SPACE-TIME TRANSMISSIONS FOR WIRELESS SECRET-KEY AGREEMENT WITH INFORMATION-THEORETIC SECRECY

Xiaohua(Edward) Li [*], *Mo Chen*

Department of Electrical and Computer Engineering
State University of New York at Binghamton
Binghamton, NY 13902
{xli,mchen0}@binghamton.edu

E. Paul Ratazzi

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

ABSTRACT

An important building block of the cross-layer network security design is the physical-layer security which addresses problems such as whether the physical-layer can have build-in security and whether physical-layer techniques can assist the upper-layer encryption-based security techniques. This paper provides a positive answer by realizing information-theoretic secrecy with space-time transmissions. While most existing results on information-theoretic secrecy rely on some impractical assumptions, we propose a more practical approach that uses the redundancy of space-time transmissions to create intentional ambiguity to the adversary. Secrecy can be guaranteed even if the adversary has extremely high receiving signal-to-noise ratio. This approach is presented as a new way for secret-key agreement. Simulations in terms of receiving error rate and secret channel capacity are presented.

1. INTRODUCTION

In terms of security, wireless transmissions are lack of physical boundary since any adversary can receive the signal within the range. This may cause a weak physical-layer security, and may potentially weaken the end-to-end network security. Innovative cross-layer security design, where the physical-layer security techniques and the upper-layer security techniques are jointly designed, is desirable for wireless networks. While traditional encryption-based techniques can be exploited to secure physical-layer (the top-down approach), it is interesting to study whether the physical-layer can have build-in security and whether physical-layer security techniques can assist upper-layers (the bottom-up approach). Existing researches are mostly in the top-down approach. In contrast, the bottom-up approach is mostly open.

We define the build-in security of the physical-layer as that physical-layer transmissions are secured against adversaries based on transmission properties such as modulations, signals and channels, without resorting to source data encryption. Physical-layer transmission with build-in security means that the transmitted signal has negligibly low probability of interception (LPI) to any adversary, but can be detected successfully by the authorized user. Importantly, such transmission does not assume that the transmitter and the authorized receiver share some *a priori* knowledge secret to the adversary, such as encryption keys. In other words, security depends on the signal and channel properties.

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

One of the fundamental issues for physical-layer security design is the capacity of the transmission channels when build-in security is guaranteed. Such capacity is named secret channel capacity, and can be measured by the number of bits per second per unit frequency that can be transmitted with certain level of LPI. As an inherent capacity limit, the secret channel capacity needs to be specified based on information theory. The corresponding secrecy should preferably be information-theoretic secrecy, i.e., the adversary's received signal gives no more information for eavesdropping than purely guessing. The information-theoretic secrecy is in fact equivalent to perfect secrecy [1]. In addition, the focus on information-theoretic secrecy makes the new physical-layer security study meaningful and competitive compared with the traditional encryption-based techniques.

Traditional network security or cryptography depends on secret encryptions keys. The procedure of generating and distributing such keys is called secret-key agreement. With cryptography terminology, the procedure 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 secret-key agreement, where Eve is assumed to have full access to the channel, i.e., she receives identical messages as Bob. It is well known that perfect secrecy is impractical according to the Shannon model. Instead, with computational secrecy, keys can be generated based on some intractable computational problems such as factorizing integers in a feasible time. Note that such intractability assumption is unproven in practice, so does the secrecy [2]. New computing power, especially the future quantum computer, has been shown to challenge such intractability assumption. For example, the complexity of factorizing integers can be polynomial on a quantum computer as shown in [3], whose results have been partially demonstrated by experiments

Although perfect secrecy is widely considered as a theoretical limit only based on the classic Shannon's secrecy model, there are results suggesting that it may be realizable in practice. One of the results is quantum key distribution (QKD), which has obtained rapid progress recently after decades of investigation. However, currently QKD still requires dedicated laser links. It is unknown how QKD can be used conveniently in ordinary multi-hop networks, especially wireless networks.

Another result, which is more desirable for wireless networks, is the information-theoretic secrecy [4], whose key idea is that in

many practical communication systems, especially in wireless systems, Eve's channels or signals are not exactly the same as those of Bob. For example, their signals may be corrupted by different noise. As a result, they may have different bit-error-rates (BER) during receiving.

One of the earliest examples on information-theoretic secrecy was the wire-tap channel invented by Wyner [5], [6], which states that if Bob and Eve have different BER ϵ and δ, respectively, then the secret channel capacity from Alice to Bob can be

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

where $h(\epsilon)$ denotes the binary entropy function defined by $h(\epsilon) = -\epsilon \log_2 \epsilon - (1-\epsilon)\log_2(1-\epsilon)$. Obviously, if noise is considered as the only source of error, it requires that Eve's channel is noisier than Bob's in order to achieve any positive capacity. Such a requirement is in most cases impractical unfortunately.

More recently it has been shown that such a noisier requirement can be relaxed to that Eve suffers from a known (and sufficient large) error floor [4]. Specifically, the secret channel capacity can be

$$C_2 = h(\epsilon + \delta - 2\epsilon\delta) - h(\epsilon), \quad (2)$$

which is obtained when Alice and Bob can exchange (insure) information via another public channel. Equation (2) means that information-theoretic 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). Unfortunately, if noise is considered as the only source of receiving error as did in the existing literature, Eve's error rate δ can be much less than that of Bob. If $\delta \ll \epsilon$, the capacity specified by (2) becomes too small to be useful.

Nevertheless, existing information-theoretic secrecy results are interesting because they suggest perfect secrecy be possible with ordinary wireless transmissions, which is in contrast to the pessimistic view from the classic Shannon secrecy model. The problem remains to find valid ways to realize such secrecy in practice, or more specifically, to guarantee a high enough δ.

Recently, we have shown that instead of considering noise only, attacking the problem within the physical-layer signal processing framework provides new approaches. In particular, signal processing techniques can be exploited to deprive Eve's receiving capability if proper space-time transmission schemes are employed. In [7], we exploit the limit of blind deconvolution to make sure Eve can not estimate her channels. In contrast, in this paper, we show that even if Eve has her channel knowledge, information-theoretic secrecy is still achievable by exploiting properly the redundancy of antenna array space-time transmissions.

We depend on a special property of wireless transmissions for secrecy, i.e., signals received by Bob and Eve are different because their channels are different. Extensive literature on space-time channels tells us that as long as the distance among antennas is large enough, the channel coefficients vary independently and randomly.

This paper is organized as follows. In Section 2, a framework of space-time transmission for secret-key agreement is formulated. In Section 3, we show that traditional transmissions do not guarantee secrecy. Then, an intentional ambiguity scheme is developed in Section 4. Simulations are given in Section 5 and conclusions are presented in Section 6.

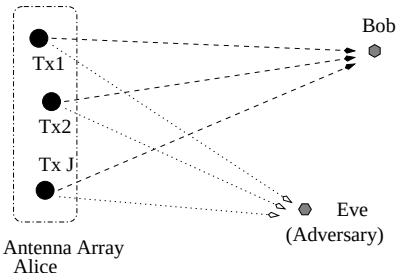

Fig. 1. System model for secret-key agreement between Alice, with J transmitters, and Bob.

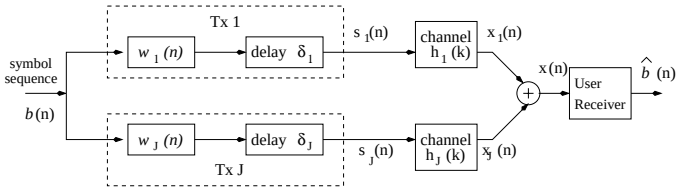

Fig. 2. The block diagram of secure space-time transmission.

2. SYSTEM DESCRIPTION

We consider a wireless network where Alice transmits to Bob using J transmitting antennas, which we call J transmitters. From the received signal, Bob needs to extract a secret key, during which Eve should be deprived of signal interception capability, as illustrated in Fig. 1.

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

If the propagation channel is Rayleigh flat fading, the signal received by Bob is

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

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 channel vector $\mathbf{h} \triangleq [h_1, \cdots, h_J]^T$, and

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

In this paper, $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ denote conjugation, transposition and Hermitian, respectively. We assume that $\mathbf{h}$ is block fading [8], i.e., it is constant or slowly time-varying when transmitting a block of symbols but may change randomly between blocks. The symbols $b(n)$ are independent uniformly distributed with zero-mean and unit variance. The transmission power is thus determined

by the transmitting weights $\mathbf{w}(n)$, whereas the received signal-to-noise-ratio (SNR) is determined by both $\mathbf{w}(n)$ and σ_v^2.

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. In addition, though the delays δ_i may not be zero because Eve adjusts δ_i in favor of Bob, in this paper we assume zero delays for simplicity. The received signal of Eve can then be written as

$$\mathbf{x}_u(n) = \mathbf{H}_u \mathbf{w}(n) b(n) + \mathbf{v}_u(n). \tag{5}$$

The notations are similar to (3) except that $(\cdot)_u$ is used to denote the unauthorized user. 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 case that Alice (with J transmitters) transmits a secret sequence to Bob. Other than that, they can communicate with each other using another insecure channel, and messages on this insecure channel may be known to Eve. If this second channel is used, then we can use (2) for a higher secret channel capacity than (1). In addition, this channel can also be used to transmit the normal high rate encrypted data with keys generated by the secret channel. Furthermore, Alice may use an extra transmitting antenna for piloting purpose, i.e., for Bob to synchronize in both time and frequency.

Note that although we study one direction secrecy 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, the scheme also fits single-point to multi-point transmission (broadcasting) schemes. Because different users have different channels, all other users can just be treated as adversaries to one specific user.

3. TRADITIONAL TRANSMISSIONS DO NOT GUARANTEE SECRECY

In this section, we assume that Eve does not know the channels $\mathbf{h}$ and $\mathbf{H}_u$. But she may try to estimate them by training/blind methods. In order to realize data transmission from Alice to Bob, ways have to be designed for them to estimate $\mathbf{h}$ and symbols.

Under such a problem setting, traditional transmit beamforming methods do not guarantee secrecy although they are optimal in terms of performance and power efficiency. A typical 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. Eve's received signal 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. Therefore, to guarantee secrecy, a necessary condition is that $\mathbf{w}(n)$ be random. Therefore, antenna array transmissions are necessary, since single-antenna transmissions are susceptible to blind detection.

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 $\mathbf{w}(n) = \mathbf{V}[1, z_2(n), \cdots, z_J(n)]^T \triangleq \mathbf{V}[1, \ \mathbf{z}_1^T(n)]^T$, where $z_j(n)$, $j = 2, \cdots, J$, can be arbitrary. However, 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

$$\mathbf{x}_u(n) \quad = \quad \mathbf{H}_u\mathbf{V}\left[\begin{array}{c} 1 \\ \mathbf{z}_1(n) \end{array}\right] b(n) + \mathbf{v}_u(n). \tag{6}$$

Here the key problem is that $\mathbf{w}(n)$ is designed with optimal power efficiency. As a result, in order to guarantee secrecy, we may not achieve the optimal unit transmission power. Therefore, there is a tradeoff of transmission power for secrecy.

4. SECRET TRANSMISSION SCHEME WITH INTENTIONAL AMBIGUITY

In this section, we develop a transmission scheme with the objective of guaranteeing secrecy even if Eve knows her own channel $\mathbf{H}_u$ and has extremely high SNR or even works in noiseless environment. Such an assumption makes this paper completely different from [7] where the limit of blind equalization is exploited for secrecy.

4.1. Transmission with intentional ambiguity

With the known channel $\mathbf{H}_u$, Eve's signal (5) can be simplified to

$$\mathbf{x}_u(n) = \mathbf{w}(n)b(n), \tag{7}$$

where the noise is skipped under the assumption of high SNR. To guarantee secrecy under (7), we propose to introduce intentional ambiguity into $\mathbf{x}_u(n)$ by designing properly $\mathbf{w}(n)$.

When Alice knows the channel $\mathbf{h}$, for example, through the reciprocity property, she can calculate a new $\mathbf{w}(n)$ in each symbol interval by generating a $J \times (J-1)$ random matrix $\mathbf{F} = [\mathbf{f}_1, \cdots, \mathbf{f}_{J-1}]$, where each $\mathbf{f}_i$ is a $J \times 1$ vector. Let

$$\mathbf{a}(n) = \left[\begin{array}{c} \|\mathbf{f}_1\| c_1(n) \\ \vdots \\ \|\mathbf{f}_{J-1}\| c_{J-1}(n) \end{array}\right], \tag{8}$$

where $\{c_i(n)\}$, $1 \le i \le J-1$, are secret sequences known only to Alice. Without loss of generality, we assume that $c_i(n) = \pm 1$, $\forall i, n$, and $\{c_i(n)\}$ and $\{c_j(n)\}$ are independent from each other. We make each column of the matrix $\mathbf{F}$ to have the same distribution as $\mathbf{h}$. In other words, each element of $\mathbf{F}$ is complex circular symmetric Gaussian distributed with zero-mean and unit variance, just as h_i. In addition, each column $\mathbf{f}_i$ has a similar time-varying property as $\mathbf{h}$. The matrix $\mathbf{F}$ is known to Alice only. To both Bob and Eve, each $\mathbf{f}_i$ looks statistically identical to $\mathbf{h}$.

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

$$\left[\begin{array}{c} \mathbf{h}^H \\ \mathbf{F}^H \end{array}\right] \mathbf{w}(n) = \left[\begin{array}{c} \|\mathbf{h}\| \\ \mathbf{a}(n) \end{array}\right]. \tag{9}$$

Since $\mathbf{F}$ is randomly generated, it is equivalent to saying that $\mathbf{w}(n)$ is random except satisfying $\mathbf{h}^H\mathbf{w}(n) = \|\mathbf{h}\|$. For Bob, the received signal becomes

$$x(n) = \|\mathbf{h}\| b(n) + v(n), \tag{10}$$

from which the symbol $b(n)$ can be detected via estimating the received signal power. The key point for guaranteeing secrecy is

that Eve becomes unable to discriminate $\mathbf{h}$ from any column of $\mathbf{F}$, as analyzed in Section 4.2.

The total transmission power of this scheme has a lower bound

$$\begin{aligned} E[\|\mathbf{w}(n)\|^2] &\geq E\left[\|[\mathbf{h}\ \ \mathbf{F}]\|^{-2}\left\|\begin{bmatrix}\|\mathbf{h}\| \\ \mathbf{a}(n)\end{bmatrix}\right\|^2\right] \\ &= \frac{\mathbf{h}^H\mathbf{h}+\mathbf{a}^H(n)\mathbf{a}(n)}{\mathrm{tr}([\mathbf{h}\ \ \mathbf{F}]^H[\mathbf{h}\ \ \mathbf{F}])} \\ &= 1. \end{aligned} \quad (11)$$

However, the unit lower bound usually can not be obtained. For example, considering the case that the columns of $\mathbf{F}$ are orthogonal to each other and to $\mathbf{h}$, the transmission power is $E[\|\mathbf{w}(n)\|^2] = J$.

From (9), the norm of $\mathbf{w}(n)$ depends on the eigenvalues of the random matrix $[\mathbf{h}\ \ \mathbf{F}]$. Since $\mathbf{F}$ is randomly generated, it is possible for $[\mathbf{h}\ \ \mathbf{F}]$ to become ill-conditioned. As we have shown, simply orthogonalizing this matrix does not give optimal transmission power.

4.2. Secrecy to Eve

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

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

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

$$\begin{aligned} P[\mathbf{h}|\{\mathbf{x}_u(n)\}] &= P[\{x_u(n)\}|\mathbf{h}]\frac{P[\mathbf{h}]}{P[\{\mathbf{x}_u(n)\}]} \\ &= P[\{\mathbf{w}(n)b(n)\}|\mathbf{h}]\frac{P[\mathbf{h}]}{P[\{\mathbf{x}_u(n)\}]} \\ &= P[\{\mathbf{w}(n)\}|\mathbf{h}]P[\{b(n)\}]\frac{P[\mathbf{h}]}{P[\{\mathbf{x}_u(n)\}]}. \end{aligned}$$

Because of (10), one element of $\mathbf{w}(n)$ is completely determined by others given $\mathbf{h}$. Let $w_1(n)$ be determined by random variables $\mathbf{z}_1(n) = [w_2(n), \cdots, w_J(n)]^T$. Then

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

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

$$P[\mathbf{f}_i|\{\mathbf{x}_u(n)\}] = P[\{\mathbf{z}_1(n)\}]P[\{b(n)\}]\frac{P[\mathbf{f}_i]}{P[\{\mathbf{x}_u(n)\}]}. \quad (12)$$

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

The proposition shows that Eve can not discriminate $\mathbf{h}$ from $\mathbf{f}_i$. In other words, she can not discriminate $b(n)$ from $c_i(n)b(n)$. This is the ambiguity created intentionally. The only way left for her is to guess $\{b(n)\}$ from all possible sequences $\{c_i(n)b(n) : 1 \leq i \leq J-1\}$, which is the essence of information-theoretic secrecy, i.e., Eve can only guess the result as if she has no any information on the received signal $\mathbf{x}_u(n)$. For the guessing-based exhaustive search, the complexity increases when the channels are (block) time-varying. Therefore, a small coherence time of the channel can greatly enhance the secrecy.

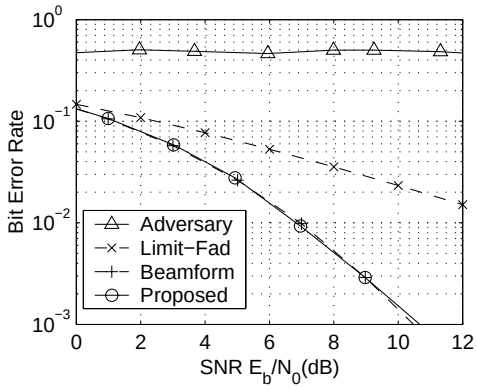

Fig. 3. Receiving performance. $J = 4$. ○: Bob in the proposed scheme. +:optimal transmit beamforming. ×:theoretical BER curve with Rayleigh fading channel. △: Eve in the proposed scheme.

5. SIMULATIONS

In this section, we show the performance of the proposed transmission scheme in terms of bit-error-rate (BER), secret channel capacity, and transmission power. We use BER to compare the receiving performance of Bob and Eve. For comparison purpose, we evaluate the performance of the optimal transmit beamforming discussed in Section 3, and give the theoretical BER curve of the Rayleigh fading channel without diversity. For Eve, we assume that she can only try to estimate each $\mathbf{w}(n)$ blindly, which is almost no difference from guessing.

Alice transmits QPSK symbol packets. Each packet contains 200 QPSK symbols. We use 5000 runs to obtain each BER value. We let Alice to find the best $\mathbf{w}(n)$ from J different realizations of $\mathbf{F}$ matrices in order to reduce transmission power and to avoid ill-conditioned matrices. The BER results are shown in Fig. 3, from which we see that Bob can reliably receive signals while Eve can not.

Based on the BER of Bob and Eve with the proposed transmission scheme, we also derive the secret channel capacity using (1) and (2). For comparison purpose, we also plot the secret capacity of the traditional transmission schemes when noise is considered as the only source of error. In this case, Eve is assumed to have the same SNR as Bob. As can be seen from Fig. 4, the proposal scheme gives much higher secret capacity. Note that considering the possibility that Eve can actually have higher SNR than Bob, the advantage of our scheme is even more exceptional.

The transmission power (both the total transmission power and the transmission power of a typical single transmitting antenna) is studied by simulation in 5(a) and (b). We compare the proposed method with the method in [7] and the optimal transmit beamforming. Obviously, the transmit beamforming is optimal in transmission power, while the proposed method and the method in [7] have a trade-off between transmission power and secrecy. The method in [7] requires both larger total transmission power and larger single-antenna transmission power than the proposed method, which is because the proposed method has better optimization when calculating transmitting coefficients $\mathbf{w}(n)$. In addition, the standard deviation of power consumption among 5000 runs is also shown. The standard deviation of transmission power

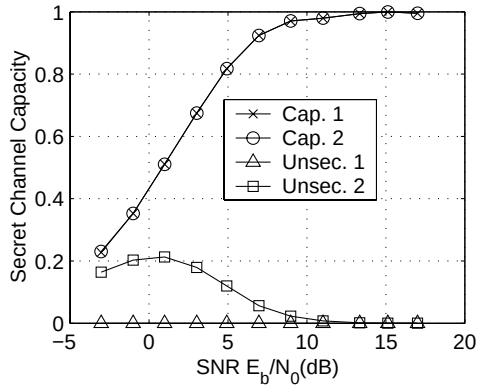

Fig. 4. Secret channel capacity. ×: proposed scheme with (1). ○: proposed scheme with (2). □:traditional transmit beamforming with (2). △:traditional transmit beamforming with (1).

of the proposed method is relatively constant.

6. CONCLUSIONS

This paper studies the informational-theoretically secret transmissions for secret-key agreement. By considering the physical-layer signal processing, the redundancy of space-time transmissions with antenna arrays can be exploited to create a difficult signal interception situation for the adversary. When the adversary suffers from high receiving errors, sufficiently high secret channel capacity can be realized in practice. This paper points out an innovative way for physical-layer security design and shows that physical-layer techniques can assist upper-layer security designs.

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

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

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

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

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

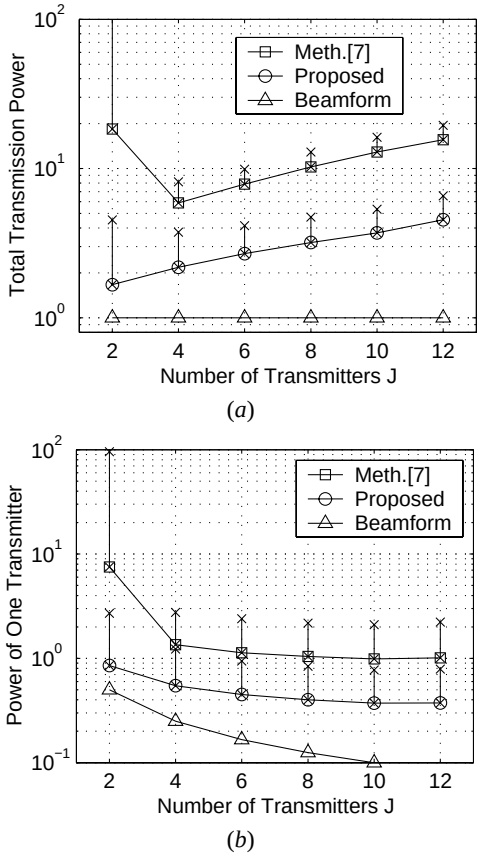

Fig. 5. Transmission power and standard deviation. Standard deviation is shown by × above the power value. (a) Total transmission power. (b) Power of a single transmitter. □:Method in [7]. ○:Proposed. △:transmit beamforming.