Multi-User Diversity for Secrecy in Wireless Networks

UMass Computer Science Technical Report UM-CS-2009-048

Sudarshan Vasudevan, Stephan Adams, Dennis Goeckel, Zhiguo Ding, Donald Towsley, and Kin Leung

***Abstract*—The ability to transmit a message securely in the presence of eavesdroppers in a dense wireless network is considered. As with a number of recent schemes, system nodes other than the transmitter and receiver are chosen to generate noise that confuses the eavesdropper. By exploiting the dynamics of the fading, significantly improved performance is achieved beyond that generated from the standard multi-user diversity gain expected from opportunistic relaying. In particular, the node with the best fading characteristics takes responsibility for message relaying, while those whose fading will significantly reduce their impact on the desired communication play the role of noise generators. For a source transmitting to a destination using a set of intermediate relays, we consider the number of eavesdroppers that can be present without the interception of packets, in both the case where the eavesdroppers operate independently and in the case where they collude. The latter case also encompasses the more likely scenario of a single eavesdropper with a sophisticated multiple-antenna receiver.**

***Index Terms*—Ad hoc networks, cooperation, secrecy, wireless security.**

I. INTRODUCTION

The secure transmission of a message from a sender Alice to a receiver Bob in the presence of an adversary Eve, who may be a passive listener and/or an active jammer, is a major concern in modern networks. At first glance, wireless communication systems appear to make the problem more challenging because the range of locations for which an eavesdropper can gain access to the transmitted signal is increased. But there can be a number of advantages versus the wired scenario, because, unlike the standard cryptographic framework, the signal observed by Bob and Eve is not the same. These advantages include, among others, key generation that exploits the common information in the fading channel characteristics (e.g. [7]), and exploiting independent packet loss of Eve and Bob [8].

We consider an approach that exploits the differences in the channels from a number of relays to the receiver and to the eavesdroppers (without knowledge of the channel to the eavesdroppers) to achieve an advantage for Bob over Eve. Depending on the application, level of security required, and assumptions on the eavesdropper's location or capabilities, this could be used outright for security, but we view it as more likely that it will be used to enhance the physical layer for schemes that are dependent on packet losses at Eve [8].

The idea proposed here fits into the recent set of techniques that employ artificial noise, where system nodes put noise into the air to confuse the eavesdropper. Many of these investigations have considered the secrecy capacity in a single-relay system (see [3] and references therein), where it has been demonstrated that even a relay without knowledge of the message can have utility [4]. Of more pertinent interest are the class of techniques that can be traced back to [2], [6]. In [6], a transmitter with multiple antennas beamforms towards the intended receiver while generating random noise in the nullspace of the receiver so as to confuse the eavesdropper. When the multiple-antenna transmitter is instead replaced by a single-antenna transmitter and a number of single-antenna available relay nodes, a two-stage process that exploits interference cancellation at the receiver allows for artificial noise to impinge on the eavesdropper that can be canceled at the receiver.

There have been numerous related works to [2], [6] in recent years, but, to our knowledge, none of these have exploited the multi-user diversity effect to arrive at a simple, implementable, protocol that: (1) does not require knowledge of the eavesdropper channel, (2) does not require distributed beamforming, and (3) does not require interference cancellation. The protocol, which will be described in detail below in Section II, uses an enhanced form of multi-user diversity. A relay node with "good" links to the source and destination relays the information. In addition, relay nodes with "bad" channels to the relay or destination produce random jamming in the appropriate transmission phase to confuse potential passive eavesdroppers.

The remainder of the paper is organized as follows. Section II presents the system assumptions and protocol.

[0] Sudarshan Vasudevan and Donald Towsley are with the Computer Science Department, University of Massachusetts, Amherst, MA, USA. Stephan Adams and Dennis Goeckel are with the Electrical and Computer Engineering Department, University of Massachusetts, Amherst, MA, USA. Zhiguo Ding is with the Department of Communication Systems, Lancaster University, Lancaster, UK. Kin Leung is with the Electrical and Electronic Engineering and Computing Departments, Imperial College, London, UK.

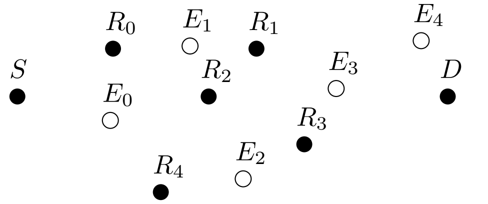

Fig. 1. System scenario: Source node S wishes to communicate securely with destination node D with the assistance of intervening system nodes $R_0, R_1, \cdots, R_{n-1}$ ($n = 5$ in the figure) in the presence of passive eavesdroppers $E_0, E_1, \cdots, E_{m-1}$ of unknown locations ($m = 5$ in the figure).

Section III considers the resulting advantage for Bob over Eve. Conclusions are presented in Section IV.

II. Model and Protocol

A. Model

Consider Figure 1, where a source node S wishes to transmit to a destination node D with the assistance of nodes R_0, R_1, $\ldots R_{n-1}$. Also present in the environment are m passive eavesdroppers[1] $E_0, \cdots, E_{m-1}$. We consider here equal path loss between each pair of nodes, reserving a more accurate path-loss model for the network case being studied in an upcoming work.

The i^{th} transmitted symbol of the source S and a relay R_j will be denoted by $x_i^{(S)}$ and $x_i^{(R_j)}$, respectively, and the i^{th} received symbol for a relay R_j, eavesdropper E_j, and destination D, will be denoted by $y_i^{(R_j)}$, $y_i^{(E_j)}$, and $y_i^{(D)}$, respectively. We assume independent frequency non-selective Rayleigh fading between each of the active transmitters and receivers. Consequently, the multipath fading on a link from a given transmitter A to a given receiver B is a complex zero-mean Gaussian random variable and will be denoted as $h_{A,B}$. Hence, for example, the received signal at R_1 if only the source S were transmitting would be:

$$y_i^{(R_1)} = h_{S,R_1}\sqrt{E_s}x_i^{(S)} + n_i^{(R_1)}$$

where E_s is the transmitted energy per symbol, and $\{n_i^{(R_1)}\}$ is an independent and identically distributed (i.i.d.) sequence of zero-mean (complex) Gaussian random variables with $E[|n_i^{(R_1)}|^2] = N_0$. The Rayleigh fading assumption implies $|h_{A,B}|^2$ is exponentially distributed with $E[|h_{A,B}|^2] = 1$.

B. Protocol

We next describe the protocol used by the source S to establish a secure link with destination D. The protocol consists of the following steps:

1) **Channel measurement between source S and relays:** In Step 1, the source S broadcasts a pilot signal to allow each relay node to measure the channel from source S to itself. Each relay receives:

$$y_i^{(R_j)} = h_{S,R_j}\sqrt{E_s}x_i^{(S)} + n_i^{(R_j)}, j = 0, 1, \ldots, n-1$$

and the eavesdroppers receive

$$y_i^{(E_j)} = h_{S,E_j}\sqrt{E_s}x_i^{(S)} + n_i^{(E_j)}, j = 0, 1, \ldots, m-1$$

Recall that the destination cannot hear the source. We assume that each of the system nodes and eavesdroppers are able to perfectly measure the channel contained in their observation; that is, after Step 1, system node $R_j, j = 0, 1, \ldots, n-1$, now perfectly knows h_{S,R_j}, and the eavesdropper $E_j, j = 0, 1, \ldots, m-1$ perfectly knows h_{S,E_j}.

2) **Channel measurement between destination D and relays:** Analogously to Step 1, the destination D broadcasts a pilot signal and each of the relays $R_j, j = 0, 1, \ldots, n-1$ measure h_{D,R_j}. We assume that each eavesdropper $E_j, j = 0, 1, \ldots, m-1$ perfectly knows h_{D,E_j}.

3) **Relay Selection:** During Step 3, the relay with the largest $\min(|h_{S,R_j}|^2, |h_{D,R_j}|^2)$ announces itself as the messaging relay using a distributed protocol. For instance, each relay picks a backoff window inversely proportional to $\min(|h_{S,R_j}|^2, |h_{D,R_j}|^2)$. Denote the messaging relay's index by j^*. We will assume perfect relay choice i.e. that the relay with the largest $\min(|h_{S,R_j}|^2, |h_{D,R_j}|^2)$ is chosen.

4) **Message Transmission from S to R_{j^*}:** In Step 4, the source S transmits the message to R_{j^*}. Concurrently, intervening system nodes with indices in $\mathcal{R}_1 = \{j \neq j^* : |h_{R_j,R_{j^*}}|^2 < \tau\}$ transmit random noise in order to generate sufficient interference at the eavesdroppers. The messaging relay receives:

$$\begin{aligned} y_i^{(R_{j^*})} &= h_{S,R_{j^*}}\sqrt{E_s}x_i^{(S)} \\ &\quad + \sum_{j\in\mathcal{R}_1} h_{R_j,R_{j^*}}\sqrt{E_s}x_i^{(R_j)} + n_i^{(R_{j^*})} \end{aligned}$$

and eavesdropper $E_j, j = 0, 1, \ldots, m-1$ receives:

$$\begin{aligned} y_i^{(E_j)} &= h_{S,E_j}\sqrt{E_s}x_i^{(S)} \\ &\quad + \sum_{j\in\mathcal{R}_1} h_{R_j,E_j}\sqrt{E_s}x_i^{(R_j)} + n_i^{(E_j)} \end{aligned}$$

5) **Message Transmission from R_{j^*} to destination D:** In a manner similar to Step 4, the messaging

[1] We only consider passive eavesdroppers in this paper. We appreciate the utility of the Diffie-Hellman protocol for key distribution *if* computational security is the goal. If key distribution in computational security is the goal, we note that the protocol is effective in the face of active jammers that will severely inhibit standard Diffie-Hellman approaches.

relay and intervening system nodes in $\mathcal{R}_2 = \{j \neq j^* : |h_{R_j,D}|^2 < \tau\}$ transmit. The signal received by the destination D and the eavesdroppers can be written in a manner similar to Step 4.

C. Limitations and Assumptions

Critical to the protocol, as with many wireless security protocols, is the ability to authenticate messages as coming from true system nodes as opposed to eavesdroppers during the system set-up. In addition, the two extra transmissions required for relay selection could help an adversary to detect a communication in the system. Potentially significant (depending on the choice of τ) power is employed to enable security.

III. Analysis

Motivated by the practical consideration of minimizing the number of packets Eve intercepts while maximizing the number of packets that Bob receives, we consider an outage metric for each. This has direct application, or could be used as an underlying physical layer in a higher-level security scheme that derives its advantage from packet losses at Eve [8].

A source to destination broadcast is in **outage** if and only if either the $S \to R_{j^*}$ link or the $R_{j^*} \to D$ falls below the required signal-to-noise ratio γ for a given rate; that is,

$$\begin{aligned} P_{\text{out}}^{(S \to D)} &= P\left(\left\{\frac{|h_{S,R_{j^*}}|^2 E_s}{\sum_{j \in \mathcal{R}_1} |h_{R_j,R_{j^*}}|^2 E_s + N_0} < \gamma\right\}\right. \\ &\bigcup \left.\left\{\frac{|h_{R_{j^*},D}|^2 E_s}{\sum_{j \in \mathcal{R}_2} |h_{R_j,D}|^2 E_s + N_0} < \gamma\right\}\right) \end{aligned} \quad (1)$$

A. Non-Collaborating Eavesdroppers

In contrast to the destination, we will assume the pessimistic case that each eavesdropper can hear both the source and relay transmission with equal average strength. Hence, each eavesdropper E_j sees effectively two independent looks at the source message. Let C_{S,E_j} denote the signal to noise and interference ratio (SINR) from source S to eavesdropper E_j. Therefore,

$$\begin{aligned} C_{S,E_j} &= \frac{|h_{S,E}|^2 E_s}{\sum_{j \in \mathcal{R}_1} |h_{R_j,E}|^2 E_s + N_0} \\ &+ \frac{|h_{R_{j^*},E}|^2 E_s}{\sum_{j \in \mathcal{R}_2} |h_{R_j,E}|^2 E_s + N_0} \end{aligned}$$

and

$$P_{\text{out}}^{(S \to E_j)} = P(C_{S,E_j} \leq \gamma) \quad (2)$$

We consider the analysis given an asymptotically large number of relays n. This is motivated by the connectivity condition for large wireless networks, where each node must have, on average, an infinite number of neighbors for the network to be connected with high probability.

For any fixed threshold γ, multi-user diversity in the form of single or multiple relay selection without artificial noise is sufficient for $P_{\text{out}}^{(S \to D)} \to 0$ as $n \to \infty$; however, the eavesdropper outage is invariant to n and non-zero. This could be remedied by letting γ go to infinity as $n \to \infty$. For example, with $\gamma = \log \log n$, $P_{\text{out}}^{(S \to D)} \to 0$ and $P_{\text{out}}^{(S \to E_j)} \to 1, 1 \leq j \leq m$ as $n \to \infty$, but this would require infinite rate on each link. Artificial noise generation offers an alternate route that can be employed for fixed γ (or rate), $\gamma > 1$, and can suppress a large number of eavesdroppers, as demonstrated here.

Let $P_{\text{out}}^{S,\mathbf{E}}$ denote probability of the event $\mathcal{E} = (C_{S,E_0} < \gamma \wedge \cdots \wedge C_{S,E_m} < \gamma)$ i.e. the probability that none of the eavesdropper nodes exceeds the required signal-to-noise-plus-interference ratio γ.

Theorem 3.1: Consider the scenario of Figure 1 with the protocol of Section II-B with n available system nodes, and $m(n)$ eavesdroppers. Let $\tau(n)$ denote the threshold used to determine the noise-generating nodes in the protocol of Section II-B. If

$$m(n) = \mathrm{o}\left(\left(\min\left\{\frac{\gamma}{e^{1-1/\gamma}}, e\right\}\right)^{\frac{n\tau(n)}{4}}\right)$$

and $\tau(n) \leq \sqrt{\frac{E_s \ln n - 2N_o\gamma}{4n\gamma}}$ and $n\tau(n) \to \infty$, as $n \to \infty$, then $P_{\text{out}}^{(S \to D)} \to 0$ and $P_{\text{out}}^{(\mathbf{E})} \to 1$.

Conversely, if $m(n) > e^{2c\gamma n\tau(n) + \frac{\gamma N_o}{E_s}}$, for some constant $c > 1$, we show that $P_{\text{out}}^{(S,\mathbf{E})} \to 0$.

Proof: First, we upper bound $P_{\text{out}}^{(S \to D)}$, as given in (1), by:

$$\begin{aligned} &\leq P\left(\left\{\frac{\min\{|h_{S,R_{j^*}}|^2, |h_{R_{j^*},D}|^2\} E_s}{\sum_{j \in \mathcal{R}_1} |h_{R_j,R_{j^*}}|^2 E_s + N_0} < \gamma\right\}\right. \\ &\quad \bigcup \left.\left\{\frac{\min\{|h_{S,R_{j^*}}|^2, |h_{R_{j^*},D}|^2\} E_s}{\sum_{j \in \mathcal{R}_2} |h_{R_j,D}|^2 E_s + N_0} < \gamma\right\}\right) \\ &= 1 - P\left(\left\{\frac{\min\{|h_{S,R_{j^*}}|^2, |h_{R_{j^*},D}|^2\} E_s}{\sum_{j \in \mathcal{R}_1} |h_{R_j,R_{j^*}}|^2 E_s + N_0} > \gamma\right\}\right. \\ &\quad \bigcap \left.\left\{\frac{\min\{|h_{S,R_{j^*}}|^2, |h_{R_{j^*},D}|^2\} E_s}{\sum_{j \in \mathcal{R}_2} |h_{R_j,D}|^2 E_s + N_0} > \gamma\right\}\right) \\ &= 1 - E_X\left[\left(P\left(\frac{X E_s}{\sum_{j \in \mathcal{R}_1} |h_{R_j,R_{j^*}}|^2 E_s + N_0} > \gamma\right)\right)^2\right] \end{aligned} \quad (3)$$

where $X = \min\{|h_{S,R_{j^*}}|^2, |h_{R_{j^*},D}|^2\}$. Now, with R_{j^*} as the relay with index j that maximizes $\min\{|h_{S,R_j}|^2, |h_{R_j,D}|^2\}$, basic probability establishes that $X = \max(X_0, X_1, \ldots, X_{N-1})$, where $X_j = \min\{|h_{S,R_j}|^2, |h_{R_j,D}|^2\}$, is the maximum of N iid random variables, each of which is exponential with mean $\frac{1}{2}$. Next, consider the following result from extreme value theory [1][pp.176-177].

Lemma 3.2: Let $Y_1, \cdots, Y_n$ be a sequence of n iid exponential random variables, each having an exponential tail $\bar{F}(y) \sim Ke^{-ay}$ where $K, a > 0$. Let $M_n = \max(Y_1, \cdots, Y_n)$. Then, $\lim_{n \to \infty} \frac{M_n}{\ln n} = \frac{1}{a}$ a.s..

From Lemma 3.2, the random variable $X = \max(X_1, \cdots, X_n)$ converges almost surely to $\ln n/2$.

In driving the $P_{\text{out}}^{S \to D}$ to 0, the choice of the threshold $\tau(n)$ is critical. For a relay node R_j, the noise-generating probability is $P(|h_{R_j,R_j^*}|^2 < \tau(n)) = 1 - e^{-\tau(n)} \simeq \tau(n)$, for small values of $\tau(n)$. Thus, the number $|\mathcal{R}_1|$ of noise generating nodes is a binomial random variable with mean $n\tau(n)$. We can now use Chernoff bounds [5][pp.67-70] to obtain bounds on the probability that $|\mathcal{R}_1|$ deviates from its expectation. In particular,

$$P(|\mathcal{R}_1| > 2n\tau(n)) < (e/4)^{n\tau(n)}$$

and

$$P(|\mathcal{R}_1| < \frac{n\tau(n)}{2}) < e^{-\frac{n\tau(n)}{8}}$$

Since $n\tau(n) \to \infty$ as $n \to \infty$, we conclude that $(n/2)\tau(n) \leq |\mathcal{R}_1| \leq 2n\tau(n)$ w.h.p. From the conditions on $|\mathcal{R}_1|$ and $\tau(n)$, we get

$$N_o + \sum_{j \in \mathcal{R}_1} |h_{R_j,R_j^*}|^2 E_s \leq N_o + 2n\tau^2(n) \leq \frac{E_s \ln n}{2\gamma}$$

w.h.p. In other words,

$$P\left(\frac{XE_s}{N_o + \sum_{j \in \mathcal{R}_1} |h_{R_j,R_j^*}|^2 E_s} > \gamma\right) \geq 1 - (e/4)^{n\tau(n)}$$

Substituting into (3) yields

$$P_{\text{out}}^{S \to D} \leq 1 - (1 - (e/4)^{n\tau(n)})^2 \simeq 1 - e^{-2(e/4)^{n\tau(n)}}$$

It can be readily seen that $P_{\text{out}}^{S \to D} \to 0$ as $n \to \infty$.

We next show that $P_{\text{out}}^{(S,\mathbf{E})} \to 1$. First, consider $P_{\text{out}}^{(S \to E_j)}$ for a given j. From Lemma 3.2, the maximum of the fading coefficients from the eavesdroppers to the source converges to $\ln m(n)$ a.s. From (2), the received SINR at eavesdropper E_j is upper bounded by:

$$C_{S,E_j} \leq \frac{\ln m(n) E_s}{N_o + \sum_{k \in \mathcal{R}_1} |h_{R_k,E_j}|^2 E_s} + \frac{\ln m(n) E_s}{N_o + \sum_{k \in \mathcal{R}_2} |h_{R_k,E_j}|^2 E_s} \quad \text{a.s.} \tag{4}$$

We have shown $|\mathcal{R}_1| \geq n\tau(n)/2$ w.h.p.; similarly, $|\mathcal{R}_2| \geq n\tau(n)/2$. Hence, we can therefore replace the sum in the denominator of (4) with an $n\tau(n)/2$-stage Erlang random variable yielding:

$$C_{S,E_j} \leq \frac{2E_s \ln m(n)}{N_o + E_s \sum_{k=1}^{n\tau(n)/2} |h_{R_k,E_j}|^2} \quad \text{w.h.p}$$

Conditioned on $|\mathcal{R}_1|, |\mathcal{R}_2| \geq n\tau(n)/2$ and from the conditions for $m(n)$, we obtain

$$C_{S,E_j} \leq \frac{E_s n\tau(n)/2}{N_o + \sum_{k=1}^{n\tau(n)/2} |h_{R_k,E_j}|^2 E_s} \quad \text{w.h.p}$$

Therefore,

$$C_{S,E_j} \leq \frac{E_s n\tau(n)/2 + \gamma N_o}{N_o + \sum_{k=1}^{n\tau(n)/2} |h_{R_k,E_j}|^2 E_s} \quad \text{w.h.p} \tag{5}$$

We next show that the sum $\sum_{k=1}^{n\tau(n)/2} |h_{R_k,E_j}|^2 E_s > \frac{E_s n\tau(n)}{2\gamma}$ w.h.p. Using Chernoff bounds for an n-stage Erlang random variable with mean $E[X] = n$ derived in Appendix V, we can conclude that:

$$P\left(\sum_{k=1}^{n\tau(n)/2} |h_{R_k,E_j}|^2 < \frac{n\tau(n)}{2\gamma}\right) < \left(\frac{e^{1-1/\gamma}}{\gamma}\right)^{\frac{n\tau(n)}{2}}$$

It can be verified that $\frac{e^{1-1/\gamma}}{\gamma} < 1, \forall \gamma > 1$. For $\gamma > 1$, the right hand side of the above inequality goes to 0, as $n \to \infty$. Therefore,

$$P\left[C_{S,E_j} \leq \gamma \mid |\mathcal{R}_1|, |\mathcal{R}_2| \geq n\tau(n)/2\right] \geq 1 - \left(\frac{e^{1-1/\gamma}}{\gamma}\right)^{\frac{n\tau(n)}{2}}$$

By symmetry, $P\left[C_{S,E_j} < \gamma \mid |\mathcal{R}_1|, |\mathcal{R}_2| \geq n\tau(n)/2\right]$ is the same for all eavesdropper nodes. Using the *union bound*, we get:

$$P\left[\mathcal{E} \mid |\mathcal{R}_1|, \mathcal{R}_2| \geq n\tau(n)/2\right] \geq 1 - m(n)\left(\frac{e^{1-1/\gamma}}{\gamma}\right)^{n\tau(n)/2}$$

Removing the conditioning and observing that $|\mathcal{R}_1|$ and $|\mathcal{R}_2|$ are independent random variables,

$$P_{\text{out}}^{S \to \mathbf{E}} \geq \left(1 - m(n)\left(\frac{e^{1-1/\gamma}}{\gamma}\right)^{\frac{n\tau(n)}{2}}\right)\left(1 - e^{-\frac{n\tau(n)}{8}}\right)^2$$

The conditions on $m(n)$ guarantee that the right hand side in the above inequality approaches 1 in the limit as $n \to \infty$.

The proof of the second part (converse) of Theorem 3.1 is straightforward. Let E_j^*, denote the eavesdropper with the maximum fading coefficient to the source S. When $m(n) = \exp\left\{2c\gamma n\tau(n) + \frac{\gamma N_o}{E_s}\right\}, c > 1$, apply Lemma 3.2 to get $|h_{S,E_j^*}|^2 \to 2c\gamma n\tau(n) + \frac{\gamma N_o}{E_s}$ a.s.

Further, we know that $|\mathcal{R}_1| \leq 2n\tau(n)$. Applying Chernoff bounds, we obtain

$$P\left(\sum_{j \in \mathcal{R}_1} |h_{R_j,E_j^*}|^2 > 2cn\tau(n)\right) < \left(\frac{c}{e^{c-1}}\right)^{2n\tau(n)}$$

Therefore,

$$P(C_{S,E_j^*} > \gamma) \geq 1 - \left(\frac{c}{e^{c-1}}\right)^{2n\tau(n)}$$

Since $c < e^{c-1}$ for $c > 1$, it follows that

$$P(\sum_{j\in\mathcal{R}_1} |h_{R_j,E_j^*}|^2 > 2cn\tau(n)) \to 0, \text{as } n \to \infty$$

In other words, $P(C_{S,E_j^*} > \gamma) \to 1, \text{as } n \to \infty$. Therefore, $P_{\text{out}}^{S\to\mathbf{E}} \to 0, \text{as } n \to \infty$ ■

B. Collaborating Eavesdroppers

In this section, we consider the case where the eavesdroppers can collaborate. Importantly, this also models the case where a single eavesdropper with m antennas is present in the environment.

Theorem 3.3: : If $m(n) = \text{o}(n\tau(n))$, $\tau(n) \leq \sqrt{\frac{E_s \ln n - 2N_o\gamma}{4n\gamma}}$, and $n\tau(n) \to \infty$ as $n \to \infty$, then $P_{\text{out}}^{(S\to\mathbf{E})} \to 1$ and $P_{\text{out}}^{(S\to D)} \to 0$.

Proof: From Theorem 3.1, it follows that $P_{\text{out}}^{(S\to D)} \to 0$. Next, consider showing $P_{\text{out}}^{(S\to\mathbf{E})} \to 1$. The total signal-to-noise ratio ($C_{S,\mathbf{E}}$):

$$\begin{aligned} C_{S,\mathbf{E}} \quad = \quad & \sum_{i=1}^{m(n)} \left(\frac{E_s|h_{S,E_i}|^2}{E_s \sum_{j\in\mathcal{R}_1}(|h_{R_j,E_i}|^2) + N_0} \right. \\ & \left. + \frac{E_s|h_{R^*,E_i}|^2}{E_s \sum_{j\in\mathcal{R}_2}(|h_{R_j,E_i}|^2) + N_0} \right) \end{aligned}$$

Using Chernoff bounds as in the independent eavesdropper case, $|\mathcal{R}_1|$,$|\mathcal{R}_2|$ can be lower bounded by $\frac{n\tau(n)}{2}$ w.h.p.; hence, the combined signal-to-noise ratio of the eavesdroppers can be upperbounded w.h.p.:

$$\begin{aligned} C_{S,\mathbf{E}} \quad \leq \quad & \sum_{i=1}^{m(n)} \left(\frac{|h_{S,E_i}|^2}{\sum_{j=1}^{n\tau(n)/2} h_{|R_j,E_i}|^2} \right) \\ + \quad & \sum_{i=1}^{m(n)} \left(\frac{|h_{R^*,E_i}|^2}{\sum_{j=1}^{n\tau(n)/2} |h_{R_j,E_i}|^2} \right) \end{aligned}$$

From Markov's Inequality and straightforward probability:

$$\begin{aligned} 1 - P_{\text{out}}^{(S\to\mathbf{E})} \quad & \leq \quad \frac{E[C_{S,\mathbf{E}}]}{\gamma} \\ & \leq \quad \frac{2mn\tau(n)}{\gamma\left(\frac{n\tau(n)}{2} - 2\right)\left(\frac{n\tau(n)}{2} - 1\right)} \end{aligned}$$

which goes to zero provided that $\frac{m(n)}{n\tau(n)} \to 0$ as $n \to \infty$. This implies $P_{\text{out}}^{(S\to\mathbf{E})} \to 1$. ■

C. Discussion

First, consider choice of the threshold $\tau(n)$. A large value of $\tau(n)$ results in more noise-generating nodes and drives more eavesdroppers into outage. However, this also increases the probability the source to destination link is in outage. Thus, pick the largest $\tau(n)$ which allows both R_{j^*} and D to decode the message w.h.p. From Section III-A, we know that $|h_{S,R_{j^*}}|^2$ and $|h_{R_{j^*}}, D|^2$ each converge to $\ln n/2$ a.s. A simple calculation based on the SINR requirements for the $S \to R_{j^*}$ and $R_{j^*} \to D$ links yields:

$$\tau^*(n) = \sqrt{\frac{E_s \ln n - 2N_o\gamma}{4n\gamma}}$$

Based on the conditions for $m(n)$ in Theorems 3.1 and 3.3, we observe that:

$$m(n) = \text{o}\left(\left(\min\left\{ \frac{\gamma}{e^{1-1/\gamma}}, e \right\} \right)^{\sqrt{\frac{E_s n \ln n - 2nN_o\gamma}{16\gamma}}} \right)$$

for the non-collaborating eavesdroppers case, and

$$m(n) = \text{o}\left(\sqrt{\frac{E_s n \ln n - 2nN_o\gamma}{16\gamma}} \right)$$

for the case of collaborating eavesdroppers.

In other words, for a given $\tau(n)$, we can allow exponentially more non-collaborating eavesdroppers as compared to collaborating eavesdroppers. Further, when eavesdroppers do not collaborate, the number of allowable eavesdroppers grows exponentially in the square root of the number of system nodes.

IV. CONCLUSIONS

A simple and easily implemented protocol for secret communication between a source and destination using a messaging relay and artificial noise transmitted from a set of intervening system nodes has been presented. The system exploits a multi-user effect in selecting both the messaging relay and the nodes for noise generation. The proposed protocol can provide for a significant advantage for the desired receiver over the eavesdropper that can then be exploited by higher layer protocols to enforce security on the link.

Extension of the analysis in the paper to the network case is currently under investigation. Incorporating a more relaxed outage metric which allows a non-zero outage probability for the source while guaranteeing outage for the eavesdroppers is also being studied.

REFERENCES

[1] P. Embrechts, C. Kluppelberg, and T. Mikosch. *Modelling extremal events for insurance and finance*. Springer-Verlag, 1997.

[2] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, 2008.

[3] X. He and A. Yener. Two-hop secure communication using an untrusted relay: a case for cooperative jamming. In *IEEE GLOBECOM*, 2008.

[4] L. Lai and H. E. Gamal. Cooperative secrecy: the relay-eavesdropper channel. In *IEEE International Symposium on Information Theory*, pages 931–935, 2007.

[5] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[6] R. Negi and S. Goel. Secret communication using artificial noise. In *IEEE Vehicular Technology Conference*, 2005.

[7] R. Wilson, D. Tse, and R. Scholtz. Channel identification: secret sharing and reciprocity in ultrawideband channels. *IEEE Transactions on Information Forensics and Security*, 2(3):364–375, 2007.

[8] S. Xiao, H. Pishro-Nik, and W. Gong. Dense parity check based secrecy sharing in wireless communications. In *IEEE GLOBECOM*, 2007.

V. Chernoff Bounds for Erlang Random Variable

We derive a probability bound on the lower tail of an n-stage Erlang random variable X. Using Chernoff bounds for a non-negative random variable,

$$P(X < a) \leq \inf_{t<0} e^{-ta} M_X(t) \tag{6}$$

where $M_X(t) = E[e^{tX}]$ denotes the moment generating function of the random variable X. For an n-stage Erlang random variable X with rate λ:

$$M_X(t) = \left(\frac{\lambda}{\lambda - t}\right)^n$$

Using elementary calculus, the value of t that minimizes the right hand side of (6) can be obtained as:

$$t^* = \lambda - \frac{n}{a}$$

Therefore,

$$P(X < a) \leq e^{-(a\lambda - n)} \left(\frac{a\lambda}{n}\right)^n$$

Setting $a = E[X]/\gamma = n/\gamma\lambda$, where $\gamma > 1$, yields:

$$P(X < \frac{E[X]}{\gamma}) \leq \left(\frac{e^{1-\frac{1}{\gamma}}}{\gamma}\right)^n$$

Since $\frac{e^{1-\frac{1}{\gamma}}}{\gamma} < 1 \quad \forall \gamma > 1$, the right hand side in the above inequality goes to 0 as $n \to \infty$.

The probability bound for the upper tail can be derived similarly. In particular, for a non-negative random variable X and $a > 0$, we have

$$P(X > a) \leq \inf_{t>0} e^{-ta} M_X(t) \tag{7}$$

Proceeding exactly in the same manner as before, it can be easily shown that

$$P(X > \gamma E[X]) \leq \left(\frac{\gamma}{e^{\gamma - 1}}\right)^n$$

For $\gamma > 1$, the right hand side goes to 0 as $n \to \infty$.