Efficient Wireless Security
Through Jamming, Coding and Routing

Majid Ghaderi*, Dennis Goeckel†, Ariel Orda‡ and Mostafa Dehghan†

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.

Index Terms

Wireless security, minimum energy routing, cooperative jamming.

I. INTRODUCTION

Protecting the secrecy of user messages has become 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 many years (or decades). 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. Both have advantages and disadvantages for the desired everlasting security in the wireless environment.

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 [1]. Since the eavesdropper is assumed to get the transmitted signal without distortion, cryptography addresses the key challenge in the wireless environment of thwarting an eavesdropper very near the transmitter. However, such an approach faces the concern that the eavesdropper can store the signal, and, then, with later advances in computational capabilities or by breaking the encryption scheme, obtain the message. The desire for everlasting security then motivates adding countermeasures at the physical layer that inhibit even the recording of the encrypted message by the eavesdropper that combine with cryptography to facilitate a defense-in-depth approach [2].

In the information-theoretic approach to obtain perfect secrecy [3], the goal is to guarantee that the eavesdroppers can never extract information from the message, regardless of their computational capability. Wyner [4] and

*Department of Computer Science, University of Calgary, Email: `mghaderi@ucalgary.ca`
†Department of Electrical and Computer Engineering, UMass Amherst, Emails: {`goeckel, mdehghan`}`@ece.umass.edu`
‡Department of Electrical Engineering, Technion, Email: `ariel@ee.technion.ac.il`

succeeding authors [5], [6] 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 [4]. 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 [7], [8] and active channel manipulation [9], [10] 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) [8]–[13]. More recently, there has been the active consideration of large networks with the introduction of the secrecy graph to consider secure connectivity [14]–[16] and a number of approaches to throughput scaling versus security tradeoffs [17]–[19]. 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.

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 network nodes. To prevent the eavesdroppers from successfully capturing communications between legitimate nodes, mechanisms to thwart such are employed at the physical layer of the network. 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 received considerable attention [9]–[13], [20]. 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 study this technique include:

1) Opportunistic techniques [7], [8] that exploit the time-varying wireless channel may suffer from excessive delays depending on the rate of channel fluctuations. 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 [9], [21]. 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) Node cooperation, while requiring a more complex physical layer, is incorporated in commercial wireless technologies such as LTE. Thus, we envision that cooperative jamming can be implemented in practice, as was demonstrated in a limited form (single jammer) in [22].

4) Anonymous wireless communication is a challenging problem. Cooperative jamming can potentially be utilized for wireless anonymous communication, as it creates confusion for wireless localization techniques [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. The cost of a path can be defined in terms of various system parameters. In a wireless network, transmission power is a critical factor affecting the throughput and lifetime of the network. While increasing the transmission power results in increased link throughput, excessive power actually results in high levels of interference, hence reducing the network throughput due to inefficient

spacial reuse. 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.

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. Section VII presents an overview of some related work, while Section VIII concludes the paper.

II. SYSTEM MODEL AND ASSUMPTIONS

Consider a wireless network with arbitrarily distributed nodes. We assume that 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 to conceal its transmissions from $\mathcal{E}_k$ is denoted by $\mathcal{J}_k = \{J_1 \ldots, J_{|\mathcal{J}_k|}\}$, where $|\mathcal{A}|$ denotes the cardinality of set $\mathcal{A}$. The set of jammers is potentially different for different links. Throughout the paper, we use the notation $(S_k, D_k, \mathcal{E}_k, \mathcal{J}_k)$ to identify link ℓ_k.

In the following subsections, we describe the models considered in this paper for the wireless channel, eavesdroppers, physical-layer security and end-to-end routing. For notational simplicity, we may drop the link index k whenever there is no ambiguity.

---

[1]Terms "path" and "route" are used interchangeably throughout the paper.

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 $\mathbb{E}[|h_{S,D}|^2] = 1/d_{S,D}^{\alpha}$, 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 [24], [25].

B. Adversary Model

We limit our attention to passive eavesdroppers as in prior work [9]–[13], [20]. 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.*, [10]) or imperfect (*e.g.*, [20]) 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. In addition, our model requires only the knowledge of *potential* eavesdropping locations in the network, yet we show that it provides guaranteed security by employing coding in conjunction with cooperative jamming.

Specifically, we assume that each link ℓ_k is subject to potential eavesdropping from a set of locations denoted by $\mathcal{E}_k = \left\{E_1, \ldots, E_{|\mathcal{E}_k|}\right\}$, where the probability of eavesdropping from location E_i is given by $p(E_i)$ for $0 \le p(E_i) \le 1$. This is a considerably general model that can be used to represent a wide range of eavesdropping scenarios[2]. For example, setting all $p(E_i)$'s to 1 for a link models multiple eavesdroppers for that link. Other examples include, for example, 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. By dividing the effective eavesdropping region to a few smaller areas [26], one can compute the most effective eavesdropping location within each area, and consequently, construct the set of eavesdropping locations for that link.

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 [27]. Since the *implementation* of beamforming in other contexts, with the same challenges of synchronization in the wireless environment, is advancing rapidly [28], [29], 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 [30]. 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 $P_J = \| \mathbf{h}_D^{\perp} \|^2$. Assuming

---

[2]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 [9]–[13], [20], and references therein).

that the source node transmits with power P_S, 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, $\mathbf{h}_E = [h_{J_1,E}, h_{J_2,E}, \ldots, h_{J_{|\mathcal{J}|},E}]^{\mathrm{T}}$ represents 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

$$
\begin{aligned}
\mathbb{P}\left\{\mathrm{SINR}_E \geq \gamma_E\right\} &= \mathbb{P}\left\{ \frac{P_S |h_{S,E}|^2}{N_0 + \mathbf{h}_E^{\mathrm{T}} \mathbf{h}_D^{\perp} \mathbf{h}_D^{\perp\,\mathrm{T}} \mathbf{h}_E} \geq \gamma_E \right\} \\
&= \mathbb{E}_{\mathbf{h}_E}\left[\mathbb{P}\left\{ \frac{P_S |h_{S,E}|^2}{N_0 + \mathbf{h}_E \mathbf{h}_D^{\perp} \mathbf{h}_D^{\perp\,\mathrm{T}} \mathbf{h}_E^{\mathrm{T}}} \geq \gamma_E \,\Big|\, \mathbf{h}_E \right\} \right] \\
&= \mathbb{E}_{\mathbf{h}_E}\left[e^{-\frac{\gamma_E d_{S,E}^{\alpha}}{P_S} \mathbf{h}_E^{\mathrm{T}} \mathbf{h}_D^{\perp} \mathbf{h}_D^{\perp\,\mathrm{T}} \mathbf{h}_E} \right] e^{-\frac{\gamma_E N_0 d_{S,E}^{\alpha}}{P_S}},
\end{aligned}
\tag{3}
$$

where $\mathbb{E}_{\mathbf{h}_E}$ means expectation with respect to channel gain vector $\mathbf{h}_E$. Using the results on quadratic forms [31, Eq. 14] to calculate the expectation, it is obtained that ($\mathbf{I}_N$ is the identity matrix of size N)

$$
\begin{aligned}
\mathbb{P}\left\{\mathrm{SINR}_E \geq \gamma_E\right\} &\leq \frac{e^{-\frac{\gamma_E N_0 d_{S,E}^{\alpha}}{P_S}}}{\left| \mathbf{I}_N + \frac{\gamma_E d_{S,E}^{\alpha}}{P_S}\left(\sum_{J_i \in \mathcal{J}} \frac{1}{d_{J_i,E}^{\alpha}}\right) \mathbf{h}_D^{\perp} \mathbf{h}_D^{\perp\,\mathrm{T}} \right|} \\
&= \frac{e^{-N_0 \gamma_E \frac{d_{S,E}^{\alpha}}{P_S}}}{1 + \frac{\gamma_E d_{S,E}^{\alpha}}{P_S}\left(\sum_{J_i \in \mathcal{J}} \frac{1}{d_{J_i,E}^{\alpha}}\right) P_J}.
\end{aligned}
\tag{4}
$$

where the final expression is derived from Sylvester's determinant theorem:

$$
\det(\mathbf{I}_m + \mathbf{A}\mathbf{B}) = \det(\mathbf{I}_n + \mathbf{B}\mathbf{A}),
$$

for $\mathbf{A}$ and $\mathbf{B}$ being $m \times n$ and $n \times m$ matrices, respectively, and the fact that $P_J = \mathbf{h}_D^{\perp\,\mathrm{T}} \mathbf{h}_D^{\perp}$ (see (31)).

In the remainder of the paper, we use (4) 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 legitimate 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, where the cost of a route 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 on the path respectively.

Let $\lambda(\Pi)$ and $\lambda(\ell_k)$ denote, respectively, the goodput of path Π and link $\ell_k \in \Pi$. Then $\lambda(\Pi)$ can be expressed as

$$\lambda(\Pi) = \min_{\ell_k \in \Pi} \lambda(\ell_k) \cdot$$

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 $\ell_k \in \Pi$, *i.e.*, all links should just achieve the minimum goodput λ. 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:

$$\Pi^* = \arg \min_{\Pi \in \mathcal{L}} \sum_{\ell_k \in \Pi} \mathcal{C}(\ell_k)$$

$$s.t. \quad \mathbb{P}\{\text{eavesdropping on route } \Pi\} \leq \pi, \tag{5}$$

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. We use the following result to convert the above inequality constraint to an equality constraint in the routing problem (5).

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

Proof: Consider a path Π between the source and destination nodes. Define the end-to-end secrecy of path Π, denoted by $\omega(\Pi)$, as follows:

$$\omega(\Pi) = \prod_{\ell_k \in \Pi} \omega_k, \tag{6}$$

where $\omega_k = (1 - \pi_k)$.

First, we show that the link cost $\mathcal{C}(\ell_k)$ is a monotonically increasing function of the the link secrecy ω_k for every link $\ell_k \in \Pi$. Let $P_S^{(k)}$ and $P_J^{(k)}$ denote the source and jamming powers allocated to the link ℓ_k, respectively. In Section III, we show that: (i) $P_S^{(k)}$ is a constant for a given link independent of the link secrecy, and (ii) $P_J^{(k)}$ is a function of the link secrecy and is given by

$$P_J^{(k)} = c_k \cdot \frac{\omega_k}{1 - \omega_k}, \tag{7}$$

where c_k is some constant independent of ω_k. Thus, for a fixed link ℓ_k, the link cost $\mathcal{C}(\ell_k) = P_S^{(k)} + P_J^{(k)}$ depends on ω_k only through the jamming power $P_J^{(k)}$. Taking the derivative on the link cost with respect to ω_k results in the following relation:

$$\frac{d}{d\omega_k} \mathcal{C}(\ell_k) = c_k \cdot \frac{1}{(1 - \omega_k)^2} > 0, \tag{8}$$

indicating that the link cost is an increasing function of the link secrecy ω_k.

Let $\mathcal{C}^*(\Pi)$ and $\mathcal{C}(\Pi)$ denote the optimal cost of the path Π computed by solving the optimization problem (14), with equality and inequality constraints, respectively. Furthermore, let $\omega^*(\Pi)$ and $\omega(\Pi)$ denote the corresponding end-to-end path secrecies. We present a proof of the lemma based on contradiction by assuming that the optimal path cost with the inequality constraint is less than that with the equality constraint. That is, we assume that

$$\mathcal{C}(\Pi) \leq \mathcal{C}^*(\Pi), \tag{9}$$

while,

$$\omega(\Pi) > \omega^*(\Pi) \cdot \tag{10}$$

Next, by manipulating the link secrecy allocation vector $[\omega_1, \ldots, \omega_k, \ldots, \omega_K]$, we construct a new link secrecy allocation vector that satisfies the equality constraint, while having a cost smaller than $\mathcal{C}^*(\Pi)$. To this end, consider some arbitrary link ℓ_k, and replace ω_k by a new ω_k' as follows

$$\omega_k' = \frac{\omega^*}{\omega} \cdot \omega_k \cdot \tag{11}$$

Since $\omega^* < \omega$, it follows that $\omega_k' < \omega_k$. Consequently, the new cost of the link ℓ_k with link secrecy ω_k' is less than $\mathcal{C}(\ell_k)$, which in turn indicates that the new path cost with secrecy allocation vector $[\omega_1, \ldots, \omega_k', \ldots, \omega_K]$ is less than $\mathcal{C}(\Pi)$. Therefore, we have

$$\mathcal{C}'(\Pi) < \mathcal{C}(\Pi) < \mathcal{C}^*(\Pi), \tag{12}$$

and,

$$\omega(\Pi) > \omega'(\Pi) = \omega^*(\Pi) \cdot \tag{13}$$

The proof follows by noting that this contradicts the assumption that $\mathcal{C}^*(\Pi)$ is the minimum cost of path Π with the equality constraint. ∎

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

$$\Pi^* = \arg\min_{\Pi \in \mathcal{L}} \sum_{\ell_k \in \Pi} \mathcal{C}(\ell_k)$$
$$s.t. \quad \sum_{\ell_k \in \Pi} \pi_k = \pi \cdot \tag{14}$$

In the rest of the paper, we focus on this optimization problem. We first show that the problem is, in general, NP-hard and then develop exact and approximate algorithms to solve it.

III. SECURE LINK COST

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

$$\mathcal{C}(\ell_k) = P_S^{(k)} + P_J^{(k)}, \tag{15}$$

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 $P_J^{(k)}$ subject to a given 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 [25, 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 [24].

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:

$$P_S^{(k)}(|h_{S_k,D_k}|^2) = \begin{cases} \frac{\gamma_D}{|h_{S_k,D_k}|^2} \cdot d_{S_k,D_k}^\alpha, & |h_{S_k,D_k}|^2 \geq \tau \\ 0, & |h_{S_k,D_k}|^2 < \tau \end{cases} \tag{16}$$

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

$$
\begin{aligned}
P_S^{(k)} &= \frac{1}{1-\rho} \int_\tau^\infty \frac{\gamma_D}{x} \cdot d_{S_k,D_k}^\alpha e^{-x} dx \\
&= \gamma_D d_{S_k,D_k}^\alpha \frac{1}{1-\rho} \int_\tau^\infty \frac{e^{-x}}{x} dx \\
&= \gamma_D \, k_\rho \, d_{S_k,D_k}^\alpha,
\end{aligned}
\tag{17}
$$

where k_ρ is a constant that depends on the parameter ρ. Hence, for a fixed network parameter ρ (which also determines γ_D), the average power consumed on a given link ℓ_k to achieve the secure goodput λ is proportional to d_{S_k,D_k}^α.

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*[3] on each link.

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. Since each coded message is hidden from at least one eavesdropping location, it is guaranteed that an eavesdropper located at location E_i, for all $E_i \in \mathcal{E}_k$, will not be able to obtain any information about the original messages.

In the following subsections, we compute the optimal jamming power per link. The derivation for the case of multiple eavesdroppers relies on the jamming power computed for the single eavesdropper case.

1) Single Eavesdropper: Because slow frequency non-selective fading is assumed and the channel to the eavesdropper is unknown, there is some probability that the eavesdropper will obtain the message by achieving a received SINR greater than a threshold γ_E. 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). Because we want to avoid placing limitations on the capabilities of the eavesdropper, assume that the eavesdropper receiver is noiseless. Let $P_J^{(k)}$ and $P_J^{(k)}(|h_{S_k,D_k}|^2)$ denote the average and instantaneous transmission power allocated to jammers in $\mathcal{J}_k$, respectively. Then, using (4), it is obtained that

$$
\pi_k(|h_{S_k,D_k}|^2) = \frac{1}{1 + \frac{\gamma_E d_{S_k,E_k}^\alpha}{P_S^{(k)}(|h_{S_k,D_k}|^2)} \left(\sum_{J_i \in \mathcal{J}_k} \frac{1}{d_{J_i,E_k}^\alpha} \right) P_J^{(k)}(|h_{S_k,D_k}|^2)} .
$$

Now, 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, recognizing that both $P_S^{(k)}(|h_{S_k,D_k}|^2)$ and $P_J^{(k)}(|h_{S_k,D_k}|^2)$ are proportional to $|h_{S_k,D_k}|^2$, we have:

$$
P_J^{(k)}(|h_{S_k,D_k}|^2) = \frac{(1/\pi_k - 1) \, P_S^{(k)}(|h_{S_k,D_k}|^2)}{\gamma_E \, d_{S_k,E_k}^\alpha \left(\sum_{J_i \in \mathcal{J}_k} \frac{1}{d_{J_i,E_k}^\alpha} \right)},
\tag{18}
$$

and, taking expectations yields

$$
P_J^{(k)} = \frac{1/\pi_k - 1}{\gamma_E d_{S_k,E_k}^\alpha \left(\sum_{J_i \in \mathcal{J}_k} \frac{1}{d_{J_i,E_k}^\alpha} \right)} P_S^{(k)},
\tag{19}
$$

---

[3]Other forms of coding, such as dividing each message to smaller chunks [32], can be equally incorporated in our algorithm.

and,

$$\pi_k = \frac{1}{1 + \frac{\gamma_E d_{S_k, E_k}^{\alpha}}{P_S^{(k)}} \left(\sum_{J_i \in \mathcal{J}_k} \frac{1}{d_{J_i, E_k}^{\alpha}} \right) P_J^{(k)}} . \tag{20}$$

2) Multiple Eavesdroppers: Recall that our objective is to compute the minimum jamming power for the link. 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:

$$\min_{P_J^{(k)}(i)} \sum_{E_i \in \mathcal{E}_k} P_J^{(k)}(i)$$
$$s.t. \quad \sum_{E_i \in \mathcal{E}_k} p_k(E_i) \cdot \pi_k(i) = \pi_k, \tag{21}$$

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, *i.e.*, the jamming power during the transmission of the coded message m_i. Define $\phi_k(i)$ as follows

$$\phi_k(i) = \frac{\gamma_E}{\gamma_S k_\rho} \left(\frac{d_{S_k, E_i}}{d_{S_k, D_k}} \right)^{\alpha} \sum_{J_j \in \mathcal{J}_k} \frac{1}{d_{J_j, E_i}^{\alpha}} . \tag{22}$$

After substituting for $\pi_k(i)$ using (20), we obtain the following optimization problem:

$$\min_{P_J^{(k)}(i)} \sum_{E_i \in \mathcal{E}_k} P_J^{(k)}(i)$$
$$s.t. \quad \sum_{E_i \in \mathcal{E}_k} \frac{p_k(E_i)}{1 + \phi_k(i) P_J^{(k)}(i)} = \pi_k . \tag{23}$$

The optimization variables in this optimization problem are the jamming powers $P_J^{(k)}(i)$. The Lagrangian for the link cost optimization problem is expressed as follows

$$L(P_J^{(k)}(1), \ldots, P_J^{(k)}(|\mathcal{E}_k|), \nu)$$
$$= \sum_{E_i \in \mathcal{E}_k} P_J^{(k)}(i) + \nu \left(\sum_{E_i \in \mathcal{E}_k} \frac{p_k(E_i)}{1 + \phi_k(i) P_J^{(k)}(i)} - \pi \right) .$$

Using the Lagrange multipliers technique, it is obtained that

$$\frac{\partial L}{\partial P_J^{(k)}(i)} = 1 - \nu \frac{\phi_k(i) p_k(E_i)}{(1 + \phi_k(i) P_J^{(k)}(i))^2}, \tag{24}$$

and,

$$\frac{\partial L}{\partial \nu} = \sum_{E_i \in \mathcal{E}_k} \frac{p_k(E_i)}{1 + \phi_k(i) P_J^{(k)}(i)} - \pi . \tag{25}$$

Using (24), we have

$$\frac{p_k(E_i)}{1 + \phi_k(i) P_J^{(k)}(i)} = \frac{\sqrt{p_k(E_i)}}{\sqrt{\nu \phi_k(i)}} . \tag{26}$$

By substituting in (25), it follows that

$$\sum_{E_i \in \mathcal{E}_k} \sqrt{\frac{p_k(i)}{\nu \phi_k(i)}} = \pi, \tag{27}$$

and, therefore,

$$\frac{1}{\sqrt{\nu}} = \frac{\pi}{\sum_{E_i \in \mathcal{E}_k} \sqrt{\frac{p_k(i)}{\phi_k(i)}}} \cdot \tag{28}$$

It is then obtained that

$$\pi_k(i) = \frac{1}{\phi_k(i)} \frac{1/\sqrt{\frac{p_k(E_i)}{\phi_k(i)}}}{\sum_{E_i \in \mathcal{E}_k} \sqrt{\frac{p_k(E_i)}{\phi_k(i)}}} \pi_k, \tag{29}$$

and,

$$P_J^{(k)}(i) = \frac{1}{\pi_k} \sqrt{\frac{p_k(E_i)}{\phi_k(i)}} \sum_{E_i \in \mathcal{E}_k} \sqrt{\frac{p_k(E_i)}{\phi_k(i)}} - \frac{1}{\phi_k(i)} \cdot \tag{30}$$

For a given link ℓ_k and eavesdropping probability π_k, we can use (30) to compute the optimal jamming power allocation for each coded message m_i. Consequently, the average jamming power per message on link ℓ_k is given by:

$$\begin{aligned} P_J^{(k)} &= \frac{1}{|\mathcal{E}_k|} \sum_{E_i \in \mathcal{E}_k} P_J^{(k)}(i) \\ &= \frac{1}{\pi_k} \frac{1}{|\mathcal{E}_k|} \left(\sum_{E_i \in \mathcal{E}_k} \sqrt{\frac{p_k(E_i)}{\phi_k(i)}} \right)^2 - \frac{1}{|\mathcal{E}_k|} \sum_{E_i \in \mathcal{E}_k} \frac{1}{\phi_k(i)} \cdot \end{aligned} \tag{31}$$

C. Discussion

1) Colluding Eavesdroppers: While we considered the case of non-colluding eavesdroppers here, our model can be extended to handle colluding eavesdroppers by requiring that at least of the coded messages be protected against all eavesdroppers. Let $\mathcal{E}_k = \{E_1, \ldots, E_{|\mathcal{E}_k|}\}$ denote the set of colluding eavesdroppers. Assume that on link ℓ_k, B_k messages are coded together for transmission, *i.e.*, B_k is the length of the coding block. Then, the probability that a coded message m is captured by all eavesdroppers is given by $\prod_{E_i \in \mathcal{E}_k} \pi_k(i)$. Thus, the probability that at least one message out of the B_k coded messages is not received by all eavesdroppers is given by

$$1 - \left(\prod_{E_i \in \mathcal{E}_k} \pi_k(i) \right)^{B_k} \cdot \tag{32}$$

To satisfy the link eavesdropping constraint π_k, the following relation should be satisfied

$$1 - \left(\prod_{E_i \in \mathcal{E}_k} \pi_k(i) \right)^{B_k} = \pi_k, \tag{33}$$

which yields

$$\prod_{E_i \in \mathcal{E}_k} \pi_k(i) = \sqrt[B_k]{\overline{\pi_k}} \cdot \tag{34}$$

This constraint can be used in the optimization problem (23) to compute the optimal link cost for the case of colluding eavesdroppers.

An interesting observation is that

$$\lim_{B_k \to \infty} \pi_k(i) = 1, \quad \text{for all } E_i \in \mathcal{E}_k \cdot \tag{35}$$

That is, by increasing the length of the coding block, the link cost can be significantly reduced. The cost to be paid is in terms of increased transmission delay.

2) End-to-End Coding: Rather than looking at individual links in isolation and then performing hop-by-hop coding, we can perform coding on an end-to-end basis only at the source node. Then by repeatedly finding paths that are secure against single eavesdropping per link, the source can securely communicate with the destination through multiple paths. This approach is appropriate if there are only a few potential eavesdropping locations in the network. If the maximum number of eavesdropping locations per link is m, then the running time of this approach is m times that of the routing algorithm with single eavesdropping location per link.

IV. SECURE PATH COST

In this section, using the link cost formulation of the previous section, we formulate the optimal cost of a *given* path Π subject to an end-to-end eavesdropping probability π. The problem essentially is to divide π across the links forming Π so that the path cost is minimized.

A. Optimal Path Cost

Consider a given path Π. We find the optimal cost of path Π by solving the optimization problem (14). 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:

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

and,

$$y_k = \frac{1}{|\mathcal{E}_k|} \sum_{E_i \in \mathcal{E}_k} \frac{1}{\phi_k(i)}.$$

Using the results obtained in the previous subsection, the following relation holds:

$$\pi_k = \frac{x_k^2}{y_k + P_J^{(k)}}.$$

By substituting the above expressions in the optimal routing formulation described in (14), the following optimization problem is obtained for minimizing the cost $\mathcal{C}(\Pi)$ of route Π:

$$\min_{P_J^{(k)}} \sum_{\ell_k \in \Pi} P_S^{(k)} + P_J^{(k)}$$
$$s.t. \quad \sum_{\ell_k \in \Pi} \left(\frac{x_k^2}{y_k + P_J^{(k)}} \right) = \pi. \tag{36}$$

The optimization variables in this optimization problem are jamming powers $P_J^{(k)}$. The Lagrangian for the routing optimization problem is expressed as follows

$$L(P_J^{(1)}, \ldots, P_J^{(K)}, \nu)$$
$$= \sum_{\ell_k \in \Pi} \left(P_S^{(k)} + P_J^{(k)} \right) + \nu \left(\sum_{\ell_k \in \Pi} \left(\frac{x_k^2}{y_k + P_J^{(k)}} \right) - \pi \right).$$

Using the Lagrange multipliers technique, it is obtained that

$$\frac{\partial L}{\partial P_J^{(k)}} = 1 - \nu \frac{x_k^2}{(y_k + P_J^{(k)})^2}, \tag{37}$$

and,

$$\frac{\partial L}{\partial \nu} = \sum_{\ell_k \in \Pi} \left(\frac{x_k^2}{y_k + P_J^{(k)}} \right) - \pi. \tag{38}$$

Using (37), we have

$$\frac{x_k^2}{y_k + P_J^{(k)}} = \frac{x_k}{\sqrt{\nu}}. \tag{39}$$

By substituting in (38), it follows that

$$\sum_{\ell_k \in \ell} \frac{x_k}{\sqrt{\nu}} = \pi, \tag{40}$$

and, therefore,

$$\frac{1}{\sqrt{\nu}} = \frac{\pi}{\sum_{\ell_k \in \Pi} x_k}. \tag{41}$$

After substitution in (39), the following relation for the optimal eavesdropping probability π_k on link ℓ_k is obtained

$$\pi_k = \frac{x_k}{\sum_{\ell_i \in \Pi} x_i} \, \pi \cdot \tag{42}$$

For a given route Π and end-to-end eavesdropping probability π, we can use (42) 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:

$$P_J^{(k)} = \frac{1}{\pi} \cdot x_k \sum_{\ell_i \in \Pi} x_i - y_k \cdot \tag{43}$$

Using the above expression for $P_J^{(k)}$, the cost of link $\ell_k \in \Pi$ is expressed as

$$\mathcal{C}(\ell_k) = \big((\gamma_S k_\rho) \cdot d_{S_k,D_k}^{\alpha} - y_k \big) + \frac{1}{\pi} \big(x_k \sum_{\ell_i \in \Pi} x_i \big) \cdot \tag{44}$$

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

$$\mathcal{C}(\Pi) = \sum_{\ell_k \in \Pi} \big((\gamma_S k_\rho) \cdot d_{S_k,D_k}^{\alpha} - y_k \big) + \frac{1}{\pi} \big(\sum_{\ell_k \in \Pi} x_k \big)^2 \cdot \tag{45}$$

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 (45). The optimal cost is achieved by allocating $P_S^{(k)}$ and $P_J^{(k)}$ to each link $\ell_k \in \Pi$ using (17) and (43), respectively. Such a power allocation scheme would result in minimum cost, while guaranteeing that the eavesdropping constraint would be satisfied. Thus, SMER is reduced to finding a path, among all possible paths between the source and destination, that minimizes the optimal path cost (45). 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 (45).

B. Optimal Path Cost Structure

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

$$\begin{aligned} \mathcal{C}_1(\ell_k) &= (\gamma_S k_\rho) \cdot d_{S_k,D_k}^{\alpha} - y_k, \\ \mathcal{C}_2(\ell_k) &= \frac{1}{\sqrt{\pi}} \cdot \sum_{\ell_k \in \Pi} x_k \cdot \end{aligned} \tag{46}$$

Then the optimal path cost (45) can be expressed as

$$\mathcal{C}(\Pi) = \sum_{\ell_k \in \Pi} \mathcal{C}_1(\ell_k) + \big(\sum_{\ell_k \in \Pi} \mathcal{C}_2(\ell_k) \big)^2 \cdot \tag{47}$$

It is important to note that, while the $\mathcal{C}_1(\ell_k)$'s may assume negative values, the path cost structure in (47) 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, (47) is minimized by a *simple* path.

V. Secure Minimum Energy Routing

In this section, we investigate the secure minimum energy routing problem, where the cost of a path is given by (45). We begin by establishing that it 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 via a reduction from the partition problem.

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 $S = \{k_1, k_2, \ldots, k_n\}$, with $\sum_{i=1}^{n} k_i = 2 \cdot K$, the Partition problem is to decide whether there is a subset S' of S such that $\sum_{i \in S'} k_i = K$.

Given an instance $S = \{k_1, k_2, \ldots, k_n\}$ 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 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 $C_1(\ell_i^{(u)}) = 2 \cdot K \cdot k_i$ and $C_2(\ell_i^{(u)}) = 0$, and a "lower" link $\ell_i^{(w)}$, to which we assign $C_1(\ell_i^{(w)}) = 0$ and $C_2(\ell_i^{(w)}) = k_i$.

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 (47) of a path between nodes k_1 and k_n, equals $3 \cdot K^2$.

Proof: A path Π between nodes k_1 and k_n consists of a (possibly empty) set of "upper" links $\mathcal{U}$ and a (possibly empty) set of "lower" links $\mathcal{W}$. Let S_u and S_w be, correspondingly, the sets of indices of the links in $\mathcal{U}$ and in $\mathcal{W}$, *i.e.*, $i \in S_u$ iff $\ell_i^{(u)} \in \mathcal{U}$ and $i \in S_w$ iff $\ell_i^{(w)} \in \mathcal{W}$. Clearly, $S_u \cup S_w = S$. The cost of the path, per (47), is given by:

$$
\begin{aligned}
C(\Pi) &= \sum_{\ell_i^{(u)} \in \mathcal{U}} C_1(\ell_i^{(u)}) + \sum_{\ell_i^{(w)} \in \mathcal{W}} C_1(\ell_i^{(w)}) \\
&\quad + \Big(\sum_{\ell_i^{(u)} \in \mathcal{U}} C_2(\ell_i^{(u)}) + \sum_{\ell_i^{(w)} \in \mathcal{W}} C_2(\ell_i^{(w)}) \Big)^2, \\
&= \sum_{i \in S_u} (2 \cdot K \cdot k_i) + \sum_{i \in S_w} 0 + \Big(\sum_{i \in S_u} 0 + \sum_{i \in S_w} k_i \Big)^2 \cdot
\end{aligned}
\tag{48}
$$

Consider first the case $\sum_{i \in S_u} k_i \geq \sum_{i \in S_w} k_i$. Since $\sum_{i \in S_u} k_i + \sum_{i \in S_w} k_i = 2 \cdot K$, denote: $\sum_{i \in S_u} k_i = K + \delta$, $\sum_{i \in S_w} k_i = K - \delta$, for some $\delta \geq 0$. Then, from (48), we have:

$$
C(\Pi) = 2 \cdot K \cdot (K + \delta) + \Big(K - \delta \Big)^2 = 3 \cdot K^2 + \delta^2 \cdot
$$

Consider now the case $\sum_{i \in S_u} k_i < \sum_{i \in S_w} k_i$. It follows similarly that

$$
C(\Pi) = 3 \cdot K^2 + \delta^2 \cdot
$$

We conclude that the length of a path between nodes k_1 and k_n is at least $3 \cdot K^2$, and, furthermore, that value is attained *iff* the set S can be partitioned into two subsets S_u and S_w, such that $\sum_{i \in S_u} k_i = \sum_{i \in S_w} k_i$, *i.e.*, *iff* there is a subset $S' = S_u$ of S such that $\sum_{i \in S'} k_i = K$, and the lemma follows. ∎

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

B. Pseudo-Polynomial Time Exact Algorithm

First, scale the values of the $C_2(\ell)$'s for any link ℓ in the network so that they are all integers.[4] Let B denote an upper-bound on the sum of the $C_2(\ell)$'s on any simple path. A trivial bound is given by $B = (N - 1) \cdot C_2^{max}$, where N is the number of nodes in the network and C_2^{max} is the maximum value of $C_2(\ell)$ among all network links. In a network with N nodes, C_2^{max} can be computed in $O(N^2)$ time via a brute-force search.

Our algorithm, termed DP-SMER, is listed below. DP-SMER iterates over all values of $C_2(\ell)$, *i.e.*, $C_2(\ell) = 1, 2, \ldots, B$, and for each value of $C_2(\ell)$, it minimizes $\sum C_1(\ell)$. 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: The first claim follows by noting that the computational complexity is dominated by an iteration on all values $1, 2, \ldots, B$, and for each such iteration, iterating on all pairs of nodes.

---

[4]The value of "1" is determined by the precision at which we compute $C_2(\ell)$'s.

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

/* path cost from s to itself is always 0 */
for $b = 1 \rightarrow B$ **do**
$\quad C_s(b) = 0$
/* initial path cost from s to any other node is infinite */
for all $n_i \in \mathcal{N}$, $n_i \neq s$ **do**
$\quad$**for** $b = 1 \rightarrow B$ **do**
$\quad\quad C_i(b) = \infty$
for $b = 1 \rightarrow B$ **do**
$\quad$/* all node pairs can form a link and be neighbors */
$\quad$**for all** $n_i \in \mathcal{N}$ **do**
$\quad\quad$**for all** $n_j \in \mathcal{N}$ **do**
$\quad\quad\quad$/* update path cost via the neighboring nodes */
$\quad\quad\quad$**if** $b + \mathcal{C}_2(\ell_{ij}) \leq B$ **then**
$\quad\quad\quad\quad t = C_i(b) + \mathcal{C}_1(\ell_{ij})$
$\quad\quad\quad\quad$**if** $t < C_j(b + \mathcal{C}_2(\ell_{ij}))$ **then**
$\quad\quad\quad\quad\quad \Pi_j(b + \mathcal{C}_2(\ell_{ij})) = i$ /* set n_j's parent to n_i */
$\quad\quad\quad\quad\quad C_j(b + \mathcal{C}_2(\ell_{ij})) = t$ /* update path cost */
/* include the "b" component, *i.e.*, $\mathcal{C}_2$, in the path costs */
for $b = 1 \rightarrow B$ **do**
$\quad \hat{C}_d(b) = C_d(b) + b^2$
/* choose the best value for reaching the destination */
$b^* = \arg\min_b \hat{C}_d(b)$
return $[\hat{C}_d(b^*), \Pi(b^*)]$

We turn to consider the second claim. First, it can be established, by induction on the values of b, that, upon completion of the b-th iteration of the main loop of the algorithm, for all nodes n_i, $C_i(b)$ is the length of a shortest path with respect to the metric of the $\mathcal{C}_1(\ell_{ij})$ values, among all paths between the source s and node n_i, whose length with respect to the metric of the $\mathcal{C}_2(\ell_{ij})$ values is precisely b.[5] Furthermore, it is easy to verify that the values of $\hat{C}_N(b)$, computed at the next step of the algorithm, stand for the lengths of the above shortest paths with respect to the metric considered by Problem SMER.

Now, let Π^* be an optimal solution (*i.e.*, a path) to Problem SMER, and denote by C^* its length with respect to the metric considered by SMER. Furthermore, denote $b^* = \sum_{\ell_{ij} \in \Pi^*} \mathcal{C}_2(\ell_{ij})$. It is easy to verify that Π^* is a shortest path with respect to the metric of the $\mathcal{C}_1(\ell_{ij})$ values, among all paths between the source s and the destination d, whose length with respect to the metric of the $\mathcal{C}_2(\ell_{ij})$ values is precisely b^*. Therefore, upon completion of the above steps of the algorithm, we will have $\hat{C}_N(b^*) = C^*$; moreover, since Π^* is an optimal solution to SMER, it must hold that $\hat{C}_N(b^*) \leq \hat{C}_N(b)$ for all values of b. The theorem follows. ∎

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

---

[5]We note that this shortest path may be non-simple, *i.e.*, include loops, due to the potentially negative values of $\mathcal{C}_1(\ell_{ij})$'s; nonetheless, it is a finite path, and, furthermore, the optimal path returned by the last step of DP-SMER is guaranteed to be simple, due to the monotonicity property explained at the end of Section IV.

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 Problem SMER by a simple employment of any solution to the RSP problem.[6] First, a technical difficulty arises in applying RSP approximation schemes to Problem SMER. Recall that while link costs as given by (44) 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: Suppose that this is not true. That is, there are paths Π and Π', both obeying the bound on $\sum \mathcal{C}_2(\ell)$ and with h hops, in such a way that Π' is a shortest path with the bias yet Π is shorter without the bias. Therefore, $\sum_{\ell \in \Pi} \mathcal{C}_1(\ell) < \sum_{\ell \in \Pi'} \mathcal{C}_1(\ell)$, yet $\sum_{\ell \in \Pi}(\mathcal{C}_1(\ell)+\delta) \geq \sum_{\ell \in \Pi'}(\mathcal{C}_1(\ell)+\delta)$. However, the second inequality can be rewritten as: $\sum_{\ell \in \Pi} \mathcal{C}_1(\ell) + h \cdot \delta \geq \sum_{\ell \in \Pi'} \mathcal{C}_1(\ell) + h \cdot \delta$, which contradicts the first inequality. ∎

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

Proof: The proof follows from the fact that the i-th hop on the shortest path from s to $d(h)$ has to go from some node $v(i-1)$ to some node $u(i)$ (see the network expansion procedure). ∎

Thus, to compute an ϵ-optimal solution to Problem SMER, for every bound on $\sum \mathcal{C}_2(\ell)$, we find the shortest path with $h = 1, \ldots, N-1$ hops in the expanded network by repeatedly employing an approximation solution to the RSP problem. 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 the RSP problem.

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 through the following lemmas and theorem.

---

[6] Other solutions, of reduced computational complexity, can be established, yet their structure is somewhat more complex.

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

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

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:

$$\mathcal{C}(\hat{\Pi}) \leq (1+\epsilon) \cdot \mathcal{C}(\Pi^*) \cdot \tag{49}$$

Proof: Let $\bar{l}$ be the smallest integer such that

$$\Big(\sum_{\ell \in \Pi^*} \mathcal{C}_2(\ell) \Big)^2 \leq \Big(\lceil (1+\eta)^{\bar{l}} \rceil \Big)^2 \cdot \tag{50}$$

Note that this implies that:

$$(1+\eta)^2 \Big(\sum_{\ell \in \Pi^*} \mathcal{C}_2(\ell) \Big)^2 \geq \Big(\lceil (1+\eta)^{\bar{l}} \rceil \Big)^2 \cdot \tag{51}$$

Let $\bar{h}$ be the number of hops of Π^*. By construction, $\Pi(\bar{l}, \bar{h})$ is an ϵ-optimal approximation for RSP, for "costs" $\mathcal{C}_1(\ell)$, "delays" $\mathcal{C}_2(\ell)$, "delay bound" $\lceil (1+\eta)^{\bar{l}} \rceil$ and precisely $\bar{h}$ hops. Moreover, by (50), the path Π^* obeys this bound. Therefore:

$$\sum_{\ell \in \Pi(\bar{l}, \bar{h})} \mathcal{C}_1(\ell) + \bar{h} \cdot \delta \leq (1+\epsilon) \sum_{\ell \in \Pi^*} \mathcal{C}_1(\ell) + \bar{h} \cdot \delta, \tag{52}$$

or, equivalently,

$$\sum_{\ell \in \Pi(\bar{l}, \bar{h})} \mathcal{C}_1(\ell) \leq (1+\epsilon) \sum_{\ell \in \Pi^*} \mathcal{C}_1(\ell) \cdot \tag{53}$$

Since $\Pi(\bar{l}, \bar{h})$ obeys the "delay bound" $\lceil (1+\eta)^{\bar{l}} \rceil$, we have:

$$\Big(\sum_{\ell \in \Pi(\bar{l}, \bar{h})} \mathcal{C}_2(\ell) \Big)^2 \leq \Big(\lceil (1+\eta)^{\bar{l}} \rceil \Big)^2 \cdot \tag{54}$$

Combining (51), (53) and (54), we have:

$$\begin{aligned} \mathcal{C}(\hat{\Pi}) &\leq \mathcal{C}(\Pi(\bar{l}, \bar{h})) \\ &\leq (1+\epsilon) \sum_{\ell \in \Pi^*} \mathcal{C}_1(\ell) + (1+\eta)^2 \Big(\sum_{\ell \in \Pi^*} \mathcal{C}_2(\ell) \Big)^2, \end{aligned} \tag{55}$$

where the first transition is due to the way that $\hat{\Pi}$ is chosen. Since $\eta = \frac{\epsilon}{3}$, for small values of ϵ (precisely, $\epsilon < 3$), (55) implies:

$$\mathcal{C}(\hat{\Pi}) \leq (1+\epsilon) \cdot \mathcal{C}(\Pi^*), \tag{56}$$

as required. ∎

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: Let M be the number of links in the original network. Each time we employ the RSP approximation scheme, we would incur a computational complexity of $O(A)$, where A corresponds to a network with N nodes and M links.

For each value of $l = 1 \ldots, L$, we call the RSP approximation as follows: once for a network with N nodes and $O(N)$ links (*i.e.*, for the network that contains s and all the $u(1)$'s), once for a network with roughly $2N$ nodes and M links (*i.e.*, for the network that contains, in addition to the above, all the $u(2)$'s and links of the form $(u(1), v(2))$, once for a network with roughly $3N$ nodes and $2M$ links (*i.e.*, for the network that contains, in addition to the above, all the $u(3)$'s and links of the form $(u(2), v(3))$, and so on up to, once (the $(N-1)$-th time) for a network with roughly $(N-1)N$ nodes and $(N-2)M$ links. The above $N-1$ instances (more precisely, all but the first, which can be neglected due to smaller complexity) aggregate to:

$$
\begin{aligned}
O\big(A \cdot (2 \cdot 1 + 3 \cdot 2 + \cdots + N \cdot (N-1))\big) \\
= O\big(A \cdot \sum_{i=1}^{N-1} i(i+1)\big) = O\big(A \cdot N^3\big) \cdot
\end{aligned}
\tag{57}
$$

The proof follows by noting that $L = O(\frac{1}{\epsilon} \cdot \log(B))$. ∎

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. Depending on the limit on the transmission power at each node, in worst-case we have $M = O(N^2)$, *i.e.*, all nodes may be neighbors[7]. 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.

D. Distributed Implementation

While it is not discussed in this paper, our routing algorithms can be implemented in a distributed manner following standard techniques of distance-vector routing. Note that the power allocation at the physical layer is a local operation performed by the transmitting node of each link based on the information from the routing algorithm and topological information (collected, for instance, through neighbor discovery before running the routing algorithm).

VI. SIMULATION RESULTS

A. Simulation Environment

We have implemented our routing algorithms in a custom-built simulator to study their performance in a variety of network scenarios. We simulate a wireless network, in which nodes are distributed uniformly at random in a square of area 5×5 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. We keep the number of eavesdroppers considerably less than that of the legitimate nodes in order to be able to establish secure routes as we put a limit on the maximum transmission power of each node. 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.

---

[7]Note that, typically, the network is sparse, *i.e.*, $M \ll N^2$, hence the dependency on N is more like N^5.

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 (42) to allocate an optimal eavesdropping probability to each link of the computed path.
3) Use (43) to allocate sufficient 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. For a fixed link between two nodes, the source transmission power is also fixed as obtained in (17). Thus, the cost of the link depends only on the jamming power which is a function of the eavesdropper location as given by (31). 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. This is the main idea behind this work.
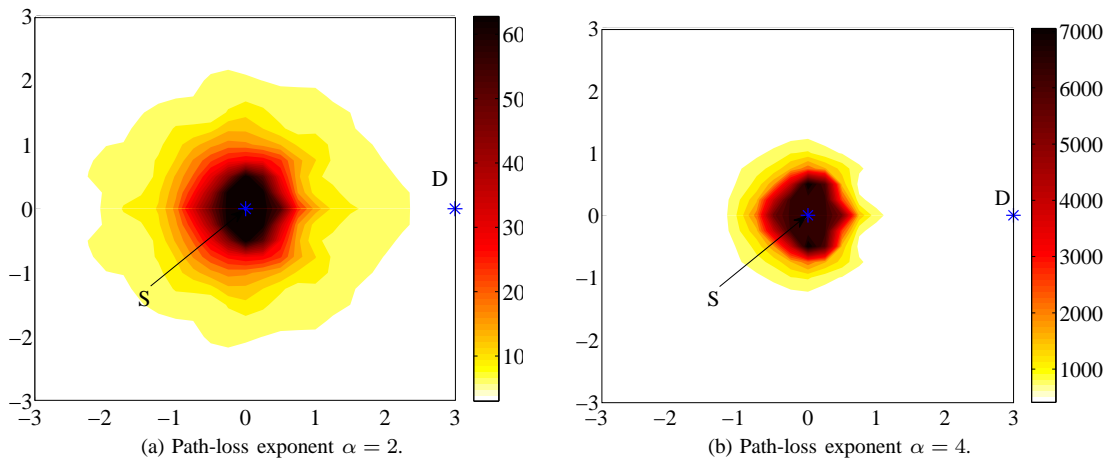

Fig. 1: Effect of eavesdropper location on link cost.

Effect of Optimal Secrecy Allocation on Path Cost. For a fixed path subject to an end-to-end secrecy requirement π, the optimal eavesdropping probability assigned to each link of the path is given by (42), which in turn determines the optimal jamming power allocated to each link of the path using (43). Specifically, this is how power allocation is performed in SASP in order to minimize power consumption. Alternatively, 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.

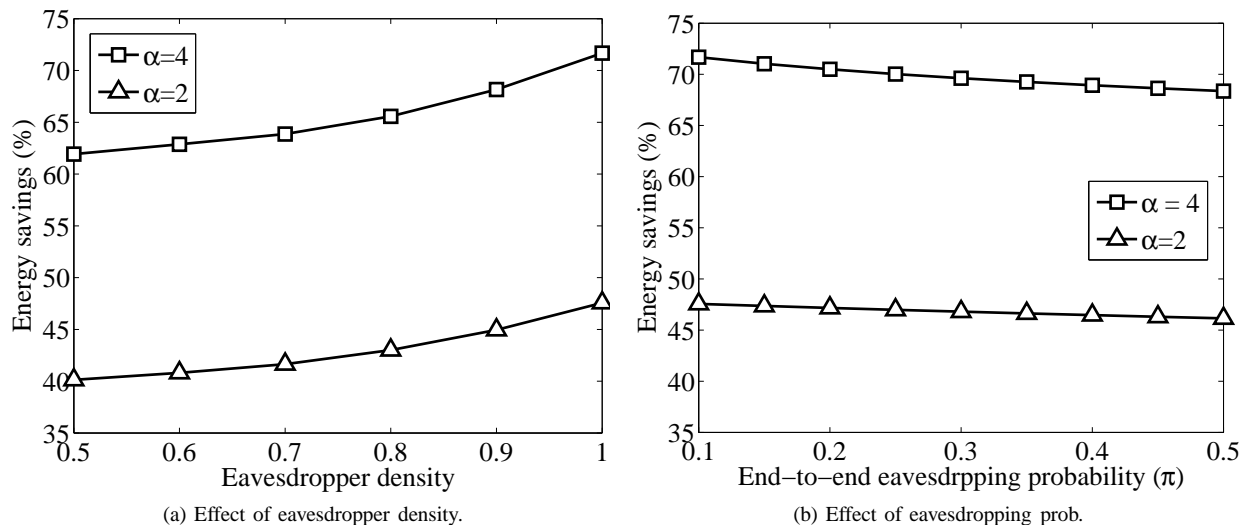(a) Effect of eavesdropper density.   (b) Effect of eavesdropping prob.

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 ('★' denotes an eavesdropper). 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.
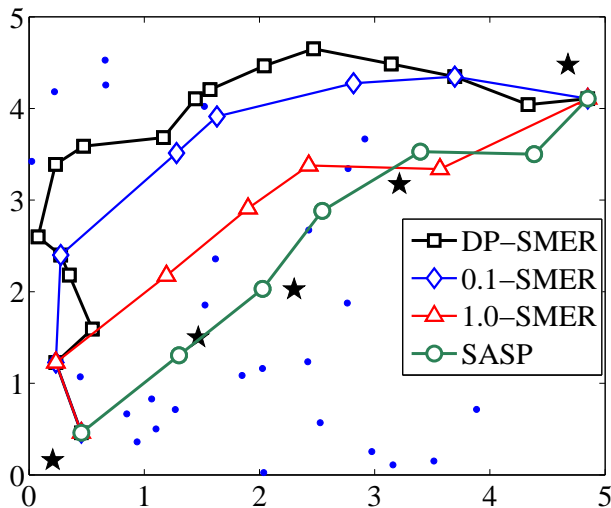

Fig. 3: Snapshot of paths computed by different algorithms.

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.

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. Interestingly, as the network size increases, the effect of the propagation environment diminishes in such a way that energy savings for $\alpha = 2$ and $\alpha = 4$ converge to the same numbers as opposed to the previous scenarios. 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.

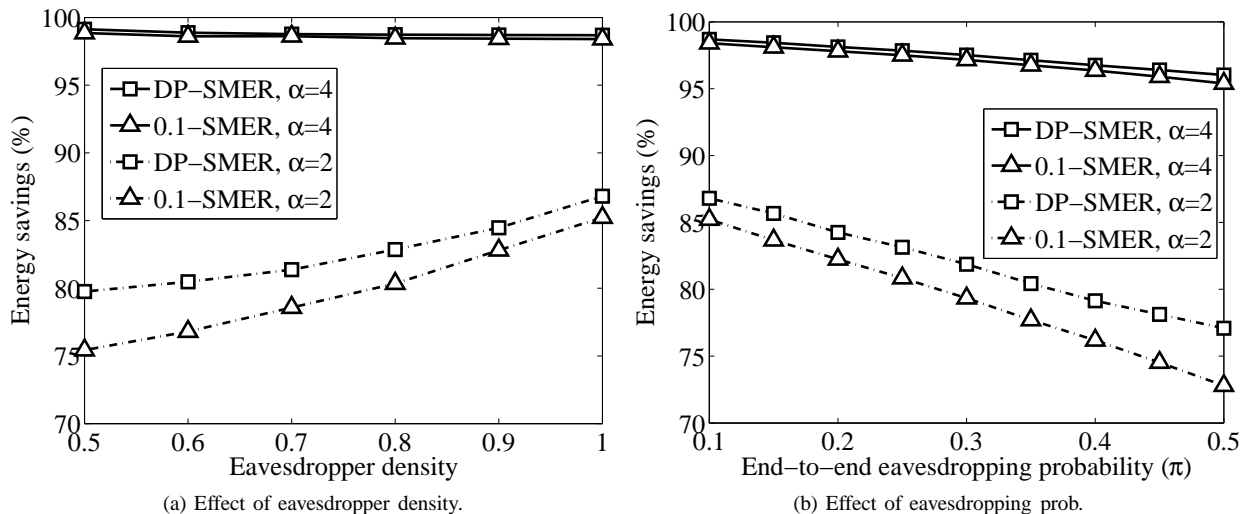(a) Effect of eavesdropper density.

(b) Effect of eavesdropping prob.

Fig. 4: Energy savings with uniform eavesdropper placement.

Those paths that are longer provide more opportunities for energy savings on each link of the path resulting in increased overall energy savings. This effect works in favor of $\alpha = 2$ as well as $\alpha = 4$. However, given the high values of energy savings for $\alpha = 4$ (due to longer paths compared to $\alpha = 2$), the effect of longer paths is more prominent for $\alpha = 2$.

(a) Non-uniform eavesdrop. placement.
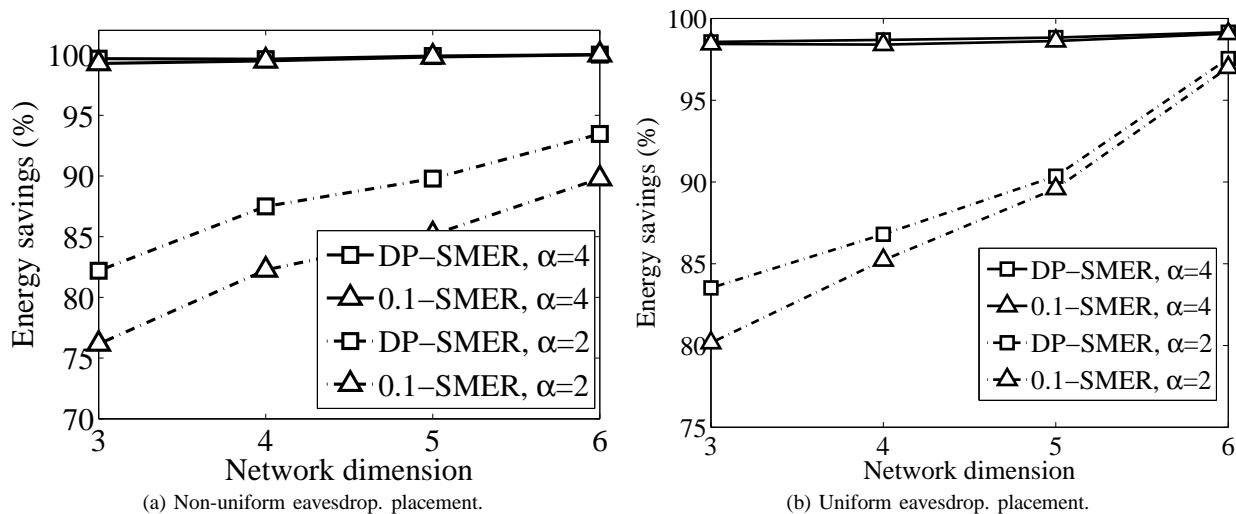
(b) Uniform eavesdrop. placement.

Fig. 5: Effect of network size on energy savings.

Effect of Jamming Set. The cardinality of the jamming set affects the power allocation to jammers. In this experiment, we change the number of jammers that participate in secure transmissions on each link and compute the energy savings achieved by different algorithms. Figs. 6(a) and 6(b), respectively, show the energy savings achieved for non-unform and uniform placement of eavesdroppers. Interestingly, in these scenarios, 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. RELATED WORK

A survey of prior work is presented in this section.

Secure Routing in Multi-hop Networks. While there are numerous works on secure routing in wireless networks (see, *e.g.*, [35] and references therein), their focus is on preventing malicious attacks that disrupt the operation of

(a) Non-uniform eavesdrop. placement.
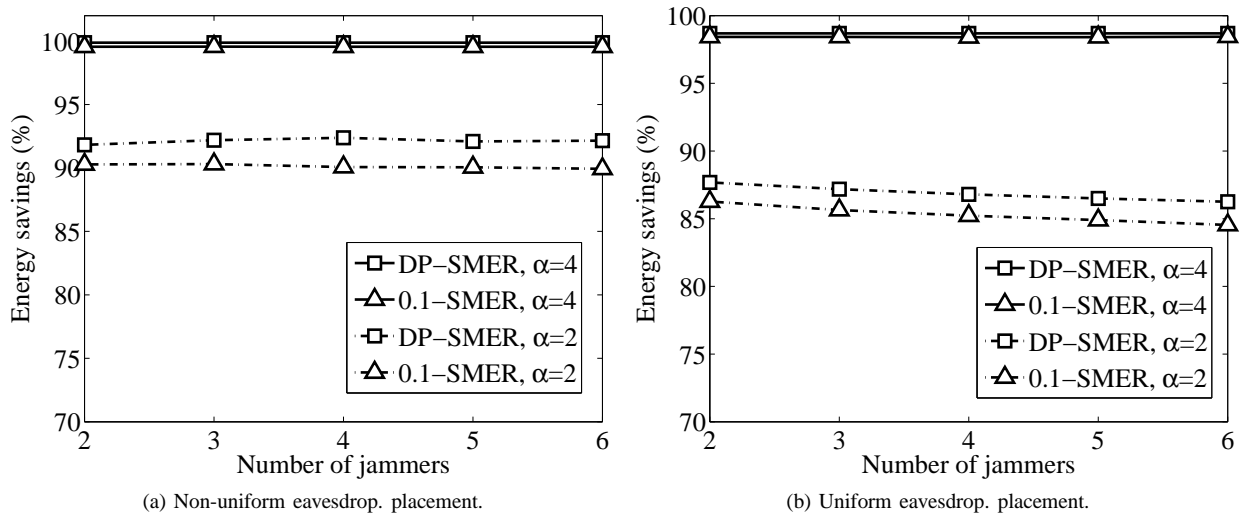
(b) Uniform eavesdrop. placement.

Fig. 6: Effect of the jamming set on energy savings.

the routing protocol using application level mechanisms such 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 in the network, which is orthogonal to the secure routing problem considered in the existing literature.

Wireless Physical Layer Security. The idea behind physical layer security is to exploit the characteristics of the wireless channel such as fading to provide secure wireless communications. The foundations of information theoretic security, which is the theoretical basis for physical layer security, were laid by Wyner and others [4]–[6] based on Shannon's notion of perfect secrecy [3]. In the classical wiretap model of Wyner, to achieve a strictly positive secrecy rate, the legitimate user should have some advantage over the eavesdropper in terms of SNR. Later, Maurer [7] proved that even when a legitimate user has a worse channel than an eavesdropper, it is possible to have secure communication. While some physical layer security techniques allow for opportunistic exploitation of the space/time/user diversity for secret communications [7], [8], others actively manipulate the wireless channel to block eavesdroppers by employing techniques such as multiple antennas [21] and jamming [10], [12]. While some of these techniques have been successfully implemented in practical systems [22], physical layer security is focused on very special network topologies, *e.g.*, single-hop networks. In this work, we have developed algorithms to extend these techniques to multi-hop networks.

Scaling Laws in Large Secure Networks. Motivated by [36], recently, throughput scaling versus security tradeoffs have been investigated in the context of large wireless networks [13], [17]–[19]. Specifically, for cooperative jamming when the eavesdroppers are uniformly distributed, it was shown that if the number of eavesdroppers grows sub-linearly with respect to the number of legitimate nodes, a positive throughput for secure communication is achievable [13].

Security Based on Network Topology. When there is sufficient path diversity in a network, different messages can be routed over different parts of the network in the hope that an eavesdropper would be incapable of capturing all messages from across the network. To exploit network diversity for security, various techniques based on multi-path routing [37], [38] and network coding [39], [40] have been investigated. While such techniques are suitable for wired networks, their application in wireless networks is challenging due to lack of path diversity at the source or destination of a communication session. Moreover, there are considerable complications when splitting a flow among several paths, in particular, at the granularity of a single session. Moreover, network topology, in wireless networks, is a function of power allocation at the physical-layer and propagation environment, *e.g.*, fading. Nevertheless, our approach is complimentary to these techniques, by providing a mechanism to find a minimum cost path that is information-theoretically secure, regardless of the network diversity.

VIII. 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.

References

[1] D. Stinson, *Cryptography: theory and practice*. CRC press, 2006.
[2] National Security Agency, "Defense in depth: A practical strategy for achieving information assurance in today's highly networked environments." [Online]. Available: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf
[3] C. Shannon, *Communication theory of secrecy systems*. AT&T, 1949.
[4] A. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, no. 8, 1975.
[5] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, 1978.
[6] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, 1978.
[7] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, 1993.
[8] M. Bloch *et al.*, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, 2008.
[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, 2008.
[10] 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.
[11] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, 2010.
[12] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, 2008.
[13] 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.
[14] M. Haenggi, "The secrecy graph and some of its properties," in *IEEE ISIT*, Jun. 2008.
[15] P. Pinto, J. Barros, and M. Win, "Physical-layer security in stochastic wireless networks," in *IEEE ICCS*, Nov. 2008.
[16] ——, "Wireless physical-layer security: The case of colluding eavesdroppers," in *IEEE ISIT*, Jun. 2009.
[17] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *IEEE ISIT*, Jun. 2009.
[18] O. Koyluoglu, E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," in *IEEE ITA*, Feb. 2010.
[19] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *ACM Mobihoc*, Sep. 2010.
[20] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels with imperfect ECSI," in *IEEE Globecom*, 2011.
[21] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *CISS*, Mar. 2007.
[22] S. Gollakota *et al.*, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *ACM Sigcomm*, 2011.
[23] S. Oh, T. Vu, M. Gruteser, and S. Banerjee, "Phantom: Physical layer cooperation for location privacy protection," in *IEEE Infocom*, Orlando, USA, Mar. 2012.
[24] D. Tse and P. Viswanath, *Fundamentals of wireless communications*. Cambridge, UK: Cambridge University Press, 2005.
[25] A. Goldsmith, *Wireless communications*. Cambridge, 2005.
[26] D. Seymour and J. Britton, *Introduction to Tessellations*. Palo Alto, USA: Dale Seymour Publications, 1990.
[27] M. Dehghan, D. Goeckel, M. Ghaderi, and Z. Ding, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Transactions on Wireless Communications*, vol. 54, no. 8, 2012.
[28] R. Mudumbai, D. Brown, U. Madhow, and H. Poor, "Distributed transmit beamforming: challenges and recent progress," *IEEE Communications Magazine*, vol. 47, no. 2, 2009.
[29] M. Rahman, H. Baidoo-Williams, R. Mudumbai, and S. Dasgupta, "Fully wireless implementation of distributed beamforming on a software-defined radio platform," in *ADM/IEEE IPSN*, 2012.
[30] D. Brown, U. Madhow, P. Bidigare, and S. Dasgupta, "Receiver-coordinated distributed transmit nullforming with channel state uncertainty," in *Conference on Information Sciences and Systems (CISS)*, Mar. 2012.
[31] G. L. Turin, "The characteristic function of hermitian quadratic forms in complex normal variables," *Biometrika*, vol. 47, no. 1/2, 1960.
[32] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, 1979.
[33] M. R. Garey and D. S. Johnson, *Computers and interactability: A guide to the theory of NP-Completeness*. New York, 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," *Operations Research Letters*, vol. 28, 1999.
[35] L. Abusalah *et al.*, "A survey of secure mobile ad hoc routing protocols," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 4, 2008.
[36] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, 2000.
[37] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "SPREAD: Improving network security by multipath routing in mobile ad hoc networks," *ACM Wireless Networks*, vol. 15, no. 3, 2009.
[38] 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.
[39] N. Cai and R. W. Yeung, "Secure network coding," in *IEEE ISIT*, Jun. 2002.
[40] K. Jain, "Security based on network topology against the wiretapping attack," *IEEE Wireless Commun. Mag.*, vol. 11, no. 1, 2004.