A Randomized Space-Time Transmission Scheme for Secret-Key Agreement

Xiaohua(Edward) Li[1], Mo Chen
Department of Electrical and Computer Engineering
State University of New York at Binghamton
Binghamton, NY 13902
e-mail:
{xli,mchen0}@binghamton.edu

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

Abstract —

In contrast to the pessimistic view on perfect secrecy, studies on information-theoretic secrecy have shown that perfect secrecy may be possible in practice. A typical example is the Wyner's wire-tap channel concept. However, existing approaches mostly depend on unrealistic noise or error-rate assumptions. We propose a more practical way in this paper which uses advanced space-time transmissions for enhanced information-theoretical secrecy. Based on the fundamental limits of MIMO blind channel identification, space-time transmissions with proper randomization can effectively prevent the adversary from channel estimation while allowing reliable transmission between the authorized parties. The high error rate suffered by the adversary enhances secret channel capacity. This paper points out a new and practical approach for secret-key agreement which achieves perfect secrecy based on the physical-layer signal processing techniques.

I. Introduction

Secret-key agreement denotes the procedure for two parties to achieve agreement on some encryption keys which are secret in a certain level to any adversary. With cryptography terminology, the problem is usually described as that Alice sends messages to Bob who will extract a secret key from the messages, during which the adversary Eve who has access to the channel between Alice and Bob can not obtain sufficient information about the key.

The Shannon secrecy model [1] is usually the basis for encryption techniques and secret-key agreement protocols, where Eve is assumed to have full access to the channel, i.e., she has identical received messages as Bob. Under such a model, perfect secrecy becomes an impractical concept, whereas keys can be generated based on some intractable computational problems such as factorizing integers in a feasible time. However, such intractability assumption is unproved, so does the secrecy [2]. New computing power, especially the future quantum computer, has been shown to challenge such intractability assumption. As an example, [3] suggests that the complexity of factorizing integers can be only polynomial with quantum computer models.

[1]This work was supported by US AFRL under Grant FA8750-04-1-0213.

As a result, there have been great interests to find ways for realizing perfect secrecy, which on the one hand is an interesting problem with great impact on cryptography, on the other hand is important to guarantee security in practice for the future. Researches on practical perfect secrecy are mostly based on the fact that the Shannon secrecy model is in many cases too strong. In contrast, Eve and Bob may have different received signals.

Under this new viewpoint, one of the most successful ways is quantum key distribution (QKD), which has obtained rapid progress recently after decades of investigation [4]. The downside of QKD might be that currently it still requires dedicated laser links, and it is unknown how QKD can be used conveniently in ordinary multi-hop networks, especially wireless networks.

For wireless networks, more promising ways may lie in the various studies on information-theoretic secrecy [5]-[8], which show that perfect secrecy (or unconditional secrecy, or information-theoretical secrecy) may be realizable in practice under some special circumstances. Their common idea is that in many practical communication systems, especially wireless systems, Eve's channels or signals are not exactly the same as Bob's, e.g., their receiving noise and thus their bit-error-rate (BER) are different.

With the wire-tap channel concept [5], if the channel from Alice to Bob and the channel from Alice to Eve have different BER $\epsilon \leq 0.5$ and $\delta \leq 0.5$, respectively, then the secret channel capacity from Alice to Bob can be [8]

$$C_1 = \begin{cases} h(\delta) - h(\epsilon), & \text{if } \delta > \epsilon \\ 0, & \text{else} \end{cases} \quad (1)$$

where $h(\epsilon)$ denotes the binary entropy function defined by $h(\epsilon) = -\epsilon \log_2 \epsilon - (1-\epsilon)\log_2(1-\epsilon)$. Obviously, it requires that Eve's channel be noisier than Bob's in order to achieve any positive capacity if only noise is considered as the factor of receiving error. Such a requirement in most cases does not seem practical, unfortunately.

It has been shown [6] that the above noise requirement can be relaxed to a level that Eve suffers from a known (and large enough) error floor only. In this case, as long as the two channels are different, then perfect secrecy is achievable with positive secret channel capacity even if Eve's channel is better than Bob's. To realize this objective, Bob and Alice have to exchange information over another public and insecure channel, e.g., they can inform each other the indices of the data bits that they have received reliably. Specifically, the

secret channel capacity is [6]

$$C_2 = h(\epsilon + \delta - 2\epsilon\delta) - h(\epsilon), \tag{2}$$

which means that perfect secrecy can be achieved in practice with positive capacity unless $\epsilon = 0.5$ (i.e., Bob does not receive reliably) or $\delta = 0, 1$ (i.e., Eve can reliably receive signals).

Obviously, (2) is better than (1) for a wide range of ϵ and δ. Unfortunately, if only noise is considered as the source of receiving error as did in the existing literature, then Eve's error rate δ can be much less than Bob's. If $\delta \ll \epsilon$, the capacity specified by (2) becomes too small to be useful. Therefore, the problem remains to find valid ways to realize perfect secrecy in practice, or more specifically, to guarantee a high enough δ.

In this paper, we show that, instead of considering noise only, attacking the problem within the physical-layer signal processing framework provides new approaches. In particular, Bob and Eve's difference on channels can be exploited. One possible way is in the multiple-input multiple-output (MIMO) systems, where space-time transmissions can be exploited to deprive Eve's blind identification capability. It is widely known that there are certain indeterminacy for the blind identification of MIMO channels, and successful blind identification is possible only for some very limited special cases. Without the knowledge of her own channels, Eve can not estimate the received signals successfully, which gives us the required high error rate δ.

Therefore, we develop a randomized space-time transmission scheme which exploits the redundancy of array transmissions to create impossible blind identification problems for Eve. This is in contrast to traditional space-time researches that focus on exploiting such redundancy for bandwidth efficiency and power efficiency.

This paper is organized as follows. In Section II, a framework of space-time transmission for secret-key agreement is described. In Section III, we develop the new space-time transmission scheme. Then, the performance of the new scheme is analyzed in Section IV in terms of the trade-off between transmission power and secrecy. Simulations are given in Section V and conclusions are presented in Section VI.

II. System description

We consider a wireless network where mobile users communicate with a base-station, as illustrated in Fig. 1. The objective is for the base-station to send secret messages to a mobile user from which the latter can obtain a secret key. During this procedure, other users, although can listen to the transmission with their own receivers, should obtain little information about the key. We therefore name the base-station as Alice, the desired mobile user as Bob, and all other users as Eve.

We assume that Alice has sufficient number of antennas so that some of them can be used for secret transmission, whereas the others can be used for general purpose unsecured transmissions. As a result, there are two channels between Alice and Bob. One is the secure channel, which is uni-directional from Alice to Bob. The other is bi-directional and insecure, which is a public channel between Alice and Bob so that they can exchange information during secret-key agreement [6] or conduct normal encrypted data transmission after secret-key agreement. Note that Eve can have perfect knowledge about the messages on the public channel, and can listen to the transmissions in the secure channel as shown in Fig. 1.

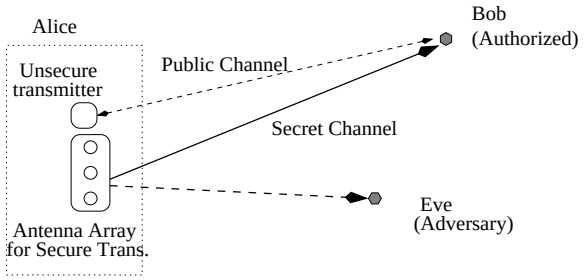
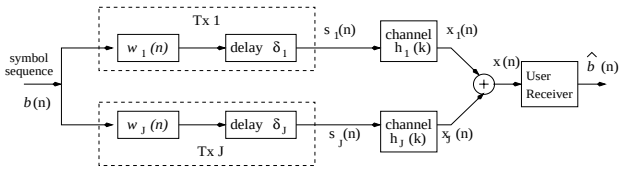


Figure 1: System model for secret-key agreement with space-time transmissions.



(b)

Figure 2: The block diagram of space-time transmission.

Let Alice have J antennas for secret transmissions, which can be realized by either physical antenna array or cooperative transmitters. We define them as J transmitters. Packets transmitted by these J transmitters are targeted for Bob only while Eve should be deprived of signal interception capability.

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

If the propagation channel is Rayleigh flat fading, and all the J transmitters are synchronized, the received signal at Bob is

$$x(n) = \sum_{i=1}^{J} h_i^* s_i(n) + v(n) \triangleq \mathbf{h}^H \mathbf{s}(n) + v(n), \tag{3}$$

where $v(n)$ denotes AWGN with zero-mean and variance σ_v^2, channel coefficients h_i^* are independent complex circular symmetric Gaussian distributed with zero-mean and unit variance. The vectors are defined as $\mathbf{h} \triangleq [h_1, \cdots, h_J]^T$ and

$$\mathbf{s}(n) \triangleq \begin{bmatrix} s_1(n) \\ \vdots \\ s_J(n) \end{bmatrix} = \begin{bmatrix} w_1(n) \\ \vdots \\ w_J(n) \end{bmatrix} b(n) \triangleq \mathbf{w}(n) b(n). \tag{4}$$

In this paper, $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ denote conjugation, transposition and Hermitian, respectively.

Since channel estimation is required, we assume that $\mathbf{h}$ is block fading [9], i.e., it is constant or slowly time-varying when transmitting a block of symbols but may change randomly between blocks. The symbols $b(n)$ are independent uniformly distributed with zero-mean and unit variance.

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

$$\begin{bmatrix} x_{u,1}(n) \\ \vdots \\ x_{u,M}(n) \end{bmatrix} = \begin{bmatrix} h_{u,1,1}(0) & \cdots & h_{u,1,J}(0) \\ \vdots & & \vdots \\ h_{u,M,1}(0) & \cdots & h_{u,M,J}(0) \end{bmatrix} \times \begin{bmatrix} w_1(n-d_{u,1})b(n-d_{u,1}) \\ \vdots \\ w_J(n-d_{u_J})b(n-d_{u,J}) \end{bmatrix} + \begin{bmatrix} v_{u,1}(n) \\ \vdots \\ v_{u,M}(n) \end{bmatrix}. \quad (5)$$

The notations are similar to (3) except that $(\cdot)_u$ is used to denote the unauthorized user Eve. The delays $d_{u,i}$ may not be zero because the transmitters adjust δ_i in favor of Bob. While introducing such delays is an important way for enhancing secrecy, in this paper we assume zero delays for simplicity, i.e., $d_{u,i} = 0$ for all i . The equation (5) can then be written as

$$\mathbf{x}_u(n) = \mathbf{H}_u\mathbf{w}(n)b(n) + \mathbf{v}_u(n). \quad (6)$$

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

In this paper, we focus only on the secrecy of the downlink transmission (from the base-station to the mobile user). Once the downlink is secured, the uplink can be easily secured. In addition, we consider passive adversary only, i.e., Eve can only passively listen to the transmissions rather than actively altering/retransmitting the packets.

We assume that Eve can not receive identical signal as Bob from the secret channel, i.e., $x(n)$ and $\mathbf{x}_u(n)$ are different. This assumption is necessary for our scheme, and is equivalent to the assumptions made in the existing information-theoretic secrecy models. In our scheme, such a difference is mainly due to the fact that the channels $\mathbf{h}$ and $\mathbf{H}_u$ are neither identical, nor highly correlated. Extensive studies on MIMO channels show that as long as the distance between Bob and Eve is larger than some wavelengths, their channels can be considered as fading independently. Therefore, we exploit the channel difference rather than the noise difference to achieve information-theoretic secrecy.

III. Randomized space-time transmissions

Though Eve does not know her channel $\mathbf{H}_u$, she may try to estimate them by either training or blind methods, or by a brute-force search of all possible channels. Interestingly, it does not matter whether Eve knows the channel $\mathbf{h}$ or not, which is one of the differences between the proposed method and those using channels directly as encryption keys. In contrast, Alice and Bob do not know both channels $\mathbf{h}$ and $\mathbf{H}_u$ either, and in particular, have no ways to estimate $\mathbf{H}_u$. Ways have to be designed for them to estimate $\mathbf{h}$ so that special transmission/receiving schemes can be designed, during which no ways should be provided to Eve for successful interception.

III.A Transmission and receiving procedure

We first give the transmission and receiving procedure from Alice to Bob with the consideration of the signal model (3)-(4). According to the received signal

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

the transmitters need to use special transmitting weights $\mathbf{w}(n)$ to fulfill the secrecy objective. Our basic idea is to make $\mathbf{h}^H\mathbf{w}(n)$ deterministic but $\mathbf{H}_u\mathbf{w}(n)$ changing randomly in each symbol interval. For this purpose, $\mathbf{w}(n)$ should be random since the transmitters do not know $\mathbf{H}_u$. In addition, ways have to be designed so that either the transmitters or the receiver can estimate the channel. Piloting methods should be avoided because we depend on that fact the Eve can not estimate the channel $\mathbf{H}_u$. As far as blind channel estimation is concerned, Bob has not priority over Eve. Therefore, it is better to let transmitters (Alice) to estimate the channel $\mathbf{h}$.

We first give the transmission and receiving procedure assuming that Alice knows the channel $\mathbf{h}$, and then provide ways for Alice to estimate the channel. Alice can design the transmitting weights vector $\mathbf{w}(n)$ such that

$$\mathbf{h}^H\mathbf{w}(n) = \|\mathbf{h}\|, \quad (8)$$

where $\|\mathbf{h}\| = \sqrt{\sum_{i=1}^{J}|h_i|^2}$. Although (8) looks similar to transmit beamforming [10], the major difference is that $\mathbf{w}(n)$ changes randomly after each symbol $b(n)$ is transmitted. This can be realized by selecting randomly the elements of $\mathbf{w}(n)$ while satisfying the constraint (8). Obviously, if the channel $\mathbf{h}$ is constant or slowly time-varying, we need $J \geq 2$ transmitters for randomization purpose. This explains why array transmission is required.

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

$$\hat{b}(n) = \|\mathbf{h}\|^{-1}x(n), \quad (9)$$

where $\|\mathbf{h}\|^2$ can be estimated as $\frac{1}{N}\sum_{n=1}^{N}|x(n)|^2$.

To implement this transmission scheme, the channel $\mathbf{h}$ has to be known to the transmitters instead of the receiver. Therefore, it is not necessary to transmit training sequences to Bob for channel estimation, which enhances secrecy because Eve has no training available either.

There are at least two ways for the transmitters to estimate the channel $\mathbf{h}$. First, if the downlink and uplink channels are reciprocal, the transmitters can estimate $\mathbf{h}$ directly from the uplink received signals. This is the case in fast time-division-duplexing (TDD) transmissions [10]. Since we consider the downlink secrecy only, Bob can transmit either training or secret sequences to Alice for the latter to estimate the channel.

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

Finally, in order for the receiver to achieve synchronization in time and frequency, some pilot tones or signals can be transmitted by a special pilot transmitting antenna, which are not within, but synchronized with the antennas for secret transmissions.

III.B Transmitting weights design

The transmitting weights vector $\mathbf{w}(n)$ has to be chosen appropriately in order to satisfy (8) while preventing Eve from detecting $b(n)$ based on (6). In addition, we need to limit the total transmission power as well as the transmission power of each single transmitter.

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

More generally, $\mathbf{w}(n)$ can be obtained from the singular value decomposition (SVD) of $\mathbf{h}$, i.e., $\mathbf{h}^H = \mathbf{U}\mathbf{D}\mathbf{V}^H$. In this special case, $\mathbf{U} = 1$, $\mathbf{D} = \mathrm{diag}\{\|\mathbf{h}\|, 0, \cdots, 0\}$, and $\mathbf{V}$ is a $J \times J$ unitary matrix whose first column equals $\mathbf{h}/\|\mathbf{h}\|$. For transmit beamforming, $\mathbf{w}(n)$ can be calculated as $\mathbf{w}(n) = \mathbf{V}[1, z_2(n), \cdots, z_J(n)]^T \triangleq \mathbf{V}[1,\ \mathbf{z}_1^T(n)]^T$, where $z_j(n)$, $j = 2, \cdots, J$, can be arbitrary. Such a classic approach does not have any secrecy even if $\mathbf{w}(n)$ is randomized by choosing randomly $\mathbf{z}_1(n)$. For example, CMA may be used to estimate symbols from

$$\mathbf{x}_u(n) \quad = \quad \mathbf{H}_u\mathbf{V}\left[\begin{array}{c} 1 \\ \mathbf{z}_1(n) \end{array}\right] b(n) + \mathbf{v}_u(n). \qquad (10)$$

Therefore, there is a tradeoff of transmission power for secrecy. In order to guarantee secrecy, we may not achieve the optimal unit transmission power. This can be further demonstrated by the following observations. For $J = 2$, if we guarantee unit transmission power, then there is no degree of freedom in $\mathbf{w}(n)$ left for randomization. In addition, if we solve (8) by first choosing randomly $w_i(n)$, $3 \le i \le J$, and then looking for $w_1(n)$ and $w_2(n)$ for both (8) and unit power, it turns out that there may not have solutions. This means that unit transmission power is not always possible at least for $J = 3$.

Based on such observations, we design transmitting weights which trade transmission power for secrecy. We first select randomly an h_i from $\mathbf{h}$. Note that h_i should be sufficiently large in order to avoid numerical problem when calculating h_i^{-1} and in order to realize certain constraints on transmission power. We can select a threshold α and choose those h_i which satisfy $|h_i|^2 > \alpha$.

Then we choose randomly $w_j(n)$, where $1 \le j \le J$ and $j \ne i$. The flexibility of choosing $w_j(n)$ is the key point for realizing transmission secrecy. By choosing $w_j(n)$ properly, we can prevent the blind equalization conducted by Eve, while Bob does not depend on channel knowledge for symbol estimation. For example, we can draw them from some i.i.d. complex Gaussian random process, which will be described more in Section IV-B.

Denote $\mathbf{z}_i(n) = [w_1(n), \cdots, w_{i-1}(n), w_{i+1}(n), \cdots, w_J(n)]^T$ and $\mathbf{h}_i = [h_1, \cdots, h_{i-1}, h_{i+1}, \cdots, h_J]^T$. The weights vector is calculated as

$$\mathbf{w}(n) = \mathbf{P}_i\left[\begin{array}{c} \frac{\|\mathbf{h}\| - \mathbf{h}_i^H\mathbf{z}_i(n)}{h_i^*} \\ \mathbf{z}_i(n) \end{array}\right]. \qquad (11)$$

The matrix $\mathbf{P}_i$ is a $J \times J$ commutation matrix whose function is to insert the first row of the following vector into the ith row. Since h_i is chosen randomly, $\mathbf{P}_i$ is also random.

The complexity of this transmission procedure is linear. Note that efficient computation is important because $\mathbf{w}(n)$ are recalculated in each symbol interval. On the other hand, the power efficiency may not be optimized, even under the consideration of the tradeoff with secrecy.

IV. Transmission power and secrecy

IV.A Transmission power

Although we do not explicitly apply any power constraints on $\mathbf{w}(n)$, the transmission power can be statistically controlled by adjusting the mean and variance of the random variables $w_j(n)$, $j \ne i$.

Let us first consider the case that the mean and variance are $\mu = 0$ and σ^2, respectively. Then the total transmission power is

$$\begin{aligned} P_{t,h_i} &= E[\mathbf{w}^H(n)\mathbf{w}(n)|\mathbf{h}, \mathbf{P}_i] \\ &= (J-1)\sigma^2 + \frac{\|\mathbf{h}\|^2}{|h_i|^2} + \frac{\|\mathbf{h}_i\|^2\sigma^2}{|h_i|^2} \end{aligned} \qquad (12)$$

for a given channel realization $\mathbf{h}$ and a given choice of h_i. We have (12) because the item $w_i(n)$ in (11) has mean $\|\mathbf{h}\|/h_i^*$ and variance $\|\mathbf{h}_i\|^2\sigma^2/|h_i|^2$.

Equation (12) shows that small h_i increases the total transmission power, so the threshold α should be carefully selected. Since h_i is a complex Gaussian random variable with zero mean and unit variance, $|h_i|^2$ is exponentially distributed with unit mean. The probability for the selected channel coefficient h_i to have energy $|h_i|^2$ greater than α is

$$P[|h_i|^2 > \alpha] = \int_\alpha^\infty e^{-t}dt = e^{-\alpha}. \qquad (13)$$

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

Proposition 1. With Rayleigh fading channels, if the coefficients are selected with energy threshold α (13), then the expected total transmission power is

$$P_t = (J-1)\sigma^2 + 1 + (J-1)(1+\sigma^2)\Gamma(0, \alpha). \qquad (14)$$

Proof. If channels are random, then the ensemble average of the power (12) becomes

$$P_t = E[P_{t,h_i}] = (J-1)\sigma^2 + 1 + E\left[\frac{\|\mathbf{h}_i\|^2}{|h_i|^2}\right](1+\sigma^2). \qquad (15)$$

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

$$P_t = (J-1)\sigma^2 + 1 + (J-1)(1+\sigma^2)E[\frac{1}{|h_i|^2}]. \qquad (16)$$

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

$$E[\frac{1}{|h_i|^2}] = \int_\alpha^\infty \frac{1}{|h_i|^2}e^{-|h_i|^2}d|h_i|^2 = \Gamma(0, \alpha). \qquad (17)$$

Hence (14) is obtained. □

For transmission secrecy, what is more important is the ratio of the transmission power between different transmitters. Transmission power should be almost identical among the transmitters because otherwise Eve may utilize power-spectral information for blind channel estimation. Such an

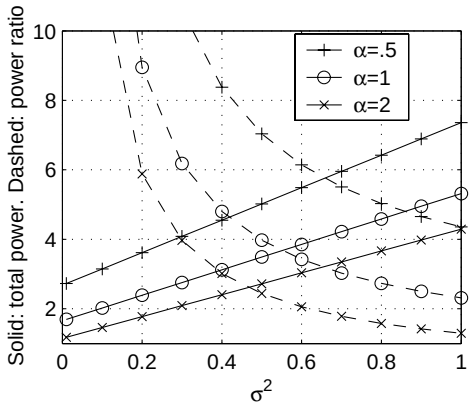


Figure 3: Total transmission power P_t and power ratio $P_{t,i}/P_{t,j}$ of the ith transmitter to the jth transmitter ($j \neq i$) when h_i is selected in (11). $J = 4$. Solid lines: total power. Dashed lines: power ratio.

objective is fulfilled by both the random matrix $\mathbf{P}_i$ and by choosing parameters μ and σ properly. Especially, if the channel $\mathbf{h}$ is slowly time-varying or even constant for a long time, we need to avoid the case that the power of one of the transmitters is exceptionally larger than the others. Otherwise the array transmission behaves as that with a single transmitter, and secrecy can be compromised. This becomes true even if the random matrix $\mathbf{P}_i$ is considered.

Therefore, we have to constrain the ratio of the transmission power of the ith transmitter $P_{t,i} = (\|\mathbf{h}\|^2 + \|\mathbf{h}_i\|^2\sigma^2)/|h_i|^2$ to that of the jth transmitter $P_{t,j} = \sigma^2$. The power ratio can be obtained from (14) as

$$\frac{P_{t,i}}{P_{t,j}} = \frac{1 + (J-1)(1+\sigma^2)\Gamma(0,\alpha)}{\sigma^2}. \tag{18}$$

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 the transmitter with 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 $\mathbf{P}_i$ is reduced.

Fig. 3 illustrates the dependence of the total transmission power or power ratio on the parameters. The total power P_t increases when σ^2 increases or α decreases, whereas 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 (13), it reduces the number of selectable h_i as well as the randomness of $\mathbf{P}_i$. Hence there is also a trade-off when choosing α. We have used $\alpha = 0.5$ in simulations.

IV.B Transmission secrecy

Eve knows only her received signal $\mathbf{x}_u(n)$ as represented by (6), and may also know that Alice and Bob depends on $\mathbf{h}$ for secret transmission, i.e., (8). One of the ways for her is to estimate $\mathbf{H}_u$ and apply $\mathbf{H}_u^{-1}$ to obtain $\mathbf{w}(n)b(n)$. If this is successful, then some information may be leaking if $\mathbf{w}(n)$ is not properly designed. Therefore, the important thing is to make Eve unable to estimate $\mathbf{H}_u$.

We have removed explicit training so that Eve has no training available for channel estimation. If the channels are reciprocal, then the transmitters can estimate channel $\mathbf{h}$ from the uplink signal transmitted by Bob, without leaking channel information to Eve. Otherwise, the transmitters depend on feedback from Bob for channel estimation. However, if raw data are fed-back and are not secure, whether they are $y(n) = \mathbf{h}^H\mathbf{w}(n)$ or raw received samples, the secrecy of the downlink transmission can be lost. For example, if Eve has intercepted the feedback data $y(n)$, $n = 1, \cdots, J$, then together with its own estimations $y_u(n) = \mathbf{H}_u\mathbf{w}(n)$, $n = 1, \cdots, J$, it can derive a vector $\mathbf{h}^H\mathbf{H}_u^{-1}$. By this vector, it can intercept symbols $b(n)$ from $\mathbf{x}_u(n)$.

Therefore, before using feedback, a secure initialization method has to be adopted to secure the first transmission for the subsequent feedback to become secure. We may exploit the reciprocal channel property to realize this objective. For example, Bob can first send a training sequence to Alice using the downlink frequency. After Alice estimates the channel, secure downlink transmission is setup. Feedback methods can then be used for channel estimation during which the feedback data can be secured via instantly exchanged keys.

Without training, Eve may turn to blind identification. In this case, the flexibility of choosing randomizing parameters helps us successfully fulfill this objective. It has been shown that for MIMO blind equalization, if the input signal vector $\mathbf{s}(n)$ is Gaussian distributed with some correlations, then there is at least a constant matrix indeterminacy. On the other hand, all the existing blind techniques require some *a priori* knowledge on the statistics of the input sequence, such as independence [11], non-Gaussian distribution [12], distinct power spectral [13], etc. From (11), we can choose $w_i(n)$ properly to violate such assumptions. For example, we can choose $w_j(n)$ such that $w_j(n)b(n)$ is Gaussian distributed with some mean μ and variance σ^2. Then $\mathbf{w}(n)$ is instantaneously jointly Gaussian distributed with some correlations. The correlations can be unknown because Eve does not know μ, σ^2, as well as channel coefficients. By using random μ and σ^2 and keeping them time-varying, the source does not have even a sufficiently constant distribution from Eve's view point.

For example, Gaussian source is completely specified by moments up to second order. For the second-order moments, Eve may obtain $\mathbf{R}_u = \mathbf{H}_u E[\mathbf{w}(n)b(n)b^*(n)\mathbf{w}^H(n)]\mathbf{H}_u^H = \mathbf{H}_u\mathbf{R}_s\mathbf{H}_u^H$. There exist some $J \times J$ unitary matrices $\mathbf{Q}$ such that $\mathbf{R}_u = \mathbf{H}_u\mathbf{Q}^H\mathbf{R}_s\mathbf{Q}\mathbf{H}_u^H$ as long as $\mathbf{Q}^H\mathbf{R}_s\mathbf{Q} = \mathbf{R}_s$. Since she does not know $\mathbf{R}_s$, there is no extra information on $\mathbf{Q}$. Moreover, the unknown $\mathbf{R}_s$ makes the ambiguity matrix arbitrary, not only unitary.

If the blind equalization is not applicable, the last way left for Eve is to try a brute-force search of all possible channels $\mathbf{H}_u$ (or, strictly speaking, $\mathbf{Q}$). Note that in this case, it does not matter whether Eve knows $\mathbf{h}$ or not. This is then the idea of information-theoretic secrecy, which means that Eve does not obtain more information from her received signals than simply guessing the channels without even looking at the signal. Hence, perfect secrecy is claimed.

Nevertheless, we may still be interested to see the complexity of Eve's exhaustive search. Let us assume that she use K-level quantization for each single value (a complex number has two such values). Then the brute-force search needs

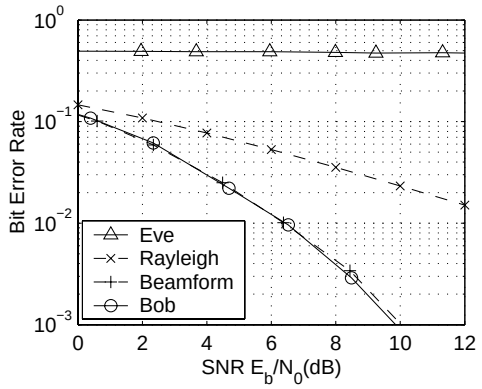


Figure 4: Receiving performance comparison. ∘:proposed method with $J = 4$. +:transmit beamforming with $J = 4$. ×:theoretical BER curve with Rayleigh fading channel (no diversity). △:blind detector of Eve.

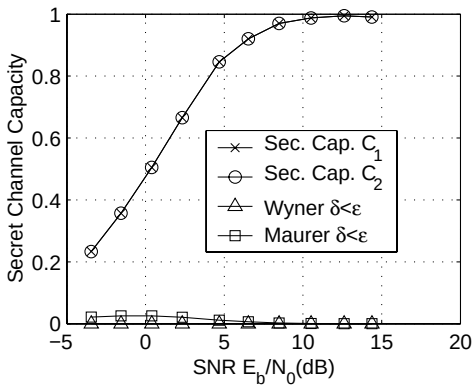


Figure 5: Secret channel capacity. ∘,×:proposed method. △,□:traditional method when Eve's BER can be lower.

to consider at least $K^{(2J)^2}$ possible combinations of $\mathbf{H}_u$ and K^{2J} possible combinations of $\mathbf{h}$. This gives an overall complexity $K^{2J(2J+1)}$. Such a complexity can in fact be much more amplified by the fact that Alice chooses randomly $\mathbf{w}(n)$ and may also adjust channels as well as (8).

With $J = 4$ and QPSK transmission, in order to achieve bit-error-rate (BER) under 0.1, by simulations we find $K \geq 4$ even in the noiseless case. When $K = 4$, the complexity becomes $4^{2\times4\times(2\times4+1)} = 2^{144}$. If considering a more realistic BER of 0.01 at signal-to-noise-ratio (SNR) 25 dB per receiving antenna, then K should be at least 128, which gives a complexity over 2^{644}. Considering that Bob's error rate is much lower than the above figures, based on either (1) or (2), we can obtain sufficiently large secret channel capacity.

V. Simulations

In this section, we show the performance of the proposed method in terms of BER and secret channel capacity. We compare the BER of Bob and Eve, which will then be used to calculate the secret channel capacity using (1) and (2). For comparison purpose, we evaluate the performance of the optimal transmit beamforming and give the theoretical BER curve of the Rayleigh fading channel without diversity. Channels are assumed block Rayleigh fading. Each packet contains 200 QPSK symbols. We use 5000 runs to obtain each BER value. We use $\alpha = 0.5$, $\sigma^2 = 0.5$.

The BER results are shown in Fig. 4. Transmissions with the proposed method have similar BER 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. Note that the proposed method uses more transmission power than beamforming. Eve can not intercept symbols.

With the obtained BER of Eve and Bob as δ and ϵ, respectively, the secret channel capacity is calculated and shown in Fig. 5, where both (1) and (2) are evaluated. For comparison purpose, we have also shown the corresponding capacity when $\delta = \epsilon/10$. As can be seen, the proposed method achieves sufficiently superior secret channel capacity in all SNR ranges.

VI. Conclusions

This paper proposes a new method for realizing perfect secrecy for secret-key agreement. With space-time transmissions and based on the limit of blind MIMO channel estimation, a randomization procedure is proposed to prevent Eve from channel estimation while permitting Bob receiving signals successfully. This induces a much higher receiving error rate for Eve so that traditional information-theoretic secrecy can be realized in practice. The trade-off between transmission power and secrecy is studied.

References

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

[2] U. M. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels – Part I: definitions and a completeness result", *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 822-831, April 2003.

[3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, 26:1484-1509, 1997.

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," *J. of Cryptology*, vol. 5, no. 1, pp. 3-28, 1992

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

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

[7] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography — Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121-1132, July 1993.

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

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

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

[11] P. Common, "Independent component analysis, A new concept?" *Signal Processing*, vol. 36, pp. 287-314, Apr. 1994.

[12] J.-F. Cardoso, "Blind signal separation: statistical principles," *Proc. IEEE*, vol. 86, no. 10, pp. 2009-2025, Oct. 1998.

[13] Y. Hua, S. An and Y. Xiang, "Blind identification of FIR MIMO channels by decorrelating subchannels," *IEEE Trans. Signal Processing*, vol. 51, no. 5, pp. 1143-1155, May 2003.