source will wait for a better channel. From the Rayleigh fading model employed, $|h_{S_k,D_k}|^2$ is exponential with parameter $1/d_{S_k,D_k}^{\alpha}$; hence, $\tau = -\ln(1-\rho)\cdot d_{S_k,D_k}^{\alpha}$ and truncated channel inversion yields:

$$P_S^{(k)}(|h_{S_k,D_k}|^2) = \begin{cases} \frac{\gamma_D}{|h_{S_k,D_k}|^2}\cdot d_{S_k,D_k}^{\alpha}, & |h_{S_k,D_k}|^2 \geq \tau \\ 0, & |h_{S_k,D_k}|^2 < \tau \end{cases} \tag{8}$$

Then, the average power employed on the link is given by:

$$P_S^{(k)} = \frac{1}{1-\rho}\int_{\tau}^{\infty}\frac{\gamma_D}{x}\cdot d_{S_k,D_k}^{\alpha} e^{-x}dx = \gamma_D\cdot k_\rho \cdot d_{S_k,D_k}^{\alpha}, \tag{9}$$

where k_ρ is a constant that depends on the parameter ρ.

B. Jammers Transmission Power

Our physical layer security primitive described in Section II can provide security only against a single eavesdropper at a fixed location. To achieve security in the presence of multiple eavesdroppers or uncertainty about the location of eavesdroppers, we utilize random linear coding on each link (other forms of coding [32] can be equally incorporated).

Consider link ℓ_k between transmitter S_k and receiver D_k with the associated set of potential eavesdropping locations $\mathcal{E}_k = \{E_1, \ldots, E_{|\mathcal{E}_k|}\}$. Transmitter S_k performs coding over $|\mathcal{E}_k|$ messages accumulated in its buffer for transmission to D_k. To generate a coded message, S_k selects a random subset of the messages in its buffer and adds them together (module-2). To recover the original messages, the receiver needs to collect $|\mathcal{E}_k|$ linearly independent coded messages. In order to transmit only linearly independent coded messages, S_k keeps track of the coded messages it has transmitted so far. Let m_i denote the i-th coded message that is being transmitted to D_k. To securely transmit m_i, S_k employs the cooperative jamming primitive of Section II assuming that there is an eavesdropper in location $E_i \in \mathcal{E}_k$. Since each coded message is hidden from at least one eavesdropping location, it is guaranteed that an eavesdropper located at location E_j, for all $E_j \in \mathcal{E}_k$, will not be able to obtain any information about the original messages.

Note that our model can be extended to handle colluding eavesdroppers by requiring that at least one of the coded messages be protected against all eavesdroppers (see [27]).

1) Single Eavesdropper: Let $\pi_k(|h_{S_k,D_k}|^2)$ denote the probability the eavesdropper achieves SINR greater than threshold γ_E for a given source to destination channel h_{S_k,D_k} (recall that the source power will fluctuate as h_{S_k,D_k} fluctuates, and this will impact the interception probability at the eavesdropper). To maintain a given π_k, it is sufficient to maintain $\pi_k(|h_{S_k,D_k}|^2) = \pi_k$ across all $|h_{S_k,D_k}|^2$. Under this condition, using (3), it is obtained that

$$\pi_k = \frac{1}{1 + \frac{\gamma_E d^{\alpha}_{S_k,E_k}}{P_S^{(k)}} \sum_{J_i \in \mathcal{J}_k} \frac{P_J^{(k)}}{d^{\alpha}_{J_i,E_k}}} \cdot \tag{10}$$

2) Multiple Eavesdroppers: Let $\pi_k(i)$ denote the successful eavesdropping probability on link ℓ_k conditioned on having an eavesdropper at location E_i. The unconditional eavesdropping probability π_k on link ℓ_k is then given by the approximate relation $\pi_k = \sum_{E_i \in \mathcal{E}_k} p_k(E_i) \cdot \pi_k(i)$, where $p_k(E_i)$ is the probability of having an eavesdropper at location E_i. Since jamming power depends on the location of the eavesdroppers, by optimally allocating jamming power to each potential eavesdropping location, we can minimize the total jamming power across all eavesdropping locations for a given link.

The minimum jamming power for link ℓ_k over all eavesdropping locations $\mathcal{E}_k$ is given by the solution of the following optimization problem:

$$\begin{aligned} &\min_{P_J^{(k)}(i)} \sum_{E_i \in \mathcal{E}_k} P_J^{(k)}(i) \\ &s.t. \quad \sum_{E_i \in \mathcal{E}_k} p_k(E_i) \cdot \pi_k(i) = \pi_k, \end{aligned} \tag{11}$$

where $P_J^{(k)}(i) = \sum_{J_j \in \mathcal{J}_k} P_j^{(k)}(i)$ is the jamming power conditioned on the eavesdropping location E_i. Define $\phi_k(i)$ as follows

$$\phi_k(i) = \frac{\gamma_E}{\gamma_S k_\rho} \left(\frac{d_{S_k,E_i}}{d_{S_k,D_k}}\right)^{\alpha} \sum_{J_j \in \mathcal{J}_k} \frac{1}{d^{\alpha}_{J_j,E_i}} \cdot \tag{12}$$

After substituting for $\pi_k(i)$ using (10), we obtain the following optimization problem:

$$\begin{aligned} &\min_{P_J^{(k)}(i)} \sum_{E_i \in \mathcal{E}_k} P_J^{(k)}(i) \\ &s.t. \quad \sum_{E_i \in \mathcal{E}_k} \frac{p_k(E_i)}{1 + \phi_k(i) P_J^{(k)}(i)} = \pi_k \cdot \end{aligned} \tag{13}$$

The optimization variables in this optimization problem are the jamming powers $P_J^{(k)}(i)$. Using the Lagrange multipliers technique, it is obtained that [27]

$$\pi_k(i) = \frac{1}{\phi_k(i)} \frac{1/\sqrt{\frac{p_k(E_i)}{\phi_k(i)}}}{\sum_{E_i \in \mathcal{E}_k} \sqrt{\frac{p_k(E_i)}{\phi_k(i)}}} \pi_k \cdot \tag{14}$$

Consequently, the average jamming power per message on link ℓ_k is given by:

$$P_J^{(k)} = \frac{1}{\pi_k} \frac{1}{|\mathcal{E}_k|} \left(\sum_{E_i \in \mathcal{E}_k} \sqrt{\frac{p_k(E_i)}{\phi_k(i)}} \right)^2 - \frac{1}{|\mathcal{E}_k|} \sum_{E_i \in \mathcal{E}_k} \frac{1}{\phi_k(i)} \cdot \tag{15}$$

IV. Secure Path Cost

In this section, we formulate the optimal cost of a *given* path Π subject to an end-to-end eavesdropping probability π.

A. Optimal Path Cost

Consider a given path Π. We find the optimal cost of path Π by solving the optimization problem (6). Consider link $\ell_k \in \Pi$, where $\ell_k = (S_k, D_k, \mathcal{E}_k, \mathcal{J}_k)$. Define x_k and y_k as follows:

$$x_k = \frac{1}{\sqrt{|\mathcal{E}_k|}} \sum_{E_i \in \mathcal{E}_k} \sqrt{\frac{p_k(E_i)}{\phi_k(i)}}, \text{ and, } y_k = \frac{1}{|\mathcal{E}_k|} \sum_{E_i \in \mathcal{E}_k} \frac{1}{\phi_k(i)} \cdot$$

By substituting the above expressions in the optimal routing formulation described in (6), the following optimization problem is obtained for minimizing the cost $\mathcal{C}(\Pi)$ of route Π:

$$\begin{aligned} &\min_{P_J^{(k)}} \sum_{\ell_k \in \Pi} P_S^{(k)} + P_J^{(k)} \\ &s.t. \quad \sum_{\ell_k \in \Pi} \left(\frac{x_k^2}{y_k + P_J^{(k)}} \right) = \pi \cdot \end{aligned} \tag{16}$$

The optimization variables in this optimization problem are jamming powers $P_J^{(k)}$. Using the Lagrange multipliers technique, the following relation for the optimal eavesdropping probability π_k on link ℓ_k is obtained [27]

$$\pi_k = \frac{x_k}{\sum_{\ell_i \in \Pi} x_i} \pi \cdot \tag{17}$$

For a given route Π and end-to-end eavesdropping probability π, we can use (17) to divide π between links $\ell_k \in \Pi$. Having computed π_k, the optimal power allocated to jammers on link ℓ_k is given by the following expression:

$$P_J^{(k)} = \frac{1}{\pi} \cdot x_k \sum_{\ell_i \in \Pi} x_i - y_k, \tag{18}$$

which yields the following expression for the cost of link ℓ_k

$$\mathcal{C}(\ell_k) = \left((\gamma_S k_\rho) \cdot d^{\alpha}_{S_k,D_k} - y_k \right) + \frac{1}{\pi} \left(x_k \sum_{\ell_i \in \Pi} x_i \right), \quad \text{for } \ell_k \in \Pi \cdot \tag{19}$$

Consequently, the cost of secure route Π is given by:

$$\mathcal{C}(\Pi) = \sum_{\ell_k \in \Pi} \big((\gamma_S k_\rho) \cdot d_{S_k, D_k}^{\alpha} - y_k \big) + \frac{1}{\pi} \Big(\sum_{\ell_k \in \Pi} x_k \Big)^2 . \quad (20)$$

To this end, for a given route Π between the source and destination, the optimal cost of Π subject to the end-to-end eavesdropping constraint π is given by (20). The optimal cost is achieved by allocating $P_S^{(k)}$ and $P_J^{(k)}$ to each link $\ell_k \in \Pi$ using (9) and (18), respectively. Thus, SMER is reduced to finding a path, among all possible paths between the source and destination, that minimizes the optimal path cost (20). The following proposition formally states this result.

Proposition 1: SMER with end-to-end eavesdropping and goodput constraint π and λ, respectively, is equivalent to finding a path that minimizes the optimal path cost $\mathcal{C}(\Pi)$ as given by (20).

B. Optimal Path Cost Structure

Define $\mathcal{C}_1(\ell_k)$ and $\mathcal{C}_2(\ell_k)$ as follows:

$$\begin{aligned} \mathcal{C}_1(\ell_k) &= (\gamma_S k_\rho) \cdot d_{S_k, D_k}^{\alpha} - y_k, \\ \mathcal{C}_2(\ell_k) &= \frac{1}{\sqrt{\pi}} \cdot x_k \,. \end{aligned} \quad (21)$$

Then the optimal path cost (20) can be expressed as

$$\mathcal{C}(\Pi) = \sum_{\ell_k \in \Pi} \mathcal{C}_1(\ell_k) + \Big(\sum_{\ell_k \in \Pi} \mathcal{C}_2(\ell_k) \Big)^2 . \quad (22)$$

It is important to note that, while the $\mathcal{C}_1(\ell_k)$'s may assume negative values, the path cost structure in (22) is monotonous in the number of links, *i.e.*, if a path $\hat{\Pi}$ is a subset of a path Π, then $\mathcal{C}(\hat{\Pi}) < \mathcal{C}(\Pi)$. This is because $\pi < 1$, and it can be shown that $\big(\sum_{\ell_k \in \Pi} x_k\big)^2 > \sum_{\ell_k \in \Pi} y_k$. Consequently, (22) is minimized by a *simple* path.

V. Secure Minimum Energy Routing

In this section, we begin by establishing that SMER is NP-hard. Then, by exploiting the structure of the optimal solution, we employ dynamic programming to obtain a pseudo-polynomial time algorithm that provides an exact solution. This means that the problem is weakly NP-hard [33], thus fully polynomial time approximate schemes are possible. Accordingly, we conclude the section by presenting a fully polynomial time ϵ-approximation algorithm for the problem, which takes an approximation parameter $\epsilon > 0$ and after running for time polynomial in the size of the network and in $1/\epsilon$, it returns a path whose cost is at most $(1+\epsilon)$ times more than the optimal value.

A. Computational Complexity

We first show that our routing problem is NP-hard.

Theorem 1: Problem SMER is NP-hard.

Proof: We describe a polynomial time reduction of the Partition problem [33] to SMER. Given a set of integers $\mathcal{S} = \{k_1, k_2, \ldots, k_n\}$, with $\sum_{i=1}^{n} k_i = 2 \cdot K$, the Partition problem is to decide whether there is a subset $\mathcal{S}'$ of $\mathcal{S}$ such that $\sum_{i \in \mathcal{S}'} k_i = K$. Given an instance $\mathcal{S} = \{k_1, k_2, \ldots, k_n\}$ of the Partition problem, with $\sum_{i=1}^{n} k_i = 2 \cdot K$, we construct the following network. The set of nodes is identical to $\mathcal{S}$. For $i = 1$ to $n-1$, we interconnect node k_i to node k_{i+1} with two links, as follows: an "upper" link $\ell_i^{(u)}$, to which we assign $\mathcal{C}_1(\ell_i^{(u)}) = 2 \cdot K \cdot k_i$ and $\mathcal{C}_2(\ell_i^{(u)}) = 0$, and a "lower" link $\ell_i^{(w)}$, to which we assign $\mathcal{C}_1(\ell_i^{(w)}) = 0$ and $\mathcal{C}_2(\ell_i^{(w)}) = k_i$.

Lemma 2: The answer to the Partition problem is affirmative *iff* the solution to SMER in the constructed network, *i.e.*, the minimum value of (22) of a path between nodes k_1 and k_n, equals $3 \cdot K^2$.

Proof: See [27]. ∎

Since the Partition problem is NP-complete [33], the theorem follows. ∎

B. Pseudo-Polynomial Time Exact Algorithm

First, scale the values of the $\mathcal{C}_2(\ell)$'s for any link ℓ in the network so that they are all integers. Let B denote an upper-bound on the sum of the $\mathcal{C}_2(\ell)$'s on any simple path. A trivial bound is given by $B = (N-1) \cdot \mathcal{C}_2^{max}$, where N is the number of nodes in the network and $\mathcal{C}_2^{max}$ is the maximum value of $\mathcal{C}_2(\ell)$ among all network links.

Algorithm 1 DP-SMER (source s, dest. d, network $\mathcal{N}$).

```
/* path cost from s to itself is always 0 */
for b = 1 → B do
    C_s(b) = 0
/* initial path cost from s to any other node is infinite */
for all n_i ∈ N, n_i ≠ s do
    for b = 1 → B do
        C_i(b) = ∞
for b = 1 → B do
    /* all node pairs can form a link and be neighbors */
    for all n_i ∈ N do
        for all n_j ∈ N do
            /* update path cost via the neighboring nodes */
            if b + C_2(ℓ_ij) ≤ B then
                t = C_i(b) + C_1(ℓ_ij)
                if t < C_j(b + C_2(ℓ_ij)) then
                    Π_j(b + C_2(ℓ_ij)) = i /* set n_j's parent to n_i */
                    C_j(b + C_2(ℓ_ij)) = t /* update path cost */
/* include the "b" component, i.e., C_2, in the path costs */
for b = 1 → B do
    Ĉ_d(b) = C_d(b) + b^2
/* choose the best value for reaching the destination */
b* = arg min_b Ĉ_d(b)
return [Ĉ_d(b*), Π(b*)]
```

Our algorithm, termed DP-SMER, is listed above. DP-SMER iterates over all values of $\mathcal{C}_2(\ell)$, *i.e.*, $\mathcal{C}_2(\ell) = 1, 2, \ldots, B$, and for each value of $\mathcal{C}_2(\ell)$, it minimizes $\sum \mathcal{C}_1(\ell)$. Upon return, the algorithm returns the cost of the optimal path from source s to destination d along with the structure Π that contains the network nodes that form the path.

Theorem 2: DP-SMER runs in time $O(N^2 \cdot B)$, where N is the number of nodes in the network. Upon completion, the algorithm returns an optimal solution to Problem SMER.

Proof: See [27]. ∎

C. Fully Polynomial Time ϵ-Approximation

As in the previous section, we scale the values of the $\mathcal{C}_2(\ell)$'s for any link ℓ in the network so that they are all integers and

denote by B an upper-bound on the sum of the $\mathcal{C}_2(\ell)$'s on any simple path.

The above pseudo-polynomial solution indicates that SMER is only weakly NP-hard (see [33]), which enables us to apply efficient, ϵ-optimal approximation schemes of polynomial time complexity, similar to the case of the widely investigated Restricted Shortest Path problem (RSP, see, *e.g.*, [34] and references therein). The RSP problem considers a network where each link has two metrics, say "cost" and "delay", and some "bound" on the end-to-end delay. Then, for a given source-destination pair, the problem is to find a path of minimum cost among those whose delay do not exceed the delay bound. This weakly NP-hard problem admits efficient ϵ-optimal approximation schemes of polynomial complexity, *e.g.*, [34].

We turn to specify our approximation scheme for SMER by a simple employment of any solution to the RSP problem. First, a technical difficulty arises in applying RSP approximation schemes to SMER. Recall that while link costs as given by (19) are non-negative, $\mathcal{C}_1(\ell)$ can be negative for some links ℓ. In RSP, specifically in the approximation scheme of [34], it is assumed that link costs are non-negative. Nevertheless, we show that the original network with possibly negative link weights can be safely transformed (*i.e.*, without affecting the identity of the solution) to an expanded network with non-negative link weights, by employing the following pre-processing step:

Algorithm 2 Expand_Network (source s, network $\mathcal{N}$).

1) Add the source node s to the expanded network.
2) For each node u ($u \neq s$) in the original network, add $N-1$ replicas denoted by $u(1), u(2), \ldots, u(N-1)$ to the expanded network.
3) For each link ℓ_{su} from node s to node u in the original network, add a link from node s to node $u(1)$ in the expanded network with the same metrics as for the original link.
4) For each link ℓ_{uv} in the original network, where $u \neq s$, $u \neq d$, $v \neq s$, and for each $h = 1, \ldots, N-2$, add a link between node $u(h)$ and node $v(h+1)$ in the expanded network with the same metrics as for the original link.
5) For each link ℓ in the expanded network, add some (identical to all links) bias $\delta \geq 0$ to each link cost $\mathcal{C}_1(\ell)$ so that the new link costs would be non-negative.

The following lemmas establish the relation between the shortest paths in the original network and the shortest paths in the expanded network.

Lemma 3: A path that is shortest w.r.t. the biased metric $(\mathcal{C}_1(\ell) + \delta)$ among those that obey a bound on the $\sum \mathcal{C}_2(\ell)$ and have precisely h hops, is also shortest w.r.t. the unbiased metric $\mathcal{C}_1(\ell)$ among those that obey the same bound on $\sum \mathcal{C}_2(\ell)$ and have precisely h hops.

Proof: See [27]. ∎

Lemma 4: A shortest path from source s to node $d(h)$ in the expanded network has precisely h hops.

Proof: See [27]. ∎

For a given approximation value $\epsilon > 0$, let $\eta = \epsilon/3$. Furthermore, let L be the smallest integer for which $\lceil (1+\eta)^L \rceil \geq B$. Our algorithm, called ϵ-SMER, is listed below. In this algorithm, ϵ-RSP refers to an ϵ-optimal approximation solution for RSP.

Algorithm 3 ϵ-SMER (error ϵ, source s, dest. d, net. $\mathcal{N}$).

$\mathcal{N}_x$ = Expand_Network(s, $\mathcal{N}$)
for all $\ell \in \mathcal{N}_x$ **do**
  $cost(\ell) = \mathcal{C}_1(\ell)$
  $delay(\ell) = \mathcal{C}_2(\ell)$
for $l = 1 \rightarrow L$ **do**
  $delay\_bound = \lceil (1+\eta)^l \rceil$
  /* compute the approximate h-hop path */
  for $h = 1 \rightarrow N-1$ **do**
    $[C(l,h), \Pi(l,h)] = \epsilon$-RSP$(\epsilon, s, d(h), \mathcal{N}_x)$
    /* compute the actual cost as per SMER metric */
    $\hat{C}(l,h) = (C(l,h) - h \cdot \delta) + \lceil (1+\eta)^l \rceil^2$
/* choose the best l and h for reaching the destination */
$(l^*, h^*) = \arg\min_{l,h} \hat{C}(l,h)$
return $[\hat{C}(l^*, h^*), \Pi(l^*, h^*)]$

In the ϵ-SMER algorithm, for each considered delay bound $\lceil (1+\eta)^l \rceil$, $N-1$ instances of the approximation solution to the RSP problem, for the same bound, are run on the expanded network: in each instance h, we consider s to be the source and $d(h)$ to be the destination. Using Lemma 4, it is straightforward to verify that, in each instance h, the RSP approximation obtains a solution that satisfies the required delay bound with the restriction that the path has *precisely* h hops (in both the expanded and the original network). Therefore, per considered bound on the $\mathcal{C}_2(\ell)$ metric and per possible number of hops up to $N-1$, we get an ϵ-optimal path with respect to the original metric $\mathcal{C}_1(\ell)$ (of precisely that many hops). It follows from Lemmas 3 and 4, that, by comparing all solutions (for all considered bounds on the $\mathcal{C}_2(\ell)$ metric and number of hops h), we will find a shortest ϵ-optimal path that corresponds to an ϵ-optimal solution to SMER. This is established next.

Lemma 5: Let Π^* be an optimal solution (path) to SMER. Denote by $\mathcal{C}(\Pi^*)$ and $\mathcal{C}(\hat{\Pi})$, the costs, per the SMER metric, of the optimal solution and of the solution obtained by ϵ-SMER, correspondingly. Then:

$$\mathcal{C}(\hat{\Pi}) \leq (1+\epsilon) \cdot \mathcal{C}(\Pi^*) \cdot \tag{23}$$

Proof: See [27]. ∎

Lemma 6: The computational complexity of ϵ-SMER is $O(A \cdot \frac{1}{\epsilon} \cdot \log(B) \cdot N^3)$, where $O(A)$ is the computational complexity of the employed approximation scheme for RSP.

Proof: See [27]. ∎

Theorem 3: ϵ-SMER is an ϵ-optimal approximation scheme of polynomial complexity. In particular, when employing the approximation solution of [34] to the RSP problem, ϵ-SMER runs in $O(N^6 \cdot (\log\log N + \frac{1}{\epsilon}) \cdot \frac{1}{\epsilon} \cdot \log(B))$ time.

Proof: The RSP scheme of [34] has computational complexity of $O\big(N \cdot M \cdot (\log\log N + 1/\epsilon)\big)$ for N nodes and M links. In worst-case, when the network forms a complete graph, we have $M = O(N^2)$. The proof then follows from Lemmas 5 and 6. ∎

More efficient versions of ϵ-SMER should be possible, yet our goal has been to show that fully polynomial time ϵ-approximation schemes (FPTAS) exist for the NP-hard problem SMER.

VI. Simulation Results

A. Simulation Environment

We have implemented our routing algorithms in a custom-built simulator. We simulate a wireless network, in which nodes are distributed uniformly at random in a 5×5 square area with node density $\sigma = 3$. We also place a number of eavesdroppers in the network with density σ_E, as described later. We consider one eavesdropper per link. Every node has a maximum transmission power that is set in such a way that the resulting network becomes connected (the absolute value of the maximum power does not affect the results). We choose two nodes s and d located at the lower left and the upper right corners of the network, respectively, and find paths from s to d. We then compute the total amount of energy consumed on each path using different routing algorithms. The performance metric "energy savings" refers to the percentage difference between total energy used by different algorithms with respect to the benchmark. For simulation purposes, we set $\pi = 0.1$, $\sigma_E = 1$, $N_0 = 1$, $\gamma_D = 0.8$, and $\gamma_E = 0.6$, unless otherwise specified. The numbers reported are obtained by averaging over 10 simulation runs with different seeds.

B. Simulated Algorithms

In addition to DP-SMER and ϵ-SMER, we have also implemented a security-agnostic algorithm based on minimum energy routing as a benchmark to measure energy savings achieved by our algorithms. The benchmark algorithm, called *security-agnostic shortest path routing (SASP)*, is described below. Note that some of the optimizations described in Sections III and IV have been incorporated in SASP, making it a considerably efficient benchmark (see Subsection VI-C).

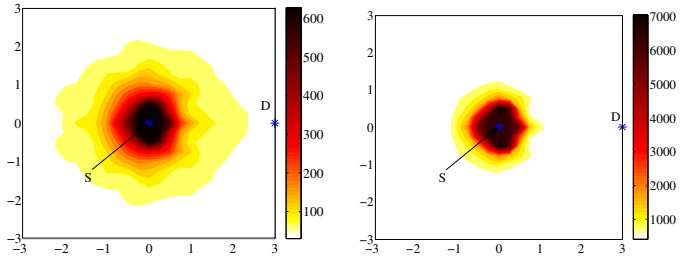
Algorithm 4 SASP (source s, dest. d, network $\mathcal{N}$).

1) Find a shortest path in terms of transmission power between s and d ignoring eavesdroppers. The standard Dijkstra's algorithm can be used for this purpose.
2) Use (17) to allocate an optimal eavesdropping probability to each link of the computed path.
3) Use (18) to allocate power to jammers on each link with respect to the allocated eavesdropping probabilities in step (2).

C. Results and Discussion

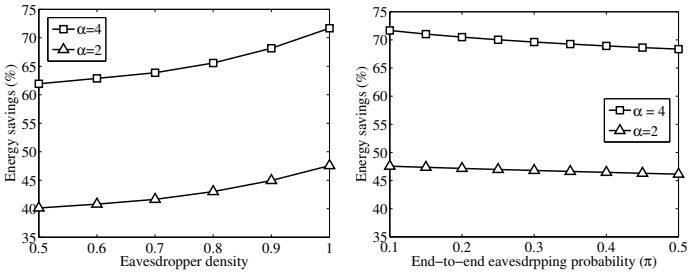
Effect of Eavesdropper Location on Link Cost. Fig. 1 shows the cost of establishing a secure link between source S (placed at the center) and destination D for different eavesdropper locations and $\pi = 0.001$. In the figure, the color intensity at each point is proportional to the amount of energy required to establish the link if the eavesdropper is placed at that point. Clearly, by some maneuvering around an eavesdropper, a significant reduction in energy cost can be achieved as the eavesdropper becomes almost ineffective in some locations.

Effect of Optimal Secrecy Allocation on Path Cost. Instead of optimal allocation of eavesdropping probability and jamming power (using (17) and (18)) to each link of a path, a simple heuristic is to divide π equally across the links. That is, if the path contains h links, then each link ℓ_k is allocated sufficient jamming power to satisfy the eavesdropping probability $\pi_k = \pi/h$. In Fig. 2, we have depicted energy savings that can be achieved "solely" by optimal secrecy allocation compared to equal allocation for a fixed path that is computed by SASP. Interestingly, as the number of eavesdroppers increases or the signal propagation becomes more restricted, optimal secrecy allocation becomes even more important, achieving energy savings of up to 72% (47%) for $\alpha = 4$ ($\alpha = 2$) in the simulated network.



(a) Path-loss exponent $\alpha = 2$. (b) Path-loss exponent $\alpha = 4$.

Fig. 1: Effect of eavesdropper location on link cost.



(a) Effect of eavesdropper density. (b) Effect of eavesdropping prob.

Fig. 2: Energy savings achieved by optimal secrecy allocation.

Non-uniform Eavesdropper Placement. To gain more insight about the behavior of different routing algorithms, in this experiment, rather than randomly distributing eavesdroppers in the network, we strategically place them close to the line that connects the source and destination. Ideally, SMER and ϵ-SMER should avoid the shortest path that crosses the network diagonally. This is indeed the behavior observed in the simulations as depicted in Fig. 3 (x and y axes show network coordinates, while '$\star$' and '$\cdot$' denote, respectively, eavesdroppers and regular network nodes). As expected, SASP blasts right through the eavesdroppers, while SMER, 0.1-SMER and 1.0-SMER route around them resulting in 88%, 86% and 85% energy savings, respectively.

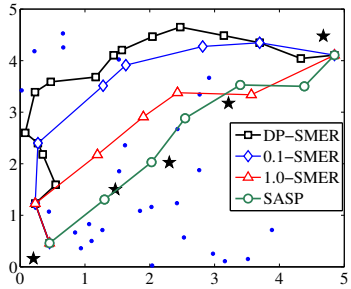
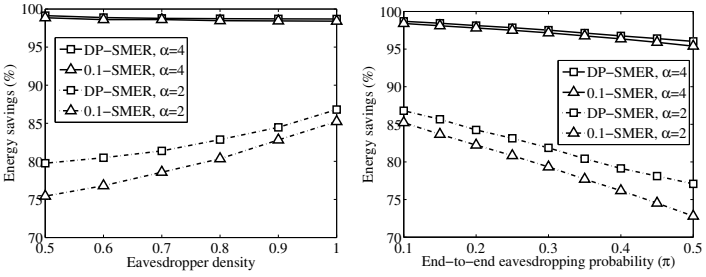


Fig. 3: Snapshot of paths computed by different algorithms.

Uniform Eavesdropper Placement. In this experiment, eavesdroppers are placed in the network uniformly at random. As

seen in Fig. 4, our algorithms consistently outperform SASP for a wide range of eavesdropper densities and eavesdropping probabilities. In particular, energy savings of up to 99% and 98% (for $\alpha = 4$) can be achieved by SMER and 0.1-SMER, respectively.



(a) Effect of eavesdropper density. (b) Effect of eavesdropping prob.

Fig. 4: Energy savings with uniform eavesdropper placement.

Effect of Network Size. Fig. 5 shows the energy savings achieved by different algorithms in networks with varying sizes. The "network dimension" refers to the length of one side of the square area that contains the network nodes. As observed from the figure, the energy saving is an increasing function of the network size. The reason is that, as the network size increases so does the average length of the path (in terms of the number of hops) between the source and destination nodes. The longer paths provide more opportunities for energy savings on each link of the path resulting in increased overall energy savings.

Effect of Jamming Set. The cardinality of the jamming set affects the power allocation to jammers. Fig. 6 show the energy savings achieved by varying the number of jammers that participate in secure transmissions on each link. Interestingly, our experiments show that a small number of jammers, namely 2, is sufficient to obtain most of the benefits of cooperative jamming, which should greatly simplify any practical implementation.

VII. Conclusion

This paper studied the problem of secure minimum energy routing in wireless networks. It was shown that while the problem is NP-hard, it admits exact pseudo-polynomial and fully polynomial time ϵ-approximation algorithmic solutions. Furthermore, using simulations, we showed that our algorithms significantly outperform security-agnostic algorithms based on minimum energy routing. Finally, we note that our work can be potentially extended to incorporate other secrecy models. Such extensions are left for future work.

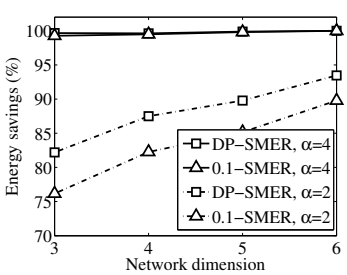


Fig. 5: Effect of network size.

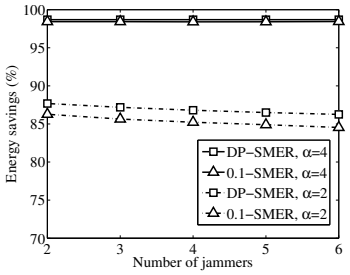


Fig. 6: Effect of jamming set.

References

[1] C. Shannon, *Communication theory of secrecy systems*. AT&T, 1949.

[2] A. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, 1975.

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, 1978.

[4] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, 1978.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, 1993.

[6] M. Bloch *et al.*, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, 2008.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, 2008.

[8] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, 2008.

[9] L. Dong *et al.*, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, 2010.

[10] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, 2008.

[11] D. Goeckel *et al.*, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, 2011.

[12] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels with imperfect ECSI," in *IEEE Globecom*, Dec. 2011.

[13] M. Haenggi, "The secrecy graph and some of its properties," in *IEEE ISIT*, Jun. 2008.

[14] P. Pinto, J. Barros, and M. Win, "Physical-layer security in stochastic wireless networks," in *IEEE ICCS*, Nov. 2008.

[15] P. Pinto, J. Barros, and M. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *IEEE ISIT*, Jun. 2009.

[16] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *IEEE ISIT*, Jun. 2009.

[17] O. Koyluoglu, E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," in *IEEE ITA*, Feb. 2010.

[18] S. Vasudevan *et al.*, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *ACM Mobihoc*, Sep. 2010.

[19] R. Mudumbai *et al.*, "Distributed transmit beamforming: Challenges and recent progress," *IEEE Commun. Mag.*, vol. 47, no. 2, 2009.

[20] M. Rahman *et al.*, "Fully wireless implementation of distributed beamforming on a software-defined radio platform," in *IEEE IPSN*, 2012.

[21] D. Lee *et al.*, "Coordinated multipoint transmission and reception in LTE-advanced: Deployment scenarios and operational challenges," *IEEE Commun. Mag.*, vol. 50, no. 2, 2012.

[22] F. Quitin *et al.*, "Distributed beamforming with software-defined radios: frequency synchronization and digital feedback," in *IEEE Glebecom*, Dec. 2012.

[23] F. Quitin *et al.*, "A scalable architecture for distributed transmit beamforming with commodity radios: design and proof of concept," *submitted to IEEE Trans. Wireless Commun.*, 2012.

[24] L. Abusalah *et al.*, "A survey of secure mobile ad hoc routing protocols," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 4, 2008.

[25] W. Lou *et al.*, "SPREAD: Improving network security by multipath routing in mobile ad hoc networks," *ACM Wireless Nets.*, 2009.

[26] T. Shu, M. Krunz, , and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Trans. Mobile Comput.*, vol. 9, no. 7, 2010.

[27] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Efficient wireless security through jamming, coding and routing," Tech. Rep. [Online]. Available: http://arxiv.org/abs/1304.2688

[28] A. Goldsmith, *Wireless communications*. Cambridge, 2005.

[29] D. Seymour and J. Britton, *Introduction to Tessellations*. Palo Alto, USA: Dale Seymour Publications, 1990.

[30] M. Dehghan *et al.*, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Trans. Wireless Commun.*, 2012.

[31] D. R. Brown *et al.*, "Receiver-coordinated distributed transmit nullforming with channel state uncertainty," in *CISS*, Mar. 2012.

[32] A. Shamir, "How to share a secret," *Commun. ACM*, 1979.

[33] M. R. Garey and D. S. Johnson, *Computers and interactability: A guide to the theory of NP-Completeness*. USA: W.H. Freeman and Company, 1979.

[34] D. H. Lorenz and D. Raz, "A simple efficient approximation scheme for the restricted shortest path problem," *Oper. Res. Lett.*, vol. 28, 1999.