AFRL-IF-RS-TR-2005-279
Final Technical Report
July 2005

COOPERATIVE COMMUNICATIONS FOR WIRELESS INFORMATION ASSURANCE

State University of New York at Binghamton

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

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

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2005-279 has been reviewed and is approved for publication

APPROVED: /s/

E. PAUL RATAZZI
Project Engineer

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, JR., Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	JULY 2005	Final May 04 – Aug 04

4. TITLE AND SUBTITLE
COOPERATIVE COMMUNICATIONS FOR WIRELESS INFORMATION ASSURANCE

5. FUNDING NUMBERS
C - FA8750-04-1-0213
PE - 61102F
PR - 558B
TA - II
WU - RS

6. AUTHOR(S)
Xiaohua (Edward) Li

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
State University of New York at Binghamton
Binghamton New York 13902

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/IFGB
525 Brooks Road
Rome New York 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2005-279

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: E. Paul Ratazzi/IFGB/(315)330-3765/ Paul.Ratazzi@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

This report describes research in the 2004 Summer Visiting Faculty Research Program from May 04 – Aug 04. Three of our research topics within the field of wireless communication networks are included: theory of physical-layer security, realizing physical-layer security for 802.11b wireless LAN, and cooperative communications in distributed sensor networks.

14. SUBJECT TERMS
WLAN, Physical-Layer Security, Cooperative Communications, Wireless Information

15. NUMBER OF PAGES
25

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

List of Figures

This report consists of two parts. The first part develops physical-layer security theory and proposes its realization in WLAN. The second part addresses cooperative communications in sensor networks. To save space, some details have been skipped, but can be referred in [31]-[34].

Part 1
Randomized Array Transmissions for Physical-layer Secured Wireless Communications

1.1. Introduction

For the rapidly growing wireless communications, security has become one of the major concerns [1]. Compared with wireline networks, wireless networks lack a physical boundary due to the broadcasting nature of wireless transmissions. This unique physical-layer weakness calls for innovative physical-layer security designs in addition to, and integrated with, the traditional data encryption approaches.

Existing physical-layer security techniques may be classified into three categories: i) power approach like beamforming and directional transmissions, ii) code approach like spread-spectrum [2], and iii) channel approach like [3,4,5]. They usually depend on some strong assumptions for secrecy, e.g., the unauthorized user has null-receiving energy, or has no information about the spreading codes or the propagation channel. If these assumptions hold, then secrecy is trivially achieved, otherwise secrecy is lost. As a result, it is difficult to conduct a meaningful secrecy analysis that measures the performance of a technique under varying conditions and assumptions.

Unfortunately, such strong assumptions can be easily violated. Beamforming techniques can only reduce, not completely nullify, the signal energy toward the unauthorized users, especially for those inside the transmission beam. Spreading codes may be easily estimated by the unauthorized user from the received signals [6]. The unauthorized user may use blind equalization algorithms [7, 8] to estimate channels, which causes many channel-based approaches such as [3] to lose secrecy. Even for the timing-based approach [4] which exploits the channel reciprocity, certain brute-force methods may efficiently break the secrecy by examining all possible timing.

It is well known that data encryption techniques realize computational secrecy instead of perfect secrecy [9] because perfect secrecy requires transmitting a key as long as the data. The key distribution usually remains as a weakness for encryption techniques. Interestingly, perfect secrecy is suggested in [5,3] as achievable with physical-layer techniques, although some unrealistic assumptions have to be made, such as channels are unknown to the unauthorized user or the channel of the unauthorized user is noisier than that of the authorized user.

We propose new physical-layer transmission techniques to realize secrecy under more reasonable assumptions. We assume that the unauthorized user may have better received signal quality and knows all the transmission protocols. There are no secret keys shared by the transmitters and the authorized user before transmission, and both of them have no knowledge of the unauthorized user.

We depend on two special properties of wireless transmissions for secure designs. First, signals received by the authorized user and the unauthorized user are different because their channels are different. Second, channels between the transmitters and the authorized user can be reciprocal [10] and can be adjusted intentionally [11]. The first property is due to multipath propagation and independent fading [12], whereas the other one has been widely accepted in literature [12] with some supportive demonstration from time-reversal mirror experiments [13]. These properties make physical-layer security techniques quite different from data encryption approaches.

Our primary objective is to develop randomized array transmission schemes for computational secrecy, though perfect secrecy is shown to be realizable under some circumstances. The transmission schemes are presented within the framework of a cooperative array formed by a group of cooperating transmitters, each of which may have only a single transmitting antenna. Physical antenna array is included in this framework as a special case. Cooperative transmitters are not only more cost-effective for implementing large arrays, but also more flexible for creating desirable channel conditions. On the other hand, cooperative array is more challenging in terms of synchronization among the transmitters.

This part is organized as follows. In Section I.2, a framework of cooperative array transmission is formulated with synchronous flat-fading channels. In Section I.3, a transmission scheme is developed for security based on the inherent ambiguity of blind equalization. Then, assuming the unauthorized user knows its own channels, a random-matrix scheme is developed in Section I.4. In Section I.5 these schemes are extended to dispersive channels with imperfect synchronization. Simulations are given in Section I.6. In Section I.7, we describe their realizations in 802.11 WLAN.

1.2. System description

We consider a wireless network where mobile users communicate with a base-station which has J transmitting antennas. The base-station has either one transmitter with a physical antenna array, or J cooperative transmitters. We consider the latter since it includes the former as a special case. The J transmitters communicate with each other using a secure link, such as the wireline Ethernet or some cables that directly connect them together. Packets are transmitted by the J transmitters cooperatively, during which any unauthorized user should be deprived of signal interception capability, as illustrated in Fig. 1.

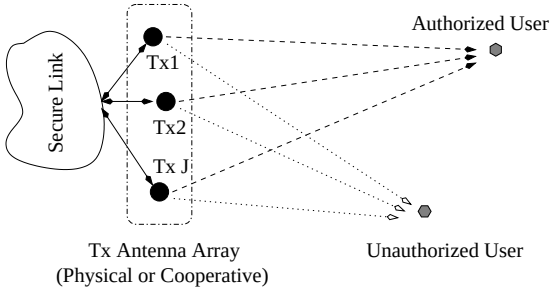


Fig. 1. System model for secured array transmission with either J cooperative transmitters or one transmitter with a physical antenna array.

A beamforming-like array transmission procedure shown in Fig. 2 is used by the J transmitters. A symbol sequence $\{b(n)\}$, obtained via any traditional modulation scheme, is fed to all J transmitters. Before transmission, the sequence is processed by the transmitters. Though more complex filters can be used, we consider single-tap weights $w_i(n)$ for simplicity. In addition, each of the transmitters may appropriately delay (or advance) the signal by δ_i. The transmitted signal from the transmitter i is thus $s_i(n)$, whereas the authorized user receives signal $x(n)$.

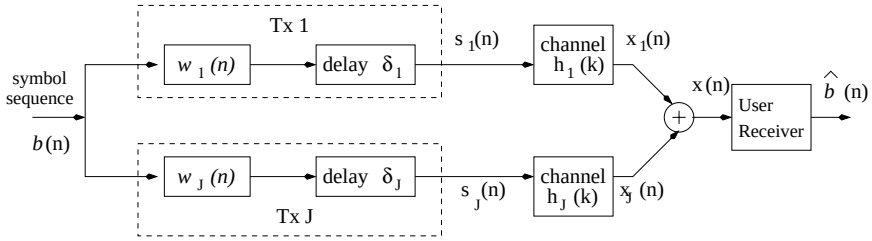


Fig. 2. The block diagram of array transmission.

If a physical antenna array is used and the propagation channel is Rayleigh flat fading, the received signal at the authorized user is

$$x(n) = \sum_{i=1}^{J} h_i^* s_i(n) + v(n) \overset{\Delta}{=} \mathbf{h}^H \mathbf{s}(n) + \mathbf{v}(n), \tag{1}$$

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

$$\mathbf{h} \overset{\Delta}{=} \begin{bmatrix} h_1 \\ \vdots \\ h_J \end{bmatrix}, \quad \mathbf{s}(n) \overset{\Delta}{=} \begin{bmatrix} s_1(n) \\ \vdots \\ s_J(n) \end{bmatrix} = \begin{bmatrix} w_1(n) \\ \vdots \\ w_J(n) \end{bmatrix} b(n) \overset{\Delta}{=} \mathbf{w}(n)\, b(n). \tag{2}$$

In this part, $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ denote conjugation, transposition and Hermitian, respectively. Since channel estimation is required, we assume that $\mathbf{h}$ is block fading [3], i.e., it is constant or slowly time-varying when transmitting a block of symbols but may change randomly between blocks. The symbols $b(n)$ are independent uniformly distributed with zero-mean and unit variance.

The unauthorized user may use multiple receiving antennas for better interception, and the interception becomes much easier with a flat-fading channel model. Therefore, we consider the worst case (to the transmitters and the authorized user) where the unauthorized user receives signals from M receiving antennas

$$\begin{bmatrix} x_{u,1}(n) \\ \vdots \\ x_{u,M}(n) \end{bmatrix} = \begin{bmatrix} h_{u,1,1} & \cdots & h_{u,1,J} \\ \vdots & & \vdots \\ h_{u,M,1} & \cdots & h_{u,M,J} \end{bmatrix} \begin{bmatrix} w_1(n-d_{u,1})b(n-d_{u,1}) \\ \vdots \\ w_J(n-d_{u,J})b(n-d_{u,J}) \end{bmatrix} + \begin{bmatrix} v_{u,1}(n) \\ \vdots \\ v_{u,M}(n) \end{bmatrix}. \tag{3}$$

The notations are similar to (1) except that $(\cdot)_u$ is used to denote the unauthorized user. The delays $d_{u,i}$ may not be zero because the transmitters adjust δ_i in favor of the authorized user. While introducing such delays is an important way for enhancing security, we assume zero delays for simplicity, i.e., $d_{u,i} = 0$ for all i. The equation (3) can then be written as

$$\mathbf{x}_u(n) = \mathbf{H}_u \mathbf{w}(n) b(n) + \mathbf{v}_u(n). \tag{4}$$

Each element of the channel matrix $\mathbf{H}_u$ has the same distribution as h_i, but is independent from h_i.

We focus only on the security of the downlink transmission (from the base-station to the authorized user). Once the downlink is secured, the uplink can be easily secured by using similar techniques and/or by exchanging encryption keys frequently.

1.3. A randomized transmission scheme and computational secrecy

In this subsection, we assume that the unauthorized user does not know the channels $\mathbf{h}$ and $\mathbf{H}_u$. But it may try to estimate them by training/blind methods, or by a brute-force search of all possible channels. The transmitters and the authorized user do not know all channels either, and have no ways to estimate $\mathbf{H}_u$. Ways have to be designed for them to estimate $\mathbf{h}$ and symbols, during which no information should be obtained by the unauthorized user for successful interception.

1.3.1. Transmission and receiving procedure

We first give the downlink transmission and receiving procedure with the consideration of the signal model (1)-(2). According to the received signal

$$x(n) = \mathbf{h}^H \mathbf{w}(n) b(n) + v(n), \tag{5}$$

the transmitters need to use special transmitting weights $\mathbf{w}(n)$ to fulfill the security objective. Our basic idea is to make $\mathbf{h}^H \mathbf{w}(n)$ deterministic but $\mathbf{H}_u \mathbf{w}(n)$ changing randomly in each symbol interval. For this purpose, $\mathbf{w}(n)$ should be random since the transmitters do not know $\mathbf{H}_u$.

We design the transmitting weights vector $\mathbf{w}(n)$ such that

$$\mathbf{h}^H \mathbf{w}(n) = \|\mathbf{h}\|, \tag{6}$$

where $\|\mathbf{h}\| = \sqrt{\sum_{i=1}^{J} |h_i|^2}$. Although (6) looks similar to transmission beamforming [10], the major difference is that $\mathbf{w}(n)$ changes randomly after each symbol $b(n)$ is transmitted. This can be realized by selecting randomly the elements of $\mathbf{w}(n)$ while satisfying the constraint (6). Obviously, if the channel $\mathbf{h}$ is constant or slowly time-varying, we need $J \geq 2$ transmitters. This explains why array transmission is required.

The authorized user can detect symbols after estimating the received signal power $\|\mathbf{h}\|^2$,

$$\hat{b}(n) = \|\mathbf{h}\|^{-1} x(n), \tag{7}$$

where $\|\mathbf{h}\|^2$ can be estimated as $\frac{1}{N}\sum_{n=1}^{N} |x(n)|^2$. If $b(n)$ is designed with constant magnitude $|b(n)|$, e.g., using PSK modulation, then we can simply use $|x(n)|$ in place of $\|\mathbf{h}\|$, i.e., use the phase of $x(n)$ for symbol detection.

To implement this transmission scheme, the channel $\mathbf{h}$ has to be known to the transmitters instead of the receiver. There are at least two ways for the transmitters to estimate the channel $\mathbf{h}$. First, if the downlink and uplink channels are reciprocal, the transmitters can estimate $\mathbf{h}$ directly from the uplink received signals. This is the case in fast time-division-duplexing (TDD) transmissions [10], [12].

The second way is to ask the authorized user to feedback some received signal information to the transmitters. Since explicit training should be avoided, the transmitters can send a training sequence randomized by $\mathbf{w}(n)$ which are known to themselves only. The authorized user only estimates and feedbacks $y(n) = \mathbf{h}^H \mathbf{w}(n)$, with which the transmitters can estimate channel $\mathbf{h}$ based on their knowledge of $\mathbf{w}(n)$,

$$\hat{\mathbf{h}}^H = \begin{bmatrix} y(1) & \cdots & y(J) \end{bmatrix} \begin{bmatrix} w_1(1) & \cdots & w_1(J) \\ \vdots & & \vdots \\ w_J(1) & \cdots & w_J(J) \end{bmatrix}^{-1}. \tag{8}$$

Note that only J samples are required for feedback if the weights $w_i(n)$ are chosen properly. An alternative method is that the authorized user sends some $x(n)$ directly back to the transmitters.

1.3.2. Transmitting weights design

Before presenting our designs, we first show that traditional transmit beamforming methods do not guarantee secrecy although they are optimal in terms of performance and power efficiency. A typical transmit beamforming method uses $\mathbf{w}(n) = \mathbf{h}/\|\mathbf{h}\|$, which has unit total transmission power since $E[\|\mathbf{s}(\mathbf{n})\|^2] = E[\mathrm{tr}(\mathbf{w}(n)b(n)b^*(n)\mathbf{w}^H(n))] = E[\|\mathbf{w}(n)\|^2] = 1$. Obviously, $\mathbf{w}(n)$ is not random if the channel $\mathbf{h}$ is constant or slowly time-varying. The received signal of the unauthorized user becomes $\mathbf{x}_u(n) = (\mathbf{H}_u\mathbf{h}/\|\mathbf{h}\|)b(n) + \mathbf{v}_u(n)$, from which many blind equalizers including the constant modulus algorithm (CMA) [15] can be applied for symbol detection. The same conclusion holds for other designs of $\mathbf{w}(n)$ that are not random. This explains why we should make $\mathbf{w}(n)$ random for randomized array transmissions.

More generally, $\mathbf{w}(n)$ can be obtained from the singular value decomposition (SVD) of $\mathbf{h}$, i.e., $\mathbf{h}^H = \mathbf{U}\mathbf{D}\mathbf{V}^H$ [16]. In this special case, $\mathbf{U} = 1$, $\mathbf{D} = \mathrm{diag}\{\|\mathbf{h}\|, 0, \cdots, 0\}$, and $\mathbf{V}$ is a $J \times J$ unitary matrix whose first column equals $\mathbf{h}/\|\mathbf{h}\|$. For transmit beamforming, $\mathbf{w}(n)$ can be calculated as $\mathbf{w}(n) = \mathbf{V}[1, z_2(n), \cdots, z_J(n)]^T \overset{\Delta}{=} \mathbf{V}[1, \mathbf{z}_1^T(n)]^T$, where $z_j(n)$, $j = 2, \cdots, J$, can be arbitrary. Such a classic

approach does not have any secrecy even if $\mathbf{w}(n)$ is randomized by choosing randomly $\mathbf{z}_1(n)$. For example, CMA may be used to estimate symbols from

$$\mathbf{x}_u(n) = \mathbf{H}_u \mathbf{V} \begin{bmatrix} 1 \\ \mathbf{z}_1(n) \end{bmatrix} b(n) + \mathbf{v}_u(n). \tag{9}$$

In summary, in order to guarantee secrecy, we may not achieve the optimal unit transmission power. This can be further demonstrated by the following observations. For $J = 2$, if we guarantee unit transmission power, then there is no degree of freedom in $\mathbf{w}(n)$ left for randomization. In addition, if we solve (6) by first choosing randomly $w_i(n)$, $3 \le i \le J$, and then looking for $w_1(n)$ and $w_2(n)$ for both (6) and unit power, it turns out that there may not have solutions.

Based on such observations, we design transmitting weights which trade transmission power for secrecy. We first select randomly an h_i from $\mathbf{h}$. We can select a threshold α and choose those h_i that satisfy $|h_i|^2 > \alpha$. Then we choose randomly $w_j(n)$, where $1 \le j \le J$ and $j \ne i$. Without loss of generality, we can draw them from an i.i.d. complex Gaussian random process. Denote $\mathbf{z}_i(n) = [w_1(n), \cdots, w_{i-1}(n), w_{i+1}(n), \cdots, w_J(n)]^T$ and $\mathbf{h}_i(n) = [h_1, \cdots, h_{i-1}, h_{i+1}, \cdots, h_J]^T$. The weights vector is calculated as

$$\mathbf{w}(n) = \mathbf{P}_i \begin{bmatrix} \dfrac{\|\mathbf{h}\| - \mathbf{h}_i^H \mathbf{z}_i(n)}{h_i^*} \\ \mathbf{z}_i(n) \end{bmatrix}. \tag{10}$$

The matrix $\mathbf{P}_i$ is a $J \times J$ commutation matrix whose function is to insert the first row of the following vector into the i th row. Since h_i is chosen randomly, $\mathbf{P}_i$ is also random. This approach is listed below as Algorithm 1.

Algorithm 1. Design weights vector $\mathbf{w}(n)$ *for each symbol*

1. Select randomly h_i, $1 \le i \le J$, such that $|h_i|^2 > \alpha$.
2. Generate i.i.d. random variables $w_j(n)$, $1 \le j \le J$, $j \ne i$.
3. Calculate $\mathbf{w}(n)$ by (10).

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

1.3.3. Transmission power

Although we do not explicitly apply any power constraints on $\mathbf{w}(n)$, the transmission power can be statistically controlled by adjusting the mean and variance of the random variables $w_j(n)$, $j \ne i$. Let us consider the case that the mean and variance are zero and σ^2, respectively. Then the total transmission power is

$$P_{t,h_i} = E\left[\mathbf{w}^H(n)\mathbf{w}(n) \middle| \mathbf{h}, \mathbf{P}_i\right] = (J-1)\sigma^2 + \frac{\|\mathbf{h}\|^2}{|h_i|^2} + \frac{\|\mathbf{h}_i\|^2 \sigma^2}{|h_i|^2} \tag{11}$$

for a given channel realization $\mathbf{h}$ and a given choice of h_i.

Equation (11) shows that small h_i increases the total transmission power, so the threshold α should be carefully selected. Since h_i is a complex Gaussian random variable with zero mean and unit variance, $|h_i|^2$ is exponentially distributed with unit mean. The probability for the selected channel coefficient h_i to have energy $|h_i|^2$ greater than α is

$$P\left[|h_i|^2 > \sigma\right] = \int_{\sigma}^{\infty} e^{-t} dt = e^{-\alpha}. \tag{12}$$

Proposition 1. With Rayleigh fading channels, if the coefficients are selected with energy threshold α (12), then the expected total transmission power is

$$P_t = (J-1)\sigma^2 + 1 + (J-1)(1+\sigma^2)\Gamma(0,\alpha). \tag{13}$$

Proof. See [31].

From (13), the total transmission power P_t is a function of the number of transmitting antennas J, the variance σ^2 of the random variables $w_j(n)$, and the threshold α for selecting h_i. Fig. 3 illustrates their relations. From Fig. 3(a), with $J = 4$, we see that P_t increases when σ^2 increases or α decreases.

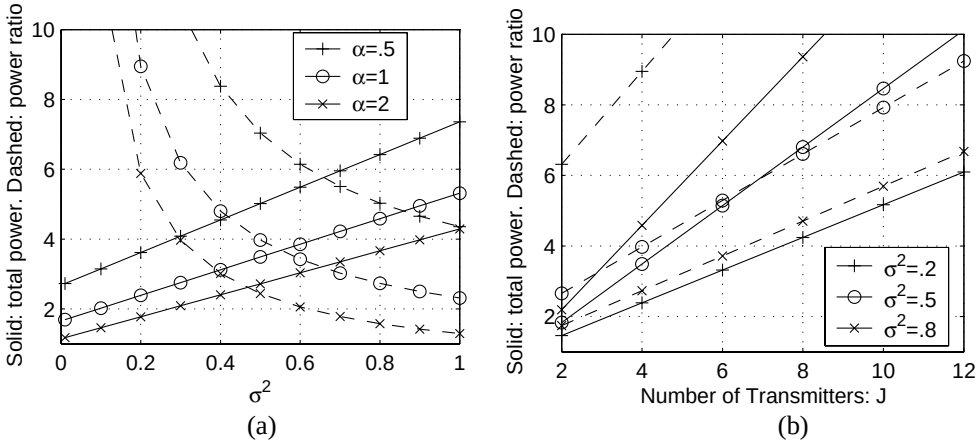


Fig. 3. Total transmission power P_t and power ratio $P_{t,i} / P_{t,j}$ of the i th transmitter to the j th transmitter ($j \neq i$) when h_i is selected in (10). $J = 4$ for (a). $\alpha = 1$ for (b). Solid lines: total power. Dashed lines: power ratio.

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 transmitters is exceptionally larger than the others. Otherwise the array transmission behaves as that with a single transmitter, and security can be compromised. Therefore, we have to constrain the ratio of the transmission power of the i th transmitter $P_{t,i} = (\|\mathbf{h}\|^2 + \|\mathbf{h}_i\|^2 \sigma^2)/|h_i|^2$ to that of the j th transmitter $P_{t,j} = \sigma^2$. The power ratio can be obtained from (13) as

$$\frac{P_{t,i}}{P_{t,j}} = \frac{1 + (J-1)(1+\sigma^2)\Gamma(0,\alpha)}{\sigma^2}. \tag{14}$$

Obviously, it is usually impossible to obtain unit ratio unless we change the probability of choosing h_i according to the value of $|h_i|^2$. From Fig. 3, the power ratio is a decreasing function of both σ^2 and α.

1.3.4. Transmission secrecy of Algorithm 1

We have removed explicit training so that the unauthorized user has no training available for channel estimation. If the channels are reciprocal, then the transmitters can estimate channel $\mathbf{h}$ from any uplink signal transmitted by the authorized user in TDD, without leaking channel information to the unauthorized user. Otherwise, the transmitters depend on feedback from the authorized user for channel estimation. In this latter case, the secrecy relies on the security of the feedback data. If the feedback data are not secure and can be obtained by the unauthorized user, whether they are $y(n) = \mathbf{h}^H \mathbf{w}(n)$ or raw received samples, the secrecy of the downlink transmission can be lost. For example, if the unauthorized

user has intercepted the feedback data $y(n)$, then together with its own estimations $y_u(n) = \mathbf{H}_u \mathbf{w}(n)$, it can derive a vector $\mathbf{h}^H \mathbf{H}_u^{-1}$. By this vector, it can intercept symbols $b(n)$ from $x_u(n)$.

Therefore, before using feedback, a secure initialization method has to be adopted to secure the first transmission for the subsequent feedback-based data transmission to become secure. We may exploit the reciprocal channel property to realize this objective. For example, the authorized user can first send a training sequence to the transmitters using the downlink frequency. After the transmitters estimate the channel, secure downlink transmission is setup by Algorithm 1. Feedback methods can then be used for channel estimation for normal data transmission, during which the feedback data can be secured via, e.g., Algorithm 1 employed at the authorized user or instantly exchanged keys. The advantage is that no secret keys are required before transmission, which is important considering that key distribution is usually a major weakness for traditional security techniques.

Without training, the unauthorized user may turn to blind equalizers. It is necessary for the transmitters to remove any constant modulus information from $s_j(n) = w_j(n)b(n)$ to prevent the application of a major category of blind equalizers: the constant modulus method [15], [17]. This is realized in Algorithm 1 by choosing $w_j(n)$ appropriately. If $w_j(n)$ is Gaussian, then $s_j(n)$ is satisfactory because $b(n)$ is independent from $w_j(n)$ and is uniformly distributed with a finite number of values. In particular, if $|b(n)|$ is constant, then $s_j(n)$ is Gaussian because the Gaussian probability density function (pdf) of $w_j(n)$ is phase symmetric. Although $\mathbf{s}(n)$ is not jointly Gaussian due to (16), it is determined completely by the first and second order moments whereas higher-order moments are zero.

In this scenario, the secrecy of Algorithm 1 comes from the fact that the received signal (4) of the unauthorized user is with a multiple-input multiple-output (MIMO) channel model. It is well known that blind MIMO channel estimation has an inherent matrix ambiguity if no source property can be exploited [17], [18]. In our case, since signals $s_j(n)$ are not drawn from a finite alphabet, there may not be any modulus information for the unauthorized user to remove such an ambiguity.

For example, the first-order moment of $\mathbf{x}_u(n)$ does not provide the unauthorized user with any useful information because it is identically zero even if $w_j(n)$ may not have zero mean. For the second-order moments, the unauthorized user may obtain $\mathbf{R}_u = \mathbf{H}_u E[\mathbf{w}(n)b(n)b^*(n)\mathbf{w}^H(n)]\mathbf{H}_u^H = \mathbf{H}_u \mathbf{R}_s \mathbf{H}_u^H$. There exist some $J \times J$ unitary matrices $\mathbf{Q}$ such that $\mathbf{R}_u = \mathbf{H}_u \mathbf{Q}^H \mathbf{R}_s \mathbf{Q} \mathbf{H}_u^H$ as long as $\mathbf{Q}^H \mathbf{R}_s \mathbf{Q} = \mathbf{R}_s$. Since the unauthorized user does not know $\mathbf{R}_s$, it has no information of $\mathbf{Q}$. Moreover, the unknown $\mathbf{R}_s$ makes the ambiguity matrix arbitrary, not only unitary.

The conclusion about the ambiguity matrix can be easily checked by the subspace method [19] with $N > J$. Therefore, if the unauthorized user can not discriminate $\mathbf{H}_u$ from $\mathbf{H}_u \mathbf{Q}^H$, it can not discriminate $\mathbf{w}(n)b(n)$ from $\mathbf{Q}\mathbf{w}(n)b(n)$. This makes the interception impossible as $\mathbf{Q}$ is unknown.

If the blind equalization is not applicable, the last way left for the unauthorized user is to try a brute-force search of all possible channels $\mathbf{H}_u$ (or, strictly speaking, $\mathbf{Q}$) and $\mathbf{h}$. Let us assume that the unauthorized user uses K-level quantization for each single value (a complex number has two such values). Then the brute-force search needs to consider at least $K^{(2J)^2}$ possible combinations of $\mathbf{H}_u$ and K^{2J} possible combinations of $\mathbf{h}$. This gives an overall complexity $K^{2J(2J+1)}$.

With $J = 4$ and QPSK transmission, in order to achieve bit-error-rate (BER) under 0.1, by simulations we find $K \geq 4$ even in the noiseless case. When $K = 4$, the complexity becomes $4^{2\times 4\times(2\times 4+1)} = 2^{144}$, which gives security well above the encryption with a 128-bit key [1]. If considering a more realistic BER of 0.01 at signal-to-noise-ratio (SNR) 25 dB per receiving antenna, then K should be at least 128, which gives a complexity over 2^{644}.

Since the complexity of the brute-force search increases rapidly with J^2, computational secrecy of Algorithm 1 can be guaranteed.

1.4. Random matrix method for intentional ambiguity

The transmission secrecy of Algorithm 1 depends on the inherent ambiguity of blind channel equalization. However, in practice, it may not be a trivial task to prevent every possible blind/non-blind equalization method, especially since networking protocol information or even the source correlations may be exploited by the unauthorized user for equalization [20], [21]. Source scrambling, networking protocols, as well as $\mathbf{w}(n)$ have to be carefully designed.

Instead of focusing on the issues relative to the overall network design, we develop another transmission algorithm with the objective of achieving secrecy even if the unauthorized user knows its own channel $\mathbf{H}_u$. This would effectively simplify the design of physical-layer secured wireless networks. We assume in this subsection that the unauthorized user knows $\mathbf{H}_u$ but not $\mathbf{h}$, and has extremely high SNR or even noiseless signal. Such assumptions make our approach distinct from most existing physical-layer security studies such as [3].

1.4.1. Transmission with intentional ambiguity

With the known $\mathbf{H}_u$, the signals of the unauthorized user (4) can be simplified to

$$\mathbf{x}_u(n) = \mathbf{w}(n)b(n), \tag{16}$$

where the noise is skipped under the assumption of high SNR. Since the unauthorized user may know the signal model of the authorized user (5)-(6) (but does not know $\mathbf{h}$, $\mathbf{w}(n)$ and $b(n)$), a brute-force search with much reduced complexity can be applied, during which it simply checks every possible $\mathbf{h}$ with (16) to see whether the rule of finite symbol alphabet is satisfied. This procedure may break the secrecy with a complexity K^{2J} only.

To resolve this weakness, one way is to make $\mathbf{h}$ time-varying, which can increase the complexity of the brute-force method in low SNR but is not effective in high SNR or noiseless cases. To guarantee secrecy under (16), we propose to introduce intentional ambiguity into $\mathbf{w}(n)$ in addition to creating time-varying channels.

Instead of using (10) to find $\mathbf{w}(n)$, we generate a $J \times (J-1)$ random matrix $\mathbf{F} = [\mathbf{f}_1, \cdots, \mathbf{f}_{J-1}]$, where each $\mathbf{f}_i$ is a $J \times 1$ vector. Let

$$\mathbf{a}(n) = \begin{bmatrix} \|\mathbf{f}_1\| c_1(n) \\ \vdots \\ \|\mathbf{f}_{J-1}\| c_{J-1}(n) \end{bmatrix}, \tag{17}$$

where $\{c_i(n)\}$, $1 \le i \le J-1$, are secret sequences known only to the transmitters. Without loss of generality, we assume that $c_i(n) = \pm 1$, $\forall i, n$, and $\{c_i(n)\}$ and $\{c_j(n)\}$ are independent from each other. We make each column of the matrix $\mathbf{F}$ to have the same distribution as $\mathbf{h}$. The matrix $\mathbf{F}$ is known to the transmitters only.

Then we calculate $\mathbf{w}(n)$ by solving

$$\begin{bmatrix} \mathbf{h}^H \\ \mathbf{F}^H \end{bmatrix} \mathbf{w}(n) = \begin{bmatrix} \|\mathbf{h}\| \\ \mathbf{a}(n) \end{bmatrix}. \tag{18}$$

For the authorized user, the received signal is still (5) and (6). The key idea is to make the unauthorized user unable to discriminate $\mathbf{h}$ from any column of $\mathbf{F}$, even with a brute-force search. This procedure is listed below as Algorithm 2 when the channel $\mathbf{h}$ is block fading.

Algorithm 2. Design $\mathbf{w}(n)$ *for intentional ambiguity*
1. Generate random matrix $\mathbf{F}$ (for a block of symbols), 2. Generate random vector $\mathbf{a}(n)$ (for each symbol), 3. Calculate $\mathbf{w}(n)$ by solving array equation (18).

The computational complexity of Algorithm 2 is $O(J^2)$. Note that $\mathbf{F}^{-1}$ is recalculated per symbol block, not per symbol. The power efficiency of Algorithm 2 can be made much higher than Algorithm 1 because the problem of inverting small h_i is gone. The lower bound of total transmission power can be determined from

$$E\left[\|\mathbf{w}(n)\|^2\right] \geq E\left[\|[\mathbf{h}\ \ \mathbf{F}]\|^2 \left\| \begin{bmatrix} \|\mathbf{h}\| \\ \mathbf{a}(n) \end{bmatrix} \right\|^2\right] = \frac{\mathbf{h}^H\mathbf{h} + \mathbf{a}^H(n)\mathbf{a}(n)}{\mathrm{tr}([\mathbf{h}\ \ \mathbf{F}]^H[\mathbf{h}\ \ \mathbf{F}])} = 1. \tag{19}$$

However, the unit lower bound usually can not be obtained.

1.4.2. Transmission secrecy of Algorithm 2

In the following, we use $P[x]$ to denote the probability of a random variable X for notational simplicity. It equals the pdf $f_X(x)$ if X is continuous, or the probability mass function p_X when X is discrete.

Proposition 2. Even if the unauthorized user knows its channel $\mathbf{H}_u$ and works in noiseless environment, it can not discriminate $\mathbf{h}$ from any column $\mathbf{f}_i$ of $\mathbf{F}$, i.e., $P\left[\mathbf{h} \middle| \{\mathbf{x}_u(n)\}\right] = P\left[\mathbf{f}_i \middle| \{\mathbf{x}_u(n)\}\right]$, $1 \leq i \leq J-1$, where $\{\mathbf{x}_u(n)\}$ denotes the sequence including all the available samples.

Proof. Considering the *maximum a posteriori* (MAP) detector for $\mathbf{h}$, the unauthorized user has

$$P\left[\mathbf{h} \middle| \{\mathbf{x}_u(n)\}\right] = P\left[\{\mathbf{x}_u(n)\} \middle| \mathbf{h}\right]\frac{P[\mathbf{h}]}{\mathbf{P}[\{\mathbf{x}_u(n)\}]} = P\left[\{\mathbf{w}(n)\} \middle| \mathbf{h}\right]P[\{b(n)\}]\frac{P[\mathbf{h}]}{\mathbf{P}[\{\mathbf{x}_u(n)\}]} \tag{20}$$

Because of (6), one element of $\mathbf{w}(n)$ is completely determined by others given $\mathbf{h}$. Without loss of generality, let $w_1(n)$ be determined by random variables $\mathbf{z}_1(n) = [w_2(n), \cdots, w_J(n)]^T$. Then

$$P\left[\mathbf{h} \middle| \{\mathbf{x}_u(n)\}\right] = P[\{\mathbf{z}_1(n)\}]P[\{b(n)\}]\frac{P[\mathbf{h}]}{\mathbf{P}[\{\mathbf{x}_u(n)\}]}.$$

Similarly, if the unauthorized user considers $\mathbf{f}_i$ instead of $\mathbf{h}$, it has

$$P\left[\mathbf{f}_i \middle| \{\mathbf{x}_u(n)\}\right] = P[\{\mathbf{z}_1(n)\}]P[\{b(n)\}]\frac{P[\mathbf{f}_i]}{\mathbf{P}[\{\mathbf{x}_u(n)\}]}.$$

Because $P[\mathbf{f}_i] = P[\mathbf{h}]$, the proposition is proved. □

Proposition 2 shows that the unauthorized user can not discriminate $\mathbf{h}$ from $\mathbf{f}_i$. In other words, it can not discriminate $b(n)$ from $c_i(n)b(n)$. This is the ambiguity created intentionally by Algorithm 2. However, if the number of vectors $\mathbf{h}$ and $\mathbf{f}_i$ that satisfy (18) is finite, then the unauthorized user can use brute-force search to determine which sequence among $\{b(n)\}$ and $\{c_i(n)b(n): 1 \leq i \leq J-1\}$ is more meaningful by recovering them to message sequences.

Therefore, we need to create suitably time-varying channels in order to make the brute-force search computationally prohibitive. Time-varying channels can be intentionally created by moving randomly transmitting antennas, or by choosing different antenna subsets from a large array. Considering the requirement of channel estimation, channel time-varying rate should be slower than symbol rate. Each channel realization is used to transmit a short block of symbols with a suitable $\mathbf{F}$. As long as the determination of $\{b(n)\}$ requires a sufficiently large number of blocks, computational secrecy can be achieved.

For example, if the symbols are sufficiently interleaved and transmitted in K blocks, the complexity of breaking secrecy is J^K. For $J = 4$ transmitters, $K = 64$ blocks gives a complexity 2^{128}. In addition, in practice, due to noise and the short block length, the unauthorized user may not have sufficient statistic measures for determining even $\mathbf{h}$ or $\mathbf{f}_i$. Hence computational secrecy can be guaranteed with a moderate number of symbol blocks.

1.4.3. Perfect secrecy

According to the perfect secrecy defined by Shannon [9], if the unauthorized user gets no information on $b(n)$ from the received signals $\{\mathbf{x}_u(n)\}$ then perfect secrecy is guaranteed. One of the ways to show perfect secrecy is that given the received signals $\{\mathbf{x}_u(n)\}$, the probability of detecting a symbol $b(n)$, i.e., $P[b(n)|\{\mathbf{x}_u(n)\}]$, is independent of $b(n)$.

Proposition 3. Assume that the unauthorized user knows its channel $\mathbf{H}_u$ but not $\mathbf{h}$, and has noiseless received signals $\{\mathbf{x}_u(n)\}$. Then $P[b(n)|\{\mathbf{x}_u(n)\}]$ can be made independent of $b(n)$ if $\mathbf{h}$ is i.i.d. for each symbol and the symbols have constant magnitude, i.e., $|b(n)| = 1$. If the channel $\mathbf{h}$ is constant or slowly time-varying, or if $|b(n)|$ is not constant, then $P[b(n)|\{\mathbf{x}_u(n)\}]$ may not be independent of $b(n)$ since the unauthorized user can exploit its knowledge of (6).

Proof. Since $\mathbf{w}(n)$ is randomly and independently generated in each symbol interval, if the channel $\mathbf{h}$ is i.i.d. for each symbol, then $\mathbf{w}(n)$ is independent from $\mathbf{x}_u(m)$ for any $m \neq n$. The same conclusion holds for $b(n)$. Therefore, $P[b(n)|\{\mathbf{x}_u(n)\}]$ is equivalent to $P[b(n)|\mathbf{x}_u(n)]$. We have

$$P[b(n)|\mathbf{x}_u(n)] = P[\mathbf{x}_u(n)|b(n)]\frac{P[b(n)]}{P[\mathbf{x}_u(n)]} = P[\mathbf{w}(n)b(n)|b(n)]\frac{P[b(n)]}{P[\mathbf{x}_u(n)]}. \quad (21)$$

The pdf of $\mathbf{w}(n)b(n)$ given $b(n)$ is $\frac{1}{|b(n)|} f_{\mathbf{w}}(\frac{\mathbf{w}(n)}{b(n)})$, where $f_{\mathbf{w}}(\cdot)$ denotes the joint pdf of $\mathbf{w}(n)$.

Because the channel coefficients in $\mathbf{h}$ are jointly Gaussian with zero mean, the pdf of $\mathbf{h}$ is phase symmetric (or phase invariant), i.e., the probability of $\mathbf{h}e^{j\theta}$ is the same as that of $\mathbf{h}$ for any θ [23]. Because $\mathbf{w}(n)$ is obtained from $\mathbf{h}$, $f_{\mathbf{w}}(\mathbf{w}(n))$ can also be phase symmetric. This can be seen from the fact that $[\mathbf{h}e^{j\theta}]^H[\mathbf{w}(n)e^{j\theta}] = \|\mathbf{h}e^{j\theta}\|$. This equation tells us that if there is a $\mathbf{w}(n)$ obtained from $\mathbf{h}$ with certain probability, then for any phase θ, $\mathbf{w}(n)e^{j\theta}$ can be obtained from $\mathbf{h}e^{j\theta}$ with the same probability. Note that different $\mathbf{h}$ and $\mathbf{h}e^{j\theta}$ do not share the same $\mathbf{w}(n)$.

Therefore, if $|b(n)| = 1$, then $\mathbf{w}(n)/b(n)$ and $\mathbf{w}(n)$ have identical probability, which means that $f_{\mathbf{w}}(\mathbf{w}(n)/b(n)) = f_{\mathbf{w}}(\mathbf{w}(n))$. Hence $P[b(n)|\mathbf{x}_u(n)] = P[\mathbf{w}(n)]P[b(n)]/P[\mathbf{x}_u(n)]$. Since $P[b(n)]$ is constant, $P[b(n)|\mathbf{x}_u(n)]$ is independent of $b(n)$.

However, if the channel $\mathbf{h}$ is not i.i.d. for each symbol, or if $|b(n)|$ are not constant, then $\frac{1}{|b(n)|} f_{\mathbf{w}}(\frac{\mathbf{w}(n)}{b(n)}) \neq f_{\mathbf{w}}(\mathbf{w}(n))$ in general. Some information about $b(n)$ may be available given $\{\mathbf{x}_u(n)\}$. □

From Proposition 3, a necessary condition for perfect secrecy is that all symbols should have identical magnitude, otherwise the different power information may be exploited. Such a conclusion is similar to that in [3], although the latter is obtained under that assumption that the unauthorized user has no information of the channel $\mathbf{H}_u$, nor can it estimate $\mathbf{H}_u$.

While it is easy to realize $|b(n)| = 1$, a more challenging task for realizing perfect secrecy in practice is to make the channel $\mathbf{h}$ random. The difficulty comes from the channel estimation requirement at either the transmitters or the authorized user. On the other hand, since it does not matter whether the

unauthorized user knows its channel $\mathbf{H}_u$ or not, training methods can be used for channel estimation with reduced complexity.

A possible way for implementing transmissions with perfect secrecy is to intentionally create channel variation by moving antennas randomly, or by selecting randomly subsets of a large antenna arrays. The latter case still requires time-varying channels, although the variation rate can be slow. With each new channel realization, a training sequence can be transmitted for channel estimation. After the transmitters know the channels from feedback, a symbol is transmitted with a randomized $\mathbf{w}(n)$. The initialization based on channel reciprocity is still required. On the other hand, channel reciprocity, if available during normal data transmission, can be exploited to remove feedback and thus enhance data rate.

1.5. Secure transmission in dispersive channels

As shown in Section III.3.1 and [31], there are three possible channel models for cooperative transmissions: *synchronous flat-fading channel model*, *synchronous dispersive channel model*, and *asynchronous dispersive channel model*. The secure transmission algorithms in Section I.3 and I.4 can be extended to the dispersive channel models. To save space, details of such extension are not included, but can be found in [31].

1.6. Simulations

In this section, we show the performance of the proposed Algorithm 1 of Section I.3 and Algorithm 2 of Section I.4. We use bit-error-rate (BER) to compare the receiving performance of the authorized user and the unauthorized user. We also examine the transmission power of these two algorithms. For comparison purpose, we evaluate the performance of the optimal transmit beamforming [16] discussed in Section I.3.2, and give the theoretical BER curve of the Rayleigh fading channel without diversity [12]. For the unauthorized user, blind equalizers [18] are simulated.

We first study the performance of the Algorithm 1. Channels are assumed block Rayleigh fading, i.e., they are constant during transmission of one packet, but randomly changing between packets. Each packet contains 200 QPSK symbols. We use 5000 runs to obtain each BER value. For Algorithm 1, we use $\alpha = 0.5$, $\sigma^2 = 0.5$. If there are less than two selectable channel coefficients under (12), then we simply select h_i between the two strongest ones in order to make $\mathbf{P}_i$ in (10) random. Both flat-fading channels and dispersive channels are simulated. For the dispersive channels, we use channel length $L = 2$.

The simulation results are shown in Fig. 4(a). Transmissions with Algorithm 1 have similar performance as the optimal transmit beamforming. The unauthorized user can not intercept symbols using the blind equalization with 8 receiving antennas and sufficiently good channels.

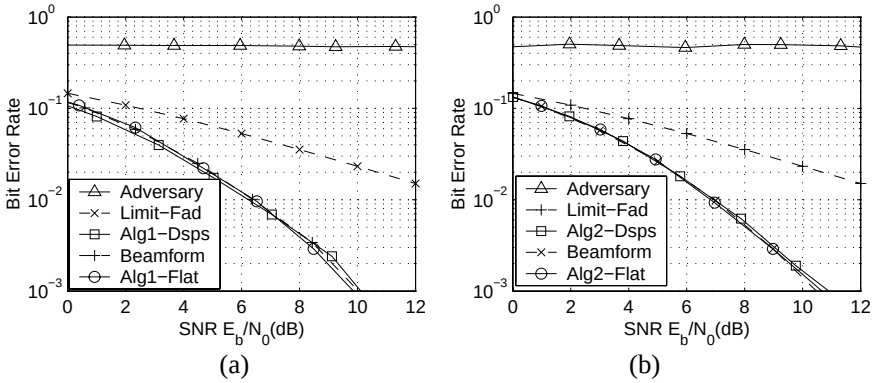
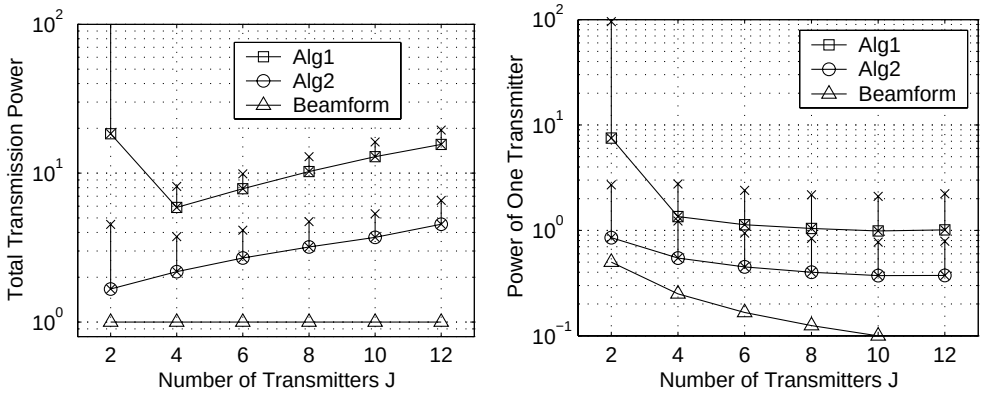


Fig. 4. Receiving performance comparison. (a) For Algorithm 1. (b) For Algorithm 2. $J = 4$. ∘ :Algorithms 1 or 2 with flat-fading channels. □:Algorithms 1 or 2 with dispersive channels. + :transmit beamforming. × :theoretical BER curve with Rayleigh fading channel. Δ :blind detector of unauthorized user.



(a) (b)

Fig. 5. Transmission power and standard deviation. Standard deviation is shown by × above the power value. (a) Total transmission power. (b) Power of a single transmitter. □:Algorithm 1. ○ :Algorithm 2. Δ :transmit beamforming.

Then we study the performance of Algorithm 2 with the similar simulation parameters. For Algorithm 2, we let the transmitters to find the best $\mathbf{w}(n)$ from J different $\mathbf{F}$ matrices in order to reduce transmission power and to avoid ill-conditioned matrices. The results are shown in Fig. 4(b), from which the conclusion similar to Algorithm 1 can be drawn.

One of the major differences between Algorithm 1 and Algorithm 2 is their transmission power, which is compared in Fig. 5(a) and (b).

1.7. Realizing Physical-layer Secured WLAN

The main purpose of this research topic is to realize the physical-layer security techniques in 802.11 WLAN without a complete overhaul of existing physical-layer hardware. First, as can be seen, physical antenna arrays not only increase system cost but also require new hardware design (because multiple parallel signal processors are required in the same board. The concept of cooperative transmissions may be more advantageous for cost reduction and for exploiting existing redundant (but separate) hardware. For example, multiple access points, or multiple WLAN cards, each of which may have only a single antenna, can be used to transmit/receive the same data packet in a collaborative manner. Therefore, our objective is to use multiple access points (AP) to jointly transmit a packet to the authorized user (client), while at the same time to make the reception at other unauthorized users impossible.

Besides showing the idea of secure wireless networks, such a demonstrative testbed can also be used to verify the practicability of cooperative communications. Cooperative communications are a new area with many challenges involved in the application and implementation such as synchronization and collaboration. A testbed, especially if constructed using WLAN COTS devices, will be an effective way to show the feasibility of cooperative communications and the potential of cooperative communications as a way to enhance the performance and function of either existing or future systems.

In the following, we propose two ways for constructing such a testbed: channel or time based approaches.

1.7.1. Channel-based approach

The channel-based approach depends on the theories described in Sections I.3 and I.4, i.e., Algorithm 1 and 2, where the difference between the propagation channels of the authorized user and the unauthorized user is exploited. The random intersymbol interference (ISI) created intentionally by the randomization procedure may stop most of the WLAN receivers from working, in particular those currently on market. Since current 802.11 WLAN receivers do not have equalizers (because of the flat fading channel models used in indoor WLAN environment), even a trivially introduced ISI may achieve certain degree of security.

The major problems are relative to channel estimation and the synchronization among the cooperating APs. For the channel estimation, we may depend on the feedback from the authorized receiver. This can be realized if the authorized receiver knows the channel. Another way is to ask the authorized receiver to feedback some received samples directly, from which the APs can estimate the channels. In order to achieve this objective, one way is to reprogram the firmware of the authorized user to ask him to transmit the received samples. For the APs, a channel estimation algorithm needs to be implemented. This can be realized by programming instead of new hardware design.

For synchronization, similarly firmware needs to be reprogrammed so that we can ask the physical-layer to maintain synchronization clock. The synchronization can not be done in the MAC or above layer only since the clock accuracy of these layers are in the units of microsecond, not accurate enough for transmission.

Another problem that we have skipped is whether the carrier frequency f_c is identical among all APs. However, this may not a big issue in 802.11 WLAN since the carrier frequency drifting is at most 25 ppm, which is sufficiently small.

1.7.2. Timing-based approach

Compared with the channel-based approach, the timing-based approach may be more feasible. By timing-based approach, we adjust the transmission delays instead of the transmission weights of the APs, as shown in Fig. 2. This is somewhat similar to wireless location using time-of-arrival (TOA). The most promising aspect is that the energy-of-arrival and thus the RSSI value in 802.11 WLAN may be directly used for deriving the timing information.

As illustrated in Fig. 2, the APs can purposely adjust the delay of their transmission time instant (i.e., the time instant that they begin transmission). Though the APs need to know all delays, such delays can in fact be obtained from their received signals from the desired user, especially through the RSSI information. With such information, the APs can adjust their delay. The effective of this approach depends on the symbol interval T. In 802.11b, T is $1/11$ micro-seconds, which gives sufficient adjustment range for the delays.

The likelihood that such a delay difference among the desired user and the undesired user is large depends on the distance between the desired user and the undesired user. This is similar to the accuracy of the wireless location problem. As long as distance between the two users are larger than $1/(2T)$, then such a likelihood is high.

The potential of the approach is that we do not have to change anything in the authorized user. We need only to reprogram the APs. However, the fireware of APs is still subject to change because the transmission delay needs to be synchronized.

1.7.3. A simple testbed for demonstrating the concepts

The major challenge for the above two methods is the synchronization in transmission timing, which requires sophisticated reprogramming work in the firmware. We need to study the firmware programming of some real implementations. The programming work may be time-consuming, especially since such programming needs to be compatible with the entire networking.

However, we have a much quicker way to setup a demonstrative testbed. Instead of working on the real 802.11 WLAN network, we work on separate 802.11 transmitters and receivers without considering the entire network. For example, we can use the standard transceiver blocks (see Comblock.com) to build the cooperative transmitters, and implement the secure transmission algorithms in general purpose PCs. This way, we can sample and analyze the signals to obtain certain performance benchmark.

Part 2
Application of STBC-encoded Cooperative Transmissions in Wireless Sensor Networks

2.1. Introduction

In wireless sensor networks, energy efficiency is a dominating design criterion. Transmission energy efficiency is especially important because wireless transceivers usually consume a major portion of battery energy. Transmission energy efficiency can be enhanced by diversity techniques with antenna arrays, among which space-time block codes (STBC) are attractive because of their linear complexity [24]. For mobile users without antenna arrays, STBC with cooperative transmission schemes have been proposed [25]-[27].

However, the requirement of extreme energy efficiency in wireless sensor networks makes the application of cooperative transmission questionable. First, when sensors schedule joint transmissions, the overhead of cooperation incurs extra energy consumption. Second, it is not an easy task to synchronize cooperating transmitters in terms of carrier frequency, carrier phase, symbol timing (symbol rate) and timing phase (sampling time instant). Without perfect synchronization, STBC-encoded transmission becomes more complex, sometimes even not applicable [27], [28]. Finally, although cooperative diversity enhances *transmission* energy efficiency, the involvement of more than one transmitting sensor increases *electronic* energy consumption [29].

So far, cooperative transmission has been studied mostly under the assumption of perfect synchronization. The overhead, synchronization, complexity and energy efficiency are to be justified. To address this task, without loss of generality we consider a typical networking/communication protocol for wireless sensor networks, i.e., low-energy adaptive clustering hierarchy (LEACH) [30]. We propose ways to incorporate cooperative transmission in LEACH and study the associated overhead, synchronization and energy efficiency.

2.2. LEACH with cooperative transmission

We consider a wireless sensor network where sensors need to transmit their data to a remote data collector. LEACH is an interesting networking/communication protocol for sensors to form hierarchical clusters and to schedule TDMA channel access. The operation of LEACH is broken up into rounds, and each round consists of four phases: advertisement, cluster setup, transmission scheduling, and data transmission.

Advertisement. In this phase, each sensor determines by itself whether it becomes a cluster head during this round. Each self-selected cluster head then broadcasts an advertisement message. We do not need to make changes in this phase for cooperative transmission, though we rename the cluster head as *primary head*.

Cluster setup. In this phase, each sensor transmits a cluster-joining packet to its desirable primary head. For *J*-sensor cooperative transmission, besides the primary head, we need to choose *J-1* secondary heads in each cluster. In our scheme, they will be selected by the primary head in the next phase. Meanwhile, when a sensor transmits cluster-joining packet, it should piggyback information about its capability of being a secondary head, e.g., its current energy status. The overhead of this procedure can be as small as just transmitting one extra byte along with the relatively long cluster-joining packet.

Schedule creation. This phase is for each primary head to create TDMA channel access schedule, and to inform each sensor the assigned slot. For cooperative transmission, each primary head first selects

the secondary heads based on both the reported energy status and the received signal power. The power can be used as an estimation of the sensor distance. Then the primary head informs the selected secondary heads about their roles in cooperative transmission, which can be implemented by piggybacking one extra byte in the original scheduling packet. The overhead includes the selection of secondary heads in the primary head, and one byte more transmission to each of the $J-1$ secondary heads. Such overhead is still negligibly small.

Data transmission. In this phase, each cluster head receives data packets from the other sensors in the cluster, fuses these packets, and transmit the fusion result to the data collector. In cooperative transmission mode, it is still the primary head that receives and fuses data packets. However, after that, the primary head first broadcasts the fused data to the secondary heads, and all J heads then transmit the data to the data collector cooperatively in the following slot. This procedure is illustrated in Fig. 6(a). The overhead in this phase, which is the major one for the proposed scheme, includes the broadcasting procedure and the added electronic energy consumption. The impact of such overhead on energy efficiency will be analyzed in Section II.4.

2.3. Synchronization among cooperating sensors

2.3.1. Synchronization and channel models

Before cooperative transmission, the secondary heads can synchronize their carrier frequency and symbol timing to their received signals when the primary head broadcasts the fused data. The remaining issue is then relative to carrier phase and timing phase synchronization.

We have to omit the transmission delays from the primary head to the secondary heads since they are difficult to estimate and compensate. Therefore, if the maximum distance between the primary head and the secondary heads is $d_{\max}$, then the beginning time of cooperative transmission at the primary head is up to $d_{\max}/c$ earlier than the secondary heads, where c is the speed of light. Among the signals transmitted by the cooperating sensors, the maximum (worst case) relative delay is $2d_{\max}/c$ when they arrive at the data collector. These delays cause synchronization error in both carrier phase and timing phase.

Let the passband signal from a head sensor i be $s_i(t) = \mathrm{Re}[\sqrt{\rho}\sum_{\ell=-\infty}^{\infty} b_i(\ell)\, p(t-\ell T)e^{j2\pi f_c t}]$ where Re[.] stands for real part, ρ is a transmission power adjustor, $b_i(\ell)$ is the complex symbol at symbol interval $[\ell T, (\ell+1)T)$ is the baseband pulse shaping filter, and f_c is the carrier frequency. The received signal at the data collector is then

$$x_p(x) = \mathrm{Re}[\sqrt{\rho}\sum_{i=1}^{J}\sum_{\ell=-\infty}^{\infty} a_i b_i(\ell)\, p(t-\ell T-\tau_i)e^{j(2\pi f_c t-\theta_i)} + v_p(t)], \tag{22}$$

where a_i and θ_i are gain and phase of the propagation channel, and τ_i is the delay. We use $v_p(t)$ to denote passband noise. Flat fading propagation is assumed, and with same ρ, the transmission power is evenly distributed among cooperating head sensors.

Because signals from head sensors have different θ_i and τ_i, it is impossible to achieve synchronization in carrier phase and timing phase. Therefore, without loss of generality, we demodulate (22) with local carrier $e^{-j2\pi f_c t}$ and then perform sampling at time instants $t_n = nT+\tau$ (for arbitrary τ). The baseband samples $x(n) = x_b(nT+\tau)$ are

$$x(n) = \sqrt{\rho}\sum_{i=1}^{J} a_i e^{-j\theta_i}[\,p(\tau-\tau_i)b_i(n) + \sum_{\ell\neq n} p((n-\ell)T+\tau-\tau_i)b_i(\ell)] + v(n)\,, \tag{23}$$

where $v(n)$ is baseband noise. Obviously, residual inter-symbol interference (ISI) is inevitable. In flat fading environment, we would prefer that single-tap channel model still be used in cooperative

transmission. This can be achieved by making $d_{\max}$ small enough to effectively reduce the upper bound of τ_i and thus the ISI to a negligible level.

By choosing $d_{\max}$ small enough, the baseband received signal (23) can be approximated as

$$x(n) = \sqrt{\rho}\sum_{i=1}^{J}\alpha_i b_i(n) + v(n)\,, \tag{24}$$

where $\alpha_i = a_i e^{-j\theta_i}$. Hence the flat fading channel assumption as in [24] can still be applied.

2.3.2. Long-term effect of frequency and timing offsets

In Section II.3.1, we assumed that synchronization on carrier frequency and symbol timing is perfect. However, such synchronization may not be accurate due to, e.g., noise, Doppler shifting, and difference on processing circuitry, in which case there are frequency and timing mismatches among cooperating nodes.

Carrier frequency mismatch makes channels time-varying so that channels have to be adaptively tracked. Timing mismatch is more devastating because it destroys the space-timing signal structure, which makes STBC not directly applicable [28]. If the ratio of the symbol rate of sensor 1 to sensor 2 is r then when sensor 1 transmits K symbols, sensor 2 can transmit K/r symbols.

One way to mitigate this problem is to limit the packet (or slot) length. Consider first the case $r \le 1$. In order to keep correct timing, both sensors need to transmit K symbols in one slot, which gives $K \le K/r \le K+1$ (the difference on transmission delay is omitted for simplicity) and we have $K < r/(r-1)$. Similarly, if $r \ge 1$, we have $K < r/(r-1)$. In summary, we need to choose packet length K such that $K < r/|1-r|$. Therefore, r needs to be close to 1 for reasonable packet lengths. For practical oscillators with up to 100 ppm drifting, we have $r \in [1-10^{-4}, 1+10^{-4}]$.

2.4. Energy efficiency

Consider the baseband signal model (24) with quasi-static Rayleigh flat fading channels, i.e., α_i are complex Gaussian distributed with zero-mean and unit variance, and are constant in one STBC block but may vary randomly between blocks. The noise is AWGN with zero mean and variance σ_v^2. After the synchronization problem is resolved, traditional STBC [24] can be directly applied. With standard STBC decoding, the data collector estimates symbols from

$$\hat{b}(n) = (\rho\sum_{i=1}^{J}|\alpha_i|^2)^{\frac{1}{2}} b(n) + w(n)\,, \tag{25}$$

where $w(n)$ is AWGN with zero mean and variance σ_v^2.

2.4.1. Improvement on transmission power efficiency

To compare the transmission power efficiency of cooperative transmission against single transmission, we consider SNR of (25) for each channel realization, i.e., $SNR = \rho\sum_{i=1}^{J}|\alpha_i|^2\sigma_b^2/\sigma_v^2$, where σ_b^2 is the variance of the symbols $b(n)$. In order to make the SNR above some threshold value *A* with a high probability *B*, from (24) we need to choose carefully the overall cooperative transmission power

$J\rho\sigma_b^2$ such that $P[\rho\sum_{i=1}^{J}|\alpha_i|^2\sigma_b^2/\sigma_v^2 > A] = B$. For single transmission, we assume $J=\rho=1$ and the channel be α_1. The ratio of single transmission power to cooperative transmission power is $1/(J\rho)$.

Proposition 4. Cooperative transmission can use less overall transmission power than single transmission for some SNR A and probability B, i.e., there exist A, B and $\rho < 1/J$ such that $P[\rho\sum_{i=1}^{J}|\alpha_i|^2\sigma_b^2/\sigma_v^2 > A] = P[|\alpha_1|^2\sigma_b^2/\sigma_v^2 > A] = B$.

Proof. See [34].

Though such a conclusion may not be surprising, the advantage of this approach lies in the convenient evaluation of power saving. Because of the lack of general BER expressions, many other approaches such as [29] have to either consider special case or resort to Monte-Carlo simulations. In our case, we can numerically calculate ρ, which then gives power saving $1/(J\rho)$. For example, the power saving $1/(J\rho)$ can be calculated as 5.7, 11.3, 16.8, 20.4 for J =2, 3, 4, 5, respectively. Interestingly, these values are close to the results in [28] obtained from BER Monte-Carlo simulations.

2.4.2. Overall sensor energy efficiency

In order to study energy efficiency with the consideration of overhead and electronic energy, we use the energy consumption model as in [30]. Transmission energy consumption is modeled as $E_a^t(k,d) = kd^2E_a$, a function of both the number of symbols transmitted (k) and the transmission distance (d). Electronic energy consumption is modeled as linear functions of k, i.e., $E_e^t(k) = kE_e^t$ for transmitters and $E_e^r(k) = kE_e^r$ for receivers.

For single transmission, the total energy consumption of both the transmitter and the receiver is

$$E_e^t(k) + E_a^t(k,d) + E_e^r(k) = kE_e^t + kE_e^r + kd^2E_a. \quad (26)$$

For the cooperative transmission, first the primary head broadcasts fusion results to the secondary heads, during which the total energy consumption is

$$E_a^t(k,d_{\max}) + E_e^t(k) + (J-1)E_e^r(k) = kE_e^r + (J-1)kE_e^r + kd_{\max}^2E_a. \quad (27)$$

Then, when all J heads perform cooperative transmission, the energy consumption is

$$JE_e^t(k_J) + E_a^t(k_J,d) + E_e^r(k_J) = Jk_JE_e^t + k_JE_e^r + k_Jd^2E_{aJ}. \quad (28)$$

In this case, $k_J \in [k,2k]$ depends on J and the STBC encoding scheme [24]. E_{aJ} is the total transmission energy of cooperative transmission.

Cooperative transmission enhances energy efficiency if the sum of (27) and (28) is less than (26). It should be readily seen that this depends on the transmission distance d. Therefore, cooperative transmission is advantageous if

$$d^2\left(\frac{k}{k_J}\frac{E_a}{E_{aJ}} - 1\right) > J\frac{E_e^t}{E_{aJ}} + \left[(J-2)\frac{k}{k_J} + 1\right]\frac{E_e^r}{E_{aJ}} + d_{\max}^2\frac{k}{k_J}\frac{E_a}{E_{aJ}}. \quad (29)$$

For example, with typical STBC code rate k/k_J, energy model parameters $E_e^t = E_e^r = 50nJ/bit$ and $E_a = 100pJ/bit/m^2$ [30], and $d_{\max} = 10$, using the energy (power) ratio E_a/E_{aJ} calculated in Section II.4.1, the minimum distances can be calculated as $d = 44, 61, 73, 92$ meters for $J = 2, 3, 4, 5$, respectively. Since those transmission distances are typical in wireless sensor network applications, cooperative transmission is useful for enhancing energy efficiency.

To simulate the proposed LEACH with cooperative transmission, we use the same network settings as [30]. The overall network energy efficiency (in terms of network lifetime) is evaluated. As shown in Fig. 6(b), cooperative transmission can extend the network lifetime over traditional LEACH. When $J = 2$, 30% longer lifetime is realized.

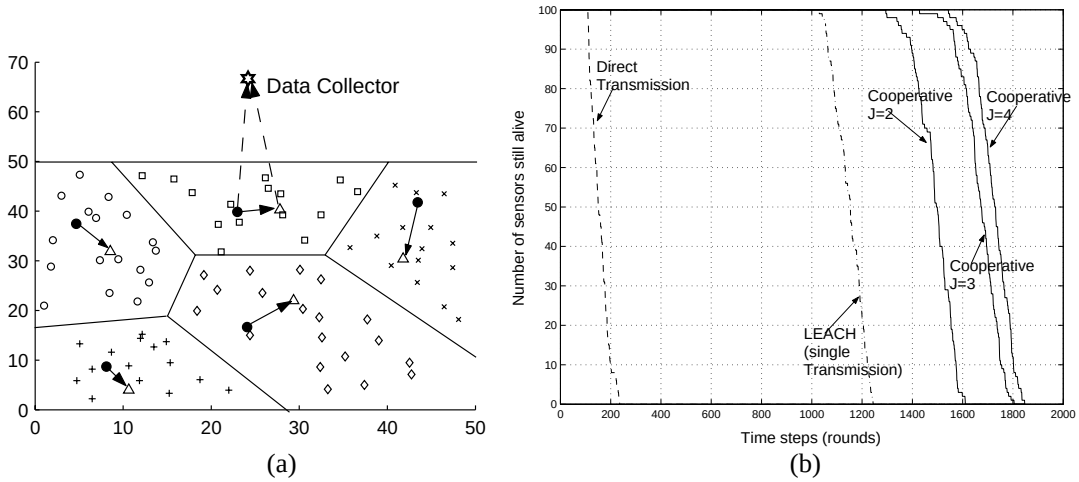


Fig.6. (a) Illustration of LEACH with cooperative transmission for wireless sensor networks. •: primary heads. Δ: secondary heads. (b) Compare energy efficiency with/without cooperative transmission in LEACH.

Part 3 Conclusions

This report summarizes the research results in the security of wireless transmissions. Both computational and perfect secrecy can be realized under more practical assumptions. Cooperative communications are proposed as tools to realize wireless information assurance as well as to enhance the performance of wireless sensor networks.

References

[1] C. E. Landwehr and D. M. Goldschlag, "Security issues in networks with internet access," *Proc. IEEE*, vol. 85, pp. 2034-2051, Dec. 1997.

[2] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," *IEEE Trans. Signal Processing*, vol. 52, no. 9, pp. 2637-2649, Sept. 2004.

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

[4] H. Koorapaty, A. A. Hassan and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, pp. 52-55, Feb. 2000.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.

[6] M. J. Mihaljevic and J. D. Golic, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence," in *Advances in Cryptology*, vol. 658, pp. 124-137, Berlin, Germany: Springer-Verlag, 1993.

[7] J. Tugnait, L. Tong and Z. Ding, "Single user channel estimation and equalization," *IEEE Signal Processing Mag.*, vol. 17, no. 3, pp. 17-28, May 2000.

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

[9] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656-715, 1949.

[10] G. Xu and H. Liu, "An effective transmission beamforming scheme for frequency-division-duplex digital wireless communication system," *ICASSP'95*, vol. 3, pp. 1729-1732, May 1995.

[11] P. Viswanath, D. Tse and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Info. Theory*, vol. 48, no. 6, June 2002.

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

[13] G. F. Edelmann, T. Akal, William S. Hodgkiss, S. Kim, W. A. Kuperman and H. C. Song, "An initial demonstration of underwater acoustic communication using time reversal," *IEEE J. Oceanic Engineering*, vol. 27, no. 3, pp. 602-609.

[14] X. Li, "Collaborative communications in wireless networks without perfect synchronization," presentation at AFOSR program review, June 2004. Available online at: *http://www.rl.af.mil/tech/programs/CITE/docs/xli.ppt*.

[15] 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.

[16] D. H. Johnson and D. E. Dudgeon, *Array Signal Processing, Concepts and Techniques*, Prentice Hall, Upper Saddle River, NJ, 1993.

[17] Y. Inouye, "Criteria for blind deconvolution of multi-channel linear time-invariant systems," *IEEE Trans. Signal Processing*, vol. 46, no. 12, pp. 3432-3436, Dec. 1998.

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

[19] E. Moulines, P. Duhamel, J. Cardoso, and S. Mayrargue, "Subspace methods for the blind identification of multichannel FIR filters," *IEEE Trans. Signal Processing*, vol. 43, no. 2, pp. 516-525, Feb. 1995.

[20] J. Q. Bao and L. Tong, "Protocol-aided channel equalization in wireless ATM," *IEEE J. Sel. Areas Comm.*, vol. 18, no. 3, pp. 418-435, Mar. 2000.
[21] X. Li, "Blind channel estimation and equalization in wireless sensor networks based on correlations among sensors," to appear in *IEEE Trans. Signal Processing*, 2004. Available online at: *http://ucesp.ws.binghamton.edu/~xli*.
[22] R. J. Muirhead, *Aspects of Multivariate Statistical Theory*, John Wiley & Sons, 1982.
[23] P. Z. Peebles, Jr., *Probability, Random Variables and Random Signal Principles*, 4th Ed., McGraw Hill, New York, NY, 2001.
[24] V. Tarokh, H. Jafarkhani and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform.Theory*, vol. 45, no. 7, pp. 1456-1467, July 1999.
[25] A. Sendonaris, E. Erkip and B. Aazhang, "User cooperation diversity, Part I, II," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927-1948, Nov. 2003.
[26] J. N. Laneman and G. W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Trans. Inform. Theory*, vol. 49. no. 10, pp. 2415-2425, Oct. 2003
[27] X. Li, "Energy efficient wireless sensor networks with transmission diversity," *Electro. Lett.*, vol. 39, no. 24, pp. 1753-1755, Nov. 2003.
[28] X. Li, "Space-time coded multi-transmission among distributed transmitters without perfect synchronization," to appear in *IEEE Signal Processing Lett*. Available on-line at: *http://ucesp.ws.binghamton.edu/~xli*.
[29] S. Cui, A. J. Goldsmith and A. Bahai, "Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks," to appear in *IEEE J. Sel. Areas Commun.*
[30] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," *Proc. Hawaii Int. Conf. System Sci.*, Maui, Hawaii, Jan. 2000.
[31] X. Li, M. Chen, E. P. Ratazzi, "Randomized array transmissions for physical-layer secured wireless communications," submitted to *IEEE Trans. Signal Processing*, Sept. 2004. Available online at: *http://bingweb.binghamton.edu/~xli/secom.pdf*.
[32] X. Li, M. Chen, E. P. Ratazzi, "Array-transmission based physical-layer security techniques for wireless networks," submitted to *ICASSP'2005*.
[33] X. Li, M. Chen, W. Liu, "Cooperative transmissions in wireless sensor networks with imperfect synchronization," to appear in the 38th Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, Nov. 2004.
[34] X. Li, M. Chen and W. Liu, "Application of STBC-encoded cooperative transmissions in wireless sensor networks," to appear in *IEEE Signal Processing Lett.*, 2004. Available online at: *http://ucesp.ws.binghamton.edu/~xli*.