Energy-Efficient Secrecy in Wireless Networks
Based on Random Jamming

Azadeh Sheikholeslami, Majid Ghaderi, Member, IEEE, Hossein Pishro-Nik, Member, IEEE,
Dennis Goeckel, Fellow, IEEE

Abstract—Secure energy-efficient routing in the presence of multiple passive eavesdroppers is considered. Previous work in this area has considered secure routing assuming probabilistic or exact knowledge of the location and channel-state-information (CSI) of each eavesdropper. In wireless networks, however, the locations and CSIs of passive eavesdroppers are not known, making it challenging to guarantee secrecy for any routing algorithm.

We develop an efficient (in terms of energy consumption and computational complexity) routing algorithm that does not rely on any information about the locations and CSIs of the eavesdroppers, and moreover, guarantees secrecy even in disadvantaged wireless environments, where multiple eavesdroppers try to eavesdrop each message, are equipped with directional antennas, or can get arbitrarily close to the transmitter. The key to achieving this is using additive random jamming to exploit inherent non-idealities of the eavesdropper’s receiver, which makes the eavesdroppers incapable of recording the messages. We have simulated our proposed algorithm and compared it with existing secrecy routing algorithms in both single-hop and multi-hop networks. Our results indicate that when the uncertainty in the locations of eavesdroppers is high and/or in disadvantaged wireless environments, our algorithm outperforms existing algorithms in terms of energy consumption and secrecy.

I. INTRODUCTION

Information secrecy has traditionally been achieved by cryptography, which is based on assumptions on current and future computational capabilities of the adversary. However, there are numerous examples of cryptographic schemes being broken that were supposedly secure [1]. This motivates the consideration of physical layer schemes which are based on information-theoretic secrecy [2]. In a scenario where an adversary tries to eavesdrop on the main channel between a transmitter and a receiver, Wyner showed that, if the eavesdropper’s channel is degraded with respect to the main channel, a positive secrecy rate can be achieved. This idea was later extended to Gaussian channels [3], and to the more general case of a wiretap channel with a "more noisy" or "less capable" eavesdropper channel [4]. Thus, the key to obtain information-theoretic secrecy is having an advantage for the main channel against the eavesdropper channel. However, such an advantage cannot always be guaranteed. In particular, the locations of eavesdroppers are not known and an eavesdropper might be much closer to the transmitter than the intended receiver. To overcome this problem, one must design algorithms to obtain the required advantage for the intended recipient over the eavesdroppers.

The idea of adding artificial noise to the signal by means of multiple antennas at the transmitter or some helper nodes was introduced in [5], [6]. The artificial noise is placed in the null space of the channel from the transmitter to the intended recipient and thus does not affect it. But, it degrades the eavesdropper’s channel with high probability. Subsequently, cooperative jamming for physical layer secrecy has been extensively studied, e.g. [7]–[12]. These works mainly focus on one-hop networks consisting of one transmitter, one receiver, one eavesdropper and maybe a few helper nodes that generate the artificial noise. The case of two-hop networks consisting of one transmitter, one receiver, one relay, one eavesdropper and maybe a few helper nodes has also been considered extensively in the literature [13]–[16]. In the case of multi-hop networks with multiple transmitters and receivers and in the presence of many eavesdroppers, often the asymptotic results for large networks have been investigated [17]–[25].

However, whereas one-hop, two-hop and asymptotically large networks are most amenable to analysis and do provide insight into wireless network operation, most ad hoc networks in practice operate with a number of nodes and a number of hops that is between these two extremes. Hence, the design of algorithms to provide secrecy in networks of arbitrary "moderate" size is of interest, which is considered here. We consider a network with multiple system nodes where a source node communicates with a destination node in a multi-hop fashion and in the presence of multiple passive eavesdroppers. We define the cost of communication to be the total

This work was supported by the National Foundation under Grant CIF-1421957.
energy spent by the system nodes to securely and reliably transmit a message from the source to the destination. Thus, our goal is to find routes that minimize the cost of transmission between the source and destination nodes. Energy efficiency is an important consideration in designing the routing algorithms, and energy efficient routing has been extensively studied in the literature, e.g. [26]–[34]. However, only a few works have considered energy-aware routing with secrecy considerations [35], [36].

In [35], [36], the authors use a general probabilistic model for the location of each eavesdropper, and introduce a routing algorithm called SMER (secure minimum energy routing) which employs cooperative jamming to provide secrecy at each hop such that the end-to-end secrecy of the multi-hop source-destination path is guaranteed. When the density of eavesdroppers is low such that there is only one eavesdropper per hop, the location of the eavesdroppers are known, and the eavesdroppers are restricted to use omni-directional antennas, this approach is promising. However, since we are considering passive eavesdroppers, their location and channel-state-information (CSI) are not known to the legitimate nodes. Further, in a disadvantaged wireless environment, many passive eavesdroppers might try to intercept the message at each hop, with large uncertainty in the locations of the eavesdroppers, and the eavesdroppers might get arbitrarily close to the transmitters. In such a situation, the energy consumption of any cooperative jamming approach including the scheme of [35], [36] can become very high. Further, if we plan for the wrong number of eavesdroppers or do not correctly anticipate the quality of the eavesdroppers’ channels, the secrecy will be compromised. Hence, in this paper we seek methods that do not rely on the quality of eavesdroppers’ channels and their locations and can provide secrecy in disadvantaged environments at a reasonable cost.

In [37], [38], the authors propose adding random jamming with large variations and based on an ephemeral key to the signal to obtain everlasting secrecy in disadvantaged wireless environments. In contrast to previous methods based on a key to facilitate secrecy in wireless networks, the work in [37], [38] does not presume that the key is kept secret from the eavesdropper indefinitely; rather, the jamming is used to build an advantage for the intended receiver over the eavesdropper by inhibiting the eavesdropper’s ability to even record a reasonable version of the message for later decoding. Here, we use the approach of [37], [38] in a network setting, where the source and intermediate relays at each hop add a random jamming signal to the message to protect it against the eavesdroppers. We design a fast (polynomial time) and efficient routing algorithm such that the aggregate energy spent to convey the message and to generate the random jamming signal is minimized. Our contributions in this paper are:

- We develop a routing algorithm that minimizes the end-to-end energy consumption of sending a message and jamming signal, while satisfying an end-to-end secrecy requirement.
- Our routing algorithm is independent of the number, location and channel-state-information of the eavesdroppers. It can guarantee secrecy in worst case scenarios: when many eavesdroppers are present, the eavesdroppers can get very close to the transmitters, and they use directional antennas pointed at the transmitters.
- We conduct detailed simulations to evaluate the performance of our proposed algorithm and compare it with the algorithm proposed in [35], [36]. Our simulation results show that our algorithm can achieve a significant improvement in terms of the average energy expended for various network simulation scenarios in disadvantaged wireless environments and/or when the uncertainty in the locations of the eavesdroppers is high.

The rest of the paper is organized as follows. Section II describes the system model, the approach which is used in this paper, and the metric. The analysis of the problem and the algorithm for minimum energy routing with secrecy constraints is presented in Section III. In Section IV, the results of numerical examples for various realizations of one-hop and multi-hop systems are provided, and the comparison of the proposed method to SMER algorithm is presented. Conclusions are discussed in Section V.

II. System Model and Approach

A. System Model

We consider a wireless network with nodes that are distributed arbitrarily. A source node generates the message and conveys it to a destination node in a multi-hop fashion. An H-hop path from the source to the destination is denoted by \( \Pi = \langle l_1, \ldots, l_H \rangle \), where \( l_i \) is the link that connects two nodes \( S_i \) and \( D_i \) along the path \( \Pi \). There are also non-colluding eavesdroppers present in the network such that the message transmission of each link is prone to be overheard by multiple eavesdroppers. We denote the set of eavesdroppers by \( \mathcal{E} \). The eavesdroppers are assumed to be passive, and thus their locations and their channel-state informations are not known to the legitimate nodes. We assume that the system nodes are equipped with omni-directional antennas while the
eavesdroppers can be equipped with more sophisticated directional antennas.

For the channel, we consider transmission in a quasi-static Raleigh fading environment. Let $h_{S,D}$ be the fading coefficient between node $S$ and node $D$ (This assumption is relaxed for eavesdroppers’ channels, as discussed later.). Without loss of generality, we assume $E[|h_{S,D}|^2] = 1$. Suppose the transmitter $S$ transmits the signal $x_S$ at power level $P_S$. The signal that the receiver $D$ (analogously, eavesdropper $E$) receives is:

$$\tilde{y}_D = \frac{x_S h_{S,D}}{d_{S,D}^\alpha} + n_D$$

where $d_{S,D}$ is the distance between $S$ and $D$, $\alpha$ is the path-loss exponent, and $n_D \sim \mathcal{N}(0, \sigma_D^2)$ is additive white Gaussian noise (AWGN) at the receiver $D$.

Because compression of a receiver’s front-end dynamic range is the biggest challenge when operating in the presence of strong jamming, we also consider the effect of the analog-to-digital converter (A/D) on the received signal, which consists of the quantization noise and the quantizer’s overflow. The quantization noise is a result of the limited resolution of the A/D, and the quantizer’s overflow happens when the range of the received signal is larger than the span of the A/D. We assume that the quantization noise is uniformly distributed [39, Section 5]. The resolution of a $b$-bit A/D with full dynamic range $[-r, r]$ is

$$\delta = \frac{2r}{2^b}$$

Since the power of the received signal at the eavesdropper $E$ (analogously, receiver $D$) is $\frac{P_S |h_{S,E}|^2}{d_{S,E}^\alpha}$, we set the range of the A/D as,

$$r = \frac{l \sqrt{P_S} |h_{S,E}|}{d_{S,E}^\alpha}$$

where $l$ is a constant that maximizes the mutual information between the transmitted signal and the received signal [40]. Hence, the resolution of the A/D of the eavesdropper $E$ (receiver $D$) is:

$$\delta = \frac{2l \sqrt{P_S} |h_{S,E}|}{2^b d_{S,E}^\alpha}.$$

### B. Approach: Random Jamming for Secrecy

We use the random jamming scheme of [37], [38] to provide everlasting secrecy. In this scheme, based on a cryptographic key that is shared between the legitimate nodes, a jamming signal with large variation is added to the transmitted signal. It is assumed that the cryptographic key should be kept secret just for the time of transmission, and can be revealed to the eavesdropper right after transmission without compromising secrecy. The legitimate receiver can use its key to cancel the effect of the jamming before analog-to-digital-conversion (A/D), while the eavesdropper must record the signal and jamming, and cancel the effect of jamming later from the recorded signal (after analog-to-digital-conversion). Hence, the signal that the legitimate receiver receives is well-matched to its A/D converter. On the other hand, the large variation of the random jamming signal causes overflow of the eavesdropper’s A/D. The eavesdropper may enlarge the span of her A/D to prevent overflows; however, it degrades the resolution of its A/D, thus increasing the A/D noise. In [37], [38] it is shown that, although increasing the span of the A/D causes the eavesdropper to suffer from more quantization noise, the overflows are more harmful, and thus the best strategy that the eavesdropper can employ is to enlarge the span of its A/D such that it captures all of the signal and thus no overflow occurs.

The random jamming signal $J$ that the transmitter adds to its signal follows a uniform distribution with $2^K$ jamming levels. Hence, $K$ bits of the cryptographic key to generate each jamming symbol are needed. The distance between two consecutive jamming levels is $2^l \sqrt{P_S}$. Thus, the average energy that is spent on the random jamming signal is,

$$P_J = E[J^2] = \frac{1}{2^K} \sum_{j=0}^{2^K-1} \left(2^l \sqrt{P_S} j\right)^2 = 4^l P_S \sum_{j=0}^{2^K-1} j^2 = 4^l P_S \times \frac{2^{3K+1} - 3 \times 2^K + 2K}{6} = \frac{2^K (2^{2K+1} - 3 \times 2^K + 1) P_S}{3}$$

where $\beta$ is a constant that depends on $K$.

Suppose that the eavesdropper uses a $b_E$-bit A/D. Since the power of the signal at the eavesdropper’s receiver is $\frac{P_S |h_{S,E}|^2}{d_{S,E}^\alpha}$, and considering the automatic-gain-control of the eavesdropper’s receiver, the resolution of the eavesdropper’s A/D before jamming is:

$$\delta_E = \frac{2l \sqrt{P_S} |h_{S,E}|^2}{2^{b_E} d_{S,E}^\alpha}.$$

Now suppose that the transmitter adds the jamming to its signal. Since the eavesdropper does not know the key,
it should enlarge the span of its A/D to capture all the signal plus jamming. The maximum amplitude of the signal plus jamming can be written as,

$$\sqrt{\frac{P_S|\bar{h}_{S,E}|^2}{d_{S,E}^2}} + (2^K - 1)\sqrt{\frac{P_S|\bar{h}_{S,E}|^2}{d_{S,E}^2}} = 2^K \sqrt{\frac{P_S|\bar{h}_{S,E}|^2}{d_{S,E}^2}}$$

Thus, the resolution of eavesdropper’s A/D is:

$$\delta_E^2 = \frac{2l\sqrt{P_S|\bar{h}_{S,E}|^2}}{2^b_E d_{S,E}^2} \times 2^K = \frac{2l\sqrt{P_S|\bar{h}_{S,E}|^2}}{2^b_E - K d_{S,E}^2}$$  \(3\)

The random jamming scheme of [37], [38] relies on the limited resolution of the eavesdropper’s A/D. Hence, we should assume that the legitimate nodes either know a bound on the quality of the eavesdroppers’ A/Ds, or plan for the case that all eavesdroppers use the best A/D technology available at the time. The realization of this assumption is facilitated by the fact that A/D technology progresses very slowly\(^1\). Hence, throughout this paper we assume that the resolution of the A/D of each eavesdropper is equal to or less than \(b_E\) bits.

C. Jamming Cancellation at the Legitimate Receiver

Nearly all techniques that exploit jamming for secrecy ignore the effects of channel estimation error (e.g. [5]–[12], [35], [37], [38]), yet it is important since in real systems the jamming power is high, and thus the residual jamming due to imperfections in channel estimation can be considerable. Note that from [41], [42], the channel estimation error might be very small, but, since we have high-power jammers, the residual interference is still important and can have an impact on system performance. Hence, we consider the residual jamming at the receiver due to errors in the channel estimates. Given a pilot-based approach for channel estimation, the channel estimate is conditionally Gaussian, where the mean of this Gaussian distribution is the minimum mean-squared estimate (MMSE) channel estimate. The estimation error of this MMSE estimate is a zero mean Gaussian random variable \(\mathcal{N}(0,\sigma^2)\) with variance (e.g. see [43]),

$$\sigma^2 = \theta^2 P_j|\bar{h}_{S,D}|^2$$

where \(\theta\) is a constant coefficient describing the normalized prediction error of the legitimate receiver. Hence, the estimation error acts like zero mean additive white Gaussian noise with variance proportional to the received jamming power.

\(^1\)For a complete discussion on this see [38, Section V].

D. Metric

Since the quantization noise is uniformly distributed [39, Section 5], the derivation of the capacity of the channel between transmitter and receiver, and the channel between transmitter and eavesdropper, is not straightforward. Thus, we apply an upper-bound and a lower-bound of the capacity of a channel with independent additive noise as described in [44] and [45]. Suppose that the resolution of the A/D of receiver \(D\) is \(\delta_D\). The capacity of the channel between the transmitter \(S\) and the receiver \(D\) conditioned on the fading coefficient can be lower bounded as [38]:

$$C_{S,D}(\log |h_{S,D}|^2) \geq \log \left( \frac{P_s|\bar{h}_{S,D}|^2 + \sigma^2_S + \delta^2_D}{\sigma^2_D + \delta^2_D} \right),$$

$$= \log \left( \frac{P_s|\bar{h}_{S,D}|^2 + \theta^2 P_j|\bar{h}_{S,D}|^2}{\sigma^2_D + \delta^2_D} \right),$$  \(4\)

and the capacity of the channel between the transmitter \(S\) and the eavesdropper \(E\) can be upper bounded as [38]:

$$C_{S,E}(\log |h_{S,E}|^2) \leq \log \left( \frac{P_s|\bar{h}_{S,E}|^2 + \sigma^2_E + \delta^2_E}{\sigma^2_E + \delta^2_E} \right).$$  \(5\)

In order to guarantee proper signal reception at the legitimate receiver, the capacity of the main channel should be greater than a predetermined threshold. Let us define,

$$\gamma_D = \frac{P_s|\bar{h}_{S,D}|^2 + \theta^2 P_j|\bar{h}_{S,D}|^2 + \sigma^2_S + 2 \delta^2_D}{\sigma^2_S + \delta^2_D}.$$  \(6\)

Hence, the communication between source and destination is reliable if,

$$\gamma_D \geq \gamma^*_D.$$  \(7\)

We define the average outage probability between \(S\) and \(D\) as,

$$p_{out} = \mathbb{P}(\gamma_D < \gamma^*_D).$$

In order to guarantee secrecy, the capacity of the channel between the transmitter and eavesdropper should be less than a predetermined threshold. We define,

$$\gamma_E = \frac{P_s|\bar{h}_{S,E}|^2 + \sigma^2_E + \delta^2_E}{\sigma^2_E + \delta^2_E}.$$  \(8\)

Hence, the communication between source and destination is secure if,

$$\gamma_E \leq \gamma^*_E.$$
We define the average secrecy-outage probability (i.e., eavesdropping probability) as,

\[ p_{\text{eav}} = P(\gamma_E \geq \gamma_E^*) \].

From (6) and (8) we conclude that if reliability and secrecy constraints are satisfied, the secrecy rate of at least,

\[ R_s = \log(\gamma_D^*) - \log(\gamma_E^*) \],

(9)
can be achieved. However as described above, instead of considering a constraint on the secrecy rate, we consider constraints on the individual success probabilities of the receiver and the eavesdropper. If we instead put the constraint on the secrecy rate, for a single secrecy rate many \((\gamma_D, \gamma_E)\) would satisfy the constraint. But codes are designed to work on a specific \((\gamma_D, \gamma_E)\) pair, and there is no universal wiretap code which is effective for all the pairs \((\gamma_D, \gamma_E)\) that satisfy (9) [46], [47]. Hence, we consider (6) and (8) as our reliability and secrecy constraints, respectively.

III. SERJ: SECURE ENERGY-EFFICIENT ROUTING USING JAMMING

Our goal is to find the optimal path with minimum energy consumption that connects the source to the destination:

\[ \Pi^* = \arg \min_{\Pi \in \mathcal{P}} C(\Pi), \]

where \(\mathcal{P}\) is the set of all routes from the source to the destination, and \(C(\Pi)\) is the cost of establishing the path \(\Pi\). In other words, \(C(\Pi)\) is the total power of the source and the relay nodes, which consists of the power to transmit the message \(\sum_{l_i \in \Pi} P_{S_i}\), and the jamming power \(\sum_{l_i \in \Pi} P_{J_i}\). Hence, our optimization objective is,

\[ C(\Pi) = \min_{\Pi \in \mathcal{P}} \sum_{l_i \in \Pi} P_{S_i} + P_{J_i}. \]

(10)

Suppose \(\Pi = \{l_1, \ldots, l_H\}\). By applying the coding technique described in [48], securing each hop is sufficient to ensure end-to-end secrecy. Hence, we consider the following secrecy constraints,

\[ \gamma_{E_{i,j}} < \gamma_E^*, \forall l_i \in \Pi \text{ and } \forall E_j \in \mathcal{E}, \]

(11)

which means that for all eavesdroppers in the network \(E_j \in \mathcal{E}\), the secrecy constraint must be satisfied. Transmission is reliable provided that an end-to-end average outage probability is guaranteed, i.e.

\[ \frac{p_{\text{out}}^{SD}}{\lambda} \leq \epsilon. \]

(12)

where \(p_{\text{out}}^{SD}\) denotes the average outage probability of the link \(l_i = \langle S_i, D_i \rangle\). Also, the following constraints should be satisfied,

\[ P_{S_i} \geq 0, \text{ and } P_{J_i} \geq 0. \]

(13)

Suppose that the number of key bits per jamming symbol that \(S_i\) utilizes is denoted by \(K_i\). From (1),

\[ P_{J_i} = \frac{2^l (2^{2K_i+1} - 3 \times 2^{K_i+1})}{3} P_{S_i}. \]

Define,

\[ \beta_i = \frac{2^l (2^{2K_i+1} - 3 \times 2^{K_i+1})}{3}. \]

Hence, the optimization objective can be written as,

\[ C(\Pi) = \min_{\Pi \in \mathcal{P}} \sum_{l_i \in \Pi} P_{S_i} (1 + \beta_i). \]

(14)

A. Analysis of Secrecy

Consider the secrecy constraint. Substituting \(\delta_{\text{E}}\) from (3) into (8) and (11), we have,

\[ \gamma_{E_{i,j}} = \frac{d_{E_{i,j}}^2 \left( 1 + \frac{1}{12 \times 2^{2\beta_{E_{i,j}}}} \right) + \sigma_E^2}{2\pi \sigma_{E_{i,j}}^2 2^{2\beta_{E_{i,j}}}}. \]

(15)

Since we do not want to make assumptions on the eavesdropper’s noise characteristics or the distance of any eavesdropper from a system node, we assume \(\sigma_E^2 = 0\). Hence, our goal is to have,

\[ \gamma_{E_{i,j}} = \frac{d_{E_{i,j}}^2 \left( 1 + \frac{1}{12 \times 2^{2\beta_{E_{i,j}}}} \right) + \sigma_{E_{i,j}}^2}{2\pi \sigma_{E_{i,j}}^2 2^{2\beta_{E_{i,j}}}} \]

\[ = 1 + \frac{1}{12 \times 2^{2\beta_{E_{i,j}}}} < \gamma_E^*. \]

(16)

Note that (16) is a deterministic function and does not depend on \(|h_{E_{i,j}}|^2\). Thus, if we choose \(K_i\) such that (16) is satisfied, none of the eavesdroppers in \(E\) can intercept the message being transmitted over the link \(l_i\). In order to guarantee secrecy, the following lower bound for the number of key bits per jamming symbol \(K_i\) at each hop must be satisfied:

\[ K_i \geq \frac{1}{2} \log_2 \left( \frac{2\pi 2^{2b_E}}{\gamma_E^* - \pi e/6} \right). \]

(17)

This bound only depends on the resolution of the eavesdropper’s A/D (which is assumed to be bounded by \(b_E\), as discussed in Section II-B), and does not depend on the eavesdropper’s location or its CSI. Intuitively, when the number of key bits per jamming symbol is sufficiently large, the quantization noise becomes large enough to
Because $\beta_i$ only depends on $K_i$, $\beta_i = \beta$, $i = 1, \ldots, H$, where $\beta$ is defined in (1). Hence, (14) becomes,

$$C(\Pi) = \min \sum_{l_i \in \Pi} P_{S_i}(1 + \beta)$$

$$= \min (1 + \beta) \sum_{l_i \in \Pi} P_{S_i}$$

(19)

Since $\beta$ is an increasing function of $K$, using the $K$ of (18) is equivalent to minimizing $\beta$. Hence, our optimization objective turns into,

$$\min \sum_{l_i \in \Pi} P_{S_i}.$$  

(20)

**B. Analysis of Reliability**

For the reliability constraint in (12), the probability of outage at $D_i$ is,

$$p_{out}^i = \mathbb{P}\left(\frac{P_{S_i}|h_{S_i,D_i}|^2 + \theta^2 P_{S_i}|h_{S_i,D_i}|^2 + \sigma^2 + \frac{\delta^2}{12} < \gamma_D^*}\right)$$

$$= \mathbb{P}\left(\frac{P_{S_i}|h_{S_i,D_i}|^2 + \theta^2 |h_{S_i,D_i}|^2 + \sigma^2 + \frac{\delta^2}{12} < \gamma_D^*}\right)$$

$$= \mathbb{P}\left(|h_{S_i,D_i}|^2 < \frac{(\gamma_D^* - 1)(\sigma^2 + \frac{\delta^2}{12})}{P_{S_i}(1 - (\gamma_D^* - 1)\theta^2 \beta)}\right)$$

$$= 1 - e^{-\frac{P_{S_i}|h_{S_i,D_i}|^2}{(1 - (\gamma_D^* - 1)\theta^2 \beta)}}$$

(21)

where the last equality follows because, for Raleigh fading, $|h_{S_i,D_i}|^2$ is exponentially distributed. Substituting (21) into (12), the end-to-end outage probability constraint is,

$$P_{OUT}^{SD} = 1 - \prod_{l_i \in \Pi} e^{-\frac{(\gamma_D^* - 1)(\sigma^2 + \frac{\delta^2}{12})}{P_{S_i}(1 - (\gamma_D^* - 1)\theta^2 \beta)}}$$

$$= 1 - \exp\left(-\sum_{l_i \in \Pi} \frac{(\gamma_D^* - 1)(\sigma^2 + \frac{\delta^2}{12})}{P_{S_i}(1 - (\gamma_D^* - 1)\theta^2 \beta)}\right)$$

$$\leq \epsilon.$$  

Thus, the end-to-end reliability constraint turns into,

$$\sum_{l_i \in \Pi} \frac{d_{S_i,D_i}}{P_{S_i}} \leq \eta,$$  

(22)

where,

$$\eta = \frac{\log \left( \frac{1}{1-\epsilon} \right) (1 - (\gamma_D^* - 1)\theta^2 \beta)}{(\gamma_D^* - 1)(\sigma^2 + \frac{\delta^2}{12})}.$$  

(23)

**C. Optimal Cost of a Given Path**

Our goal is to find the optimal path, which requires the minimum transmission and jamming power to satisfy both outage and reliability constraints. The optimal path is not known in advance. Hence, first we find the optimal transmit and jamming power allocation for a given path $\Pi$, and then we use it to design a routing algorithm that finds the optimal path. From (20)-(23), in order to find the optimal transmit and jamming power allocation for a given path, we should solve the following optimization problem,

$$\min_{P_{S_i} \geq 0} \sum_{l_i \in \Pi} P_{S_i}$$  

(24)

subject to:

$$\sum_{l_i \in \Pi} \frac{d_{S_i,D_i}}{P_{S_i}} \leq \eta$$  

(25)

The left side of (25) is a decreasing function of $P_{S_i}$, and our goal is to find the minimum $P_{S_i}$. Hence, we can substitute the inequality with an equality,

$$\sum_{l_i \in \Pi} \frac{d_{S_i,D_i}}{P_{S_i}} = \eta$$  

(26)

This optimization problem can be solved using the technique of Lagrange multipliers. We must solve (24) and the following equations simultaneously,

$$\frac{\partial}{\partial P_{S_i}} \left\{ \sum_{l_i \in \Pi} P_{S_i} + \lambda \left( \sum_{l_i \in \Pi} \frac{d_{S_i,D_i}}{P_{S_i}} - \eta \right) \right\} = 0,$$  

for $i = 1, \ldots, H.$

Taking derivatives we have,

$$1 - \lambda \frac{d_{S_i,D_i}^2}{P_{S_i}^2} = 0, \quad i = 1, \ldots, H,$$  

(27)

and thus,

$$P_{S_i} = \sqrt{\lambda \frac{d_{S_i,D_i}^2}{\eta}}.$$  

(28)

Substituting $P_{S_i}, i = 1, \ldots, H$ from (28) into (26), we obtain that,

$$\lambda = \frac{1}{\eta^2} \left( \sqrt{\lambda \frac{d_{S_i,D_i}^2}{\eta}} \right)^2.$$  

(29)
Substituting $\lambda$ from (29) into (28), the optimal transmit power at each link is given by,

$$P_{S_i} = \frac{1}{\eta} \sqrt{\frac{d_{S_i,D_i}^\alpha}{\sum_{l_k \in \Pi} \eta d_{S_k,D_k}^\alpha}}$$  \hspace{1cm} (30)

Hence, the aggregate cost of transmitting the message is,

$$\sum_{l_i \in \Pi} P_{S_i} = \frac{1}{\eta} \left( \sum_{l_k \in \Pi} \eta d_{S_k,D_k}^\alpha \right)^2$$  \hspace{1cm} (31)

and the cost of jamming is,

$$\sum_{l_i \in \Pi} P_{J_i} = \frac{\beta}{\eta} \left( \sum_{l_k \in \Pi} \eta d_{S_k,D_k}^\alpha \right)^2$$  \hspace{1cm} (32)

The total cost of establishing the optimal path $\Pi$ is,

$$C(\Pi) = \frac{1 + \beta}{\eta} \left( \sum_{l_k \in \Pi} \eta d_{S_k,D_k}^\alpha \right)^2$$  \hspace{1cm} (33)

D. Routing Algorithm

Considering the structure of the total cost of establishing the optimal path (33) yields the routing algorithm. Assign the link weight $\sqrt{\frac{d_{S_i,D_i}^\alpha}{\sum_{l_k \in \Pi} \eta d_{S_k,D_k}^\alpha}}$ to each potential link $l_i$ between nodes $S_i$ and $D_i$ of the network. Then, run a classical shortest-path algorithm such as Dijkstra’s algorithm to find the route $\Pi$ with minimum total weight, which is $\sum_{l_i \in \Pi} \eta d_{S_i,D_i}^\alpha$. Clearly this route also minimizes the total cost in (33). From (30), each node along $\Pi$ forwards the message to the next node using the total (transmit and jamming) power,

$$C(l_i) = \frac{1 + \beta}{\eta} \sqrt{\frac{d_{S_i,D_i}^\alpha}{\sum_{l_k \in \Pi} \eta d_{S_k,D_k}^\alpha}}$$  \hspace{1cm} (34)

IV. NUMERICAL RESULTS

In this section we numerically compare the performance of our algorithm with that of the SMER algorithm [35] in different scenarios.

SMER Algorithm. In SMER, the system nodes employ cooperative jamming to establish a secure path, and, if the eavesdroppers get very close to a transmitter, the secrecy is compromised. Hence, while the SERJ algorithm proposed here has no need or sense of a “guard region”, to employ SMER we must introduce such into the scenario. Thus, for the sake of comparison to SMER, assume a guard region with radius $r_{\text{min}} > 0$ around each transmitter and assume that no eavesdropper can enter the guard regions. Further, in SMER a set of locations and the probability that an eavesdropper exists in each location must be known. In order to address this requirement of SMER, we divide a circle centered at the transmitter $S$ and with radius $r_{\text{max}}$ into many sectors. Each sector is a location where an eavesdropper might exist. For instance, when three eavesdroppers are present, three sectors have an eavesdropper with probability one, and the rest of the sectors have an eavesdropper with probability zero (Fig. 1). Unlike the SERJ algorithm proposed in this paper, the secrecy outage probability of SMER is non-zero. In the next section, we will see how this non-zero eavesdropping probability affects the power consumption of secret communication.

To get more insight into the problem, first we consider secure one-hop transmission from a transmitter $S$ to a receiver $D$ in the presence of eavesdroppers. Next, we will consider multi-hop minimum energy routing in a network and in the presence of multiple eavesdroppers. In both cases, we assume that the system nodes and the eavesdroppers use 14-bit A/Ds, and we set $\theta = 10^{-6}$. We set the source-destination outage probability $\pi = 0.1$, receiver noise power $N_0 = 1$ (eavesdropper noise power is zero), $\gamma_B = 42$ and $\gamma_E = 34$, which results in the secrecy rate $R_s = 0.2$. We consider different propagation attenuation scenarios: $\alpha = 2$ which is the path-loss exponent corresponding to free space, and $\alpha = 3$ and $\alpha = 4$ which are the path-loss exponents corresponding to a terrestrial environment.

A. One-Hop Communication

Consider a single hop in a wireless network, consisting of a transmitter $S$ and a receiver $D$ (Fig. 2). For SMER, suppose two jammers $J_1$ and $J_2$ help the transmitter to convey its message to the receiver securely [35]. The distance between each jammer and the source is denoted
Fig. 2: One-hop communication between source $S$ and destination $D$ in the presence of eavesdroppers ($Es$). In SMER, two jammers $J_1$ and $J_2$ help to make the link secure.

Fig. 3: Power consumption of SERJ and SMER versus the number of eavesdroppers for various values of path-loss exponent $\alpha$.

Section III, the power required when employing SERJ does not depend on the number of eavesdroppers. On the other hand, when the number of eavesdroppers increases, the power needed to establish a secure link using SMER increases dramatically. Since the cost of communication using SERJ only depends on the distance between the transmitter and the receiver which is normalized to $d_{SD} = 1$, the cost of using SERJ does not change with the change of path-loss exponent in these plots.

**Guard Region Radius.** Whereas the proposed algorithm (SERJ) does not require a guard region, recall that SMER cannot be utilized without such. Fig. 4 shows the power versus $r_{\min}$ in the presence of $n_E = 5$ eavesdroppers, and for various values of the path-loss exponent $\alpha$. We set $d_{SD} = 1$, $p_{eav} = 10^{-5}$ and $r_{\max} = 2$. We observe that when $r_{\min}$ gets small, the power needed to establish a secure link using SMER increases dramatically, while the power needed to establish a secure link using SERJ does not depend on the allowable location of the eavesdropper. In fact as is shown in Section III, the power used by SERJ is independent of the distance between the transmitter and the eavesdroppers, and, even if the eavesdroppers get very close to the transmitter, they cannot intercept the message.

**Uncertainty in the Location of Eavesdroppers.** In Fig. 5, the power needed to transmit the message securely versus $r_{\max}$ for various values of the path-loss exponent $\alpha$ is depicted. For SMER we set $p_{eav} = 10^{-5}$.

by $d$. In the remainder of this section, we consider the effect of various parameters of the network on the energy consumption of our scheme and SMER.

**Number of Eavesdroppers.** Fig. 3 shows the transmission power versus the number of eavesdroppers around the transmitter\(^2\). In this figure, $p_{eav} = 10^{-5}$, $r_{\min} = 0.01$, $r_{\max} = 2$, and $d_{SD} = 1$. As shown in \(^2\)In all figures in this section, $P$ denotes the aggregate power consumed by the algorithm.
Fig. 5: Power consumption of SERJ and SMER versus $r_{\text{max}}$ for various values of $\alpha$ and when $n_E = 5$ eavesdroppers are present. The performance of SMER is closely dependent on the uncertainty in the locations of the eavesdroppers, while the performance of SERJ does not depend on the locations of the eavesdroppers.

Fig. 6: Power consumption of SERJ and SMER versus eavesdropping probability for various values of $\alpha$ and when $n_E = 5$ eavesdroppers are present. For small secrecy outage probabilities, the power consumption of SMER is substantially higher than the power consumption of SERJ.

and $r_{\text{min}} = 0.01$. As $r_{\text{max}}$ increases, the uncertainty in the location of the eavesdroppers increases, and thus in SMER the jammers need to consume more power to cover a larger area. On the other hand, with SERJ, the transmit power is independent of the locations of the eavesdroppers.

Eavesdropping Probability. As was shown in Section III, the eavesdropping probability of SERJ is zero. But, the eavesdropping probability of SMER is not zero. Fig. 6 shows the power needed to establish a secure link versus the eavesdropping probability when $n_E = 5$ eavesdroppers are present, and when for SMER $r_{\text{min}} = 0.01$, and $r_{\text{max}} = 2$. It can be seen that the power consumption of SMER dramatically changes when the secrecy outage probability changes. In particular, for small secrecy outage probabilities, the power consumption of SMER is substantially higher than the power consumption of SERJ.

Distance between Source and Destination. Fig. 7 shows the transmission power versus the distance between source and destination $d_{SD}$ for various values of $\alpha$ and when $n_E = 5$ eavesdroppers are present. As the distance between the transmitter and the receiver gets longer, the transmit power of both schemes increases.

B. Multi-Hop Communication

We consider a wireless network that consists of $n$ system nodes and $n_E$ eavesdroppers which are distributed uniformly at random on a $5 \times 5$ square. Our goal is to find a secure path with minimum aggregate energy from the source to the destination, using SERJ and SMER.

Before we proceed to the numerical results for a multi-hop network, we compare the complexity of SERJ and SMER algorithms in a network that consists of $n$ system nodes.

Running Time. In order to find the optimal path using SERJ we need to apply the Dijkstra’s algorithm, which is a polynomial algorithm with running time $O(n^2)$. On the other hand, SMER is a pseudo-polynomial algorithm of order $O(n^2 B)$, where $B$ is the maximum cost of any
path in the network. Note that, while the running time of SMER is polynomial in $B$, the actual value of $B$ grows exponentially with the size of the input (i.e., the number of bits used to represent link costs). That is, if $l$ bits are used to represent the link cost values then $B$ will be of order $2^l$.

For the remainder of this section, we assume that in SMER, for every node two friendly jammers exist that help the node to establish a secure link. We average the results over 10 random realizations of the network. In each realization, the system nodes are distributed uniformly at random, and the closest system node to the point $(0, 0)$ is the source of the message and the closest system node to the point $(5, 5)$ is the destination. We consider the path-loss exponent $\alpha = 3$, since $\alpha = 2$ corresponds to non-terrestrial environments, and $\alpha = 4$ leads to very high link costs of SMER, which make the running time of this algorithm excessively high. In the sequel, we investigate the effect of various parameters on the total energy consumption of SERJ and SMER, and compare their performance.

**Number of Eavesdroppers.** The average power $P$ versus the number of eavesdroppers for SERJ and SMER is shown in Fig. 8. There are $n = 25$ system nodes in addition to the eavesdroppers. The path-loss exponent of the environment is $\alpha = 3$. For SMER, we set $p_{eav} = 10^{-5}$, $r_{min} = .03$, and $r_{max} = 2$. It can be seen that for very small numbers of eavesdroppers, the performance of SMER is better than that of SERJ. However, as the number of eavesdroppers increases, the amount of power that SMER uses increases and becomes more than the power that SERJ consumes. As is shown in Section III, the amount of power that SERJ uses does not depend on the number and location of the eavesdroppers.

**Number of System Nodes.** The effect of the number of system nodes on the average aggregate power consumption is shown in Fig. 9. There are $n_E = 25$ eavesdroppers, and the path-loss exponent of the environment is $\alpha = 3$. For SMER, we set $p_{eav} = 10^{-5}$, $r_{min} = .03$, and $r_{max} = 2$.

It can be seen that the performance of SERJ is always superior to the performance of SMER. For both algorithms the average power is not sensitive to the number of system nodes. The fluctuations in this figure are due to the random generation of network configurations.

**Uncertainty in the Location of the Eavesdroppers.** In Fig. 10, the power needed to transmit the message securely versus $r_{max}$ is shown. There are $n = 25$ system nodes and $n_E = 25$ eavesdroppers, and the path-loss exponent of the environment is $\alpha = 3$. For SMER we set $p_{eav} = 10^{-5}$ and $r_{min} = 0.03$. With SERJ, the transmit power is independent of the location of the eavesdroppers. With SMER, as $r_{max}$ increases, the uncertainty in the location of the eavesdroppers increases, and thus the jammers need to consume more power to cover a larger area. For the case that SMER is secure against any eavesdropper in the network (i.e., $r_{max} = 5$, if we do not consider the guard regions around the transmitters), the power spent by SMER is substantially higher than the power spent by SERJ.
system nodes or pointed directional antennas at system nodes would significantly degrade the performance of SMER, but there would be no impact on the performance of SERJ. Hence, the proposed algorithm directly addresses one of the key roadblocks to the implementation of information-theoretic security in wireless networks: robustness to the operating environment.

V. CONCLUSIONS

In this paper, we have considered secure energy-efficient routing in a quasi-static multi-path fading environment in the presence of passive eavesdroppers. Since the eavesdroppers are passive, their locations and CSIs are not known to the legitimate nodes. Thus we looked for approaches that do not rely on the locations and quality of the channels of the eavesdroppers. We developed an energy-efficient routing algorithm based on the random jamming to exploit non-idealities of the eavesdropper’s receiver to provide secrecy. Our routing algorithm is fast (finds the optimal path in polynomial time), and does not depend on the number of eavesdroppers and their location and/or channel state information.

We have performed several simulations over single-hop and multi-hop networks with various network parameters, and compared the performance of our proposed algorithm with that of the SMER algorithm of [35], [36]. A major weakness of SMER is that it requires the definition of a guard region that restricts how close eavesdroppers can come to system nodes. Even with such a guard region, which SERJ does not require, we observed that when the uncertainty in the location of the eavesdroppers is high and in disadvantaged wireless environments, the energy consumption of our algorithm is substantially less than that of the SMER algorithm. Gains of SERJ over SMER would be even more substantial in environments with "smart" eavesdroppers; for example, eavesdroppers that located themselves close to

REFERENCES


