A Stochastic Model for Misbehaving Relays in Cooperative Diversity

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

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

Abstract—Existing cooperative diversity protocols are designed with the inherent assumption that users exhibit cooperative behavior all the time. However, in a practical cooperative wireless system users may misbehave in malicious or selfish manner. Thus existing cooperative diversity protocols are inherently vulnerable to misbehaving users as they lack a mechanism to detect the presence of such users. In this paper we examine the physical layer consequences of a malicious user which exhibits cooperative behavior in a stochastic manner. We assume that the malicious user exploits the inherent uncertainty of the wireless channel to hide its malicious behavior. We consider a malicious user which exhibits cooperative and malicious behaviors according to first-order Markov chain. By behaving stochastically the malicious user attempts to mimic the underlying Markov property of Rayleigh fading channels. Based on this model we examine physical layer performance of cooperative Detect-and-Forward (DF). We show that a malicious user incurs significant degradation in cooperative diversity gain. Our results indicate that misbehaving users may pose formidable challenge to practical implementation of cooperative diversity. Hence, it may be difficult to implement practical wireless cooperative networks without a mechanism to ensure cooperation.

I. INTRODUCTION

Cooperative wireless communication avails MIMO-class performance benefits to single-antenna wireless users. The performance benefits are realized through various cooperation strategies such as cooperative Detect-and-Forward (DF) which are designed with the inherent assumption that users always behave according to the cooperation protocol. In other words, existing cooperative diversity protocols inherently attribute a higher degree of trust to all users. However, in a practical wireless cooperative network users may misbehave for malicious or selfish intentions. Thus in the presence of misbehaving users, existing cooperative diversity protocols are vulnerable as they are primarily designed to realize the envisioned performance improvements.

In this paper we examine the physical layer consequences of a malicious user in cooperative Detect-and-Forward (DF). We restrict our analysis to cooperative DF due to the higher degree of trust its attributes to cooperators (relay). That is, a relay is allowed to perform physical layer operations on its partner’s signal such as detection and estimation of the signal before retransmitting to a destination [1]. It is obvious to see that a misbehaving relay may retransmit a maliciously manipulated signal to disrupt communication between its partner and a destination.

In practical wireless cooperative networks malicious behavior may arise when a relay node is compromised by an adversary. Existing physical layer security techniques such as LPD (low probability of detection) may not be effective to detect malicious intentions as they are primarily designed to provide protection against unauthorized sources. Since relays are attributed a high degree of trust, cooperative diversity introduces a new form of vulnerability at the physical layer.

In this work we consider a malicious relay with the disposition to impede communication between sender and receiver. We assume that the malicious relay behaves stochastically to mimic the underlying Markov property of Rayleigh fading channels. We model the stochastic behavior of the relay assuming first-order Markov chain with states designated as cooperative and malicious. The intuition behind such characterization is valid from security viewpoint where users with malicious intentions often exploit system vulnerability to hide their disposition. The unpredictable nature of the wireless channel is one such vulnerability which could be exploited for malicious intentions. It is important to note that the relay exhibits ambiguous behavior as it flip-flops stochastically between the two states. Such ambiguous behavior incurs uncertainty which in the absence of a malicious detection mechanism may be attributed to channel dynamics.

Based on the stochastic relay model, we characterize the performance penalty incurred due to the absence of a mechanism to detect malicious relays in cooperative DF. We show both analytically and by simulation the severe degradation in bit error rate (BER) and diversity performance. Our results reveal that misbehaving users present formidable challenges to the practical implementation of cooperative diversity. Al-
though our observation is based on a three-terminal cooperative network, we believe that it gives a significant insight into the physical layer consequences of malicious relays.

The rest of the paper is organized as follows. The communication channel, modulation scheme and cooperation protocol settings are described in Section II. In Section III, we describe a stochastic model for a misbehaving relay. Section IV describes performance analysis in the presence of a malicious relay. Simulation results are presented in Section V. Finally, we provide summary and concluding remarks.

II. SYSTEM MODEL

A. Channel Model and Communication Scheme

Consider the cooperative wireless network depicted in Fig. 2. In this work an orthogonal transmit scheme is considered, where the source and 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) which is also received by relay (R) due to the broadcast nature of the channel. The received signals at the destination and relay during this time, respectively are:

\[
\begin{align*}
  y_{sd} &= h_{sd}x_s + n_{sd} \\
  y_{sr} &= h_{sr}x_s + n_{sr}
\end{align*}
\]

During this time slot the relay processes the received signal based on DF cooperation strategy. That is, it detects and then generates an estimate \( \hat{x}_s \) of the transmitted signal. During the next time slot \( T_R \), relay transmits \( \hat{x}_s \) to the destination. The received signal at the destination, during time slot \( T_R \) is,

\[
y_{rd} = h_{rd}\hat{x}_s + n_{rd}
\]

where, channel \( h : \{ h_{sd}, h_{sr}, h_{rd} \} \) are statistically independent zero mean complex Gaussian random variables that capture effects of path loss and fading; \( n : \{ n_{sd}, n_{sr}, n_{rd} \} \) are statistically independent zero mean Gaussian random variables with power spectral density \( N_0 \). The channels between the nodes (S-D, S-R and R-D) are statistically independent Rayleigh fading channels. It is assumed that the fading statistics remains constant for two consecutive symbol durations. We define the received instantaneous signal-to-noise ratio (snr) in each channel as \( \gamma_{sd} = \gamma|h_{sd}|^2 \), \( \gamma_{sr} = \gamma|h_{sr}|^2 \), \( \gamma_{rd} = \gamma|h_{rd}|^2 \), where \( \gamma = \frac{E_s}{N_0} \) is received snr per bit without fading. For Rayleigh fading channel, the instantaneous snr \( \gamma_{sd}, \gamma_{sr}, \gamma_{rd} \) are independent and identically chi-square distributed with expected snr denoted by \( \bar{\gamma} \). We assume uncoded BPSK where source signal \( x_s \in \{-\sqrt{E_s}, +\sqrt{E_s} \} \) with \( E[|x_s|^2] \leq E_s \). We assume coherent detection where the channel state information (CSI) is fully known at the receivers. Hence, Maximum Ratio Combining (MRC) technique is considered at the destination.

B. Cooperation Strategy

In this work we consider adaptive Detect-and-Forward (ADF), where the relay cooperates only when the source-relay (S-R) channel is reliable. In this work reliability of the S-R channel is determined based on a quality of service (QoS) requirement, which is defined in terms of an acceptable bit error rate, \( BER \leq P_{QoS}(e) \). The relay can then reliably contribute to the signal quality at the destination if,

\[
|h_{sr}|^2 \geq \frac{\text{erf}^{-1}(1 - 2P_{QoS}(e))^2}{\gamma}
\]

where \( \text{erf}^{-1}(z) \) is inverse of the error function which is defined as \( \text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \). \( P_{QoS}(e) \) is the acceptable bit error rate on the S-R channel. The condition in (3) states that the S-R channel exhibits BER which enables reliable detection at the relay. In the event when the S-R channel is in outage, i.e., (3) does not hold, the source repeats its transmission.

III. A STOCHASTIC MODEL FOR MALICIOUS RELAYS

Modeling relay’s behavior provides a mathematical representation of possible relay actions (cooperative, malicious, selfish, etc.) while providing a tool to characterize system performance. In this section we develop a stochastic model for a malicious relay which attempts to mimic dynamics of the S-R channel. We first revisit (3) to capture the two parameters that have significant impact on relay’s contribution to the signal quality at the destination. Considering (3) it states that a relay with no malicious intentions defers cooperation when the S-R channel is in outage as illustrated in Fig. 3. The S-R channel dynamics and the QoS parameter determine relay’s contribution to the cooperative gain. It is evident that these two parameters are available at the relay. This availability enables a malicious relay to manipulate the parameters to curtail the cooperative gain. We first describe effects of malicious manipulation of the QoS parameter. Assume that relay maliciously reduces the acceptable BER requirement \( P_{QoS}(e) \) to a new value \( P_{mal}(e) \), i.e., \( P_{mal}(e) < P_{QoS}(e) \). Malicious manipulation of the QoS parameter incurs frequent outage on the S-R channel which causes the cooperation region to shrink as illustrated in Fig. 3. As we are considering selection relaying [2] (cooperative ADF), source repeats its transmission to the destination whenever the S-R channel is in outage. Thus malicious manipulation of the QoS parameter causes the source to repeat its transmission more often. Although such malicious behavior may not significantly reduce the cooperative gain due to repetition coding from source to destination, it incurs power penalty to the source. Next we describe a
malicious behavior where relay cooperates ambiguously in a stochastic manner.

We describe briefly the underlying Markov property of slow fading channels. Slow fading channels are characterized by slower channel variations compared to the baseband signal. This indicates correlated fading process as the fading amplitude varies slowly with reference to its rms value. Hence, by properly specifying a threshold for the fading amplitude, the fading process can be approximated with two states, fading and non-fading. A slow fading channel can thus be approximated by a two state Markov chain as described in detail in [3], [4].

Here we describe a malicious relay which mimics the Markov property of slow fading channels. We model behavior of the malicious relay assuming a first-order Markov chain where states are designated as cooperative (C), state 0, and malicious (M), state 1. The states are defined with reference to a threshold which is a function of \( P_{\text{mal}}(e) \) and the received snr measured at the relay.

A first-order Markov chain is defined by its transition probabilities,

\[
\begin{pmatrix}
    p_{00} & p_{01} \\
    p_{10} & p_{11}
\end{pmatrix}
\]  

where the transition probabilities are defined as follows,

\[
\begin{align*}
    p_{00} &= p([h_{sr}(n)] > [h_{\text{mal}}] | [h_{sr}(n-1)] > [h_{\text{mal}}]) \\
    p_{01} &= p([h_{\text{QoS}}] < [h_{sr}(n)] | [h_{sr}(n)] > [h_{\text{mal}}]) \\
    p_{10} &= p([h_{sr}(n)] > [h_{\text{mal}}] | [h_{QoS}] < [h_{sr}(n-1)] < [h_{\text{mal}}]) \\
    p_{11} &= p([h_{QoS}] < [h_{sr}(n)] < [h_{sr}(n-1)] < [h_{\text{mal}}])
\end{align*}
\]

(5)

where, \( [h_{\text{QoS}}] \) is fading amplitude threshold determined based on the QoS requirement and is obtained when (3) is met with equality, \( h_{\text{mal}} \) is determined based on a maliciously modified QoS requirement and it is obtained as

\[
|h_{\text{mal}}|^2 = \frac{\text{erf}^{-1}(1 - 2 P_{\text{mal}}(e))^2}{\gamma}
\]

(6)

We can see from (6) that the transition probabilities depend on system parameters and behavior of relay. Note that relay behaves maliciously only when it can reliably detect the transmitted bits as described in (5). It is important to note that a new form of uncertainty is introduced in R-D channel due to the stochastically behaving relay. In existing diversity protocols this incurred uncertainty is attributed to channel dynamics due to the lack of a detection mechanism. It is interesting to note that the transition probability matrix (4) defines the instantaneous uncertainty due to relay. The long term relay behavior or uncertainty can be obtained from (4) as,

\[
\begin{pmatrix}
    \pi_0 \\
    \pi_1
\end{pmatrix} = \begin{pmatrix}
    p_{10} & p_{01} \\
    p_{01} & p_{10}
\end{pmatrix}
\]

\[
\begin{pmatrix}
    \pi_0 \\
    \pi_1
\end{pmatrix} = \begin{pmatrix}
    \frac{p_{10}}{p_{01} + p_{10}} \\
    \frac{p_{01}}{p_{01} + p_{10}}
\end{pmatrix}
\]

(7)

where \( \pi_0 : \) average probability with which relay cooperates, \( \pi_1 : \) average probability with which relay behaves maliciously. The Markov property we just described captures dynamics of the malicious relay, e.g., its transition from cooperative to malicious state and its long term tendency. However, a model is required to characterize effects of cooperative and malicious states. We model effects of the malicious relay assuming a communication channel which incurs signal distortion in a stochastic manner. To incorporate outcomes of the two states in the system model, (2) is modified where the received signal at the destination incorporating relay’s behavior is,

\[
y_{rd}(\Theta) = h_{rd}(\theta_s \hat{x}_s) + n_{rd}
\]

(8)
where $y_{rd}(\Theta)$ is received signal which is characterized by uncertainty due to relay's behavior and R-D channel dynamics, $\theta_i$ is outcome of the Markov chain in state $i$, $i \in [0, 1]$. It is important to mention that output of malicious state $\theta_i$ depends on the modulation scheme considered. For instance, for BPSK signaling it is defined as,

<table>
<thead>
<tr>
<th>amplitude distortion</th>
<th>$\theta_i \ll 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>phase distortion</td>
<td>$\theta_i = e^{j\pi}$</td>
</tr>
</tbody>
</table>

**TABLE I**

**OUTPUT OF THE MALICIOUS STATE FOR BPSK SIGNALING.**

IV. BIT ERROR RATE (BER) ANALYSIS

In this section we examine BER and diversity performance of cooperative ADF in the presence of a relay that behaves according to the model developed in the previous section. Our analysis is based on the basic assumption in cooperative diversity protocols which attribute a higher degree of trust to the relay. That is, both source and destination assume that relay is always willing to cooperate. We work with this basic assumption to examine the inherent vulnerability in cooperative diversity protocols. We assume that when the S-R channel is in outage (3 does not hold), source repeats its transmission after receiving notification from relay. We argue that relay reliably notifies source when S-R channel is in outage to hide its malicious disposition.

The received signals at the destination from the two diversity branches (S-R and R-D channels) assuming correct detection at the relay is,

$$y_{sd} = h_{sd}x_s + n_{sd}$$
$$y_{rd}(\Theta) = h_{rd}(\theta_i)x_s + n_{rd}$$

where $\theta_i$ is as defined in Table I. Assuming identical noise variance, the diversity combining coefficients at MRC can be shown as, $h_{sd}^*, h_{rd}^*$. Thus the MRC output is given by,

$$y(\Theta) = (|h_{sd}|^2 + |h_{rd}|^2)(\theta_i)x_s + h_{sd}^*n_{sd} + h_{rd}^*n_{rd}.$$  

(10)

From (10) we can see that the desired signal, $\hat{x}_s = (|h_{sd}|^2 + |h_{rd}|^2)\theta_i x_s$ is a function of both channel gain and relay behavior. The instantaneous received snr at the output of MRC is then,

$$\gamma_{adf} = \frac{|h_{sd}|^2 + |h_{rd}|^2}{|h_{sd}|^2 + |h_{rd}|^2}.$$  

(11)

For the uncoded BPSK system under consideration, the Markov chain output is defined in the range: $\theta_i \in [-1, 1]$ where $\theta_i = 1$ captures output of the cooperative state. Then $\gamma_{adf}$ can be approximated as,

$$\gamma_{adf} = \gamma\frac{\theta_i}{|h_{sd}|^2 + |h_{rd}|^2} \leq 1$$
$$|h_{sd}|^2 + |h_{rd}|^2$$

$$\gamma_{adf} \leq \gamma(|h_{sd}|^2 + \theta_i|h_{rd}|^2)$$

(12)

Thus the average received snr, $\gamma_{avg} = E[\gamma_{adf}]$ can be shown as,

$$\gamma_{avg} \leq \gamma (1 + \mu_\theta)$$

(13)

where the Rayleigh distributed fading amplitude has unit mean power and $\mu_\theta$ captures relay’s mean tendency which can be shown to be less than one as $\theta_i \in [-1, 1]$. Thus the average received snr is determined by both channel dynamics and relay’s behavior. For instance, consider the case where relay incurs malicious amplitude distortion, i.e., $\theta_1 \ll 1$ with probability $\pi_1$ (relay cooperates $\theta_0 = 1$ with probability $1 - \pi_1$). Then the mean relay tendency is given as $\mu_\theta = \theta_0(1 - \pi_1) + \theta_1\pi_1 \approx 1 - \pi_1$, since $\theta_1 \ll 1$. The average received snr is then a function of relay behavior as shown,

$$\gamma_{avg} \leq \gamma (2 - \pi_1)$$

(14)

It is obvious to see from (14) that $\gamma_{avg}$ degrades with $\pi_1$. Next we show that $\gamma_{adf}$ exhibits severe degradation when relay maliciously incurs phase distortion. As shown in Table I, for BPSK signaling phase distortion amounts to multiplying a signal by $e^{j\pi}$. In this case the mean tendency of the relay is given by $\mu_\theta = 1 - 2\pi_1$. Thus the $\gamma_{avg}$ is,

$$\gamma_{avg} \leq 2\gamma (1 - \pi_1)$$

(15)

It can be seen from (15) that $\gamma_{avg}$ exhibits severe degradation when relay maliciously incurs phase distortion. This severe degradation in $\gamma_{adf}$ constrains the destination’s ability to perform reliable detection which consequently incurs BER degradation. Next we examine end-to-end BER and diversity performance. The end-to-end BER is given as,

$$P_{adf}(\epsilon, \theta_i|h_{sd}, h_{sr}, h_{rd}) = P(|h_{sr}|^2 \geq t)R_m P_{e}^{\text{mrc}(\theta_i)} + P_{out} P_{e}^d$$

(16)

where $t$ is threshold defined in (3), $P(|h_{sr}|^2 \geq t)$ is probability that S-R channel supports the QoS requirement, $P_{out} = P(|h_{sr}|^2 < t)$ defines outage probability in S-R channel, $P_{e}^r$ is probability of detection at the relay, $P_{e}^{\text{mrc}(\theta_i)} = Q(\sqrt{2\gamma_{adf}})$ is BER given MRC output, $P_{e}^d$ is BER for repetition coding from source to destination and $Q(x) = \frac{1}{\sqrt{2\pi}} \int_{x}^{\infty} e^{-\frac{z^2}{2}} dz$. For the purpose of simplifying the exposition, we assume that $P(|h_{sr}|^2 < t) \ll 1$ which indicates that relay makes negligibly small detection errors. Thus using the approximation (12) the instantaneous end-to-end BER can be approximated as,

$$P_{adf}(\epsilon, \theta_i|h_{sd}, h_{sr}, h_{rd}) \approx Q(\sqrt{2\gamma_{adf}}) \leq e^{-\frac{gamma_{adf}}{2}}$$

(17)

where the inequality is due to Chernoff bound, $Q(x) \leq e^{-\frac{x^2}{2}}$. It can be seen that the end-to-end BER is a function of system uncertainty which is characterized by channel dynamics and stochastic relay behavior. In order to examine impact of relay’s
behavior on the cooperative diversity gain, we consider the end-to-end BER averaged over channel statistics. The average BER is,

\[ P_{\text{avg}}(e, \theta_i) \leq \int_0^\infty \int_0^\infty e^{-\gamma(h_{sd}|^2 + |h_{rd}|^2)} f(h_{sd}, h_{rd}) dh_{sd} dh_{rd} \]

as the Rayleigh fading statistics \(|h_{sd}|^2, |h_{rd}|^2\) are independent and exponentially distributed with unit mean:

\[ P_{\text{avg}}(e, \theta_i) \leq \int_0^\infty 2h_{rd} e^{-(|h_{rd}|^2(\gamma_{\theta_i}+1))} dh_{rd} \times \int_0^\infty 2h_{sd} e^{-(|h_{sd}|^2(\gamma_{\theta_i}+1))} dh_{sd} \]

At high SNR the average BER behaves as

\[ P_{\text{avg}}(e, \theta_i) \leq \frac{1}{(\theta_i \gamma_{\text{avg}} + 1)(\gamma_{\text{avg}})} \] (18)

It is evident from (18) that the diversity performance is determined by uncertainty incurred due to stochastic behavior of the relay. In the special case where relay exhibits deterministic cooperative behavior (\(\theta_i = 1, \pi_0 = 1\)), it can be shown that cooperative ADF exhibits second-order diversity. To characterize the impact of a stochastically behaving relay on the diversity performance, we examine the high SNR behavior of (18) averaged over \(\theta_i\), i.e., \(P_{\text{avg}}(e) \leq \sum_{k=1}^n P_{\text{avg}}(e, \theta_i) P(k = i)\). The high SNR behavior of the average BER as a function of relay behavior is,

\[ P_{\text{avg}}(e) \leq \frac{\pi_0}{(\gamma_{\text{avg}})^2} + \frac{\pi_1}{(\theta_i \gamma_{\text{avg}} + 1)(\gamma_{\text{avg}})^2} \] (19)

where \(P(k = \theta_i) = \pi_1\) (7). It is obvious to see from (19) that the diversity performance depends on Markov chain parameters \(\pi_0\) and \(\pi_1\) and outcome of the malicious state. For instance, in the presence of a relay with no malicious intentions, i.e., \(\pi_0 = 1\), cooperative ADF exhibits second-order diversity \(P_{\text{avg}}(e) \leq (\gamma_{\text{avg}})^2\). In the presence of a malicious relay, the diversity performance is limited by \(\pi_1\) and outcome of the malicious state. In the next section we quantify the degradation in cooperative diversity gain.

In this section we have shown the performance degradation in cooperative ADF due to a stochastically behaving malicious relay. Although the performance analysis is highly ideal, we believe that it provides a significant insight into the physical layer consequences of misbehaving relays in cooperative diversity.

V. BIT ERROR SIMULATION RESULTS

In this section, we quantify the degradation in BER and diversity performance in the presence of a malicious relay. In our simulation we consider a wireless system with acceptable uncoded BER of \(10^{-2}\). We assume that the malicious relay incurs signal distortion with average probability \(\pi_1\), where the distortion factors are as described in Table I. We first examine performance of cooperative ADF assuming a relay with no malicious intention.

Consider a relay which behaves according to the cooperation strategy with probability \(\pi_0 = 1\). In this case the relay contributes significantly to the signal quality at the destination. It is evident that cooperative ADF exhibits significant performance improvement in terms of BER and diversity performance. For instance at BER of \(4 \times 10^{-4}\), the cooperative diversity gain is about 12 dB over SISO as shown in Fig. 6. Note that this gain is due to repetition coding from the source and relay to destination. In terms of diversity performance, cooperative ADF exhibits second-order diversity as can be observed from the high SNR behavior of the BER curve (labeled SIMO in Fig. 6). Next we examine how this attained performance is affected due to a lack of mechanism to detect a malicious behavior. For the purpose of simplifying the exposition, we consider malicious amplitude and phase distortion separately.

Consider a malicious relay which incurs amplitude distortion with average probability \(\pi_1\), i.e., the relay transmits a signal with attenuated amplitude with probability \(\pi_1\). In this case it is obvious to see that that cooperative ADF exhibits degradation in repetition coding gain. To quantify the incurred degradation in repetition coding gain, we consider various levels of maliciousness as measured by \(P_{\text{mal}}(e)\), i.e., \(P_{\text{mal}}(e) < P_{\text{QoS}}(e)\). Note that \(P_{\text{mal}}(e)\) is arbitrarily chosen for the purpose of simplifying the exposition. First consider a malicious relay which modifies the QoS requirement from \(10^{-2}\) to \(P_{\text{mal}}(e) = 5 \times 10^{-3}\). In this case cooperative ADF exhibits slight degradation in repetition coding gain compared to SIMO as shown in Fig. 6. For instance, at BER of \(4 \times 10^{-4}\) the coding gain is about 10 dB over SISO. However, at the same BER there is performance loss of about 2 dB with respect to SIMO (fully cooperating relay). As we slightly increase the level of maliciousness to \(P_{\text{mal}}(e) = 10^{-3}\), we observe significant degradation in coding gain. At the same BER of \(4 \times 10^{-4}\), the gain over SISO is about 7 dB. This corresponds to a performance loss of about 5 dB with respect to SIMO. In terms of diversity performance, the system exhibits second-order diversity as shown in Fig. 6. As we will show next, cooperative ADF exhibits severe degradation due to malicious phase distortion.

In BPSK signaling, phase distortion amounts to transmitting a signal which is \(180^\circ\) out of phase with the signal transmitted from source. Suppose that \(+x\) is transmitted from source and that it is reliably detected at the relay. A relay with malicious intentions will transmit \(-x\) to destination to severely impede communication between source and destination. In this case the decision variable at the output of MRC is,

\[ \hat{x} = (|h_{sd}|^2 - |h_{rd}|^2)x + h_{sd}n_{sd} + h_{rd}n_{rd} \] (20)

It can be seen from (20) that probability of correct decision is conditioned on \(|h_{sd}|^2 > |h_{rd}|^2\) due to the malicious transmission from the relay. It can be shown that \(p(|h_{sd}|^2 > |h_{rd}|^2) = \frac{1}{2}\) assuming iid Rayleigh fading channels. Thus malicious phase distortion increases uncertainty of detecting the
transmitted signal at the destination, which leads to frequent detection errors. Consequently cooperative ADF will exhibit severe degradation in repetition coding gain. To quantify the amount of incurred degradation, we consider two levels of maliciousness. We first consider a malicious relay which degrades the QoS requirement to BER of $P_{\text{mal}}(e) = 7.5 \times 10^{-3}$. In this case at BER of $5 \times 10^{-4}$, cooperative ADF exhibits 3 dB repetition coding gain over SISO as shown in Fig. 7. As we increase the level of maliciousness to $P_{\text{mal}}(e) = 10^{-3}$, it can be observed from Fig. 7 that BER exhibits severe degradation. At BER of $3 \times 10^{-3}$ the performance is about 6 dB worse than that of SISO. It is evident from Fig. 7 that the BER curve runs parallel to that of SISO. This indicates that cooperative ADF exhibits first-order diversity. Hence, the diversity performance is degraded to SISO in the presence of a relay which incurs malicious phase manipulation.

VI. CONCLUSION AND CURRENT EFFORTS

In this paper we characterize the inherent vulnerability of cooperative diversity in the presence of a misbehaving relay. This vulnerability arises as a result of the assumption that relays conform to the cooperation strategy at all times. However, in practice there are no mechanisms to ensure that a relay adheres to the rules of cooperation. To characterize the performance penalty due to the lack of such mechanism, we consider a relay which mimics the underlying Markov property of slow fading channels. We model maliciousness as a stochastic process where relay exhibits cooperative and malicious behavior according to first-order Markov chain. Based on this model, we present detailed performance analysis of cooperative ADF. We showed analytically that a malicious relay significantly degrades the cooperative diversity gain. We quantify by simulation the degradation in BER and diversity order for various levels of maliciousness. In the presence of a relay which incurs malicious phase distortion, cooperative ADF exhibits first-order diversity. Our results indicate that without a mechanism to ensure cooperation, it may be difficult to implement a practical cooperative wireless network. Currently, we are looking at cooperative diversity within a game theoretic framework which conditions the cooperation between source and relay on an established level of trust/reputation.

REFERENCES