Compressed Sensing-Based Pilot Contamination Attack Detection for NOMA-IoT Communications

Ning Wang, Weiwei Li, Amir Alipour-Fanid, Monireh Dabaghchian, and Kai Zeng

***Abstract*—Non-orthogonal multiple access (NOMA) technology can significantly promote Internet-of-Thing (IoT) networks on spectral efficiency and massive connectivity. However, NOMA-IoT communications are vulnerable to pilot contamination attacks, where the attacker can send the same pilot signals as legitimate IoT users. Most existing countermeasures to this physical-layer threat struggle to adapt to NOMA-IoT networks, in which superimposed signals appear and low-cost IoT devices exist. In this paper, we propose a compressed sensing-based detection scheme to defend against pilot contamination attacks in NOMA-IoT networks. In particular, we present a multiple measurement vector (MMV) compressed sensing model and a security spreading code generation (SSCG) framework to prevent pilot contamination attacks from spoofing base station (BS) in NOMA-IoT networks. Furthermore, to efficiently reconstruct the superimposed signals based on the SSCG-framework, a matching pursuit (MP) multiple response sparse Bayesian learning (MSBL) algorithm, MP-MSBL, is proposed. The security analysis and algorithm complexity of the proposed algorithms are provided. Simulation results evaluate and confirm the effectiveness of the proposed detection schemes. The reconstruction and detection accuracy of pilots can be higher than 99% under different scenarios.**

I. Introduction

Non-orthogonal multiple access (NOMA) is a promising wireless technology that can significantly improve the connectivity of Internet-of-Thing (IoT) networks. Specifically, power-domain NOMA is capable of bringing a new power dimension to perform multiplexing in the existing access domain [1]. It can be regarded as superposing multiple signals into one frequency-time resource block. Via non-orthogonal resource allocation, NOMA can help IoT networks improve spectral efficiency with low transmission latency and signaling cost [2], [3].

Despite its great potential benefits, NOMA-IoT networks are vulnerable to physical-layer threats due to the broadcast characteristics of radio communications. Particularly, pilot contamination attacks pose one of the most serious threats, where the attacker can send the same pilot signals as those of legitimate IoT users to control the channel estimation results [4]. Pilot contamination attacks could lead to severe communication performance degradation in NOMA-IoT networks, and leakage of secret information of legitimate users.

Most existing countermeasures to pilot contamination attacks focus on orthogonal multiple access (OMA) communications, where different users are assigned different frequency-time resource blocks. When it detects that more than one transmitter exists in one frequency-time resource block, these detection mechanisms will raise alarms, for example random pilot-based detection methods [5]–[7]. These detection schemes are hard to be used in NOMA communications, where the received signals at the base station (BS) form a superimposed signal during an orthogonal frequency-time resource block, which is occupied by different transmitters at the same time. Under this case, if these detection methods are directly applied in NOMA-IoT networks, excessive false alarms will be raised since the superimposed signal with multiple transmitters might be seen as pilot contamination attacks.

Pilot contamination attack detection schemes in NOMA communications are studied in [4], [8], where the sparsity of channels in mmWave massive MIMO is exploited. Nevertheless, this detection scheme struggles to be applied to low-cost and low-complexity IoT networks. For many typical IoT networks, IoT devices with a signal antenna in the sub-6GHz band are the main IoT users to support various application scenarios, such as smart farming and environmental monitoring. In this case, these low-cost IoT devices are hard to support mmWave and massive MIMO technologies. As a result, these existing countermeasures to pilot contamination attacks in NOMA communications cannot apply to NOMA-IoT networks.

To tackle these issues, in this paper, we propose a compressed sensing-based detection scheme to defend against pilot contamination attacks in NOMA-IoT networks. A typical NOMA-IoT network with power-domain NOMA technologies is considered, where a user pairing method with a fixed number of users is employed [1]. In particular, the multiple measurement vector (MMV) compressed sensing is employed to form the detection model. To protect the measurement matrix in compressed sensing, a new security spreading code generation (SSCG) framework is presented. Furthermore, inspired by the fast search capability of matching pursuit (MP) algorithms and the high accuracy of multiple response sparse Bayesian learning (MSBL) algorithms, we introduce an MP-

Ning Wang, Weiwei Li, Amir Alipour-Fanid, and Kai Zeng are with the Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA, US 22030 e-mail: ({nwang5, wli25, aalipour, kzeng2}@gmu.edu).

Weiwei Li is also with School of Information and Electrical Engineering, Hebei University of Engineering, Handan, Hebei, China 056001.

Monireh Dabaghchian is with Department of Computer Science, Morgan State University, Baltimore, MD, US 21251, e-mail: (monireh.dabaghchian@morgan.edu).

MSBL algorithm to efficiently reconstruct the superimposed signals under the SSCG-framework. Simulation results validate the effectiveness of the proposed detection schemes, where we show that the reconstruction and detection accuracy can reach to 99% under different scenarios.

The contributions of this work lie in four aspects:

- We propose an MMV compressed sensing model to defend against pilot contamination attacks in NOMA-IoT communications. To the best of our knowledge, this is the first work that utilizes compressed sensing-based coding to counter pilot contamination attacks.
- To avoid the collision of spreading codes, we provide an SSCG-framework to generate random spreading codes in the MMV-compressed sensing model.
- We present a tailored MP-MSBL algorithm for the SSCG-framework to efficiently achieve the reconstruction of the superimposed signals in NOMA-IoT communications.
- We provide system security analysis, computational complexity analysis, and simulation results under various scenarios.

The proposed compressed sensing-based pilot contamination attack detection scheme has the following salient features:

- *Pilot contamination attack detection and channel estimation can be achieved simultaneously.* Based on the compressed sensing theory, the reconstruction of pilot signals and pilot contamination attack detection can be performed simultaneously; hence no additional detection mechanism is required.
- *The proposed scheme is applicable to resource-constrained IoT devices.* The proposed detection scheme can be applied to low-cost and low-complexity IoT devices equipped with only a single antenna. It does not resort to complex hardware at the end users, such as massive MIMO and mmWave radios employed in [4], [8].

The rest of this paper is organized as follows. Section II introduces related works. Section III describes the system model, challenges and motivation. The proposed detection model is presented in Section IV. In Section V, the security analysis and computational complexity are provided. Section VI shows the simulation and evaluation results, and Section VII concludes this paper.

II. Related work

This section will introduce the technical background of this study, including NOMA technologies, pilot contamination attack detection, and compressed sensing.

A. NOMA technologies

NOMA technologies can be categorized into power-domain NOMA and code-domain NOMA. Here, we focus on power-domain NOMA [9], which can serve multiple users in the same frequency-time slot and achieve multiple access by allocating different power levels to different users. For simplification, power-domain NOMA will be called NOMA in the following presentation. NOMA can transmit superposed signals in one frequency-time resource block to significantly improve the spectral efficiency of IoT networks. In general, there are at least two legitimate users' messages in a superimposed signal, at the same time slot or OFDMA subcarrier. In NOMA-IoT networks, based on accurate channel state information (CSI), the BS can extract the signals corresponding to different IoT users by relying on the successive interference cancellation (SIC) technique [1]. Furthermore, according to CSI, IoT users in NOMA-IoT networks are usually grouped based on different pairing schemes to share the same time slot or OFDMA subcarrier, called NOMA group. The IoT users in the NOMA group realize multiple access by allocating different power levels [10]. For communication efficiency, the size of a group is usually fixed, for example two users are considered in a group in [1]. As a result, the security and accuracy of the pilot signal that is employed to estimate CSI are a very crucial issue in NOMA-IoT networks.

B. Pilot contamination attack detection

Pilot contamination attacks were first proposed in [11]. Later, an overview of countermeasures to this attack was provided in [12], [13]. Most existing pilot contamination attack detection schemes mainly consider OMA communications, where an orthogonal frequency-time resource block is occupied by one user. For example, random pilot sequences are designed to detect whether there are other transmitters in the current frequency-time resource block. Random phase-shift keying (PSK) pilot was first proposed in [5], and an improved variation which considers the case of three or more observations was provided in [7]. The other random pilot scheme is based on random frequency shifts [6]. However, these existing pilot contamination attack detection schemes in OMA communications are hard to adapt to NOMA-IoT networks. In NOMA-IoT communications, the orthogonal frequency-time resource block is shared by different users, thus superimposed signals with multiple transmitters are formed at BS. This superimposed signal may cause excessive false alarms in those detection schemes designed for OMA communications.

For NOMA communications, the sparsity of virtual channels has been used to achieve the pilot contamination attack detection, where mmWave and massive MIMO technologies are employed [4], [8]. However, low-cost IoT devices with a single antenna under the sub-6GHz band in NOMA-IoT networks are hard to support massive MIMO and mmWave technologies exploited by these detection schemes.

Different from these existing detection methods, our proposed compressed sensing-based detection scheme can apply to NOMA-IoT communications, where superimposed signals with multiple transmitters appear and low-cost IoT devices exist.

C. Compressed sensing

Compressed sensing is a signal processing technique for efficiently acquiring and reconstructing a signal [14], [15]. A notable feature of compressed sensing is that the computation complexity is very low on the compression side. This feature is very suitable for IoT networks in which there are some low-complexity IoT devices. Compressed sensing has been used on active user detection in NOMA communications such as [16] and [17]. It is worth noting that the proposed compressed sensing-based pilot contamination attack detection is different from these active user detection methods. For active user detection, the signal reconstruction under the fixed measurement matrix is the goal. In our pilot contamination attack detection, however, we aim to protect the security of the measurement matrix in the compressed sensing process. To this end, random spreading codes are proposed to prevent the attacker from gaining the same supports in the measurement matrix as legitimate users.

III. System model and attack model

This section will introduce the system model and the attack model.

A. System model

Here, we consider a typical up-link channel estimation in NOMA-IoT networks under the sub-6GHz band, where BS can serve multiple IoT users at the same frequency-time resource block relying on the power-domain NOMA technique. The BS has multiple antennas and sufficient computing resources. In the network, there are a large number of IoT users with only one single antenna. In the channel estimation phase, IoT users send superimposed pilots to BS, and BS will estimate the corresponding channels based on these superimposed signals [18].

Let y_p denote the received superimposed signal at BS. Formally, the process of pilot transmission in NOMA-IoT communications can be described as follow:

$$y_p = \sum_{m=1}^{M} h_m x_{p,m} + W_p, \tag{1}$$

where $x_{p,m}$ denotes the pilot symbol and h_m indicates the corresponding channel coefficient. $p = 1, .., P$ and P indicates the length of the pilot sequence, $m = 1, .., M$ and $M \geq 2$ denotes the number of legitimate IoT users in one NOMA-IoT group. W_p is the noise and follows the complex Gaussian distribution $CN(0, \sigma_p^2 \mathbf{I})$.

B. Attack model

We assume one or multiple pilot contamination attackers aim to masquerade as legitimate IoT users by modifying its pilot sequence into that of the legitimate user. The location of the pilot contamination attackers in the network is arbitrary. To distort the channel estimation, the pilot contamination attacker might send the same pilot sequence as of the legitimate IoT users during the pilot transmission phase.

As a result, if there are pilot contamination attacks in the NOMA-IoT communication, Eq. (1) will become

$$\tilde{y}_p = \sum_{s=1}^{S} h_s x_{p,s} + W_p, \tag{2}$$

where $s = 1, .., S$, $S > M$ denotes the number of transmitters, and $S - M$ is the number of pilot contamination attackers. The pilot messages from attackers are superimposed into the received signal $\tilde{y}_p$.

As mentioned in Section II-A, generally, the size of the NOMA group is fixed, i.e., the number of legitimate IoT users related to one superimposed signal is fixed. Thus, the problem of pilot contamination attack detection becomes how to distinguish the superimposed signal y_p from $\tilde{y}_p$, where the number of transmitters is different. Based on compressed sensing, spreading codes can be employed to achieve active user detection in NOMA-IoT networks [16], [17], in which the spreading codes are fixed and preassigned to different users. However, one the other hand, if the spreading codes are random and specific to different transmitters, the compressed sensing process can reveal the number of transmitters of the superimposed signal. Based on this observation, we can develop a novel compressed sensing-based pilot contamination attack detection scheme.

IV. Compressed sensing-based detection scheme

In this section, we will introduce the proposed pilot contamination attack detection scheme based on compressed sensing, involving the motivation and challenges of this study, MMV-compressed sensing model, SSCG-framework, and MP-MSBL.

A. Motivation and challenges

Inspired by the compressed sensing theory [19], the channel estimation depending on superimposed pilot signals in NOMA communications can be transformed into an MMV model. If we can design a secure spreading coding strategy for the pilot sequence of legitimate IoT users, all transmitters for the superimposed pilot signal can be detected by the compressed sensing reconstruction process at BS. It is worth noting that the spreading codes introduced in this study are different from the spreading codes in the code division multiple access (CDMA) [20]. The spreading codes in CDMA are one of the orthogonal division codes, while the spreading codes based on the compressed sensing are one of the non-orthogonal division codes. As a result, if the number of transmitters (i.e., S) is larger than the size of the NOMA group (i.e., M), pilot contamination attacks can be flagged. Besides, according to the communication mechanism of NOMA, the IoT users in the network must send their pilots to a BS during the channel estimation phase, so that the BS can estimate the CSI of different IoT users and extract the corresponding message from the superimposed signals.

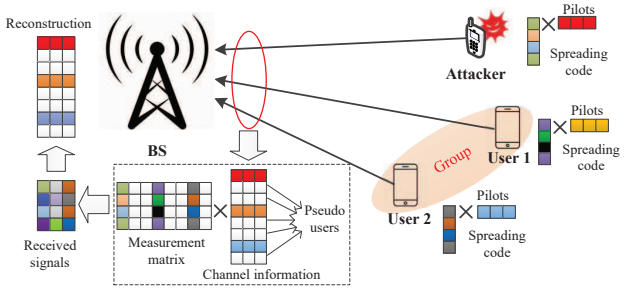


Fig. 1. Compressed sensing-based pilot contamination attack detection.

However, to achieve a desirable pilot contamination attack detection in the NOMA-IoT network based on compressed sensing, we have to tackle two issues:

1) *Ensure the security and availability of the spreading codes.* In the compressed sensing reconstruction algorithms, the spreading codes of IoT users are used to separate the different transmitters. If the spreading code is preassigned to IoT users in advance, it is easy to reveal to pilot contamination attackers. This will lead to the failure of pilot contamination attack detection. For this issue, a reasonable solution is that IoT users can generate a set of random and unpredictable spreading codes. Furthermore, these spreading codes must meet the limitation condition in the compressed sensing theory, such as the Restricted Isometry Property (RIP) condition [14], [15]. As a result, how to design these random spreading codes (i.e., measurement matrix) is a challenge.
2) *Efficiently reconstruct the superimposed signal.* As mentioned above, to protect the privacy of IoT users, the spreading codes need to be randomly generated. Under this case, random spreading codes will lead to a very large measurement matrix in the reconstruction phase, since all possible forms of the random spreading codes should be considered. Thus, it is an open problem to efficiently reconstruct the superimposed signals based on a huge measurement matrix.

B. MMV-compressed sensing model for NOMA-IoT

To tackle these challenges, we propose a compressed sensing-based pilot contamination attack detection in NOMA-IoT communications. An SSCG-framework is presented to generate the random spreading codes, and an MP-MSBL algorithm is introduced to efficiently reconstruct the superimposed signals.

Based on the compressed sensing theory, when the channels of legitimate IoT users are sparse, the estimation of the superimposed pilot signal at BS can be seen as the reconstruction of the compressed signals based on an MMV model [16] [17]. To achieve this, a pseudo transmitter with channel gain 0 is introduced to expand the channel cardinality. This pseudo-user is not a real user and just to improve the sparsity of legitimate IoT users in the network. Fig. 1 illustrates the pilot transmission and reconstruction process based on compressed sensing. In this example, the number of IoT users in the NOMA group is 2, the length of pilots is 3, and the size of the spreading code is 4. Moreover, there is a pilot contamination attacker and five pseudo users in the network. As shown in Fig. 1, with different spreading codes, the pilots of all IoT users are transmitted to BS. Because the channel gain of pseudo users is 0, the superimposed signal received by BS just contains the signals from two legitimate users and one pilot contamination attacker. The BS can reconstruct the messages corresponding to different users by using compressed sensing reconstruction algorithms based on the fact that the spreading codes are different between different users.

Formally, let L be the number of pseudo users, thus Eq. (1) will become

$$\mathbf{y}_p = \sum_{k=1}^{K} h_k \mathbf{s}_{p,k} x_{p,k} + \mathbf{w}_p, \tag{3}$$

where $\mathbf{s}_{p,k}$ is the spreading code for the p-th pilot of the k-th user and its size is N. $L >> M$, $K = L + M$, and K is the sum of pseudo users and real users, where the real users include legitimate IoT users and potential attackers. ${\mathbf{w}_p}^{1\times K}$ is the noise vector, $x_{p,k}$ indicates the p-th pilot of the k-th user, and $\mathbf{s}_{p,k}$ denotes the spreading code for the p-th pilot of the k-th user.

For simplicity, we can set the pilot symbol $x_{p,k}$ to 1. Thus, when considering all of the users and pilots at BS, Eq. (3) will become

$$\mathbf{Y} = \mathbf{A}\mathbf{H} + \mathbf{W}, \tag{4}$$

where $\mathbf{Y}$ is the superimposed signal of all users at BS, and $\mathbf{Y} = [\mathbf{y}_1, ..., \mathbf{y}_p, .., \mathbf{y}_P]^{N\times P}$ where $\mathbf{y}_p = [y_{1,p}, ..., y_{N,p}]^T$. $\mathbf{A} = \left[\mathbf{S}^{(1)}, ..., \mathbf{S}^{(k)}, ..., \mathbf{S}^{(K)}\right]^{N\times K}$ is the spread pilot matrix, where $\mathbf{S}^{(k)} = \mathbf{s}_{p,k} \cdot x_{p,k}$. $\mathbf{H} = [\mathbf{h}_1, ..., \mathbf{h}_p, ..., \mathbf{h}_P]^{K\times P}$ indicates the matrix of channel coefficients, and $\mathbf{h}_p = [h_1, h_2, ..., h_K]^T$. $\mathbf{W}^{N\times P}$ denotes the noise matrix.

For all NOMA-IoT users including real and pseudo users, each row of $\mathbf{H}$ contains the channel coefficients corresponding to each user. Due to the existence of the pseudo users, $\mathbf{H}$ is sparse, i.e., all rows are zeros except those real users. Thus, since all columns of $\mathbf{H}$ have the same sparse structure, the detection of $\mathbf{H}$ given $\mathbf{Y}$ can be seen as an MMV problem, where $\mathbf{A}$ can be seen as the measurement matrix in compressed sensing and $\mathbf{Y}$ is the compressed signal received by BS [16]. Furthermore, to detect all real transmitters, the measurement matrix $\mathbf{A}$ is designed as a random matrix that can be randomly generated to prevent the collision of spread codes between different users. To achieve this, an SSCG-framework is introduced as follows.

C. SSCG-framework

The column of the measurement matrix $\mathbf{A}^{N\times K}$ contains the spreading code corresponding to each user. To avoid code collision, the generation of spreading codes is designed as a

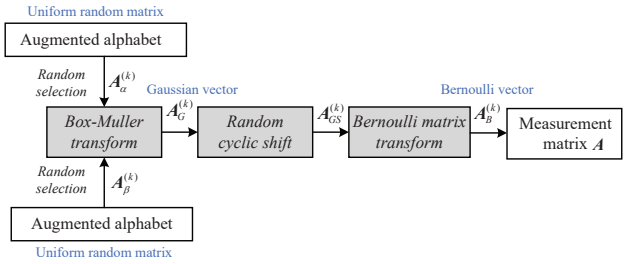


Fig. 2. Generation of measurement matrix.

process of random selection and transformation. Firstly, two vectors following uniform distribution are randomly selected from two different augmented alphabets. Based on the Box-Muller transform, the two vectors can be transformed into a Gaussian random vector [21]. Then, through random circulant shifting and Bernoulli transforming, the random spreading codes for IoT users can be generated. The flow chart of the measurement matrix generation is shown in Fig. 2.

Formally, let $\mathbb{A}_\alpha$ and $\mathbb{A}_\beta$ denote two augmented alphabets, where $\mathbb{A}_\alpha = \{\mathbf{A}_{\alpha,1}, ..., \mathbf{A}_{\alpha,i}, ..., \mathbf{A}_{\alpha,I}\} \in \mathbb{R}^{N\times I}$ and $\mathbb{A}_\beta = \{\mathbf{A}_{\beta,1}, ..., \mathbf{A}_{\beta,j}, ..., \mathbf{A}_{\beta,J}\} \in \mathbb{R}^{N\times J}$. The elements of the augmented alphabets follow the uniform distribution. Assume $\mathbf{A}_{\alpha,i} = [A_{\alpha,i,1}, ..., A_{\alpha,i,n}, ..., A_{\alpha,i,N}]^{1\times N}$ where $A_{\alpha,i,n} \sim U[0,1]$ and $\mathbf{A}_{\beta,j} = [A_{\beta,j,1}, ..., A_{\beta,j,n}, ..., A_{\beta,j,N}]^{1\times N}$ where $A_{\beta,j,n} \sim U[0,1]$. For the p-th pilot of the k-th user, two vectors $\mathbf{A}_{\alpha,i}^{(k)}$ and $\mathbf{A}_{\beta,j}^{(k)}$ can be randomly selected from the augmented alphabets $\mathbb{A}_\alpha$ and $\mathbb{A}_\beta$, respectively, where $i \in \{1, ..., I\}$ and $j \in \{1, ..., J\}$.

Then, $\mathbf{A}_{\alpha,i}^{(k)}$ and $\mathbf{A}_{\beta,j}^{(k)}$ can be transformed into a Gaussian random vector $\mathbf{A}_G^{(k)}$ based on Box-Muller transform:

$$\begin{aligned} \mathbf{A}_G^{(k)} &= \sqrt{-2\ln \mathbf{A}_{\alpha,i}^{(k)}}\cos(2\pi \mathbf{A}_{\beta,j}^{(k)}) \\ &\quad or \\ \mathbf{A}_G^{(k)} &= \sqrt{-2\ln \mathbf{A}_{\beta,j}^{(k)}}\cos(2\pi \mathbf{A}_{\alpha,i}^{(k)}). \end{aligned} \tag{5}$$

Next, the items of Gaussian random vector $\mathbf{A}_G^{(k)} = [A_{G,1}^{(k)}, ..., A_{G,i}^{(k)}, ..., A_{G,N}^{(k)}]^{1\times N}$ can be randomly circulant shifted, i.e.,

$$\mathbf{A}_{GS}^{(k)} = [A_{G,\theta+1}^{(k)}, ..., A_{G,N}^{(k)}, A_{G,1}^{(k)}, ..., A_{G,\theta}^{(k)}]^{1\times N}, \tag{6}$$

where parameter θ is a non-negative integer random variable and $\theta \in [0, N]$.

Thus, the Gaussian random vector $\mathbf{A}_{GS}^{(k)}$ can be transformed into a Bernoulli vector, $\mathbf{A}_B^{(k)} = [A_{B,1}^{(k)}, ..., A_{B,i}^{(k)}, ..., A_{B,N}^{(k)}]^{1\times N}$ based on

$$A_{B,i}^{(k)} = \begin{cases} -1 & , \quad A_{GS,i}^{(k)} \in [L_1, L_2) \\ 1 & , \quad A_{GS,i}^{(k)} \in [L_2, L_3] \end{cases} \tag{7}$$

where $i = 1, ..., N$, $L_1 = \min(\mathbf{A}_{GS}^{(k)})$, $L_3 = \max(\mathbf{A}_{GS}^{(k)})$, and $L2 = L_1 + \frac{1}{2}(L_3 - L_1)$.

Thus, we can obtain the measurement matrix after collecting all of the spreading codes for all users,

$$\mathbf{A} = [\mathbf{A}_B^{(1)}, ..., \mathbf{A}_B^{(K)}]^{N\times K}. \tag{8}$$

As a result, the overhead of IoT users with SSCG framework includes the transformation from $\mathbf{A}_{\alpha,\beta}^{(k)}$ to $\mathbf{A}_B$ and the storage of $\mathbb{A}_\alpha$ and $\mathbb{A}_\beta$. Generally speaking, storing two matrices with low dimensions is not a significant storage burden for IoT devices (e.g., as the dimension of the matrix is 100×10, the requirement of storage space is around 90Kb). Moreover, the computing complexity of the transformation is low and we will provide a more detail analysis in Section V.

D. MP-MSBL reconstruction and detection algorithm

In general, two kinds of algorithms can address the problem of signal reconstruction in MMV-compressed sensing: sparse Bayesian learning (e.g., MSBL algorithms) [22] and iterative greedy algorithms (e.g., MP algorithms) [23]. These algorithms cannot be directly utilized in our SSCG-framework, because the measurement matrix exploited in the reconstruction process will be very large at the BS. MSBL algorithms can accurately reconstruct the compressed MMV signal, however, its computing complexity is very high when considering a large measurement matrix. MP algorithms can achieve a fast reconstruction process, but its reconstruction accuracy is hardly as good as MSBL algorithms [22].

To tackle these issues, inspired by the fast search capability of MP algorithms, we propose an improved MSBL algorithm, called MP-MSBL reconstruction algorithm. The basic idea is that the MP algorithm is exploited to search for the most relevant supports in the measurement matrix used in the reconstruction process. Then, these supports are collected to form a new measurement matrix. Thus, the MSBL algorithm can be used to recover the compressed signal based on this new measurement matrix.

Formally, let $\mathbf{A}_E^{N\times M}$ denote the extension of $\mathbf{A}^{N\times K}$, where $\mathbf{A}_E$ indicates all possibilities of $\mathbf{A}$. According to Section IV-C, we have $M = 2 \times I \times J \times N$. In the MP-MSBL algorithm, MP algorithm is employed to search the supports (i.e., column vectors) that best match the compressed signal $\mathbf{Y}$ in the extension measurement matrix $\mathbf{A}_E^{N\times M}$. Searching the column vectors of $\mathbf{A}_E$ can be seen as a maximization problem,

$$\max_t |\mathbf{A}_{E,t} \odot \mathbf{r}_{l-1}|, \tag{9}$$

where $\odot$ denotes the inner product operation, $\mathbf{A}_{E,t}$ indicates the column of $\mathbf{A}_E$, $t = 1, 2, ..., M$, and $\mathbf{r}_{l-1}$ denotes the residual whose initialization is the raw signal $\mathbf{Y}$.

We can collect all signal-related column vectors by updating the residuals,

$$\mathbf{r}_l = (\mathbf{I} - \mathbf{P}), \tag{10}$$

where $\mathbf{P} = \mathbf{A}_E(c)(\mathbf{A}_E(c)'\mathbf{A}_E(c))^{-1}\mathbf{A}_E(c)'$ denotes the projection onto the linear space spanned by the elements of $\mathbf{A}_E(c)$, where $\mathbf{A}_E(c)$ indicates the subset of columns of $\mathbf{A}_E$ and $c = c \cup \{t\}$. $\mathbf{I}$ indicates identity matrix.

When the stopping condition is achieved, i.e., the residual is less than a parameter λ, we can obtain $\mathbf{A}_E(c)$ that is a subset of columns of $\mathbf{A}_E$. Using $\mathbf{A}_E(c)$ as the measurement matrix in the reconstruction process, we can exploit MSBL algorithm to effectively reconstruct the compressed signal Y under MMV model, i.e.,

$$\mathbf{X} = \mathrm{MSBL}\left(\mathbf{Y}, \mathbf{A}_E(c)\right), \tag{11}$$

where $\mathbf{X}$ is the reconstruction of the compressed signal $\mathbf{Y}$, and $\mathrm{MSBL}(\cdot)$ denotes the MSBL reconstruction algorithm [22].

The rows of the reconstruction signal $\mathbf{X}$ contain channel information which can be used to estimate the channel states for different users. The number of row vectors indicates the number of real transmitters. Thus, if the BS can detect the number of transmitters S and find that S is larger than the size of the group M, pilot contamination attacks will be flagged. Algorithm 1 shows the pseudo-code of the proposed MP-MSBL algorithm.

Algorithm 1 MP-MSBL algorithm

Initialization: $\mathbf{r}_0 = \mathbf{Y}$, $\mathbf{A}_E(c) = \emptyset$ and iteration counter $i = 1$

1) **While** $\mathbf{r}_i > \lambda$
2) Find the column vectors $\mathbf{A}_{E,t}$ based on Eq. (9);
3) Add $\mathbf{A}_{E,t}$ to the set of $\mathbf{A}_E(c)$, $c_i = c_{i-1} \cup \{t\}$;
4) Update residual $\mathbf{r}_i$ according to Eq. (10);
5) Update $i = i + 1$;
6) **End**
7) Extract $\mathbf{A}_E(c)$ as the measurement matrix.
8) Execute MSBL algorithm to reconstruct $\mathbf{X}$ based on Eq. (11).
9) **If** $S = M$
10) No attack.
11) **Else**
12) Raise alarm.
13) **End If**

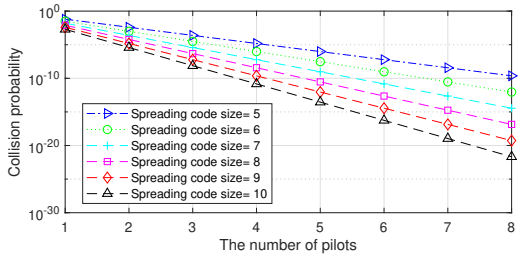
V. Security Analysis and Computational Complexity

This section will provide the security analysis and computational complexity of the proposed algorithms.

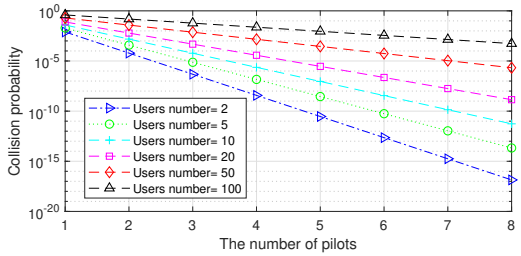
A. Security analysis

According to the attack model shown in Section III-B, the attacker can superimpose its pilot signal on the received signal at BS. If the spreading codes are random and different users use different spreading codes, the reconstruction process of compressed sensing can distinguish the pilot contamination attack case from the normal case. However, if the pilot contamination attacker gains the same spreading codes as any legitimate user, this compressed sensing-based detection scheme will fail, since the compressed sensing technique cannot recognize the difference of signals with the same spreading codes.

In this section, we will analyze the security of the proposed detection. According to the SSCG-framework, the pilot contamination attacker has two ways to obtain the same spreading code as legitimate IoT users:



(a) Under different spreading code sizes .



(b) Under different NOMA-IoT user group sizes.

Fig. 3. Collision probability. (a) The number of users is fixed, i.e., $M = 2$; (b) The spreading code size is fixed, i.e., $N = 8$.

1) The pilot contamination attacker guesses the Gaussian vector $\mathbf{A}_{GS}^{(k)}$ based on Eq. (6) to gain the corresponding spreading codes.
2) The pilot contamination attacker directly guess the Bernoulli vector $\mathbf{A}_{B}^{(k)}$.

For the first attack method, since the spreading code is randomly selected from $\mathbb{A}_\alpha$ and $\mathbb{A}_\beta$, according to Section IV-C, the correct probability of this guess (i.e., the collision probability) is $1/M$ where $M = 2 \times I \times J \times N$. If we assume a set of reasonable parameters, $I = 100$, $J = 100$ and $N = 8$, the collision probability is equal to one in 160,000. Moreover, this probability will be further decreased as the spreading code size increases, as shown in Fig. 3(a). For example, if there are 8 pilots, the collision probability can reach 10^{-10} even when the size of the spreading code is 5.

For the second attack method, the successful probability of pilot contamination attackers is also very low, and the collision probability of spreading codes under this situation is illustrated in Fig. 3(b). We can see that as the number of pilots increases, the collision probability significantly decreases. For instance, the collision probability is around 10^{-3} even there are 100 users in a NOMA group when we collect 8 pilot signals. As there are two legitimate IoT users in a NOMA group, the collision probability can reach 10^{-16}.

In short, based on the analysis above, PCA attackers would find it difficult to correctly gain the spreading codes of the legitimate users in the proposed SSCG-framework.

B. Computational complexity analysis

For IoT users, according to Section IV-C, the core algorithm is Eq. (5) in the proposed SSCG-framework. Thus, the

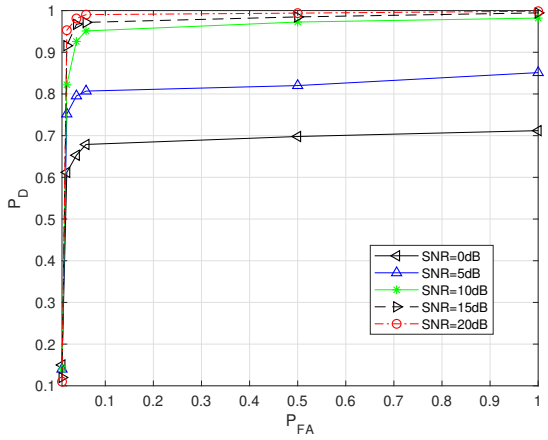


Fig. 4. Compressed sensing-based pilot contamination attack detection with different SNRs.

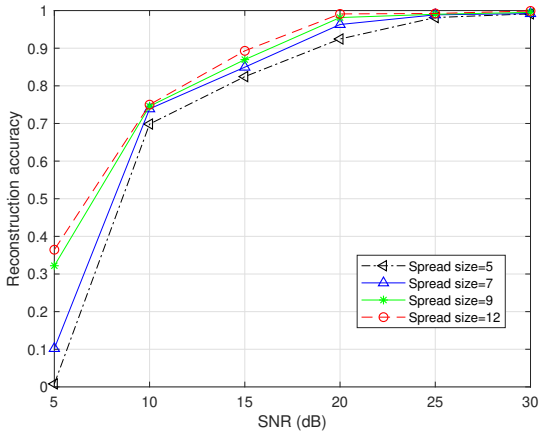


Fig. 5. Compressed sensing-based pilot contamination attack detection with different spreading codes.

computational complexity can be represented as $O(N)$ where N is the size of the spreading code. In other words, SSCG-framework is a lower complexity algorithm that can adapt to IoT devices.

For BS, the computational complexity of the proposed MP-MSBL is $O(N^2V)$, where N is the size of the spreading code and V is the number of candidate basis vectors [22]. The MP-MSBL is more complex compared with SSCG-framework, but BS is generally more powerful and has sufficient computing resources.

VI. Simulation Results

In this section, we will present simulation results based on Monte Carlo experiments, involving the effectiveness of PCA detection and pilot reconstruction, the evaluation of MP-MSBL, and the validation of the proposed scheme for multiple users under various conditions. We used MATLAB to evaluate the Monte Carlo experiment data on a general computer, which operates on a 64-bit system with a 16G memory and an i7-7700 CPU.

A. Effectiveness of detection scheme and pilot reconstruction

In Fig. 4, the detection performance of the proposed scheme is presented by a receiver-operating-characteristic (ROC) curve, where P_D denotes the detection rate and P_{FA} is the false alarm rate. Without loss of generality, there are two legitimate users and one pilot contamination attacker in a NOMA-IoT group, the parameters of SSCG-framework are $I = 100$, $J = 100$, the spreading code size is 7, and the number of Monte Carto simulations is 10,000. We can see that the detection performance gets better as the SNR increases. For example, when SNRs are higher than 10dB, the detection rate can exceed 95% and the false alarm rate is 0.05. Higher SNR means less interference in the MMV-compressed sensing model, and that is helpful for channel reconstruction and pilot contamination attack detection.

In order to evaluate the channel estimation under different conditions, we introduce reconstruction accuracy (RC) as a performance criterion, given by

$$\mathrm{RC} = \frac{CR}{AR} \tag{12}$$

where AR is the number of all reconstruction pilots, and CR is the number of correctly reconstruction pilots.

Fig. 5 shows the effect of the noise on the reconstruction of the channel estimation. Under the same SNR condition, using more spreading codes can improve the reconstruction performance of the channel. For instance, when the spreading code sizes are $\{5, 7, 9\}$, the reconstruction accuracy is less than 90%. As SNR=15dB, the reconstruction accuracy can reach 90% as the size of the spreading code is 12. The reason behind this phenomenon lies in that when the number of IoT users is fixed, the larger spreading code size implies a higher sparsity of the MMV-compressed sensing model. Thus, the increase of the spreading code size can help CS reconstruction algorithm improve the reconstruction accuracy.

It is worth noting that the study of the signal reconstruction in compressed sensing under noisy environments is beyond the scope of this paper. Here, the anti-noise ability in the proposed MP-MSBL reconstruction algorithm mainly depends on the MSBL algorithm. Meanwhile, we notice that pilot contamination attack detection is easy to implement when the channel is correctly reconstructed. To simplify the analysis, we directly use reconstruction accuracy to evaluate the MP-MSBL algorithm as follows.

B. Evaluation of MP-MSBL algorithm

The evaluation of the proposed MP-MSBL algorithm will emphasize operation efficiency and reconstruction performance. The competition algorithms include three different popular compressed sensing reconstruction algorithms: orthogonal matching pursuit (OMP) [24], MSBL algorithm [22], and basis pursuit (BP) algorithm [25].

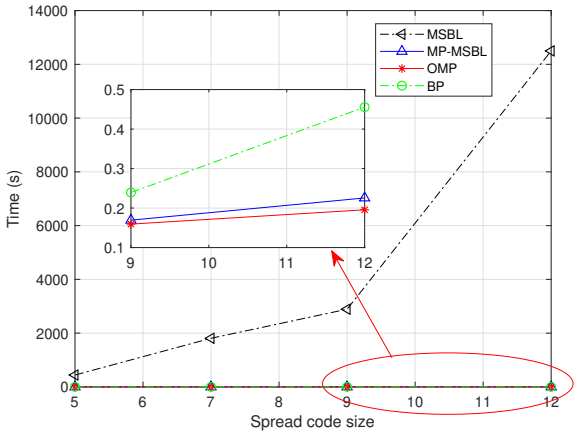


Fig. 6. The operation efficient of different reconstruction algorithms under different spread code sizes.

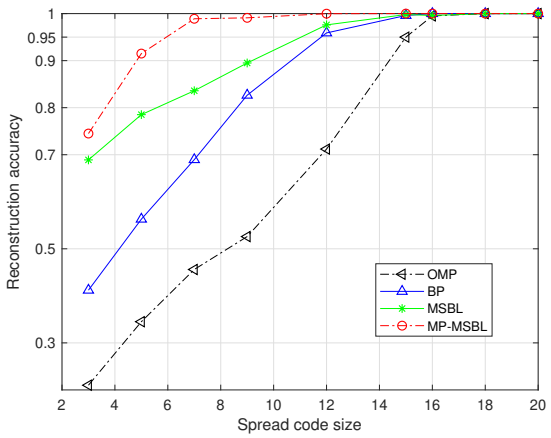


Fig. 7. Reconstruction accuracy under different reconstruction algorithms.

Fig. 6 demonstrates the operation efficiency of the different algorithms for the same detection data. Here, the size of the NOMA group is 2, the number of the pilots is 3, and the parameters of SSCG-framework are $I = 100$ and $J = 100$, respectively. In addition, in this experiment, the noise level is SNR=20dB, the considered spreading code sizes are $N = \{5, 7, 9, 12\}$, and the number of Monte Carto simulations is 10,000. From Fig. 6, we notice that the execution time of the proposed scheme MP-MSBL algorithm doesn't remarkably increase as the spread code size gets larger. The operation efficiency of MP-MSBL is close to that of OMP, where the required time is around 0.2s when the size of the spread code is 12. In contrast, under the same environment, the required time of original MSBL is significantly impacted by the size of the spread code. For example, when the size of the spread code is 9, the execution time of MSBL requires 3000s approximately.

Fig. 7 illustrates the reconstruction accuracy under different algorithms. We can see that MP-MSBL can achieve a higher reconstruction accuracy compared with other algorithms when

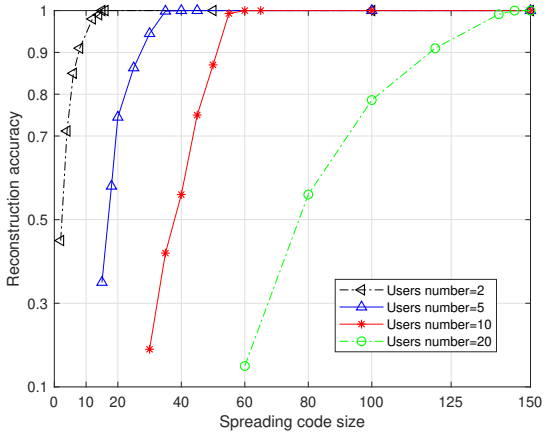


Fig. 8. Reconstruction accuracy under multiple NOMA-IoT users.

considering the same size of the spreading codes. For instance, when the reconstruction accuracy of MP-MSBL is close to 99%, the number of the required spreading codes is around 7. To achieve the same reconstruction accuracy, BP and MSBL need 15 spreading codes and OMP requires 16 spreading codes, respectively. As a result, Fig. 6 and Fig. 7 imply that the proposed reconstruction algorithm MP-MSBL can beat the popular algorithms, i.e., OMP, BP and MSBL, when considering both operation efficiency and reconstruction performance under the SSCG-framework.

C. Effectiveness under multiple NOMA-IoT users

In Fig. 8, we study the reconstruction performance of the proposed scheme with varying numbers of NOMA-IoT users. Here, the sizes of the NOMA IoT user group are $M = \{2, 5, 10, 20\}$, the number of the pilots is 2, and the parameters of SSCG-framework are $I = 100$ and $J = 100$, respectively. In addition, in this experiment, the noise level is SNR=20dB, the considered spreading code sizes are from 2 to 150, and the number of Monte Carto simulations is 10,000. Form Fig. 8, we can see that the NOMA group with smaller user size requires fewer spreading codes to achieve a desirable reconstruction performance. For example, when the number of users is 2, the reconstruction accuracy can exceed 90% using only 8 spreading codes. To achieve the same reconstruction accuracy, more than 50 spreading codes are required when the group size is 10. Meanwhile, we also notice that if we can use enough spreading codes, a NOMA group with a number of IoT users can also get a better reconstruction performance. For instance, when the group size is 20, the reconstruction accuracy can reach 99% with 130 spreading codes. Hence, pilot contamination attack detection can be achieved in the NOMA-IoT with a large user group if the size of the spreading code is acceptable.

VII. Conclusion

In this paper, we studied pilot contamination attack detection in NOMA-IoT communications. The MMV-compressed sens-

ing model was exploited to detect pilot contamination attacks. To protect the privacy of the IoT users, we proposed an SSCG-framework to randomly generate the spreading codes. An MP-MSBL algorithm was presented to handle the reconstruction of superimposed signals under the SSCG-framework. This compressed sensing detection scheme can achieve channel estimation and attack detection simultaneously, handle the superimposed signals in NOMA communications, and adapt to low-cost and low-complexity IoT networks. The security of the system was demonstrated and the computational complexity of the proposed algorithm was provided. Simulation results verified the effectiveness of the proposed detection schemes, where the reconstruction and detection accuracy can reach 99% under different scenarios.

REFERENCES

[1] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5g," *IEEE communications surveys & tutorials*, vol. 20, no. 3, pp. 2294–2323, 2018.

[2] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive non-orthogonal multiple access for cellular iot: Potentials and limitations," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55–61, 2017.

[3] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical layer security of 5g wireless networks for iot: Challenges and opportunities," *IEEE Internet of Things Journal*, 2019.

[4] N. Wang, L. Jiao, and K. Zeng, "Pilot contamination attack detection for noma in mm-wave and massive mimo 5g communication," in *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, Conference Proceedings, pp. 1–9.

[5] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive mimo," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*. IEEE, 2013, pp. 13–18.

[6] W. Zhang, H. Lin, and R. Zhang, "Detection of pilot contamination attack based on uncoordinated frequency shifts," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2658–2670, 2018.

[7] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, and F. Rusek, "Detection of active eavesdroppers in massive mimo," *2014 Ieee 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (Pimrc)*, pp. 585–589, 2014. [Online]. Available: WOS:000392729300113

[8] N. Wang, L. Jiao, A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for noma in 5g mm-wave massive mimo networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1363–1378, 2019.

[9] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5g networks: Research challenges and future trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, 2017.

[10] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5g nonorthogonal multiple-access downlink transmissions," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6010–6023, 2016.

[11] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell tdd systems," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2640–2651, 2011.

[12] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, 2015.

[13] O. Elijah, C. Y. Leow, T. A. Rahman, S. Nunoo, and S. Z. Iliya, "A comprehensive survey of pilot contamination in massive MIMO 5g system," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 905–923, 2016.

[14] N. Wang, T. Jiang, W. Li, and S. Lv, "Physical-layer security in internet of things based on compressed sensing and frequency selection," *IET Communications*, vol. 11, no. 9, pp. 1431–1437, 2016.

[15] W. Li, T. Jiang, and N. Wang, "Compressed sensing based on the characteristic correlation of ecg in hybrid wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 11, no. 10, p. 325103, 2015.

[16] A. Quayum, H. Minn, and Y. Kakishima, "Non-orthogonal pilot designs for joint channel estimation and collision detection in grant-free access systems," *IEEE Access*, vol. 6, pp. 55 186–55 201, 2018.

[17] Z. Zhang, X. Wang, Y. Zhang, and Y. Chen, "Grant-free rateless multiple access: A novel massive access scheme for internet of things," *IEEE Communications Letters*, vol. 20, no. 10, pp. 2019–2022, 2016.

[18] K. Upadhya, S. A. Vorobyov, and M. Vehkapera, "Superimposed pilots are superior for mitigating pilot contamination in massive mimo," *IEEE Transactions on Signal Processing*, vol. 65, no. 11, pp. 2917–2932, 2017.

[19] Z. Gao, L. Dai, S. Han, I. Chih-Lin, Z. Wang, and L. Hanzo, "Compressive sensing techniques for next-generation wireless communications," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 144–153, 2018.

[20] S. Moshavi, "Multi-user detection for ds-cdma communications," *IEEE communications magazine*, vol. 34, no. 10, pp. 124–136, 1996.

[21] A. Fetanat, G. Shafipour, and F. Ghanatir, "Box-muller harmony search algorithm for optimal coordination of directional overcurrent relays in power system," *Scientific Research and Essays*, vol. 6, no. 19, pp. 4079–4090, 2011.

[22] D. P. Wipf and B. D. Rao, "An empirical bayesian strategy for solving the simultaneous sparse approximation problem," *IEEE Transactions on Signal Processing*, vol. 55, no. 7, pp. 3704–3716, 2007.

[23] W. Dai and O. Milenkovic, "Subspace pursuit for compressive sensing signal reconstruction," *IEEE transactions on Information Theory*, vol. 55, no. 5, pp. 2230–2249, 2009.

[24] A. Kulkarni and T. Mohsenin, "Low overhead architectures for omp compressive sensing reconstruction algorithm," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 6, pp. 1468–1480, 2017.

[25] P. R. Gill, A. Wang, and A. Molnar, "The in-crowd algorithm for fast basis pursuit denoising," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4595–4605, 2011.