Secure Transmissions via Compressive Sensing in Multicarrier Systems

Jinho Choi

***Abstract*—In this paper, we consider an encryption scheme based on compressive sensing for multicarrier systems, where artificial noise is selectively transmitted together with a sparse message signal in the frequency domain to make an adversary's attack difficult. In order to minimize the impact of artificial noise on the performance of a legitimate receiver, the channel state information at the transmitter is exploited under the assumption of channel reciprocity in time division multiplexing mode. We consider attack to estimate the measurement matrix using the maximum likelihood approach and find the probability of correct recovery (or successful attack) under certain assumptions which might be favorable for the adversary.**

***Index Terms*—Compressive sensing (CS), encryption.**

I. Introduction

COMPRESSIVE sensing (CS) [1]–[3] has been considered for encryption in [4], where a measurement matrix generated by a (private) key is used to encrypt a sparse message. A legitimate receiver uses the same measurement matrix to decrypt the message by solving an optimization problem. CS-based encryption is applied to secure transmissions of the readings of smart meters in a smart grid in [5] and to a multiclass CS system to provide different recovery qualities in [6]. As discussed in [4], while CS-based encryption can provide a computational guarantee of secrecy, its key to generate the measurement matrix has to be unknown to an adversary. In [7], the notion of physical layer security [8]–[10] is exploited to generate a secret key shared between a pair of legitimate transmitter and receiver in wireless communications.

In this paper, based on the approach in [4], we consider a CS-based encryption scheme for a multicarrier system [11] and study attack by an adversary to estimate the measurement matrix. We assume that the adversary knows the structure of a generator that generates the measurement matrix except the shared secret key between a legitimate pair of transmitter and receiver. In order to lower the probability of successful attack (or correct recovery of the measurement matrix) by the adversary, we propose to transmit artificial noise together with a sparse message. Since the artificial noise can also degrade the performance at the legitimate receiver, the known channel state information (CSI), which is available from the channel reciprocity in time division duplexing (TDD) mode, is exploited to selectively transmit an artificial noise in the frequency domain. Under certain assumptions, we derive an upper bound on the probability of successful attack, which would be useful to decide the values of key parameters to provide a guarantee of secrecy in terms of the probability of successful attack.

Notation: The superscripts T and H denote the transpose and complex conjugate, respectively. The p-norm of a vector $\mathbf{a}$ is denoted by $||\mathbf{a}||_p$ (If $p=2$, the norm is denoted by $||\mathbf{a}||$ without the subscript). The superscript † denotes the pseudo-inverse. For a vector $\mathbf{a}$, $\mathrm{diag}(\mathbf{a})$ is the diagonal matrix with the diagonal elements from $\mathbf{a}$. For a matrix $\mathbf{X}$ (a vector $\mathbf{x}$), $[\mathbf{X}]_n$ ($[\mathbf{x}]_n$) represents the nth column (element, resp.). If $\mathcal{A}$ is a set of indices, $[\mathbf{x}]_{\mathcal{A}}$ is a subvector of $\mathbf{x}$ obtained by taking the corresponding elements. $\mathbb{E}[\cdot]$ 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

A. System Model and Assumptions

Suppose that there is a pair of legitimate transmitter and receiver, called Alice and Bob, respectively, and an adversary (or an eavesdropper), called Eve. We consider a multicarrier system for transmissions from Alice to Bob with L subcarriers over a wideband channel. Suppose that Alice transmits a block of signal over L subcarriers, which is denoted by $\mathbf{s}\in\mathbb{C}^{L\times 1}$. Then, 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 (frequency-domain) channel matrix. Here, H_l denotes the channel coefficient over the lth subcarrier from Alice to Bob, and given by $H_l=\sum_{p=0}^{P-1}h_p e^{-j2\pi\frac{pl}{L}}$, where $\{h_p\}$ is the channel impulse response (CIR) and P is the length of CIR.

Similarly, the received signal at Eve is given by

$$\mathbf{z}=\mathbf{G}\mathbf{s}+\mathbf{w} \tag{2}$$

where $\mathbf{w}\sim\mathcal{CN}(0,N_0\mathbf{I})$ is the background noise vector and $\mathbf{G}=\mathrm{diag}(G_0,\ldots,G_{L-1})$ is a diagonal (frequency domain) channel matrix. Here, G_l represents the channel coefficient over the lth subcarrier, which is given by $G_l=\sum_{p=0}^{P-1}g_p e^{-j2\pi\frac{pl}{L}}$, where $\{g_p\}$ is the CIR from Alice to Eve.

Throughout the paper, we assume that h_p and g_p are independent zero-mean CSCG random variables. In particular, we assume that

$$h_p\sim\mathcal{CN}\left(0,\sigma_h^2/P\right)\ \text{and}\ g_p\sim\mathcal{CN}\left(0,\sigma_g^2/P\right) \tag{3}$$

Manuscript received July 15, 2016; accepted July 26, 2016. Date of publication July 27, 2016; date of current version August 11, 2016. This work was supported by the Agency for Defense Development (the title of the project is *PHY/MAC-NETWORK Technologies Against Jamming Attack and Eavesdropping*. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yong Xiang.

The author is with the School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, Korea (e-mail: jchoi0114@gist.ac.kr).

Digital Object Identifier 10.1109/LSP.2016.2595524

which is based on the multipath Rayleigh fading channel model. Thus, from (3), we consider the following assumption.

A1) The channel coefficients in the frequency domain are

$$H_l \sim \mathcal{CN}(0, \sigma_h^2) \text{ and } G_l \sim \mathcal{CN}(0, \sigma_g^2), l = 0, \ldots, L-1.$$

Let $\alpha_l = |H_l|^2$ and $\beta_l = |G_l|^2$. We also assume TDD mode. Bob can transmit a pilot signal to allow Alice to estimate the Bob's CSI, $\mathbf{H}$. In addition, Alice sends a pilot signal to Bob so that Bob can have his CSI, $\mathbf{H}$, to estimate $\mathbf{s}$. Note that due to the pilot signal from Alice, Eve can also have her CSI, $\mathbf{G}$. Therefore, throughout the paper, we assume that both Alice and Bob know $\mathbf{H}$, but not $\mathbf{G}$, and Eve knows $\mathbf{G}$, but not $\mathbf{H}$.

Throughout the paper, we assume that the signal transmitted from Alice is a sparse signal that is given by

$$\mathbf{s} = \mathbf{\Psi}\mathbf{x} \tag{4}$$

where $\mathbf{\Psi} \in \mathbb{C}^{L \times N}$ is a precoding (or measurement) matrix and $\mathbf{x} \in \mathbb{C}^{N \times 1}$ is a Q-sparse signal vector. For convenience, we define the set of Q-sparse signals as $\Sigma_Q = \{\mathbf{x} \,\big|\, ||\mathbf{x}||_0 = Q\}$. Thus, $\mathbf{x} \in \Sigma_Q$. In addition, we assume that $[\mathbf{x}]_n \in \{0, A\}$, i.e., the nonzero elements of $\mathbf{x}$ are $A > 0$. The number of bits for each $\mathbf{x}$ becomes $N_{\text{bit}} = \lfloor \log_2 \binom{N}{Q} \rfloor$.

For the measurement matrix, we consider the following assumption for tractable analysis.

A2) The elements of $\mathbf{\Psi}$, $[\mathbf{\Psi}]_{m,n} \in \{\pm 1/\sqrt{L}\}$, are equally likely independent random variables.

Under *A2)*, $\mathbf{\Psi}$ becomes subGaussian random matrix [12].

B. Artificial Noise

For eavesdropping, Eve needs to know $\mathbf{\Psi}$. Thus, her attack is to estimate $\mathbf{\Psi}$ from $\mathbf{z}$. In this section, we use an artificial noise in the frequency domain to reduce the number of the received signals for attack to estimate $\mathbf{\Psi}$ at Eve without a significant performance degradation at Bob in recovering the sparse signal $\mathbf{x}$.

In the proposed scheme, we divide L subcarriers into two subsets. Secure transmissions from Alice to Bob are performed through one subset, while artificial noise is transmitted through the other subset to degrade Eve's channel. Denote by $k(m)$, the index of the mth largest α_l and define the index set of the M $(< L)$ largest channel coefficients as

$$\mathcal{I} = \{k(1), \ldots, k(M)\}. \tag{5}$$

For the sake of reliable transmissions from Alice to Bob, the subcarriers associated with $\mathcal{I}$ (of high channel gains) are chosen, while artificial noise, denoted by $\mathbf{c}$, is transmitted over the subcarriers associated with $\mathcal{I}^c$ as

$$[\mathbf{c}]_l = \begin{cases} 0, & \text{if } l \in \mathcal{I} \\ \mathcal{CN}(0, \sigma_{\text{AN}}^2), & \text{otherwise} \end{cases} \tag{6}$$

where σ_{AN}^2 is the variance of the artificial noise, which is sufficiently large. It is important to note that although the subcarriers associated with $\mathcal{I}^c$ are not reliable for the transmissions from Alice to Bob, they can be reliable at Eve as $\mathbf{H}$ and $\mathbf{G}$ are independent. Without transmitting artificial noise, since Eve can take advantage of high channel gains to perform known-plaintext attacks from the signals through the subcarriers associated with $\mathcal{I}^c$, we need to avoid this using the artificial noise. As a result, the signal to be transmitted from Alice becomes $\mathbf{b} = \mathbf{s} + \mathbf{c}$.

III. Recovery of Sparse Signals and an Attack to Estimate a Measurement Matrix

In this section, we consider the signal recovery at Bob and Eve and study the impact of the artificial noise and $|\mathcal{I}| = M$ on the performances at Bob and Eve.

A. Low-Complexity Recovery at Bob Using Sparsity

Suppose that Bob has $\mathbf{\Psi}$ or (a key to generate $\mathbf{\Psi}$) and is to recover $\mathbf{x}$ from the following received signal vector:

$$\mathbf{y} = \mathbf{H}\mathbf{b} + \mathbf{n} = \mathbf{H}\mathbf{\Psi}\mathbf{x} + \mathbf{H}\mathbf{c} + \mathbf{n}. \tag{7}$$

To avoid the artificial noise $\mathbf{c}$, the received signals associated with $\mathcal{I}$ can be used. Let

$$\mathbf{r} = \mathbf{y}_{\mathcal{I}} = \mathbf{B}\mathbf{x} + \mathbf{n}_{\mathcal{I}} \tag{8}$$

where $\mathbf{B}$ is the submatrix of $\mathbf{H}\mathbf{\Psi}$ obtained by taking the rows vectors whose indices are in $\mathcal{I}$. To estimate $\mathbf{x}$, we can consider the maximum likelihood (ML) approach as follows:

$$\hat{\mathbf{x}} = \underset{\mathbf{x} \in \bar{\Sigma}_Q}{\operatorname{argmax}} f(\mathbf{r} \,|\, \mathbf{x}) = \underset{\mathbf{x} \in \bar{\Sigma}_Q}{\operatorname{argmin}} ||\mathbf{r} - \mathbf{B}\mathbf{x}||^2 \tag{9}$$

where $\bar{\Sigma}_Q = \{\mathbf{x} \,|\, \mathbf{x} \in \Sigma_Q, [\mathbf{x}]_n \in \{0, A\}\}$. Clearly, since $|\bar{\Sigma}_Q| = \binom{N}{Q}$, the complexity of the ML approach is proportional to $\binom{N}{Q}$. Thus, when Bob has limited computing power, it would be difficult to use the ML approach at Bob to estimate $\mathbf{x}$ for a large L with $Q > 1$.

Using the notion of CS, we can estimate $\mathbf{x}$ with low-complexity. We can consider the following optimization:

$$\min ||\mathbf{x}||_p \text{ subject to } ||\mathbf{r} - \mathbf{B}\mathbf{x}||_2^2 \leq \epsilon \tag{10}$$

where p is the parameter for the sparsity and ϵ is given by the background noise. While $p = 0$ is desirable to estimate the sparse signal vector $\mathbf{x}$, $p = 1$ (i.e., basis pursuit) is preferable due to the computational complexity [3], [13]. There are also various low-complexity greedy algorithms [3, Ch. 8] to estimate the sparse vector, $\mathbf{x}$, e.g., the orthogonal matching pursuit (OMP) algorithm [14], [15].

In most CS recovery algorithms, it is important to have a sufficiently large number of measurements or M and a small residual error vector, $\mathbf{n}_{\mathcal{I}}$ (in terms of two-norm). We can show that the solution to (10) (with $p = 1$) becomes $\mathbf{x}$ with a high probability if

$$A \geq C_0 \frac{1}{M} \sum_{m=1}^{M} \frac{1}{\alpha_{k(m)}} \text{ and } M \geq C_1 Q \ln \frac{eN}{Q} \tag{11}$$

where the constants, C_0 and C_1, are independent of the parameters, N, M, and Q. Although it is not presented in this paper (due to the space limitation), the proof is straightforward based on Theorem 9.13 in [12].

B. ML Approach for Attack by Eve

In this section, we consider Eve's attack to estimate $\mathbf{\Psi}$. We will show that it becomes difficult for Eve to perform attack with a fraction of the received signals due to artificial noise.

From (2), the received signal at Eve is given by

$$\mathbf{z} = \mathbf{G}\mathbf{\Psi}\mathbf{x} + \mathbf{G}\mathbf{c} + \mathbf{w} = \mathbf{G}\mathbf{s} + \mathbf{G}\mathbf{c} + \mathbf{w}. \tag{12}$$

Due to the artificial noise, $\mathbf{c}$, Eve would be forced to use the subvector of $\mathbf{z}$, $\mathbf{v} = \mathbf{z}_{\mathcal{I}} = \mathbf{E}\mathbf{x} + \mathbf{w}_{\mathcal{I}}$, where $\mathbf{E}$ is the submatrix of $\mathbf{G}\mathbf{\Psi}$ obtained by taking the rows vectors whose indices are in $\mathcal{I}$. That is, Eve is able to use a fraction of the received signals to estimate $\mathbf{\Psi}$. In addition, since $\mathbf{x}$ is Q-sparse, from $\mathbf{v}$, Eve can only estimate the submatrix of size $M \times Q$ from $\mathbf{\Psi}$ of size $L \times N$. The rows and columns of the submatrix are decided by $\mathcal{I}$ and the support of $\mathbf{x}$, respectively. Note that this estimation attack becomes possible only when $\mathcal{I}$ and $\mathbf{x}$ are known to Eve as a known-plaintext attack to extract the key, $\mathbf{\Psi}$. Thus, for this attack, we assume favorable conditions for Eve. For convenience, the submatrix of $\mathbf{\Psi}$ is denote by $\bar{\mathbf{\Psi}}$. In order to build $\mathbf{\Psi}$, there might be a sufficient number of submatrices of size $M \times Q$ with different realizations[1] of $\mathcal{I}$ and supports of $\mathbf{x}$. For tractable analysis (to easily derive an upper bound on the probability of successful attack later), we consider the following assumption.

A3) L/M and N/Q are integers. Thus, there are disjoint $\frac{L}{M}\frac{N}{Q}$ submatrices.

Under *A3)*, Eve may need at least[2] $\frac{L}{M}\frac{N}{Q}$ observations of the received signals of disjoint submatrices of $\bar{\mathbf{\Psi}}$ to estimate $\mathbf{\Psi}$.

Suppose that Eve has a good computing power to employ the ML approach to estimate a submatrix $\bar{\mathbf{\Psi}}$, which is the optimal one since it minimizes the average error probability, as follows: $\bar{\mathbf{\Psi}}_{\mathrm{ml}} = \mathrm{argmax}_{\bar{\mathbf{\Psi}}} f(\mathbf{v} \mid \bar{\mathbf{\Psi}})$. As shown in [16], an iterative approach can be employed to perform the ML estimation for sparse signal estimation with reasonably moderate complexity. Noting that $\mathbf{v} = A\bar{\mathbf{G}}\bar{\mathbf{\Psi}}\mathbf{1} + \mathbf{w}_{\mathcal{I}}$, where $\mathbf{1}$ is the vector of all 1's and $\bar{\mathbf{G}}$ is the square submatrix of $\mathbf{G}$ obtained by taking the rows and columns corresponding to $\mathcal{I}$, we can have the following expression for the probability of erroneous decision to choose $\bar{\mathbf{\Psi}}' \neq \bar{\mathbf{\Psi}}$ conditioned on $\bar{\mathbf{G}}$:

$$P(\bar{\mathbf{\Psi}} \to \bar{\mathbf{\Psi}}' \mid \bar{\mathbf{G}}) = \Pr\left(||\mathbf{v} - A\bar{\mathbf{G}}\bar{\mathbf{\Psi}}\mathbf{1}||^2 > ||\mathbf{v} - A\bar{\mathbf{G}}\bar{\mathbf{\Psi}}'\mathbf{1}||^2\right) = \mathcal{Q}\left(\frac{||\bar{\mathbf{G}}\mathbf{d}_{\mathcal{I}}||}{\sqrt{2N_0}}\right)$$

where $\mathbf{d}_{\mathcal{I}} = A(\bar{\mathbf{\Psi}} - \bar{\mathbf{\Psi}}')\mathbf{1}$ and $\mathcal{Q}(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^- z^2/2 \mathrm{d}z$. In [17], a lower bound on the Q-function is derived as $\mathcal{Q}(x) \geq C(\kappa) e^{-\frac{\kappa x^2}{2}}$, where $\kappa \geq 1$ and $C(\kappa)$ is a function of κ. Then, a lower bound on the probability of erroneous decision to choose $\bar{\mathbf{\Psi}}'$ is given by

$$P(\bar{\mathbf{\Psi}} \to \bar{\mathbf{\Psi}}') = \mathbb{E}[P(\bar{\mathbf{\Psi}} \to \bar{\mathbf{\Psi}}' | \bar{\mathbf{G}})] \geq C(\kappa)\mathbb{E}\left[e^- \kappa \frac{||\bar{\mathbf{G}}\mathbf{d}_{\mathcal{I}}||^2}{4N_0}\right]. \tag{13}$$

In order to derive the probability of successful attack from (13), let us consider the following assumption.

A4) For each submatrix of $\mathbf{\Psi}$, $\bar{\mathbf{\Psi}}$, only one candidate submatrix $\bar{\mathbf{\Psi}}'$ whose elements are the same as those of $\bar{\mathbf{\Psi}}$ except one is considered.

Note that in *A4)* the other candidates for $\bar{\mathbf{\Psi}}'$ that have more than one element differences are ignored as they may be easily discarded by Eve. Furthermore, for each $\bar{\mathbf{\Psi}}$, only one candidate submatrix $\bar{\mathbf{\Psi}}'$ (of one element difference) is taken into account (although there might be more than one such candidate submatrices). This is a pessimistic assumption for Bob. However, if the measurement matrix is generated from a finite length key, say $\frac{L}{M}\frac{N}{Q}$, we can assume that there might two possible candidates per each $\bar{\mathbf{\Psi}}$. In this case, *A4)* would be reasonable.

Since all the elements of $\mathbf{d}_{\mathcal{I}}$ are zero except one that has value $\pm\frac{2A}{\sqrt{L}}$ under *A4)*, from (13), we have

$$P(\bar{\mathbf{\Psi}} \to \bar{\mathbf{\Psi}}') \geq \bar{P}\left(A, L, \frac{\sigma_g^2}{N_0}\right) \triangleq \max_{\kappa \geq 1} \frac{C(\kappa)}{1 + \frac{\kappa \sigma_g^2 A^2}{L N_0}} \tag{14}$$

where the lower bound is maximized[3] for a tight lower bound. Furthermore, since a correct decision is made if all submatrices are correctly decided under *A3)*, the probability of correct decision or successful attack by Eve is upper bounded as

$$P_{\mathrm{SA}} \leq \left(1 - \bar{P}\left(A, L, \frac{\sigma_g^2}{N_0}\right)\right)^{\frac{L}{M}\frac{N}{Q}}. \tag{15}$$

According to (15), we can see that a large $\frac{N}{Q}$ (or $\frac{L}{M}$) is desirable to decrease the probability of successful attack, P_{SA}. Furthermore, P_{SA} decreases with L. The significance of (15) is that Alice can decide the value of key parameters to ensure a guarantee of secrecy in terms of the probability of successful attack under given Eve's channel conditions (e.g., σ_g^2 and N_0) and parameters (L, N, Q, and so on).

IV. Simulation Results

In this section, we present simulation results under *A1)* with $\sigma_h^2 = \frac{1}{P}$ and CIR length $P = 20$. In addition, the measurement matrix is randomly generated as in *A2)*. To see Eve's performance of estimation attack, we consider *A3)* and *A4)*. Let $F = \frac{\sigma_g^2}{\sigma_h^2}$. The signal-to-noise ratio (SNR) is defined as $\frac{A^2}{N_0}$. At Bob, the OMP algorithm is used to recover the sparse signal $\mathbf{x}$.

Fig. 1 shows the performances at Bob and Eve for various SNRs when $L = 256$, $N = 2\,L$, $Q = 4$, $M = 128$, and $F \in \{1, 10\}$. A sufficiently high SNR is required to have a low probability of decision error at Bob. Unfortunately, a high SNR also provides a better performance at Eve. However, as shown in Fig. 1(b), the probability of successful attack, which is obtained from (15), is sufficiently low at a high SNR. For example, for an SNR of 15 dB, the lower bound on $\bar{P}(A, L, \frac{\sigma_g^2}{N_0})$ is about 0.117 when $F = 10$, which results in $P_{\mathrm{SA}} \leq 1.467 \times 10^{-14}$.

Fig. 2 shows the performances at Bob and Eve for various values of M when $L = 256$, $N = 2\,L$, $Q = 4$, SNR $= 16$ dB, and $F = 1$. Like the SNR, the increase of M improves both Bob's and Eve's[4] performances. Thus, a minimum value of M that can provide a reasonable recovery performance at Bob

[1] Since $\mathcal{I}$ depends on $\{\alpha_l\}$, if Eve observes a sufficiently large number of the received signals, the union of realizations of $\mathcal{I}$'s can be $\{0, \ldots, L-1\}$.

[2] This is the case that each Eve's observation is associated with disjoint $\mathcal{I}$ and disjoint the support of $\mathbf{x}$.

[3] A closed-form expression for the maximum is not available. But, the maximization can be carried out using a numerical approach.

[4] Note that $\bar{P}(A, L, \frac{\sigma_g^2}{N_0})$ is independent of M. But, P_{SA} depends on M, as it increases with M.

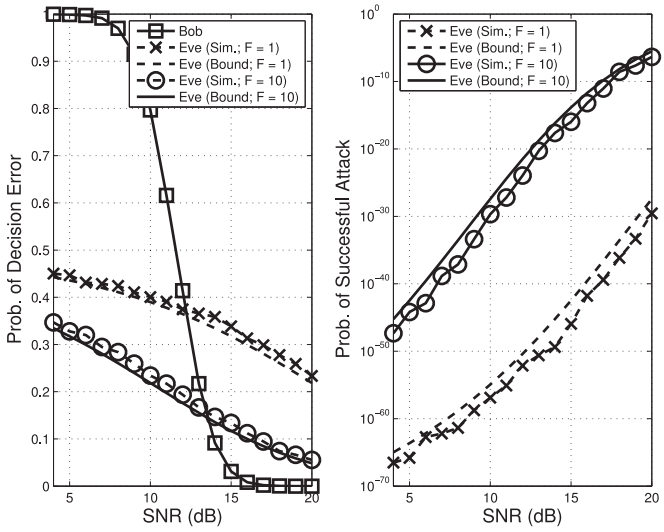

Fig. 1. Performances for various SNRs ($L = 256$, $N = 2\,L$, $Q = 4$, $M = 128$, and $F \in \{1, 10\}$): (a) the probability of decision errors at Bob and Eve; (b) the probability of successful attack by Eve.

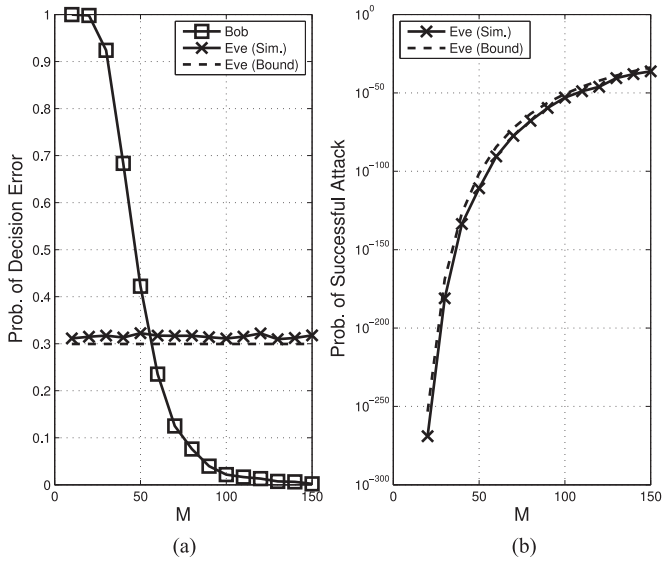

Fig. 2. Performances for various values of M ($L = 256$, $N = 2\,L$, $Q = 4$, SNR $= 16$ dB, and $F = 1$): (a) the probability of decision errors at Bob and Eve; (b) the probability of successful attack by Eve.

would be desirable (e.g., when $M = 120$, the probability of decision error at Bob becomes less than 5×10^{-3}).

In Fig. 3, the impact of Q on the performances at Bob and Eve is shown with $L = 256$, $N = 2\,L$, $M = 128$, SNR $= 16$ dB, and $F = 1$. While more bits can be transmitted as Q increases, the performances can be degraded. Thus, it is desirable to have a small value of Q (e.g., $Q = 4$).

Finally, Fig. 4 shows the performances at Bob and Eve for various values of L when $Q = 4$, $N = 2\,L$, $M = L/2$, SNR $= 16$ dB, and $F = 1$. Since the increase of L results in a lower probability of decision error at Bob and a low probability of correct recover at Eve, it is crucial for Alice and Bob to have

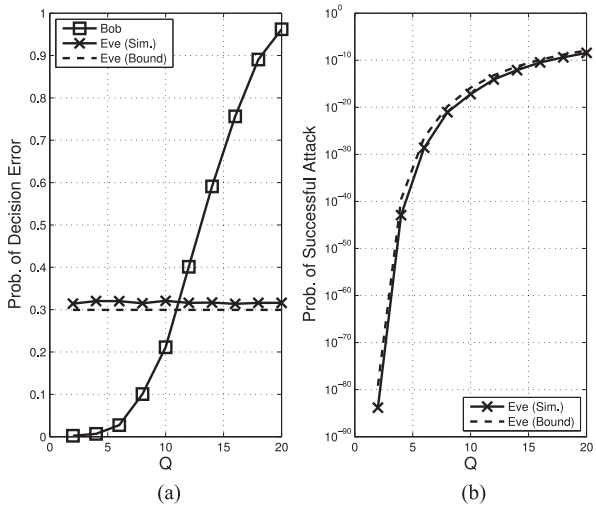

Fig. 3. Performances for various values of Q ($L = 256$, $N = 2\,L$, $M = 128$, SNR $= 16$ dB, and $F = 1$): (a) the probability of decision errors at Bob and Eve; (b) the probability of successful attack by Eve.

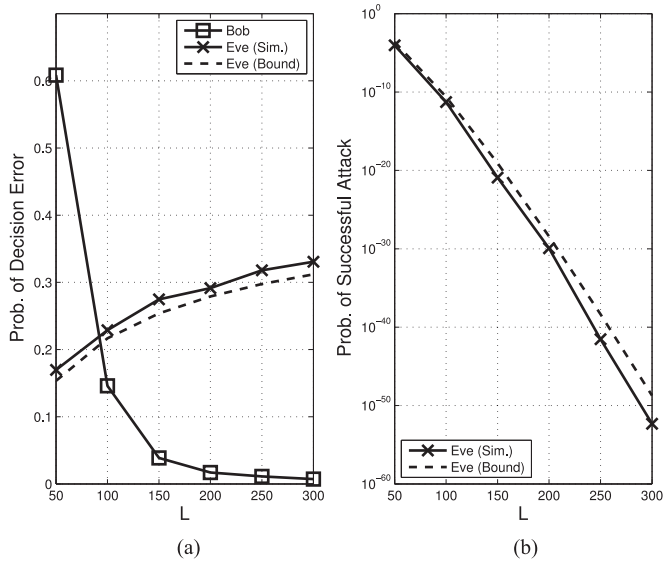

Fig. 4. Performances for various values of L ($Q = 4$, $N = 2\,L$, $M = L/2$, SNR $= 16$ dB, and $F = 1$): (a) the probability of decision errors at Bob and Eve; (b) the probability of successful attack by Eve.

a large L for not only reliable transmissions, but also secure transmissions.

V. Concluding Remarks

In this paper, we considered CS-based encryption for multicarrier systems where artificial noise is transmitted to lower the probability of successful attack by an adversary who may perform attack to estimate the measurement matrix. To minimize the performance degradation at Bob, artificial noise was selectively transmitted in the frequency domain based on known CSI. We derived an upper bound on the probability of successful attack that allows to decide key parameters in order to provide a guarantee of secrecy in terms of the probability of successful attack under certain conditions.

REFERENCES

[1] D. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[2] E. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[3] Y. C. Eldar and G. Kutyniok, *Compressed Sensing: Theory and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[4] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 813–817.

[5] H. Li, R. Mao, L. Lai, and R. C. Qiu, "Compressed meter reading for delay-sensitive and secure load report in smart grid," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 114–119.

[6] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-complexity multiclass encryption by compressed sensing," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2183–2195, May 2015.

[7] R. Dautov and G. R. Tsouri, "Establishing secure measurement matrix for compressed sensing using wireless physical layer security," in *Proc. Int. Conf. Comput., Netw. Commun.*, Jan. 2013, pp. 354–358.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 2515–2534, Jun. 2008.

[9] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations Trends Commun. Inf. Theory*, vol. 5, no. 45, pp. 355–580, 2008.

[10] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[11] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications With MATLAB*. New York, NY, USA: Wiley, 2010.

[12] S. Foucart and H. Rauhut, *A Mathematical Introduction to Compressive Sensing*. New York, NY, USA: Springer, 2013.

[13] E. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.

[14] Y. Pati, R. Rezaiifar, and P. Krishnaprasad, "Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition," in *Proc. Conf. Rec. 27th Asilomar Conf. Signals, Syst. Comput.*, Nov. 1993, vol. 1, pp. 40–44.

[15] G. M. Davis, S. G. Mallat, and Z. Zhang, "Adaptive time-frequency decompositions," *Opt. Eng.*, vol. 33, no. 7, pp. 2183–2191, 1994.

[16] J. Choi, "Sparse signal detection for space shift keying using the Monte Carlo EM algorithm," *IEEE Signal Process. Lett.*, vol. 23, no. 7, pp. 974–978, Jul. 2016.

[17] F. D. Côté, I. N. Psaromiligkos, and W. J. Gross, "A Chernoff-type lower bound for the Gaussian Q-function," Feb. 2012, to be published.