Using Antenna Array Redundancy and Channel Diversity for Secure Wireless Transmissions

Xiaohua Li and Juite Hwu
Department of Electrical and Computer Engineering
State University of New York at Binghamton, Binghamton, NY 13902
Email: {xli,jhwu1}@binghamton.edu

E. Paul Ratazzi
Air Force Research Laboratory, AFRL/IFGB, Rome, NY 13441
Email: paul.ratazzi@afrl.af.mil

***Abstract*— The use of signal processing techniques to protect wireless transmissions is proposed 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. Extensive simulations and some preliminary experiments are conducted to demonstrate its effectiveness. The proposed method is useful for securing wireless transmissions, or for supporting upper-layer key management protocols.**

***Index Terms*— antenna array, transmit beamforming, diversity, channel, wireless information assurance**

I. INTRODUCTION

Along with the rapid development of wideband wireless communication networks, wireless security has become a critical concern [1]. 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 listen/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/untrustful 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-interception (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 [2], ii) scrambling code approaches like spread-spectrum [3], and iii) propagation channel approaches like [4]–[6]. 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 [7].

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 [8]. Eavesdroppers may use non-blind or blind deconvolution algorithms [9], [10] to estimate channels and signals, which makes many channel-based approaches such as [6] 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 [11]–[15], we have shown that physical-layer security can be realized based on channel diversity by using antenna array transmissions. This idea

This paper is based on "Array Redundancy and Diversity for Wireless Transmissions with Low Probability of Interception," by X. Li, J. Hwu, and E. P. Ratazzi, which appeared in the Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2006), Toulouse, France, May 2006. © 2007 IEEE.

This work was supported in part by US AFRL under Grants FA8750-05-1-0233 and FA8750-06-2-0167.

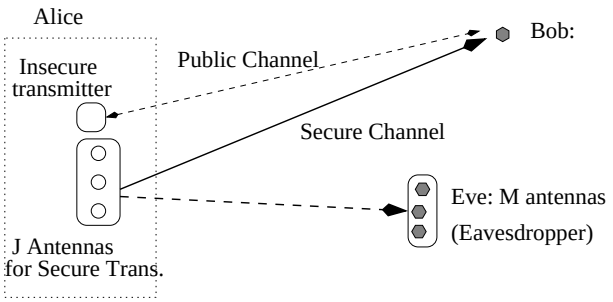

Figure 1. Secure wireless transmission model. Alice transmits to Bob using antenna array, in face of passive eavesdropper Eve. Eve may have receiving antenna array for better interception.

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 [10] for security, rather than information theory [4], [6]. The advantage is that LPI can be guaranteed much easier in more practical transmissions.

Based on [15], in this paper we propose a special deliberate randomization method for designing the transmit antenna weights, with more detailed explanation, security analysis and the proof of LPI. A transmission power analysis is also conducted to guide weights design. Extensive simulations and the development of a testbed are shown to demonstrate the proposed transmission scheme.

One of the major differences between our approach and existing physical-layer approaches is that we do not assume that the eavesdroppers have noisier received signals than the authorized receiver. Instead, we depend on two special properties of wireless transmissions for security: channel diversity that makes signals received by the eavesdroppers and the authorized receiver different, and array redundancy that provides degrees of freedom for randomizing the transmitted signals deliberately.

This paper is organized as follows. In Section II, a framework of secure array transmission is introduced. In Section III, we propose a deliberate signal randomization scheme and analyze the LPI. An analysis of transmission power for proper parameter selection is performed in Section IV. Simulations and experiments are given in Section V and conclusions are presented in Section VI.

II. Secure array transmission model

We consider a wireless network where Alice transmits to Bob in face of a passive eavesdropper Eve, as shown in Fig. 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 [16].

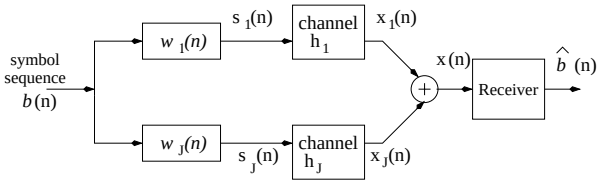

Figure 2. Transmit beamforming-like transmission block diagram. The transmitter randomizes the transmitting antenna weights $w_i(n)$ based on the channel state information, and $w_i(n)$ varies in each symbol interval n.

We consider only the secure channel from Alice to Bob in this paper. A beamforming-like array transmission procedure shown in Fig. 2 [2], [17] 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 $w_i(n)$. The transmitted signal from the antenna i is $s_i(n) = w_i(n)b(n)$. Therefore, through the J antennas, Alice transmits signal vectors

$$\begin{aligned}\mathbf{s}(n) &\triangleq \begin{bmatrix} s_1(n) \\ \vdots \\ s_J(n) \end{bmatrix} = \begin{bmatrix} w_1(n) \\ \vdots \\ w_J(n) \end{bmatrix} b(n) \\ &\triangleq \mathbf{w}(n)b(n), \end{aligned} \tag{1}$$

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 [14]. The signal received by Bob is

$$x(n) = \sum_{i=1}^{J} h_i^* s_i(n) + v(n) \triangleq \mathbf{h}^H \mathbf{s}(n) + v(n), \tag{2}$$

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

$$\mathbf{h} \triangleq \begin{bmatrix} h_1 \\ \vdots \\ h_J \end{bmatrix}. \tag{3}$$

In this paper, $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ denote conjugation, transposition and Hermitian, respectively. Since we need channel estimation, we assume that $\mathbf{h}$ is block fading [6], i.e., it is constant or slowly time-varying when transmitting a block of symbols but may change randomly between blocks. Under this model, the transmission power is determined by the transmitting weights $\mathbf{w}(n)$, whereas the received signal-to-noise-ratio (SNR) is determined by both $\mathbf{w}(n)$ and σ_v^2.

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

$$\begin{bmatrix} x_1^e(n) \\ \vdots \\ x_M^e(n) \end{bmatrix} = \begin{bmatrix} h_{11}^e & \cdots & h_{1J}^e \\ \vdots & & \vdots \\ h_{M1}^e & \cdots & h_{MJ}^e \end{bmatrix} \begin{bmatrix} s_1(n) \\ \vdots \\ s_J(n) \end{bmatrix} + \begin{bmatrix} v_1^e(n) \\ \vdots \\ v_M^e(n) \end{bmatrix} \quad (4)$$

The notations are similar to (2) except that $(\cdot)^e$ is used to denote the eavesdropper. The equation (4) can then be denoted as

$$\mathbf{x}_e(n) = \mathbf{H}_e \mathbf{s}(n) + \mathbf{v}_e(n), \quad (5)$$

where $\mathbf{x}_e(n)$ and $\mathbf{H}_e$ are with dimensions $M \times 1$ and $M \times J$, respectively. 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 [18]. This will be further demonstrated by simulations and experiments in Section V.

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 $b(n)$.

In addition, we focus only on the security of the transmission from Alice to Bob, under the assumption that Alice and Bob share no secret keys beforehand and know nothing about the eavesdropper Eve. Once this direction is secured, the reverse direction can be easily secured by using similar techniques and/or by exchanging encryption keys frequently.

III. 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], [19], [20]. Without training, the only way left for Eve is blind deconvolution [10], [21]–[24]. 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 unresolvable ambiguity.

A. Transmission and receiving procedure from Alice to Bob

In order for Bob to estimate symbols $b(n)$, the channel $\mathbf{h}$ from Alice to Bob has to be resolved. Traditionally, channel deconvolution can be conducted by either Alice or Bob, in terms of pre-equalization or equalization, respectively. 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 [17], [18], [25], 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.

An alternative way is for Bob to feedback some received samples $x(n)$ to Alice, so that Alice can estimate the channel $\mathbf{h}$ based on her knowledge on the transmitted signal. In this case, even if Eve can intercept the feedback samples $x(n)$, she can not estimate channels if both training-based deconvolution and blind deconvolution are prevented. To save space, we do not discuss it in details because it is in the same situation as the normal transmission discussed in the sequel.

Our basic idea is to make $\mathbf{h}^H \mathbf{w}(n)$ a deterministic constant, while $\mathbf{H}_e \mathbf{w}(n)$ 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

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

where $\|\mathbf{h}\| = \sqrt{\sum_{i=1}^{J} |h_i|^2}$ is the norm of $\mathbf{h}$. Although (6) looks similar to transmit beamforming [2], [17], the major difference is that $\mathbf{w}(n)$ changes randomly in each symbol interval n. 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, which explains why array transmission is necessary.

From the received signal

$$x(n) = \|\mathbf{h}\| b(n) + v(n), \quad (7)$$

Bob can detect symbols as

$$\hat{b}(n) = \arg\min_{b(n)} \left| x(n) - \|\mathbf{h}\| b(n) \right|^2, \quad (8)$$

where $\|\mathbf{h}\|$ can be easily estimated from the received signal power $\frac{1}{N}\sum_n |x(n)|^2$. Especially, if $b(n)$ has constant magnitude $|b(n)|$, e.g., PSK, then we can simply use $|x(n)|$ in place of $\|h\|$, which means we can simply use the phase of $x(n)$ as symbol estimation.

Alice's design of $\mathbf{w}(n)$ under the constraint (6) 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

$$\mathbf{w}(n) = \mathbf{P}_i(n) \left[\begin{array}{c} a_i - \mathbf{f}_i^H \mathbf{z}_i(n) \\ \mathbf{z}_i(n) \end{array} \right] \tag{9}$$

where

$$\begin{aligned} a_i &= \frac{1}{h_i^*}\|\mathbf{h}\|, \\ \mathbf{f}_i &= \frac{1}{h_i}[h_1, \cdots, h_{i-1}, h_{i+1}, \cdots, h_J]^T, \\ \mathbf{z}_i(n) &= [w_1(n), \cdots, w_{i-1}(n), w_{i+1}(n), \cdots, w_J(n)]^T. \end{aligned} \tag{10}$$

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 $w_j(n)$, $1 \le j \le J$, $j \ne i$.
3. Calculate $\mathbf{w}(n)$ by (9)-(10).

The selection of the threshold α in Step 1 will be discussed in Section IV, whereas Step 2 will be detailed in Section III.B.

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.

B. A deliberate randomization scheme

From (9), 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 [10] [19]. 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., $\mathbf{r}_i(n) \sim \mathcal{N}_{J-1}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ [26]. The parameters $\boldsymbol{\mu}$ and $\boldsymbol{\Sigma}$ are arbitrary and unknown to both Eve and Bob, and can even be time-varying.

From (9) and (1), the transmitted signal vector is thus

$$\mathbf{s}(n) = \mathbf{P}_i(n) \left[\begin{array}{c} a_i b(n) - \mathbf{f}_i^H \mathbf{r}_i(n) \\ \mathbf{r}_i(n) \end{array} \right]. \tag{11}$$

C. LPI of the randomized transmission

1) Traditional beamforming guarantees no LPI: To justify our new deliberate randomization scheme, we first show that traditional transmit beamforming methods do not guarantee LPI although they are optimal in terms of power efficiency. A typical transmit beamforming method uses $\mathbf{w}(n) = \mathbf{h}/\|\mathbf{h}\|$, which has unit total transmission power since $E[\|\mathbf{s}(n)\|^2] = E[\text{tr}(\mathbf{w}(n)b(n)b^*(n)\mathbf{w}^H(n))] = E[\|\mathbf{w}(n)\|^2] = 1$ [2]. Obviously, $\mathbf{w}(n)$ is not random if the channel $\mathbf{h}$ is constant or just slowly time-varying. Eve's received signal becomes $\mathbf{x}_e(n) = (\mathbf{H}_e\mathbf{h}/\|\mathbf{h}\|)b(n) + \mathbf{v}_e(n)$, from which many blind equalizers such as the constant modulus algorithm (CMA) [21] 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 make $\mathbf{w}(n)$ random in our secure array transmissions.

More generally, $\mathbf{w}(n)$ can be obtained from the singular value decomposition (SVD) of $\mathbf{h}$, i.e., $\mathbf{h}^H = \tilde{\mathbf{U}}\tilde{\mathbf{D}}\tilde{\mathbf{V}}^H$ [2]. In this special case, $\tilde{\mathbf{U}} = 1$, $\tilde{\mathbf{D}} = \text{diag}\{\|\mathbf{h}\|, 0, \cdots, 0\}$, and $\tilde{\mathbf{V}}$ 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 $\mathbf{w}(n) = \tilde{\mathbf{V}}[1, c_2(n), \cdots, c_J(n)]^T \triangleq \tilde{\mathbf{V}}[1, \ \mathbf{c}_1^T(n)]^T$, where $c_j(n)$, $j = 2, \cdots, J$, can be arbitrary. Such a classic approach does not have any LPI capability even if $\mathbf{c}_1(n)$ is random. For example, the blind equalization method CMA can be used to estimate symbols from the received signal

$$\mathbf{x}_e(n) = \mathbf{H}_e\tilde{\mathbf{V}} \left[\begin{array}{c} 1 \\ \mathbf{c}_1(n) \end{array} \right] b(n) + \mathbf{v}_e(n). \tag{12}$$

2) Indeterminacy of Eve's blind deconvolution: As discussed in Section III.A, we have removed explicit training so that Eve has no training available for channel estimation. In this subsection, we show that Eve's blind deconvolution is also prevented by the deliberate signal randomization.

After the transmitting weights $w_j(n)$ are randomized, a major issue for security comes from the requirement that $\mathbf{w}(n)$ must satisfy (9), which makes the proof of LPI non-trivial.

From (11), Alice's transmitted signal can be written as $\mathbf{s}(n) = \mathbf{G}(n)\mathbf{r}_i(n) + \mathbf{g}(n)b(n)$ where

$$\begin{aligned} \mathbf{G}(n) &= \mathbf{P}_i(n) \left[\begin{array}{c} -\mathbf{f}_i^H \\ \mathbf{I}_{J-1} \end{array} \right], \\ \mathbf{g}(n) &= \mathbf{P}_i(n) \left[\begin{array}{c} a_i \\ \mathbf{0}_{J-1} \end{array} \right]. \end{aligned} \tag{13}$$

We have used $\mathbf{0}_{J-1}$ to denote a $J-1$ dimensional zero vector. With the notations in (13), Eve's received signal (5) can be written as

$$\mathbf{x}_e(n) = \left[\begin{array}{cc} \mathbf{H}_e\mathbf{G}(n) & \mathbf{I}_M \end{array} \right] \left[\begin{array}{c} \mathbf{r}_i(n) \\ \mathbf{v}_e(n) \end{array} \right] + \mathbf{H}_e\mathbf{g}(n)b(n). \tag{14}$$

Obviously, in each symbol interval n, Eve's signal is an M-variate Gaussian distributed vector [due to the random $\mathbf{r}_i(n)$], i.e.,

$$\begin{aligned} \mathbf{x}_e(n) \quad \sim \quad & \mathcal{N}_M\left(\mathbf{H}_e\mathbf{G}(n)\boldsymbol{\mu} + \mathbf{H}_e\mathbf{g}(n)b(n), \right. \\ & \left. \mathbf{H}_e\mathbf{G}(n)\boldsymbol{\Sigma}\mathbf{G}^H(n)\mathbf{H}_e^H + \sigma_v^2\mathbf{I}_M\right) \end{aligned} \tag{15}$$

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

$$\mathbf{Q} = \mathbf{P}_i(n) \left[\begin{array}{cc} u & \mathbf{0} \\ \mathbf{0} & \mathbf{V} \end{array} \right] \mathbf{P}_i^{-1}(n), \tag{16}$$

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

Proof. Define

$$\begin{aligned} \tilde{\mathbf{H}}_e &= \mathbf{H}_e\mathbf{Q}, \\ \tilde{\mathbf{G}}(n) &= u^{-1}\mathbf{G}(n)\mathbf{V}, \\ \tilde{\mathbf{g}}(n) &= u^{-1}\mathbf{g}(n) \\ \tilde{\boldsymbol{\mu}} &= \mathbf{V}^{-1}\boldsymbol{\mu}, \\ \tilde{\boldsymbol{\Sigma}} &= \mathbf{V}^{-1}\boldsymbol{\Sigma}(\mathbf{V}^{-1})^H. \end{aligned}$$

Then we can verify that $\tilde{\mathbf{H}}_e\tilde{\mathbf{G}}(n) = \mathbf{H}_e\mathbf{G}(n)\mathbf{V}$, $\tilde{\mathbf{H}}_e\tilde{\mathbf{g}}(n) = \mathbf{H}_e\mathbf{g}(n)$, and $\tilde{\mathbf{H}}_e\tilde{\mathbf{G}}(n)\tilde{\boldsymbol{\mu}}\tilde{\mathbf{G}}(n)^H\tilde{\mathbf{H}}_e^H = \mathbf{H}_e\mathbf{G}(n)\boldsymbol{\Sigma}\mathbf{G}^H(n)\mathbf{H}_e^H$. The distribution (15) does not change if $\mathbf{H}_e$, $\mathbf{G}(n)$, $\mathbf{g}(n)$, $\boldsymbol{\mu}$ and $\boldsymbol{\Sigma}$ are replaced by $\tilde{\mathbf{H}}_e$, $\tilde{\mathbf{G}}(n)$, $\tilde{\mathbf{g}}(n)$, $\tilde{\boldsymbol{\mu}}$ and $\tilde{\boldsymbol{\Sigma}}$, respectively. Therefore, there is a matrix $\mathbf{Q}$ ambiguity for estimating $\mathbf{H}_e$ blindly. □

The same conclusion holds if considering the sequence $\{\mathbf{x}_e(n)\}$ with respect to an unknown sequence $\{b(n)\}$ because $\mathbf{x}_e(n)$ are independent for different n. The known statistics of $\{b(n)\}$ does not help.

Let us assume that Eve can estimate $\mathbf{H}_e$ up to the ambiguity matrix $\mathbf{Q}$ in (16), then by substituting $\mathbf{H}_e$ with $\mathbf{H}_e\mathbf{Q}$ and removing $\mathbf{H}_e$, Eve's signal can be changed to

$$\begin{aligned} \tilde{\mathbf{x}}_e(n) \quad = \quad & \mathbf{P}_i(n) \left[\begin{array}{c} u\mathbf{f}_i^H \\ \mathbf{V} \end{array} \right] \mathbf{r}_i(n) \\ & + \mathbf{P}_i(n) \left[\begin{array}{c} ua_i \\ \mathbf{0}_{J-1} \end{array} \right] b(n) + \tilde{\mathbf{v}}_e(n). \end{aligned} \tag{17}$$

In order to detect $b(n)$, Eve has to first resolve $\mathbf{P}_i(n)$, i.e., determine which h_i for $i \in [1, J]$ is chosen in each symbol interval. If the decision is wrong, then Eve in fact detects $b(n)$ from an entry in $\mathbf{V}\mathbf{r}_i(n)$, which gives a BER of 0.5. On the other hand, if the decision is correct, then the detection of $b(n)$ is susceptible to the interference $\mathbf{f}_i^H\mathbf{r}_i(n)$. The signal-to-interference ratio (SIR) can be made large enough for a high BER by choosing properly $\boldsymbol{\Sigma}$.

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 [14].

IV. Transmission power analysis

From Section III.C.1, it can be seen that the conventional transmit beamforming achieves the optimal transmission power efficiency (with unit transmission power), but has no LPI capability. There is a tradeoff of transmission power for security. For example, for $J = 2$, if we guarantee the minimum unit transmission power, then there is no degree of freedom in $\mathbf{w}(n)$ left for randomization. Our design of transmitting weights has taken such a trade-off. Moreover, the procedure outlined in Algorithm 1 focuses primarily on computational simplicity instead of power efficiency.

On the other hand, a detailed analysis of transmission power is quite 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, from (11), conditioned on each selected channel coefficient h_i, the total transmission power is

$$\begin{aligned} & \mathrm{tr}\{E[\mathbf{s}(n)\mathbf{s}^H(n)|\mathbf{h}, \mathbf{P}_i(n)]\} = \\ & \quad \mathrm{tr}\{\boldsymbol{\mu}\boldsymbol{\mu}^H + \boldsymbol{\Sigma}\} + |a_i|^2 + \mathbf{f}_i^H(\boldsymbol{\mu}\boldsymbol{\mu}^H + \boldsymbol{\Sigma})\mathbf{f}_i, \end{aligned} \tag{18}$$

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 $\mathbf{h}$ and a given choice of h_i becomes

$$\begin{aligned} P_{t,h_i} &= E[\mathbf{s}^H(n)\mathbf{s}(n)|\mathbf{h}, \mathbf{P}_i(n)] \\ &= (J-1)\sigma^2 + |a_i|^2 + \|\mathbf{f}_i\|^2\sigma^2. \end{aligned} \tag{19}$$

Equations (19) and (10) show 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, $|h_i|^2$ 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

$$P[|h_i|^2 > \alpha] = \int_\alpha^\infty e^{-t}dt = e^{-\alpha}. \tag{20}$$

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

$$P_t = (J-1)\sigma^2 + 1 + (J-1)(1+\sigma^2)\Gamma(0,\alpha). \quad (21)$$

Proof. For random channels, the expected total transmission power is the ensemble average of the power (19)

$$P_t = E[P_{t,h_i}] = (J-1)\sigma^2 + 1 + E\left[\|\mathbf{f}_i\|^2\right](1+\sigma^2). \quad (22)$$

Since the channel coefficients are independent from each other, we have

$$P_t = (J-1)\sigma^2 + 1 + (J-1)(1+\sigma^2)E[\frac{1}{|h_i|^2}]. \quad (23)$$

Because $|h_i|^2$ has exponential distribution, we have

$$E[\frac{1}{|h_i|^2}] = \int_\alpha^\infty \frac{1}{|h_i|^2} e^{-|h_i|^2} d|h_i|^2 = \Gamma(0,\alpha). \quad (24)$$

Hence (21) is obtained. □

From (21), 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. Fig. 3 illustrates their relationships under $J = 4$.

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 ith transmit antenna $P_{t,i} = |a_i|^2 + \|\mathbf{f}_i\|^2\sigma^2$ to that of the jth transmit antenna $P_{t,j} = \sigma^2$. The power ratio can be obtained from (21) as

$$\frac{P_{t,i}}{P_{t,j}} = \frac{1 + (J-1)(1+\sigma^2)\Gamma(0,\alpha)}{\sigma^2}. \quad (25)$$

Obviously, it is usually impossible to obtain unit ratio unless we change the probability of choosing h_i according to the value of $|h_i|^2$ in a way that smaller $|h_i|^2$ has smaller probability of being selected. But the probability difference among all selectable channel coefficients should not be too large, because otherwise the randomness of $\mathbf{P}_i(n)$ is reduced. From Fig. 3, 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 in Section V, 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 (20), 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.

One may ask whether it is possible to make the power ratio $P_{t,i}/P_{t,j}$ unit while minimizing the total transmission power P_t. This may be accomplished by choosing elements of $\mathbf{r}(n)$ with nonzero mean μ and variance σ^2.

Proposition 3. Given a channel realization $\mathbf{h}$ and a choice of h_i, the problem of minimizing total transmission power with unit power ratio is equivalent to optimizing μ and σ^2 from

$$\begin{aligned} \min \quad & P_t = J(|\mu|^2 + \sigma^2) \\ \text{s.t.,} \quad & \left(\frac{2|h_i|^2}{\|\mathbf{h}\|^2} - 1\right)|\mu|^2 + 2\frac{1}{\|\mathbf{h}\|}\mathrm{Re}\left[\mu\sum_{j\neq i} h_j^*\right] \\ & + \left(\frac{2|h_i|^2}{\|\mathbf{h}\|^2} - 1\right)\sigma^2 = 1. \end{aligned} \quad (26)$$

where $\mathrm{Re}[\cdot]$ stands for real part.

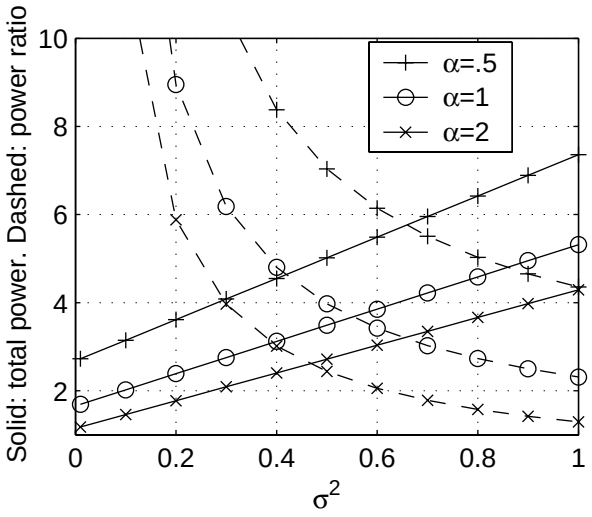

Figure 3. Total transmission power P_t and power ratio $P_{t,i}/P_{t,j}$ of the ith transmit antenna to the jth transmit antenna ($j \neq i$) when h_i is selected in (9). $J = 4$. Solid lines: total power. Dashed lines: power ratio.

Proof. From (9), $w_i(n)$ has mean $\frac{\|\mathbf{h}\| - \mu\sum_{j\neq i} h_j^*}{h_i^*}$ and variance $\frac{\|\mathbf{h}_i\|^2}{|h_i|^2}\sigma^2$. Since the power of the jth transmitter ($j \neq i$) is $|\mu|^2 + \sigma^2$ and that of the ith transmitter is $\frac{\left|\|\mathbf{h}\| - \mu\sum_{j\neq i} h_j^*\right|^2}{|h_i|^2} + \frac{\|\mathbf{h}_i\|^2}{|h_i|^2}\sigma^2$, the equation (26) is readily available for unit power ratio. □

We can solve the complex equation (26) for all μ and σ^2, and then find the minimum total transmission power. Unfortunately, (26) may not have solutions for all channel realizations, i.e., the total power P_t may become negative when (26) has to be satisfied. This means that unit power ratio can not be guaranteed for all channels and all choices of h_i when Algorithm 1 is used.

V. 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), or by directly using Bob's method, i.e., (8).

In the first simulation experiment, we used randomly generated channels. For comparison purpose, we evaluated the performance of the optimal transmit beamforming [2], and gave the theoretical BER curve of the Rayleigh fading channel without diversity [18]. Channels were

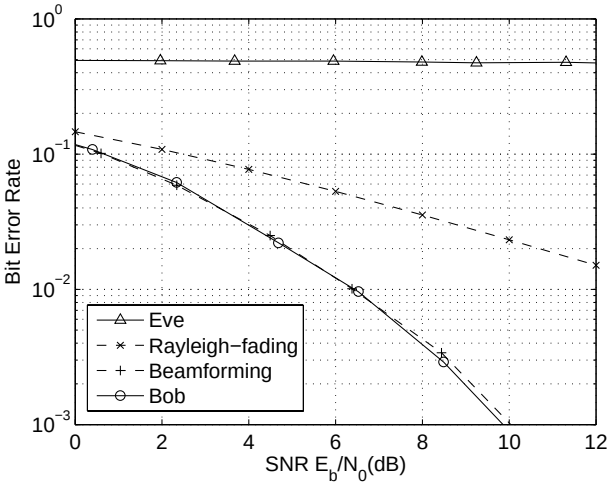

Figure 4. Receiving performance comparison. $J = 4$. ○:Algorithms 1. +:transmit beamforming. ×:theoretical BER curve with Rayleigh fading channel. △:Eve with blind equalizer.

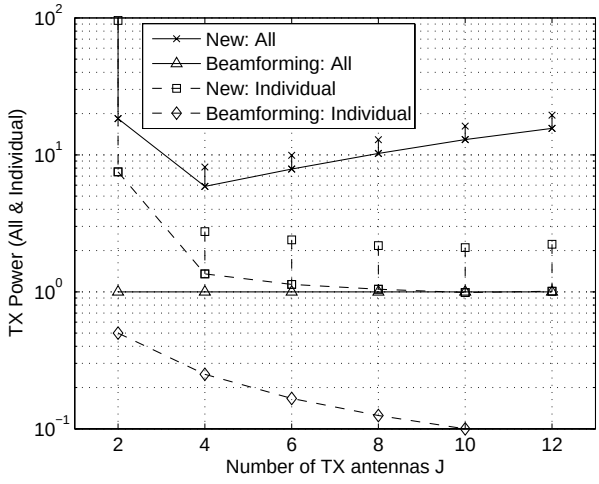

Figure 5. Total transmission power and the transmission power of each individual antenna, as well as their standard deviations. Standard deviation is shown by × or □ above the power value. ×:Total transmission power of Algorithm 1. △:total transmission power of transmit beamforming. □: individual antenna transmission power of Algorithm 1. ⋄: individual antenna transmission power of beamforming.

assumed block Rayleigh fading, i.e., they were constant during transmission of one packet, but randomly changing between packets. Each packet contained 200 QPSK symbols. We used 5000 runs to obtain each BER value. We used $\alpha = 0.5$, $\sigma^2 = 0.5$ for proper trade-off between transmission power and security. If there were less than two selectable channel coefficients under (20), then we simply selected h_i between the two strongest ones in order to make $\mathbf{P}_i(n)$ random.

The simulation results of the first experiment are shown in Fig. 4 and Fig. 5. Transmissions with the proposed Algorithm 1 have similar performance as the optimal transmit beamforming. They both exploit the diversity of $J = 4$ transmitters, which makes their BER curves much better than that of the theoretical Rayleigh fading without diversity. Eve can not intercept symbols using blind equalization with 8 receiving antennas and sufficiently good channels.

On the other hand, from Fig. 5, Algorithm 1 requires both larger total transmitting power and larger single-antenna transmission power than the conventional beamforming. In addition, the standard deviation of power consumption among 5000 runs is also shown. For Algorithm 1, when J is small, especially when $J = 2$, both the power and the standard deviation become large. This is because the limited number of channel coefficients causes very small h_i being chosen.

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 Fig. 6. 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 $\lambda = 0.3$ meters, where λ is the wavelength of 1GHz 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 $\lambda = 0.3$ meter grid. Details of the EM simulation and source data can be obtained at [27].

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, i.e., $\mathbf{x}_e(n) = \mathbf{h}\mathbf{s}(n) + (\mathbf{H}_e - \mathbf{h})\mathbf{s}(n) + \mathbf{v}_e(n)$, then LPI depends on the difference between $\mathbf{h}$ and $\mathbf{H}_e$, Specifically, the channel difference will contribute an interference to Eve's detection, which degrades the signal-to-interference ratio (SIR) to be approximately [c.f., (19)]

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

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 Fig. 7, 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.

As the third experiment, 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 Fig. 9 as the dashed curves. It can be seen that for almost all cases, Eve's error rate is extremely large.

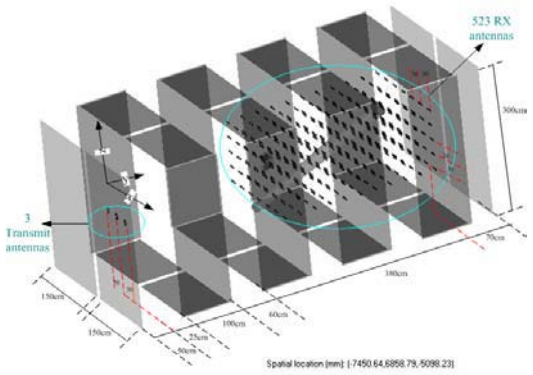

Figure 6. Settings of a room for electromagnetic wave propagation simulation. Refer to [27] for a detailed description.

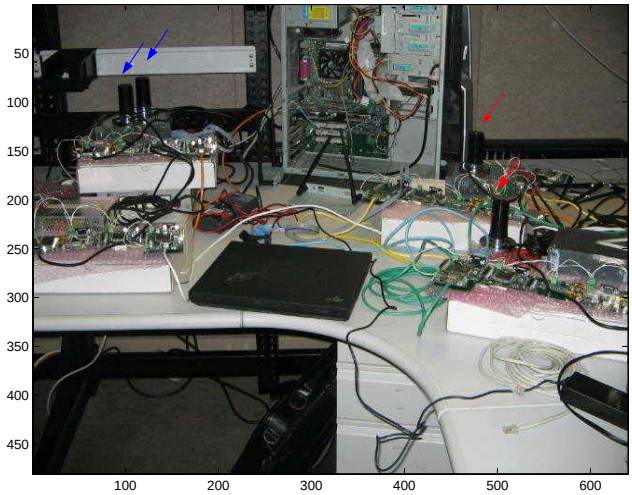

Figure 8. Experiment setup with 2 transmitting antennas (arrows) and 2 receive antennas (arrows). Notice the short distance between the two receive antennas.

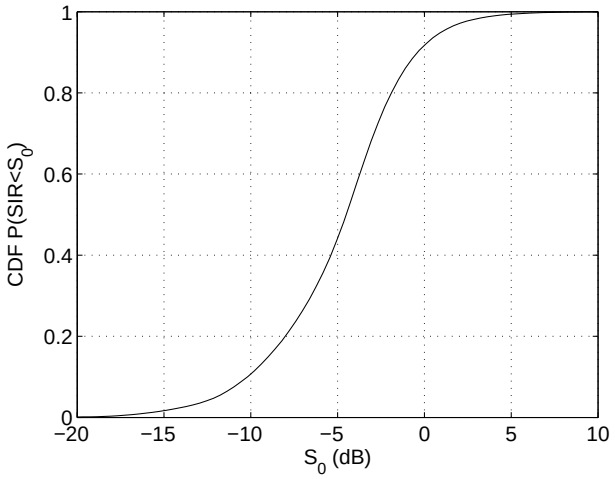

Figure 7. Cumulative distribution function of the SIR of Eve's signals due to the difference between Bob's and Eve's channels. Channels are derived by EM simulations.

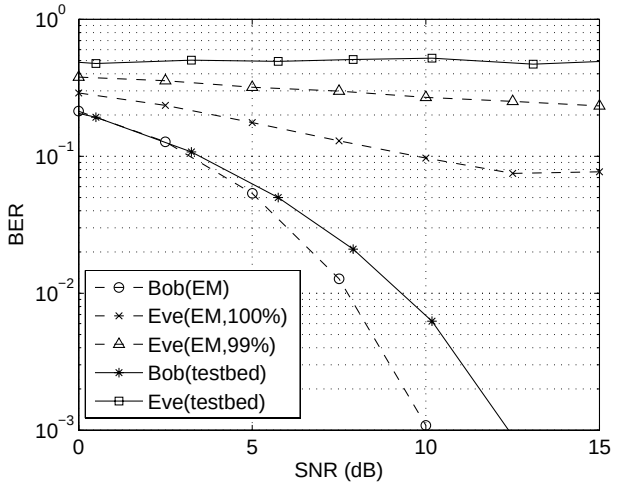

Figure 9. BER of Bob and Eve. Solid lines: using channels measured from testbed. Dashed lines: using channels obtained from EM simulation.

We are also building a testbed using the wireless transmission modules of ComBlock.com [27]. We implemented two QPSK transmitters and two QPSK receivers. One snap shot of the experiment is shown in Fig. 8. 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 Fig. 9). Note that the two receiving antennas (one for Bob, one for Eve) were purposely placed very close to each other.

VI. Conclusion

In this paper, we propose to use deliberately randomized array transmissions to guarantee wireless transmissions with LPI. The array redundancy is exploited to create indeterminacy of the eavesdropper's blind deconvolution, from which LPI is proved. The method is demonstrated by both simulations and preliminary testbed experiments. The proposed scheme trades transmission power for transmission security in terms of LPI.

Although another security objective LPD (low-probability-of-detection) is not directly addressed, the randomization procedure may in fact reduce the received power at any unwanted places when the array is large enough. A more detailed study on LPD is left for future.

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] D. H. Johnson and D. E. Dudgeon, *Array signal processing, concepts and techniques*, Prentice Hall, Upper Saddle River, NJ, 1993.

[3] 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.

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

[5] H. Koorapaty, A. A. Hassan and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, pp. 52-55, Feb. 2000.
[6] A. O. Hero, III, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235-3249, Dec. 2003.
[7] E. Ghashghai, "Communications networks to support integrated intelligence, surveillance, reconnaissance, and strike operations," *Rand Project Air Force Report*, 2005.
[8] 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.
[9] 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.
[10] S. Haykin, *Blind Deconvolution*, Prentice Hall, Englewood Cliffs, NJ, 1994.
[11] X. Li, M. Chen and P. Ratazzi, "A randomized space-time transmission scheme for secret-key agreement," *CISS'2005*, Johns Hopkins University, Mar. 2005.
[12] 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.
[13] 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.
[14] 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.
[15] X. Li, J. Hwu and E. P. Ratazzi, "Array redundancy and diversity for wireless transmissions with low probability of interception," *ICASSP'2006*, Toulouse, France, May 2006.
[16] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733-742, Mar. 1993.
[17] 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.
[18] J. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.
[19] 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.
[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] 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.
[22] Y. Inouye, "Criteria for blind deconvolution of multichannel linear time-invariant systems," *IEEE Trans. Signal Processing*, vol. 46, no. 12, pp. 3432-3436, Dec. 1998.
[23] 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.
[24] 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.
[25] 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.
[26] R. J. Muirhead, *Aspects of Multivariate Statistical Theory*, John Wiley & Sons, 1982.
[27] Simulation data and experiment details are available at *http://ucesp.ws.binghamton.edu/SecTran07.htm*.

Xiaohua(Edward) Li received the B.S. and M.S. degrees from Shanghai Jiao Tong University, Shanghai, China, in 1992 and 1995, respectively, and the Ph.D. degree from the University of Cincinnati, Cincinnati, OH, in 2000.

He was an assistant professor from 2000 to 2006, and has been an associate professor since 2006, both with the Department of Electrical and Computer Engineering, State University of New York at Binghamton, Binghamton, NY. His research interests are in the fields of adaptive and array signal processing, blind channel equalization, and digital and wireless communications.

Juite Hwu is currently a Ph.D. candidate at the Department of Electrical and Computer Engineering, State University of New York at Binghamton, Binghamton, New York, USA. He received his BS degree from the National Taiwan Ocean University, Taiwan in 2002, and his MS degree from the State University of New York at Binghamton in 2005, respectively. His research interests lie in wireless communications.

E. P. Ratazzi received the B.S. in Electrical Engineering from Rensselaer Polytechnic Institute in 1987, the M.S. in Electrical Engineering from Syracuse University in 1992, and the M.S. in Management from RPI in 2006.

He is currently a Principle Engineer at the Air Force Research Laboratory in Rome, New York where he is the Technical Advisor for the Cyber Operations Branch. In this position he leads a team of approximately 40 Government scientists and engineers developing the next generation of cyber defense and cyber attack technologies.

Besides his broad interest in the cyber operations field, his specific technical interests include physical layer techniques for wireless network security and IA applications of software-defined radios. Mr. Ratazzi is a Senior Member of the Institute of Electrical and Electronics Engineers, Past Chair of the Mohawk Valley Section of the IEEE, and Chair of the Mohawk Valley's joint Antennas and Propagation/Microwave Theory and Techniques Society Chapter. Mr. Ratazzi is also an adjunct faculty member at Syracuse University where he teaches classes in wireless security and networking.