NONCOHERENT MISBEHAVIOR DETECTION IN SPACE-TIME CODED COOPERATIVE NETWORKS

Li-Chung Lo, Zhao-Jie Wang and Wan-Jen Huang

National Sun Yat-Sen University, Institute of Communications Engineering
Kaohsiung 80424, Taiwan

ABSTRACT

Consider a two-relay decode-and-forward (DF) cooperative network where Alamouti coding is adopted among relays to exploit spatial diversity. However, the spatial diversity gain is diminished with the existence of misbehaving relays. Most existing work on detecting malicious relays requires the knowledge of instantaneous channel status, which is usually unavailable if the relays garble retransmitted signals deliberately. With this regard, we propose a noncoherent misbehavior detection using the second-order statistics of channel estimates for relay-destination links. It shows from simulation results that increasing the number of received blocks provides significant improvement even at low SNR regime.

Keywords: Cooperative communications, Misbehavior detection, Channel estimation, Noncoherent detection

1. INTRODUCTION

Cooperative communications [1–3] have drawn wide attention to the development of wireless broadband communications. With intelligent sharing of radio resources, cooperative systems allow users with single antenna to exploit spatial diversity by mimicking multi-input-multi-output (MIMO) systems. Furthermore, numerous cooperative strategies have been developed from physical to MAC to network layers in order to further enhance spectral or energy efficiency [3]. However, most of these strategies provide significant performance gain under an important assumption that relays are fully cooperative and trustworthy at all times. In adversarial environments, some relays may behave selfishly by preserving its transmission power for its own use or behave maliciously by garbling the forwarded symbols deliberately. In these cases, the cooperative systems could be broken down severely, which are even worse than non-cooperative systems.

To determine whether a relay misbehaves, several tracing-based and blind detection methods have been investigated in [4–9] for cooperative networks. In tracing-based schemes, tracing symbols which are often generated by pseudo-random number generator (PRNG) are inserted among source messages in a random manner [4–6]. In case the relay avoids misbehavior detections, generating key of the PRNG and locations of the tracing symbols are known only at the source and the destination. After extracting and demodulating the tracing symbols sent by each relay, the destination performs misbehavior detection according to the correlation between tracing symbols received from each relay and their exact values generated from PRNG. On the other hand, blind schemes have been proposed by comparing the correlation between signals received from the source and each relay [7–9]. Blind misbehavior detection is more bandwidth-efficient since no tracing symbol is required, but it demands reliable link between the source and destination. The aforementioned misbehavior detections work well under an assumption that instantaneous channel state information (CSI) is perfectly known at the destination. Nevertheless, symbols retransmitted by a malicious relay could be garbled randomly, which leads to questionable channel estimates and in consequence misdetections of malicious relays. Therefore, misbehavior detection becomes challenging if the instantaneous CSI is not available at the destination.

In this work, we consider a space-time coded cooperative network where two relays adopt decode-and-forward (DF) protocol. It is assumed that both relays decode source message reliably to focus our discussions on misbehavior detection. To deal with the challenge of no channel information, our proposed scheme begins with channel estimation of the relay-destination links based on the received tracing symbols. Under assumption of Rayleigh and block faded channels, these channel estimates have distinguishable statistical properties when either relay or both relays misbehave. Therefore, we proposed a two-stage misbehavior detection according to the second-order statistics of channel estimates between relays and the destination. In the first stage, we first determine whether one of the relays misbehaves or both relays have consistent behavior based the difference between variances of two channel estimates averaged over all possible channel realizations. Next, the cases of both relays behaving cooperatively or maliciously are further distinguished according to the variances of channel estimates given some channel realization. Through computer simulations, it shows that detection performance depends more on the number of received blocks than the transmission power. Increasing the number of received blocks results in significant improvement even at low SNR regime.

2. SYSTEM MODEL

We consider a canonical cooperative network where one user acts as a source, and two cooperating partners serve as relays by forwarding the source's information to the destination. In this work, we assume that the source-destination channel is weak due to path loss and shadowing effects. The cooperative transmission is accomplished in two phases. In phase I, the source transmits a block of K symbols, which are modulated by quadrature phase-shift keying (QPSK) with unit energy. Let $\mathbf{x}_s^{(n)} = [x_s^{(n)}[1], x_s^{(n)}[2], \cdots, x_s^{(n)}[K]]^T$ be the n-th block transmitted by the source. Among each block, B tracing symbols have been inserted to perform misbehavior detection. After receiving signal, each relay proceeds to decode the source block and retransmit it after applying space-time coding. To focus our discussion on the behavior of relays, we assume that both relays can reliably decode each source block. Let $\hat{x}_\ell^{(n)}[k]$ be the k-th symbol

This research was supported in part by the National Science Council, Taiwan, under grant NSC-100-2221-E-110-062

retransmitted by the relay ℓ during the n-th block period. During the n-th block period of Phase II, the k-th symbol received at the destination is given by

$$y_d^{(n)}[k]=\sqrt{\frac{P_r}{2}}\left(h_{1,d}^{(n)}\hat{x}_1^{(n)}[k]+h_{2,d}^{(n)}\hat{x}_2^{(n)}[k]\right)+w_d^{(n)}[k], \quad (1)$$

where P_r is total transmission power of the relays, $h_{\ell,d}^{(n)}$ is channel coefficient between relay ℓ and the destination during the n-th block period, and $w_d^{(n)}[k]$ is additive white Gaussian noise (AWGN) occurred at the destination with variance σ_w^2. In this work, all channels are Rayleigh and block faded with variance σ_h^2, and the channel coefficients vary independently block-by-block.

To be more specifically, symbols retransmitted by each relay can be modeled as

$$\hat{x}_\ell^{(n)}[k]=\theta_\ell^{(n)}[k]x_\ell^{(n)}[k], \ell=1,2 \quad (2)$$

where $\theta_\ell^{(n)}[k]$ is a random variable with distribution depending on the misbehaving pattern of the relay ℓ [7], and $x_\ell^{(n)}[k]$ is space-time codeword of the relay ℓ using Alamouti scheme, *i.e.,*

$$\begin{bmatrix} x_1^{(n)}[2m-1] & x_2^{(n)}[2m-1] \\ x_1^{(n)}[2m] & x_2^{(n)}[2m] \end{bmatrix}=\begin{bmatrix} x_s^{(n)}[2m-1] & x_s^{(n)}[2m] \\ -(x_s^{(n)}[2m])^* & (x_s^{(n)}[2m-1])^* \end{bmatrix}.$$

If a relay is fully cooperative, $\theta_\ell^{(n)}[k]$ equals to one at all times. If both relays are trustworthy, the constellation points of received symbols within a block period are mostly centered at one of 16 signal points. On the other hand, a misbehaving relay may alter the phase or amplitude of the retransmitted symbols randomly. Consider that either or both relays arbitrary change the phase and amplitude of the retransmitted symbols randomly. In this case, the constellation points of the received symbols have different distribution from those of fully cooperative case, which can be easily detected from the statistics of received symbols in quasi-static fading environment. However, if a misbehaving relay simply garbles the retransmitted symbols as one of other QPSK signal points randomly, it is hard to distinguish whether the relay misbehaves from the statistics of received signals. With this regards, we consider the misbehaving pattern, *i.e.,* $\{\theta_\ell^{(n)}[k]\}$ are *i.i.d.* with probability mass function (PMF)

$$\Pr\left\{\theta_\ell^{(n)}[k]=e^{\frac{jq\pi}{2}}\right\}=\frac{1}{4}, \quad q=0,1,2,3.$$

The distribution of $\theta_\ell^{(n)}[k]$ is assumed available at the destination based on the record of misbehavior detections.

3. STATISTICS OF CHANNEL ESTIMATES

After signal reception during phase II, the destination first proceeds to generate a sequence of channel estimates of each relay-destination link using received tracing symbols. Under quasi-static fading environment, the channel estimates within the same block period shall be approximately consistent especially at high SNR regime. Thus, the statistical properties of the sequence of channel estimates can be employed to perform misbehavior detection. Different from the training symbols used in conventional channel estimation, the values and positions of tracing symbols are pseudo-random and only known at the destination. The underlying reason is to prevent the relays from being aware of the existence of tracing symbols and avoiding misbehavior detection. Since Alamouti code is applied among the relays, the tracing symbols are inserted pairwisely. Let $[x_s^{(n)}[2L_i-1], x_s^{(n)}[2L_i]]$ be the i-th pair of tracing symbols inserted in the n-th source block, where L_i indicates its position. The corresponding received vector $\mathbf{y}_i^{(n)}\triangleq[y_d^{(n)}[2L_i-1], y_d^{(n)}[2L_i]]^T$ is

$$\mathbf{y}_i^{(n)}=\sqrt{P_r}\hat{\mathbf{X}}_i^{(n)}\mathbf{h}^{(n)}+\mathbf{w}_i^{(n)}, i=1,2,\cdots,B \quad (3)$$

where

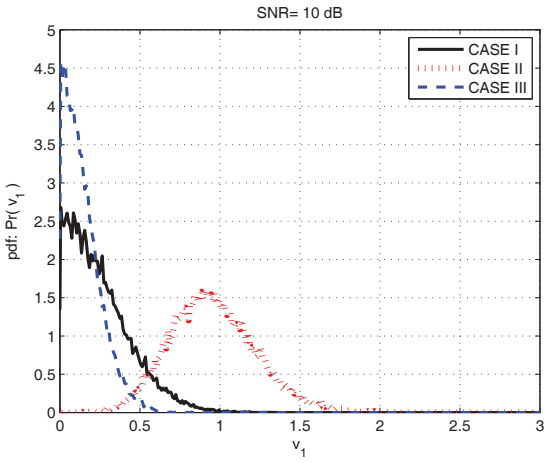

Fig. 1. The empirical PDFs of v_1 conditioning on the cases with $N=20$ given $B=10$ and $SNR=10$ dB

$$\hat{\mathbf{X}}_i^{(n)}=\frac{1}{\sqrt{2}}\begin{bmatrix} \hat{x}_1^{(n)}[2L_i-1] & \hat{x}_2^{(n)}[2L_i-1] \\ \hat{x}_1^{(n)}[2L_i] & \hat{x}_2^{(n)}[2L_i] \end{bmatrix},$$

$\mathbf{h}^{(n)}=[h_{1,d}^{(n)}, h_{2,d}^{(n)}]^T$, and $\mathbf{w}_i^{(n)}=[w_d^{(n)}[2L_i-1], w_d^{(n)}[2L_i]]^T$ is a Gaussian noise vector. Note that $\mathbf{X}_i^{(n)}$ is unitary when both relays are fully cooperative. In this case, the least-square (LS) channel estimate $\hat{\mathbf{h}}_i^{(n)}\triangleq[\hat{h}_{1,d}^{(n)}[L_i], \hat{h}_{2,d}^{(n)}[L_i]]^T$ equals to

$$\hat{\mathbf{h}}_i^{(n)}=\frac{1}{\sqrt{P_r}}(\mathbf{X}_i^{(n)})^H\mathbf{y}_i^{(n)}=\mathbf{\Theta}_i^{(n)}\mathbf{h}^{(n)}+\tilde{\mathbf{w}}_i^{(n)}, \quad (4)$$

where

$$\mathbf{\Theta}_i^{(n)}=\begin{bmatrix} \psi_{1,i}^{(n)} & (x_s^{(n)}[2L_i-1])^* x_s^{(n)}[2L_i]\zeta_{2,i}^{(n)} \\ -x_s^{(n)}[2L_i-1](x_s^{(n)}[2L_i])^*\zeta_{1,i}^{(n)} & \psi_{2,i}^{(n)} \end{bmatrix},$$

$\psi_{\ell,i}^{(n)}=\frac{1}{2}(\theta_\ell^{(n)}[2L_i]+\theta_\ell^{(n)}[2L_i-1])$, $\zeta_{\ell,i}^{(n)}=\frac{1}{2}(\theta_\ell^{(n)}[2L_i]-\theta_\ell^{(n)}[2L_i-1])$, and $\tilde{\mathbf{w}}_i^{(n)}$ is a circularly symmetric Gaussian random vector with covariance matrix $\frac{\sigma_w^2}{P_r}\mathbf{I}$. Both $\psi_{\ell,i}^{(n)}$ and $\zeta_{\ell,i}^{(n)}$ have zero mean and variance $\frac{1}{2}$ when relay ℓ misbehaves.

The second-order statistical properties of the channel estimates depend on behavior of two relays. In the following, we will explore the channel estimates based on three different cases.

Case I : When both relays are fully cooperative, we have $\mathbf{\Theta}_i^{(n)}=\mathbf{I}$. Conditioning on a channel realization $\mathbf{h}^{(n)}$, means and variances of each channel estimates are

$$\mathbf{E}\left[\hat{h}_{\ell,d}^{(n)}[L_i]|\mathbf{h}^{(n)}\right]=h_{\ell,d}^{(n)}, \quad \ell=1,2, \quad (5)$$

$$\mathrm{Var}\left(\hat{h}_{\ell,d}^{(n)}[L_i]|\mathbf{h}^{(n)}\right)=\frac{\sigma_w^2}{P_r}, \quad \ell=1,2. \quad (6)$$

It shows that unbiased channel estimates can be obtained with cooperative relays. Furthermore, variances of the channel estimates averaged over all channel realizations equal to

$$\mathrm{Var}\left(\hat{h}_{\ell,d}^{(n)}[L_i]\right)=\sigma_h^2+\frac{\sigma_w^2}{P_r}, \quad \ell=1,2. \quad (7)$$

Case II : Consider one of the relay, say relay ℓ_m, is malicious. It can be verified that conditional means and variances given channel realization $\mathbf{h}^{(n)}$ are

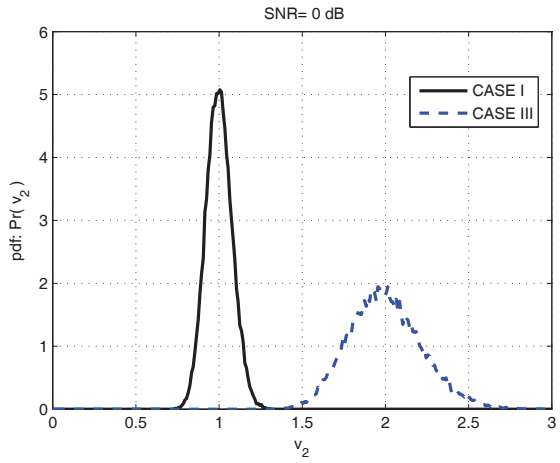

Fig. 2. The empirical PDFs of v_2 conditioning on the cases with $N = 20$ given $B = 10$ and $SNR = 0$ dB

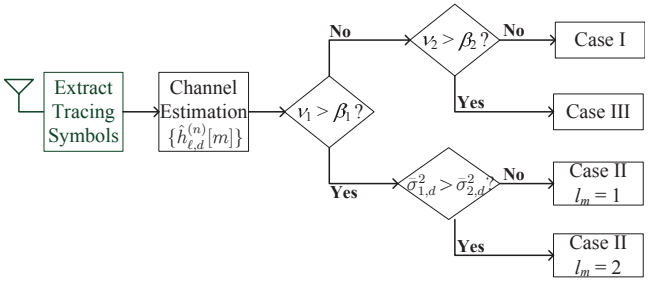

Fig. 3. Block diagram of the proposed misbehavior detection.

$$\mathbf{E}\left[\hat{h}_{\ell,d}^{(n)}[L_i]|\mathbf{h}^{(n)}\right] = \begin{cases} h_{\ell,d}^{(n)}, & \ell \neq \ell_m, \\ 0, & \ell = \ell_m, \end{cases} \tag{8}$$

$$\mathrm{Var}\left(\hat{h}_{\ell,d}^{(n)}[L_i]|\mathbf{h}^{(n)}\right) = \frac{1}{2}|h_{\ell_m,d}^{(n)}|^2 + \frac{\sigma_w^2}{P_r}, \quad \ell = 1, 2. \tag{9}$$

It implies that it is by no mean to estimate the channel coefficient between the misbehaving relay and the destination. The variances of the channel estimates for all possible channel realizations are

$$\mathrm{Var}\left(\hat{h}_{\ell,d}^{(n)}[L_i]\right) = \begin{cases} \frac{3}{2}\sigma_h^2 + \frac{\sigma_w^2}{P_r}, & \ell \neq \ell_m, \\ \frac{\sigma_h^2}{2} + \frac{\sigma_w^2}{P_r}, & \ell = \ell_m. \end{cases} \tag{10}$$

Case III : When both relays are malicious, means and variances of the channel estimates conditioning on channel realization $\mathbf{h}^{(n)}$ are

$$\mathbf{E}\left[\hat{h}_{\ell,d}^{(n)}[L_i]|\mathbf{h}^{(n)}\right] = 0, \quad \ell = 1, 2, \tag{11}$$

$$\mathrm{Var}\left(\hat{h}_{\ell,d}^{(n)}[L_i]|\mathbf{h}^{(n)}\right) = \frac{1}{2}\|\mathbf{h}^{(n)}\|^2 + \frac{\sigma_w^2}{P_r}, \quad \ell = 1, 2. \tag{12}$$

Moreover, if we consider all possible channel realizations, variances of the channel estimates are

$$\mathrm{Var}\left(\hat{h}_{\ell,d}^{(n)}[L_i]\right) = \sigma_h^2 + \frac{\sigma_w^2}{P_r}, \quad \ell = 1, 2. \tag{13}$$

4. MISBEHAVIOR DETECTION

According to the statistics of channel estimates described in Sec.3, we propose a two-stage method to determine misbehaving relays. In the first stage, we first examine whether both relays behaves consistently. From (7) and (13), two channel estimates have identical variances when both relays behaves cooperatively or maliciously. On the other hand, it shows form (10) that the estimate of the channel from the misbehaving relay to the destination has lower variance when either user is adversarial. Denote sample variance of $\hat{h}_{\ell,d}^{(n)}$ as

$$\bar{\sigma}_{\ell,d}^2 = \frac{1}{N \times B - 1} \sum_{n=1}^{N} \sum_{i=1}^{B} |\hat{h}_{\ell,d}^{(n)}[L_i] - \bar{u}_\ell|^2, \tag{14}$$

where $\bar{u}_\ell$ is the corresponding sample mean,

$$\bar{u}_\ell = \frac{1}{N \times B} \sum_{n=1}^{N} \sum_{i=1}^{B} \hat{h}_{\ell,d}^{(n)}[L_i].$$

Define a testing statistic of the first stage as the absolute difference between variances of two channel estimates, *i.e.,*

$$\nu_1 \triangleq |\bar{\sigma}_{1,d}^2 - \bar{\sigma}_{2,d}^2|. \tag{15}$$

Empirical PDFs of ν_1 conditioning on three cases are illustrated in Fig.1 at SNR$=$ 10 dB. In this stage, one can determine whether case I or case III occurs if $\nu_1 \leq \beta_1$; otherwise, case II occurs. The threshold β_1 can be predetermined numerically based on Maximum-a-Posteriori (MAP) criterion. Furthermore, if case II is identified, one may detect relay ℓ_m is malicious if $\bar{\sigma}_{\ell_m,d}^2$ is minimal.

In the second stage, we further determine whether both relays is trustworthy or misbehaving according to the conditional variances expressed in (6) and (12). Denote the sample variance of $\hat{h}_{\ell,d}^{(n)}$ conditioning on channel state $\mathbf{h}^{(n)}$ as

$$(\check{\sigma}_{\ell,d}^{(n)})^2 = \frac{1}{B-1} \sum_{i=1}^{B} \left|\hat{h}_{\ell,d}^{(n)}[L_i] - \check{u}_\ell^{(n)}\right|^2, \tag{16}$$

where $\check{u}_\ell^{(n)}$ is the corresponding conditional sample mean

$$\check{u}_\ell^{(n)} = \frac{1}{B} \sum_{i=1}^{B} \hat{h}_{\ell,d}^{(n)}[L_i].$$

The difference of two variances in (6) and (12) depends on the instantaneous channel gain of two relay-destination links. If both links are in deep fade, it is highly possible to mis-detect as case I or case III. To eliminate the effect of channel fading, define the testing statistic of the second stage as the conditional variance averaged over two channel estimates and N block periods, *i.e.,*

$$\nu_2 = \frac{1}{2N} \sum_{n=1}^{N} \sum_{\ell=1}^{2} (\check{\sigma}_{\ell,d}^{(n)})^2. \tag{17}$$

Empirical PDFs of ν_2 conditioning on case I and case III are illustrated in Fig.2 at SNR$=$ 0 dB. In the second stage, we can determine that both relays are fully cooperative if $\nu_2 \leq \beta_2$. Otherwise, both relays are detected as malicious ones. Similarly, the threshold β_2 can be predetermined numerically. The block diagram of the proposed misbehavior detection scheme is illustrated in Fig.3.

5. COMPUTER SIMULATIONS

In this section, we demonstrate detection performance of the proposed misbehavior detection scheme through computer simulations. In this section, the channel coefficients, $h_{2,d}$ and $h_{1,d}$ are *i.i.d.* complex Gaussian distributed with zero mean and unit variance and variances of Gaussian white noises $w_d^{(n)}[k]$ are normalized to one. Transmission power of the source is assumed equal to the total power of two relays, *i.e.,* $P_s = P_r \triangleq \texttt{SNR}$. In each source block, $B = 10$ tracing symbols have been inserted. The a priori probability that any relay misbehaves is $P_{\mathrm{m}} = 0.1$, which is assumed perfectly known at the destination. In Figs.4–6, detection error probabilities

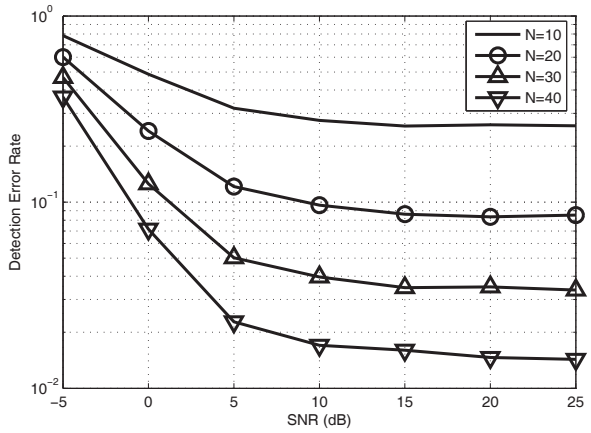

Fig. 4. Probabilities of detection errors occurred during the first stage 1 with various N and $B = 10$.

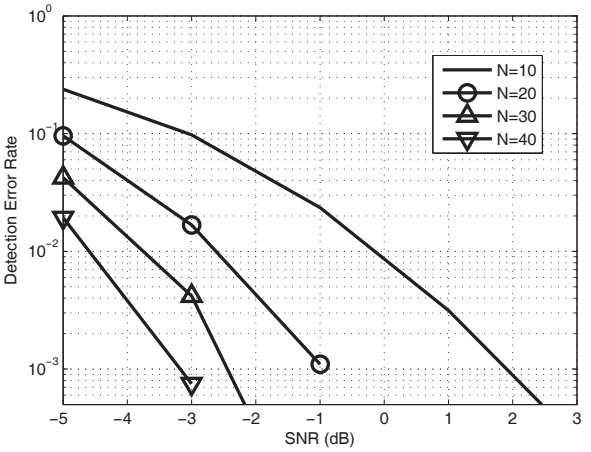

Fig. 5. Probabilities of detection errors occurred during the second stage 1 with various N and $B = 10$.

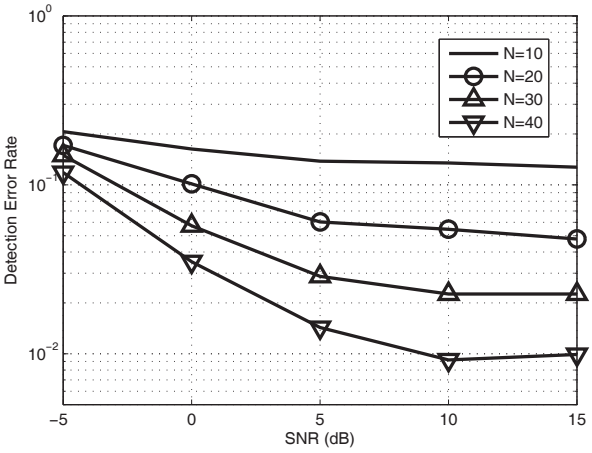

Fig. 6. Probability of overall detection errors for the proposed misbehavior detection scheme with various N and $B = 10$

of the proposed scheme in terms of SNR are compared under various number of received block collected for misbehavior detection. In Fig.4 and Fig.5, we demonstrate detection error probabilities of the first stage and the second stage, respectively. In Fig.4, it shows that raising transmission power results in limited performance improvement during the first stage. Moreover, increasing the number of received block leads to significant performance gain. The reason is that the testing statistic of the first stage is to estimate the difference between variances of two channel estimates averaged over all possible channel realizations. Thus, accuracy of the testing statistic highly depends on the value of N. As shown in Fig.5, the value of transmit SNR brings more improvement in the second stage. Moreover, the detection error probability occurred in the second stage is much less than that of the first stage. Therefore, the overall detection error probability, as shown in Fig.6, is dominated by the detection errors occurred in the first stage. Therefore, allowing sufficient time to collect received blocks is more critical in our proposed scheme than increasing transmission power.

6. CONCLUSION

This paper proposed a misbehavior detection scheme for DF space-time coded cooperative networks. In the absence of perfect CSI, the destination performs misbehavior detection by exploiting the statistical properties of channel estimates. Simulation results show that increasing number of received blocks can improve detection probability effectively.

7. REFERENCES

[1] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity – Part I: System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, no.12, Dec. 2004.

[3] Y.-W. Hong, W.-J. Huang, F.-H. Chiu, and C.-C. J. Kuo, "Cooperative communications in resource-constrained wireless networks," *IEEE Signal Processing Mag.*, vol. 24, no. 3, pp. 47–57, May 2007.

[4] Y. Mao and M. Wu, "Security issues in cooperative communications: Tracing adversarial relays," in *Proc. of the IEEE ICASSP*, pp. IV69–IV72, 2006.

[5] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," in *IEEE Trans. on Information Forensics and Security*, vol.2, no.2, pp. 198–212, Jun. 2007.

[6] T. A. Khalaf and S. W. Kim; "Error probability in multi-source, multi-relay networks under falsified data injection attacks," in *Proc. of IEEE Military Communications Conference (MILCOM)*, Nov. 2008.

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

[8] Y. Liu, Y. Wu, and J. Tang, "Two tier detection model for misbehavior of low-power nodes in virtual MIMO based wireless networks," in *Proc. of IEEE International Conf. on Information Assurance and Security (IAS)*, pp. 155–160, Aug. 2010.

[9] S. Dehnie, H. Sencar, and N. Memon, "Detecting malicious behavior in cooperative diversity," in *Proc. of the Conf. on Information Science and Systems* (CISS), pp. 895–899, 2007.