Low-rank Matrix Completion based Malicious User Detection in Cooperative Spectrum Sensing

Zhijin Qin, Yue Gao, Mark D. Plumbley, Clive G. Parini, Laurie G. Cuthbert
Electronic Engineering and Computer Science
Queen Mary University of London
London, United Kingdom
{zhijin.qin,yue.gao,mark.plumbley,c.g.parini,laurie.cuthbert}@eecs.qmul.ac.uk

***Abstract*—In a cognitive radio (CR) system, cooperative spectrum sensing (CSS) is the key to improving sensing performance in deep fading channels. In CSS networks, signals received at the secondary users (SUs) are sent to a fusion center to make a final decision of the spectrum occupancy. In this process, the presence of malicious users sending false sensing samples can severely degrade the performance of the CSS network. In this paper, with the compressive sensing (CS) technique being implemented at each SU, we build a CSS network with *double sparsity* property. A new malicious user detection scheme is proposed by utilizing the adaptive outlier pursuit (AOP) based low-rank matrix completion in the CSS network. In the proposed scheme, the malicious users are removed in the process of signal recovery at the fusion center. The numerical analysis of the proposed scheme is carried out and compared with an existing malicious user detection algorithm.**

Keywords: cognitive radio, cooperative spectrum sensing, malicious users, compressive sensing, low-rank matrix completion.

I. Introduction

One of the most challenging tasks in cognitive radio (CR) is to perform spectrum sensing to identify the potential spectral holes to be accessed by secondary users (SUs). In spectrum sensing, the detection performance may be significantly degraded by multipath fading, shadowing, etc [1]. Cooperative spectrum sensing (CSS) is proposed to solve this problem by taking advantage of the spatial diversity among collaborative SUs [2]. However, malicious users in CSS networks sending dishonest samples can also severely degrade the detection performance.

Normally, there are three types of malicious users. One is that the SUs may send high values to the fusion center when there is no primary users (PUs). This will decrease the vacant bandwidth available for SUs in the CSS network. Malicious users may also send low values when PUs exist in the spectrum. This may cause serious interference to the PUs. The third type of malicious users will send random values for sensing malfunctioning. This may increase the false alarm probability or decrease the detection probability [3]. These malicious user scenarios have posed significant challenges in the CSS networks, especially the last type one. Therefore, they should be removed before making the final decision.

A number of algorithms have been proposed to mitigate the influence of malicious users. In [4], a simple outlier detection mechanism was firstly implemented to identify the malicious users which produce false extreme values in CSS networks. A robust outlier detection utilizing outlier factors and user spatial information was proposed to identify the "Always Yes" malicious users in [3]. In addition, an outlier detection scheme based on Dixon's test was proposed to detect the presence of malicious users which may randomly send true or false value of received energy to confuse the other SUs in [5]. In these proposed algorithms, the malicious users were considered to send very high values, low values or random values with either very high or very low. Furthermore, malicious users that give random false values slightly above or below threshold was proposed in [6]. However, in reality, a malicious user sending random false values in a bounded range is extremely challenging to detect.

During malicious user detection, the sampling rate should be at least twice of the signals' bandwidth at each SU. However, for wideband signals, it is difficult to achieve such a high sampling rate due to hardware limitations. In order to reduce the cost of data acquisition, the concept of compressive sensing (CS) is proposed by utilizing the sparsity property of the signals [7]. In CSS networks, the CS technique can be implemented at each SU [8]. Therefore, each SU only needs to collect the compressed samples at a sub-Nyquist rate. When these compressed measurements are sent out, an incomplete matrix can be generated at the fusion center, and the incomplete matrix can be recovered by matrix completion. As malicious users exits in the CSS network, some of the compressed samples are corrupted. If those corrupted samples are used to perform the matrix completion, the recovery would be not exact. So it is essential to remove those corrupted measurements before matrix recovery.

For matrix completion, an adaptive outlier pursuit (AOP) algorithm was proposed in [9] to deal with the sparse random-valued noise in the incomplete matrix. It has been successfully applied in image reconstruction corrupted by impulse noise [10]. We notice that the samples corrupted by malicious users are sparsely distributed in these incomplete measurements, and the values corrupted by malicious users are limited in a range. Therefore, the AOP algorithm is applied to remove the samples corrupted by malicious users. And the matrix completion is performed at the fusion center simultaneously in this paper. Meanwhile, we define the CSS network with a *double sparsity* property, in which malicious users send random false values in a bounded range. The proposed scheme is analyzed

 Published in: Proceedings of the 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP), December 3-5, 2013, Austin, Texas, USA, pp. 1186-1189. DOI:10.1109/GlobalSIP.2013.6737119

numerically and compared with an existing malicious user detection algorithm.

II. Cooperative Spectrum Sensing System Model

In a CSS network, J SUs are implemented spatially to sense the occupancy of spectrum of interest. It is assumed that the wide bandwidth of the whole spectrum of interest is B, and it is divided into I sub-channels. M out of the I sub-channels are occupied by the PUs. As shown in Fig. 1, each SU monitors the whole spectrum of interest. In order to reduce the sampling rate, each SU only sends P ($P < I$) samples by implementing the CS technique. Malicious users are considered to exist in this CSS network, and these malicious users send random values ranging from the smallest value to largest value of all the received samples to the fusion center.

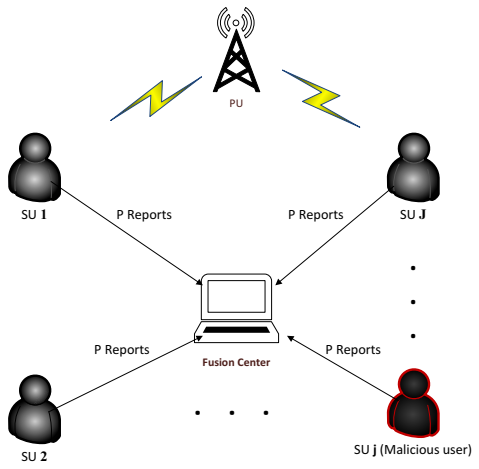

Fig. 1: System model for centralized CSS network.

It is assumed that $s_f \in C^{I\times 1}$ is the unknown transmitted spectrum of PUs, and all cooperating SUs stay silent. r_j refers to spectral states received at the jth SU (SU_j):

$$r_j = H_j s_f \tag{1}$$

where $H_j \in C^{I\times I}$ is the diagonal channel fading matrix for SU_j, and the ith element in the matrix is the fading coefficient on the ith channel of SU_j.

The received time domain signals at SU_j are obtained by doing the inverse DFT to r_j, which can be expressed as:

$$r_{jt} = F^{-1} r_j \tag{2}$$

where F^{-1} is the inverse DFT coefficients.

Then the compressed samples can be obtained by:

$$x_{jt} = \Phi_j F^{-1} r_j = A_j r_{\mathrm{j}} \tag{3}$$

where $\Phi_j \in C^{P\times I}$ is the random compression matrix collecting compressed P linear projections from r_{jt}. Here we can see that $A_j = \Phi_j F^{-1}$ is independent with the channel state information (CSI) since it only contains the local information (Φ_j and F^{-1}). The measurements matrix X received at the fusion center is given by:

$$X = AR = \sum_{j=1}^{J} A_j r_j \tag{4}$$

If malicious users exist in the CSS network, the measurements from the malicious users are corrupted. As a result, the measurements matrix generated at the fusion center in CSS network can be expressed as:

$$X_C = \begin{cases} X & X \in \mathrm{O} \\ Z_C & X \in \Omega \backslash \mathrm{O} \end{cases} \tag{5}$$

where Ω is the domain where X is defined, and O is the set in which X is not corrupted. Z_C is the received samples when X is corrupted by malicious users. Here, Z_C is randomly taken from $[X_S, X_L]$, where X_S and X_L are the smallest and largest values of the compressed samples, respectively. Those corrupted samples are sparsely and randomly distributed in the compressed samples received at the fusion center.

These compressed samples should be recovered at the fusion center before the final decision is made. The recovered matrix R ($I \times J$) at the fusion center is as:

$$\begin{bmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,J-1} & r_{1,J} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,J-1} & r_{2,J} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ r_{I-1,1} & r_{I-1,2} & \cdots & r_{I-1,J-1} & r_{I-1,J} \\ r_{I,1} & r_{I,2} & \cdots & r_{I,J-1} & r_{I,J} \end{bmatrix}_{I\mathrm{x}J} \tag{6}$$

where the ith row of the recovered matrix represents the different spectrum states sensed by different SUs at ith channel , and the jth column refers to the spectrum states for different sub-channels sensed by SU_j. At the fusion center, the key is to reconstructing the original signals from the compressed measurements before making the final decision. In the matrix recovery process, the samples generated from the malicious users should be removed from the compressed samples.

III. Low-rank Matrix Completion based Malicious User Detection

A. Low-rank Matrix Completion

By utilizing the CS technique at each SU in the CSS network, only P out of I samples are sent to the fusion center at each SU. Then the matrix generated at the fusion center is incomplete. The rank order of R equals to the number of active PUs in the CSS network, which is usually low due to the low utilization of the spectrum [11]. As the signals at each SU are sparse, this sparsity property can be transferred into the low rank property of the matrix at fusion center. We define this as the *double sparsity* property. This *double sparsity* property makes it possible to recover the original signals from the incomplete matrix by utilizing AOP based matrix completion algorithm proposed in [9].

In the AOP based matrix completion algorithm for CSS networks, the reconstruction problem at fusion center can be formulated as:

$$\min_{U,W,\Lambda} \frac{1}{2} \sum_{(i,j)\in O} C_{ij}^2 \Lambda_{ij} ((UW)_{ij} - R_{ij})^2 + \frac{\lambda^2}{2} \sum_{(i,j)\notin \widetilde{O}} (UW)_{ij}^2$$
$$s.t. \sum_{(i,j)\in O} (1 - \Lambda_{ij}) \le K, \quad \Lambda_{ij} \in \{0,1\} \tag{7}$$

where $U \in R^{I\times m}$, $W \in R^{m\times J}$ and m is predicted rank bound. The number of corrupted samples in the compressed measurements is defined to be k, and C_{ij} refers to the confidence coefficient, which is set to be 1. Λ_{ij} is a binary matrix denotes the uncorrupted samples as (8). $\widetilde{O}$ is a subspace of O with all indexes $\Lambda_{ij} = 1$. τ is the kth largest term in $(UW)_{ij}^2$, and λ is the weighted parameter set to be 10^{-8}.

$$\Lambda_{ij} = \begin{cases} 1, & \text{if } (i,j) \in O,\ ((UW)_{ij} - R_{ij})^2 < \tau \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

B. Sensing Decisions

Once the recovered $\hat{R}$ is obtained from (7), the fusion center can make a final decision on the spectrum occupancy based on the energy detection. The ith channel is determined as occupied if the average energy of that channel is higher than the empirical threshold $\left(\frac{\mu}{2}\right)^2$, where $\mu = \|s_f\|_1 / \|s_f\|_0$ is the average absolute value of all the M nonzero elements in s_f [8]. A final binary decision $\hat{d}$ on the spectrum state is determined as:

$$\hat{d}[i] = \left(\frac{1}{J} \sum_{j=1}^{J} |r_{ij}|^2 \ge \left(\frac{\mu}{2}\right)^2 \right), \quad \forall i \tag{9}$$

IV. Numerical Analysis

In the simulation process, we assume that each sub-channel is only occupied by an active PU, and an active PU completely locates in one sub-channel. The rank order of R is set to be $r = M = \|s_f\|_0$, which reflects the spectral sparsity order. The fading coefficients follows the uniformly distributed and the malicious users ratio is defined as the percentage of samples corrupted by malicious user among all the compressed samples received at fusion center.

As aforementioned, Kaligineedi et al. present a secure cooperative sensing techniques (SCST) for the CSS networks in [4] to deal with malicious users. Li et al. have shown the performance comparison of their algorithms with that of SCST under different malicious ratios in [12]. We compare the performance of our proposed algorithm with that of SCST by varying the malicious user ratio, network scale, rank order and compression ratio.

In the simulation, the number of SU in the CSS network is set to $I = 50$ and the whole spectrum of interest is divided into $J = 50$ sub-channels. The compression ratio is set to $P/I = 0.6$ and the the number of active PUs in the spectrum of interest is 1. Fig. 2 shows that our AOP based malicious user detection scheme can achieve almost 100% detection accuracy when the malicious user ratio is no higher than 40%. When the malicious user ratio gets further higher, the detection probability of our proposed scheme decreases dramatically and the performance is not as good as SCST. It shows that the detection performance of our proposed scheme drops to 0 when the malicious user ratio is increased to be 60%. This is because that those samples corrupted by malicious users would be removed from the samples used to recover the original signals at the fusion center. When the malicious user ratio reaches 60%, most of the compressed samples would be removed, the number of samples can be used to recover the original matrix is too small. However, the probability of false alarm of our proposed scheme is much lower than the SCST. We can observe that the false alarm probability of our proposed scheme keeps close 0 when malicious user ratio is no higher than 60%, while that of SCST increases greatly with increasing malicious user ratio. Meanwhile, it is noticed that the sampling rate is reduced by 40% as the CS techniques are implemented at each SU. So the energy consumption at each SU is greatly reduced in our proposed scheme.

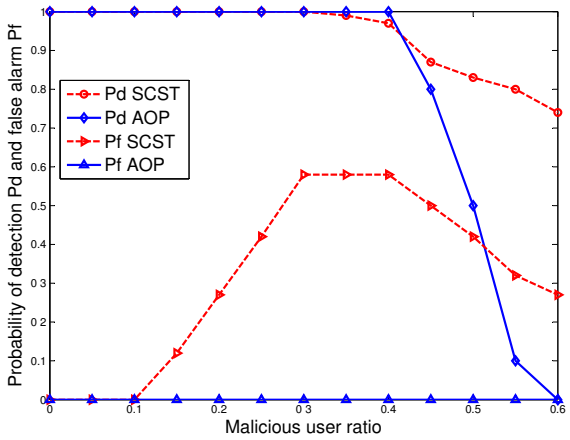

Fig. 2: Detection performance comparison between SCST and our proposed scheme.

Fig. 3 illustrates the impact of the networks scale on the detection performance of our proposed scheme. In this scenario, the number of SUs are set to be 50, 200 and 500. The number of active PUs are set to be 1 and the compression ratio is fixed to be 0.6. It can be seen that the detection performance increases with larger network size, since more information about the spectrum states is sent to the fusion center for final decision making when the network scale becomes larger. With increasing number of SUs, the cooperative gains of the CSS network are improved.

Fig. 4 shows the detection performance of our proposed scheme with differen rank orders, where the threshold at 0dB is as the one set in (9). In this scenario, the network scale is set to be 500 and the rank order is set to be 1, 5, 10. The malicious user ratio is fixed to be 0.6 and the compression ratio is 1 to simplify the scenario. We can see that the detection performance gets worse with increasing rank order. This can be understood as the less active PUs, the easier to be detected.

Fig. 5 shows the detection performance with different compression ratios ranging from 0.4, 0.5, 0.6, 0.8, 1. The threshold

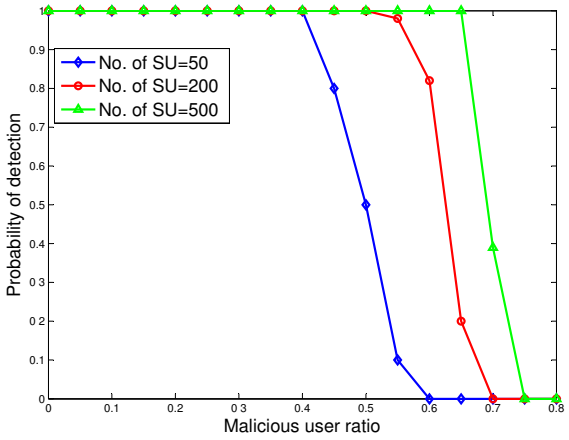

Fig. 3: Detection performance comparison under different network scales.

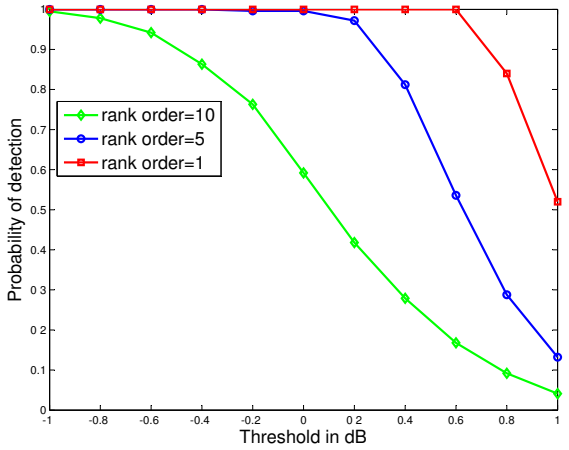

Fig. 4: Detection probability under different rank orders.

setting is the same as that in Fig. 4. In this scenario, the number of SUs in the CSS network and the number of sub-channels are both set to be 500 with rank order $r = 5$. The malicious user ratio is fixed to be 0.6. We can see that the probability of detection increases with increasing compression ratio. This is because that it is easier to recover the original signals with increasing number of observations. It is also noticed that when the compression ratio reaches 0.6 or above, the improvement of detection becomes smaller. So we choose compression ratio as 0.6 in order to minimize the sampling rate at each SU. This is the reason why compression ratio is set to be 0.6 in Fig. 2 and Fig. 3.

V. Conclusion

The existence of malicious users, which send false samples to the fusion center, may lead to false decision about the spectrum occupancy in CSS networks. In this paper, a CSS network scenario with *double sparsity* property was established to tackle malicious users which send random false values in a bounded range. In our malicious user detection method, the low-rank matrix completion based AOP algorithm was utilized

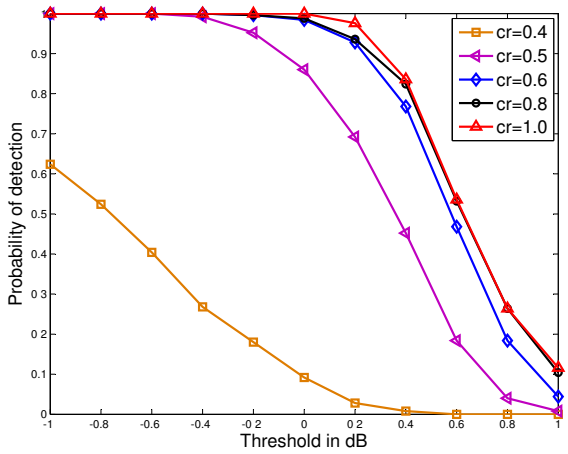

Fig. 5: Detection probability under different compression ratios.

to remove the corrupted samples and perform the signals recovery at the fusion center simultaneously. Numerical results showed that the proposed malicious user detection algorithm outperformed the existing STSC method.

References

[1] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 4, no. 1, pp. 40–62, Mar. 2011.

[2] A. Ghasemi and E. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *DySPAN 2005. 2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005.*, Nov. 2005, pp. 131 –136.

[3] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 8, pp. 2488–2497, Jun. 2010.

[4] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Communications, 2008. ICC '08*, May 2008, pp. 3406–3410.

[5] S. Kalamkar, A. Banerjee, and A. Roychowdhury, "Malicious user suppression for cooperative spectrum sensing in cognitive radio networks using dixon's outlier detection method," in *2012 National Conference on Communications (NCC)*, Feb. 2012, pp. 1–5.

[6] T. Sakaguchi and T. Ohtsuki, "Cooperative spectrum sensing techniques using decision comparison for cognitive radio systems including malicious nodes," in *2010 International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, Oct. 2010, pp. 464–469.

[7] D. Donoho, "Compressed sensing," *Information Theory, IEEE Transactions on*, vol. 52, no. 4, pp. 1289 –1306, Apr. 2006.

[8] Y. Wang, Z. Tian, and C. Feng, "Collecting detection diversity and complexity gains in cooperative spectrum sensing," *IEEE Transactions on Wireless Communications*, vol. 11, no. 8, pp. 2876 –2883, Aug. 2012.

[9] M. Yan, Y. Yang, and S. Osher, "Exact low-rank matrix completion from sparsely corrupted entries via adaptive outlier pursuit," *Journal of Scientific Computing*, pp. 433–449, Jan. 2013.

[10] M. Yan, "Restoration of images corrupted by impulse noise and mixed gaussian impulse noise using blind inpainting," *SIAM Journal on Imaging Sciences*, pp. 1227–1245, 2013.

[11] J. Meng, W. Yin, H. Li, E. Hossain, and Z. Han, "Collaborative spectrum sensing from sparse observations in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 2, pp. 327–337, Jan. 2011.

[12] H. Li, X. Cheng, K. Li, C. Hu, N. Zhang, and W. Xue, "Robust collaborative spectrum sensing schemes for cognitive radio networks," *IEEE Transactions on Parallel and Distributed Systems*, Mar. 2013.