AFRL-IF-RS-TR-2006-104
Final Technical Report
March 2006

WIRELESS INFORMATION ASSURANCE AND COOPERATIVE COMMUNICATIONS

SUNY Binghamton

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-2006-104 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

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	MARCH 2006	Final Jun 05 – Sep 05

4. TITLE AND SUBTITLE
WIRELESS INFORMATION ASSURANCE AND COOPERATIVE COMMUNICATIONS

5. FUNDING NUMBERS
C - FA8750-05-1-0233
PE - 62702F
PR - 558B
TA - II
WU - RS

6. AUTHOR(S)
Xiaohua (Edward) Li

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
SUNY Binghamton
PO Box 6000
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-2006-104

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: E. Paul Ratazzi/IFGB/(315) 330-3766/ 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 consists of four parts. The first part develops physical-layer security techniques with both multi-input single-output (MISO) transmissions and multi-input multi-output (MIMO) transmissions. The second part addresses cooperative communications, whereas the third part involves the testbed development. The final part contains conclusions. To save space, some details were omitted but may be found in (16) – (19).

14. SUBJECT TERMS
Multi-Input Single-Output, MISO, Multi-Input Multi-Output, MIMO

15. NUMBER OF PAGES
24

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

Table of Figures

This report consists of four parts. The first part develops physical-layer security techniques with both multi-input single-output (MISO) transmissions and multi-input multi-output (MIMO) transmissions. The second part addresses cooperative communications, whereas the third part involves the testbed development. The final part contains conclusions. To save space, some details were omitted, but may be found in [16]-[19].

Part I. Array Redundancy and Deliberate Randomization for Inherently Secure Wireless Transmissions

This part is organized as follows. In Section I.1, we consider the MISO secure transmission [18]. Then in Section I.2, secure MIMO transmission is proposed [16]. Note that the main focus of both of them is the theoretic proof of the transmission security. Simulations are conducted for each of them.

I.1. Secure MISO transmission

I.1.1. Introduction

Along with the rapid development of 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 call for innovative wireless security design. Wireless transmissions are inherently broadcasting without physical boundary (any receivers nearby can hear the transmission). Wireless nodes have more severe constraints on energy and bandwidth, whereas wireless networks have more dynamic topology. Since physical-layer security techniques can address directly such special wireless characteristics, they are helpful to provide boundary control, to enhance efficiency, as well as to assist upper-layer security techniques for innovative cross-layer security designs.

An important issue of physical-layer security is to realize inherently secure transmissions, i.e., 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.

In [13,14], 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. This section gives a further development over [13] with a new deliberate randomization scheme and a rigorous security proof.

The new approach's contribution to cryptography lies in realizing provable secrecy which we call (weak) information-theoretic secrecy. It means that LPI can be proved but the secrecy is theoretically susceptible to exhaustive search. The complexity of exhaustive search is also provable, and can be made practically prohibitive.

It is well known that classical encryption techniques have only unproven complexity-based secrecy [3]. We also know that (strong) information-theoretic secrecy or perfect secrecy is achievable by quantum cryptography based on some special quantum effects such as intrusion detection and impossibility of signal clone [20]. Unfortunately, the dependence on such effects results in extremely low transmission efficiency because weak signals have to be used. For example, the channel capacity (assume a binary symmetric channel) may be in the level of 10^{-6} [21]. A recent development in quantum cryptography [22] is to implement direct data encryption by quantum principles so that strong signals can be used for high efficiency. The secrecy in this case is just the provable secrecy or (weak) information-theoretic secrecy.

With similarly low efficiency, (strong) information-theoretic secrecy is also achievable by ordinary wireless transmissions such as broadcasting with weak signals [1] or transmitting in time-varying channels [14]. The approach developed in this section gives provable secrecy similar to [22]. However, fading channels in wireless transmissions can be a good source of initial advantage (compared to the short initial secret key in [21, 22]) as required between the legitimate users. The channel reciprocity gives a simple but reliable way of creating such advantage (compared to the unknown mysterious ways of exchanging the short initial secret key). Therefore, wireless transmissions can be a competitive alternative to quantum cryptographic techniques in wireless networks.

I.1.2. Secure array transmission model

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.

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 (required by many secrecy protocols [1, 20]).

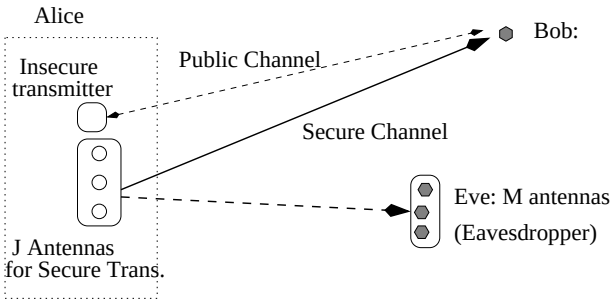

Figure 1. Secure transmission model.

We consider only the secure channel from Alice to Bob in this section. Using J antennas, Alice transmits symbol sequence $\{b(n)\}$ which is assumed as i.i.d. uniformly distributed with zero-mean and unit variance. With a transmit-beamforming-like scheme, Alice transmits vectors

$$\mathbf{s}(n) = \begin{bmatrix} w_1(n) \\ \vdots \\ w_J(n) \end{bmatrix} \stackrel{\Delta}{=} \mathbf{w}(n)b(n), \tag{I.1}$$

where $w_i(n)$ denotes the weighting coefficient of the i^{th} transmit antenna during the symbol interval n. Assume the propagation channel be Rayleigh flat fading. The signal received by Bob (with one antenna) is

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

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, $(\square)^*$, $(\square)^T$ and $(\square)^H$ denote conjugate, transpose and Hermitian, respectively.

With M receiving antennas, Eve receives signals

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

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 use simulations to demonstrate it in Section I.1.4. Eve does not know $\mathbf{h}$ and $\mathbf{H}_e$, but she may try blind or non-blind methods to estimate $\mathbf{H}_e$ from $\mathbf{x}_e(n)$.

If Bob and Eve have receiving bit-error-rate (BER) ε and δ, respectively, then the secret channel capacity from Alice to Bob (with guaranteed information-theoretic secrecy) is $C = H(\delta) - H(\varepsilon)$ if $\delta > \varepsilon$ and $C = 0$ otherwise [2, 5], where $H(p)$ denotes the binary entropy function. If Alice and Bob can

exchange information over the public channel, the secret channel capacity becomes $C = H(\varepsilon + \delta - 2\varepsilon\delta) - H(\varepsilon)$ [1]. Obviously, for small δ, the capacity becomes too small to be useful. Therefore, our objective is to design $\mathbf{w}(n)$ to guarantee high δ but small ε.

I.1.3. Deliberate randomization for provable secrecy

A way to guarantee high δ is to prevent Eve from channel/symbol estimation. We propose to design 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, which will be prevented by a deliberate randomization scheme. Note that the necessary pilots for Bob's synchronization purpose can be transmitted by the antennas of the public channel.

I.1.3.1 Transmission and receiving procedure from Alice to Bob

Since it is necessary to exploit $\mathbf{h}$ as an initial advantage, we ask Alice instead of Bob to utilize the knowledge of $\mathbf{h}$. Alice can estimate $\mathbf{h}$ based on channel reciprocity. 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 use the estimated channel as $\mathbf{h}$ to design transmission parameters. Note that this step gives no useful information to Eve.

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

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

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

We use the method in [13] to design $\mathbf{w}(n)$ under the constraint (I.4). In each symbol interval, we first select 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

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

where $a_i = \|\mathbf{h}\| / h_i^*, \mathbf{f}_i = \left[h_1, \cdots, h_{i-1}, h_{i+1}, \cdots, h_J\right]^T / h_i$, $\mathbf{z}_i(n) = \left[w_1(n), \cdots, w_{i-1}(n), w_{i+1}(n), \cdots, w_J(n)\right]^T$, 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.

I.1.3.2 A deliberate randomization scheme

From (I.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 [13]. Nevertheless, to furbish a rigorous quantitative analysis, 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 $\sum$, i.e., $\mathbf{r}_i(n) \sim N_{J-1}(\boldsymbol{\mu}, \sum)$. The parameters $\boldsymbol{\mu}$ and $\sum$ are arbitrary and unknown to both Eve and Bob, and can even be time-varying.

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

$$\mathbf{s}(n) = \mathbf{P}_i(n) \begin{bmatrix} a_i b(n) - \mathbf{f}_i^H \mathbf{r}_i(n) \\ \mathbf{r}_i(n) \end{bmatrix}. \tag{I.6}$$

I.1.3.3 Indeterminacy of Eve's blind deconvolution

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

$$\mathbf{G}(n) = \mathbf{P}_i(n)\begin{bmatrix} -\mathbf{f}_i^H \\ \mathbf{I}_{J-1} \end{bmatrix}, \quad \mathbf{g}(n) = \mathbf{P}_i(n)\begin{bmatrix} a_i \\ \mathbf{0}_{J-1} \end{bmatrix}. \tag{I.7}$$

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

$$\mathbf{x}_e(n) = \begin{bmatrix} \mathbf{H}_e\mathbf{G}(n) & \mathbf{I}_M \end{bmatrix}\begin{bmatrix} \mathbf{r}_i(n) \\ \mathbf{v}_e(n) \end{bmatrix} + \mathbf{H}_e\mathbf{g}(n)b(n). \tag{I.8}$$

Obviously, in each symbol interval n, Eve's signal is M -variate Gaussian distributed [6] due to the random $\mathbf{r}_i(n)$, i.e.,

$$\mathbf{x}_e(n) \sim \mathcal{N}_M\left(\mathbf{H}_e\mathbf{G}(n)\boldsymbol{\mu} + \mathbf{H}_e\mathbf{g}(n)b(n), \mathbf{H}_e\mathbf{G}(n)\sum\mathbf{G}^H(n)\mathbf{H}_e{}^H + \sigma_v{}^2\mathbf{I}_M\right). \tag{I.9}$$

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

$$\mathbf{Q} = \mathbf{P}_i(n)\begin{bmatrix} u & \mathbf{0} \\ \mathbf{0} & \mathbf{V} \end{bmatrix}\mathbf{P}_i^{-1}(n), \tag{I.10}$$

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

Proof. Define

$$\mathbf{H}_e = \mathbf{H}_e\mathbf{Q},$$
$$\tilde{\mathbf{G}}(n) = u^{-1}\mathbf{G}(n)\mathbf{V}, \quad \tilde{\mathbf{g}}(n) = u^{-1}\mathbf{g}(n)$$
$$\boldsymbol{\mu} = \mathbf{V}^{-1}\boldsymbol{\mu}, \quad \tilde{\sum} = \mathbf{V}^{-1}\sum\left(\mathbf{V}^{-1}\right)^H,$$

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 $\tilde{\mathbf{H}}_e\tilde{\mathbf{G}}(n)\boldsymbol{\mu}\tilde{\mathbf{G}}(n)^H\tilde{\mathbf{H}}_e{}^H = \mathbf{H}_e\mathbf{G}(n)\sum\mathbf{G}(n)^H\mathbf{H}_e{}^H$. The distribution (I.9) does not change if $\mathbf{H}_e$, $\mathbf{G}(n)$, $\mathbf{g}(n)$, $\boldsymbol{\mu}$ and $\sum$ are replaced by $\tilde{\mathbf{H}}_e$, $\tilde{\mathbf{G}}(n)$, $\tilde{\mathbf{g}}(n)$, $\tilde{\boldsymbol{\mu}}$ and $\tilde{\sum}$, 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 (I.10), then by substituting $\mathbf{H}_e$ with $\mathbf{H}_e\mathbf{Q}$ and removing $\mathbf{H}_e$, Eve's signal can be changed to

$$\tilde{\mathbf{x}}_e(n) = \mathbf{P}_i(n)\begin{bmatrix} u\mathbf{f}_i^H \\ \mathbf{V} \end{bmatrix}\mathbf{r}_i(n) + \mathbf{P}_i(n)\begin{bmatrix} ua_i \\ \mathbf{0}_{J-1} \end{bmatrix}b(n) + \tilde{\mathbf{v}}_e(n). \tag{I.11}$$

In order to detect $b(n)$, Eve has to first resolve $\mathbf{P}_i(n)$, i.e., determine which $i \in [1, \quad J]$ 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 $\sum$.

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 I.1.4.

I.1.4. Simulations

In this section, we use two experiments to study the security 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 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. 2 as the solid lines, from which we see that Bob can reliably receive signals while Eve can not.

In the second experiment, we study how confident we can say that Bob and Eve's channels are different. We considered a $3\times3\times7$ (height/wide/length) room with some blocks, and used electromagnetic simulation software (based on FDTD) to estimate all channels on a $\lambda = 0.3$ meters grid. Consider 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 experiments. 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 is within 2λ of Bob are avoided. The results are shown in Fig. 2 as the dashed curves. It can be seen that for at least (99%) of all possible channels, Eve's error rate is extremely large.

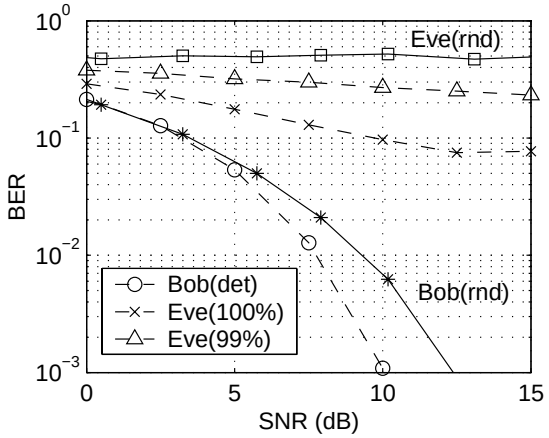

Figure 2. BER of Bob and Eve.
Solid lines: Rayleigh fading channels. Dashed lines: channels obtained from EM propagation simulation in a special room.

I.2. Secure MIMO transmission

I.2.1. Introduction

Advanced wireless techniques such as multi-input multi-output (MIMO) techniques are important to broadband and highly dynamic wireless communication networks that are essential for military operations. Such techniques are developed with efficiency instead of security as the primary criterion, or even without security consideration at all. Because wireless transmissions are lack of physical boundary (any adversary can receive the signal within the range), the lack of security in these techniques may potentially result in a weak physical-layer security, which may even weaken the end-to-end network security.

Innovative cross-layer security designs with both physical-layer security and upper-layer security techniques are desirable for military wireless networks. While the physical-layer may rely on upper-layer encryption techniques for security, it is interesting to study whether the physical-layer can have built-in security and whether physical-layer security techniques can assist upper-layer security designs.

The built-in security of the physical-layer is defined as that physical-layer transmissions guarantee low-probability-of-interception (LPI) based on transmission properties such as modulations, signals and channels, without resorting to source data encryption. No secret keys are required before transmission. This

is in contrast to the traditional techniques such as spread spectrum that rely on secret codes shared between the transmitter and the receiver.

One of the fundamental issues for physical-layer built-in security is the capacity of the transmission channel when built-in security is guaranteed. Such capacity is named secret channel capacity. The secrecy is defined as information-theoretic secrecy, i.e., the adversary's received signal gives no more information for eavesdropping than purely guessing. Information-theoretic secrecy is in fact equivalent to perfect secrecy [3]. Practically, it means negligibly low interception probability.

One of the recent attempts on specifying secret channel capacity is [4], where the MIMO secret channel capacity is analyzed under the assumption that the adversary does not know even his own channel. Unfortunately, such an assumption does not seem practical if considering deconvolution or blind deconvolution techniques. As a matter of fact, almost all existing results on secret channel capacity are based on some kinds of assumptions that appear impractical [1, 2, 5]. It has been a challenge in information theory for decades (after [2]) to find practical ways to realize information-theoretic secrecy.

Recently, we have found that antenna array transmissions may provide valid ways to realize information-theoretic secrecy when the transmission redundancy and the limit of blind deconvolution are appropriately exploited [13]. LPI can be guaranteed by using some extra antennas with some more transmission power or bandwidth. This innovative concept of secure waveform design is completely different from the traditional techniques such as spread spectrum.

This section extends the results of [13] and Section I.1 into multiple-input multiple-output transmissions so that the complexity of exhaustive search, the only way left for the adversary, is an order of magnitude higher.

I.2.2. MIMO transmission model

We consider the case where Alice transmits to Bob using J transmitting antennas. Bob uses K receiving antennas. During this procedure, Bob extracts a secret key whereas Eve should be deprived of signal interception capability, as illustrated in Fig. 3. In this section, we consider the secret channel only, where Alice transmits a secret sequence to Bob using the J transmitting antennas.

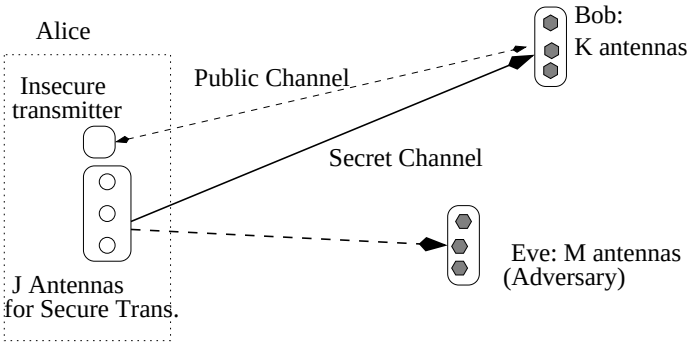

Figure 3. System model for a secret-key agreement between Alice and Bob.

In the secret channel, a MIMO transmission scheme shown in Fig. 4 is used by Alice and Bob. A vector symbol sequence $\{\mathbf{b}(n)\}$ is processed by Alice with a corresponding matrix sequence $\mathbf{W}(n)$, which gives the transmitted signal vector sequence $\{\mathbf{s}(n)\}$. Specifically, we have

$$\mathbf{s}(n) = \mathbf{W}(n)\mathbf{b}(n), \tag{I.12}$$

where $\mathbf{s}(n)$, $\mathbf{W}(n)$, and $\mathbf{b}(n)$ have dimensions $J \times 1$, $J \times K$ and $K \times 1$, respectively.

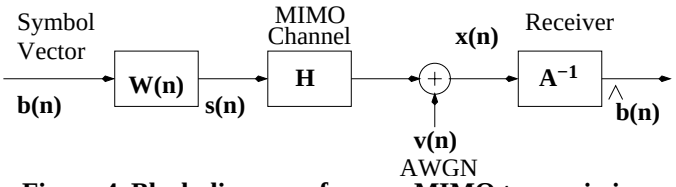

Figure 4. Block diagram of secure MIMO transmission.

The signal vector $\mathbf{s}(n)$ is transmitted through the J transmitting antennas in the n^{th} symbol interval. Assume the propagation channel be Rayleigh flat fading. The signal received by Bob is

$$\mathbf{x}(n) = \mathbf{H}\mathbf{s}(n) + \mathbf{v}(n), \tag{I.13}$$

where $\mathbf{x}(n)$ is the $K \times 1$ received sample vector, $\mathbf{v}(n)$ denotes the $K \times 1$ AWGN vector with zero-mean. The channel matrix $\mathbf{H}$ is $K \times J$, whose coefficients are independent complex circular symmetric Gaussian distributed with zero-mean and unit variance.

We assume that $\mathbf{H}$ is block fading [4], i.e., it is constant or slowly time-varying during the transmission of a block of symbol vectors, but may change randomly between blocks. The symbols (i.e., elements in $\mathbf{b}(n)$) are independent uniformly distributed with zero-mean and unit variance. The transmission power is thus determined by the processing weights $\mathbf{W}(n)$.

Eve may use multiple receiving antennas for better interception, and the interception becomes much easier when the propagation is flat-fading. Therefore, we consider the worst case (to Alice and Bob) where Eve receives signals from M receiving antennas,

$$\mathbf{x}_u(n) = \mathbf{H}_u\mathbf{s}(n) + \mathbf{v}_u(n), \tag{I.14}$$

where $\mathbf{x}_u(n)$ and $\mathbf{H}_u$ are with dimension $M \times 1$ and $M \times J$, respectively. The vector $\mathbf{v}_u(n)$ is AWGN with zero-mean and covariance matrix $\sigma_v{}^2\mathbf{I}_M$. The notations are similar to (I.13) except that $(\square)_u$ is used to denote the unauthorized user Eve. Each element of $\mathbf{H}_u$ has the same distribution as, but is independent from, those of $\mathbf{H}$. From the extensive studies on MIMO 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.

Eve does not know the channels $\mathbf{H}$ and $\mathbf{H}_u$, but she may try blind or non-blind methods to estimate $\mathbf{H}_u$ from $\mathbf{x}_u(n)$. Alice and Bob do not know both channels either, and in particular, they can not estimate $\mathbf{H}_u$.

Note that although we study the secrecy in one direction only, the same scheme can be set up on the other direction. Or, as one direction is secured, the other direction can easily be secured too. In addition, although we consider a single-point to single-point transmission in this paper, the scheme also fits single-point to multi-point transmission (multi-user communication or broadcasting) scenarios. For each specific user, all other ones can be treated as adversaries because different users have different channels.

I.2.3. MIMO transmission procedure

Since we can not depend on noise as the only source of receiving error for Eve, we create some intentional difference between Bob and Eve's signals by exploiting the redundancy of antenna array transmissions. Traditionally, such redundancy is used completely to optimize transmission efficiency. When some of the redundancy is used for secrecy, the optimal transmission efficiency may not be available. This indicates the fundamental trade-off between the transmission efficiency and secrecy. Our objective is not to make our scheme competing against the traditional encryption-based schemes in terms of transmission efficiency. But rather, we are interested in information-theoretic secrecy for a security level higher than the latter. Nevertheless, the efficiency loss can be small.

I.2.3.1 Transmission and receiving from Alice to Bob

As shown in [13], a valid way to guarantee a high error rate for Eve is to prevent Eve from channel estimation. In terms of channel estimation, Bob has no advantage over Eve. Therefore, our objective is to design a transmission scheme so that Bob can detect signals without channel knowledge,

which can be realized by shifting the channel estimation task from the receiver Bob to the transmitter Alice. Once Alice has the channel knowledge, she can adjust the MIMO transmission so that Bob does not need to estimate channel in order for symbol estimation.

There are various ways for Alice to estimate the channel $\mathbf{H}$ [13]. We use the reciprocity of the forward and backward channels in this paper. Bob first transmits a pilot signal to Alice using the same carrier frequency as the secret channel, during which Alice can estimate the backward channel, and use it for array transmission. Note that this procedure is required only once as an initialization, and gives no useful information to Eve.

From (I.12)-(I.13), Alice designs the matrix $\mathbf{W}(n)$ so that

$$\mathbf{HW}(n) = \mathbf{A}, \tag{I.15}$$

where $\mathbf{A}$ is a $K \times K$ diagonal matrix determined by Alice but unknown to Bob and Eve. The key point is to make $\mathbf{A}$ to have positive diagonal elements so that Bob can estimate them easily. Without loss of generality, we assume that $\mathbf{H}$ is full row rank. Otherwise the system simply reduces to the one with a smaller K.

From the received signal $\mathbf{x}(n) = \mathbf{Ab}(n) + \mathbf{v}(n)$, Bob can easily detect signals as

$$\hat{\mathbf{b}}(n) = \mathbf{A}^{-1}\mathbf{x}(n). \tag{I.16}$$

where $\mathbf{A}$ can be estimated from the received signal power because $\mathbf{A}$ is diagonal with positive elements. Since no channel estimation is required, it is not necessary for Alice to transmit training sequences. As a result, Eve has no training available either, and has to rely on blind deconvolution.

I.2.3.2 Transmission weights design

Although (I.15) looks similar to transmit beamforming, the major difference is that $\mathbf{W}(n)$ changes randomly in each symbol interval n so that $\mathbf{H}_u\mathbf{W}(n)$ becomes random. This prevents Eve from channel/symbol estimation. This can be realized by selecting randomly the elements of $\mathbf{W}(n)$ while satisfying the constraint (I.15). Obviously, we need $J > K$, i.e., more transmitting antennas than receiving antennas.

The criteria for designing $\mathbf{W}(n)$ include satisfying (I.15), preventing Eve from detecting $\mathbf{b}(n)$ based on (I.14), limiting the total transmission power, balancing the transmission power among the transmitting antennas, and finally, being computationally efficient.

Considering those criteria, we use a procedure similar to [13] to determine $\mathbf{W}(n)$. We first select randomly K columns from $\mathbf{H}$ to form a $K \times K$ submatrix $\mathbf{H}_0$ (with sufficiently large $\|\mathbf{H}_0\|$). Without loss of generality, we assume that the first K columns of $\mathbf{H}$ are chosen, i.e.,

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_0 & \mathbf{H}_1 \end{bmatrix}. \tag{I.17}$$

We can subdivide the matrix $\mathbf{W}(n)$ accordingly into $\mathbf{W}_0(n)$ and $\mathbf{W}_1(n)$ so that (I.15) becomes

$$\mathbf{H}_0\mathbf{W}_0(n) + \mathbf{H}_1\mathbf{W}_1(n) = \mathbf{A}. \tag{I.18}$$

Then the MIMO processing matrix $\mathbf{W}(n)$ is

$$\mathbf{W}(n) = \begin{bmatrix} \mathbf{H}_0^{-1}\left[\mathbf{A} - \mathbf{H}_1\mathbf{W}_1(n)\right] \\ \mathbf{W}_1(n) \end{bmatrix}. \tag{I.19}$$

Therefore, the transmission weights design procedure is to first select $\mathbf{H}_0$, then generate randomly $\mathbf{W}_1(n)$, and finally calculate $\mathbf{W}(n)$.

The computational complexity is $O(J^3)$ per transmission. Nevertheless, the matrix inversion is required only once for each channel realization. Transmission power can be adjusted by choosing $\mathbf{W}_1(n)$, $\mathbf{A}$ and selecting $\mathbf{H}_0$ appropriately.

As a comparison, the optimal $\mathbf{W}(n)$ in the traditional MIMO is the so-called eigen-beamforming. In this case,

$$\mathbf{W}_{opt}(n) = \mathbf{V}_{opt}\begin{bmatrix} \mathbf{D}_{opt}{}^{-1}\mathbf{U}_{opt}{}^{H}\mathbf{A}_{opt} \\ \mathbf{B} \end{bmatrix}, \tag{I.20}$$

with the singular-value decomposition (SVD) $\mathbf{H} = \mathbf{U}_{opt}\begin{bmatrix}\mathbf{D}_{opt}, & \mathbf{0}\end{bmatrix}\mathbf{V}_{opt}{}^{H}$, $\mathbf{A}_{opt} = \mathbf{I}_K / \sqrt{tr\left(\mathbf{D}^{-2}\right)}$, and $\mathbf{B} = \mathbf{0}$. Unfortunately, even though $\mathbf{B}$ can be random, this design is susceptible to the blind deconvolution of Eve, similarly as shown in [13].

I.2.4. Transmission secrecy

I.2.4.1 A randomization scheme

Since the matrix $\mathbf{W}_1(n)$ is with dimension $(J-K)\times K$, there are $K(J-K)$ degrees of freedom in designing $\mathbf{W}(n)$, which can be exploited to randomize $\mathbf{W}(n)$ so that the transmitted signal vector $\mathbf{s}(n)$ has distribution unknown to Eve (and Bob). It is well known that blind deconvolution requires some *priori* knowledge about the statistics of the transmitted sequence $\{\mathbf{s}(n)\}$, such as independence, non-Gaussian distribution, and/or distinct power spectral [13]. From (I.19), we can choose $\mathbf{W}_1(n)$ appropriately to violate all such conditions in order to prevent Eve from blind deconvolution.

Nevertheless, Eve knows that Alice and Bob depends on (I.15) for secret transmission although she does not know $\mathbf{H}$ and the diagonal elements of $\mathbf{A}$. This makes it non-trivial to design and analyze the secret transmission.

We propose that Alice simply designs $\mathbf{W}_1(n)$ such that $\mathbf{s}_1(n) = \mathbf{W}_1(n)\mathbf{b}(n)$ is $J\times K$ -variate Gaussian distributed [6] with mean $\boldsymbol{\mu}$ and covariance matrix $\sum$, i.e., $\mathbf{s}_1(n) \sim \mathcal{N}_{J-K}(\boldsymbol{\mu}, \sum)$, where

$$E[\mathbf{s}_1(n)] = \boldsymbol{\mu}, \qquad E\left[(\mathbf{s}_1(n)-\boldsymbol{\mu})(\mathbf{s}_1(n)-\boldsymbol{\mu})^H\right] = \sum. \tag{I.21}$$

In particular, $\boldsymbol{\mu}$ and $\sum$ can be made unknown to both Eve and Bob.

From (I.19) and (I.12), we have

$$\mathbf{s}(n) = \begin{bmatrix}\mathbf{s}_0(n)\\ \mathbf{s}_1(n)\end{bmatrix} = \begin{bmatrix}\mathbf{H}_0{}^{-1}\left[\mathbf{A}\mathbf{b}(n) - \mathbf{H}_1\mathbf{s}_1(n)\right] \\ \mathbf{s}_1(n)\end{bmatrix}. \tag{I.22}$$

The total transmission power is

$$tr\left\{E\left[\mathbf{s}(n)\mathbf{s}^H(n)\right]\right\} = tr\left\{\boldsymbol{\mu}\boldsymbol{\mu}^H + \sum\right\} + tr\left\{\mathbf{H}_0{}^{-1}\left[\mathbf{A}\mathbf{A}^H + \mathbf{H}_1\left(\boldsymbol{\mu}\boldsymbol{\mu}^H + \sum\right)\mathbf{H}_1{}^H\right]\mathbf{H}_0{}^{-H}\right\}, \tag{I.23}$$

whereas the diagonal entry of $E\left[\mathbf{s}(n)\mathbf{s}^H(n)\right]$ 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 $\mathbf{A}$, $\boldsymbol{\mu}$ and $\sum$. Details will be reported elsewhere due to space limit. Instead, we focus on the transmission secrecy analysis in this paper.

I.2.4.2 Indeterminacy of Eve's blind deconvolution

Since $\mathbf{s}_1(n)$ is multi-variate Gaussian $\mathcal{N}_{J-K}(\boldsymbol{\mu}, \sum)$, from (I.22), for a given symbol vector $\mathbf{b}(n)$, the signal vector

$$\mathbf{s}_0(n) = -\mathbf{H}_0{}^{-1}\mathbf{H}_1\mathbf{s}_1(n) + \mathbf{H}_0{}^{-1}\mathbf{A}\mathbf{b}(n) \underline{\Delta}\mathbf{G}\mathbf{s}_1(n) + \mathbf{g} \tag{I.24}$$

is K -variate Gaussian $\mathcal{N}_K(\mathbf{G}\boldsymbol{\mu} + \mathbf{g}, \mathbf{G}\sum\mathbf{G}^H)$.

From (I.14) and (I.24), Eve's received signal becomes

$$\mathbf{x}_u(n) = \begin{bmatrix}\mathbf{H}_u\mathbf{F} & \mathbf{I}_M\end{bmatrix}\begin{bmatrix}\mathbf{s}_1(n)\\ \mathbf{v}_u(n)\end{bmatrix} + \mathbf{H}_u\mathbf{f}\,, \tag{I.25}$$

where

$$\mathbf{F} = \begin{bmatrix}\mathbf{G}\\ \mathbf{I}_{J-K}\end{bmatrix}, \quad \mathbf{f} = \begin{bmatrix}\mathbf{g}\\ \mathbf{0}\end{bmatrix}. \tag{I.26}$$

Obviously, for a given symbol vector $\mathbf{b}(n)$,

$$\begin{bmatrix} \mathbf{s}_1(n) \\ \mathbf{v}_u(n) \end{bmatrix} \sim \mathcal{N}_{M+J-K}\left(\begin{bmatrix} \boldsymbol{\mu} \\ \mathbf{0} \end{bmatrix}, \begin{bmatrix} \Sigma & \mathbf{0} \\ \mathbf{0} & {\sigma_v}^2 \mathbf{I}_M \end{bmatrix} \right). \tag{I.27}$$

Then Eve's signal is M-variate Gaussian distributed,

$$\mathbf{x}_e(n) \sim \mathcal{N}_M(\mathbf{H}_u \mathbf{F}\boldsymbol{\mu} + \mathbf{H}_u \mathbf{f}, \mathbf{H}_u \mathbf{F} \Sigma \mathbf{F}^H {\mathbf{H}_u}^H + {\sigma_v}^2 \mathbf{I}_M). \tag{I.28}$$

Since the distribution (I.28) depends on $\boldsymbol{\mu}$ and Σ, the unknown $\boldsymbol{\mu}$ and Σ contribute to the indeterminacy of $\mathbf{H}_u$.

Proposition 2. For an unknown symbol vector $\mathbf{b}(n)$ and unknown $\mathbf{H}$, $\boldsymbol{\mu}$ and Σ, from the distribution of $\mathbf{x}_u(n)$, the channel matrix $\mathbf{H}_u$ is indistinguishable from $\mathbf{H}_u\mathbf{P}$ with a $J \times J$ matrix

$$\mathbf{P} = \begin{bmatrix} \mathbf{U} & \mathbf{GV} - \mathbf{UG} \\ \mathbf{0} & \mathbf{V} \end{bmatrix}, \tag{I.29}$$

where $\mathbf{U}$ and $\mathbf{V}$ are arbitrary nonsingular $K \times K$ and $(J-K)\times(J-K)$ matrices, respectively.

Proof. See [16].

As a result, there is ambiguity of a $K \times K$ matrix $\mathbf{U}$ and a $(J-K)\times(J-K)$ matrix $\mathbf{V}$ for Eve's blind channel estimation. This ambiguity is also reflected in symbol vector estimation.

Proposition 3. Assume $\mathbf{x}_u(n)$ is generated by transmitting $\mathbf{b}(n)$. $\mathbf{x}_u(n)$ has identical distribution as those generated by transmitting any other symbol vector $\mathbf{d}(n)$.

Proof. See [16].

Note that the distribution defined above is due to the random $\mathbf{W}_1(n)$, conditioned on the symbol vector, i.e., $P\left[\mathbf{x}_u(n) \middle| \mathbf{b}(n)\right]$. When considering random sequences $\{\mathbf{b}(n)\}$ and $\{\mathbf{d}(n)\}$, we have $P\left[\{\mathbf{x}_u(n)\} \middle| \{\mathbf{b}(n)\}\right]$ because the symbol vectors are i.i.d.

The only way left for Eve is an exhaustive search of all possible channels $\mathbf{H}_u$. In fact, she just needs to guess a $K \times K$ complex detection matrix, which gives a complexity of q^{2K^2} with quantization level q. For example, the complexity of exhaustive search can be at least 2^{128} for $K = 4$ and $q = 16$ in order to obtain meaningfully low BER [13].

I.2.5. Simulations

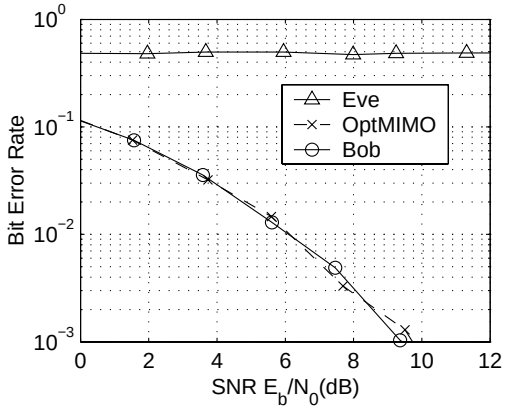

Figure 5. Receiving performance.
J = 6, K = 4. **○: Bob in the proposed scheme. ×:optimal MIMO eigen-beamforming. : Eve in the proposed scheme.**

In this section, we show the performance of the proposed transmission scheme in terms of bit-error-rate (BER) and secret channel capacity. For comparison purpose, we also evaluate the performance of the optimal eigen-beamforming (I.20). Eve is assumed to estimate symbols blindly, which is almost no different from guessing.

Alice transmits QPSK symbol packets. Each packet contains 400 QPSK symbols. $J = 6$ and $K = 4$ are used. We use 5000 runs to obtain each BER value. The BER results are shown in Fig. 5, from which we see that Bob can reliably receive signals while Eve can not.

Based on the BER of Bob and Eve, we can derive the secret channel capacity. For comparison purpose, we also plot the secret capacity when noise is considered as the only source of error. In this case, Eve is assumed to have the same BER as Bob. As can be seen from Fig. 6, the proposal scheme gives much higher secret capacity.

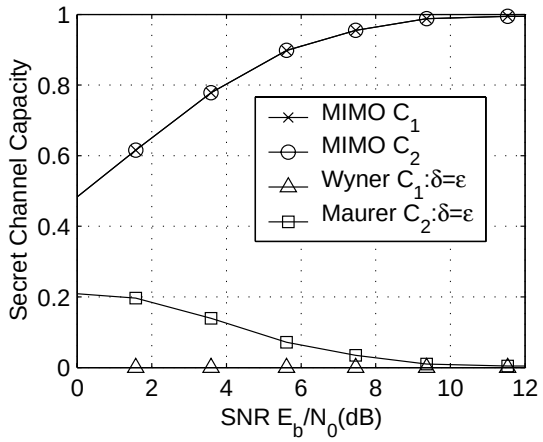

Figure 6. Secret channel capacity.
×, ○: proposed scheme. □, : traditional transmissions.

Part II. STBC-encoded Cooperative Transmissions

II.1. Introduction

Space-time coding and processing are powerful techniques for enhancing transmission efficiency of wireless networks. Among various widely investigated space-time techniques, space-time block codes (STBC) [7, 8] are especially promising because of their low computational complexity, i.e., maximum likelihood performance can be achieved with linear processing at the receivers. As a result, the Alamouti code [7], one of the simplest STBC exploiting two transmitting antennas, has already been adopted in the 3G WCDMA specification for transmission diversity. Since diversity enhances transmission energy efficiency in fading environment, STBC would be desirable for mobile users in wireless networks such as ad hoc and sensor networks where energy efficiency is a critical design criterion. However, traditional STBC require physical antenna arrays that are hardly available in small-sized mobile devices. This is why STBC were proposed for base stations from the beginning [8].

In order to take the benefits of STBC for distributed mobile networks, recently there have been great interests to investigate cooperative communications encoded by STBC. By exploiting the cooperation capability of multiple mobile users, STBC can still be used based on virtual instead of physical antenna array. Ideas of cooperative transmission have been proposed in cellular networks for cooperative diversity [9] and in sensor networks for energy efficiency and fault tolerance [12], where the employment of STBC takes the advantage of high bandwidth efficiency besides the targeted diversity benefits [10].

So far, most existing researches on cooperative transmission assume perfect synchronization among cooperative users, which means that the users' timing, carrier frequency and propagation delay are identical [9]. Under this assumption, there is in fact little diversity difference between cooperative STBC and traditional STBC except certain cooperation overhead. Unfortunately, it is difficult, and in most cases impossible, to achieve perfect synchronization among distributed transmitters. This is even more a reality when low-cost, small-sized transmitters are used, such as tiny sensors [11, 12, 15].

Without perfect synchronization, channels become dispersive even in flat fading environment. Due to the transmitting/receiving pulse shaping filters, if the sampling time instants are not ideal, intersymbol interference (ISI) is introduced. This certainly brings performance degradation or performance loss in cooperative STBC. More important, asynchronism among the transmitters may break the orthogonal STBC signal structure, which makes most of the existing STBC decoders fail instead of performance loss or complexity increase only. Therefore, for the cooperative STBC, one of the major challenges is the synchronization among the distributed nodes. In contrast to classical transmissions where synchronization refers to only that the receiver synchronizes to the transmitter, we have three synchronization issues here, i.e., synchronization among the transmitters, synchronization among the receivers, and synchronization of the receivers to the transmitters.

As far as STBC are concerned, the problem of synchronization among the transmitters is the most challenging one. It is in fact completely new to communications researches. Similar transmitters synchronization problem would happen in multi-access CDMA, but is fortunately avoided by the spreading and single-user detector, i.e., Rake receiver.

The synchronization requirement among the transmitters is different from that between the transmitter and the receiver. For the latter case, the receiver can perform the synchronization task using either pilot or blind methods, and the synchronization can be performed in the physical layer only. However, for the former one, usually hand-shaking has to be conducted among the transmitters, and thus both MAC and physical-layer should be involved. Therefore, the synchronization task becomes a cross-layer design problem.

We have recently addressed partially the problem of imperfect synchronization [11] by introducing a new transmission scheme different from the classical STBC-encoded transmissions, which uses a guard interval between two packets. An alternative method is using OFDM transmission, where certain asynchronism can be tolerated by increasing the cyclic prefix (guard interval) [23]. One of the major problems for these schemes is that the guard interval greatly reduced bandwidth efficiency, especially when the channels are time-varying so that the packet between the guard intervals can not be long. As a matter of fact, channel is very likely time-varying with asynchronous transmitters due to the different carrier frequency drifting and Doppler shifting among the transmitters. Strictly spreading, such techniques address the *imperfect synchronization* only instead of the complete *asynchronism* among the transmitters.

In this section, we consider the complete asynchronous transmitters with STBC-encoded transmissions. However, we consider only the asynchronism caused by different transmission time instants and propagation delays among them. In this case, equalization techniques can be developed to detect symbols from the received asynchronous signals. The advantage is that the traditional STBC-encoded transmission scheme can be directly used whether synchronization can be achieved or not. Because complete asynchronous transmissions are supported, synchronization and cooperation overhead can be much reduced. So does the symbol rate and carrier frequency synchronization. More important, by studying the performance of distributed STBC with a more practical consideration on asynchronism, we can justify the advantage of cooperative transmissions in distributed wireless networks.

II.2. System model

Consider an ad hoc wireless network where a source node needs to transmit a data packet to a destination node through multi-hop relaying as shown in Fig. 7. In each intermediate hop, the data packet is received by multiple nodes, e.g., nodes 1 to J in hop 1. Then these nodes can re-transmit it to the next hop in a cooperative manner with STBC encoding. Another scenario is that the source node may first transmit the packet to nearby relay nodes (with low transmission power), then they will transmit the packet cooperatively to the nodes in hop 1.

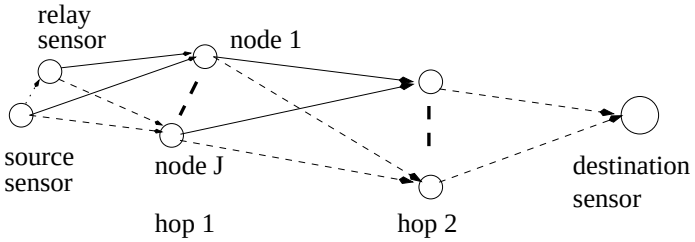

Figure 7. Multi-hop ad hoc network model wil cooperative transmissions.

Without loss of generality, we consider the cooperative transmission among nodes 1 to J in hop 1. Consider first the passband signal. The passband signal to be transmitted by each transmitter has a general form

$$\mathrm{Re}\left[\sum_{n=-\infty}^{\infty} s_i(n)\, p_b(t-nT)\, e^{j2\pi f_c t}\right], \tag{II.1}$$

where $s_i(n)$ is the complex signal transmitted within symbol interval $\left[nT, (n+1)T\right)$, $p_b(t)$ is the baseband pulse shaping filter, and f_c is the carrier frequency. After delaying with δ_i, the passband signal transmitted from the transmitter i, $1 \le i \le J$, is $\mathrm{Re}\left[\sum_{n=-\infty}^{\infty} s_i(n)\, p_b(t-nT-\delta_i)\, e^{j2\pi f_c (t-\delta_i)}\right]$.

We assume flat-fading propagation in this paper. The received passband signal at a receiver is

$$r_p(t) = \mathrm{Re}\left[\sum_{i=1}^{J} \alpha_i \sum_{n=-\infty}^{\infty} s_i(n)\, p_b(t-nT-\delta_i-\tau_i)\, e^{j2\pi f_c (t-\delta_i-\tau_i)} + v_p(t)\right], \tag{II.2}$$

where α_i and τ_i are (complex) gains and delays of the propagation. We can adjust δ_i to compensate τ_i for carrier phase synchronization. But in general, such synchronization is impossible, especially when the distributed cooperating transmitters have no perfect information on τ_i.

II.2.1. Signal models with asynchronous transmitters

Considering the asynchronous transmissions and assuming flat fading propagation, to simplify the problem, in this paper we consider only the asynchronism in transmission time and propagation delays, which means that δ_i and τ_i are different for different transmitters.

Without loss of generality, we can demodulate (II.2) by $e^{-j2\pi f_c t}$ to obtain the continuous-time complex baseband signal

$$r_b(t) = \sum_{i=1}^{J} \alpha_i e^{-j\theta_i} \sum_{n=-\infty}^{\infty} s_i(n)\, p_b(t - nT - \delta_i - \tau_i) + v_b(t)\,, \tag{II.3}$$

where $v_b(t)$ is the equivalent baseband noise, and the phase $\theta_i = 2\pi f_c(\delta_i + \tau_i)$.

If δ_i and τ_i are different among the transmitters, it is impossible to achieve timing synchronization. Then without loss of generality, we perform baseband sampling at time instant nT, which gives $x(n) \underline{\Delta} r_b(nT)$. The samples $x(n)$ can be written as (details in [19])

$$x(n) = \sum_{i=1}^{J} \begin{bmatrix} h_i^*(0) & \cdots & h_i^*(L) \end{bmatrix} \begin{bmatrix} s_i(n-d_i) \\ \vdots \\ s_i(n-d_i-L) \end{bmatrix} + v(n)\,, \tag{II.4}$$

where $v(n)$ is the noise sample, and the channel coefficients are

$$h_i^*(m) = \alpha_i e^{-j\theta_i}\, p_b(mT + d_i T - \delta_i - \tau_i), \quad d_i \geq 0, \quad 0 \leq m \leq L\,. \tag{II.5}$$

The baseband channel length L and coefficients $h_i^*(m)$ are determined by both fading and asynchronism.

On the other hand, the dispersive channel model in this case is different from that due to multipath propagations. One of the major differences is that we can make the channel of one of the transmitters to be single tap. Another difference is that the channel length can be deterministic, and can be rather small with certain approximation.

As a special case, it can be shown that it is approximately sufficient to consider only several channel taps [19], where the signals become

$$x(m) = \begin{bmatrix} h_1(0) & h_2(0) & h_2(1) \end{bmatrix} \begin{bmatrix} s_1(m) \\ s_2(m-d_2) \\ s_2(m-d_2-1) \end{bmatrix} + v(m)\,. \tag{II.6}$$

The feasibility of making such an approximation of considering only two-tap channel models can be demonstrated by the numerical evaluations using raised-cosine pulse-shaping filter. Note that (II.6) is simplified because $p(0) = 1$, and we consider only the un-modeled taps as residual ISI beyond channel model. Because of the dispersion of the channel of the second transmitter, there is heavy ISI. However, the ISI drastically reduces when the roll-off factor increases. The 2-tap channel model is a relatively good approximation when the roll-off factor is not too small.

II.3. Viterbi equalizer and linear prediction blind equalizer

Without loss of generality, assume that the first transmitter (Tx 1) advances the second one by d during transmission. The receiver can perform sampling with timing synchronized to that of Tx 2. Therefore, the signal model (II.6) becomes

$$x(m) = \begin{bmatrix} h_1(0) & \cdots & h_1(L) \end{bmatrix} \begin{bmatrix} s_1(m) \\ \vdots \\ s_1(m-L) \end{bmatrix} + h_2(0) s_2(m-d) + v(m)\,. \tag{II.7}$$

Define $\mathbf{h}_1 = \left[h_1(0), \cdots, h_1(L)\right]^T$.

First, consider the case with even delay difference $d = d_1 - d_2$. Without loss of generality, we let $d_1 = d$ and $d_2 = 0$. When the receiver knows the delays, it can perform sampling with respect to the one that falls behind. The received even numbered samples are

$$x(2n) = \mathbf{h}_1 \left[s_1(2n), \cdots, s_1(2n-L)\right]^T + h_2(0) s(2n-d+1) + v(2n)\,. \tag{II.8}$$

In general, we have the following rule to change $s_1(\cdot)$ into $s(\cdot)$ according to the STBC structure

$$s_1(m) = \begin{cases} s(m), & \text{for even} \quad m \\ -s^*(m), & \text{for odd} \quad m \end{cases} \tag{II.9}$$

In other words, the even numbered sample $x(2n)$ contains the symbols $\{s(2n-\max(L,d-1)),\cdots,s(2n-3),s(2n-2),s(2n-1),s(2n)\}$.

On the other hand, the received odd numbered samples are

$$x(2n+1)=\mathbf{h}_1\left[s_1(2n+1),\cdots,s_1(2n+1-L)\right]^T+h_2(0)s^*(2n-d)+v(2n+1), \quad \text{(II.10)}$$

which means that symbols $\{s(2n-\max(L-1,d)),\cdots,s(2n-2),s(2n-1),s(2n),s(2n+1)\}$ are contained in $x(2n+1)$.

II.3.1. Viterbi equalizer

It is well known that one of the major advantages of STBC is that computationally efficient maximum likelihood detection is available with flat fading propagation. However, in case of asynchronous transmissions, since the channels become dispersive, we have to use the Viterbi equalizer for the maximum likelihood performance.

Consider the received signal models developed in the above section, we find that the maximum number of symbols contained in a sample can be $L_s=\max\{L+1,d+2\}$. Therefore, with signaling alphabet size K, we need a trellis with K^{L_s-1} states. If each transmitter transmits N symbols, then we can perform $N+d$ rounds of trellis updating. Of course, when N is large, we usually use a truncated trellis for immediate symbol estimation in order to reduce complexity. Detail can be found in [19].

II.3.2. Linear prediction-based blind equalizer

It is interesting to consider the computationally more efficient linear equalization schemes for the STBC-encoded transmissions when the transmitters are not synchronized in time. Due to the suboptimal performance of the linear equalizers, we would like to verify the advantage of applying cooperative transmissions in this case. Flat-fading is assumed, but the channels can be dispersive due to timing mismatch. We have outlined the traditional MMSE equalizer and proposed a new linear-prediction based equalizer which exploits the special property of this transmission scheme. Interestingly, the linear prediction method is effectively a blind equalizer, but is immune from the severe limits of traditional linear prediction-based blind equalizers used in fractional-space equalization. Note that in our case, we consider single-input single-out system with only one receiver, and without over-sampling. Details can be found in [19].

II.4. Simulations

In this section, we use simulations to evaluate the proposed equalization algorithms. We compare the Viterbi equalizer with the classical STBC decoder when the latter works in perfect synchronization, which gives the optimal maximum likelihood performance with linear complexity. In addition, we compare this algorithm when it works with asynchronous transmissions. All these algorithms are compared with the case without diversity. They are labelled as, respectively, ``Asyn", ``SynSTBC", ``w/o Equ" and ``noDvst". This simulation tries to see how the new method compared with the optimal diversity case.

For the Viterbi equalizer experiments, the delay $d=1$, and a trellis with 128 states are used. 1000 randomly generated symbols are transmitted and detected during each run. Simulation results are shown in Fig. 8. The proposed Viterbi equalizer can achieve almost the optimal performance of the synchronous STBC. The slight performance gap may be due to the channel dispersion rather than the optimality of the detector. Both the two cases provide diversity advantage beyond the case transmissions without diversity. On the other hand, if no equalization is conducted, then the asynchronous transmission induced ISI brings severe symbol detection error.

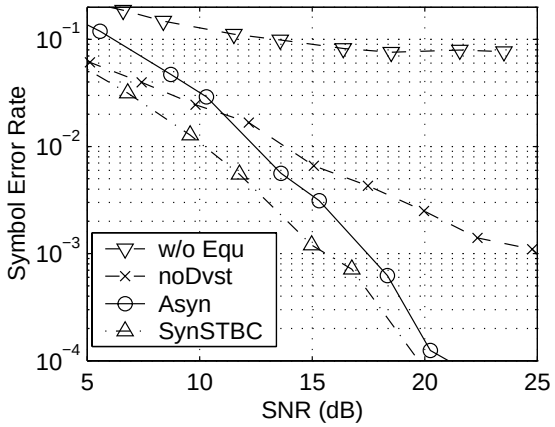

Figure 8. Symbol-error-rate (SER) as function of SNR.
(w/o Equ): using standard STBC receiver in asynchronous transmission. (noDvst): no diversity case with flat-fading single-tap channels. ○(Asyn): Viterbi equalizer proposed for STBC with asynchronous transmitters. (SynSTBC): standard STBC for synchronous STBC transmissions.

Part III. Testbed Development

III.1. Introduction

In this section, we describe the implementation of BPSK and QPSK transmissions using ComBlock modules. We have implemented two single-antenna transmission branches and two single-antenna receiving branches. However, due to time limit, we have only tested the single-antenna to single-antenna transmissions. More work is required to resolve the synchronization problem in order to implement cooperative transmission, which is under way though. The major work is the receiver programming which addresses especially the frequency synchronization problem. Some discussions for cooperative array transmission will be given at the end.

III.2. Testbed hardware

We use the communication modules from *ComBlock.com* to build our testbed. A single transmission branch (a single antenna) is built with the following components:

Com5001: LAN/IP network interface ($295)
Com8001: arbitrary waveform generator (256 MB), 40 Msamples/s ($345)
Com2001: Dual 10-bit D/A converter (baseband, 40Msamples) ($295)
Com4001: Dual-band 915MHz/2.4 GHz Quadrature modulator ($345)
Com4102: 2.4 GHz transceiver (25dBm power) ($295)
2.4 GHz antenna,
110V/4A power source.

A single receiving branch (a single antenna) is built with the following components:

Com4102: 2.4 GHz transceiver (25dBm power) ($295)
Com3001: Dual-band 915MHz/2.4GHz receiver ($345)
Com8002: High speed data acquisition (256MB, 40M samples/s) ($345)
Com5001: LAN/IP network interface ($295)
2.4 GHz antenna,
110V/4A power source.

The transmitter block diagram:

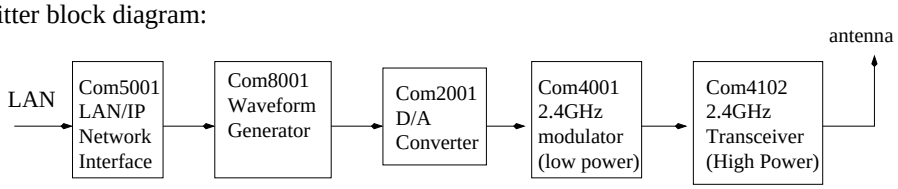

Figure 9. Transmitter block diagram.

The receiver block diagram:

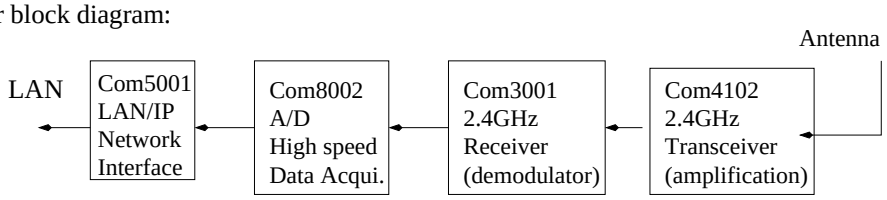

Figure 10. Receiver block diagram.

The photos of the transmitter and the receiver are shown below:

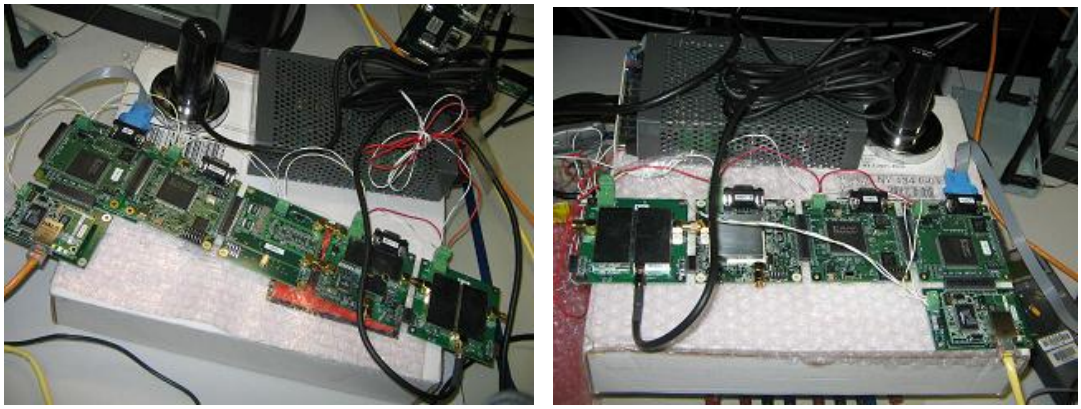

Figure 11. Prototype transmitter and receiver.

Both the transmitter and the receiver are connected to the LAN, and are assigned with a unique IP address. The IP address, gateway address must be written into the transmitter and receiver before they can be accessed via the LAN. Before LAN setting up, such parameters can be written into the modules via serial cable.

III.3. Preliminary results

BPSK and QPSK transmissions are implemented. Some channel estimation results have been obtained. Experiments are conducted in two or three places (only about 2 or 3 feet away), in each place several runs of the experiments are performed. Simulation data and preliminary results are available online at: *http://ucesp.ws.binghamton.edu/~xli/ComBlockSource.zip*.

From the preliminary results, we have found that channels appear effectively random and time-varying, which is required for the secure transmission scheme. The randomness is due to two major reasons: multipath fading, and residue carrier. Multipath fading contributes to both magnitude and phase of the channel response. Residue carrier contributes to channel time-variation. The difference of the residue carrier between the two transmitters will be a major issue for experimenting cooperative transmission array. But timing/clock does not seem a problem. It is accurately identical between the transmitter and the receiver during transmitting a sufficiently long packet. For array transmission, however, a problem is that it may not be possible to ask two transmitters to transmit at the same time. The ComBlock modules have relatively long delay during communication with the PC. We are working on resolving such problems.

Conclusions

This report summarizes the research results obtained during the Summer 2005 VFRP term. Physical-layer secure transmission techniques are proposed and proved. Cooperative communications are proposed as tools to realize wireless information assurance as well as to enhance the performance of wireless sensor networks. A testbed is in developing to demonstrate the proposed techniques.

References

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

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

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

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

[5] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE *Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, Mar. 1978.

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

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

[8] 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.

[9] 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.

[10] 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.

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

[12] X. Li, M. Chen and W. Liu, "Application of STBC-encoded cooperative transmissions in wireless sensor networks," *IEEE Signal Processing Lett*., Feb. 2005.

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

[14] X. Li, M. Chen and E. P. Ratazzi, "Array-transmission based physical-layer security techniques for wireless sensor networks," *IEEE ICMA'2005*, Niagara Falls, Ontario, Canada, July 2005.

[15] F. Ng, J.-H. Hwu, M. Chen and X. Li, "Asynchronous space-time cooperative communications in sensor and robotic networks," *IEEE ICMA'2005*, Niagara Falls, Ontario, Canada, July 2005.

[16] X. Li and E. P. Ratazzi, "MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks," to appear in *IEEE Military Communications Conference* (MILCOM'2005), Atlantic City, NJ, Oct. 17-20, 2005.

[17] X. Li, F. Ng, J.-H. Hwu and M. Chen, "Channel equalization for STBC-encoded cooperative transmissions with asynchronous transmitters," to appear in *Proceedings of the 39th Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, Oct. 30-Nov. 2, 2005.

[18] X. Li, J.-T. Hwu and E. P. Ratazzi, "Array redundancy and deliberate randomization for inherently secure wireless transmissions," submitted to IEEE Commun. Lett., 2005.

[19] X. Li, F. Ng and J.-T. Hwu, "Equalization of STBC-encoded transmissions with asynchronous transmitters," submitted to IEEE Trans. Signal Processing, 2005.

[20] C. H. Bennett and G. Brassard, IEEE *Int. Conf. Computers, Systems and Signal Processing*, Bangalore, India, pp. 175-179, 1984.

[21] H. Yuen, "KCQ: a new approach to quantum cryptography," *quant-ph/0311061*, 2004.

[22] E. Corndorf, G. Barbosa, C. Liang, H. P. Yuen and P. Kumar, "Quantum-noise randomized data encryption for WDM fiber-optic networks," *Optics. Letters*, vol. 28, pp. 2040-2042, 2003.