SECURITY ISSUES IN COOPERATIVE COMMUNICATIONS: TRACING ADVERSARIAL RELAYS

Yinian Mao and Min Wu

Department of ECE, University of Maryland, College Park, MD, USA

ABSTRACT

Cooperative communication system explores a new dimension of diversity in wireless communications to combat unfriendly wireless environment through strategic relays. While this emerging technology is promising in improving communication quality, some security problems inherent to cooperative relay also arise. In this paper we investigate the security issues in cooperative communications that consist of multiple relay nodes using decode-and-forward strategy. In particular, we consider the situation where one of the relay nodes is adversarial and tries to corrupt the communications by sending garbled signals. We show that the conventional physical-layer signal detection will not be effective in such a scenario, and the application-layer cryptography alone is not sufficient to identify the adversarial relay. To combat adversarial relay, we propose a cross-layer scheme that uses pseudo-random tracing symbols, with an adaptive signal detection rule at the physical layer, and direct sequence spread spectrum symbol construction at the application layer for tracing and identifying adversarial relay. Our experimental simulations show that the proposed tracing scheme is effective and efficient.

1. INTRODUCTION

Cooperative communication system explores a new dimension of diversity in wireless communications to combat unfriendly wireless environment. Consider a simple example in Fig. 1, where node A is transmitting to node B, the direct transmission link may be obstructed for geological reasons. In such a scenario, two other nodes C and D between A and B, can serve as relay nodes to improve the communication quality. Among the strategies employed by the relay nodes, amplify-and-forward and decode-and-forward are two most straightforward strategies [1]. In amplify-and-forward, the relay nodes simply boost the energy of the signal received from sender and re-transmit to the receiver. Such a strategy may also amplify the noise in the received signal at the relay nodes. In decode-and-forward, the relay nodes will perform physical layer decoding (demodulation plus signal detection) and then forward the decoding result. When multiple relay nodes are available, more sophisticated relay strategy can be employed. For example, the relay nodes can employ space-time code to transmit relay signals [2][3][4]. However, the involvement of multiple relay nodes also poses a challenge to the reliability of the relay information. In an adversarial environment, the relay nodes could be compromised. Potentially, the compromised nodes can maliciously modify the relay information, injecting falsified information, or choose not to relay at all. Such situations call for security protection mechanisms for detecting the abnormal behavior in relay, and for tracing adversarial relay nodes.

Authors' email: {ymao, minwu}@eng.umd.edu.

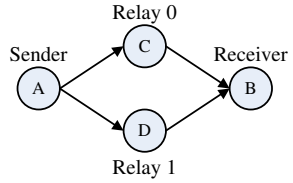

Fig. 1. Cooperative communication using two relay nodes

For some strategies employed by an adversarial relay node, application-layer cryptographical mechanisms would be able to defend against them. For example, by using message authentication code (MAC), the falsified packets can be identified and removed. However, as we shall see in later sections, application-layer cryptography alone cannot ensure the capability of tracing adversarial relay node without the knowledge of the signals from each relay path. Obtaining such information requires the assistance from physical-layer signal detection. In this paper, we present a simple scenario where there are two relay nodes employing decode-and-forward strategy in a cooperative communication system. We show that when an adversarial relay node does not follow the cooperation rules and transmits garbled signals, the conventional signal detection would fail. To defend against such malicious attacks, we propose a cross-layer scheme for tracing the adversarial relay, which involves using tracing symbols at pseudo-random locations in the symbol stream, assisted by an adaptive signal detection scheme at the physical layer.

The rest of this paper is organized as follows. In Section 2 we discuss system settings and impacts of potential attacks by adversarial relay. Section 3 presents the cross-layer scheme for tracing the adversarial relay. The simulation results are presented in Section 4.

2. SYSTEM SETTING AND ATTACK MODELLING

In this paper, we focus on a two-node relay shown in Fig. 1 with decode-and-forward, and consider two relay nodes employing a simple space-time code described in Table 1 for message forwarding [3]. Nonetheless, the analysis can be extended to other decode-and-forward strategies.

Suppose the signal constellation set $\mathcal{M}$ consists of $M = 2^m$ symbols. After decoding, the relay nodes take two decoded symbols $\mathbf{s_0}$ and $\mathbf{s_1}$ at consecutive time slots for relay transmission. At the receiving side, the received signals at the two consecutive symbol durations are

$$\mathbf{r_0} = \mathbf{h_0 s_0} + \mathbf{h_1 s_1} + \mathbf{n_0}, \;\; \mathbf{r_1} = -\mathbf{h_0 s_1^*} + \mathbf{h_1 s_0^*} + \mathbf{n_1}.$$

Table 1. Space-Time Code Used by Two Relay Nodes

	relay node 0	relay node 1
t	$\mathbf{s_0}$	$\mathbf{s_1}$
$t+T$	$-\mathbf{s_1^*}$	$\mathbf{s_0^*}$

Table 2. Garbled Signals Transmitted by Relay Nodes

	relay node 0	relay node 1
t	$\mathbf{s_0}$	$\mathbf{s_2}$ (instead of $\mathbf{s_1}$)
$t+T$	$-\mathbf{s_1^*}$	$\mathbf{s_3^*}$ (instead of $\mathbf{s_0^*}$)

Here $\mathbf{n_0}$ and $\mathbf{n_1}$ are complex Gaussian noise; $\mathbf{h_0} = \alpha_0 e^{j\theta_0}$ and $\mathbf{h_1} = \alpha_1 e^{j\theta_1}$ are slow fading channel coefficients, which does not change in two symbol durations. We assume the channel conditions $\mathbf{h_0}$ and $\mathbf{h_1}$ are known at the receiver side, but not at the relay node. This is achieved by using proper channel estimation and inserting pilot symbols that are frequent enough relative to channel variations [3].

The goal of an adversarial relay node is to corrupt the communication between the sender and receiver without being caught. We consider two types of attacks. The first is not to transmit the relay signals, which corresponds to a *passive* adversary model. The second is to transmit garbled signal, which corresponds to an *active* adversary model. We consider the case that one of the two relay nodes is compromised. When both relay nodes are compromised and not forwarding the messages, we can identify such a situation by comparing the received signal energy with noise energy. When both compromised relay nodes transmit garbled signals, the attack analysis and defense strategies will be the same as that of one adversarial node.

Transmit Nothing: The adversarial node can choose not to relay at all. This is similar to what is known as *soft failure* [3], i.e., one of the relay nodes (or transmit antenna) fails to function. In this situation, the receiver can still detect the received signals through a maximum likelihood detector [3]. Thus the damage by this type of passive adversary is limited. In subsequent discussions, we will focus on active adversary model.

Transmit Garbled Signal: Instead of transmitting the valid information, the adversarial relay node can arbitrarily change the signal symbol and transmit the garbled signal. In order to confuse the receiver and not to be detected as a malicious attacker, the adversarial node transmits the symbols $\mathbf{s_2}$ and $\mathbf{s_3^*}$ from signal constellations, as shown in Table 2. The receiver obtains combined signals from both relay paths with noise, which are

$$\mathbf{r_0} = \mathbf{h_0 s_0} + \mathbf{h_1 s_2} + \mathbf{n_0};\ \ \mathbf{r_1} = -\mathbf{h_0 s_1^*} + \mathbf{h_1 s_3^*} + \mathbf{n_1}.$$

To illustrate the challenge in detecting the transmitted symbols from each relay path, we consider the conventional maximum likelihood signal detector designed for the ST code in Table 1. The detector for symbol $\mathbf{s_0}$ is

$$\hat{\mathbf{s}}_\mathbf{0} = \mathbf{argmin}_{x_i \in \mathcal{M}} \{(\alpha_0^2 + \alpha_1^2 - 1)|\mathbf{x_i}|^2 + d^2(\mathbf{c_0}, \mathbf{x_i})\} \quad (1)$$

Here $\mathbf{c_0}$ is computed from the received signals and channel gain

$$\mathbf{c_0} = \mathbf{h_0^* r_0} + \mathbf{h_1 r_1^*}. \quad (2)$$

When the actual transmitted signal is garbled, as shown in Table 2, the combined signals using the conventional decoding rule (2) produces the following result

$$\mathbf{c_0}^{(g)} = \alpha_0^2 \mathbf{s_0} + \mathbf{h_1 h_0^* s_2} - \mathbf{h_0^* h_1 s_1} + \alpha_1^2 \mathbf{s_3} + (\mathbf{h_0^* n_0} + \mathbf{h_1 n_1^*}).$$

Compared to $\mathbf{c_0} = (\alpha_0^2 + \alpha_1^2)\mathbf{s_0} + (\mathbf{h_0^* n_0} + \mathbf{h_1 n_1^*})$, which is the combined signal without signal garbling, $\mathbf{c_0}^{(g)}$ contains the same noise signal but the deterministic signal has been significantly altered, which can easily lead to a detection error.

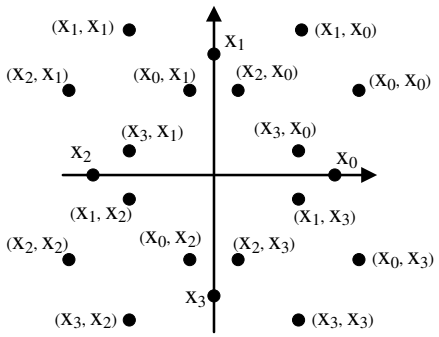

Fig. 2. The pair-wise combined signal constellations. Notation (x_i, x_j) indicates the signal point is formed by the combination $h_0 x_i + h_1 x_j$, where $h_0 = 1/2$ and $h_1 = e^{j\pi/4}$.

Example: Suppose the signalling scheme is QPSK, and the information symbols are chosen as $\mathbf{s_0} = -\mathbf{s_3}$ and $\mathbf{s_1} = -\mathbf{s_2}$. Furthermore, consider identical channel gain $\mathbf{h_0} = \mathbf{h_1} = \alpha e^{j\theta}$. Thus we have the combined signal as

$$\begin{aligned} \mathbf{c_0}^{(g)} &= \alpha^2(\mathbf{s_0} + \mathbf{s_2} - \mathbf{s_1} + \mathbf{s_3}) + (\mathbf{h_0^* n_0} + \mathbf{h_1 n_1^*}) \\ &= 2\alpha^2 \mathbf{s_2} + (\mathbf{h_0^* n_0} + \mathbf{h_1 n_1^*}) \end{aligned} \quad (3)$$

Under the maximum likelihood detection rule, the receiver outputs the signal constellation $\mathbf{x_i}$ that is closest to $\mathbf{c_0}^{(g)}$ in Euclidean distance. Hence the detection result will most probably be $\mathbf{s_2}$, while the actual signal sent by the cooperative relay node is $\mathbf{s_0}$. This illustrates the ambiguity in the conventional signal detector when facing the adversarial relay node.

3. PROPOSED CROSS-LAYER SCHEME FOR TRACING ADVERSARIAL RELAY

There are two main challenges to tracing the adversarial relay. At the physical layer, we need to separately detect the signal symbols from the two relay paths. Noticing that such symbol-by-symbol detection may have low reliability, an upper-layer scheme is necessary to aggregate the symbol detection results for reliably distinguishing adversary from cooperator. We propose the following approach to obtain assistance from lower layers as follows. The sender inserts a small number of pseudo-random signalling symbols at random locations in the symbol stream. We refer to the inserted symbols as the *tracing symbols*. Both the insertion location and the inserted tracing symbols are generated using a cryptographically secure function with a secret key, which is shared by the sender and receiver but unknown to the relay nodes. Upon receiving the relay signals, the receiver uses the secret key to find out the location of the tracing symbols, extract them, and apply signal detection. On the other hand, receiver also compute the "ground truth" of the tracing symbols using the secret key and compare them with the detected tracing symbols from the relay path. Such a comparison can tell whether a relay node is adversarial or cooperative. The details of the tracing scheme consists of two parts: (1) how to detect the garbled tracing symbols; and (2) how to aggregate the detection results to achieve a reliable decision.

3.1. Detecting Garbled Signals

3.1.1. Resolving Ambiguity Using One Receive Antenna

In this part we discuss how the receiver can resolve the ambiguity in the garbled signal and estimate the information sent respectively

Table 3. Channel Conditions with Two Receive Antennas

	relay node 0	relay node 1
Rx 0	$\mathbf{h_0}$	$\mathbf{h_1}$
Rx 1	$\mathbf{h_2}$	$\mathbf{h_3}$

Table 4. Received Signals at the Receive Antennas

	Rx 0	Rx 1
t	$\mathbf{r_0}$	$\mathbf{r_2}$
$t+T$	$\mathbf{r_1}$	$\mathbf{r_3}$

by the two relay nodes. To see the feasibility of such detection, we consider the following example. The channel gain $\mathbf{h_0} = 1/2$ and $\mathbf{h_1} = e^{j\pi/4}$. The signalling is through QPSK with constellations $\mathcal{M} = \{\mathbf{x_0}, \mathbf{x_1}, \mathbf{x_2}, \mathbf{x_3}\}$. If the received signal is noise-free, i.e., $\mathbf{y} = \mathbf{h_0 s_0} + \mathbf{h_1 s_1}$, we can see that $\mathbf{y}$ can take 16 distinct patterns in the complex signalling plane, as shown in Fig. 2. In this figure, the combined signal constellations are shown together with the original QPSK constellations. When the received signal contains additive noise, the received signal takes the form $\mathbf{r} = \mathbf{h_0 s_0} + \mathbf{h_1 s_1} + \mathbf{n}$, where $\mathbf{n}$ is the complex Gaussian noise.

Rewriting the received signal as $\mathbf{r} = \mathbf{y} + \mathbf{n}$, we can detect the signal $\mathbf{y}$ from $\mathbf{r}$ as if the original signal contains 16 constellations. Under the complex Gaussian noise, the maximum likelihood detector is equivalent to the minimum distance detector. Here we outline a procedure for detecting combined signal and computing the probability of error:

(a) Suppose the original signal constellation is $\mathcal{M}$ and the condition of the two channels are known as $\mathbf{h_0}$ and $\mathbf{h_1}$. We first find all the possible signal combinations $\mathbf{y_k} = \mathbf{h_0 x_i} + \mathbf{h_1 x_j}$, where $\mathbf{x_i}, \mathbf{x_j} \in \mathcal{M}$. Denote the combined signal constellations by $\mathcal{Y} = \{\mathbf{y_k}\}$.

(b) In the two-dimensional signal plane, find the Voronoi diagram $\mathcal{V}$ associated with the signal constellations $\mathcal{Y}$. The Voronoi cell V_k delimits the areas that are closer to a signal $\mathbf{y_k}$ than any other signal constellations. If the received signal $\mathbf{r} \in V_k$, the detection output is $\mathbf{y_k}$. Then map $\mathbf{y_k}$ to the pair $(\mathbf{x_i}, \mathbf{x_j}) \in \mathcal{M}$.

(c) Assuming the actual combined signal is $\mathbf{y_k} \in \mathcal{Y}$, estimate the error probability by a 2-D numerical integration

$$\Pr(e|\mathbf{y_k}) = 1 - \int_{V_k} \frac{1}{2\pi\sigma_n^2} \exp\{-|\mathbf{x} - \mathbf{y_k}|^2/(2\sigma_n^2)\} d\mathbf{x},$$

where σ_n^2 is the noise variance.

We note that the detection complexity is $\mathcal{O}(M^2)$. The detection rule no longer benefits from the time diversity originally in the ST code. The error probability depends on the channel coefficients $\mathbf{h_0}$ and $\mathbf{h_1}$, which influence the geometry of the combined signal constellations.

3.1.2. Resolving Ambiguity Using Two Receive Antennas

When the receiving side has more than one receive antenna, we have more resource to defend against signal garbling using a more effective strategy. We again assume that the channel conditions between the two relay nodes and the two receive antennas are known at the receiver, as shown in Table. 3. The channel variation is negligible for adjacent transmission time slots. The signals sent by the two relay nodes are according to Table 2. The received signals at the two time slots are shown in Table 4. The signals received at the first time slot are

$$\begin{aligned} \mathbf{r_0} &= \mathbf{h_0 s_0} + \mathbf{h_1 s_2} + \mathbf{n_0}, \\ \mathbf{r_2} &= \mathbf{h_2 s_0} + \mathbf{h_3 s_2} + \mathbf{n_2}. \end{aligned} \tag{5}$$

We observe that signals $\mathbf{s_0}$ and $\mathbf{s_2}$ only appear in the received signals at the first time slot. Therefore the signal detector for $\mathbf{s_0}$ and $\mathbf{s_2}$ will only rely on (5). The detector for $\mathbf{s_1}$ and $\mathbf{s_3}$ can be obtained similarly. Let us define

$$d_1 = d(\mathbf{r_0}, \mathbf{h_0 x_i} + \mathbf{h_1 x_j}), \;\; d_2 = d(\mathbf{r_2}, \mathbf{h_2 x_i} + \mathbf{h_3 x_j}). \tag{6}$$

It can be shown that under uncorrelated Gaussian noise, the maximum likelihood detector for $\mathbf{s_0}$ and $\mathbf{s_2}$ chooses signal constellations $\mathbf{x_i}, \mathbf{x_j} \in \mathcal{M}$ that minimizes the summation $(d_1^2 + d_2^2)$. After some algebraic manipulations, we can show that minimizing $(d_1^2 + d_2^2)$ is equivalent to minimizing the detection statistics

$$\begin{aligned} T = {} & d^2(\mathbf{w_0}, \mathbf{x_i}) + d^2(\mathbf{w_1}, \mathbf{x_j}) - d^2(\mathbf{v}, \mathbf{x_i^* x_j}) + |\mathbf{x_i}|^2 |\mathbf{x_j}|^2 \\ & + (\alpha_0^2 + \alpha_2^2 - 1)|\mathbf{x_i}|^2 + (\alpha_1^2 + \alpha_3^2 - 1)|\mathbf{x_j}|^2. \end{aligned} \tag{7}$$

Here three auxiliary variables $\mathbf{w_0}$, $\mathbf{w_1}$, and $\mathbf{v}$ are defined as $\mathbf{w_0} = \mathbf{h_0^* r_0} + \mathbf{h_2^* r_2}$, $\mathbf{w_1} = \mathbf{h_1^* r_0} + \mathbf{h_3^* r_2}$, and $\mathbf{v} = \mathbf{h_0 h_1^*} + \mathbf{h_2 h_3^*}$. For PSK signals, the detection statistics (7) can be reduced to

$$T_{PSK} = d^2(\mathbf{w_0}, \mathbf{x_i}) + d^2(\mathbf{w_1}, \mathbf{x_j}) - d^2(\mathbf{v}, \mathbf{x_i^* x_j}). \tag{8}$$

The optimum detector has the following structure

$$(\hat{\mathbf{s}}_\mathbf{0}, \hat{\mathbf{s}}_\mathbf{2}) = \mathbf{argmin}_{(x_i, x_j) \in \mathcal{M}} T(\mathbf{x_i}, \mathbf{x_j}). \tag{9}$$

The complexity in solving (9) is $\mathcal{O}(M^2)$. Similar to the case of one receive antenna, the symbol error probability in the case of two receive antenna does not render itself to close-form expression. We can use Monte-Carlo methods to approximate the symbol error probability. It can be shown that with two receive antennas, the receiver is able to detect the garbled information symbols more effectively than the signal receive antenna case. The only "luck" required by such a signal detection scheme is that the two-by-two channel condition matrix $\mathbf{H}$ in (5) is non-singular and not ill-conditioned. Otherwise, it would be easy to see that the situation described in (5) reduces to the situation of only having one receive antenna, as discussed in Section 3.1.1.

3.2. The Tracing Algorithm

The sender inserts random tracing symbols and the signals will go through the relay nodes. At the receiver side, the receiver first extracts the physical layer tracing symbols $[\mathbf{s_1}, \mathbf{s_2}, ..., \mathbf{s_n}]$ from the symbol stream. The extracted tracing symbols, together with the "ground truth" of the tracing symbols $[\mathbf{t_1}, \mathbf{t_2}, ..., \mathbf{t_n}]$ computed using the secret key, are provided to upper layer. In addition, a confidence value p_i for each detected tracing symbol $\mathbf{s_i}$, indicating the probability of correct detection is also provided. From here on, the information from each relay path should be treated separately. We focus on processing the information from one relay path. The algorithm for determining whether the relay node is cooperative or adversarial takes the following steps:

(1) Pre-processing: Remove the detected tracing symbols $\mathbf{s_i}$ (and the corresponding ground truth $\mathbf{t_i}$) whose confidence value p_i is below a pre-determined threshold τ.

(2) Symbol mapping: Map each complex symbol to a binary string using Gray code. Use antipodal signal to represent the results, i.e., represent binary bit one by "1" and binary bit zero by "-1". Thus the mapping results are two sequences $[s_1, s_2, ..., s_m]$ and $[t_1, t_2, ..., t_m]$, whose elements take value in $\{-1, +1\}$.

(3) Correlation decision: Compute the normalized correlation coefficient

$$\rho = \frac{\sum_i s_i t_i}{\sqrt{\sum_i s_i^2} \sqrt{\sum_i t_i^2}}. \tag{10}$$

Then compare it with a threshold value η to make a decision. If $\rho \geq \eta$, declare the relay node as cooperative; if $\rho < \eta$, declare it as adversarial.

In the above algorithm, the pre-processing is to ensure that each tracing symbol involved in the final decision is reliable enough, i.e., with probability of correct detection $p_c \geq \tau$. The mapping from signal constellations to binary data using Gray coding will ensure that the constellations that are close in Euclidean distance are mapped to binary strings with small Hamming distance. The correlation decision is similar to the technique used in digital watermarking to enhance the reliability of the decision.

Since each tracing symbols are randomly and independently chosen, it can be shown that as the number of detected tracing symbols becomes large, ρ converges to a Gaussian random variable. When a relay node is cooperative (Hypothesis H_0), the mean of ρ is close to 1, i.e., $\mathrm{E}(\rho|H_0) \approx 1$; when relay node is adversarial (Hypothesis H_1), $\mathrm{E}(\rho|H_1) = 0$. The variance of ρ under both hypothesis decreases linearly with the reciprocal of the number of reliably detected tracing symbols. Therefore we can set the threshold $\eta = 1/2$. With more tracing symbols, the receiver can sequentially update ρ and gradually improve the reliability of the tracing decision.

The main costs for such a tracing scheme include: (1) the computation at the receiver side; (2) the bandwidth cost by inserting the tracing symbols into the data stream (an estimated 1-3 % overhead would incur); (3) the cost of setting up the secret key for the tracing scheme, which can be done at the same time when setting up the application-layer encryption and authentication keys. We note that the mechanism for tracing the adversarial relay is only necessary when the receiver detects abnormal behavior from the relay signals. For example, when application layer cryptographic authentication frequently cannot pass or decryption often results in meaningless data.

4. SIMULATION RESULTS

In this section we present simulation results of the tracing statistics ρ for the cooperative and adversarial relay. The channel conditions are generated using the modified Jakes model in [8]. Each channel follows time-correlated slow Rayleigh fading. Different channels are uncorrelated. QPSK is chosen as the signalling scheme. Symbol rate is 20K symbols per second. Every 64 symbols are grouped as a frame. In each frame the sender will send 1, 2, or 3 tracing symbols, with equal probability $1/3$. At the receiver side, the threshold probability for determining reliably detected tracing symbol is $\tau = 0.9$.

In Fig. 3 we present the tracing statistics ρ with respect to the number of tracing symbols, under 10 dB SNR. The adversarial relay randomly chooses one symbol to send with equal probability. The simulation runs in a 200-frame duration. We can see that using one receive antenna (upper figure), only 27% of the tracing symbols can be reliably detected. However, using two receive antennas (lower figure) significantly improves symbol detection reliability. As many as 88% of the symbols are reliable and thus it takes a shorter time for the tracing statistics ρ to converge. We can also observe that the tracing statistics from adversarial relay converges to its mean 0; and that from the cooperative relay converges to its mean close to 1. In both cases the convergence rate is fast, requiring only 50-100 reliable tracing symbols. We note that the simulation time duration is about 0.6 second, which indicates that the proposed tracing scheme can obtain a highly confident result efficiently, within half a second.

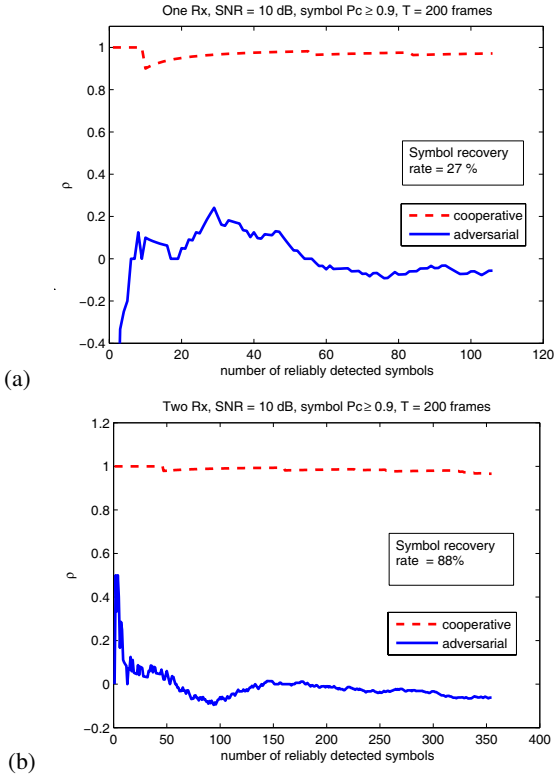

Fig. 3. Tracing statistics ρ under 10 dB SNR. (a) one receive antenna. (b) two receive antennas.

In conclusion, we have investigated in this paper the unique security issues in cooperative wireless communications caused by adversarial relay. We proposed a cross-layer tracing scheme for identifying the adversary with high reliability. The simulation results show that the proposed tracing algorithm is both effective and efficient.

5. REFERENCES

[1] J. N. Laneman, D. N. C. Tse and G. W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior", *IEEE Trans. on Info. Theory*, 50(12), 2004, pp. 3062 - 3080.

[2] J. N. Laneman and G. W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks", *IEEE Trans. on Info. Theory*, 49(10), 2003, pp. 2415 - 2425.

[3] S. M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communications", *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, Oct. 1998, pp. 1451-1458.

[4] V. Tarokh, H. Jafarkhani and A. R. Calderbank, "SpaceTime Block Codes from Orthogonal Designs", *IEEE Trans. on Info. Theory*, 45(5), 1999, pp. 1456 - 1467.

[5] J. G. Proakis, *Digital Communications*, Fourth Ed., McGraw Hill, 2001.

[6] T. S. Rappaport, *Wireless Communications: Principles and Practice*, Prentice Hall, 1996.

[7] H. V. Poor, *An Introduction to Signal Detection and Estimation*, 2nd Ed., Springer, 1994.

[8] P. Dent, G. E. Bottomley, and T. Croft, "Jakes Fading Model Revisited", *IEEE Electronic Letter*, vol. 29, no. 13, June 1993, pp 1162 – 1163.