Secret Key Transmission Based on Channel Reciprocity for Secure IoT

Jinho Choi
School of EECS
Gwangju Institute of Science and Technology (GIST)
e-mail: jchoi0114@gist.ac.kr

Jeongseok Ha
Department of EE
Korea Advanced Institute of Science and Technology
e-mail: jsha@kaist.edu

***Abstract*—Machine type communications (MTC) play a crucial role in the Internet of things (IoT) where a number of devices are connected by wireless communications. Unfortunately, wireless communications are prone to various security threats including eavesdropping due to the broadcast nature. In this paper, we propose an approach that can generate a sequence of random numbers for a secret-key in an orthogonal frequency division multiplexing (OFDM) system. Since the random key is based on channel dependent signature (CDS) and generated without any predetermined sequences, a device can have a unique secret-key in the proposed approach, which suits to MTC for secure communications.**

I. Introduction

The Internet of Things (IoT) [1] has been widely studied to provide networks of physical objects or things. In the IoT, a wide range of connectivity solutions for a number of devices is required and machine type communications (MTC) [2] become crucial. Since there would be a number of devices in a certain area, wireless communications are considered for MTC. However, wireless communications are prone to various security threats including eavesdropping due to the broadcast nature. Thus, in order to avoid eavesdropping, it might be necessary to encrypt signals using various approaches in cryptography.

For encryption, it is necessary to share a secret-key. In particular, the secret-key generation and agreement are to be carried out in MTC without human involvement at devices. To this end, by exploiting the notion of channel reciprocity in time division duplexing (TDD) mode over wireless channels for a pair of transceivers, secret-key generation methods in [3]–[6] can be employed as keys are based on randomness of wireless channels and new keys are available when channels are varying (i.e., secure MTC do not need to rely on pre-stored keys at devices and new keys could be available if needed). A practical example with measurement results is also presented in [7]. These key generation methods aim at extracting a secret-key from raw channel measurements without using any particular transmission schemes. In this kind of approaches, the calibration of the gains of radio frequency (RF) chains at both transceivers [8] would be important so that measured channels at each transceiver do not have different gains of the channel state information (CSI). Note that as in [5], a level-crossing approach can be used in case of different gains of RF chains at both transceivers. However, this approach is limited as the CSI distribution needs to be symmetric.

This work was supported by Agency for Defense Development (the title of the project is *PHY/MAC-NETWORK Technologies Against Jamming Attack and Eavesdropping*.

In this paper, we consider symbol-level secure transmissions for secret-key transmissions or over-the-air (OTA) key delivery in orthogonal frequency division multiplexing (OFDM), multiple input multiple output (MIMO), or MIMO-OFDM systems. In the proposed approach, multiple incorrect symbols are transmitted simultaneously to confuse eavesdroppers, while the correct symbol can be received by a legitimate receiver using the shared secret of the CSI with a legitimate transmitter based on the channel reciprocity in TDD mode. Unlike existing secret-key generation methods in [4], [5], [7], the CSI is not directly used for secret-key generation. Thus, the proposed approach is insensitive to different gains of RF chains. As a result, the proposed scheme becomes suitable for sensors or IoT devices whose RF chains' gains may not be precisely decided due to inexpensive RF circuitry.

Notation: Matrices and vectors are denoted by upper- and lower-case boldface letters, respectively. The superscripts T and H denote the transpose and complex conjugate, respectively. The 2-norm of $\mathbf{a}$ is denoted by $||\mathbf{a}||$. $\mathbb{E}[\cdot]$ denotes the statistical expectation. $\mathcal{CN}(\mathbf{a}, \mathbf{R})$ represents the distribution of circularly symmetric complex Gaussian (CSCG) random vectors with mean vector $\mathbf{a}$ and covariance matrix $\mathbf{R}$.

II. System Model

Suppose that there is a pair of legitimate transmitter and receiver, called Alice and Bob, respectively, and an eavesdropper, called Eve. In MTC, Alice and Bob might be a gateway and a sensor, respectively. We consider an OFDM system for transmission from Alice to Bob with L subcarriers over a wideband channel. In this paper, we consider a secure scheme to transmit a secret-key sequence from Alice (i.e., a gateway) to Bob (i.e., a sensor) by exploiting the randomness of channels.

The signal vector to be transmitted is denoted by $\mathbf{s} \in \mathbb{C}^{L\times 1}$. For convenience, $\mathbf{s}$ is referred to as an OFDM signal block, while its elements are referred to as data symbols. The received signal at Bob is given by

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{n}, \tag{1}$$

where $\mathbf{n} \sim \mathcal{CN}(0, N_0\mathbf{I})$ is the background noise vector and $\mathbf{H} = \mathrm{diag}(H_0, \ldots, H_{L-1})$ is a diagonal channel matrix. Here, H_l denotes the channel coefficient over the lth subcarrier from Alice to Bob, and given by $H_l = \sum_{p=0}^{P-1} \tilde{h}_p e^{-j2\pi \frac{pl}{L}}$, where $\{\tilde{h}_p\}$ is the channel impulse response (CIR) and P is the length of CIR.

Similarly, the channel coefficient over the lth subcarrier from Alice to Eve is denoted by G_l. Then, the received signal at Eve is

$$\mathbf{z} = \mathbf{G}\mathbf{s} + \tilde{\mathbf{n}}, \tag{2}$$

where $\tilde{\mathbf{n}} \sim \mathcal{CN}(0, N_0\mathbf{I})$ is the background noise vector at Eve and $\mathbf{G} = \mathrm{diag}(G_0, \ldots, G_{L-1})$ is the diagonal channel matrix from Alice to Eve.

Throughout the paper, we assume TDD for communications between Alice and Bob to exploit the channel reciprocity for the shared secret, which is based on the CSI between Alice and Bob, as in [3], [6], [9]. To this end, Bob can transmit a pilot training sequence to Alice so that Alice can estimate $\{H_l\}$, and vice versa. Note that since this approach also allows Eve to estimate her CSI, $\{G_l\}$, we assume that Eve knows her CSI. However, we assume that Alice and Eve do not know the other's CSI.

For narrowband signals (with a single carrier), a similar model to that in (1) can be considered if Bob and Alice are equipped with multiple antennas. Suppose that Alice and Bob have M_{A} and M_{B} antennas, respectively. Then, the received signal at Bob can be written as in (1). In this case, $\mathbf{H}$ becomes the MIMO channel matrix of size $M_{\mathrm{B}} \times M_{\mathrm{A}}$. Eve can be equipped with multiple antennas (denote by M_{E} the number of antennas at Eve), and her MIMO channel matrix can be denoted by $\mathbf{G} \in \mathbb{C}^{M_{\mathrm{E}} \times M_{\mathrm{A}}}$.

III. Existing Secure Transmission Schemes based on Channel Reciprocity

In MTC, a gateway (i.e., Alice) may need to send a new secret-key sequence to a sensor (i.e., Bob) through a wireless channel. This transmission should be secure and avoid eavesdropping. To this end, in this section, we present an existing approach proposed in [9] for secure transmissions from Alice to Bob based on the channel reciprocity. We also briefly explain another approach proposed in [3].

We can modify the approach in [9] to be used for MIMO-OFDM. Consider the singular value decomposition (SVD) of $\mathbf{H}$, i.e., $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{\mathrm{H}}$, where $\mathbf{U} = [\mathbf{u}_1 \ \ldots \ \mathbf{u}_{\bar{L}}]$, $\mathbf{V} = [\mathbf{v}_1 \ \ldots \ \mathbf{v}_{\bar{L}}]$, and $\mathbf{\Sigma} = \mathrm{diag}(\sigma_1, \ \ldots, \sigma_{\bar{L}})$. Here, $\bar{L} = LM_{\mathrm{A}}$ and $\mathbf{u}_l$ and $\mathbf{v}_l$ denote the left and right singular vectors, respectively, corresponding to the lth singular value, σ_l. Throughout the paper, we assume that the singular values are ordered as follows:

$$|\sigma_1|^2 > \ \ldots \ > |\sigma_{\bar{L}}|^2. \tag{3}$$

This order is referred to as Alice's order, which is also known to Bob. This order plays a crucial role in deriving a secure transmission scheme in Section IV.

With $Q \in \{1, \ldots, \bar{L}-1\}$, the OFDM symbol vector to be transmitted is decomposed as

$$\mathbf{s} = \mathbf{V}\mathbf{x} = (\mathbf{V}_S\mathbf{x}_S + \mathbf{V}_N\mathbf{x}_N), \tag{4}$$

where $\mathbf{V} = [\mathbf{V}_S \ \mathbf{V}_N]$ and $\mathbf{x} = [\mathbf{x}_S^{\mathrm{T}} \ \mathbf{x}_N^{\mathrm{T}}]^{\mathrm{T}}$. Here, $\mathbf{V}_S = [\mathbf{v}_1 \ \ldots \ \mathbf{v}_Q] \in \mathbb{C}^{\bar{L} \times Q}$, $\mathbf{V}_N = [\mathbf{v}_{Q+1} \ \ldots \ \mathbf{v}_{\bar{L}}] \in \mathbb{C}^{\bar{L} \times (\bar{L}-Q)}$, $\mathbf{x}_S \in \mathbb{C}^{Q \times 1}$, and $\mathbf{x}_N \in \mathbb{C}^{(\bar{L}-Q) \times 1}$. The signal vector to be transmitted to Bob is $\mathbf{x}_S$, while $\mathbf{x}_N$ is an artificial noise vector. For convenience, the signal transmission via $\mathbf{v}_l$ is referred to as the signal transmission over mode l. In (4), Alice transmits a secret sequence over the first Q modes and artificial noise over the last $\bar{L} - Q$ modes.

The received signal at Bob becomes

$$\mathbf{y} = \mathbf{H}\mathbf{V}\mathbf{x} + \mathbf{n} = \mathbf{U}\mathbf{\Sigma}\mathbf{x} + \mathbf{n}. \tag{5}$$

Noting that $\mathbf{H}\mathbf{V}_S = \mathbf{U}_S\mathbf{\Sigma}_S$ and $\mathbf{H}\mathbf{V}_N = \mathbf{U}_N\mathbf{\Sigma}_N$, where $\mathbf{\Sigma}_S = \mathrm{diag}(\sigma_1, \ldots, \sigma_Q)$, $\mathbf{\Sigma}_N = \mathrm{diag}(\sigma_{Q+1}, \ldots, \sigma_{\bar{L}})$, $\mathbf{U}_S = [\mathbf{u}_1 \ \ldots \ \mathbf{u}_Q]$, and $\mathbf{U}_N = [\mathbf{u}_{Q+1} \ \ldots \ \mathbf{u}_{\bar{L}}]$, at Bob, we have

$$\mathbf{y}_S = \mathbf{U}_S^{\mathrm{H}}\mathbf{y} = \mathbf{\Sigma}_S\mathbf{x}_S + \mathbf{n}_S, \tag{6}$$

where $\mathbf{n}_S = \mathbf{U}_S^{\mathrm{H}}\mathbf{n}$. Thus, Bob can decode $\mathbf{x}_S$ without any interference from the artificial noise. On the other hand, at Eve, the received signal becomes

$$\mathbf{z} = \mathbf{G}\mathbf{V}_S\mathbf{x}_S + \mathbf{G}\mathbf{V}_N\mathbf{x}_N + \tilde{\mathbf{n}} = \mathbf{G}(\mathbf{a}_S + \mathbf{a}_N) + \tilde{\mathbf{n}}, \tag{7}$$

where $\mathbf{a}_S = \mathbf{V}_S\mathbf{x}_S$ and $\mathbf{a}_N = \mathbf{V}_N\mathbf{x}_N$. Eve can suffer from the artificial noise vector, $\mathbf{x}_N$. The resulting approach for an MIMO-OFDM system can be seen as a modification of that in [9], where the MIMO system is considered. To see this, we now suppose that $\mathbf{H}$ is an MIMO channel matrix. In addition, assume that $M_{\mathrm{B}} = 1$. In this case, $\mathbf{H} = \mathbf{h}^{\mathrm{T}}$ becomes a row vector of size $1 \times M_{\mathrm{A}}$ and $\mathbf{V}_S$ becomes $\frac{\mathbf{h}^*}{||\mathbf{h}||}$, while $\mathbf{V}_N\mathbf{x}_N$ is orthogonal to the signal, $\mathbf{V}_S\mathbf{x}_S$. As studied in [9], while the artificial noise does not interfere with the signal to Bob, it can confuse Eve (or degrade Eve's channel). Thus, when Alice is to transmit a secret-key to Bob, she can generate artificial noise as above to have a positive secrecy rate, and transmit a secret-key sequence to Bob at a rate below the secrecy rate. However, the secrecy rate is unknown unless $\mathbf{G}$ (or at least statistical properties of $\mathbf{G}$) is available to Alice.

In [3], an approach for secure transmissions without knowing the Eve's channel has been proposed, which might be used for MTC. While this approach is conceptually similar to [9], it does not need any information of $\mathbf{G}$. The symbol vector $\mathbf{s}$ is given by

$$\mathbf{s} = \mathbf{w}b, \tag{8}$$

where $\mathbf{w}$ is a weight vector that depends on $\mathbf{H}$ and b is the data symbol that is to be securely transmitted to Bob. For convenience, as in [3], we consider a multiple-input single-output (MISO) channel[1] with $\mathbf{H} = \mathbf{h}^{\mathrm{T}}$ (i.e., Bob has a single

[1] In order to apply to OFDM systems, we assume a linear combiner at Bob and the output, which is given by $y = \mathbf{q}^{\mathrm{H}}(\mathbf{H}\mathbf{s} + \mathbf{n})$, where $\mathbf{q}$ is the weight vector. Then, $\mathbf{h}^{\mathrm{T}}$ becomes $\mathbf{q}^{\mathrm{H}}\mathbf{H}$.

receive antenna). At Alice, for given $\mathbf{h}^{\mathrm{H}}$, $\mathbf{w}$ is decided to satisfy the following relation:

$$\begin{bmatrix} \mathbf{h}^{\mathrm{H}} \\ \mathbf{F}^{\mathrm{H}} \end{bmatrix} = \mathbf{w} \begin{bmatrix} ||\mathbf{h}|| \\ \mathbf{a} \end{bmatrix}, \tag{9}$$

where $\mathbf{F} = [\mathbf{f}_1 \ \ldots \ \mathbf{f}_{L-1}]$ is a random matrix of size $L \times (L-1)$ and $\mathbf{a} = [||\mathbf{f}_1||c_1 \ \ldots \ ||\mathbf{f}_{L-1}||c_{L-1}]^{\mathrm{T}}$. Here, c_l is an independent random variable. In [3], it is claimed that if $\mathbf{w}$ satisfies (9), the probability that Eve can choose $\mathbf{h}$ among $\{\mathbf{h}, \mathbf{f}_1, \ \ldots \ \mathbf{f}_{L-1}\}$ is the same as that of choosing $\mathbf{f}_l$ provided that Eve knows $\{\mathbf{h}, \mathbf{f}_1, \ \ldots \ \mathbf{f}_{L-1}\}$. Thus, Eve can choose one of $\{b, c_1 b, \ldots, c_{L-1} b\}$ equally likely.

Unfortunately, there are few drawback of the approach in [3]. One of them is that the transmission power that is decided by $\mathbf{w}$ can be random (as it depends on randomly generated $\mathbf{F}$). Another important drawback is that Eve can estimate b with a higher probability if L is smaller (i.e., the maximum equivocation may not be achieved). To see this, suppose that $L = 2$ and Eve is able to have $\psi = [b, c_1 b]$ or $\psi = [c_1 b, b]$, where $b, c_1 \in \{-1, +1\}$. As claimed in [3], Eve may not know the order of the contents in ψ. Thus, if $b = 1$, we have $\psi \in \{[1, -1], [1, 1]\}$ In addition, if $b = -1$, we have $\psi \in \{[-1, -1], [-1, 1]\}$. From this, if $\psi = [1, 1]$, b must be 1, and if $\psi = [-1, -1]$, b must be -1. This implies that with a probability of $1/2$, Eve can correctly decide the value of b if $L = 2$.

IV. Secure Precoded OFDM using Multiple Incorrect Data Symbols

A. Equivocation at Eve

For convenience, we mainly consider the OFDM system (in this case, $\mathbf{V}$ becomes a permutation matrix as $\mathbf{H}$ becomes diagonal). Suppose that the size of the signal vector, $\mathbf{x}_1$ is $Q \times 1$. In addition, for convenience, we assume that $L = QK$, where K is a positive integer. For example, if $L = 2^8$ and $Q = 2^4$, we have $K = 2^4 = 16$. When Alice transmits $\mathbf{x}_1$, she can transmit other signal vectors simultaneously to confuse Eve. They are denoted by $\mathbf{x}_2, \ldots, \mathbf{x}_K$.

The OFDM symbol vector to be transmitted is given by

$$\mathbf{s} = \sum_{k=1}^{K} \mathbf{V}_k \mathbf{x}_k, \tag{10}$$

where $\mathbf{V}_k = [\mathbf{v}_{(k-1)Q+1} \ \cdots \ \mathbf{v}_{(k-1)Q+Q}]$ and $\mathbf{x}_k \in \mathcal{X}$. For convenience, $\mathbf{V}_k$ is referred to as the kth signature matrix. In addition, let $\{\mathbf{V}_1, \ldots, \mathbf{V}_K\}$ denote the Alice's ordered signature matrices. We assume that $\mathbf{x}_1$ is the desired signal vector as a symbol of a secret-key sequence from Alice to Bob, while $\mathbf{x}_2, \ldots, \mathbf{x}_K$ are incorrect signal vectors used to confuse Eve. Furthermore, we consider the following scheme.

S1) We assume that $\mathbf{x}_1$ is one of the elements in $\mathcal{X}$, where $\mathcal{X}$ has K elements as follows: $\mathcal{X} = \{\mathbf{m}_1, \ \ldots, \ \mathbf{m}_K\}$. Furthermore, for a given $\mathbf{x}_1 \in \mathcal{X}$, we have

$$\{\mathbf{x}_2, \ldots, \mathbf{x}_K\} = \mathrm{RandomPerm}(\mathcal{X} \setminus \mathbf{x}_1),$$

where $\mathrm{RandomPerm}(\mathcal{S})$ is a random permutation of the elements in a set $\mathcal{S}$.

For example, suppose that $\mathcal{X} = \{1, -1, j\}$ (in this case, it is assumed that $K = 3$ and $Q = 1$). If $\mathbf{x}_1 = j$, we can have $\{\mathbf{x}_2, \mathbf{x}_3\} = \{1, -1\}$ or $\{-1, 1\}$ equally likely.

The transmission scheme based on (10) with **S1)** uses channel dependent signature to transmit a symbol $\mathbf{x}_1$, which is a symbol of a secret-key sequence. We are now interested in Eve's equivocation. At Eve, the received signal becomes

$$\mathbf{z} = \mathbf{G} \sum_{k=1}^{K} \mathbf{V}_k \mathbf{x}_k + \tilde{\mathbf{n}} = \mathbf{G} \sum_{k=1}^{K} \mathbf{a}_k + \tilde{\mathbf{n}}. \tag{11}$$

Suppose that Eve can reduce the background noise effectively. In this case, since Eve knows $\mathbf{G}$, she can have $\sum_{k=1}^{K} \mathbf{a}_k$ from $\mathbf{z}$. We can show that this information, i.e., $\sum_{k=1}^{K} \mathbf{a}_k$, does not help Eve to reduce the equivocation as follows.

Theorem 1: Suppose that Eve can have the knowledge of $\{\mathbf{V}_1, \ldots, \mathbf{V}_K\}$ except their order (which is referred to as Alice's order). Let $\mathbf{V}_{(k)}$ denote the kth Eve's ordered signature matrix (i.e., Eve has $\{\mathbf{V}_{(1)}, \ldots, \mathbf{V}_{(K)}\}$). Then, for a given $\sum_{k=1}^{K} \mathbf{a}_k$, the equivocation of $\mathbf{x}_1$ is

$$H\left(\mathbf{x}_1 \middle| \sum_{k=1}^{K} \mathbf{a}_k\right) = H(\mathbf{x}_1) = \log_2 K, \tag{12}$$

where $H(X)$ stands for the entropy of X and $H(X|Y)$ denotes the conditional entropy of X for given Y or equivocation.

Proof: Let $\mathbf{a} = \sum_{k=1}^{K} \mathbf{a}_k$. Then, for given $\mathbf{a}$, suppose that Eve can decide $\{\mathbf{m}_{(k)} \in \mathcal{X}\}$ that satisfies $\mathbf{a} = \sum_{k=1}^{K} \mathbf{V}_{(k)} \mathbf{m}_{(k)}$. In this case, $\mathbf{m}_{(1)}$ is the estimate of $\mathbf{x}_1$, denoted by $\hat{\mathbf{x}}_1$, at Eve. There are $K!$ combinations for $\{\mathbf{V}_{(1)}, \ldots, \mathbf{V}_{(K)}\}$. Thus, the knowledge of $\mathbf{a}$ does not reduce the entropy of $\mathbf{x}_1$, because $\log_2(K!) \geq \log_2 K$ for all $K \geq 1$. Since $\hat{\mathbf{x}}_1 = \mathbf{m}_{(1)}$ can be any element of $\mathcal{X}$ with an equal probability, i.e., $\frac{1}{K}$, the equivocation of $\mathbf{x}_1$ becomes the entropy of $\mathbf{x}_1$, which is $\log_2 K$. ■

From Theorem 1, we can see that although Eve can have a better channel gain than Bob (e.g., $\min_l |G_l|^2 \gg \max_l |H_l|^2$), Eve cannot choose the correct data symbol $\mathbf{x}_1$ with a probability higher than $\frac{1}{K}$. Furthermore, although there are multiple eavesdroppers colluding to decide $\mathbf{x}_1$ with multiple received signals, they cannot do better than random guess unless $\mathbf{H}$ is known.

Note that in Theorem 1, we assume that Eve can estimate $\{\mathbf{V}_k\}$ except Alice's order. In order to see that this is not impossible, consider (2) that is rewritten as

$$\mathbf{z} = \sum_{k=1}^{K} \mathbf{G}_k \mathbf{x}_k + \tilde{\mathbf{n}}, \tag{13}$$

where $\mathbf{G}_k = \mathbf{G}\mathbf{V}_k$. From this, $\mathbf{z}$ can be seen as a superposition of the received signals from multiple users. There are blind (or semi-blind) channel estimation methods for this, e.g., [10], [11]. Thus, it might be a reasonable assumption that $\{\mathbf{G}_k\}$ can be available at Eve or $\{\mathbf{V}_k\}$ (as $\mathbf{G}$ is assumed to be known). However, the order is uncertain unless a known different pilot

signal is transmitted for each $\mathbf{x}_k$ to allow Eve to identify Alice's order of $\{\mathbf{V}_k\}$, which is not the case in this paper. Therefore, the proposed scheme is secure without wiretap channel coding. For convenience, this scheme is referred to as the channel dependent signature based secure OFDM (CDS-SOFDM) scheme.

It is noteworthy that the CDS-SOFDM scheme for the OTA key delivery can be carried out in any conventional OFDM systems. That is, no significant modification of existing OFDM systems is required to implement the CDS-SOFDM scheme for the OTA key delivery. In particular, since $\mathbf{V}_k$ is a permutation matrix and each element of $\mathbf{x}_k$ is a point of a given constellation, $\mathcal{X}$, the OFDM symbol vector in (10), $\mathbf{s}$, is seen as an ordinary OFDM symbol vector with elements from $\mathcal{X}$, if $\mathcal{X}$ is any conventional signal constellation, e.g., quadrature amplitude modulation (QAM).

Example 1: Suppose that $K = 2$ and $Q = 1$ with $x_k \in \{-1, +1\}$. In addition, the size of $\mathbf{G}_k = \mathbf{g}_k$ are 2×1. Eve knows $\{\mathbf{g}_1, \mathbf{g}_2\}$ except order (i.e., Alice's order). Letting $x_1 = x \in \{-1, +1\}$, since Eve does not know Alice's order, Eve's received signal can be written as

$$\mathbf{z} = \begin{cases} \mathbf{g}_1 x - \mathbf{g}_2 x + \tilde{\mathbf{n}}, & \text{with probability } \frac{1}{2} \\ -\mathbf{g}_1 x + \mathbf{g}_2 x + \tilde{\mathbf{n}}, & \text{with probability } \frac{1}{2} \end{cases}$$

or $\mathbf{z} = \tilde{\mathbf{g}}\kappa x + \tilde{\mathbf{n}}$, where $\tilde{\mathbf{g}} = \mathbf{g}_1 - \mathbf{g}_2$ and $\kappa \in \{-1, +1\}$ is an independent binary random variable with $\Pr(\kappa = +1) = \Pr(\kappa = -1) = \frac{1}{2}$. Note that κ is introduced due to the lack of Alice's order at Eve. The likelihood function becomes $f(\mathbf{z}|x) = c\left(e^{-\frac{1}{N_0}||\mathbf{z}-\tilde{\mathbf{g}}x||^2} + e^{-\frac{1}{N_0}||\mathbf{z}+\tilde{\mathbf{g}}x||^2}\right)$, which is a symmetric function of $x \in \{-1, +1\}$. Here, c is the normalizing constant. Thus, the equivocation becomes $H(X|\mathbf{z}) = 1$, which is the same as the entropy of X, $H(X) = 1$.

Note that the transmission of all the symbols in $\mathcal{X}$ with random permutation is the key difference from the approach in [3]. If we apply the approach in [3] to this example, we have $x_1 = b$ and $x_2 = bc_1$, where $b \in \{-1, +1\}$ is the secret symbol and c_1 is an independent binary random variable. Since Eve knows $\mathbf{G}$, she can recover x_1 and x_2 without the correct order. Denote by $x_{(k)}$ the x_k's of the Eve's order (i.e., $x_{(k)} = x_1$ or x_2 equally likely, $k = 1, 2$, at Eve). As explained earlier, in this case, we have

$$\Pr(b \,|\, x_{(1)} = x_{(2)}) = \begin{cases} 1, & \text{if } x_{(1)} = x_{(2)} = b \\ 0, & \text{if } x_{(1)} = x_{(2)} \neq b \end{cases}$$

and $\Pr(b \,|\, x_{(1)} \neq x_{(2)}) = \frac{1}{2},\ b \in \{-1, +1\}$. Then, it can be shown that $H(b \,|\, x_{(1)}, x_{(2)}) = 1/2$ if b is equally likely. This shows that the maximum equivocation, $H(b) = 1$, cannot be achieved by the approach in [3].

Note that $||\mathbf{s}||^2 = \sum_{k=1}^{K} ||\mathbf{x}_k||^2$. Thus, the proposed method does not have random transmission powers. In addition, as shown above, the maximum equivocation can be achieved. Consequently, the drawbacks of the approach in [3] do not exist in the proposed approach.

B. Detection Performance at Bob

Since Bob knows $\mathbf{H}$, the SVD of $\mathbf{H}$ is available. We can rewrite (6) as

$$\mathbf{d} = \mathbf{U}_1^{\mathrm{H}}\mathbf{y} = \mathbf{\Sigma}_1\mathbf{x}_1 + \mathbf{U}_1^{\mathrm{H}}\mathbf{n}. \tag{14}$$

The ML detection can be carried out as

$$\hat{\mathbf{x}}_1 = \underset{\mathbf{x}' \in \mathcal{X}}{\operatorname{argmin}} ||\mathbf{d} - \mathbf{\Sigma}_1\mathbf{x}'||^2. \tag{15}$$

For given $\mathbf{\Sigma}_1$, the symbol error rate (SER) of the ML detection is given by

$$\begin{aligned} P_e(K) &= \Pr(\hat{\mathbf{x}}_1 \neq \mathbf{x}_1) \\ &\leq P_{\mathrm{bnd}}(K) \\ &= \sum_{\mathbf{x}' \in \mathcal{X} \setminus \mathbf{x}_1} \Pr(||\mathbf{d} - \mathbf{\Sigma}_1\mathbf{x}_1||^2 > ||\mathbf{d} - \mathbf{\Sigma}_1\mathbf{x}'||^2), \end{aligned} \tag{16}$$

where $P_{\mathrm{bnd}}(K)$ is an upper-bound on the SER. It follows that

$$P_{\mathrm{bnd}}(K) = \sum_{\mathbf{x}' \in \mathcal{X} \setminus \mathbf{x}_1} \mathcal{Q}\left(\frac{||\mathbf{\Sigma}_1(\mathbf{x}_1 - \mathbf{x}')||}{\sqrt{2N_0}}\right), \tag{17}$$

where $\mathcal{Q}(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$. It can be shown that $||\mathbf{\Sigma}_1(\mathbf{x}_1 - \mathbf{x}')||^2 = \sum_{q=1}^{Q} |\sigma_q|^2 |e_{1,q}|^2$, where $e_{1,q} = [\mathbf{x}_1 - \mathbf{x}']_q$.

Let $\lambda_q = |\sigma_q|^2$. Since the $|\sigma_q|^2$'s are ordered, we can have $||\mathbf{\Sigma}_1(\mathbf{x}_1 - \mathbf{x}')||^2 \geq \lambda_Q ||\mathbf{x}_1 - \mathbf{x}'||^2$. Furthermore, we can show that $\sum_{q=1}^{Q} |e_{1,q}|^2 \geq d_{\min}^2 = \min_{\mathbf{x}_1 \in \mathcal{X}} \min_{\mathbf{x} \in \mathcal{X} \setminus \mathbf{x}_1} ||\mathbf{x}_1 - \mathbf{x}||^2$, where $d_{\min}$ denotes the minimum signal distance of $\mathcal{X}$. Thus, it can be shown that

$$\mathbb{E}[P_{\mathrm{bnd}}(K)] \leq (K-1)\mathbb{E}\left[\mathcal{Q}\left(\sqrt{\frac{\lambda_Q d_{\min}^2}{2N_0}}\right)\right]. \tag{18}$$

V. Simulation Results

In this section, we present simulation results of the (narrowband) MIMO system instead of OFDM[2] systems. Note that the resulting scheme will be referred to as the CDS based secure MIMO (CDS-SMIMO) scheme, although there is no difference between CDS-SOFDM and CDS-SMIMO in principle. For simulations, we consider the (narrowband) MIMO system where the elements of $\mathbf{H}$ and $\mathbf{G}$ are independent zero-mean CSCG random variables. That is, $[\mathbf{H}]_{m,l} \sim \mathcal{CN}\left(0, \frac{\sigma_H^2}{M_{\mathrm{A}}}\right)$ and $[\mathbf{G}]_{m,l} \sim \mathcal{CN}\left(0, \frac{\sigma_G^2}{M_{\mathrm{A}}}\right)$. For normalization purposes, we assume that $\sigma_H^2 = 1$ and $N_0 = 1$, while σ_G^2 varies. In addition, we assume that $M_{\mathrm{A}} = M_{\mathrm{E}} = 2^4 = 16$, $Q = 1$, and 16-QAM with $M_{\mathrm{A}} = K = 16$. The signal-to-noise ratio (SNR) is given by $\mathsf{SNR} = \frac{E_{\mathrm{b}}}{N_0}$, where E_{b} denotes the bit energy.

In order to see the impact of M_{B} on Bob's detection performances, we consider the bit error rate (BER) for various values of M_{B} and present simulation results in Fig. 1. As Bob can have a higher (receive) diversity gain with more antennas, a lower BER is achieved, which is shown in Fig. 1 (a). Fig. 1

[2]The main purpose to consider MIMO systems is to demonstrate that the approach for OFDM systems in Section IV is also applicable to MIMO systems.

(b) shows that the probability that Eve can choose the correct signature using signature attack is $\frac{1}{K} = \frac{1}{16} = 0.0625$, which is independent of $E_{\rm b}/N_0$.

Note that in the CDS-SMIMO scheme, since K symbols are transmitted simultaneously, the bit energy should be multiplied by K. That is, $E_{\rm b} = 16$ or 12.04 dB means that the bit energy for x_1 is 1 or 0 dB in the case of $K = 16$.

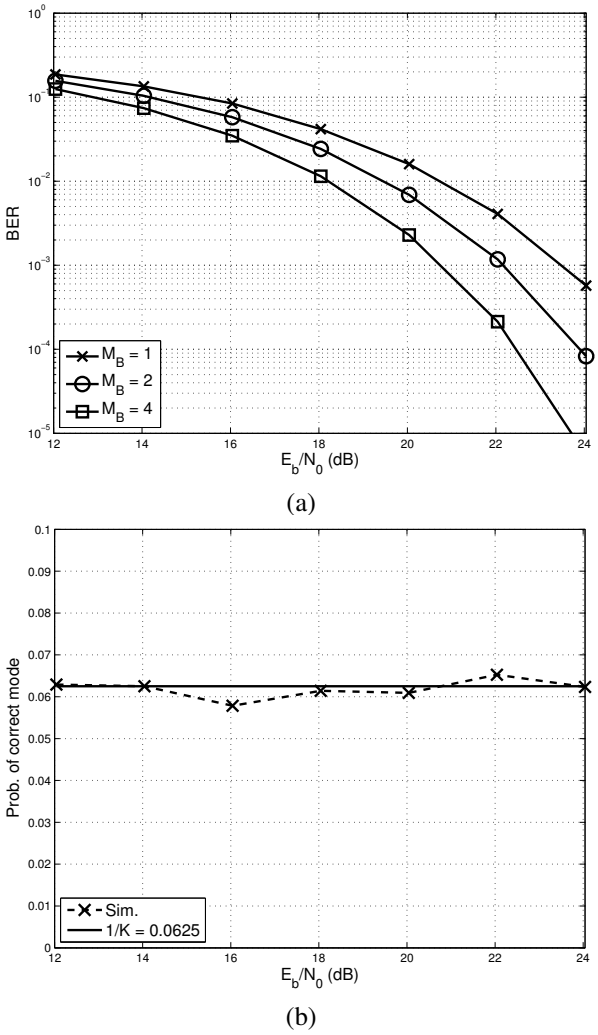

Fig. 1. Performances of CDS-SMIMO with various $M_{\rm B}$: (a) Bob's BER performance; (b) Eve's probability of correct signature.

Fig. 2 shows that the probability that Eve can choose the correct signature using signature attack for different Eve's channel gains, σ_G^2. Since σ_H^2 is fixed, as σ_G^2 increases, Eve has a relatively better channel gains than Bob. From the results in Fig. 2, as we expect, the probability that Eve can choose the correct signature is independent of σ_G^2 and is about $\frac{1}{K} = \frac{1}{16} = 0.0625$. Thus, Eve's equivocation is $H(K) = \log_2 K = 4$.

VI. Concluding Remarks

In this paper, we proposed a simple secure transmission scheme for the OTA key delivery that is suitable for sensors

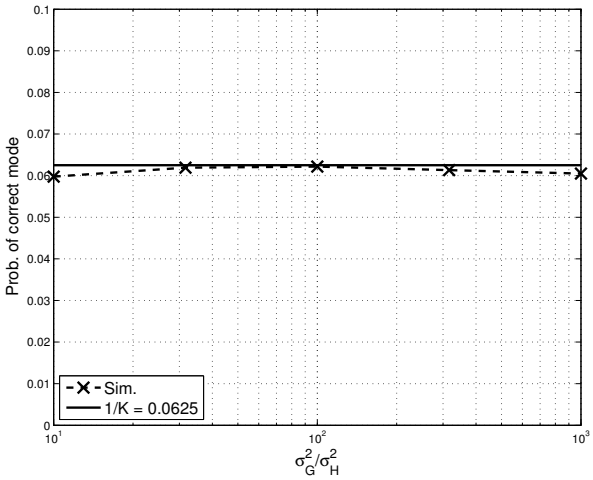

Fig. 2. Eve's probability of correct signature for different values of $\frac{\sigma_G^2}{\sigma_H^2}$.

or IoT devices whose RF chains' gains may not be precisely decided due to inexpensive RF circuitry. The proposed scheme transmits multiple incorrect data symbols simultaneously to confuse Eve. In this scheme, Bob can choose the correct data symbol based on the channel dependent signature to extract a key. A salient feature of the proposed scheme for the OTA key delivery was that it can be used in the conventional OFDM or MIMO-OFDM systems without any significant modification.

References

[1] ITU-T Y.2060, *Overview of the Internet of things*, 2012.

[2] 3GPP TR 37.868 V11.0, *Study on RAN improvments for machine-type communications*, October 2011.

[3] X. Li, M. Chen, and E. Ratazzi, "Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy," in *IEEE Workshop on Signal Processing Advances in Wireless Communications*, pp. 811–815, June 2005.

[4] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Information Forensics and Security*, vol. 2, pp. 364–375, Sept 2007.

[5] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Information Forensics and Security*, vol. 5, pp. 240–254, June 2010.

[6] S. Im, H. Jeon, J. Choi, and J. Ha, "Secret key agreement under an active attack in MU-TDD systems with large antenna arrays," in *Global Communications Conference (GLOBECOM), 2013 IEEE*, pp. 1849–1855, Dec 2013.

[7] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Computing*, vol. 12, pp. 917–930, May 2013.

[8] F. Kaltenberger, H. Jiang, M. Guillaud, and R. Knopp, "Relative channel reciprocity calibration in MIMO/TDD systems," in *Future Network and Mobile Summit, 2010*, pp. 1–10, June 2010.

[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, June 2008.

[10] Y. Zeng and T.-S. Ng, "A semi-blind channel estimation method for multiuser multiantenna OFDM systems," *IEEE Trans. Signal Process.*, vol. 52, pp. 1419–1429, May 2004.

[11] S. ShahbazPanahi, A. Gershman, and G. Giannakis, "Semiblind multiuser mimo channel estimation using capon and music techniques," *IEEE Trans. Signal Process.*, vol. 54, pp. 3581–3591, Sept 2006.