Detecting Malicious Behavior in Cooperative Diversity

Sintayehu Dehnie
Electrical and Computer Engineering Department
Polytechnic University
5 MetroTech Center,Brooklyn, NY 11201

Huserv T. Sencar, Nasir Memon
Computer and Information Science Department
Polytechnic University
5 MetroTech Center,Brooklyn, NY 11201

***Abstract*—We consider a cooperative diversity scheme where a relay cooperatively enhances communication between a source and destination. In cooperative diversity, due to lack of a mechanism to ensure relay's adherence to the cooperation strategy, the receiver is often assumed to be passive. In this paper, we consider a *smart* destination which examines relay's signal prior to applying diversity combining. This is attributed to the assumption that relay may not conform to the cooperation strategies at all times and may behave maliciously. Based on this assumption, we develop a statistical detection technique to mitigate malicious relay behavior in decode-and-forward cooperation strategy. The detection technique statistically compares the signals received from the two diversity branches to determine the relay's behavior. As the uncertainty in the direct path is only due to the channel, correlation of received signals from the source and relay provides a basis to characterize relay behavior. We show, both by analysis and simulation, that a malicious relay reduces the correlation between the received signals in the diversity branch. Finally, we investigate bit-error rate and outage behavior performance in the presence of a *smart* destination.**

***Index Terms*—Diversity techniques, fading channels, relay channel, communication system security.**

I. Introduction

Cooperative wireless communications is a new and emerging form of diversity that emulates transmit antenna diversity to mitigate fading in the wireless channel. By exploiting the broadcast nature of the wireless channel, cooperative diversity allows single-antenna radios share their antennas to form a virtual antenna array. The formation of the virtual antenna array, through cooperative diversity, provides reliable communication and improved Quality of Service (QoS), like BER, outage probability, etc., to single-antenna wireless devices.

Cooperative diversity may be achieved in a relay channel [1], [2], [3] setting or through user cooperation [4], [5], [6]. A relay channel is a three-terminal network consisting of a source, a relay and a destination, Figure $1(a)$. Whereas in user cooperative communications, Figure $1(b)$, each wireless user transmits their own data as well as act as a relay. In both cases, the relay enhances communication between the source and destination.

Cooperative diversity schemes employ various cooperation strategies, commonly known as cooperative diversity protocols. The two main fixed cooperative diversity protocols are amplify-and-forward (**AF**) and decode-and-forward (**DF**). The two protocols are fixed as the cooperation strategy does not depend on the state of the source-relay channel. In the adaptive version of **AF** and **DF**, the cooperation strategy relies on the decoding ability of the relay. That is, relay cooperates only when amplitude of the source-relay channel is above a certain threshold.

Consider the scenario depicted in Figure 1 where the source transmits directly to the destination. Due to the broadcast nature of the wireless channel and its proximity to the source, the *relay* also receives the transmitted signal. In the **AF** strategy, the cooperating radio simply amplifies the faded and noisy received signal and retransmits it to the destination. It is important to note that *relay* amplifies the received signal subject to its power constraint. In the **DF** strategy, the *relay* decodes the received source codeword. It then re-encodes the source codeword and retransmits the encoded source bits to the destination. The relay might fully decode, i.e., estimate without error the entire source codeword [6]. At the destination, the retransmitted signal from relay provides redundancy to resolve the uncertainty in decoding the signal received from the direct path. The destination combines the received signals using any one of the diversity combining techniques yielding less number of detection errors compared to single path transmission.

Cooperative diversity protocols are primarily designed to improve QoS at the physical layer with the assumption that relays always cooperate. That is, the source and destination implicitly assume that the relay conforms with the cooperation strategy at all times. From a security point of view, this inherent assumption implies that relays are always trusted. However, this assumption may not be valid in a practical setting with adversarial elements wherein relays might exhibit malicious behavior. As achieving reliable communication with cooperative diversity depends on relays conformance to rules of cooperation protocol, a malicious relay can constrain the envisaged performance improvements severely. Due to this trust assumption, cooperative diversity presents a new security challenge at the physical layer.

One approach to detect malicious behavior is where source and destination can agree on a mechanism to authenticate relay's signal, e.g. employing tracing symbols. Such an approach, although it may be effective, incurs a cost to the system in terms of bandwidth and additional complexity to generate tracing symbols. In this work, we argue that correlation between signals received in the two diversity branches

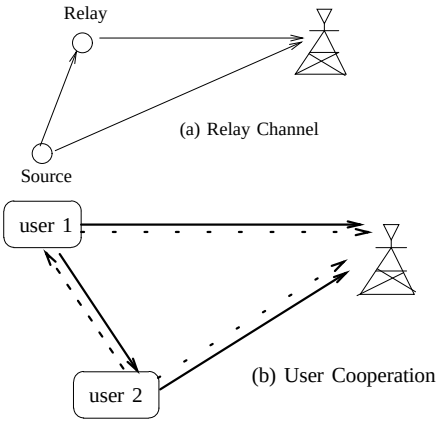

Fig. 1. Cooperative Diversity.

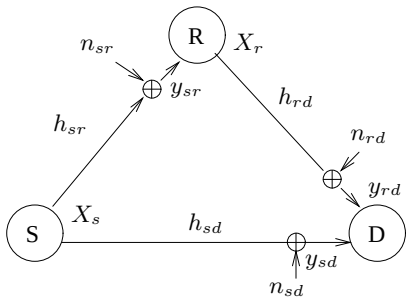

Fig. 2. Relay network.

is significantly reduced due to malicious behavior. Based on this argument, we propose a statistical detection technique to mitigate malicious relay behavior. The detection technique is restricted to **DF** cooperation strategy as it promises further performance improvement and attributes a higher degree of trust to relay. However, the detection technique can easily be extended to other cooperation strategies.

The rest of the paper is organized as follows. The communication (channel, modulation scheme, protocol settings) model is describe in section II. A model that capture relay's behavior is also described in section II. Discussion of the proposed detection technique is presented in section III. In section IV, the proposed technique is evaluated using simulation. Finally, we present concluding remarks and discussion on going works.

II. System Model

Consider the relay network depicted in Figure 2. In this work an orthogonal transmit scheme is considered, where the source and the relay transmit in non-overlapping time slots, T_S and T_R, respectively. During time slot T_S, the source (S) transmits signal X_s to the destination (D). Due to the broadcast nature of the channel, the relay (R) also receives the transmitted signal, X_s. During this time slot, the relay processes the received signal, implementing **DF** cooperative diversity protocol, and generates relay signal X_r. The received signals at the destination and the relay during this time, respectively are:

$$\begin{aligned} y_{sd} &= h_{sd}X_s + n_{sd} \\ y_{sr} &= h_{sr}X_s + n_{sr} \end{aligned} \tag{1}$$

where, channel $\boldsymbol{h} : \{h_{sd}\ h_{sr}\ h_{rd}\}$ is zero mean complex Gaussian random variable that captures the effects of path loss and fading in the wireless channels; $\boldsymbol{n} : \{n_{sd}\ n_{sr}\ n_{rd}\}$ is assumed to be additive white gaussian with power spectral density $\frac{N_0}{2}$. Throughout this work we assume uncoded BPSK signals, where $X_s \in \{-\sqrt{E_s}, +\sqrt{E_s}\}$ with $\mathbf{E}(|X_s|^2) = E_s$.

We assume an adaptive cooperation strategy where the relay cooperates only when it can reliably decode the BPSK signal, X_s. Thus, during the next time slot (T_R) relay retransmits X_s to the destination. The source transmits nothing during this time. The received signal at the destination, during time slot (T_R) is,

$$y_{rd} = h_{rd}X_s + n_{rd} \tag{2}$$

Rayleigh fading channels with independent channel dynamics in source-relay, source-destination and relay-destination channels is assumed. It is also assumed that the fading amplitude remains constant for two consecutive symbol durations. The noise processes are assumed to be independent and identically distributed.

The destination implements a diversity combining technique to combine the received signals during consecutive and non-overlapping time slots. We assume coherent detection where the channel state information (CSI) is fully known at the receivers. In this work, the Maximum Ratio Combining (MRC) technique is considered.

The relay behavior is represented assuming a probabilistic model [7]. In this model, the relay exhibits cooperating behavior in a stochastic manner. That is, the relay might cooperate with probability p_1, or act maliciously with probability p_2. As the relay exhibits mixed behavior of cooperation or maliciousness, we will refer to such relay behavior as semi-malicious. The randomness of the relay behavior introduces a new form of uncertainty in the system. To incorporate this new uncertainty in the system model, (2) is modified. Hence, the received signal at the destination can be described as

$$y_{rd}^{\Theta} = h_{rd}(\Theta X_s) + n_{rd} \tag{3}$$

where y_{rd}^{Θ} is the received signal in the presence of semi-malicious relay and Θ is a random variable that captures the relay behavior; the probability density function of Θ is given by:

$$\begin{aligned} &f_{\Theta}(\theta) = p_1\delta(\theta-\theta_1) + p_2\delta(\theta-\theta_2) + p_3\delta(\theta-\theta_3) + \ldots \\ &+p_m\delta(\theta-\theta_m) \end{aligned} \tag{4}$$

where p_m is the probability of occurrence of relay behavior m and θ_m represents the associated relay action. For instance, a cooperating relay is represented by ($p_m\ ,\ \theta_m = 1$) while a malicious relay will have ($p_m\ ,\ \theta_m \ll 1$).

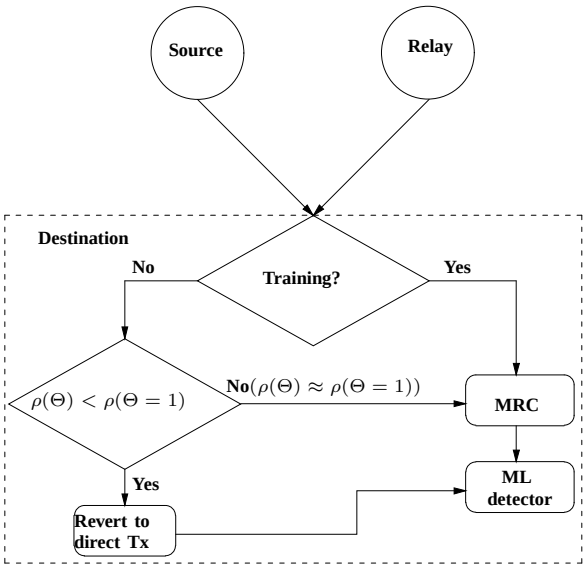

Fig. 3. Proposed Detection Technique.

III. Proposed Detection Technique

In the literature the destination is often assumed to behave in passive manner. That is, it simply combines signals received from the source and relay employing one of the diversity combining techniques without examining the relay's signal. The passive behavior signifies the lack of a mechanism to ensure relay's adherence to the cooperation strategy and inherent assumption that relay always behaves according to the cooperation strategies. As detection of malicious behavior is difficult under such assumption, we consider a *smart* destination which examines relay's signal prior to applying diversity combining. The proposed detection technique statistically compares the signals received from the two diversity branches. As the uncertainty in the direct path is only due to the channel, correlation of the signals from the source and relay provides a basis to characterize relay behavior.

The received signals at the destination in two consecutive time slots, assuming the relay correctly decodes, can be expressed as

$$\begin{aligned} y_{sd} &= h_{sd}X_s + n_{sd} \\ y_{rd}^{\Theta} &= h_{rd}(\Theta X_s) + n_{rd} \end{aligned} \tag{5}$$

As can be seen in (5), the uncertainty in the direct path is only due to the channel. Whereas the relay-destination channel is characterized by the additional uncertainty due to the relay behavior. Due to this, the statistical similarity between the received signals (5) decreases. Thus, correlation between the signals in the two diversity branches (5) provides a basis to determine relay behavior. Taking the correlation of the received signals at destination,

$$\mathbf{E}[y_{sd}y_{rd}^{\Theta}] = \mathbf{E}[h_{sd}]\mathbf{E}[h_{rd}]\mathbf{E}[\Theta]\mathbf{E}[X_s^2] \tag{6}$$

For the case of iid Rayleigh fading channels with unit mean power ($\mathbf{E}[h^2] = 1$), (6) becomes

$$\mathbf{E}[y_{sd}y_{rd}^{\Theta}] = \frac{\pi}{4}E_s\mathbf{E}[\Theta] \tag{7}$$

Thus, the normalized correlation, $\frac{\mathbf{E}[y_{sd}y_{rd}^{\Theta}]}{\sqrt{\mathbf{E}[y_{sd}]^2\mathbf{E}[y_{rd}^{\Theta}]^2}}$ is,

$$\rho(\Theta) = \frac{\frac{\pi}{4}E_s\mu_{\Theta}}{\sqrt{(E_s+\sigma_n^2)(E_s\mu_{\Theta^2}+\sigma_n^2)}} \tag{8}$$

where $\mu_{\Theta}, \mu_{\Theta^2}$ are the first and second moments of Θ.

Considering the special case where the relay cooperates at all times ($\Theta = 1$ with probability $p = 1$), (8) is reduced to,

$$\rho(\Theta = 1) = \frac{\frac{\pi}{4}E_s}{(E_s+\sigma_n^2)} \tag{9}$$

Thus, the correlation coefficient given by (9) provides a threshold to characterize the relay behavior. This can be further established analytically as,

$$\frac{\rho(\Theta)}{\rho(\Theta = 1)} = \mu_{\Theta}\sqrt{\frac{SNR+1}{SNR\mu_{\Theta^2}+1}} \tag{10}$$

where $SNR = \frac{E_s}{\sigma_n^2}$. It can be shown that the first and second moments of Θ are less than *u*nity ($\mu_{\Theta} < 1$, $\mu_{\Theta^2} < 1$). Thus,

$$\rho(\Theta) < \rho(\Theta = 1) \tag{11}$$

As shown above (11), the correlation between signals received in the diversity branch is smaller in the presence of a malicious relay. This result is intuitive as a maliciously modified signal is not statistically similar to the source transmitted signal. In the next section, this result is verified by simulation.

To implement the proposed technique shown in Figure 3, the destination estimates $\rho(\Theta)$ which will then be compared to the ground truth (9). The best estimate of $\rho(\Theta)$ is obtained using a sufficiently large number of received signals at the destination. Suppose the source transmits R_S $Kbits$ in a given symbol duration. The destination may use $x\%$ of those R_S $Kbits$ to estimate $\rho(\Theta)$. Thus, a portion of the symbol duration may be considered as a training period to determine relay's behavior. Note that during the training period, the destination continues to process signals from the two diversity branches. The overhead in implementing the proposed scheme is the additional computation required to learn the behavior of the relay. This overhead is negligible in an uplink transmission where the source transmits to a base station or an access point. At the end of the training period, the destination determines the relay behavior using (11). In case malicious behavior is detected, the destination reverts to direct transmission.

IV. Simulation Results

In [7], it has been shown that bit error probability and outage performance exhibit significant performance degradation due to a semi-malicious relay. In this section, we discuss the bit error probability and outage behavior performance improvement

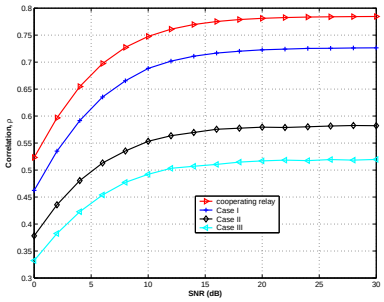

Fig. 4. Correlation between received signals.

due to the proposed scheme. We assume a relay that behaves according to the probability distribution,

$$f_\Theta(\theta) = p_1\delta(\theta-\theta_1)+p_2\delta(\theta-\theta_2)+(1-p_1-p_2)\delta(\theta-\theta_3) \quad (12)$$

According to this model, the relay distorts each correctly decoded signal with probability p_1 and a distortion factor $\theta_1(\theta_1 \ll 1)$. That is, the relay introduces random amplitude distortion. It might also introduce random phase distortion with probability p_2 and distortion factor $\theta_2(\theta_2 < 0)$. This represents the worst malicious behavior. This is because the relay retransmits the BPSK signal after shifting its phase. For instance, $+X_s$ might be the correctly decoded signal at the relay but a malicious relay might send $-X_s$ in place of $+X_s$. That is, the phase distortion due to the malicious relay repositions signals in the BPSK constellation. At the destination, a decision variable is formed by combining (using MRC) received signals ($h_{sd}X_s + n_{sd}$) and ($h_{rd}(-X_s) + n_{rd}$), from the source and relay respectively. Due to this, the destination gets confused as to which signal is transmitted from the source. Thus, it makes decision error with relatively higher probability.

We consider three different cases of (12) to estimate (8) for the purpose of verifying (11). In the first case, the relay introduces only amplitude distortion with probability $p_1(p_1 \ll 1)$ ($p_2 = 0$). In the second case, we consider a relay that introduces only phase distortion ($\theta_2 < 0$) with probability $p_2(p_2 \ll 1)$ ($p_1 = 0$). Finally, we consider a relay that introduces both amplitude and phase distortions with probability $p_1 + p_2$ ($p_1 = p_2$).

For the three different cases, we estimate the correlation between received signals in the two diversity branches to verify the claim in (11). Thus, malicious behavior reduces correlation between the received signals as shown in Figure 4. We also observe that lower correlation is observed when the relay introduces random phase distortion. This supports our argument that malicious phase distortion represents the worst behavior.

The detection technique is applied to the single relay channel where the relay behaves according to (12). We focus evaluation of the technique to two cases, namely, ($p_1 \ll 1, \theta_1 \ll 1,\ p_2 = 0$) and ($p_2 \ll 1, \theta_2 < 0,\ p_1 = 0$). As shown in Figure 5, we observe BER and outage performance improvement with reference to a *dumb* receiver. In the first

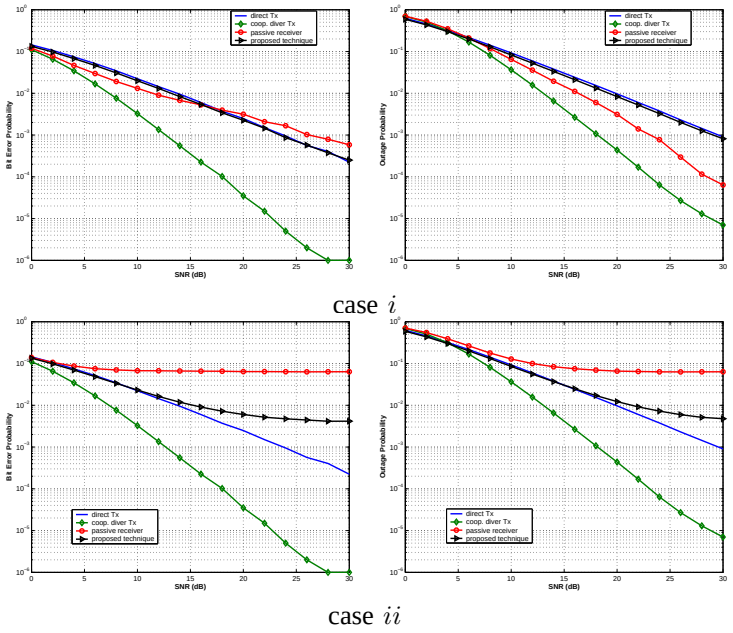

Fig. 5. Proposed detection technique performance.

case, the communications is reverted to direct transmission as shown by the overlap of the BER and outage probability curves. Significant performance improvement is also observed in the second case. However, the performance at high SNR is worse than that of direct transmission. This is due to a significantly long training period which incurs higher cost. We consider various length training periods to show the impact on performance of the detection scheme. As shown in Figure 6, longer training periods incur penalty in terms of relatively higher BER and outage probability. Note that the destination processes all bits within a training period without prior examination.

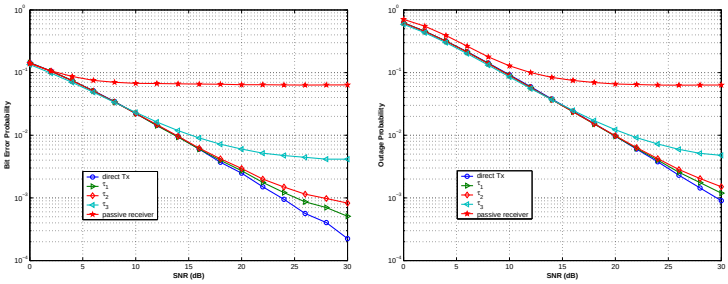

Fig. 6. Proposed detection technique for various training periods, $\tau_1 < \tau_2$ and $\tau_3 \gg \tau_2$.

V. Conclusion and Ongoing Work

In this paper we propose a statistical detection technique to mitigate malicious behavior in adaptive **DF** cooperative diversity. To this end, we introduce a *smart* destination which examines relay's signal prior to applying diversity combining.

In the proposed technique, the *smart* destination computes the correlation between the received signals in the two diversity branches. We showed both analytically and by simulation that malicious activity significantly lowers this correlation. We determine performance of the proposed technique in the presence of a relay that behaves in probabilistic manner. We showed the detection technique improves the BER and outage performance by reverting to single path communication. We also showed the tradeoff between implementing training periods and performance of the proposed technique.

Currently, we investigate cooperative diversity from a game-theoretic point of view which conditions the communication between relay and destination based on a trust and reputation model. The trust/reputation based system will provide the mechanism to detect misbehaving (malicious and selfish) partners and possibly impose penalty on such partners. Such an argument is equally valid in cooperative diversity where relays are characterized by selfish and malicious behavior. For the purpose of trust formation, we model cooperative diversity as a repeated game with one-sided uncertainty where destination maintains beliefs (probability based on past actions) about relay's behavior. Finally, we will extend our approach to other cooperative diversity protocols such as amplify-and-forward.

REFERENCES

[1] T. M. Cover and A. Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572–584, September 1979.

[2] R. U. Nabar, H. Bölcskei, and F. W. Kneubühler, "Fading channels : Performance limits and space-time signal design," *IEEE Journals on Selected Areas in Communications*, vol. 22, no. 6, pp. 1099–1109, August 2004.

[3] E. Zimmerman, P. Herhold, and G. Fettweis, "On the performance of cooperative diversity protocols in practical wireless systems," in *IEEE 58th Vehicular Technology Conference,2003*, vol. 4, IEEE. IEEE, October 2003, pp. 2212–2216.

[4] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity - part i: System description," *IEEE Transaction on Communications*, vol. 51, no. 11, pp. 1927–1938, November 2003.

[5] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 74–80, October 2004.

[6] N. J. Laneman, D. N. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transaction on Information Theory*, vol. 50, no. 12, December 2004.

[7] S. Dehnie, H. T. Sencar, and N. Memon, "Cooperative diversity in the presence of misbehaving relay : Performance analysis," submitted to IEEE Sarnoff Symposium 2007.

[8] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Willey and Sons, 2006.

[9] Y. Mao and M. Wu, "Security issues in cooperative communications: Tracing adversarial relays," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 4, 2006, pp. IV–69–IV–72.

[10] P. Herhold, E. Zimmermann, and G. Fettweis, "A simple cooperative extension to wireless relaying," in *International Zurich Seminar On Communications*, February 2004, pp. 36–39.