ARRAY REDUNDANCY AND DIVERSITY FOR WIRELESS TRANSMISSIONS WITH LOW PROBABILITY OF INTERCEPTION

Xiaohua Li and Juite Hwu

Department of Electrical and Computer Engineering
State University of New York at Binghamton
Binghamton, NY 13902
{xli,jhwu1}@binghamton.edu

E. Paul Ratazzi

Air Force Research Laboratory
AFRL/IFGB
Rome, NY 13441
paul.ratazzi@afrl.af.mil

ABSTRACT

In contrast to the classical spread spectrum or data encryption methods, we propose an array redundancy-based approach for wireless transmissions with inherent low probability of interception (LPI). The redundancy of transmit antenna arrays introduces some degrees of freedom for deliberate signal randomization, based on which, diversity is exploited to randomize the eavesdropper's signal. LPI is analyzed by proving the indeterminacy of eavesdroppers' blind deconvolution. Extensive simulations and preliminary experiments are conducted to demonstrate the proposed method.

1. INTRODUCTION

Along with the rapid development of wideband wireless communication networks, wireless security has become a critical concern. While many security techniques developed in wired networks can be applied, the special characteristics of wireless networks and wireless transmissions call for innovative wireless security design.

Wireless transmissions are inherently broadcasting, and thus have no physical boundary. Any receivers nearby can hear the transmissions, and can potentially listen/analyze the transmitted signals, or conduct jamming. In addition, wireless nodes have more severe constraints on energy and bandwidth, which means more efficient security designs have to be developed specifically for wireless networks. Wireless links are inherently unreliable and untrustful, whereas wireless networks have more dynamic topology. They all make wireless security a challenging task.

Considering that most of such issues are related to the unique physical-layer of wireless communications, physical-layer security techniques are important. They are necessary to resolve the boundary control issue, and are better for bandwidth/power efficiency optimization. They can also assist resolving the unreliable link issue, which help upper-layer security techniques within a framework of innovative cross-layer security design.

An important issue of physical-layer security is to guarantee wireless transmissions with negligibly low probability of interception (LPI) without relying on upper layer data encryption. Many existing physical-layer secure transmissions either can not withstand a strict LPI analysis, or rely on encryption keys so that the security is not in the physical-layer [1]. Traditionally, spread spectrum techniques are the most widely used techniques for LPI/LPD (low probability of detection). However, when data transmissions are evolving toward wideband, spread spectrum alone may not be enough because of the reduced space of spreading gain [2].

This work was supported by US AFRL under Grant FA8750-05-1-0233.

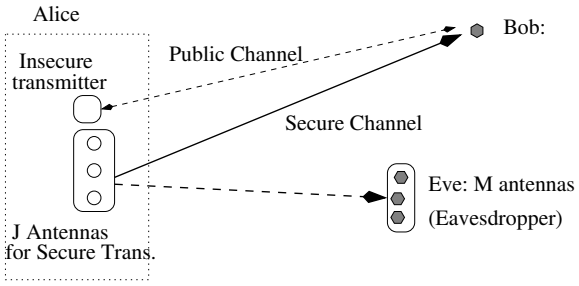

Fig. 1. Secure wireless transmission model.

In [3], we have shown that inherent security can be realized based on the diversity of antenna array transmissions. The array redundancy makes it possible to randomize the transmitted signals to prevent deconvolution, especially blind deconvolution, so as to prevent eavesdropping. Such an approach represents an innovative way of secure waveform design, differently from the widely used spread spectrum or data encryption techniques. Based on [3], in this paper we propose a special randomization method for determining the transmit antenna weights. We also give a proof of LPI. In addition, extensive simulations and the development of a testbed to support the proposed transmission schemes are presented.

This paper is organized as follows. In Section 2, a framework of secure array transmission is introduced. In Section 3, we propose a deliberate randomization scheme and analyze the security. Simulations and experiments are given in Section 4 and conclusions are presented in Section 5.

2. SECURE ARRAY TRANSMISSION MODEL

As shown in Fig. 1, Alice transmits to Bob without any shared encryption keys, in face of the passive eavesdropper Eve. Other than the J transmit antennas in the secure channel, Alice may also use some other antennas communicating with Bob, which gives an insecure public channel. This public channel may be used for the synchronization purpose between Alice and Bob, or for some special secret key management protocols [4].

We consider only the secure channel from Alice to Bob in this paper. Using J antennas, Alice transmits to Bob a symbol se-

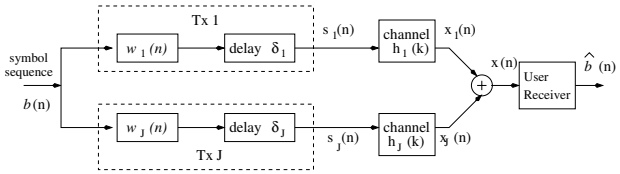

Fig. 2. Transmit beamforming-like transmission block diagram.

quence $\{b(n)\}$ which is assumed as i.i.d. uniformly distributed with zero-mean and unit variance. With a transmit-beamforming-like scheme [5] as shown in Fig. 2, Alice transmits vectors

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

where $w_i(n)$ denotes the weighting coefficient of the i^{th} transmit antenna during the symbol interval n. Note that transmitters may introduce intentional delays δ_i, or even use more complex space-time processing, which will be investigated in the future.

Assume the propagation channel be Rayleigh flat fading. The signal received by Bob (with one antenna) is

$$x(n) = \mathbf{h}^H \mathbf{s}(n) + v(n), \quad (2)$$

where $v(n)$ is zero-mean AWGN. The coefficients of the $J \times 1$ channel vector $\mathbf{h}$ are independent complex circular symmetric Gaussian distributed with zero-mean and unit variance. In this letter, $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^H$ denote conjugate, transpose and Hermitian, respectively.

With M receiving antennas, Eve receives signals

$$\mathbf{x}_e(n) = \mathbf{H}_e \mathbf{s}(n) + \mathbf{v}_e(n), \quad (3)$$

where $\mathbf{x}_e(n)$ and $\mathbf{H}_e$ are with dimension $M \times 1$ 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 several carrier wavelengths, then their channels can be considered as independent. We will use simulations and experiments to demonstrate it in Section 4.

Therefore, we assume that channels $\mathbf{h}$ and $\mathbf{H}_e$ are different, and 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 $\mathbf{x}_e(n)$. On the other hand, Alice and Bob do not know $\mathbf{h}$ and $\mathbf{H}_e$ either. Our objective is to design the transmission weights $\mathbf{w}(n)$ so that Bob can detect symbols $b(n)$ successfully with low bit-error-rate (BER) while Eve can not estimate symbols.

3. DELIBERATE RANDOMIZATION FOR LPI

A way to create high BER for Eve is to prevent Eve from channel/symbol estimation, which means, first, Alice can not transmit training signals by the J transmit antennas, and second, Eve's blind deconvolution capability has to be prevented as well. In this section, we propose a transmission scheme with which Bob can detect signals without channel knowledge so that no training is to be transmitted. Without training, Eve has to rely on blind deconvolution. Then, we propose a deliberate randomization scheme to randomize Eve's signal so that blind deconvolution has unresolvable ambiguity. Note that the necessary pilots for Bob's synchronization purpose can be transmitted by the antennas of the public channel.

3.1. Transmission and receiving procedure from Alice to Bob

In order for Bob to estimate symbols, the channel from Alice to Bob has to be resolved. Traditionally, this can be conducted by either Alice or Bob. We ask Alice instead of Bob to estimate and utilize the knowledge of $\mathbf{h}$. Alice can estimate $\mathbf{h}$ based on channel reciprocity [5]. Bob first transmits a training signal to Alice using the same carrier frequency as the secret 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 parameters. This procedure can be repeated for time-varying channels. Note that this procedure gives no useful information to Eve.

With the knowledge of $\mathbf{h}$, Alice designs $\mathbf{w}(n)$ so that

$$\mathbf{h}^H \mathbf{w}(n) = \|\mathbf{h}\|, \quad (4)$$

where $\|\mathbf{h}\|$ denotes the norm of $\mathbf{h}$. From the received signal $x(n) = \|\mathbf{h}\|b(n)+v(n)$, Bob can detect symbols from $\hat{b}(n) = \|\mathbf{h}\|^{-1}x(n)$, where $\|\mathbf{h}\|^{-1}$ can be easily calculated from the received signal power.

Therefore, Alice needs to design $\mathbf{w}(n)$ under the constraint (4), which can be performed as follows. In each symbol interval, Alice first selects randomly an element with sufficiently large magnitude from $\mathbf{h}$. Let h_i be selected during the symbol interval n. The weighting vector $\mathbf{w}(n)$ is then calculated as

$$\mathbf{w}(n) = \mathbf{P}_i(n) \begin{bmatrix} a_i - \mathbf{f}_i^H \mathbf{z}_i(n) \\ \mathbf{z}_i(n) \end{bmatrix} \quad (5)$$

where $a_i = \|\mathbf{h}\|/h_i^*$, $\mathbf{f}_i = [h_1, \cdots, h_{i-1}, h_{i+1}, \cdots, h_J]^T/h_i$, $\mathbf{z}_i(n) = [w_1(n), \cdots, w_{i-1}(n), w_{i+1}(n), \cdots, w_J(n)]^T$, and $\mathbf{P}_i(n)$ is a $J \times J$ permutation matrix whose function is to insert the first row of the following vector into the i^{th} row. Note that $\mathbf{z}_i(n)$ is arbitrary.

3.2. A deliberate randomization scheme

From (5), we can choose $\mathbf{z}_i(n)$ appropriately to prevent Eve from blind deconvolution. For example, this purpose can be fulfilled by simply making $\mathbf{z}_i(n)$ with a distribution unknown to Eve since blind deconvolution requires known source statistics. It is well known that successful blind deconvolution requires that the receiver knows some special statistics or structure of the transmitted signals. However, most of existing researches have been on when blind deconvolution can be conducted, not when blind deconvolution can not be conducted [6]. 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., $\mathbf{r}_i(n) \sim \mathcal{N}_{J-1}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ [7]. The parameters $\boldsymbol{\mu}$ and $\boldsymbol{\Sigma}$ are arbitrary and unknown to both Eve and Bob, and can even be time-varying.

From (5) and (1), the transmitted signal vector is

$$\mathbf{s}(n) = \mathbf{P}_i(n) \left[\begin{array}{c} a_i b(n) - \mathbf{f}_i^H \mathbf{r}_i(n) \\ \mathbf{r}_i(n) \end{array} \right]. \quad (6)$$

For each selected channel coefficient h_i, the expected total transmission power is

$$\begin{aligned} \mathrm{tr}\{E[\mathbf{s}(n)\mathbf{s}^H(n)]\} = \mathrm{tr}\{\boldsymbol{\mu}\boldsymbol{\mu}^H + \boldsymbol{\Sigma}\} + \\ |a_i|^2 + \mathbf{f}_i^H(\boldsymbol{\mu}\boldsymbol{\mu}^H + \boldsymbol{\Sigma})\mathbf{f}_i, \end{aligned} \quad (7)$$

whereas the diagonal entry of $E[\mathbf{s}(n)\mathbf{s}^H(n)]$ gives the transmission power of each antenna. We need both to reduce the total power and to balance the power among the transmitting antennas. This can be conducted by choosing properly $\boldsymbol{\mu}$ and $\boldsymbol{\Sigma}$. Details will be reported elsewhere due to space limit.

3.3. Indeterminacy of Eve's blind deconvolution

From (6), Alice's transmitted signal can be written as $\mathbf{s}(n) = \mathbf{G}(n)\mathbf{r}_i(n) + \mathbf{g}(n)b(n)$ where

$$\mathbf{G}(n) = \mathbf{P}_i(n) \left[\begin{array}{c} -\mathbf{f}_i^H \\ \mathbf{I}_{J-1} \end{array} \right], \quad \mathbf{g}(n) = \mathbf{P}_i(n) \left[\begin{array}{c} a_i \\ \mathbf{0}_{J-1} \end{array} \right]. \quad (8)$$

We have used $\mathbf{0}_{J-1}$ to denote a $J-1$ dimensional zero vector. Eve's received signal can be written as

$$\mathbf{x}_e(n) = \left[\begin{array}{cc} \mathbf{H}_e\mathbf{G}(n) & \mathbf{I}_M \end{array} \right] \left[\begin{array}{c} \mathbf{r}_i(n) \\ \mathbf{v}_e(n) \end{array} \right] + \mathbf{H}_e\mathbf{g}(n)b(n). \quad (9)$$

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

$$\begin{aligned} \mathbf{x}_e(n) \sim \mathcal{N}_M\left(\mathbf{H}_e\mathbf{G}(n)\boldsymbol{\mu} + \mathbf{H}_e\mathbf{g}(n)b(n), \right. \\ \left. \mathbf{H}_e\mathbf{G}(n)\boldsymbol{\Sigma}\mathbf{G}^H(n)\mathbf{H}_e^H + \sigma_v^2\mathbf{I}_M\right) \end{aligned} \quad (10)$$

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

$$\mathbf{Q} = \mathbf{P}_i(n) \left[\begin{array}{cc} u & \mathbf{0} \\ \mathbf{0} & \mathbf{V} \end{array} \right] \mathbf{P}_i^{-1}(n), \quad (11)$$

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

Proof. Define

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

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 (10) 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 statistic property of $\{b(n)\}$ does not help.

Let us assume that Eve can estimate $\mathbf{H}_e$ up to the ambiguity matrix $\mathbf{Q}$ in (11), then by substituting $\mathbf{H}_e$ with $\mathbf{H}_e\mathbf{Q}$ and removing $\mathbf{H}_e$, Eve's signal can be changed to

$$\tilde{\mathbf{x}}_e(n) = \mathbf{P}_i(n) \left[\begin{array}{c} u\mathbf{f}_i^H \\ \mathbf{V} \end{array} \right] \mathbf{r}_i(n) + \mathbf{P}_i \left[\begin{array}{c} ua_i \\ \mathbf{0}_{J-1} \end{array} \right] b(n) + \tilde{\mathbf{v}}_e(n). \quad (12)$$

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 an bit error rate 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 error rate by choosing properly $\boldsymbol{\Sigma}$.

Since Eve can not estimate $\mathbf{H}_e$, she may use a brute-force exhaustive search to look for a vector $\mathbf{h}^H\mathbf{H}_e^{-1}$ (assume $\mathbf{H}_e$ is invertible). The complexity increases exponentially with the channel length J. If such a complexity becomes prohibitive, the best way left for Eve is to directly use Bob's symbol detection procedure, in which case the error rate depends on the difference between $\mathbf{h}$ and $\mathbf{H}_e$ (with $M = 1$). We will examine it by extensive simulations in Section 4.

4. SIMULATIONS AND EXPERIMENTS

In this section, we use two simulations and experiments to study the effectiveness of the proposed transmission scheme by evaluating the BER of Bob and Eve. Eve is assumed to estimate symbols directly using Bob's method. In the first simulation experiment, we used randomly generated channels. We used $J = 4$ and QPSK transmission. Each BER was evaluated as the average of 5000 runs, and 400 QPSK symbols were transmitted during each run. The results of BER as functions of receiving SNR are shown in Fig. 5 as the solid lines, from which we see that Bob can reliably receive signals while Eve can not.

In the second simulation experiment [8], our objective is to show how confident we can say that Bob and Eve's channels are different. We considered a $3\times3\times7$ (height/wide/length, in meters) room, where there were some objects (such as a Box), as shown in Fig. 3. We placed an antenna grid, with the minimum distance between antennas (grid length) to be half of a wavelength. Some of the grid antennas are shown in the figure, together with a transmit antenna placed in the other end of the room. We let the transmit antenna to transmit signals, and we obtained the signals received by all the receive antennas. This procedure is conducted using electromagnetic simulation software (based on FDTD). From the signals we can estimate all effective channels on a $\lambda = 0.3$ meters grid.

Considering the far field only, we obtained altogether 490 channels. Then we used each of them as $\mathbf{h}$ while each of the rest as $\mathbf{H}_e$ to find the error rates of Bob and Eve with the simulation parameters in the first experiment. For each SNR value, Bob's error rate was the average of all these 490 cases, while Eve's error rate was obtained as the minimum value among all possible channels (100%) or the majority (99%) of the channels. Note that the positions where Eve was within 2λ of Bob were avoided. The results are shown in Fig. 5 as the dashed curves. It can be seen that for at least 99% of all possible channels, Eve's error rate is extremely large.

We are also building a testbed using the wireless transmission modules of ComBlock.com [8]. We implemented two QPSK transmitters and two QPSK receivers. One snap shot of the experiment is shown in Fig. 4. 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. 5). Note that the two receiving antennas (one for Bob, one for Eve) were purposely placed very close to each other.

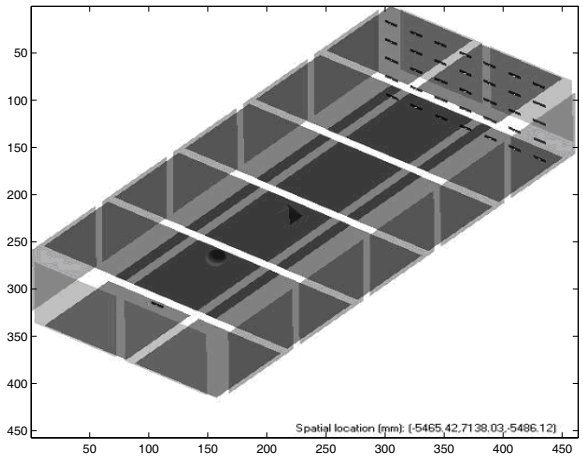

Fig. 3. Settings of a room for electromagnetic wave propagation simulation.

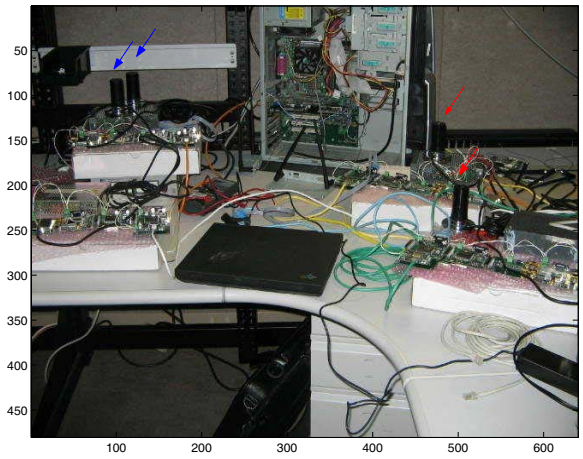

Fig. 4. Experiment setup with 2 transmitting antennas (red arrow) and 2 receive antennas (blue arrow).

5. CONCLUSIONS

In this paper, we propose to use deliberately randomized array transmissions to realize wireless transmissions with LPI. The array redundancy is exploited to guarantee the indeterminacy of the eavesdropper's blind deconvolution. The LPI is proved. The method is demonstrated by both simulations and preliminary testbed experiments.

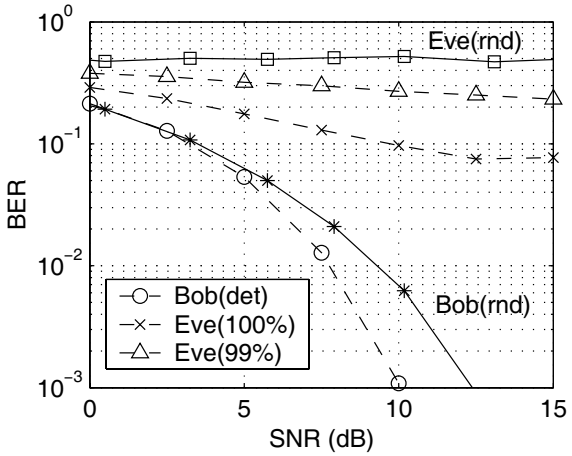

Fig. 5. BER of Bob and Eve. Solid lines: Rayleigh fading channels. Dashed lines: channels for a special room.

The proposed scheme uses higher transmission power, and thus trade power for transmission security. Although LPD 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.

6. REFERENCES

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

[2] E. Ghashghai, "Communications networks to support integrated intelligence, surveillance, reconnaissance, and strike operations," *Rand Project Air Force Report*, 2005.

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

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

[5] 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.

[6] 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.

[7] R. J. Muirhead, *Aspects of Multivariate Statistical Theory*, John Wiley & Sons, 1982.

[8] Simulation data and experiment details are available at *http://ucesp.ws.binghamton.edu/SecTran05.htm*.