SECRECY ANALYSIS OF UNAUTHENTICATED AMPLIFY-AND-FORWARD RELAYING WITH ANTENNA SELECTION

Jing Huang, Amitav Mukherjee, and A. Lee Swindlehurst

Dept. of Electrical Engineering and Computer Science
University of California, Irvine
Irvine, CA 92697
{jing.huang,amukherj,swindle}@uci.edu

ABSTRACT

We investigate the secrecy outage performance for a cooperative unauthenticated relay network where antenna selection is employed at the multi-antenna relay. Both traditional amplify-and-forward (AF) relaying and a cooperative jamming (CJ) protocol are studied. We characterize the exact secrecy outage probability (SOP) for the AF scheme, and analyze the asymptotic behaviour in terms of SOP for the CJ scheme. Although both the unauthenticated relay and the destination perceive diversity gain from antenna selection, we show that as the number of antennas grows, the SOP approaches one for AF, while it approaches zero for CJ. For a fixed number of antennas, we demonstrate that the CJ scheme is better than AF relaying for high SNR, and its SOP approaches zero when the SNR goes to infinity. The theoretical analysis is also validated via several numerical examples.

Index Terms— Wiretap channel, wireless security, amplify-and-forward, cooperative jamming, antenna selection.

1. INTRODUCTION

Security is an important issue for both single-hop links and relay networks [1,2], in which secure transmissions may be compromised by external eavesdroppers that are distinct from the source and the relay nodes. However, even if external eavesdroppers are absent, it may still be desirable to keep the source signal confidential from the relay node itself in spite of its assistance in forwarding the data to the destination [3]. For example, the unauthenticated relay may belong to a heterogeneous network without the same security clearance as the source and destination. This scenario has also been denoted as cooperative communication via an untrusted relay in [4], where the authors presented bounds on the achievable secrecy rate.

When multiple antennas are employed in relay networks, any potential performance benefits must be balanced against increased hardware complexity and power consumption. As a reduced-complexity solution that can maintain full diversity, antenna selection has received extensive attention in amplify-and-forward (AF) relay networks, especially for cases where only one RF chain is available at the relay. In [5], a low-complexity near-optimal antenna selection algorithm was proposed for maximizing the achievable rate. The bit error rate performance obtained by choosing the best antenna pairs over both relay hops was examined in [6]. However, the open problem addressed in our paper is the tradeoff between the diversity gain for the legitimate receiver versus the inadvertent diversity gain of the information leaked to an unauthenticated relay in the first hop.

This paper analyzes a three-node network where a single-antenna source can potentially utilize an unauthenticated multi-antenna relay with antenna selection to augment the direct link to its destination. We use the secrecy outage probability [7, 8] (SOP) as the performance metric, which describes the probability of simultaneously reliable and secure data transmission. Both conventional AF relaying and cooperative jamming (CJ) [2, 9, 10] schemes are investigated for the unauthenticated relay channel. We prove the interesting result that the SOP of AF increases with the number of antennas deployed at the relay and ultimately converges to unity as the number of relay antennas approaches infinity, while the SOP of CJ behaves in the opposite way. We also show that in the high SNR regime, it is in fact better to ignore the direct link in the first hop and perform CJ, since the outage probability of CJ is arbitrarily small when the transmit power approaches infinity, while the outage probability of AF converges to a non-zero constant.

2. MATHEMATICAL MODEL

We consider a half-duplex two-hop relaying system composed of a source (Alice), a destination (Bob), and an unauthenticated relay that employs the AF protocol. Alice and Bob are both single-antenna nodes, and the relay is assumed to be equipped with K antennas. This model is similar to that in [9], except the external eavesdropper in this paper is also the relay. The channel is assumed to be quasi-static (constant during the two hops) with Rayleigh fading. We also assume all nodes in the network have the same power budget P. A single antenna at the relay is selected for reception and transmission during each relaying phase [11], and a direct link between Alice and Bob is assumed to be available.

2.1. Relay Protocol

We now provide the signal model for the AF relaying channel. During the first phase, the relay receives

$$y_R = \alpha_{Am} x_A + n_m \tag{1}$$

where $m \in \{1, 2, \ldots, K\}$ represents the selected receive antenna on the relay, x_A is the zero-mean signal transmitted by Alice with variance $\mathbb{E}\{x_A^H x_A\} \leq P$, $\alpha_{ij} \sim \mathcal{CN}(0, \bar{\gamma}_{ij})$ is the complex circularly symmetric Gaussian channel coefficient between node i and j, with $i, j \in \{A, B, m\}$ denoting which of the terminals or antennas is involved, and $n_i \sim \mathcal{CN}(0, N_0)$ is additive white Gaussian noise.

This work was supported by the U.S. Army Research Office under the Multi-University Research Initiative (MURI) grant W911NF-07-1-0318, and by the National Sciene Foundation under grant CCF-1117983.

For simplicity, we assume that the noise at all nodes is Gaussian with power N_0. Let $\gamma_{ij} \triangleq |\alpha_{ij}|^2$ be the instantaneous squared channel strength, so that γ_{ij} is exponentially distributed with hazard rate $\frac{1}{\bar{\gamma}_{ij}}$, and the probability density function (p.d.f.) is given by

$$p_{\gamma_{ij}}(x) = \frac{1}{\bar{\gamma}_{ij}} \exp\left(-\frac{x}{\bar{\gamma}_{ij}}\right), \quad x \geq 0. \tag{2}$$

During the second phase, the relay normalizes its received signal y_R and selects an antenna $n \in \{1, 2, \ldots, K\}$ to transmit a scaled version $x_R = \frac{\sqrt{P}}{\sigma} y_R$ where $\sigma = \sqrt{\mathbb{E}\{|y_R|^2\}}$. The received signal at Bob over both phases is

$$\mathbf{y}_B = \begin{bmatrix} \alpha_{AB} \\ \frac{\sqrt{P}}{\sigma}\alpha_{nB}\alpha_{Am} \end{bmatrix} x_A + \begin{bmatrix} n_{B1} \\ \frac{\sqrt{P}}{\sigma}\alpha_{nB} n_m + n_{B2} \end{bmatrix}. \tag{3}$$

The subscripts 1 and 2 refer to the first and second transmission phases, respectively. Since the antennas on the relay are much closer together compared to their distances to the source and the destination, we assume $\{\bar{\gamma}_{Am}\}_{m=1}^{K} = \bar{\gamma}_{AR}$ and $\{\bar{\gamma}_{nB}\}_{n=1}^{K} = \bar{\gamma}_{RB}$.

2.2. Cooperative Jamming

For the cooperative jamming scheme, we use a model similar to [8], where Bob ignores the direct link and transmits jamming signals during the first phase. Thus the received signal at the relay is

$$y_R = \alpha_{Am} x_A + \alpha_{mB} z_B + n_R$$

where z_B is a noise-like signal transmitted by Bob to jam the relay and degrade its eavesdropping capability. We assume a reciprocal channel between the relay and Bob, so that $\alpha_{mB} = \alpha_{Bm}$.

Similar to the AF scheme, during the second phase the relay scales y_R and forwards it to Bob, and thus the received signal at Bob can be written as

$$\mathbf{y}_B = \frac{\sqrt{P}}{\sigma}\alpha_{nB}\alpha_{Am} x_A + \frac{\sqrt{P}}{\sigma}\alpha_{nB}\alpha_{mB} z_B + \frac{\sqrt{P}}{\sigma}\alpha_{nB} n_m + n_{B2}$$

where the intentional interference term can be removed by Bob since z_B is known to him.

3. SECRECY OUTAGE ANALYSIS

In this section, we characterize the secrecy outage probability for AF and CJ. We consider an antenna selection scheme in which the unauthenticated relay chooses the receive antenna with the largest channel gain for maximizing her wiretapping ability in the first hop, while still assisting Alice by using the best transmit antenna to forward the message to Bob in the second hop, *i.e.*, the relay is unauthenticated but not malicious. In other words, we consider the same selection scheme as the traditional one that chooses the best antenna pair in the first and second hop respectively [11].

3.1. Amplify-and-Forward (AF)

When the unauthenticated AF relay is employed for cooperation, the channel is equivalent to the conventional wiretap channel where Bob receives the signal from two orthogonal channels [4], and thus the achievable secrecy rate can be computed from $R_s^{AF} = \left[I_B^{AF} - I_R^{AF}\right]^+$, where $[x]^+ \triangleq \max\{0, x\}$, I_B^{AF} and I_R^{AF} represent the mutual information between Alice and Bob and between Alice and the relay, respectively, and are given by

$$I_B^{AF} = \frac{1}{2}\log_2\left(1 + \rho\gamma_{AB} + \rho\frac{\gamma_{n^*B}\gamma_{Am^*}}{\gamma_{n^*B} + \bar{\gamma}_{AR} + \frac{1}{\rho}}\right) \tag{4}$$

$$I_R^{AF} = \frac{1}{2}\log_2\left(1 + \rho\gamma_{Am^*}\right), \tag{5}$$

where $\rho \triangleq \frac{P}{N_0}$ is the transmit SNR, and the receive and transmit antennas on the relay are selected using the following criteria:

$$m^* = \arg\max_m \{\gamma_{Am}\} \tag{6}$$

$$n^* = \arg\max_n \{\gamma_{nB}\}. \tag{7}$$

The SOP of the AF scheme for a given secrecy rate R is defined as

$$\mathcal{P}_{out}^{AF}(R) = \mathcal{P}\left\{\frac{1}{2}\log_2\left(\frac{1 + \rho\gamma_{AB} + \rho\frac{\gamma_{n^*B}\gamma_{Am^*}}{\gamma_{n^*B} + \bar{\gamma}_{AR} + \frac{1}{\rho}}}{1 + \rho\gamma_{Am^*}}\right) < R\right\}, \tag{8}$$

and an expression for the exact SOP is given by the following proposition.

Proposition 1. *The secrecy outage probability for AF relaying with antenna selection can be expressed as*

$$\begin{aligned}\mathcal{P}_{out}^{AF}(R) = 1 - K^2 \sum_{m=1}^{K}\sum_{n=1}^{K}\binom{K-1}{m}\binom{K-1}{n}(-1)^{m+n} \\ \times \frac{\bar{\gamma}_{AB}}{(2^{2R}-1)\bar{\gamma}_{AR} + \bar{\gamma}_{AB}(n+1)} \exp\left(-\frac{2^{2R}-1}{\rho\bar{\gamma}_{AB}}\right) \\ \times \left[\mu(\beta_n - 1)\exp(\mu\beta_n(m+1))\mathrm{Ei}(-\mu\beta_n(m+1)) + \frac{1}{\mu(m+1)}\right]\end{aligned} \tag{9}$$

where $\mu = \frac{\bar{\gamma}_{AR}+1/\rho}{\bar{\gamma}_{RB}}$, $\beta_n = \frac{2^{2R}\bar{\gamma}_{AR}+\bar{\gamma}_{AB}(n+1)}{(2^{2R}-1)\bar{\gamma}_{AR}+\bar{\gamma}_{AB}(n+1)}$, *$R$ is the target secrecy rate, and* $\mathrm{Ei}(\cdot)$ *is the exponential integral* $\mathrm{Ei}(x) = \int_{-\infty}^{x} e^t t^{-1}\, dt$.

Proof. Assume $X = \gamma_{AB}$, $Y = \gamma_{Am}$, and $V = \frac{\gamma_{nB}}{\gamma_{nB}+\bar{\gamma}_{AR}+1/\rho}$. Correspondingly, $Y^* = \gamma_{Am^*}$ and $V^* = \frac{\gamma_{n^*B}}{\gamma_{n^*B}+\bar{\gamma}_{AR}+1/\rho}$. Since Y is exponentially distributed as in (2), using the theory of order statistics [12], we have

$$p_{Y^*}(y) = \frac{K}{\bar{\gamma}_{AR}}\sum_{n=0}^{K-1}(-1)^n \exp\left[-\frac{y}{\bar{\gamma}_{AR}}(n+1)\right]. \tag{10}$$

For V, using the Jacobian transformation, we have

$$p_V(v) = \frac{\bar{\gamma}_{AR} + 1/\rho}{\bar{\gamma}_{RB}(1-v)^2}\exp\left[-\frac{(\bar{\gamma}_{AR}+1/\rho)v}{\bar{\gamma}_{RB}(1-v)}\right],$$

and the corresponding p.d.f. of V^* can be expressed using order statistics as

$$p_{V^*}(v) = \frac{K\mu}{(1-v)^2}\sum_{m=0}^{K-1}(-1)^m \exp\left[-\frac{\mu v}{1-v}(m+1)\right], \tag{11}$$

where $\mu = \frac{\bar{\gamma}_{AR}+1/\rho}{\bar{\gamma}_{RB}}$. The proof of (9) is completed by inserting (10) and (11) into

$$P_{out}^{AF}(R) = \mathcal{P}\left\{Z < 2^{2R}\right\} = \mathbb{E}_{V^*}\{\mathbb{E}_{Y^*}\{F_{Z|Y^*,V^*}(2^{2R})\}\}$$

where $Z = \frac{1+\rho X+\rho V^* Y^*}{1+\rho Y^*}$. □

Corollary 1. *When AF relaying is used, the secrecy outage probability converges to a non-zero constant at high SNR.*

This corollary can be directly inferred from (8). In the high SNR regime, (8) can be approximated as

$$\mathcal{P}_{out}^{AF}(R) \simeq \mathcal{P}\left(\frac{\gamma_{AB} + \frac{\gamma_{RB}\gamma_{AR}}{\gamma_{RB}+\bar{\gamma}_{AR}}}{\gamma_{AR}} < 2^{2R}\right), \tag{12}$$

which is a function independent of ρ. More specifically, as seen from (9), only μ is a function of ρ, and $\mu \to \mu' = \frac{\bar{\gamma}_{AR}}{\bar{\gamma}_{RB}}$ as $\rho \to \infty$. Therefore, the asymptotic result can be obtained by replacing μ with μ' in (9). This result indicates that the AF scheme does not approach zero SOP even as the transmit power is increased. Intuitively, this is reasonable since any increase in the transmit power will bolster the SNR at both the legitimate user and the eavesdropper.

Corollary 2. *The secrecy outage probability of AF relaying approaches unity as the number of relay antennas grows: $\mathcal{P}_{out}^{AF} \to 1$ as $K \to \infty$.*

Proof. This corollary can be proved by showing that a lower bound for $\mathcal{P}_{out}^{AF}$ goes to 1 as $K \to \infty$. Following the notation in the proof of Proposition 1, we have

$$\begin{aligned}
\mathcal{P}_{out}^{AF}(R) &= \mathcal{P}\left(\frac{1+\rho X+\rho V^* Y^*}{1+\rho Y^*} < 2^{2R}\right) \\
&\overset{a}{\geq} \mathcal{P}\left(\frac{1+\rho X+\rho Y^*}{1+\rho Y^*} < 2^{2R}\right) \qquad (13) \\
&\overset{b}{\geq} \mathcal{P}\left(\frac{X}{Y^*} < 2^{2R}-1\right) \\
&= \mathcal{P}\left(\min_m\left\{\frac{\gamma_{AB}}{\gamma_{Am}}\right\} < 2^{2R}-1\right) \\
&\overset{c}{=} 1 - \left[1 - \frac{\bar{\gamma}_{AR}(2^{2R}-1)}{\bar{\gamma}_{AB}+\bar{\gamma}_{AR}(2^{2R}-1)}\right]^K, \qquad (14)
\end{aligned}$$

where it is obvious that (14) converges to 1 as K goes to ∞. Note that inequality (a) holds since $V^* \leq 1$. Since the fraction in (13) is a quasi-linear function of ρ, and is monotonically increasing with respect to ρ since $X+Y^* \geq Y^*$, inequality (b) is obtained by letting $\rho \to \infty$. To obtain (14), we have used the result

$$F_{\gamma_{AB}/\gamma_{Am}}(u) = \frac{\bar{\gamma}_{AR}u}{\bar{\gamma}_{AB}+\bar{\gamma}_{AR}u}. \qquad \square$$

Corollary 2 shows that although both the relay and the destination receive diversity gain from increasing the number of relay antennas, the unauthenticated relay accrues a proportionally greater benefit to the detriment of the information confidentiality.

3.2. Cooperative Jamming (CJ)

In this scheme, according to the signal model in Section 2.2, Bob will transmit jamming signals during the first phase and remove its own artificial interference from the received signals in the second phase. We thus have the following expressions for the mutual information at Bob and the relay for the cooperative jamming scenario:

$$I_B^{CJ} = \frac{1}{2}\log_2\left(1+\rho\frac{\gamma_{n^*B}\gamma_{Am^*}}{\gamma_{n^*B}+\bar{\gamma}_{AR}+\bar{\gamma}_{RB}+\frac{1}{\rho}}\right) \tag{15}$$

$$I_R^{CJ} = \frac{1}{2}\log_2\left(1+\frac{\gamma_{Am^*}}{\gamma_{m^*B}+\frac{1}{\rho}}\right), \tag{16}$$

where the antennas are chosen according to (6) and (7).

The corresponding SOP for the CJ protocol is then given by

$$\mathcal{P}_{out}^{CJ}(R) = \mathcal{P}\left(\frac{1+\rho\frac{\gamma_{n^*B}\gamma_{Am^*}}{\gamma_{n^*B}+\bar{\gamma}_{AR}+\bar{\gamma}_{RB}+\frac{1}{\rho}}}{1+\frac{\gamma_{Am^*}}{\gamma_{m^*B}+\frac{1}{\rho}}} < 2^{2R}\right) \tag{17}$$

which is difficult to characterize with an exact analytical expression. In the following, we analyze the asymptotic behaviour of CJ in terms of SOP with respect to the values of ρ and K, and subsequently validate our results through simulation.

Proposition 2. *The secrecy outage probability of CJ approaches zero as the SNR increases: $\mathcal{P}_{out}^{CJ} \to 0$ as $\rho \to \infty$.*

Proof. We first give an upper bound for $\mathcal{P}_{out}^{CJ}$. It is obvious that the fraction in (17) is monotonically increasing with respect to γ_{n^*B}. For γ_{Am^*}, the fraction can be rewritten as

$$f(\gamma_{Am^*}) = \frac{1+\alpha\gamma_{Am^*}}{1+\beta\gamma_{Am^*}},$$

where $\alpha = \rho\gamma_{n^*B}/(\gamma_{n^*B}+\bar{\gamma}_{AR}+\bar{\gamma}_{RB}+\frac{1}{\rho})$ and $\beta = 1/(\gamma_{m^*B}+\frac{1}{\rho})$. The existence of a positive secrecy rate requires $\alpha > \beta$, which implies that $f(\gamma_{Am^*})$ is a monotonically increasing function of γ_{Am^*}. Therefore, the SOP of CJ with antenna selection is upper bounded by the SOP with random selection. That is, since $\gamma_{Am} \leq \gamma_{Am^*}$ and $\gamma_{nB} \leq \gamma_{n^*B}$, we have

$$\begin{aligned}
\mathcal{P}_{out}^{CJ}(R) \leq \bar{\mathcal{P}}_{out}^{CJ}(R) &= \mathcal{P}\left(\frac{1+\rho\frac{\gamma_{nB}\gamma_{Am}}{\gamma_{nB}+\bar{\gamma}_{AR}+\bar{\gamma}_{RB}+\frac{1}{\rho}}}{1+\frac{\gamma_{Am}}{\gamma_{mB}+\frac{1}{\rho}}} < 2^{2R}\right) \\
&\overset{a}{=} 1 - \frac{1}{\bar{\gamma}_{RB}}\int_t^\infty \exp\left(-\frac{2^{2R}-1}{\bar{\gamma}_{AR}h(z)} - \frac{z}{\bar{\gamma}_{RB}}\right) dz,
\end{aligned}$$

where

$$h(z) = \frac{\rho z}{z+\bar{\gamma}_{AR}+\bar{\gamma}_{RB}+\frac{1}{\rho}} - \frac{2^{2R}}{z+\frac{1}{\rho}},$$

$$t = \frac{(2^{2R}-1)+\sqrt{(2^{2R}-1)^2+\rho 2^{2R+1}(\bar{\gamma}_{AR}+\bar{\gamma}_{RB}+1/\rho)}}{2\rho}$$

and the derivation of (a) is skipped due to space constraints. Since $t \to 0$ and $h(z) \to \infty$ as $\rho \to \infty$, we have $\bar{\mathcal{P}}_{out}^{CJ}(R) \to 1 - \frac{1}{\bar{\gamma}_{RB}}\int_0^\infty e^{-\frac{z}{\bar{\gamma}_{RB}}}\, dz = 0$, and thus $\mathcal{P}_{out}^{CJ}(R)$ also approaches zero. $\square$

Proposition 2 indicates that compared to the AF protocol where $\mathcal{P}_{out}^{AF}$ converges to a non-zero constant as ρ increases, CJ is a better alternative at high SNR when security is paramount. Also from the above proof, since the fraction in (17) is a monotonically increasing function of both γ_{Am^*} and γ_{n^*B}, and due to the fact that both γ_{Am^*} and γ_{n^*B} increase as K grows, we can conclude that $\mathcal{P}_{out}^{CJ} \to 0$ as $K \to \infty$, *i.e.* the legitimate user with CJ can obtain diversity benefits from antenna selection.

4. NUMERICAL RESULTS

In this section, we present numerical examples of the outage performance for AF and CJ. The SOP is evaluated for various values of the transmit power and number of antennas. For comparison purposes, we also simulate the direct transmission (DT) case where Alice treats the relay as a pure eavesdropper and no relaying occurs.

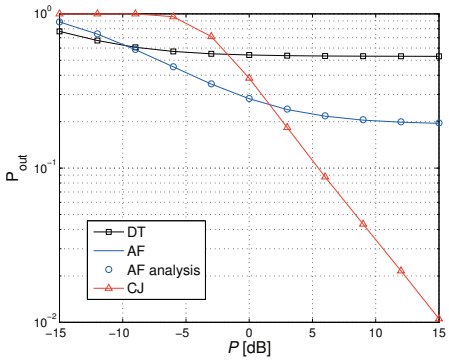

Fig. 1. Secrecy outage probability versus P, $K = 6$, $\bar{\gamma}_{AB} = 5$dB, $\bar{\gamma}_{AR} = 0$dB, $\bar{\gamma}_{RB} = 5$dB.

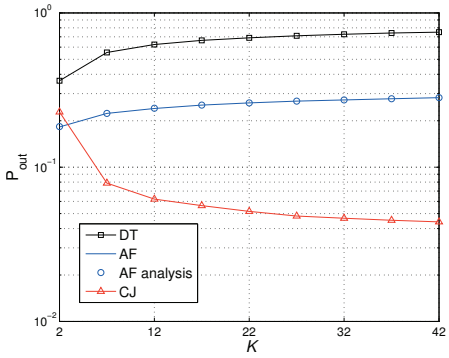

Fig. 2. Secrecy utage probability versus number of antennas, $P = 6$dB, $\bar{\gamma}_{AB} = 5$dB, $\bar{\gamma}_{AR} = 0$dB, $\bar{\gamma}_{RB} = 5$dB.

The normalized target secrecy rate is set equal to $R = 0.1$ bits per channel use [7], and the noise power N_0 is set to unity.

Fig. 1 depicts the SOP as a function of P, where the average channel gains are $\bar{\gamma}_{AB} = 5$dB, $\bar{\gamma}_{AR} = 0$dB, $\bar{\gamma}_{RB} = 5$dB, and $K = 6$. The analytical result of the outage probability for AF is evaluated through Eq. (9), which is seen to agree well with the simulation result. This figure shows that when $P \to \infty$, the SOP converges to a non-zero constant for AF while it goes to 0 for CJ, which agrees with the discussion in Section 3. This is due to the fact that the jamming signals from Bob only interfere with the relay and have no impact on the overall quality of the two-hop information signal. Therefore, the SOP for CJ is better than AF and DT in the high SNR regime, while the converse is true in the low SNR regime, since the fact that CJ ignores the direct link from Alice to Bob considerably degrades its performance. We can also see that for the most part, DT performs worse than both AF and CJ when the unauthenticated relay has multiple antennas and thus has enhanced wiretapping capabilities.

The impact of the number of relay antennas K on the SOP is illustrated in Fig. 2, where $\bar{\gamma}_{AB} = 5$dB, $\bar{\gamma}_{AR} = 0$dB, $\bar{\gamma}_{RB} = 5$dB, and $P = 6$dB. Observe that when K increases, the outage probabilities for DT and AF gradually approach 1, indicating that growth in the number of antennas only provides diversity benefits for the unauthenticated relay. On the other hand, the SOP for CJ decreases as K grows and gradually approaches zero, which suggests that the legitimate user can obtain diversity benefits from antenna selection on an unauthenticated relay, as analyzed in Section 3.2. Note that the SNR is relatively high in this example, and thus the performance gain of CJ over AF and DT is obvious.

5. CONCLUSIONS

This paper has analyzed a three-node network where a single-antenna source can potentially utilize a cooperative unauthenticated multi-antenna relay to supplement the direct link to its destination. The goal of the work is to study when a jamming signal can be used by the destination to degrade the ability of the relay to obtain information from the relayed signal. We characterize the exact SOP for conventional AF relaying, and study the asymptotic outage performance for CJ. We also provide analytical and numerical illustrations showing that CJ outperforms AF in the high SNR regime, or in the case when the number of relay antennas grows.

6. REFERENCES

[1] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[2] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[3] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Sep. 2001, pp. 87–89.

[4] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Jul. 2010.

[5] Y. Zhang, G. Zheng, C. Ji, K.-K. Wong, D. J. Edwards, and T. Cui, "Near-optimal joint antenna selection for amplify-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2401–2407, Aug. 2010.

[6] J.-B. Kim and D. Kim, "End-to-end BER performance of cooperative MIMO transmission with antenna selection in Rayleigh fading," in *Proc. Fortieth Asilomar Conf. Signals, Systems and Computers*, Oct. 2006, pp. 1654–1657.

[7] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int Information Theory Symp*, Dec. 2006, pp. 356–360.

[8] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, Jun. 2011.

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE/SP 15th Workshop on Statistical Signal Processing*, Aug. 2009, pp. 417–420.

[10] J. Huang and A. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, to appear.

[11] G. Amarasuriya, C. Tellambura, and M. Ardakani, "Feedback delay effect on dual-hop MIMO af relaying with antenna selection," in *Proc. IEEE Global Telecommunications Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5.

[12] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 4th ed. New York: McGraw-Hill, 2002.