Outage Performance for Amplify-and-Forward Channels with an Unauthenticated Relay

Jing Huang, Amitav Mukherjee, and A. Lee Swindlehurst
Electrical Engineering and Computer Science
University of California, Irvine, CA 92697
Email: {jing.huang; amukherj; swindle}@uci.edu

Abstract—We investigate a relay network where the source can potentially utilize an unauthenticated amplify-and-forward (AF) relay to augment its direct transmission of a confidential message to the destination. Since the relay is unauthenticated, it is desirable to protect the confidential data from it while simultaneously making use of it to increase the reliability of the transmission. We study the likelihood of achieving simultaneously secure and reliable message transmission via the secrecy outage probability (SOP) of the relay network. We first characterize the SOP for three different schemes: direct transmission, conventional AF relaying, and cooperative jamming. Subsequently, an asymptotic analysis is conducted to determine the optimal policies for different power budgets and channel gains. Numerical results are presented to verify the theoretical predictions of the preferred transmission policies from a secrecy outage perspective.

I. INTRODUCTION

There has recently been intensive interest in improving information security at the physical layer of wireless networks [1], [2]. Besides the widely-used metric of secrecy rate, an alternative secrecy criterion that has recently been investigated for fading channels is the secrecy outage probability, which describes the probability of simultaneously reliable and secure data transmission [3].

In the context of relay channels, the secrecy outage probability has been investigated in [4], [5] for networks compromised of external eavesdroppers that are distinct from the source/sink and relay nodes. However, even if external eavesdroppers are absent, it may 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 [6]. For example, the unauthenticated relay may belong to a heterogeneous network without the same security clearance as the source and destination nodes. This scenario has also been denoted as cooperative communication via an untrusted relay in [7], where the authors presented bounds on the achievable secrecy rate. Furthermore, they showed that amplify-and-forward (AF) and compress-and-forward relaying (including a direct link) admit a non-zero secrecy rate even when the relay is untrusted, which does not hold for decode-and-forward relaying. Therefore, in this work we focus on the AF relaying protocol due to its increased security vis-à-vis decode-and-forward, and its lower complexity as compared to compress-and-forward.

This paper analyzes a three-node network where the source can potentially utilize an unauthenticated relay to augment the direct link to its destination. The relay thus is in effect also an eavesdropper, even though it complies with the source’s request to act as a relay to the destination. We characterize the exact secrecy outage probability of three different transmission policies: direct transmission where the relay is ignored, conventional AF relaying, and cooperative jamming by the destination to selectively degrade the relay’s eavesdropping capability. Subsequently, an asymptotic analysis of the outage probabilities is conducted to elicit the optimal policies for different power budgets and channel gains. Among our findings, we demonstrate that direct transmission is best when either of the relay hops is weak, the AF protocol is preferred when both links to the destination are strong, and cooperative jamming is optimal in the high transmit power regime.

The remainder of this work is organized as follows. The mathematical model of the relaying protocols is introduced in Section II. The exact and asymptotic secrecy outage probabilities of direct transmission, AF relaying, and cooperative jamming are derived in Sections III and IV, respectively. Selected numerical results are shown in Section V, and we conclude in Section VI.

II. MATHEMATICAL MODEL

We consider a half-duplex two-hop relaying system composed of a source (Alice), a destination (Bob), and an unauthenticated AF 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. Relay Protocol

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

\[ y_R = \alpha_{AR} x_A + n_R \tag{1} \]

\[ y_{B1} = \alpha_{AB} x_A + n_{B1} \tag{2} \]

respectively, where \( x_A \) is the signal transmitted at 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 gain between node \( i \) and \( j \), with \( i, j \in \{A, R, B\} \) denoting which of the three terminals is involved, and \( n_i \sim \mathcal{CN}(0, N_0) \) is additive white Gaussian noise at node \( i \). 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 $\gamma_{ij}$ is exponentially distributed with hazard rate $\frac{1}{\bar{\gamma}_{ij}}$, and the probability density function (p.d.f.) is given by
\[
p_{\gamma_{ij}}(x) = \frac{1}{\bar{\gamma}_{ij}} \exp\left(-\frac{x}{\bar{\gamma}_{ij}}\right), \quad x \geq 0.
\]

During the second phase, the relay normalizes its received signal $y_R$ and transmits a scaled version $x_R = \sqrt{\frac{P}{\sigma}} y_R$ where $\sigma = \sqrt{\mathbb{E}[|y_R|^2]}$. The received signal at Bob during both phases is then given by
\[
y_R = \left[\frac{\alpha_{AB}}{\alpha_{RB}\alpha_{AR}}\right] x_A + \left[\frac{\sqrt{P}}{\sigma}\alpha_{RB}\sigma_{RB} + n_R\right].
\]

### B. Cooperative Jamming

For the cooperative jamming scheme, we follow a model similar to [5], where Bob ignores the direct link and transmits cooperative jamming signals during the first phase. Thus the received signal at the relay is
\[
y_R = \alpha_{AR} x_A + \alpha_{RB} z_B + n_R
\]
where $z_B$ is a noise-like signal transmitted by Bob to selectively jam the relay. We assume a reciprocal channel between the relay and Bob: $\alpha_{RB} = \alpha_{BR}$.

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
\[
y_B = \left[\frac{\sqrt{P}}{\sigma}\alpha_{RB}\alpha_{AR}\sigma_{RB} + \frac{\sqrt{P}}{\sigma}\alpha_{RB}\sigma_{RB} + n_B\right] x_A + \left[\frac{\sqrt{P}}{\sigma}\alpha_{RB}\sigma_{RB} + n_B\right] z_B + \left[\frac{\sqrt{P}}{\sigma}\alpha_{RB}\sigma_{RB} + n_B\right] n_R
\]
where the intentional interference term can be removed by Bob since $z_B$ is known to him.

### III. Transmission with an Unauthenticated Relay

#### A. Direct Transmission (DT)

Under certain conditions, as will be discussed later, a better option for Alice is to perform single-hop transmission instead of cooperating with the relay. In this case, the relay is simply treated as a pure eavesdropper. Thus the model will be simplified to a traditional wiretap channel with Rayleigh fading, which has been fully characterized in [3], for example.

Since the channel gains are assumed to be quasi-static, the achievable secrecy rate for one channel realization is given by
\[
R_s^{DT} = [I_B^{DT} - I_R^{DT}]^+.
\]
where $[x]^+ \triangleq \max\{0, x\}$, $I_B^{DT}$ and $I_R^{DT}$ represent the mutual information between Alice and Bob, and between Alice and the relay respectively, and are given by $I_B^{DT} = \log_2(1 + \rho\gamma_{AB})$ and $I_R^{DT} = \log_2(1 + \rho\gamma_{AR})$, where $\rho \triangleq \frac{P}{N_0}$ is the SNR.

Therefore, the probability of a positive secrecy rate is [3]
\[
P_{\text{pos}}^{DT} = P\left(I_B^{DT} - I_R^{DT} > 0\right) = P\left(\gamma_{AB} > \gamma_{AR}\right) = \frac{\gamma_{AB}}{\gamma_{AR}}.
\]

It is interesting to note that, in the presence of fading, a positive secrecy rate is achievable even when $\gamma_{AB} > \gamma_{AR}$, i.e. when the eavesdropper’s channel is on average better than the legitimate channel. Eq. (7) also indicates that Alice will be unable to reliably transmit secret messages when $\gamma_{AB} > \gamma_{AR}$, e.g., when the unauthenticated relay is proximate to Alice.

The outage probability for a given target secrecy rate $R$ is then given by [3]
\[
P_{out}^{DT}(R) = P\left(\log_2\left(1 + \frac{\gamma_{RB}^2}{\gamma_{RB} + \gamma_{AR} + \frac{1}{\rho}}\right) < R\right) = 1 - \frac{\gamma_{AB}}{2\gamma_{AR}} \exp\left(-\frac{\gamma_{AR} - 1}{\rho\gamma_{AB}}\right).
\]

Note that the secrecy outage probability is a well-known criterion that characterizes the probability of simultaneously reliable and secure data transmission as defined in [4], [5], and we adopt the same definition in this paper.

#### B. 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 nodes $\alpha_{RB} = \alpha_{BR}$.

Let $U = \frac{\gamma_{AB}}{\gamma_{AR}}$ and $V = \frac{\gamma_{RB}}{\gamma_{RB} + \gamma_{AR} + \frac{1}{\rho}}$, where the p.d.f.s of $U$ and $V$ can be obtained as
\[
p_U(u) = \frac{\gamma_{AB}^2}{\gamma_{AR}^2} (\gamma_{AR} + \gamma_{RB} + \frac{1}{\rho})^2 \exp\left(-\frac{\gamma_{AR}^2}{\gamma_{RB}(1 - v)}\right),
\]
and $I_R^{AF}$ are the corresponding expressions for mutual information.

Therefore, the probability of achieving a positive secrecy rate for AF relaying is formulated as
\[
P_{\text{pos}}^{AF} = P\left(U + V > 1\right) = \int_0^1 \int_{-v}^v p_U(u)p_V(v) dudv.
\]

Let $U = \frac{\gamma_{AB}}{\gamma_{AR}}$ and $V = \frac{\gamma_{RB}}{\gamma_{RB} + \gamma_{AR} + \frac{1}{\rho}}$, where the p.d.f.s of $U$ and $V$ can be obtained as
\[
p_U(u) = \frac{\gamma_{AB}^2}{\gamma_{AR}^2} (\gamma_{AR} + \gamma_{RB} + \frac{1}{\rho})^2 \exp\left(-\frac{\gamma_{AR}^2}{\gamma_{RB}(1 - v)}\right),
\]
and $I_R^{AF}$ are the corresponding expressions for mutual information.

Therefore, the probability of achieving a positive secrecy rate for AF relaying is formulated as
\[
P_{\text{pos}}^{AF} = P\left(U + V > 1\right) = \int_0^1 \int_{-v}^v p_U(u)p_V(v) dudv.
\]
where $\mu_1 = \frac{\gamma_{AB}}{1 + \rho}$, $\beta_1 = 1 + \frac{\gamma_{AB}}{1 + \rho}$, and $\text{Ei}(\cdot)$ is the exponential integral $\text{Ei}(x) = \int_{-\infty}^{x} e^{t} t^{-1} \, dt$.

The outage probability of the AF scheme for a given secrecy rate $R$ can then be written as

$$P_{\text{out}}^{AF}(R) = \mathcal{P} \left\{ \frac{1}{2} \log_2 \left( 1 + \rho \gamma_{AB} + \frac{\rho \gamma_{AB}}{1 + \rho \gamma_{AR}} \right) < R \right\},$$

(15)

and the exact SOP is given by the following proposition.

**Proposition 1:** The secrecy outage probability for AF relaying can be expressed as

$$P_{\text{out}}^{AF}(R) = 1 - \frac{\gamma_{AB}}{(2^{2R} - 1)(\gamma_{AB} + \gamma_{AR})} \exp \left(-\frac{2^{2R} - 1}{\rho \gamma_{AB}} \right) \times [\mu_1(\beta_2 - 1) \exp(\mu_1 \beta_2) \text{Ei}(-\mu_1 \beta_2) + 1]$$

(16)

where $\mu_1 = \frac{\gamma_{AB} + 1}{\gamma_{AR}}$, $\beta_2 = \frac{2^{2R} \gamma_{AB} + \gamma_{AR}}{(2^{2R} - 1) \gamma_{AR} + \gamma_{AR}}$, and $R$ is the target secrecy rate.

**Proof:** Let $X = \gamma_{AR}$, $Y = \gamma_{AB}$ and define

$$Z = \frac{1 + \rho \gamma_{AB} + \rho \gamma_{AB} \gamma_{AR}}{1 + \rho \gamma_{AR}} = \frac{\gamma_{RB}}{\gamma_{RB} + \gamma_{AR} + 1}, \quad V = \frac{\gamma_{RB}}{\gamma_{RB} + \gamma_{AR} + 1}$$

where the p.d.f. of $V$ is given by (13). We thus have

$$P_{\text{out}}^{AF} = \mathcal{P} \left\{ \frac{1}{1 + \rho Y} \frac{1 + \rho X + \rho Y V}{1 + \rho Y} < 2^{2R} \right\}$$

$$= \mathbb{E}_V \{ \mathbb{E}_Y \{ F_Z | Y, V(2^{2R}) \} \}$$

$$= \int_0^1 \int_0^1 \left( 1 - \exp \left[ -\frac{1}{\gamma_{AB}} \left( \frac{2^{2R} - 1}{\rho} + (2^{2R} - v)y \right) \right] \right) \times p_Y(y) p_V(v) \, dy \, dv$$

$$= 1 - \frac{\gamma_{AB} + 1}{\gamma_{AR} \gamma_{RB}} \exp \left(-\frac{2^{2R} - 1}{\rho \gamma_{AB}} \right) \int_0^1 \int_0^1 \left( 1 - v \right)^2 \times \exp \left(-\frac{(2^{2R} - v)y - y - (\gamma_{AR} + 1) v}{\gamma_{RB}(1 - v)} \right) \, dy \, dv.$$

After further manipulations by using the transformation $x = \frac{y}{1 - v}$, $\mu_1 = \frac{\gamma_{AB} + 1}{\gamma_{AR}}$, $\beta_2 = \frac{2^{2R} \gamma_{AB} + \gamma_{AR}}{(2^{2R} - 1) \gamma_{AR} + \gamma_{AR}}$ and the identity in [8, eq. 3.353.5], the result in (16) can be obtained.

**C. Cooperative Jamming (CJ)**

Various cooperative jamming schemes involving the transmission of artificial interference from the destination have been proposed in [5], [9], [10], and in this paper we adopt the scheme investigated in [5], where Bob transmits cooperative jamming signals in the first transmission phase. According to the signal model in Section II-B, we have the following expressions for the mutual information at Bob and the relay for the cooperative jamming scenario:

$$I_{B}^{CJ} = \frac{1}{2} \log_2 \left( 1 + \frac{\gamma_{RB} \gamma_{AR}}{\gamma_{RB} + \gamma_{AR} + 1} \right)$$

(18)

$$I_{R}^{CJ} = \frac{1}{2} \log_2 \left( 1 + \frac{\gamma_{AR}}{\gamma_{RB} + 1} \right),$$

(19)

and the corresponding probability of a positive secrecy rate is given by

$$P_{\text{pos}}^{CJ} = \mathcal{P} \left\{ \frac{\gamma_{RB}}{\gamma_{RB} + \gamma_{AR} + 1} > 1 \right\}$$

(20)

$$= \exp \left(-\frac{1}{\gamma_{RB}} \sqrt{\frac{\gamma_{AR} + \gamma_{RB} + 1}{\rho}} \right).$$

From (20), we see that $P_{\text{pos}}^{CJ}$ is a monotonically increasing function of $\gamma_{RB}$ when $\gamma_{AB}$ is fixed. In other words, CJ is not appropriate when the second hop channel is too weak. This is not surprising since, when CJ is employed, the half-duplex constraint for Bob means that the information from the direct link is ignored, and Bob relies heavily on the second hop to obtain the information from Alice.

The outage probability of the CJ scheme can be written as

$$P_{\text{out}}^{CJ}(R) = \mathcal{P} \left\{ \frac{1}{1 + \rho \gamma_{AR} \gamma_{RB} + \gamma_{AR} + 1} < 2^{2R} \right\}$$

(21)

and the exact expression is given by the following proposition.

**Proposition 2:** The secrecy outage probability for the CJ scheme is given by

$$P_{\text{out}}^{CJ}(R) = 1 - \frac{1}{\gamma_{RB}} \int_{\frac{1}{\gamma_{RB}}}^{\infty} \exp \left(-\frac{2^{2R} - 1}{\gamma_{AR} h(z)} - \frac{z}{\gamma_{RB}} \right) \, dz,$$

(22)

where

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

$$t = \frac{(2^{2R} - 1) + \sqrt{(2^{2R} - 1)^2 + \rho 2^{2R+1} (\gamma_{AR} + \gamma_{RB} + 1)}}{2 \rho}.$$

**Proof:** See [11].

**IV. ASYMPTOTIC BEHAVIOR AND DISCUSSION**

The choice of which scheme (DT, AF or CJ) to employ depends on the specific power budget and channel gains; each of these methods is optimal for different operating regimes. Here we investigate the asymptotic behavior of the outage probability to determine the conditions under which each approach offers the best performance.
1) Case of $P \to \infty$: From (8), we have $\lim_{P \to \infty} P_{DT}^{\text{out}} = 1 - \frac{\gamma_{AB}}{2R \gamma_{AB} + \gamma_{AB}}$, and according to (16),

$$
\lim_{\rho \to \infty} P_{AF}^{\text{out}} = 1 - \frac{\gamma_{2R}}{\rho \gamma_{2R} + \gamma_{2R}} \exp \left( -\frac{\gamma_{2R}}{\rho \gamma_{2R}} \right),
$$

where $\rho = \frac{\gamma_{2R}}{\gamma_{AB}}$. Therefore, both $P_{DT}^{\text{out}}$ and $P_{AF}^{\text{out}}$ converge to non-zero constants as $P \to \infty$. For CJ, however, according to (22), we have

$$
\lim_{\rho \to \infty} P_{CJ}^{\text{out}} = 1 - \frac{1}{\gamma_{AR}} \int_{0}^{\infty} \exp \left( -\frac{z}{\gamma_{AR}} \right) dz = 0,
$$

which shows that CJ is preferable as $P \to \infty$.

2) Case of $\gamma_{AB} \to \infty$ or 0: From (8) and (16), it is also straightforward to obtain that $P_{DT}^{\text{out}}, P_{AF}^{\text{out}} \to 0$ as $\gamma_{AB} \to \infty$. When $\gamma_{AB}$ is sufficiently large, using the fact that $1 - \exp(x) = x + O(x^2)$, we can observe that with respect to $\gamma_{AB}$, both DT and AT decay proportionally to $1/\gamma_{AB}$. Conversely, we also have that $P_{DT}^{\text{out}}, P_{AF}^{\text{out}} \to 1$ as $\gamma_{AB} \to 0$. Since $P_{CJ}^{\text{out}}$ does not depend on $\gamma_{AB}$, we can conclude that the DT and AF schemes are better than CJ when the direct link is significantly stronger than the others, while CJ will perform better when the direct link is relatively weak.

3) Case of $\gamma_{RB} \to \infty$ or 0: Since $P_{DT}^{\text{out}}$ is not a function of $\gamma_{RB}$, it will be the same as (8). When $\gamma_{RB} \to \infty$, according to (16) and using the result that $z \exp(-z) \to 0$ as $x \to 0$ [5], we have

$$
\lim_{\gamma_{RB} \to \infty} P_{AF}^{\text{out}} = 1 - \frac{\gamma_{AB}}{(2R - 1) \gamma_{AR} + \gamma_{AB}} \exp \left( -\frac{2R - 1}{\rho \gamma_{AB}} \right).
$$

For CJ, when $\gamma_{RB} \to \infty$, the cooperative jamming support from Bob can fully prevent the relay from eavesdropping, and thus the outage event will only depend on the relay channel:

$$
\lim_{\gamma_{RB} \to \infty} P_{CJ}^{\text{out}} = P \left( 1 + \rho \frac{\gamma_{RB} \gamma_{AR}}{\gamma_{RB} + \gamma_{AR} + \gamma_{RB} + \frac{2R}{\rho}} \right) = \frac{(2R - 1)}{\rho \gamma_{AR}}
$$

According to (22) with further manipulation, we have

$$
\lim_{\gamma_{RB} \to \infty} P_{CJ}^{\text{out}} = \frac{1}{\gamma_{RB}} \int_{0}^{\infty} \exp \left( -\frac{z}{\gamma_{RB}} \right) dz = 0
$$

where $K_{1}(\cdot)$ is the modified Bessel function of the second kind, and [8, eq. 3.324.1] is used for obtaining the above result. Therefore, as $\gamma_{RB} \to \infty$, the outage probability for all schemes converges to different constants, and the analysis does not reveal an advantage of one method over another.

When $\gamma_{RB} \to 0$, CJ is obviously not applicable since $P_{out}^{CJ} \to 1$. When AF is used, as seen from (15), the outage probability will converge to

$$
P_{AF}^{\text{out}} = P \left\{ \frac{1}{2} \log_2 \left( \frac{1 + \rho \gamma_{AR}}{1 + \rho \gamma_{AR}} \right) < R \right\}
$$

which indicates that DT is a better choice when $\gamma_{RB} \to 0$ due to the resource division factor 1/2.

4) Case of $\gamma_{AR} \to 0$: In this case, for CJ, it is easy to verify from (22) that $\lim_{\gamma_{AR} \to 0} P_{CJ}^{\text{out}} = 1$, since $t \to \infty$ as $\gamma_{AR} \to 0$ and the result of the integral in (22) approaches 0. However, for DT and AF, the outage probability will converge to constants given by

$$
\lim_{\gamma_{AR} \to 0} P_{DT}^{\text{out}} = 1 - \exp \left( -\frac{2R - 1}{\rho \gamma_{AR}} \right)
$$

Due to the resource division factor again, similar to the case in Section IV-3, we have $\lim_{\gamma_{AR} \to 0} P_{AF}^{\text{out}} = \lim_{\gamma_{AR} \to 0} P_{DT}^{\text{out}}$, and thus DT is preferred in terms of secrecy outage probability.

Based on the above observations, we summarize the preferred scenarios for each scheme as follows:

- **Direct transmission**: when $\gamma_{AR} \to 0$ or $\gamma_{RB} \to 0$, i.e., when either of the relay hops is extremely weak, DT is a better scheme since the outage performance of both AF and CJ is sensitive to the quality of the two-hop channels.
- **Amplify-and-forward**: when $\gamma_{AR} \to \infty$ and $\gamma_{RB} \to \infty$, i.e., when both the direct link and the second hop channel are relatively strong, AF should be used.
- **Cooperative jamming**: when $P \to \infty$ or $\gamma_{AR} \to 0$, i.e., when the transmit power is high or there is no direct link between Alice and Bob (the latter is especially applicable to the case studied in [4], [12] where the direct path between the source and destination is blocked by an obstacle or undergoes shadowing), CJ is preferred.

V. Numerical Results

In this section, we present numerical examples of the outage performance for the investigated transmission schemes: direct transmission (DT), amplify-and-forward (AF), and cooperative jamming (CJ). The normalized target secrecy rate is set equal to $R = 0.1$ bits per channel use [3], [4].

Fig. 1 depicts the outage probability as a function of $P$, where the average channel gains are $\gamma_{AB} = \gamma_{AR} = \gamma_{RB} = 0$ dB. The analytical SOP results for AF and CJ are evaluated through Eqs. (16) and (22), and are seen to agree well with the simulations. This figure also shows that when $P \to \infty$, the outage probability converges to a constant for AF while it goes to 0 for CJ, which agrees with the discussion in Section IV-1. This is due to the fact that the jamming signals from Bob only selectively interfere with the relay and have no impact on the overall two-hop data signal reception. Therefore, the outage performance for CJ is better than AF in the high SNR regime, while the converse is true in the low SNR regime.
Fig. 2. Outage probability versus $\gamma_{AR}, \gamma_{RB} = 5\text{dB}, \gamma_{AB} = 0\text{dB}, P = 20\text{dB}$, asymptotic results computed with Eqs. (26) for DT, and (27) for AF.

Fig. 3 shows the performance as a function of $\gamma_{AB}$, with $\gamma_{AR} = 2\text{dB}$, and $\gamma_{RB} = 10\text{dB}$. It is shown that when $\gamma_{AB}$ is small, CJ is the best scheme since both DT and AF will be in outage. Conversely, with large $\gamma_{AB}$, the outage probability for DT and AF decays to 0. Moreover, as discussed in Section IV-2, the outage probability for both DT and AF is seen to decay as $1/\gamma_{AB}$.

VI. CONCLUSIONS

This paper analyzes a three-node network where the source can potentially utilize an unauthenticated relay to supplement the direct link to its destination. We characterize the exact secrecy outage probability of three different transmission policies: direct transmission, conventional AF relaying, and cooperative jamming. Subsequently, an asymptotic analysis of the outage probabilities is conducted to elicit the optimal policies in different operating regimes. Numerical results reveal that each of the three transmission schemes enjoys an advantage over the others for different values of the transmit power and channel gains. Among the numerous avenues for future work in this topic are extensions to multiple-antenna sources and relays, for example.

REFERENCES


