AFRL-IF-RS-TR-2007-150
Final Technical Report
June 2007

COOPERATIVE COMMUNICATIONS FOR WIRELESS INFORMATION ASSURANCE: SECURE COOPERATIVE COMMUNICATIONS AND TESTBED DEVELOPMENT

Research Foundation of SUNY at Binghamton

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

AFRL-IF-RS-TR-2007-150 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/	/s/
E. PAUL RATAZZI Work Unit Manager	WARREN H. DEBANY, Jr. Technical Advisor, Information Grid Division Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
JUN 2007	Final	May 06 – Jan 07

4. TITLE AND SUBTITLE

COOPERATIVE COMMUNICATIONS FOR WIRELESS INFORMATION ASSURANCE: SECURE COOPERATIVE COMMUNICATIONS AND TESTBED DEVELOPMENT

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA8750-06-2-0167

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)

Xiaohua (Edward) Li

5d. PROJECT NUMBER
231G

5e. TASK NUMBER
WI

5f. WORK UNIT NUMBER
RE

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of California
10920 Wilshire Blvd 1200
Los Angeles CA 90024-6523

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/IFGB
525 Brooks Rd
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2007-150

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# 07-299

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report summaries our progress and accomplishments for the project "Secure Cooperative Communications and Testbed Development." We have worked on physical-layer security and cooperative communications, and have been developing a wireless cooperative transmission testbed to demonstrate our theoretic results. In this project, we have obtained some major achievements. We have developed an innovative secure transmission scheme, have studied the limit of cooperative transmissions, and have invented a new cooperative OFDM transmission scheme to combat transmission asynchronism. They are helpful to the development of future physical-layer wireless information assurance techniques as well as the cooperative communication techniques. We have successfully implemented the wireless cooperative transmission testbed, implemented array transmissions, and estimated channels which partially verified the validness of our theories.

15. SUBJECT TERMS
Wireless networking, physical layer, information assurance, information theoretic security, PHY, radio frequency, cooperative communications, OFDM

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			E. Paul Ratazzi
U	U	U	UL	33	19b. TELEPHONE NUMBER (*Include area code*)

Table of Contents

List of Figures

Abstract

This report summarizes our progress and accomplishments for the project "Secure Cooperative Communications and Testbed Development", funded by AFRL under project FA8750-06-2-0167 from May 8, 2006 to January 8, 2007. We have worked on physical-layer security and cooperative communications, and have been developing a wireless cooperative transmission testbed to demonstrate our theoretic results. We have finished or made significant progress on all topics from the original proposal.

In this project, we have obtained some major achievements. We have developed an innovative secure transmission scheme, have studied the limit of cooperative transmissions, and have invented a new cooperative OFDM transmission scheme to combat transmission asynchronism. They are helpful to the development of future physical-layer wireless information assurance techniques as well as the cooperative communication techniques. We have successfully implemented the wireless cooperative transmission testbed, implemented array transmissions, and estimated channels which verified partially the validness of our theories.

First, as shown in Part I, for secure transmissions, we have proposed the use of signal processing techniques to protect wireless transmissions as a way to secure wireless networks at the physical layer. This approach addresses a unique weakness of wireless networks whereby network traffic traverses a public wireless medium making traditional boundary controls ineffective. Specifically, a randomized array transmission scheme is developed to guarantee wireless transmissions with inherent low-probability-of-interception (LPI). In contrast to conventional spread spectrum or data encryption techniques, this new method exploits the redundancy of transmit antenna arrays for deliberate signal randomization which, when combined with channel diversity, effectively randomizes the eavesdropper's signals but not the authorized receiver's signals. The LPI of this transmission scheme is analyzed via proving the indeterminacy of the eavesdropper's blind deconvolution. The proposed method is useful for securing wireless transmissions, or for supporting upper-layer key management protocols.

Second, as shown in Part II, for cooperative transmissions, in contrast to most existing work that depends on the assumption of perfect synchronization among the transmitters, we consider the inevitable asynchronism among the cooperative transmitters. Our studies show that the interference caused by asynchronism-induced channel dispersion introduces an average signal-to-interference-ratio (SIR) degradation of at least 10 dB in flat fading environment, which may greatly limit the cooperative diversity gain. We also show that in OFDM transmissions, the cyclic prefix (CP) can be used to resolve such asynchronism. In particular, for the first time, we show that the carrier-frequency offset (CFO) can be removed completely with extended CP. This finding is very useful for cooperative OFDM transmissions and for the future multi-carrier-based OFDM transmissions.

Finally, in Part III, a testbed is setup in order to demonstrate the secure transmission scheme and the cooperative transmission scheme, from which many important assumptions have been demonstrated, such as transmission asynchronism, channel dispersion, channel independence, etc. We implement BPSK/QPSK array transmissions using ComBlock modules. Channels are measured and used in the simulation of secure transmissions.

This research has generated 4 journal papers (one formally accepted, one in 2nd round review, two in preparation), and 4 conference papers published in major conferences.

In summary, we have made significant progress and achievements in this project, and thus satisfactorily conclude this project. Nevertheless, there are still many interesting problems open which deserve continuous investigation should future funding be available.

Background

This is the final report for the project "Secure cooperative communications and testbed development," funded by Air Force Research Laboratory under grant FA8750-06-2-0167.

This report consists of three parts. Part I develops physical-layer security transmission techniques. Part II addresses cooperative communications. Part III is devoted to the testbed development. To save space, many details have to be skipped, but can be referred from our publications listed below:

[P1] X. Li, J. Hwu and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," submitted to *Journal of Communications* (formally accepted).

[P2] X. Li and F. Ng, "Carrier frequency offset mitigation in asynchronous cooperative OFDM transmissions," in 2nd round review in *IEEE Trans. Signal Processing*.

[P3] F. Ng and X. Li, "CFO-resistant receiver for asynchronous MC-DS-CDMA systems," *Proceedings of ICASSP'2007,* Honolulu, Hawaii, April 15, 2007.

[P4] X. Li and F. Ng, "Using cyclic prefix to mitigate carrier frequency and timing asynchronism in cooperative OFDM transmissions," in *Proceedings of the 40th Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, Oct. 29-Nov. 1, 2006.

[P5] X. Li and J. Hwu, "Performance of cooperative transmissions in flat fading environment with asynchronous transmitters," *IEEE Military Communications Conference* (MILCOM 2006), Washington, DC, Oct. 23-25, 2006.

[P6] X. Li, J. Hwu and E. P. Ratazzi, "Array redundancy and diversity for wireless transmissions with low probability of interception," *Proceedings of ICASSP'2006,* Toulouse, France, May 14, 2006.

Part I: Using Antenna Array Redundancy and Channel Diversity for Secure Wireless Transmissions

1. Introduction

Along with the rapid development of wideband wireless communication networks, wireless security has become a critical concern. Compared with wireline networks, wireless networks lack a physical boundary due to the broadcasting nature of wireless transmissions. Any receivers nearby can hear the transmissions, and can potentially record or analyze the transmitted signals, or conduct jamming. This makes wireless security design a challenging task, and the challenge becomes even more severe if considering together other unique characteristics of wireless networks, such as severe energy/bandwidth constraints of wireless nodes, unreliable/untrusted wireless links, and dynamic wireless network topology. Noticing that the challenge is closely related to the unique physical-layer of wireless communications, physical-layer security techniques are thus helpful, since they can be more effective in resolving the boundary, efficiency, and link reliability issues.

One of the important objectives of physical-layer security design is to guarantee wireless transmissions with low-probability-of-intercept (LPI). In particular, we are interested in LPI techniques which do not directly rely on upper-layer data encryption or secret keys.

Existing physical-layer LPI techniques can be classified into three categories: i) Signal power approaches like beamforming and directional transmissions, ii) scrambling code approaches like spread-spectrum, and iii) propagation channel approaches. Traditionally, spread spectrum is the most widely used technique for LPI. However, when data transmissions are evolving toward wideband, spread spectrum alone may not be enough because of the reduced space of spreading gain.

In general, the security of most existing approaches depends on some strong (and ideal) assumptions, such as eavesdroppers have null-receiving energy, or have no information about the spreading codes, or can not estimate the propagation channels. Unfortunately, these strong assumptions can hardly hold in practice. Beamforming techniques can only reduce, but not completely nullify, the signal energy toward eavesdroppers. Spreading codes may be easily estimated by eavesdroppers from their received signals. Eavesdroppers may use non-blind or blind deconvolution algorithms to estimate channels and signals, which makes many channel-based approaches such as [1] to lose security. As a result, most existing approaches can hardly guarantee LPI, or can even hardly withstand a rigorous LPI analysis.

There have been many important advanced wireless transmission techniques developed in recent years, such as antenna array, channel diversity and channel deconvolution, some of which may bring new opportunities for achieving LPI. In [2]-[5], we have shown that physical-layer security can be realized based on channel diversity by using antenna array transmissions. This idea in fact represents an innovative way of secure waveform design, differently from the conventional spread spectrum or data encryption techniques. Another innovative concept is that we rely on signal processing theory such as the indeterminacy of blind deconvolution [6] for security, rather than information theory [1][7]. The advantage is that LPI can be guaranteed much easier in more practical transmissions.

Based on [2], in this project we propose a special deliberate randomization method for designing the transmit antenna weights. A transmission power analysis is also conducted to guide weights design. Extensive simulations and the development of a testbed are shown.

2. Secure array transmission model

We consider a wireless network where Alice transmits to Bob in face of a passive eavesdropper Eve, as shown in figure 1. Alice uses J transmit antennas in the secure channel, and may use some other antennas communicating with Bob which form an insecure public channel. This public channel may be used for the synchronization purpose between Alice and Bob, e.g., for Bob to track carrier frequency and timing. Note that such a setting with a secure channel and a public channel is standard in many information-theoretic security studies or key management protocols [7].

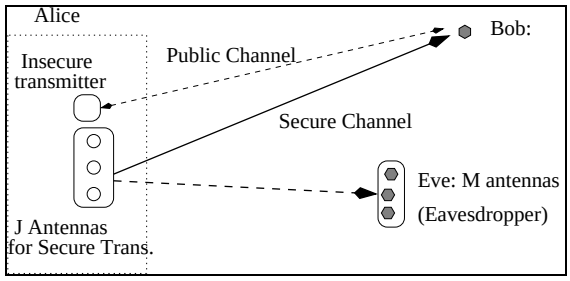

Figure 1. Secure wireless transmission model. Alice transmits to Bob using antenna array, in face of passive eavesdropper Eve.

We consider only the secure channel from Alice to Bob. A beamforming-like array transmission procedure is used by Alice to transmit to Bob a symbol sequence $\{b(n)\}$ which is assumed as i.i.d. uniformly distributed with zero-mean and unit variance. Though more complex pre-processing can be exploited, Alice just uses a simple weighting scheme with weighting coefficients $w_i(n)$. Therefore, through the J antennas, Alice transmits signal vectors

$$\mathbf{s}(n) = \begin{bmatrix} s_1(n) \\ \vdots \\ s_J(n) \end{bmatrix} = \begin{bmatrix} w_1(n) \\ \vdots \\ w_J(n) \end{bmatrix} b(n) = \mathbf{w}(n) b(n) \qquad (1.1)$$

where $w_i(n)$ denotes the weighting coefficient of the i^{th} transmit antenna during the symbol interval n.

Assume Rayleigh flat fading channels and assume Bob use only one receiving antenna for both simplicity and worst case consideration. Extension to receiving antenna arrays can be found in [5]. The signal received by Bob is

$$x(n) = \sum_{i=1}^{J} h_i^* s_i(n) + v(n) = \mathbf{h}^H \mathbf{s}(n) + v(n) \qquad (1.2)$$

where $v(n)$ denotes AWGN with zero-mean and variance σ_v^2, h_i^* denotes channel coefficients which are independent complex circular symmetric Gaussian distributed with zero-mean and unit

variance, and $\mathbf{h} = [h_1 \ \cdots \ h_J]^T$. $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^H$ denote conjugation, transposition and Hermitian, respectively.

The eavesdropper Eve may use multiple receiving antennas for better interception, and the interception becomes much easier with flat-fading channels. Therefore, we consider the worst case to Alice and Bob where Eve receives signals from M receiving antennas, whose received signals can be denoted as

$$\mathbf{x}_e(n) = \mathbf{H}_e\mathbf{s}(n) + \mathbf{v}_e(n) \tag{1.3}$$

The vector $\mathbf{v}_e(n)$ is AWGN with zero-mean and covariance matrix $\sigma_v^2\mathbf{I}_M$, where $\mathbf{I}_M$ is the $M \times M$ identity matrix.

We assume that each element of $\mathbf{H}_e$ has the same distribution as, but is independent from, those of $\mathbf{h}$. From the extensive studies on antenna array channels, we know that as long as the distance between Bob and Eve is larger than half of a carrier wavelength, then their channels can be considered as independent [8].

Under the above assumption, channels $\mathbf{h}$ and $\mathbf{H}_e$ are different almost surely, especially when J is large. We further assume that Eve does not know $\mathbf{h}$ and $\mathbf{H}_e$. However, Eve may try blind or non-blind methods to estimate $\mathbf{H}_e$ from her received signal $\mathbf{x}_e(n)$. On the other hand, Alice and Bob do not know $\mathbf{h}$ and $\mathbf{H}_e$ either. We will discuss ways for Alice to obtain channel knowledge $\mathbf{h}$ since transmit beamforming requires transmitter-side channel information. Nevertheless, our major focus in this paper is the design of transmission weights $\mathbf{w}(n)$ so that Bob can detect symbols $b(n)$ successfully with low bit-error-rate (BER) while Eve can estimate neither $\mathbf{H}_e$ nor $b(n)$.

3. Array transmission with deliberate signal randomization

To introduce high BER to Eve is to prevent Eve from channel/symbol estimation. This means, firstly, Alice can not transmit training signals by the J transmit antennas, because otherwise Eve can trivially utilize such training for channel estimation [9][10]. Without training, the only way left for Eve is blind deconvolution [6][11][12]. Therefore, secondly, Eve's blind deconvolution capability must be prevented. Because Bob has no more advantage over Eve on channel estimation, such requirements also mean that Bob can hardly estimate his own channel $\mathbf{h}$.

To meet both requirements, we propose a transmission scheme in which Bob can detect symbols $b(n)$ without the knowledge of channel $\mathbf{h}$. In addition, we use a deliberate signal randomization technique in this scheme to randomize Eve's signal but not Bob's signal so that blind deconvolution of Eve has irresolvable ambiguity.

In order for Bob to estimate symbols $b(n)$, the channel $\mathbf{h}$ from Alice to Bob has to be resolved. In our scheme, we ask Alice instead of Bob to estimate and utilize the knowledge of $\mathbf{h}$. Alice can estimate $\mathbf{h}$ based on channel reciprocity [8], where Bob first transmits a training signal to Alice using the same carrier frequency as the secure channel, from which Alice can estimate the backward channel. Since the forward channel $\mathbf{h}$ equals the backward channel according to

reciprocity, Alice can immediately use the estimated channel as $\mathbf{h}$ to design transmission weights. Note that this procedure gives no useful information to Eve because the latter can only estimate the channel from Bob.

Our basic idea is to make $\mathbf{h}^H\mathbf{w}(n)$ a deterministic constant, while $\mathbf{Hw}(n)$ changing randomly in each symbol interval, by exploiting the knowledge of $\mathbf{h}$. For this purpose, Alice designs the transmitting weights vector $\mathbf{w}(n)$ so that

$$\mathbf{h}^H\mathbf{w}(n) = \|\mathbf{h}\| \tag{1.4}$$

Obviously, if the channel $\mathbf{h}$ is constant or slowly time-varying, we need $J \geq 2$ transmitters, which explains why array transmission is necessary.

From the received signal $x(n) = \|\mathbf{h}\| b(n) + v(n)$, Bob can detect symbols as

$$\hat{b}(n) = \arg\min_{b(n)} \; | x(n) - \|\mathbf{h}\| b(n) |^2 \tag{1.5}$$

where $\|\mathbf{h}\|$ can be easily estimated from the received signal power.

Alice's design of $\mathbf{w}(n)$ under the constraint (1.4) can be performed as follows. In each symbol interval n, Alice first selects from $\mathbf{h}$ randomly an element h_i with sufficiently large magnitude. The weighting vector $\mathbf{w}(n)$ is then generated as

$$\mathbf{w}(n) = \mathbf{P}_i(n) \begin{bmatrix} a_i - \mathbf{f}_i^H \mathbf{z}_i(n) \\ \mathbf{z}_i(n) \end{bmatrix} \tag{1.6}$$

where

$$\begin{aligned} a_i &= \frac{1}{h_i^*} \|\mathbf{h}\| \\ \mathbf{f}_i &= \frac{1}{h_i^*} \begin{bmatrix} h_1 & \cdots & h_{i-1} & h_{i+1} & \cdots & h_J \end{bmatrix}^T \\ \mathbf{z}_i(n) &= \begin{bmatrix} w_1(n) & \cdots & w_{i-1}(n) & w_{i+1}(n) & \cdots & w_J(n) \end{bmatrix}^T \end{aligned} \tag{1.7}$$

The matrix $\mathbf{P}_i(n)$ is a $J \times J$ permutation matrix corresponding to the selection of h_i from the vector $\mathbf{h}$, i.e., its function is to insert the first row of the following vector into the i^{th} row. The vector $\mathbf{z}_i(n)$ is arbitrary, whose dimension $J-1$ is the degrees of freedom in antenna array transmissions that we can exploit for deliberate signal randomization.

This array weights design procedure is outlined below as algorithm 1.

Algorithm 1. Update array weights vector $\mathbf{w}(n)$ in each symbol interval n

1. Select randomly a channel coefficient h_i, with sufficiently large magnitude $|h_i| > \alpha$.
2. Generate random variables $w_j(n)$, $1 \leq j \leq J$, $j \neq i$.
3. Calculate $\mathbf{w}(n)$ by (1.6)-(1.7).

The selection of the threshold α in step 1 will be discussed in section 4, whereas step 2 will be detailed in the sequel.

One of the major advantages of algorithm 1 is its linear computational complexity. Efficient computation is important because $\mathbf{w}(n)$ is recalculated in each symbol interval.

From (1.6), we can choose $\mathbf{z}_i(n)$ appropriately to prevent Eve from blind deconvolution. In general, this purpose can be fulfilled by simply making $\mathbf{z}_i(n)$ to have a distribution unknown to Eve since it is well known that successful blind deconvolution requires the receiver know some special statistics or structure of the transmitted signals [6][9]. However, existing results of blind deconvolution are mostly on how to conduct blind deconvolution, not on how to prevent blind deconvolution. The proof of the incapability of blind deconvolution is rarely seen.

To furbish a rigorous quantitative proof of the incapability of blind deconvolution, we consider a more structured scheme where Alice designs $\mathbf{z}_i(n)$ such that $\mathbf{r}_i(n) = \mathbf{z}_i(n)b(n)$ is $(J-1)$-variate Gaussian distributed with mean $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$, i.e., $\mathbf{r}_i(n) \sim \mathcal{N}_{J-1}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$. The parameters $\boldsymbol{\mu}$ and $\boldsymbol{\Sigma}$ are arbitrary and unknown to both Eve and Bob, and can even be time-varying. Based on this, a formal proof of the LPI can be furbished by applying the indeterminacy of Eve's blind deconvolution. Detailed can be found in our paper [P1]. One of the major arguments is the following proposition.

Proposition 1. From the distribution of $\mathbf{x}_e(n)$, the channel matrix $\mathbf{H}_e$ is indistinguishable from $\mathbf{H}_e\mathbf{Q}$ with a $J \times J$ matrix

$$\mathbf{Q} = \mathbf{P}_i(n)\begin{bmatrix} u & \mathbf{0} \\ \mathbf{0} & \mathbf{V} \end{bmatrix}\mathbf{P}_i^{-1}(n) \tag{1.8}$$

where u is an arbitrary non-zero scalar and $\mathbf{V}$ is a $(J-1)\times(J-1)$ arbitrary nonsingular matrix.

Since Eve can not estimate $\mathbf{H}_e$, what's left for her is a brute-force exhaustive search of vector $\mathbf{h}^H\mathbf{H}_e^{-1}$ (assume $\mathbf{H}_e$ is invertible). The complexity increases exponentially with the number of transmit antennas J. If Eve must use K-level quantization of channel coefficients, then the brute-force search needs to consider at least K^{2J} possible coefficients (real and imaginary parts), which means a complexity of $O(K^{2J})$. For example, for QPSK transmission at SNR 25 dB, in order to guarantee BER 0.01, K should be at least 128. In this case, a $J = 8$ transmit antenna array brings a complexity of $O(2^{112})$. This complexity rapidly increases with larger J, with frequency-selective fading, and with a receiving antenna array used by Bob [5].

4. Transmission power analysis

Analysis of transmission power is necessary, not only for enhancing power efficiency, but also for guaranteeing LPI. Specifically, we need both to reduce the total transmission power and to balance the power among the transmitting antennas. We will show in this section that this objective can be conducted by choosing properly $\boldsymbol{\mu}$ and $\boldsymbol{\Sigma}$.

For our proposed scheme, conditioned on each selected channel coefficient h_i, the total transmission power is

$$\mathrm{tr}\{E[\mathbf{s}(n)\mathbf{s}^H(n)\,|\,\mathbf{h},\mathbf{P}_i(n)]\} = \mathrm{tr}\{\boldsymbol{\mu}\boldsymbol{\mu}^H + \boldsymbol{\Sigma}\} + |\,a_i\,|^2 + \mathbf{f}_i^H(\boldsymbol{\mu}\boldsymbol{\mu}^H + \boldsymbol{\Sigma})\mathbf{f}_i \tag{1.9}$$

whose diagonal entry gives the transmission power of each antenna.

Let us consider specifically the case that $\boldsymbol{\mu} = \mathbf{0}$ and $\boldsymbol{\Sigma} = \sigma^2\mathbf{I}_{J-1}$. The total transmission power for a given channel realization h_i and a given choice of h_i becomes

$$P_{t,h_i} = E[\mathbf{s}^H(n)\mathbf{s}(n)\,|\,\mathbf{h},\mathbf{P}_i(n)] = (J-1)\sigma^2 + |\,a_i\,|^2 + \|\,\mathbf{f}_i\,\|^2\,\sigma^2 \tag{1.10}$$

Equation (1.10) shows that small h_i increases the total transmission power. In order to reduce transmission power, we need to select h_i with magnitude larger than certain threshold α, and α should be carefully selected. Since h_i is a complex Gaussian random variable with zero mean and unit variance, the probability for the selected channel coefficient h_i to have energy greater than α is

$$P[|\,h_i\,|^2 > \alpha] = \int_\alpha^\infty e^{-t}dt = e^{-\alpha} \tag{1.11}$$

In other words, with J transmit antennas, the average number of selectable coefficients is $Je^{-\alpha}$.

Proposition 2. With Rayleigh flat-fading channels, if the channel coefficients are selected with threshold α, then the expected total transmission power is

$$P_t = (J-1)\sigma^2 + 1 + (J-1)(1+\sigma^2)\Gamma(0,\alpha) \tag{1.12}$$

From (1.12), we can see that the expected total transmission power P_t is a function of the number of transmitting antennas J, the variance σ^2 of the random weights, and the threshold α for selecting h_i. Especially, P_t increases when σ^2 increases, or α decreases, or J increases. Figure 2 illustrates their relationships under $J = 4$.

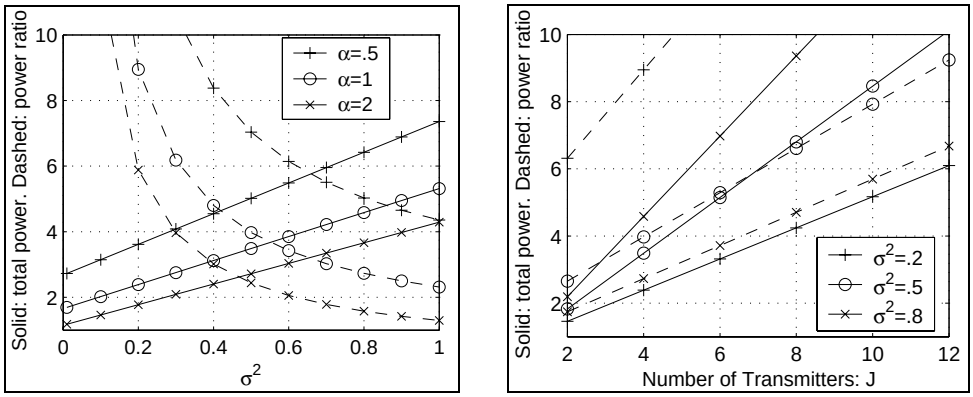

Figure 2. Total transmission power P_t and power ratio $P_{t,i}/P_{t,j}$ of the i^{th} transmit antenna to the j^{th} transmit antenna ($j \neq i$) when h_i is selected. Solid lines: total power. Dashed lines: power ratio.

If the channel $\mathbf{h}$ is slowly time-varying or even constant for a long time, we need to avoid the case that the power of one of the transmit antennas is exceptionally larger than the others. Otherwise the array behaves as a single antenna and the security can be compromised. Therefore, we have to constrain the ratio of the transmission power of the i^{th} transmit antenna $P_{t,i} = |a_i|^2 + \|\mathbf{f}_i\|^2 \sigma^2$ to that of the j^{th} transmit antenna $P_{t,j} = \sigma^2$. The power ratio can be obtained as

$$\frac{P_{t,i}}{P_{t,j}} = \frac{1 + (J-1)(1+\sigma^2)\Gamma(0,\alpha)}{\sigma^2} \tag{1.13}$$

Obviously, it is usually impossible to obtain unit ratio. From figure 2, the power ratio is a decreasing function of both σ^2 and α.

Larger σ^2 increases P_t but decreases $P_{t,i}/P_{t,j}$. Since both P_t and $P_{t,i}/P_{t,j}$ should be small, there is a trade-off between them when choosing σ^2. In the simulations, we have chosen $\sigma^2 = 0.5$. On the other hand, larger α reduces both P_t and $P_{t,i}/P_{t,j}$. But from (1.11), it reduces the number of selectable h_i as well as the randomness of $\mathbf{P}_i(n)$. Hence there is also a trade-off when choosing α. We have used $\alpha = 0.5$ in simulations.

5. Simulations and experiments

In this section, we use three simulation experiments to study the effectiveness of the proposed transmission scheme by evaluating the BER of Bob and Eve. Eve is assumed to estimate symbols either by blind equalization (specifically, via the CMA algorithm [11]), or by directly using Bob's method.

In the first simulation experiment, we used randomly generated channels. For comparison purpose, we evaluated the performance of the optimal transmit beamforming, and gave the theoretical BER curve of the Rayleigh fading channel without diversity. The simulation results are shown in figure 3. Transmissions with the proposed Algorithm 1 have similar performance as the optimal transmit beamforming. Eve can not intercept symbols using blind equalization. On the other hand, Algorithm 1 requires both larger total transmitting power and larger single-antenna transmission power than the conventional beamforming. In addition, the standard deviation of transmission power becomes large as well.

Next, considering the importance of verifying the extent of channel similarity between Bob and Eve, in the second simulation experiment, our objective is to show how confident we can claim that Bob and Eve's channels are different. We considered a $3 \times 3 \times 7$ (height/wide/length, in meters) room with some objects (a box and a beam) inside, as shown in figure 4. We placed 3 transmitting antennas at one end, and 523 receiving antennas at the other end, where the receiving antennas were put on a grid of 0.3 meter, where 0.3 is near to the wavelength of 1 GHz carrier. Specifically, there were 15 planes, each had 35 receiving antennas (two antennas were missing where there were conflictions with the objects). We let the transmit antennas to transmit impulse signals, and obtained the signals received by each of the receive antennas. This procedure was conducted using electromagnetic (EM) simulation software (based on FDTD). From the signals we then estimated all effective channels on a 0.3 meter grid. Details of the EM simulation and source data can be obtained at [13].

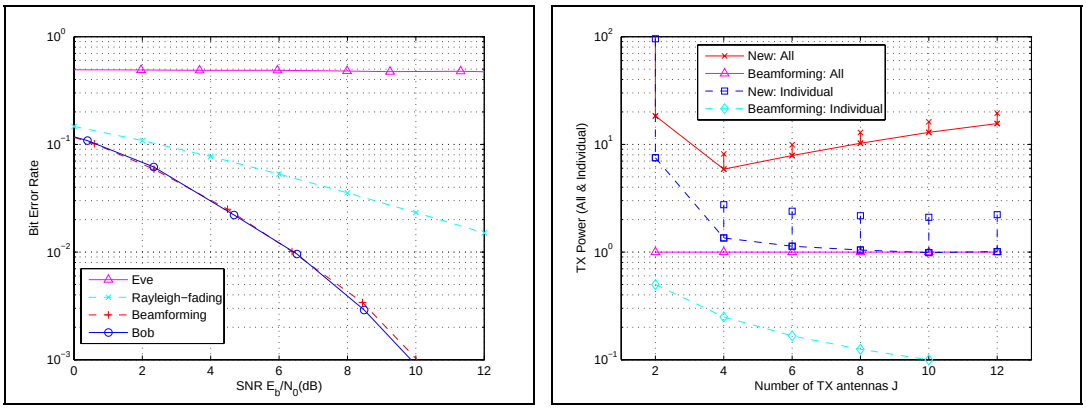

Figure 3. Left: Receiving performance comparison. Right: Total transmission power and the transmission power of each individual antenna, as well as their standard deviations. Standard deviation is shown by × or □ above the power value.

In this simulation, we obtained altogether 523 array channel vectors ($J = 3$). Then we used each of them as Bob's $\mathbf{h}$ while each of the rest as Eve's $\mathbf{H}_e$ to examine LPI. Assuming Eve use Bob's detection method, then LPI depends on the difference between $\mathbf{h}$ and $\mathbf{H}_e$. Specifically, the channel difference will contribute interference to Eve's detection, which degrades the signal-to-interference ratio (SIR) to be approximately

$$\mathrm{SIR} \approx \frac{\|\mathbf{h}\|^2}{\|\mathbf{h}_e - \mathbf{h}\|^2 \frac{1}{J}\sum_{i=1}^{J}(J-1)\sigma^2 + |a_i|^2 + \|\mathbf{f}_i\|^2 \sigma^2} \qquad (1.14)$$

Therefore, we evaluated the cumulative distribution of Eve's SIR (under noiseless assumption) for 523×522 possible transmission/eavesdropping cases. The results are shown in figure 4, from which we clearly see that in almost all cases (i.e., almost 100%), Eve's signals suffer a very high SIR loss, which prevents Eve from symbol detection.

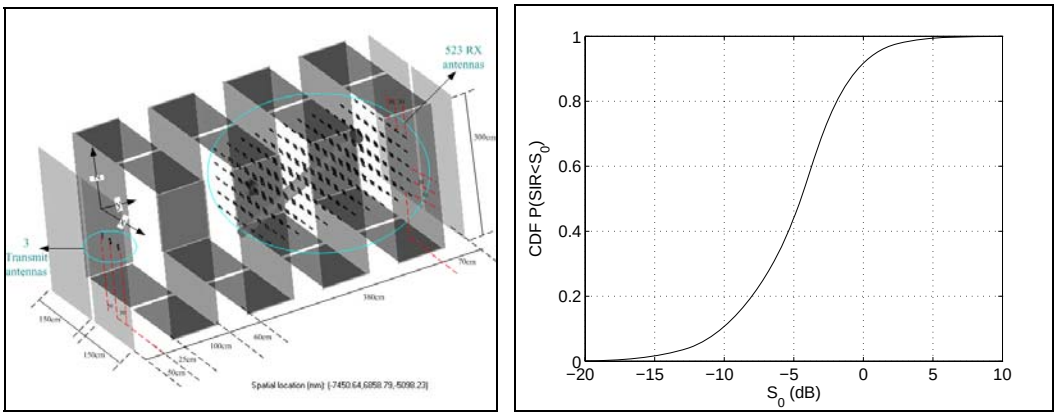

Figure 4. Left: Settings of a room for electromagnetic wave propagation simulation. Refer to [13] for a detailed description. Right: Cumulative distribution function of the SIR of Eve's signals due to the difference between Bob's and Eve's channels. Channels are derived by EM simulations.

As the third experiment, by using the channels obtained from the EM simulation, we have also simulated the error rates of Bob and Eve. For each SNR value, Bob's error rate was the average of all these 523 cases, while Eve's error rate was obtained as the minimum value among all 523×522 cases (100%) or the majority (99%) of 523×522 cases. The results are shown in figure 6 as the dashed curves. It can be seen that for almost all cases, Eve's error rate is extremely large.

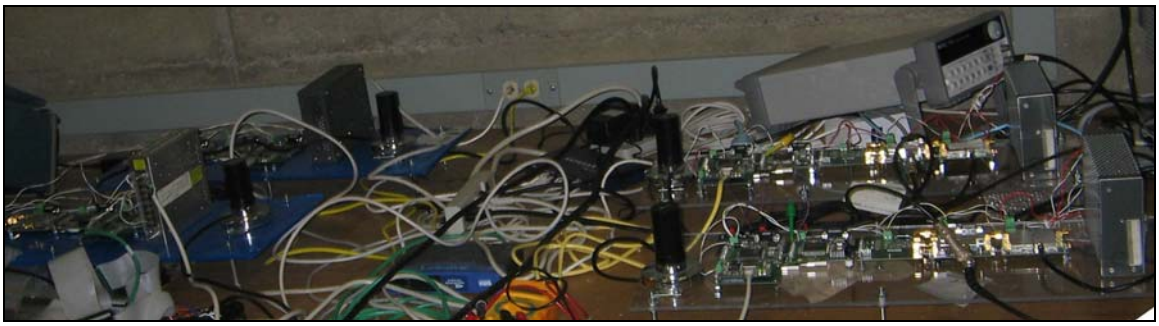

Figure 5. Experiment setup with 2 transmitting antennas (right) and 2 receive antennas (left). Notice the short distance between the two receive antennas.

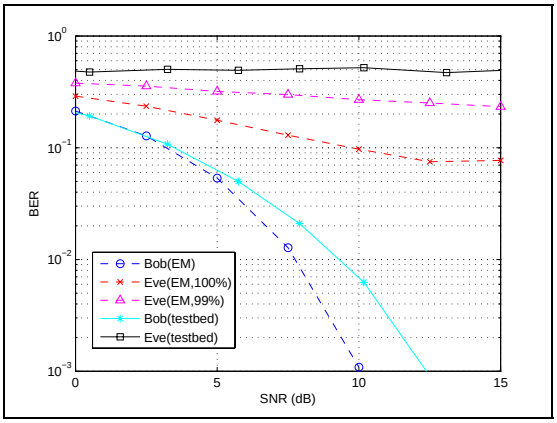

Figure 6. BER of Bob and Eve. Solid lines: using channels measured from testbed. Dashed lines: using channels obtained from EM simulation.

We are also building a testbed using the wireless transmission modules of ComBlock.com [13]. We implemented two QPSK transmitters and two QPSK receivers. One snap shot of the experiment is shown in figure 5. Four channels were estimated and fed into the program of the first simulation experiment to estimate BER. The results fit well with those obtained by purely simulations (solid lines in figure 6). Note that the two receiving antennas (one for Bob, one for Eve) were purposely placed very close to each other.

Part II: Cooperative Transmissions with Asynchronous Transmitters

1. Introduction

Recently there have been great research interests in cooperative transmissions, where the increased density of network communication devices can be exploited to enhance performance. Since cooperative transmissions use an array of transmitters similarly as physical antenna array transmissions, the rich research results of the latter can naturally be extended for the former. Especially, space-time block codes (STBC) [14] have been widely investigated for cooperative transmissions because of their efficient computation. Nevertheless, only very recently, there has been work toward the major difference between cooperative transmissions and conventional array transmissions, i.e., the synchronization of cooperative transmitters [15]-[17]. It is difficult, and in most cases impossible, to achieve perfect synchronization among distributed transmitters.

When the cooperative transmitters are not synchronized, their signals arrive at the receiver with arbitrary delays. This has two effects. First, any intended signal structure, such as the orthogonal structure of STBC encoding, is destroyed, so that the conventional receivers may not work anymore. Next, there is channel dispersion because of the pulse shaping and because universally ideal sampling time instants for all transmitter's signals do not exist. If the environment is flat fading, as expected in wireless sensor networks, such dispersion makes the channels fundamentally different. In contrast to flat fading, dealing with dispersive channels not only makes the receiver excessively complex and energy consuming, but also greatly reduces performance, especially if the optimal maximum-likelihood sequence estimation is not affordable.

Considering that it is still not very clear as to whether cooperative transmissions really provide positive overall gain in asynchronous flat fading environment, we will first investigate the performance of asynchronous cooperative transmissions by studying the ISI due to channel dispersion, and by comparing its signal-to-interference ratio (SIR) against the original flat fading cases. In this case, we mainly consider the delay asynchronism and ISI. Next, we consider OFDM transmissions which can resolve the ISI issues efficiently, but suffer from the carrier frequency asynchronism.

2. Performance of cooperative transmissions with delay asynchronism and ISI

We consider the cooperative transmission among nodes 1 to J. The passband signal to be transmitted by each transmitter i has a general form $\mathrm{Re}[\sum_{m=-\infty}^{\infty} s_i(m)\, p_b(t-mT) e^{j2\pi f_c t}]$, where $s_i(m)$ is the complex symbol transmitted, $p_b(t)$ is the baseband pulse shaping filter, and f_c is the carrier frequency. After delaying with δ_i, the signal received by the receiver is

$$r_p(t) = \mathrm{Re}\left[\sum_{i=1}^{J} \alpha_i \sum_{m=-\infty}^{\infty} s_i(m)\, p_b(t-mT-\delta_i) e^{j2\pi f_c (t-\delta_i)} + v_p(t) \right] \qquad (2.1)$$

where α_i are (complex) fading of the propagation. Without loss of generality, we can demodulate (2.1) to obtain the continuous-time complex baseband signal

$$r_b(t) = \sum_{i=1}^{J} \alpha_i e^{j\theta_i} \sum_{m=-\infty}^{\infty} s_i(m)\, p_b(t - mT - \delta_i) + v_b(t) \tag{2.2}$$

where the phase $\theta_i = -2\pi f_c \delta_i$.

Since δ_i may be different for different transmitters, without loss of generality we perform baseband sampling at time instant $nT + \tau$, which gives the sample $x(n) = r_b(nT + \tau)$, where $0 \le \tau < T$. The sample can be written as

$$x^{(\tau)}(n) = \sum_{i=1}^{J} \alpha_i e^{j\theta_i} \sum_{m=-\infty}^{\infty} s_i(m)\, p_b[(n-m)T + \tau - \delta_i] + v^{(\tau)}(n) \tag{2.3}$$

We assume that the pulse shaping filter have support $[-KT, KT]$. Obviously, each sample $x^{(\tau)}(n)$ depends on multiple transmitted symbols, so the channel should be dispersive.

Define channel coefficients (due to pulse shaping only, not the propagation flat fading) as

$$h_i(l) = p_b(lT + \tau - \delta_i) \tag{2.4}$$

Then the received sample can be written as

$$x^{(\tau)}(n) = \sum_{i=1}^{J} \alpha_i e^{j\theta_i} \sum_{l=-\infty}^{\infty} h_i(l)\, s_i(n-l) + v^{(\tau)}(n) \tag{2.5}$$

Define the lower range and the upper range of l as

$$L_{i,\tau}^{L} = \left\lceil -K + \frac{\delta_i - \tau}{T} \right\rceil, \quad L_{i,\tau}^{U} = \left\lfloor K + \frac{\delta_i - \tau}{T} \right\rfloor \tag{2.6}$$

Then the channel model becomes

$$x^{(\tau)}(n) = \sum_{i=1}^{J} \alpha_i e^{j\theta_i} \begin{bmatrix} h_i(L_{i,\tau}^{L}) & \cdots & h_i(L_{i,\tau}^{U}) \end{bmatrix} \begin{bmatrix} s_i(n - L_{i,\tau}^{L}) \\ \vdots \\ s_i(n - L_{i,\tau}^{U}) \end{bmatrix} + v^{(\tau)}(n) \tag{2.7}$$

Using the model (2.7), we can either find ways to mitigate the channel dispersion, and hence ISI, or otherwise suffer from ISI-induced SIR reduction. To evaluate the performance degradation due to channel dispersion, we consider only the *pre-processing* of the received samples without knowing the encoding details. We will try to restore the original flat fading channels by mitigating dispersion (though we still have delays in integer symbol intervals). Then we will evaluate the interference due to residue dispersion, and the reduction of SIR.

As a basis for comparison, we let the receiver just use the flat fading channel model by assuming all other channel coefficients in (2.7) are interference. We define the SIR as

$$\mathrm{SIR} = \frac{\sum_{i=1}^{J} \max_l |h_i(l)|^2}{J \sum_{i=1}^{J} \left(\sum_l |h_i(l)|^2 - \max_l |h_i(l)|^2 \right)} \tag{2.8}$$

For the ideal noisy case (without asynchronism) the signal-to-noise ratio (SNR) can be defined as $\mathrm{SNR} = J\sigma_s^2 / \sigma_v^2$, which is also the average over the fading coefficients. Then, in case of asynchronism, the extra interference in (2.7) makes the receiver's signal-to-interference-and-noise ratio (SINR) to be

$$\mathrm{SINR} = \frac{1}{\frac{1}{J\mathrm{SIR}} + \frac{1}{\left(\sum_{i=1}^{J} \max_l \frac{|h_i(l)|^2}{J}\right)\mathrm{SNR}}} \tag{2.9}$$

Therefore, both SIR and the reduced value of channel coefficients $\max_l |h_i(l)|^2$ make the SINR lower than the ideal case SNR. In particular, if SIR<<SNR, then SIR dominates and becomes the SINR floor, which means in high SNR environment, the SINR is limited to be SIR. On the other hand, if SIR>>SNR, then the interference does not degrade system performance too much.

By examining SIR instead of SINR, we can reduce complexity while are still able to show the impact of the asynchronism-induced interference. Therefore, to simplify the problem, we consider noiseless transmission so as to focus on the interference.

2.1 Use fixed sampling timing

We refer (2.7) as the "fixed" sampling scheme, and use it as a basis for comparison. With the fixed scheme, without loss of generality, we can use $\tau = 0$. We can decompose the delay δ_i into an integer value $\delta_i^{(1)}$ and a fractional value $\delta_i^{(2)}$. In addition, we assume that the delays of the transmitters are independent and uniformly distributed, which means $\delta_i^{(2)}$ is a uniform random variable. Then SIR (2.8) becomes

$$\mathrm{SIR} = \frac{\sum_{i=1}^{J} |\, p_b(\delta_i^{(2)} T)\,|^2}{J \sum_{i=1}^{J} \sum_k |\, p_b(kT + \delta_i^{(2)} T)\,|^2} \tag{2.10}$$

where the range of the integer k in the denominator of (2.10) is

$$\lceil -K - \delta_i^{(2)} \rceil \le k \le \lfloor K - \delta_i^{(2)} \rfloor, \quad k \ne 0 \tag{2.11}$$

2.2 Mitigate interference by optimizing sampling timing

A simple enhancement scheme is to look for the optimal time instant τ_o such that $\tau_o = \arg\max_{\tau \in [0,T)} \mathrm{SIR}$. With the optimized τ_o, we have channel coefficients $h_i(l) = p_b(lT + \tau_o - \delta_i)$. Similarly, we can define $\tau_o - \delta_i = d_i T + z_i T$, where d_i is an integer and $z_i \in (-1/2, 1/2]$. Then the SIR expression (2.8) becomes

$$\mathrm{SIR} = \frac{\sum_{i=1}^{J} |\, p_b(z_i T)\,|^2}{J \sum_{i=1}^{J} \sum_k |\, p_b(kT + z_i T)\,|^2} \tag{2.12}$$

where the range of the integer k in the denominator of (2.12) is

$$\lceil -K - z_i \rceil \le k \le \lfloor K - z_i \rfloor, \quad k \ne 0 \tag{2.13}$$

The major difference between (2.10) and (2.12) is that $\delta_i^{(2)}$ has uniform distribution, but z_i has a distribution more concentrated around 0, so that (2.12) is more likely larger than (2.13).

2.3 Mitigate interference by over-sampling and combining

The basic idea is that the received signals have a rich structure because of different delays, so the over-sampled signals contain new information. Consider over-sampling by a factor N, which means we have $N+1$ samples in each symbol interval at time instants τ_k, $k = 0,1,\cdots,N$, where $0 \le \tau_k < T$. Then for each τ_k, we have a sample model similar to (2.7). We can stack $N+1$ samples of each symbol interval for

$$\mathbf{x}(n) = \sum_{i=1}^{J} \alpha_i e^{j\theta_i} \mathbf{H}_i \mathbf{s}_i(n) + \mathbf{v}(n) \tag{2.14}$$

where the $(N+1)\times(L_i^U - L_i^L + 1)$ dimensional channel matrices

$$\mathbf{H}_i = \begin{bmatrix} \mathbf{0}_{L_{i,\tau_0}^L - L_i^L} & h_i(L_{i,\tau_0}^L) & \cdots & h_i(L_{i,\tau_0}^U) & \mathbf{0}_{L_i^U - L_{i,\tau_0}^U} \\ \vdots & & & & \vdots \\ \mathbf{0}_{L_{i,\tau_N}^L - L_i^L} & h_i(L_{i,\tau_N}^L) & \cdots & h_i(L_{i,\tau_N}^U) & \mathbf{0}_{L_i^U - L_{i,\tau_N}^U} \end{bmatrix} \tag{2.15}$$

Note that $\mathbf{0}_k$ denotes a $1\times k$ dimensional zero vector.

Then we can combine the samples by an $N+1$ dimensional vector $\mathbf{f}$ to obtain $y(n) = \mathbf{f}^H \mathbf{x}(n)$. Ideally (with zero-forcing criterion) we expect

$$y(n) \approx \sum_{i=1}^{J} \alpha_i e^{j\theta_i} g_i s_i(n - d_i) + w(n) \tag{2.16}$$

which becomes a flat fading channel model, although there may have integer delays. The key point is that the problems with respect to dispersive channels are gone.

Using zero-forcing criterion means that $\mathbf{f}^H \mathbf{H}_i \approx g_i \mathbf{e}_{d_i}^T$, $i = 1,\cdots,J$, where $\mathbf{e}_{d_i}$ is a unit vector with value 1 in the d_i^{th} entry and zeros elsewhere. One way to calculate the vector $\mathbf{f}$ is

$$\mathbf{f}^H = \begin{bmatrix} \mathbf{e}_{d_1}^T & \cdots & \mathbf{e}_{d_1}^T \end{bmatrix} \begin{bmatrix} \mathbf{H}_1 & \cdots & \mathbf{H}_J \end{bmatrix}^+ \tag{2.17}$$

The SIR of $y(n)$ can be calculated similarly as (2.8), but with the composite vectors $\mathbf{f}^H \mathbf{H}_i$ in place of $h_i(l)$.

2.4 Simulations and performance comparison

In this section, we use simulations to compare the SIR of the three schemes: *fixed* sampling time (Section 2.1), *selective* optimized sampling time (Section 2.2), and linear *combining* (Section 2.3). Figure 7 shows the cumulative distribution of SIR. Specifically, we see that for fixed method, the SIR has 80% probability of being lower than 15 dB. But for the selective method, the SIR has 80% probability to be higher than 15 dB. The combining method has 99% probability higher than 30 dB.

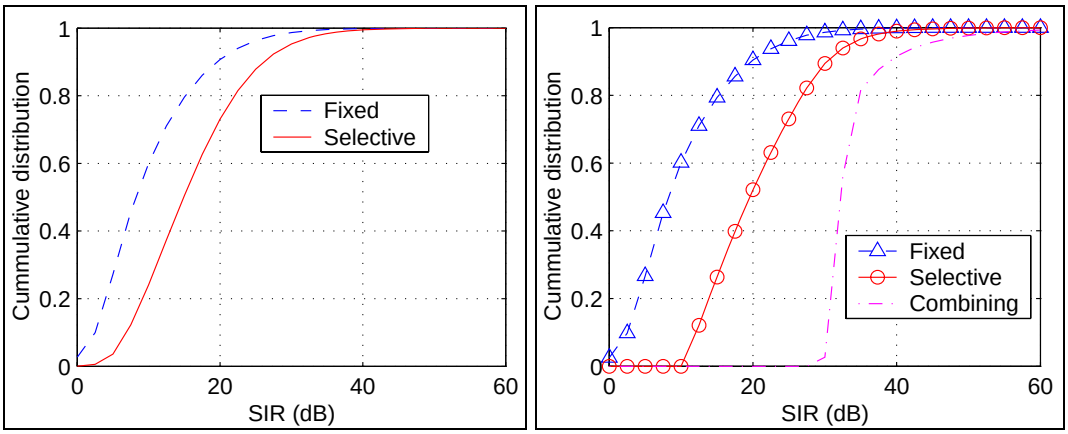

Figure 7. Cumulative distribution of SIR.

3. Using OFDM transmissions to combat channel dispersion

Orthogonal frequency division multiplexing (OFDM) transmission technique is desirable for combating the loss of timing-phase synchronization, since any limited propagation delay (or timing-phase) difference among the signals of cooperative transmitters can be tolerated by simply increasing the length of cyclic prefix (CP) [18][19]. Because of this, it may find wide applications in cooperative transmissions. Nevertheless, OFDM suffers critically from the loss of carrier frequency synchronization where the carrier-frequency offset (CFO) incurs inter-carrier interference (ICI). This CFO problem becomes much worse in multi-transmitter OFDM systems because of the increase in inter-transmitter interference, not only ICI [19]. Unfortunately, there have been no method that claims complete CFO cancellation (to our knowledge), and most existing methods primarily deal with small CFO only.

Considering that the CFO, or the overhead of achieving perfect synchronization otherwise, may severely degrade the gain of cooperation, it is more desirable to develop methods for the receiver to cancel CFO completely in cooperative OFDM transmissions. We here present a novel approach to realize such an objective. Our basic idea is to utilize the redundancy of the long CP for CFO mitigation or even cancellation. A unique feature of our approach is that it is implemented purely as a "pre-processing" procedure, independent from cooperative encoding/decoding details. In other words, it simply makes the CFO problem transparent to the cooperative OFDM transmission designs.

Consider a cooperative transmission system with I cooperative transmitters and one receiver. All the I cooperative transmitters are assumed to have the same data packet that is to be encoded and transmitted, using some predefined cooperative encoding schemes such as cooperative STBC. The encoder outputs $b_i(n)$ are then OFDM modulated, which gives the OFDM signal $s_i(n)$. The discrete baseband channel from the i^{th} transmitter to the receiver is assumed frequency selective fading with coefficients $h_i(l)$.

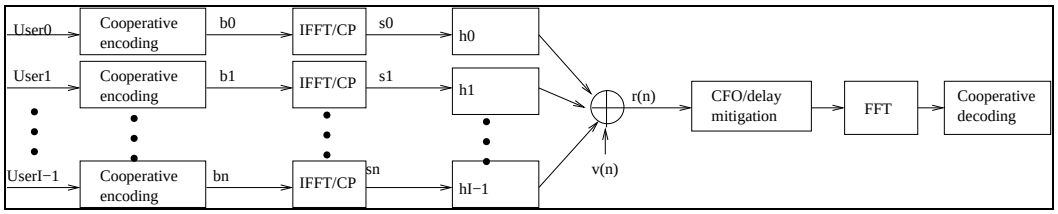

Figure 8. Multi-transmitter cooperative OFDM transmission and receiving block diagram.

From the received signal $r(n)$, the receiver mitigates the asynchronism in carrier frequency and timing using our proposed method, after which conventional OFDM demodulation and cooperative decoding techniques are applied.

With the consideration of asynchronous transmitters, the signal of each transmitter i may have a propagation delay d_i and a CFO ε_i (relative to a reference timing and a reference local carrier) when received at the receiver. We assume d_i to be integer (with symbol interval as unit) since the fractional portion of the delay contributes nothing but some extra channel dispersion which can be assimilated into the dispersive channel model. The CFO ε_i is derived as the residual carrier frequency normalized by the OFDM sub-carrier frequency separation.

The transmitted signal $s_i(n)$ is derived from the Inverse Fourier Transform (IFT) of the encoded symbol $b_i(n)$. Since there is no inter-block interference (IBI) thanks to cyclic prefix, we consider one OFDM block for notational simplicity. Then the i^{th} transmitter's signal $s_i(n)$ can be written as

$$s_i(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} b_i(k) e^{j2\pi nk/N}, \quad -N_g \le n \le N-1 \tag{3.1}$$

where N_g is the length of the CP and N is the IFT block length (we also define it as OFDM block length). The composite signal received by the receiver, with delay d_i and CFO ε_i considered, is

$$\mathbf{r}(0) = \sum_{i=0}^{I-1} e^{j\phi_i} \mathbf{E}_i(0) \mathbf{H}_i \mathbf{s}_i + \mathbf{v}(0) \tag{3.2}$$

where ϕ_i is the initial phase, the sample vector $\mathbf{r}(0) = \left[r(0) \ \cdots \ r(N-1) \right]^T$, the $N \times N$ diagonal matrix $\mathbf{E}_i(0) = \text{diag}\left\{ 1, e^{j\varepsilon_i}, \cdots, e^{j\varepsilon_i (N-1)} \right\}$ is the CFO matrix, the symbol vector $\mathbf{s}_i = [s_i(0), \cdots, s_i(N-1)]^T$, and the channel matrix is $N \times N$ circulant

$$\mathbf{H}_i = \begin{bmatrix} \mathbf{0}_{N-L-d_i} & h_i(L) & \cdots & h_i(0) & \mathbf{0}_{d_i-1} \\ \mathbf{0}_{N-L-d_i+1} & h_i(L) & \cdots & h_i(0) & \mathbf{0}_{d_i-2} \\ \vdots & \vdots & & \vdots & \vdots \\ \mathbf{0}_{N-L-d_i-1} & h_i(L) & \cdots & h_i(0) & \mathbf{0}_{d_i} \end{bmatrix} \tag{3.3}$$

Our basic idea is to exploit the redundancy of the CP based on the structure of the signal model (3.2). If the CP length N_g is longer than $L + \max\limits_{0 \le i < I-1} d_i$, then in addition to those in $\mathbf{r}(0)$, we have more IBI-free samples with which we can construct new sample vectors $\mathbf{r}(m) = [r(-m), \cdots, r(N-1-m)]^T$. Similarly to (3.2), we have

$$\mathbf{r}(m) = \sum_{i=0}^{I-1} e^{j\phi_i} \mathbf{E}_i(m)\mathbf{H}_i\mathbf{s}_i + \mathbf{v}(m) \tag{3.4}$$

where

$$\mathbf{E}_i(m) = \begin{bmatrix} \mathbf{0}_{(m|N)\times(N-m|N)} & \text{diag}\{e^{j\varepsilon_i(-m)},\cdots,e^{j\varepsilon_i(-m-1+m|N)}\} \\ \text{diag}\{e^{j\varepsilon_i(-m+m|N)},\cdots,e^{j\varepsilon_i(N-m-1)}\} & \mathbf{0}_{(N-m|N)\times(m|N)} \end{bmatrix} \tag{3.5}$$

Note that $(x \mid N)$ denotes $x \bmod N$.

Noticing that (3.2) and (3.4) contain the same $\mathbf{H}_i$ and $\mathbf{s}_i$ but have different CFO matrices, we can stacking together all available vectors $\mathbf{r}(m)$,

$$\begin{bmatrix} \mathbf{r}(0) \\ \vdots \\ \mathbf{r}(M-1) \end{bmatrix} = \sum_{i=0}^{I-1} e^{j\phi_i} \begin{bmatrix} \mathbf{E}_i(0) \\ \vdots \\ \mathbf{E}_i(0) \end{bmatrix} \mathbf{H}_i\mathbf{s}_i + \begin{bmatrix} \mathbf{v}(0) \\ \vdots \\ \mathbf{v}(M-1) \end{bmatrix} \tag{3.6}$$

which for notational simplicity can be denoted as

$$\mathbf{y} = \sum_{i=0}^{I-1} e^{j\phi_i} \mathbf{A}_i\mathbf{H}_i\mathbf{s}_i + \mathbf{u} \tag{3.7}$$

The dimensions of $\mathbf{y}$ and $\mathbf{A}_i$ are $MN \times 1$ and $MN \times N$, respectively.

Our basic idea is thus to design an $N \times MN$ CFO mitigation matrix $\mathbf{X}$ such that

$$\mathbf{X}\mathbf{A}_i = \mathbf{I}_N \tag{3.8}$$

for all $i = 0,\cdots,I-1$. If $\mathbf{X}$ is available for (3.8), then CFO can be mitigated via

$$\mathbf{z} = \mathbf{X}\mathbf{y} \tag{3.9}$$

Note that a straightforward solution for $\mathbf{X}$ is

$$\mathbf{X} = \begin{bmatrix} \mathbf{I}_N & \cdots & \mathbf{I}_N \end{bmatrix} \begin{bmatrix} \mathbf{E}_0(0) & \cdots & \mathbf{E}_{I-1}(0) \\ \vdots & & \vdots \\ \mathbf{E}_0(M-1) & \cdots & \mathbf{E}_{I-1}(M-1) \end{bmatrix}^{+} \tag{3.10}$$

If (3.8) can be satisfied perfectly, then we have $\mathbf{z} = \sum_{i=0}^{I-1} e^{j\phi_i} \mathbf{H}_i\mathbf{s}_i + \mathbf{X}\mathbf{u}$, which is a conventional CFO-free OFDM sample vector after removing the CP. With the vector $\mathbf{z}$, conventional OFDM demodulation can be applied to detect symbols $b_i(k)$.

We have found in [P2] that CFO can be completely removed only if CP is long enough and appropriate sample vectors $\mathbf{r}(m)$ are used. Not all available $\mathbf{r}(m)$ need to be used though and in fact, using less $\mathbf{r}(m)$ leads to reduced complexity. The inverse of the big matrix $\mathbf{X}$ can be avoided by exploiting the special structure of $\mathbf{E}_i(m)$.

Specifically, the computational complexity consists of two parts. The first part is the calculation of $\mathbf{X}$, where the good news is that $\mathbf{X}$ needs to be calculated only once (for all OFDM blocks) if ε_i is not time-varying. In this case, the complexity is in the order of $O(NI^3)$. The second

part is the calculation of $\mathbf{Xy}$ for each OFDM block, where the complexity is $O(NI)$ since the majority of $\mathbf{X}$ entries are zeros. Considering that the first part happens only once and I (the number of cooperative transmitters) is usually much smaller than N, the proposed algorithm has complexity almost linear in N, which is very efficient.

We have also derived the following proposition regarding complete CFO cancellation.

Proposition 2: Let the CP length be $N_g \geq (I-1)N + L + \max_{0 \leq i < I} d_i$. With appropriate parameters m for $\mathbf{r}(m)$, CFO can be completely canceled if $\varepsilon_i - \varepsilon_j \neq 2\pi l / N$, for any $i \neq j$ and integer l.

The proposed method is desirable for cooperative transmissions in ad hoc wireless networks, where the long CP (repeated transmissions like spectrum-spreading) is used for CFO cancellation, for high transmission power efficiency as well as for better noise/interference suppression. Some other benefits of the implementation specified by the Proposition 2 come from the Vandermonde matrix. Vandermonde equation systems have very efficient algorithms to solve, with complexity $O(I^2)$ instead of $O(I^3)$. As a result, the complexity of calculating $\mathbf{X}$ becomes $O(NI^2)$, instead of $O(NI^3)$. Furthermore, Vandermonde system solver can usually give surprisingly accurate solutions, even for ill-conditioned matrix. This property is especially helpful in the case where some CFOs ε_i are close to each other.

In order to evaluate the performance of our algorithm, we have simulated a system with two cooperative transmitters and one receiver, using Alamouti STBC. We compared the performance of our algorithm against the ideal cooperative transmissions with perfect synchronization ("Perfect"), as well as two other OFDMA CFO mitigation methods: [20] ("CLJL") and [21] ("HL"). We used $N = 32$, QPSK. The integer delays d_i, the CFOs ε_i, and the channels (with order $L = 3$) were all randomly generated for each transmitter during each run of the simulation. We used 10,000 runs of the simulations to derive the average symbol error rate (SER) under various signal-to-noise ratios (SNR) or various CFO.

From the simulations results shown in figure 9, we can see that our algorithm has much better performance when SNR is not extremely low, and the advantage is even more significant for large relative CFO. In particular, when relative CFO is 0.5, "HL" and "CLJL" failed, but our algorithm had a performance almost independent of the size of relative CFO. In addition, we have verified the "independence" of our algorithm to various CFOs. The conventional method did not resolve the CFO problem, and neither did the "HL" scheme when the rCFO was not very small. In contrast, our new method showed almost constant performance under various rCFO.

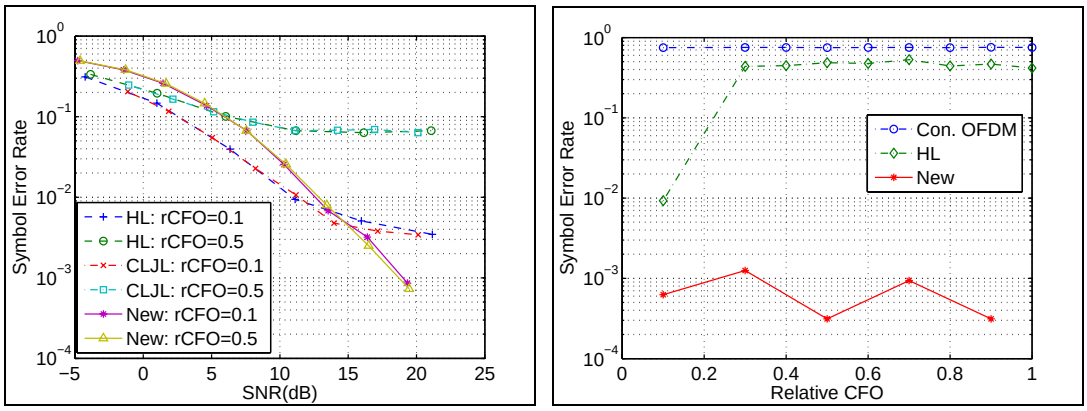

Figure 9. Left: Performance comparison of our algorithm with HL [21] and CLJL [20] for CFO mitigation under rCFO 0.1 and 0.5. Right: Performance comparison of our "New" CFO mitigation algorithm with the conventional OFDM receiver and the CFO mitigation algorithm "HL" [21]. SNR 20 dB.

4. Extensions to MC-DS-CDMA

In [P3], we have extended the CFO mitigation method in Section 3 into MC-DS-CDMA systems, and have proposed a new receiving algorithm for MC-DS-CDMA systems when carrier frequency offset (CFO) is significant. By exploiting the special structure of the CFO contaminated signals, the new algorithm cancels CFO completely during the dispreading procedure, after which the despread CFO-free signal is demodulated via normal FFT-based OFDM demodulator. While guaranteeing complete CFO cancellation, this method is advantageous over the majority existing CFO-mitigation techniques that can only mitigate but not completely remove CFO. An efficient algorithm is developed, and simulations are conducted to demonstrate the performance.

Cooperative communication is an important concept in wireless networks. We will continue study its implementations and applications, not only in wireless security, but also in communication efficiency. On the other hand, we have also noticed its interesting relation to another important concept: cross-layer design. Work is being conducted by us along this line.

Part III: Cooperative Transmissions Testbed Development

1. Introduction

The objective for this testbed development is to demonstrate the concepts of cooperative transmissions and secure array transmissions that we have developed. By using wireless communication modules purchased from comblock.com, we are building a wireless transmission testbed for demonstrating our results in both secure communications and cooperative communications. As specified in the research topic 4.2 of the project proposal, the testbed is needed to show that the proposed security schemes work in practice and also to show how difficult it is to implement it. The testbed is also important to demonstrate the cooperative transmission schemes, since we have considered practical problems such as the lack of synchronization.

The reason that we use comblock.com modules is for low-cost implementation. However, those devices are for single antenna transmission and receiving only, not for antenna array transmissions. Therefore, we need overcome this major hurdle, i.e., find ways to use such ComBlock modules to emulate antenna array transmissions and receiving. We have been trying two different approaches for this objective.

The first approach is to re-wire hardware. After some studying and trying, we find a specific wire that initializes the working of the module. Therefore, we replace this wire by an external trigger signal that is under our control, by which we are able to initiate the transmission of the two transmitters at the same time, so as to have them to emulate antenna array transmissions.

The second approach is to develop new software to replace the existing "ComBlock Control Center" software provided by comblock.com. The existing software is designed to control one ComBlock module only, so for two transmitters, we have to use either two computers or to open two "ComBlock control center" windows in the same computer. This means it is impossible for us to make the two transmitters to begin transmit at the same time. Our objective is to design new software so that we can initiate the two transmitters at the same time. Much effort has been spent from the summer of 2006, and some initial progress has been achieved. For example, we have setup the new control window, and can "ping" the modules via TCP/IP communications. We have also demonstrated that our software can initiate the transmission of two transmitters, which is achieved by writing to some special registers. Nevertheless, this software approach needs more time to finish. So far, most of our efforts are in the hardware approach.

We have adopted a hardware approach to wire the two transmitters together. In order for the two transmitters to transmit at approximately the same time, we use the optional external trigger signal of the ComBlock devices, and use an external switch to initiate the transmission of the two devices at the same time. In addition, the two transmitters need to guarantee a similar carrier frequency, which is achieved by using a common external carrier frequency reference signal. Another issue is the sampling clock, which fortunately does not show any extra requirement for further synchronization. The sampling clocks of the two transmitter devices are already close enough. But if otherwise, we can also use an external sampling clock reference signal. So far this does not seem necessary.

2. Testbed development description

First, we have screwed the devices onto hard plastic boards. Each whole transmitter or receiver is screwed on one board, as shown in figure 10.

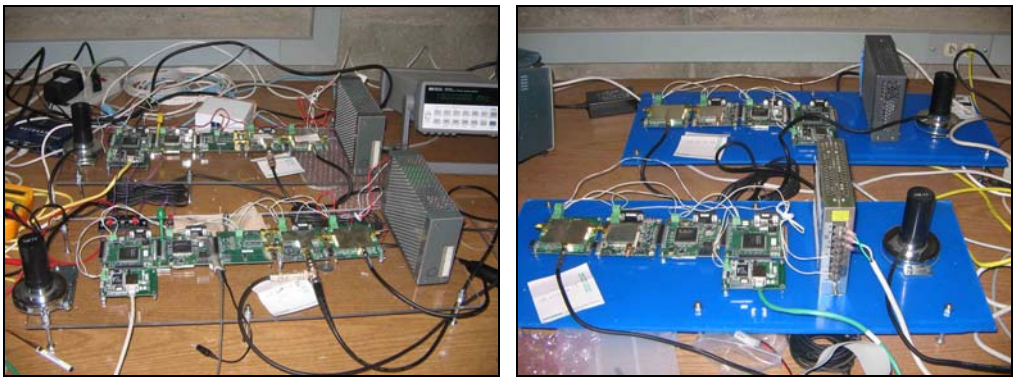

Figure 10. Left: two transmitters. Right: two receivers.

Next, in order to explain the working of the transmitters, let us first have a look at the whole transmitter structure shown in figure 11.

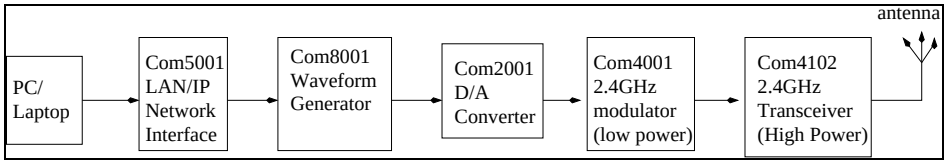

Figure 11. Transmitter bock diagram as implemented by ComBlock boards.

Using the ComBlock Control Center GUI software provided by comblock.com, the initialization of the transmission is as follows: 1) upload the transmission data (generated from MATLAB modulator) into Com8001; 2) in ComBlock Control Center, select "continuous download" to begin transmission.

We exploit the fact that ComBlock devices provide an optional initiation approach, i.e., using an external trigger signal. In Com8001, there is an "EXT_TRIGGER_IN" input signal (connected to Com5001 EXT_TRIGGER_OUT). This trigger signal is optional in default. To use this external trigger feature, we can apply either a software approach or a hardware approach. We have thus far implemented the hardware approach. As shown in the right figure, we connect the EXT_TRIGGER_IN to a 3.3V output signal provided by the Com8001, through a switch. So, in order to initiate transmission, we do the following:

1) Upload the transmission data (generated from MATLAB modulator) into Com8001;

2) Use ComBlock Control Center to set Com8001 in “continuous download” and “external trigger enable” modes, i.e., set the Register 19 to “09” for the former and the Register 21 to “01” for the latter;

3) Press the switch once, then the transmitter begins transmission repeatedly. Note that in order to stop the transmission, we just need to use ComBlock Control Center to set the Register 19 of Com8001 into “0B”.

The same trigger signal can be sent to anther transmitter, so that the two transmitters can be set to start transmission at approximately the same time. This is the hardware approach for us to wire the two independent transmitters for emulating a transmission array.

In order to make sure that the two transmitters have approximately the same carrier frequency, we can use the same external 10 MHz reference signal. The Com4001 can use either the internal reference signal or the external 10 MHz reference signal for the oscillator to generate the carrier signal. As shown in figure 11, we provide the external 10 MHz reference signal (from a signal generator) to the Com4001 of both transmitters. Then we use ComBlock Control Center to set the Com4001 Register 6, bit 1, to be “1” to use the external reference signal. Note that this is for emulating antenna array transmissions. For emulating cooperative transmissions, we may not need such a common reference signal, because carrier frequency difference is actually something we have to deal with, as shown by our research results described in the last report.

With the external reference signal, the carrier frequencies of the two transmitters become very similar. In our preliminary modulation/demodulation experiments, the two transmitters have carrier frequencies as close as to 100 Hz. Furthermore, this small discrepancy may be due to our current demodulation algorithm that does not estimate carrier frequency accurately enough.

Using the above wiring schemes, we have also tried array transmissions. The demodulation results are very good, almost without errors. The error rate is only slightly worse than a single transmitter case. Note that this preliminary result only shows that the array transmission is in effective. In order to estimate channels from two transmitters by only a single receiver, we simulated direct-sequence spread spectrum (DSSS) transmissions, and compiled receiving algorithms. We have successfully run the experiments, and have estimated the channels. Detailed of experiment, MATLAB codes, and source data can be found in [13].

3. Some observations and future work

The testbed is very good to demonstrate the cooperative transmissions with asynchronous transmitters.

We have clearly seen the delay difference and carrier frequency difference between the two transmitters. We have two journal papers in preparation, one for the synchronization-induced ISI, and the other for CFO mitigation in MC-DS-CDMA. We have the plan of including the testbed experiments as demonstrations in these two papers.

In addition, we have found that the residue phase of the carrier has a significant impact on the channels. We have run multiple experiments, and found that the channels usually have the same power, but different phase from each running. This indicates that propagation channels are quite

constant, but they have a phase changing due to the phase synchronization error. This effect has both advantages and disadvantages for our proposed secure transmissions.

The advantage is that the phase difference can be exploited by the transmitters and the receivers to make the channels even more independent. For example, some intentional phase jitter may be introduced by the PLL circuits to make the channels different.

On the other hand, the disadvantage is that a time-varying channel may change the channel reciprocity, or may prevent the application of channel-feedback for the transmitters to get and utilize the channel state information.

We have realized that this special phase synchronization problem is specific to our testbed. Because the receiver has no built-in PLL for carrier tracking, but just using its own local carrier to conduct demodulation, it relies on the receiving program to compensate for the carrier offset. We have programmed successfully to track perfectly the carrier frequency, but the phase tracking is still a problem.

In the future work, we will continue to work on the phase tracking problem, and would like to see how accurate we can track the phase. Although we have found that our program can successfully track phase in clear (good) artificial signals, but it still has some problems when applied to real received signals. Furthermore, we would like to see how actual analog/digital PLL circuits such as the Costas' Loop can track the phase.

After we have the new phase tracking programs that are able to process real signals, we will estimate the channel properties of the array, and test our secure transmission schemes. In particular, we need to verify the channel reciprocity or channel feedback property. Various cooperative transmission schemes can also be verified.

A software-approach can be helpful for more flexible experiments, not only for our secure/cooperative transmissions, but also for extending our testbed to a more general software-defined radio or cognitive radio. For this purpose we need to program our own control software instead of using the ComBlock Control Center. So far, we have showed the critical TCP/IP communications between our program and the ComBlock devices. As a result, the subsequent work might just be some painstaking programming.

References

[1] O. Hero, III, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235-3249, Dec. 2003.

[2] X. Li, M. Chen and P. Ratazzi, "A randomized space-time transmission scheme for secret-key agreement," *CISS'2005*, Johns Hopkins University, Mar. 2005.

[3] X. Li, M. Chen and E. P. Ratazzi, "Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy," *the 6th IEEE Int. Workshop on Signal Processing Advances in Wireless Commun.* (SPAWC'05), Columbia University, New York, Jun. 2005.

[4] X. Li, M. Chen and E. P. Ratazzi, "Array-transmission based physical-layer security techniques for wireless sensor networks," *the 2005 IEEE Int. Conf. on Mechatronics and Automation* (IEEE ICMA'2005), Niagara Falls, Ontario, Canada, July 2005.

[5] X. Li and E. P. Ratazzi, "MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks," *IEEE MILCOM'2005*, Atlantic City, NJ, Oct. 2005.

[6] S. Haykin, *Blind Deconvolution*, Prentice Hall, Englewood Cliffs, NJ, 1994.

[7] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733-742, Mar. 1993.

[8] J. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.

[9] G. B. Giannakis, Y. Hua, P. Stoica and L. Tong, *Signal Processing Advances in Mobile and Wireless Communications, Vol. 1: Trends in Channel Estimation and Equalization*, Prentice-Hall, Englewood Cliffs, NJ, 2000.

[10] J. Q. Bao and L. Tong, "Protocol-aided channel equalization in wireless ATM," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 418-435, Mar. 2000.

[11] D. N. Godard, "Self-recovering equalization and carrier tracking in two-dimensional data communication systems," *IEEE Trans. Commun.*, vol. COM-28, pp. 1867-1875, Nov. 1980.

[12] X. Li, "Blind channel estimation and equalization in wireless sensor networks based on correlations among sensors," *IEEE Trans. Signal Processing*, vol. 53, no. 4, pp. 1511-1519, Apr. 2005.

[13] Simulation data and experiment details are available at *http://ucesp.ws.binghamton.edu/SecTran07.htm*.

[14] S. M. Alamouti, "A simple transmitter diversity scheme for wireless communications," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 1451-1458, Oct. 1998.

[15] X. Li, "Space-time coded multi-transmission among distributed transmitters without perfect synchronization," *IEEE Signal Process. Lett.*, vol. 11, no. 12, pp. 948-951, Dec. 2004.

[16] Y. Mei, Y. Hua, A. Swami and B. Daneshrad, "Combating synchronization errors in cooperative relay," *IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Philadelphia, PA, Mar. 2005.

[17] Y. Shang and X.-G. Xia, "Shift full rank matrices and applications in space-time trellis codes for relay networks with asynchronous cooperative diversity," *IEEE Trans. Inform. Theory*, July 2006, to appear.

[18] S. Barbarossa and G. Scutari, "Distributed space-time coding strategies for wideband multi-hop networks: regenerative vs. non-regenerative relays," *Proc. of ICASSP 2004*, Montreal, Canada, June 2004.

[19] F. Ng and X. Li, “Cooperative STBC-OFDM transmissions with imperfect synchronization in time and frequency,” *IEEE 39th Asilomar Conf. on Signals, Systems and Computers*, Pacific Grove, CA, Oct. 30-Nov. 2, 2005.

[20] J. Choi, C. Lee, H. W. Jung and Y. H. Lee, “Carrier frequency offset compensation for uplink of OFDM-OFDMA system,” *IEEE Commun. Lett.*, vol. 4, no. 12, pp. 414-416, Dec. 2000.

[21] D. Huang and K. B. Letaief, “An interference-cancellation scheme for carrier frequency offsets correction in OFDMA systems,” *IEEE Trans. Commun.*, vol. 53, no. 7, pp. 1155-1165, July 2005.

List of Acronyms

AFRL	Air Force Research Laboratory
AGWN	Additive Gaussian White Noise
BER	Bit Error Rate
BPSK	Binary Phase-Shift Keying
CDMA	Code Division Multiple Access
CFO	Carrier Frequency Offset
CP	Cyclic Prefix
DSSS	Direct Sequence Spread Spectrum
EM	Electromagnetic
FDTD	Finite Difference Time Domain
FFT	Fast Fourier Transform
GUI	Graphical User Interface
IBI	Inter-Block Interference
ICI	Inter-Carrier Interference
IFT	Inverse Fourier Transform
LPI	Low Probability of Intercept
MILCOM	Military Communications Conference
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
OPSK	Quadrature Phase-Shift Keying
PI	Principal Investigator
PLL	Phase Locked Loop
SER	Symbol Error Rate
SINR	Signal-to-Interference-and-Noise Ratio
SIR	Signal-to-Interference Ratio
SNR	Signal-to-Noise Ratio
STBC	Space-Time Block Codes
TCP/IP	Transmission Control Protocol/Internet Protocol