Secure Collaborative Spectrum Sensing: A Peer-Prediction Method

Yu Gan, Chunxiao Jiang, *Senior Member, IEEE*, Norman C. Beaulieu, *Fellow, IEEE*,
Jian Wang, *Member, IEEE*, and Yong Ren, *Senior Member, IEEE*

***Abstract*— Collaborative spectrum sensing is an effective method to improve detection rates in cognitive radio networks. However, it is vulnerable to spectrum sensing data falsification (SSDF) attacks when malicious secondary users (SUs) report fraudulent sensing data. In order to improve the robustness, numerous attack prevention schemes have been proposed to identify malicious SUs. Nevertheless, most of them neglect to incentivize SUs to send truthful reports. An incentive method based on peer-prediction is proposed to identify malicious suspects, punish attackers, and incentivize SUs to send truthful reports simultaneously for decision fusion. Moreover, continuous peer-prediction derived from the binary case is introduced, which is capable of preventing attacks in the continuous domain. Theoretical analysis and simulation results demonstrate that honest SUs are rewarded for accurate and truthful sensing results, while malicious SUs incur penalty for making falsified sensing reports. A significant improvement of detection rates is obtained by the proposed scheme when there are no more than half of malicious SUs conducting SSDF attacks.**

***Index Terms*— Collaborative spectrum sensing, data fusion, decision fusion, peer-prediction, spectrum sensing data falsification attacks.**

I. Introduction

FREQUENCY spectrum is becoming increasingly crowded as the consequence of the rapid development of wireless communications and growing number of wireless devices. However, it is utilized inefficiently because of the idle time of the licensed users (primary users, PUs) [1], [2]. In order to solve this problem, cognitive radio networks (CRNs) were proposed, allowing unlicensed users (secondary users, SUs) to utilize the spectrum without causing interference to the PUs [3]–[6]. An essential step in CRNs is spectrum sensing, which aims to detect the spectrum holes that are not occupied by the PUs and thus avoid causing interference. Many spectrum sensing methods have been proposed to identify the existence of the PU's signal, including energy detection, matched filtering, waveform based sensing, spectral correlation, etc. [7]. Energy detection is the most common approach among all because it is easy to implement and does not require prior information of the signal [8], [9]. However, single-user energy detection is often inaccurate because of the fading and shadowing effects in wireless channels [10]–[13]. To improve the accuracy, collaborative spectrum sensing (CSS) has been proposed, in which a fusion center (FC) combines all SUs' observations to make the final decision. At present, there are two types of fusion protocols in CSS, namely decision fusion and data fusion. In decision fusion, each SU sends a 1-bit decision to the FC based on its own observation whether the PU is busy or not. In data fusion, the SU directly sends the raw observation data to the FC. Both methods significantly improve the reliability of the spectrum sensing, but data fusion performs superior to decision fusion [14]. Nevertheless, the CSS is vulnerable to spectrum sensing data falsification (SSDF) attacks. In such attacks, malicious SUs deliberately send falsified local reports to the FC and corrupt the overall decision in order to either disturb the data transmission of the PUs or occupy the frequency spectrum exclusively.

To improve the performance of CSS, it is vitally important to protect the system against SSDF attacks. Many attack-resistant mechanisms have been proposed in [15]–[22]. Most existing works focus on the study of algorithms to identify malicious SUs while ignoring incentivizing SUs in CRNs to announce truthful local reports. Considering the fact that all SUs participating in CSS are ostensibly self-interested and that they have the objective to access the frequency spectrum possessed by the PU to transmit their own data, every SU has the potential to become malicious. In order to maximize its utility in data transmission, an SU may intend to send falsified sensing reports, if there is no mechanism to punish dishonest SUs. In addition, mere removal of a large number of malicious SUs leads to the decline of collaborative sensing efficiency because fewer SUs get involved in the decision fusion process as the number of malicious SUs increases.

Furthermore, some of the previous schemes rely on common prior knowledge of the activity of the PU, and assume each SU's private error rate of sensing is the same and shared by all SUs, which is not realistic. Moreover, CSS networks are extremely vulnerable to heavy cooperative attacks by a high

Manuscript received November 21, 2016; revised April 14, 2016 and June 24, 2016; accepted August 4, 2016. Date of publication August 16, 2016; date of current version October 14, 2016. This research was supported by NSFC China under projects 61371079, 61271267 and 91338203. The associate editor coordinating the review of this paper and approving it for publication was J. Yuan. *(Corresponding author: Chunxiao Jiang.)*

Y. Gan, J. Wang, and Y. Ren are with the Department of Electronic Engineering, Tsinghua University, Beijing 100084, China (e-mail: gany12@mails.tsinghua.edu.cn; jian-wang@tsinghua.edu.cn; reny@tsinghua.edu.cn).

C. Jiang is with the Tsinghua Space Center, Tsinghua University, Beijing 100084, China (e-mail: jchx@tsinghua.edu.cn).

N. C. Beaulieu is with the Beijing Key Laboratory of Network System Architecture and Convergence, School of Information and Communication Engineering, Beijing University of Posts and Telecomunications, Beijing 100876, China (e-mail: nborm@bupt.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2016.2600563

percentage of malicious SUs, but only a few previous works consider this extreme condition in their studies. Last but not least, while most of the attack prevention methods are based on decision fusion schemes, there are only few methods aimed at defending SSDF attacks using data fusion methods, which may be difficult to implement but more accurate in identifying the malicious SUs.

Therefore, in this paper, we propose two mechanisms based on the *private-prior peer-prediction mechanism* with both incentive scheme and attacker identification scheme to motivate SUs to send honest sensing reports, and distinguish malicious SUs from honest ones simultaneously for data fusion and decision fusion. The *continuous private-prior peer-prediction mechanism* is derived from the basic private-prior peer-prediction mechanism in this paper, specifically for the CSS where the probability density function of the signal reports can be explicitly expressed. The two peer-prediction schemes require the SU's approximate subjective estimation of the prior knowledge of the PU's activity and the signal-to-noise ratio (SNR) obtained by SNR estimation techniques [23].

Overall, the contributions of this paper are listed as below:

- We view the SSDF attack prevention problem from the perspective of game theory, and design an effective and incentive compatible mechanism to solve the problem.
- We propose an incentive SSDF attack prevention mechanism based on private-prior peer-prediction for decision fusion, which is able to incentivize SUs' truthful reports and detect malicious SUs.
- We propose a continuous private-prior peer-prediction mechanism to prevent attacks in the data fusion with low computation overhead based on the binary private-prior peer-prediction.
- We evaluate our mechanism through simulation and validate its performance in heavy SSDF attacks.

The rest of this paper is organized as follows. The system model is described in detail in Section II. Then, a private-prior peer-prediction method to incentivize SUs' truthful reporting and identify malicious suspects is applied to CSS based on decision fusion in Section III. Next in Section IV, the continuous private-prior peer-prediction method derived from the basic idea is proposed. The scheme is aimed at motivating SUs' truthful reporting and identification of malicious suspects in CSS based on data fusion. Simulation results are given in Section V, and conclusions are drawn in Section VI.

II. Related Work

In this section, previous study on SSDF attack prevention schemes and peer-prediction methods are introduced.

A. SSDF Attack Prevention Scheme

In [16], an outlier-detection scheme with partial prior knowledge of the PU was proposed to identify malicious SUs whose results differ greatly from other SUs. In [17], a double-sided neighbor distance algorithm with adaptive threshold selection has been proposed to detect the outliers of the sensing report vectors, which are extremely close to or far away from other SUs' reports. Both dependent and independent attacks are considered in the study and the scheme is able to recognize multiple malicious SUs without any prior information of attack strategies. In [18], Duan *et al.* have proposed a mechanism with direct and indirect penalties to SUs when the FC announces busy, but collisions impact the PU. The method is designed to prevent both hit-and-run and stay-with attacks under the circumstances where several cooperative attackers are able to overhear the honest SUs' reports. However, the mechanism is invalid if some SUs only aim to disrupt the CSS network, but are not interested in data transmission.

Recently, in light of artificial intelligence and data mining, methods based on likelihood detection and clustering have been proposed. Considering various types of honest and malicious SUs, Soltanmohammadi and Naraghi-Pour in [21] have introduced an iterative expectation maximization based algorithm to identify malicious SUs. However, the high computational complexity makes it difficult to implement. Inspired by data mining methods, Hyder *et al.* in [22] have presented an adaptive reputation clustering based algorithm to defend against attacks. In their study, partitioning around medoid algorithm is utilized to cluster SUs based on their binary report vectors. Further, a reputation adjustment approach is applied as a feedback loop to update the reputation of each node and increase the number of clusters.

B. Peer-Prediction Method

In [24], Miller *et al.* have initially introduced the method of peer-prediction to create incentives for online raters to make honest reviews by appropriate rewards. Witkowski and Parkes have improved the method and proposed the *private-prior peer-prediction mechanism* in [25]. The peer-prediction scheme is adequate for the circumstances where prior knowledge is subjective and private to each agent. It has been utilized to collect truthful reports on website reviews, pollution detection [26] and private surveys [27], and is regarded as an effective way to elicit truthful feedback. However, the original private-prior peer-prediction method can only be effective with decision fusion because its application is limited to domains with binary signal reports [25]. Some continuous peer-prediction methods have been proposed in [28] and [29], but either the method is inadequate for the specific situation where malicious SUs can take advantage of the scoring system when sending contradictory information and signal reports, or the computation and data transmission is too complex for the method to be implemented on mobile devices.

III. System Model

A. Local Spectrum Sensing With Energy Detection

In our system illustrated in Fig. 1, we consider a CRN with one PU who has a license to transmit data in one channel and N SUs who conduct local spectrum sensing independently in a total number of T time slots. The two different states of the channel are denoted by hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, which represent the channel is idle or busy, respectively. Each SU i has its subjective prior belief in regard to the state of the channel $P_i(\mathcal{H}_1)$ which is implicit to the FC and other SUs. They remain constant in T time slots for simplicity. The SUs

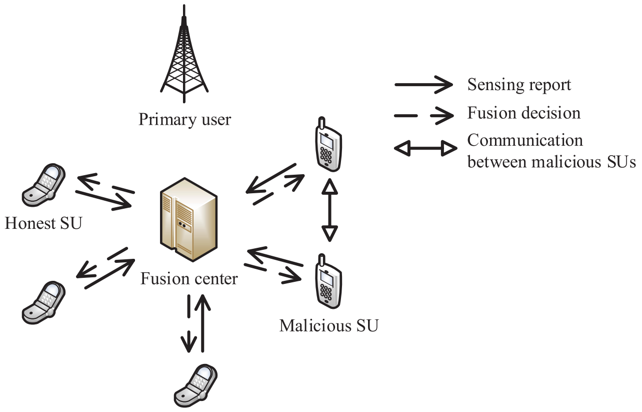

Fig. 1. The collaborative spectrum sensing network.

are assumed to be able to make an approximate estimation of $P(\mathcal{H}_1)$ based on the regularity of the PUs activity. The aim of collaborative spectrum sensing is to solve the binary hypothesis-testing problem with specific signal sensing techniques. Energy detection is the most popular sensing method because of its low computation complexity not requiring any prior information of the PU's signal. Consider the observed signal $x_i(t)$ of the ith SU [30],

$$x_i(t) = \begin{cases} n_i(t), & \mathcal{H}_0 \\ h_i s(t) + n_i(t), & \mathcal{H}_1 \end{cases} \tag{1}$$

where h_i is the channel parameter of the sensing channel between the PU and the ith SU, which remains constant during the whole sensing process, $s(t)$ is the instantaneous signal of the PU and $n_i(t)$ is additive white Gaussian noise. Assuming the local energy detector measures the signal within a fixed bandwidth W over an observation time window τ in each time slot, the energy E_i which is measured in the frequency domain follows a distribution as follows [1].

$$E_i \sim \begin{cases} \chi^2_{2\mu}, & \mathcal{H}_0 \\ \chi^2_{2\mu}(2\gamma_i), & \mathcal{H}_1 \end{cases} \tag{2}$$

where $\chi^2_{2\mu}$ indicates a central chi-square distribution with the degrees of freedom 2μ and $\chi^2_{2\mu}(2\gamma_i)$ indicates a non-central chi-square distribution with 2μ degrees of freedom and a non-centrality parameter $2\gamma_i$. μ is the time bandwidth product τW which is assumed to be a constant for all SUs in T time slots and known by the system. γ_i is the instantaneous SNR of the ith SU which is varying across different SUs and time slots, and can be calculated using the SNR estimation technique.

Among N SUs, there are M malicious SUs and they cannot be dominant in a normal CSS network, thus $M < \frac{1}{2}N$. All honest SUs report what they detect truthfully and are uninterested in the final fusion results, while malicious SUs report based on their attack strategies and attempt to dominate the FC's final decision.

B. Collaborative Spectrum Sensing Based on Decision Fusion

In the decision fusion, the ith SU makes a binary decision, denoted by $D_i \in \{0, 1\}$, on whether the channel is idle or busy by comparing the value of E_i to a threshold λ_i, and generates a binary sensing report, denoted by $S_i \in \{0, 1\}$, sent to the FC. The SU i has its own false alarm probability of sensing, $P_{fa,i} = P(D_i = 1|\mathcal{H}_0)$, missed detection probability of sensing, $P_{md,i} = P(D_i = 0|\mathcal{H}_1)$, false alarm probability of reporting, $P_{f,i} = P(S_i = 1|\mathcal{H}_0)$ and missed detection probability of reporting, $P_{m,i} = P(S_i = 0|\mathcal{H}_1)$. The FC aggregates all SUs' binary reports together and makes the final decision according to:

$$Y = \sum_{i=1}^{N} S_i \begin{cases} < n, & \text{the FC decides } \mathcal{H}_0 \\ \geq n, & \text{the FC decides } \mathcal{H}_1. \end{cases} \tag{3}$$

A majority rule decision results when the FC decides $\mathcal{H}_1$ only if more than half of the N SUs observe the channel is busy, with the threshold $n = \frac{1}{2}N$.

C. Collaborative Spectrum Sensing Based on Data Fusion

In the data fusion, the sensing report $S_i \in \mathbb{R}^+$ is continuous. Instead of sending the binary decision D_i, the SU directly transmits the detected signal energy $S_i = E_i$ to the FC. Then, the FC will make its decision based on all SUs' signal reports by applying the Neyman-Pearson criterion [14], namely,

$$LR(\mathbf{S}) = \prod_{i=1}^{N} \frac{P(S_i|\mathcal{H}_1)}{P(S_i|\mathcal{H}_0)} \begin{cases} < \lambda, & \text{the FC decides } \mathcal{H}_0 \\ \geq \lambda, & \text{the FC decides } \mathcal{H}_1. \end{cases} \tag{4}$$

According to Eq. (2), $P(S_i|\mathcal{H}_0)$ and $P(S_i|\mathcal{H}_1)$,

$$P(S_i|\mathcal{H}_0) = \frac{1}{2^{\mu}\Gamma(\mu)} S_i^{\mu-1} e^{-\frac{S_i}{2}} \tag{5}$$

$$P(S_i|\mathcal{H}_1) = \frac{1}{2} e^{-\frac{S_i+2\gamma_i}{2}} \left(\frac{S_i}{2\gamma_i}\right)^{\frac{\mu-1}{2}} I_{\mu-1}(\sqrt{2\gamma_i S_i}) \tag{6}$$

where $I_{\upsilon}(y)$ is the modified Bessel function of the first kind of order υ [31],

$$I_{\upsilon}(y) = i^{-\upsilon} J_{\upsilon}(iy) = \sum_{m=0}^{\infty} \frac{1}{m!\Gamma(m+\upsilon+1)} \left(\frac{y}{2}\right)^{2m+\upsilon}. \tag{7}$$

IV. Peer-Prediction Method for Decision Fusion

In this section, we first introduce the private-prior peer-prediction method for collecting truthful reports of SUs based on the decision fusion protocol. Using a strictly proper scoring rule, we then explain the mechanism to motivate SUs to report honestly and identify malicious suspects by distinguishing scores that different types of SUs report. Lastly, we propose an uncertainty index and a method to enlarge the loss to malicious SUs when conducting attacks; the method is based on the threshold of the uncertainty index.

A. Private-Prior Peer-Prediction

The private-prior peer-prediction method is an incentive compatible mechanism originally proposed to motivate agents to report actual binary feedback on online reviewing websites. Each agent will receive its reward from a fusion center and the amount of the reward is depended on the agent's report and the reports given by other agents [25]. In private-prior peer-prediction, each agent i is coupled with another agent $j = i+1$ and is required to send an information report before sensing the world state and a prediction report after sensing the world state. The center will comprehend the implicit decision of each agent by comparing its information and prediction reports, and calculating the score of each agent, which determines the agent's reward, according to an appropriate scoring rule.

In our system, considering the existence of cooperative attacks, each SU i has a peer SU j selected randomly from other SUs without repetition in each time slot. Before sensing the PU's signal in the channel, the SU i is required to provide its information report of the probability that the peer SU j will report the channel being busy ($S_j = 1$), denoted by $X_{i,j} \in [0, 1]$, to the FC. $X_{i,j}$ can be expressed as,

$$\begin{aligned} X_{i,j} &= P_i(S_j = 1) \\ &= P_i(S_j = 1|\mathcal{H}_0) \cdot P_i(\mathcal{H}_0) \\ &\quad + P_i(S_j = 1|\mathcal{H}_1) \cdot P_i(\mathcal{H}_1) \\ &= P^i_{f,j} \cdot P_i(\mathcal{H}_0) + (1 - P^i_{m,j}) \cdot P_i(\mathcal{H}_1) \end{aligned} \tag{8}$$

where $P_i(\mathcal{H}_0)$ and $P_i(\mathcal{H}_1)$ are SU i's subjective prior of the PU's activity, and $P^i_{f,j}$ and $P^i_{m,j}$ are SU j's error rates of reporting in SU i's perspective. Assuming that $\psi^i_{m,j}$ and $\psi^i_{f,j}$ are SU j's missed detection attack rate and false alarm attack rate observed by SU i, $P^i_{f,j}$ and $P^i_{m,j}$ can be calculated from SU i's respective subjective prior information according to

$$\begin{aligned} P^i_{f,j} &= (1 - P^i_{fa,j}) \cdot \psi^i_{f,j} + P^i_{fa,j} \cdot (1 - \psi^i_{m,j}) \\ P^i_{m,j} &= (1 - P^i_{md,j}) \cdot \psi^i_{m,j} + P^i_{md,j} \cdot (1 - \psi^i_{f,j}). \end{aligned} \tag{9}$$

However, SU i cannot obtain $P^i_{fa,j}$, $P^i_{md,j}$, $\psi^i_{m,j}$ and $\psi^i_{f,j}$ directly from SU j. Thus, $P^i_{f,j}$ and $P^i_{m,j}$ will be estimated by comparing the observation history vector of SU j to the actual activity of the PU. Since neither of the SUs nor the FC knows the exact activity of the PU, the SU i can compare the observation history vector of SU j to a reference vector that it believes to be the same as or similar to the activity history of the PU to estimate SU j's error rates. The SU i can choose either the decision history vector of the FC or its own observation history vector as the reference vector, depending on their accuracy, and calculate the error rates of SU j by summing the different bits between observation history vector of SU j and the reference vector.

After observing the PU's signal in the channel, the SU i makes its own decision $D_i = d_i$ and sends its prediction report of the probability that peer SU j will report the channel being busy ($S_j = 1|D_i = d_i$), denoted by $Y_{i,j} \in [0, 1]$, to the FC. $Y_{i,j}$ can be expressed as,

$$\begin{aligned} Y_{i,j} &= P_i(S_j = 1|D_i = d_i) \\ &= P_i(S_j = 1|\mathcal{H}_0) \cdot P_i(\mathcal{H}_0|D_i = d_i) \\ &\quad + P_i(S_j = 1|\mathcal{H}_1) \cdot P_i(\mathcal{H}_1|D_i = d_i). \end{aligned} \tag{10}$$

For convenience, the prediction report is abbreviated as $Y^0_{i,j}$ when SU i observes the channel is idle and is abbreviated as $Y^1_{i,j}$ when SU i observes the channel is busy, namely

$$\begin{aligned} Y^0_{i,j} &= P_i(S_j = 1|D_i = 0) \\ &= \frac{P^i_{f,j} \cdot (1 - P_{fa,i})P_i(\mathcal{H}_0) + (1 - P^i_{m,j})P_{md,i}P_i(\mathcal{H}_1)}{P_{md,i} \cdot P_i(\mathcal{H}_1) + (1 - P_{fa,i})P_i(\mathcal{H}_0)} \end{aligned} \tag{11}$$

$$\begin{aligned} Y^1_{i,j} &= P_i(S_j = 1|D_i = 1) \\ &= \frac{P^i_{f,j}P_{fa,i}P_i(\mathcal{H}_0) + (1 - P^i_{m,j})(1 - P_{md,i})P_i(\mathcal{H}_1)}{P_{fa,i} \cdot P_i(\mathcal{H}_0) + (1 - P_{md,i})P_i(\mathcal{H}_1)}. \end{aligned} \tag{12}$$

The prediction report made by a well-functioning honest SU with low P_{fa} and P_{md} are not identical to the information report because more information about the channel has been revealed after i senses the PU's signal, as will be seen in the sequel. Therefore, the FC is able to estimate SU i's sensing report by comparing $X_{i,j}$ and $Y_{i,j}$.

Proposition 1: If all SUs satisfy $P_f + P_m < 1$ and $P_{fa} + P_{md} < 1$, for any two SUs i and j, it holds that

$$P_i(S_j = 1|D_i = 1) > P_i(S_j = 1) > P_i(S_j = 1|D_i = 0). \tag{13}$$

Proof: For any two SUs i and j, $P^i_{f,j} + P^i_{m,j} < 1$ always holds because no SU will estimate $P^i_{f,j} + P^i_{m,j} \geq 1$ knowing that all SUs' error rates of reporting satisfy $P_f + P_m < 1$. So,

$$\begin{aligned} &P_i(S_j = 1|D_i = 1) - P_i(S_j = 1) \\ &= (1 - P^i_{m,j}) \cdot \frac{(1 - P_{md,i}) \cdot P_i(\mathcal{H}_1)}{P(D_i = 1)} + P^i_{f,j} \cdot \frac{P_{fa,i} \cdot P_i(\mathcal{H}_0)}{P(D_i = 1)} \\ &\quad - P^i_{f,j} \cdot P_i(\mathcal{H}_0) - (1 - P^i_{m,j})P_i(\mathcal{H}_1) \\ &= \frac{1}{P(D_i = 1)}\Big\{ - \big[P^i_{f,j} \cdot P_i(\mathcal{H}_0) + (1 - P^i_{m,j})P_i(\mathcal{H}_1)\big] \\ &\quad \cdot \big[P_{fa,i} \cdot P_i(\mathcal{H}_0) + (1 - P_{md,i})P_i(\mathcal{H}_1)\big] \\ &\quad + (1 - P^i_{m,j})(1 - P_{md,i})P_i(\mathcal{H}_1) + P^i_{f,j} \cdot P_{fa,i} \cdot P_i(\mathcal{H}_0)\Big\} \\ &= \frac{P_i(\mathcal{H}_0)P_i(\mathcal{H}_1)}{P(D_i = 1)}\big[1 - P^i_{f,j} - P^i_{m,j} - P_{fa,i} - P_{md,i} \\ &\quad + (P^i_{f,j} + P^i_{m,j})(P_{fa,i} + P_{md,i})\big] \\ &= \frac{P_i(\mathcal{H}_0)P_i(\mathcal{H}_1)}{P(D_i = 1)}(1 - P^i_{f,j} - P^i_{m,j})(1 - P_{fa,i} - P_{md,i}) \\ &> 0. \end{aligned}$$

Thus, $P_i(S_j = 1|D_i = 1) > P_i(S_j = 1)$. $P_i(S_j = 1) > P_i(S_j = 1|D_i = 0)$ can be proved analogously by symmetry. ■

In our mechanism, to satisfy the condition of Proposition 1, the FC will restrict participation in the CSS process to the SUs for whom $P_f + P_m \geq 1$ or $P_{fa} + P_{md} \geq 1$. This is wise because such SUs are either malicious SUs with high attacking rates or honest SUs with low performance and their decisions will corrupt the final CSS results severely. According to Proposition 1, it is implied in the prediction report that SU i has observed $\mathcal{H}_0$ if $Y_{i,j} < X_{i,j}$, or $\mathcal{H}_1$ if $Y_{i,j} > X_{i,j}$. Thus the implied sensing report each SU makes in one time slot can be estimated by the FC according to the rule,

$$S_i = \begin{cases} 1 & Y_{i,j} > X_{i,j} \\ 0 & Y_{i,j} < X_{i,j}. \end{cases} \tag{14}$$

Note the fact that the accuracy in $P^i_{f,j}$ and $P^i_{m,j}$ are unnecessary for Proposition 1 to hold. It can be concluded that imprecise estimation will have little influence on the accuracy of the judgement on SU i's decision using eq. (14).

For each honest SU, $S_i = D_i$, while for the malicious SU, $S_i = \sigma_i(D_i)$, where $\sigma_i : \{0,1\} \to \{0,1\}$ is a binary function according to its attack strategy. In order to conduct SSDF attacks, the malicious SU may not report $X_{i,j}$ and $Y_{i,j}$ honestly. Therefore, a mechanism should be designed to incentivize each SU to report truthful and accurate values of $X_{i,j}$ and $Y_{i,j}$, approaching as close as possible to the actual probabilities $P(S_j = 1)$ and $P(S_j = 1|D_i = d_i)$ by giving SUs different scores according to their reports. The score of each SU in each time slot is defined by the scoring function,

$$U_i = \underbrace{\alpha \cdot R(X_{i,j}, S_j)}_{\text{Information Score}} + \underbrace{\beta \cdot R(Y_{i,j}, S_j)}_{\text{Prediction Score}} + \gamma \tag{15}$$

where $R(x, q)$ is a strictly proper scoring rule and will be introduced in the following subsection. $\alpha > 0$, $\beta > 0$ and γ are parameters chosen according to different application conditions. Such scores are cumulative as the sensing process continues. A negative score can be a reflection of either monetary punishment or frequency spectrum access limitation and the negative benefits will be transferred as positive benefits to the SUs as rewards for their honesty and accuracy.

B. Scoring Rules and Incentive Compatibility

A proper scoring rule $R(x, q)$ incentivizes the agents' accurate probabilistic prediction reports for a binary report $q \in \{0, 1\}$, by assigning different scores according to their reports x. A strictly proper scoring rule maximizes the expectation of the scores if and only if the prediction reports equal the actual probabilities [32]. Furthermore, the binary quadratic scoring rule, according to Selten [33], is an incentive compatible strictly proper scoring rule. It is given by

$$\begin{aligned} R(x, 0) &= 1 - x^2 \\ R(x, 1) &= 2x - x^2 \end{aligned} \tag{16}$$

for $x \in [0, 1]$. Assuming p is the probability that $q = 1$, the expectation of the score is $E[R(x, \cdot)] = (1 - p)(1 - x^2) + p(2x - x^2)$. By taking the derivative with respect to x, setting it to zero, and checking the second-order condition, $\frac{\partial E[x]}{\partial x} = 2p - 2x = 0 \Leftrightarrow x = p$, $\frac{\partial^2 E[x]}{\partial x^2} = -2 < 0$, we obtain a maximum when $x = p$ [25].

In addition, if $R(x, \cdot)$ is a strictly proper scoring rule and $\alpha > 0$, $R^*(x, \cdot) = \alpha \cdot R(x, q) + \beta$ is also strictly proper [24]. In our scoring function $U_i(X_{i,j}, Y_{i,j})$, due to the temporal separation of the information report and the prediction report, $X_{i,j}$ and $Y_{i,j}$ are independent and thus $E[U_i(X_{i,j}, Y_{i,j})] = \alpha \cdot E[R(X_{i,j}, \cdot)] + \beta \cdot E[R(Y_{i,j}, \cdot)|D_i = d_i] + \gamma$. Therefore, $E[U_i(X_{i,j}, Y_{i,j})]$ reaches the maximum when both the information report and the prediction report maximize, which requires $X_{i,j} = P(S_j = 1)$ and $Y_{i,j} = P(S_j = 1| D_i = d_i)$ exactly. In a long term, an honest SU always expects higher scores for its accurate information and prediction reports, while the malicious user will have a certain loss in score each time it announces falsified report data.

To keep the budget balanced, $\gamma = -\frac{1}{N}\sum_{i=1}^{N}\left[\alpha \cdot R(X_{i,j}, S_j) + \beta \cdot R(Y_{i,j}, S_j)\right]$. The principle for designing α and $beta$ is to ensure the mechanism is individually rational for only the honest SUs. Assume that M malicious SUs can get a total reward $\mathcal{R}_1$ by occupying the channel and transmitting data when the PU is absent but the FC announces the channel is busy, and get a total reward $\mathcal{R}_2$ by interfering with the PU when the PU is present but the FC announces the channel is idle. Suppose the system has a missed detection rate Q_m and a false alarm rate Q_f and each malicious user has an average information score $\bar{R}_m(X, S)$ and an average prediction score $\bar{R}_m(Y, S)$. A minimum of positive coefficients α and β can be derived from the inequality $\alpha \cdot \bar{R}_m(X, S) + \beta \cdot \bar{R}_m(Y, S) + \gamma + \frac{\mathcal{R}_1}{M} Q_f \cdot P(\mathcal{H}_0) + \frac{\mathcal{R}_2}{M} Q_m \cdot P(\mathcal{H}_1) < 0$. To balance the weights of the information score and the prediction score, we set $\alpha = \beta$ in our mechanism.

On the one hand, with the appropriate scoring function, a rational malicious SU aware that it cannot gain a positive income in each time slot when conducting attacks, tends to announce honest reports when the loss exceeds its tolerance. On the other hand, it is reasonable for the FC to suspect that SUs with relatively low cumulative scores are malicious. Thus, the FC sets an integer K and removes the decisions made by K SUs with lowest cumulative scores from the decision pool. The optimized value of K depends on M and N, and equals M if all malicious SUs obtain lower scores than honest ones.

Furthermore, unlike other reputation based schemes proposed previously, the scoring function proposed in this paper is independent of the FC's final decision. The reputation systems in [19] and [20] rely on the FC's decision and can easily break down if the FC itself makes incorrect decisions due to being misled by malicious SUs; this of course, forms positive feedback and affects subsequent decision results. However, in our proposed scheme, the score of each SU will not be affected by an incorrect final decision and is more likely to be assessed with an honest peer's sensing report as long as $M < \frac{1}{2}N$ and $P_f + P_m < 1$, as assumed. Therefore, the scoring system is more stable and robust than the reputation systems of previous schemes.

C. Uncertainty Index and Threshold

While attacking, the malicious SU can minimize its loss on scores by making the prediction report as close as possible to the information report, i.e., reporting $Y^0_{i,j} = X_{i,j} - \varepsilon$ under $\mathcal{H}_1$ or $Y^1_{i,j} = X_{i,j} + \varepsilon$ under $\mathcal{H}_0$, where ε is a smallest possible positive number. Thus, it is necessary to set a threshold to limit the minimum difference between $X_{i,j}$ and $Y_{i,j}$. By taking the derivative of $Y^0(P_{md}, P_{fa})$ and $Y^1(P_{md}, P_{fa})$ with respect to P_{md} and P_{fa}, $\frac{\partial Y^1}{\partial P_{md}} < 0$, $\frac{\partial Y^1}{\partial P_{fa}} < 0$, $\frac{\partial Y^0}{\partial P_{md}} > 0$ and $\frac{\partial Y^0}{\partial P_{fa}} > 0$. Thus, $Y^1(P_{md}, P_{fa})$ is a decreasing function, while $Y^0(P_{md}, P_{fa})$ is increasing, with respect to both independent variables.

In other words, assuming that P_f, P_m and $P(\mathcal{H}_1)$ are fixed, the honest SU with lower missed detection rate and false alarm rate will make a higher prediction report Y^1 or a lower prediction report Y^0, compared to the honest SU with relatively higher error rates, or the malicious SU who makes prediction reports conservatively in order to minimize its loss.

Therefore, an individual uncertainty index $\phi_{i,j}$ can be defined as the uncertainty of SU i when it makes a prediction report $Y_{i,j}$, which can be expressed by i's error rates of sensing derived inversely from prediction report $Y_{i,j}$, denoted by $\widetilde{P}^j_{md,i}$ and $\widetilde{P}^j_{fa,i}$, respectively. Furthermore, by comparing $\frac{\partial Y^0}{\partial P_{md}}$, $\frac{\partial Y^0}{\partial P_{fa}}$, $\frac{\partial Y^1}{\partial P_{md}}$ and $\frac{\partial Y^1}{\partial P_{fa}}$, it can be concluded that Y^0 is more sensitive to P_{md} than to P_{fa}, and Y^1 is more sensitive to P_{fa} than to P_{md} when $P_{fa} < 0.5$ and $P_{md} < 0.5$, which are always true in the real case. Thus, the SU with low $\widetilde{P}^j_{md,i}$ is more confident and reliable than the one with high $\widetilde{P}^j_{md,i}$ under $\mathcal{H}_0$ and so is the SU with low $\widetilde{P}^j_{fa,i}$ under $\mathcal{H}_1$. Therefore, the individual uncertainty index $\phi_{i,j}$ can be expressed as the maximum of $\widetilde{P}^j_{md,i}$ on condition that $\widetilde{P}^j_{fa,i} = 0$ when reporting Y^0_i, or maximum of $\widetilde{P}^j_{fa,i}$ on condition that $\widetilde{P}^j_{md,i} = 0$ when reporting Y^1_i. The expression for $\phi_{i,j}$ is then

$$\phi_{i,j} = \begin{cases} \frac{(P_{f,j}-Y_{i,j})P(\mathcal{H}_0)}{\left[Y_{i,j}-(1-P_{m,j})\right]P(\mathcal{H}_1)}, & \text{if } X_{i,j} > Y_{i,j} \\ \frac{\left[Y_{i,j}-(1-P_{m,j})\right]P(\mathcal{H}_1)}{(P_{f,j}-Y_{i,j})P(\mathcal{H}_0)}, & \text{if } X_{i,j} < Y_{i,j}. \end{cases} \tag{17}$$

Eq. (17) above can be derived from eqs. (11) and (12) by setting $P_{fa,i} = 0$ and $P_{md,i} = 0$, respectively. To compute the uncertainty index, the FC observes each SUs report error rate $P_{f,j}$ and $P_{m,j}$, and prior belief $P(\mathcal{H}_1)$ with the activity history of the PU and all SUs. Typically, the SU with a high uncertainty index is either a badly-functioning one who cannot be certain whether another honest SU will make the same prediction, or a malicious one sending a conservative falsified prediction report close in value to its information report. Therefore, the FC sets a threshold θ for the uncertainty index so that the decision made by the SU whose $\phi_{i,j} \geq \theta$ will be removed from the decision pool and will not be considered by the FC when it aggregates SUs' decisions and decides the final result. θ is unknown to all SUs and will be designed according to typical error rates of normal SUs so that most of the well-functioning honest SUs' uncertainty indices are below the threshold.

Furthermore, for the minority of honest SUs whose uncertainty index exceeds the threshold, their best choice is still to report honestly and it is unnecessary for them to adjust their prediction reports because the income only comes from the score, as determined by the accuracy of $X_{i,j}$ and $Y_{i,j}$, rather than acceptance of their decisions by the FC. On the contrary, the income of the malicious SUs comes from both their scores and the FC's final decision. In order to falsify the sensing results, malicious SUs have to decrease their uncertainty indices below the threshold by enlarging the difference between their information reports and prediction reports to be similar to a typical honest user, to ensure that their misleading decisions will be taken into account by the FC. Consequently, they have to afford more loss for conducting attacks because the lower uncertainty index leads to further distance between falsified $Y_{i,j}$ and actual $P(S_j = 1|D_i = d_i)$, resulting in a lower average prediction score.

Algorithm 1 A Private-Prior Peer-Prediction Method for CSS

```
Given the time slot index $t = 0$, the FC initializes the parameters $\alpha$ and $\beta$, the threshold $\theta$ and the number of malicious suspects $K$;
for each time slot $t$ do
    Remove the SUs with $P_f + P_m \geq 1$ and $P_{fa} + P_{md} \geq 1$;
    for each SU $i$ do
        Choose an SU $j \neq i$ randomly which isn't the peer of any previous SU;
        Ask SU $i$ for its information report $X_{i,j}$;
    end for
    All SUs sense the signal of the PU in the channel;
    for each SU $i$ do
        Ask SU $i$ for its prediction report $Y_{i,j}$;
        Get the implied decision using Eq. (14);
        Calculate uncertainty index $\phi_{i,j}$ utilizing Eq. (17);
        if $\phi_{i,j} \geq \theta$ then
            Remove SU $i$'s decision from the decision pool;
        end if
    end for
    Calculate each SU's score using Eqs. (15) and (16);
    Remove the decisions of $K$ SUs with lowest accumulative scores from the decision pool;
    Make the final decision of CSS by fusion rule in the decision pool;
end for
```

In Algorithm 1, we provide the procedures of the proposed private-prior peer-prediction algorithm in detail. In the following section, we will examine the effectiveness of the algorithm by simulation.

V. Peer-Prediction Method for Data Fusion

In this section, we first propose a continuous peer-prediction method for elicit truthful reports from SUs based on data fusion. Then, we utilize a continuous strictly proper scoring rule to incentivize SUs to report honestly and identify malicious suspects simultaneously. In addition, we will prove the incentive compatibility of the continuous private-prior peer-prediction method by verifying it is a perfect Bayesian equilibrium. Finally, a report consistency threshold is proposed to prevent SUs sending contradictory reports to mitigate their loss while attacking.

A. Continuous Private-Prior Peer-Prediction

In addition to the basic private-prior peer-prediction, in order to incentivize SUs to report honest continuous signals in the data fusion, we propose continuous private-prior peer-prediction based on the fundamental case. Similarly, the FU selects a peer SU j randomly for each SU i without repetition in each time slot. Before the energy detector senses the PU's signal in the channel in each time slot, each SU i is required to predict the probability density function (PDF) of the energy of the received signal reported by its peer SU to the FC, denoted as $\mathbf{X}_{i,j}$. According to Eq. (2), the energy of the signal that SU j receives follows the linear combination of two chi-square distributions, namely,

$$S_j \sim P_i(\mathcal{H}_0)\chi^2_{2\mu} + P_i(\mathcal{H}_1)\chi^2_{2\mu}(2\gamma_{i,j}) \tag{18}$$

where $\gamma_{i,j}$ is the jth SU's SNR from prospective of SU i before sensing the signal in the channel. Because the time bandwidth product is a constant by assumption, there are two degrees of freedom $P_i(\mathcal{H}_1)$ and $\gamma_{i,j}$ when deciding the actual distribution of the signal energy. Therefore, SU i merely needs to report $P_i(\mathcal{H}_1)$ and $\gamma_{i,j}$ to the FC and the PDF is given by

$$\begin{aligned}\mathbf{X}_{i,j}(x) &= f_i(S_j = x)\\ &= P_i(\mathcal{H}_1)P_i(S_j = x|\mathcal{H}_1) + P_i(\mathcal{H}_0)P_i(S_j = x|\mathcal{H}_0)\\ &= P_i(\mathcal{H}_1)\frac{1}{2}e^{-\frac{x+2\gamma_{i,j}}{2}}\left(\frac{x}{2\gamma_{i,j}}\right)^{\frac{\mu-1}{2}} I_{\mu-1}(\sqrt{2\gamma_{i,j}x})\\ &\quad +P_i(\mathcal{H}_0)\frac{1}{2^{\mu}\Gamma(\mu)}x^{\mu-1}e^{-\frac{x}{2}}.\end{aligned} \tag{19}$$

After observing the PU's signal and measuring the energy of the signal using the energy detector, SU i is required to submit the signal report $S_i = E_i$ and the prediction report which is the PDF of the energy observed by SU j, denoted by $\mathbf{Y}_{i,j}$, based on the signal it received. After SU i updates the posterior probability, $\mathbf{Y}_{i,j}$ can be obtained as

$$\begin{aligned}&\mathbf{Y}_{i,j}(x)\\ &\quad = f_i(S_j = x|E_i = e_i)\\ &\quad = P_i(\mathcal{H}_1|E_i = e_i)P_i(S_j = x|\mathcal{H}_1)\\ &\qquad +P_i(\mathcal{H}_0|E_i = e_i)P_i(S_j = x|\mathcal{H}_0)\\ &\quad = P_i(\mathcal{H}_1|E_i = e_i)\frac{1}{2}e^{-\frac{x+2\gamma'_{i,j}}{2}}\left(\frac{x}{2\gamma'_{i,j}}\right)^{\frac{\mu-1}{2}} I_{\mu-1}(\sqrt{2\gamma'_{i,j}x})\\ &\qquad +P_i(\mathcal{H}_0|E_i = e_i)\frac{1}{2^{\mu}\Gamma(\mu)}x^{\mu-1}e^{-\frac{x}{2}}\end{aligned} \tag{20}$$

where $\gamma'_{i,j}$ is the SNR of the signal received by SU j, which is estimated by SU i after it receives the PU's signal and

$$\begin{aligned}&P_i(\mathcal{H}_1|E_i = e_i)\\ &\quad = \frac{P(E_i = e_i|\mathcal{H}_1)P_i(\mathcal{H}_1)}{P(E_i = e_i|\mathcal{H}_1)P_i(\mathcal{H}_1) + P(E_i = e_i|\mathcal{H}_0)P_i(\mathcal{H}_0)}\end{aligned} \tag{21}$$

which can be obtained from Eqs. (5) and (6). Similar to the information report, $\mathbf{Y}_{i,j}$ also has two degrees of freedom $P_i(\mathcal{H}_1|E_i = e_i)$ and $\gamma'_{i,j}$. Once SU i reports the two values, its prediction report is uniquely determined. In addition, all subjective prior information about the PU's signal of each SU will not affect its signal report, but merely the accuracy of its information and prediction report, which are related to the score it will obtain in each time slot.

Similarly, K SUs who have the lowest cumulative scores will be removed from the fusion pool when the FC makes the final decision.

B. The Continuous Scoring Rule

Without loss of generality, if the peer of SU h is SU i, and the peer of SU i is SU j, the score of SU i in each time slot is the weighted sum of its signal score, information score and prediction score calculated by the continuous strictly proper scoring rule, namely,

$$U_i = \underbrace{\alpha R(\mathbf{Y}_{h,i}, S_i)}_{\text{Signal Score}} + \underbrace{\beta R(\mathbf{X}_{i,j}, S_j)}_{\text{Information Score}} + \underbrace{\gamma R(\mathbf{Y}_{i,j}, S_j)}_{\text{Prediction Score}} + \delta \tag{22}$$

where α, β and γ are positive coefficients chosen according to the actual situation and δ is a parameter to balance the average score of the whole system in each time slot to equal zero. The function $R(\mathbf{y}, x_0)$ is the quadratic scoring rule defined by

$$R(\mathbf{y}(x), x_0) = 2\mathbf{y}(x_0) - \int_{x\in Q}\mathbf{y}^2(x)dx \tag{23}$$

where Q is the domain of x [34]. Similar to the binary rule, one can strictly maximize the expectation of the continuous quadratic scoring function by reporting the PDF $\mathbf{y}(x)$ which is equal to the actual distribution of the signal x [32], [34].

C. Incentive Compatibility

To prove the incentive compatibility of the mechanism, generally consider the score of SU i in the system, with the relationship among the SUs h, i and j the same as is presumed previously. We assume that SU h and SU j are honest and that SU h believes SU i is also honest. SU i's belief that S_j will follow the distribution $f_i(S_j)$ before receiving the PU's signal, that S_j will follow the distribution $f_i(S_j|E_i = e_i)$ after receiving the PU's signal and that SU h will make the density $f_h(S_i|E_h = e_h)$ the prediction report, is consistent being derived from the Bayes rule under the assumed strategy profile. In addition, because of the temporal separation, the one SU's information report, signal report and prediction report only affects their corresponding scores and do not interfere with other SUs. Thus to maximize the total score, the SU i should maximize the three scores independently. First of all, only by reporting $\mathbf{X}_{i,j}$ and $\mathbf{Y}_{i,j}$ that follow the actual distribution of the signal S_j can SU i maximize the expectations of its information and prediction scores. Secondly, due to the stochastic relevance of S_i and E_h, $f_h(S_i|E_h = e_h) \neq f_h(\hat{S}_i|E_h = e_h)$ if S_i and $\hat{S}_i$ are two different random variables distributed differently. Recalling the fact that the strict proper scoring rule strictly maximizes the expectation only when the signal follows its distribution function, SU i can only obtain the maximum expectation of the signal score by truthfully providing its signal report following the actual distribution. Thus, the mechanism is sequentially rational.

Because of the consistency and sequential rationality of the mechanism, it is a perfect Bayesian equilibrium when every SU truthfully reports the sensing data, and it is strict since the strict proper scoring rule guarantees maximizing the expectation of the score uniquely [29]. Therefore, it is a strictly incentive compatible mechanism to incentivize SUs to report truthfully.

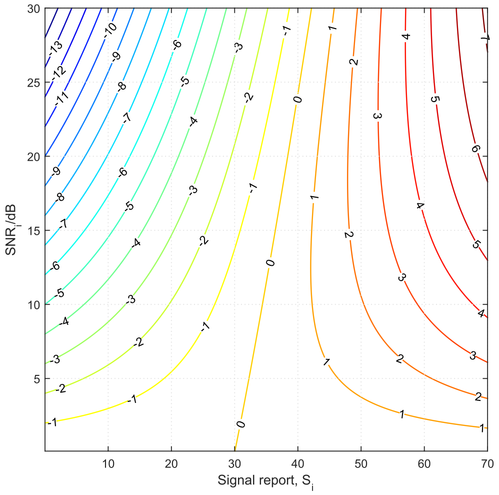

Fig. 2. Contour plot of $\log\left(\frac{P(S_i|\mathcal{H}_1)}{P(S_i|\mathcal{H}_0)}\right)$ for different values of SNR_i and signal reports S_i ($\mu = 15$ is assumed).

D. Report Consistency

In order to achieve a high score while conducting SSDF attacks, the malicious SU may submit the information and prediction report as accurately as possible but misstate the signal report if no further punishment is rendered to deter the report inconsistency. Thus, a mechanism to check the consistency among the three reports of one SU is proposed to identify potential attacks. Taking advantage of the data fusion rule, the malicious SU i can effectively manipulate the final decision by reporting S_i as far away as possible from the actual E_i such that $\frac{P(S_i|\mathcal{H}_1)}{P(S_i|\mathcal{H}_0)}$ is much smaller than λ under $\mathcal{H}_1$ or much larger than λ under $\mathcal{H}_0$ to neutralize the contribution of other honest SUs. The value of $\frac{P(S_i|\mathcal{H}_1)}{P(S_i|\mathcal{H}_0)}$ can be obtained with the signal report of the SU and γ_i by updating the two chi-square distribution functions in eqs. (5) and (6). In addition, when it truthfully reports the information and prediction reports, $\frac{P(E_i|\mathcal{H}_1)}{P(E_i|\mathcal{H}_0)}$ can be obtained as,

$$\frac{P(E_i|\mathcal{H}_1)}{P(E_i|\mathcal{H}_0)} = \frac{P_i(\mathcal{H}_1)\big(1 - P_i(\mathcal{H}_1|E_i)\big)}{P_i(\mathcal{H}_1|E_i)\big(1 - P_i(\mathcal{H}_1)\big)} \tag{24}$$

where $P_i(\mathcal{H}_1)$ and $P_i(\mathcal{H}_1|E_i)$ can be obtained directly from the information and prediction reports. If SU i truthfully reports $S_i = E_i$, and γ_i obtained by the FC is consistent with the actual SNR_i, $\frac{P(E_i|\mathcal{H}_1)}{P(E_i|\mathcal{H}_0)} = \frac{P(S_i|\mathcal{H}_1)}{P(S_i|\mathcal{H}_0)}$ is always true.

Fig. 2 demonstrates that if $\frac{P(S_i|\mathcal{H}_1)}{P(S_i|\mathcal{H}_0)}$ is certain, the truthful signal report is restricted in a limited domain by the range of the reasonable SNR. Therefore, any signal report outside of the range can be regarded as a falsified report and thus can be rejected by the FC. In order to identify such inconsistency, the system sets a consistency threshold θ to constrain the error between the implied SNR_i, denoted by $\hat{\gamma}_i$, and γ_i. If $\frac{P(E_i|\mathcal{H}_1)}{P(E_i|\mathcal{H}_0)} = \frac{P(S_i|\mathcal{H}_1)}{P(S_i|\mathcal{H}_0)}$ is assumed, $\hat{\gamma}_i$ can be calculated by eqs. (5) and (6) or indicated by the contour plot with the corresponding time bandwidth product and replacing $\frac{P(S_i|\mathcal{H}_1)}{P(S_i|\mathcal{H}_0)}$ with $\frac{P(E_i|\mathcal{H}_1)}{P(E_i|\mathcal{H}_0)}$ obtained by eq. (24). The signal report made by the SU who satisfies $|\hat{\gamma}_i - \gamma_i| > \theta$ will be removed by the FC from the fusion pool. Not expecting its signal report to be rejected, the malicious SU, otherwise, will adapt its information and prediction report. As a consequence, it will expect lower scores by the scoring rule since the information and prediction report do not conform with the actual distributions.

Algorithm 2 A Continuous Private-Prior Peer-Prediction Method for CSS

```
Given the time slot index $t = 0$, the FC initializes the parameters $\alpha$, $\beta$, $\gamma$, the consistency threshold $\theta$ and the number of malicious suspects $K$;
for each time slot $t$ do
    for each SU $i$ do
        Choose an SU $j \neq i$ randomly which isn't the peer of any previous SU;
        Ask SU $i$ for its information report $\mathbf{X}_{i,j}$;
    end for
    All SUs sense the signal of PU in the channel with the time bandwidth product $\mu$;
    for each SU $i$ do
        Ask SU $i$ for its signal report $S_i$ and prediction report $\mathbf{Y}_{i,j}$;
        Check if $S_i$ is restricted in the range based on the consistency checking scheme;
        if $|\hat{\gamma}_i - \gamma_i| > \theta$ then
            Remove SU $i$'s decision from the fusion pool;
        end if
    end for
    Calculate each SU's score using Eqs. (22) and (23);
    Remove the decision of $K$ SUs with lowest cumulative scores from the fusion pool;
    Make the final decision of the CSS by fusion rule in the fusion pool;
end for
```

The proposed continuous private-prior peer-prediction method for data fusion is illustrated in Algorithm 2 in detail and we will assess the performance of the algorithm in the next section.

VI. Simulation Results

A. Decision Fusion

In this section, we demonstrate the effectiveness of Algorithm 1 for collaborative spectrum sensing in cognitive radio based on decision fusion by simulation. Assume that due to the varying distances of different SUs, each SU i has its error rates of sensing $P_{md,i} \in [0.05, 0.1]$ and $P_{fa,i} \in [0.05, 0.1]$. Also assume each SU has subjective prior knowledge of the activity of the PU with an error up to ±10% compared to the actual value. Trained by several groups of typical sensing data, the threshold of the uncertainty index θ is set as 0.1. We consider a large number of malicious SUs conducting SSDF attacks who are able to afford any great loss from the scheme. All malicious SUs attack simultaneously, while each controls its error rates of reporting $P_f < 0.5$, $P_m < 0.5$ and the uncertainty index $\phi_{i,j} < \theta$ to avoid its decision being removed by the FC from the decision pool. Parameters α and β are set as 1. A censored majority rule

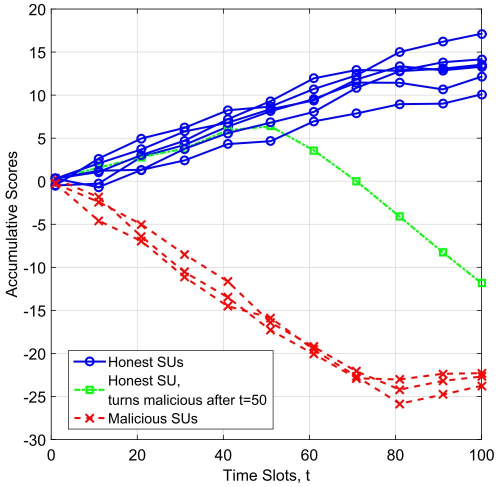

Fig. 3. The score variation under different types of SU behaviors, with subjective prior information $P(\mathcal{H}_1)$.

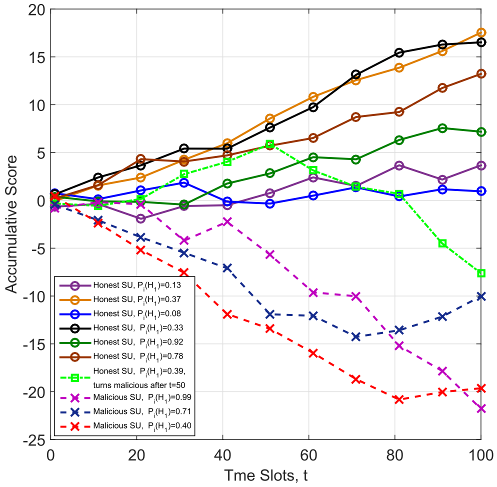

Fig. 4. The score variation under different types of SU behaviors, without prior information $P(\mathcal{H}_1)$.

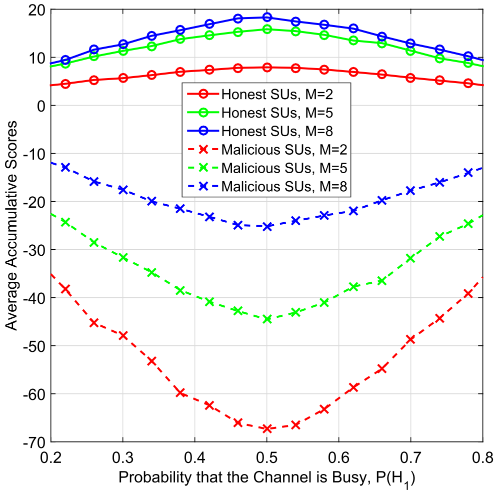

Fig. 5. The stability of scores for different proportions of malicious SUs and PU's activities.

is adopted in our proposed scheme and we will compare our proposed scheme with the uncensored majority rule scheme.

1) Effectiveness of Incentive Mechanism: In the simulation, we set the number of SUs N as 10 and the total number of time slots T as 100. The number of attackers M is set to be 3 and $P(\mathcal{H}_1) = 0.5$. In Fig. 3 we demonstrate the varying scores between honest SUs and malicious SUs according to time. After $t = 50$, one of the honest SUs becomes malicious, and after $t = 80$, the initial three malicious SUs stop conducting attacks. The following results can be inferred from the observations. (i). There is merely minor variation of the scores of different SUs among the same type due to the different sensing error rates and the peers matched to them in each time slot. (ii). After 10 time slots, all honest SUs gain cumulative scores higher than malicious SUs, and the scores of malicious SUs decrease rapidly while those of honest SUs increase, so that the scores in the whole CSS system sum up to zero. (iii). The proposed incentive scheme is sensitive and impartial because once an honest SU turns malicious, its score reduces rapidly as fast as the scores of Fakother malicious SUs. Moreover, as long as a malicious SU stops sending falsified reports, the cumulative score merely fluctuates slightly and the total penalty remains approximately constant. It is interesting that after $t = 80$, the scores of both the initial malicious SUs and honest SUs increase slightly. That is because the score of the SU who turns malicious partway still decreases, but the total income of the system has to remain zero.

To demonstrate the proposed incentive algorithm is robust, Fig. 4 is plotted for the case when all SUs do not have accurate subjective prior knowledge and assume a completely arbitrary $P_i(\mathcal{H}_1) \in [0, 1]$. θ is set as 0.5. Compared to Fig. 3, the scores of SUs among the same type vary more widely because of the incorrect estimation of $P(\mathcal{H}_1)$ when computing information and prediction reports with Eqs. (8), (11) and (12). Although the SU who obtains more accurate subjective prior belief gains more reward, malicious SUs still have the lowest scores, even if some of the malicious SUs get more accurate prior knowledge. However, every SU is actually able to get a relatively accurate subjective prior knowledge from the expected regularity of the PU's activity, so $P_i(\mathcal{H}_1)$ will be more reliable than what is assumed in this simulation.

2) Stability of the Scores: In the simulation, we set the number of SUs N as 20 and the total number of time slots T as 200. We examine the stability of the scoring function when M and $P(\mathcal{H}_1)$ vary. It can be observed from Fig. 5 that honest SUs always have higher average cumulative scores than malicious SUs do, despite variation in the values of $P(\mathcal{H}_1)$ and the number of malicious SUs. When M declines, the malicious SU is more likely to be matched with an honest peer and thus will have to afford greater loss than the situation where it is matched with another cooperating attacker. The difference in scores between honest SUs and malicious SUs decreases when $P(\mathcal{H}_1)$ is extremely high or low mainly because malicious SUs have fewer opportunities to attack while maintaining $P_f < 0.5$ and $P_m < 0.5$, and honest SUs have lower expectations on prediction scores under those circumstances. However, an adaptive design of α and β can be introduced to the proposed scheme according to $P(\mathcal{H}_1)$ observed by the FC, in order to maintain the loss in scores resulting from malicious activities constant when $P(\mathcal{H}_1)$ varies.

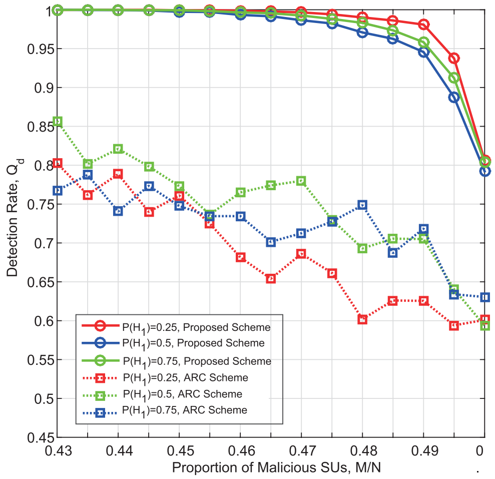

Fig. 6. Comparison of the detection rates for the proposed scheme and the ARC scheme under heavy SSDF attacks.

3) Performance Evaluation: In this section, we set the number of SUs N as 200, and the total number of time slots T as 200. The number of attackers M varies from 86 to 100 and $P(\mathcal{H}_1)$ varies from 0.25 to 0.75. We do not consider the maximum loss that a malicious SU can afford. We demonstrate better performance results from our peer-prediction based mechanism than that of the ARC scheme proposed in [22]. In Fig. 6, the detection rate of the ARC scheme is below 85% because some honest SUs are aggregated into malicious clusters and have relatively lower reputation. Considering the rationality of malicious SUs and their tolerance for loss, they have to reduce their attacking rate or even become reluctant to attack, for they cannot expect a positive income when attacking.

B. Data Fusion

In this section, we use simulation to illustrate the performance of Algorithm 2 in collaborative spectrum sensing based on data fusion. In the simulation, we assume the time bandwidth product $\mu = 15$ and the average SNR of all SUs $\bar{\gamma} = 15$ dB. To optimize the detection rate, we set the threshold $\lambda = 1$ and consistency threshold $\theta = 5$. Similar to the decision fusion, we consider heavy SSDF attacks and every malicious SU can afford any large loss from the attacks without turning into a honest node when the punishment reaches the maximum of its tolerance. Parameters α, β and γ are set as 20 because the scale of the continuous peer-prediction itself is not large enough.

1) Effectiveness of Incentive Mechanism: In the simulation, we will demonstrate the score difference between honest SUs and malicious SUs. We set the number of SUs N as 10 and the total number of time slots T as 100. The number of malicious SUs M is set as 3. As is illustrated in Fig. 7, all honest SUs have scores larger than 15, while those of the malicious SUs are all less than -50. A significant gap between malicious SUs and honest ones can be observed. However, the score of continuous private-prior peer-prediction is slightly more unstable than in the binary case, since the SUs report actual continuous sensing data, instead of 0 and 1 decisions.

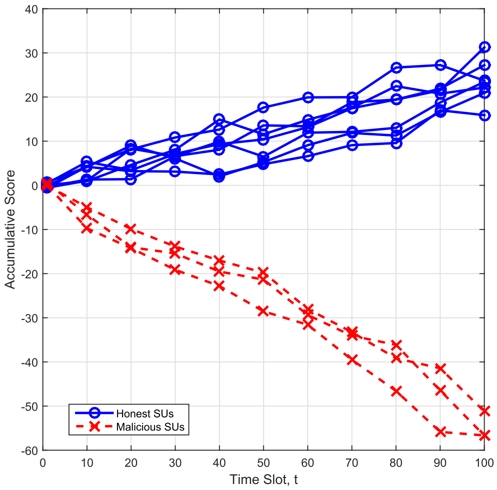

Fig. 7. The score variation under different types of SU behaviors.

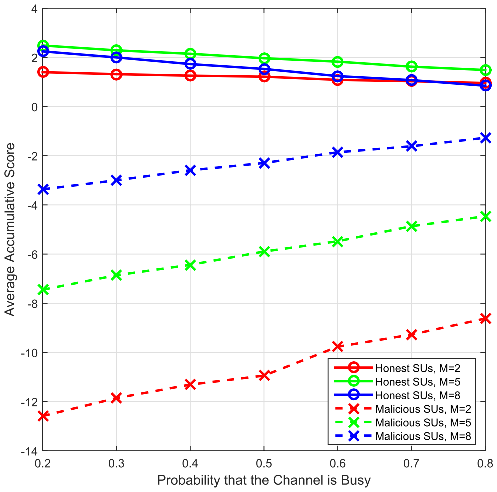

Fig. 8. The stability of scores for different proportions of malicious SUs and PU's activities.

The larger diversity of the reports contributes to the fluctuation and the larger diversity of the scores within the SU group with the same type.

2) Stability of the Scores: We set the number of SUs N as 20 and the total number of time slots T as 200 in order to examine the stability of the mechanism with different numbers of attackers and values of $P(\mathcal{H}_1)$. It is indicated from Fig. 8 that honest SUs always have a significantly higher average score than the malicious SUs. Similar to the results found for decision fusion, a smaller number of malicious SUs leads to heavier punishment to each attacker. In addition, malicious SUs earn more scores when the PU has a higher possibility of occupying the channel, which mainly results from different values that malicious SUs report to mislead the sensing results based on the current attack strategy. Such unbalance will also be adjusted by assigning different values of the coefficients α, β and γ when $P(\mathcal{H}_1)$ changes.

3) Performance Evaluation: Fig. 9 shows the improvement in detection probability (Q_d) of the proposed continuous private-prior peer-prediction method compared to the basic scheme without attack prevention. We set the number of SUs N as 100 and the total number of time slots T as 200.

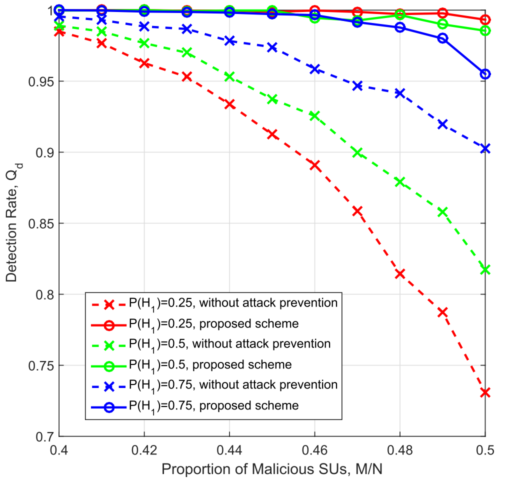

Fig. 9. Comparison of the detection rates for the proposed scheme and the basic scheme without attack prevention under heavy SSDF attacks.

The number of malicious SUs M varies from 40 to 50 and $P(\mathcal{H}_1)$ is set as 0.25, 0.5 and 0.75. Observe that when the number of malicious SUs is less than 50%, the proposed method has a significantly better performance than the method without attack prevention. The detection rate of the proposed method is above 95% no matter what $P(\mathcal{H}_1)$ is, while that of the method without attack prevention is around 75% to 90%. The value of the detection threshold λ is selected according to the different requirements of false alarm probability and missed detection probability, which also leads to the results demonstrated in Fig. 9 that the system performs the best when $P(\mathcal{H}_1) = 0.75$ without using the attack prevention method. However, the proposed scheme performs the worst when $P(\mathcal{H}_1) = 0.75$ because malicious SUs obtain relatively higher scores when the PU occupies the channel more frequently as is shown in Fig. 8.

VII. Conclusion

In this paper, we have proposed two incentive attack prevention schemes, for collaborative spectrum sensing in CRNs based on decision fusion and data fusion to motivate SUs to report truthful sensing results and identify malicious suspects based on private-prior peer-prediction and continuous private-prior peer-prediction.

In the decision fusion, each SU's local sensing decision is judged by comparing the relationship between the information report and the prediction report, and then the score can be calculated by the binary quadratic scoring rule; while in the data fusion, each SU's local signal report is directly sent to the FC, together with the information report and the prediction report for calculating the score by utilizing the continuous quadratic scoring rule. In order to increase the loss incurred by malicious SUs, we have introduced the threshold of the uncertainty index for the decision fusion to constrain the value of the prediction reports, and consistency threshold for the data fusion to ensure the coherence among signal, information and prediction reports. Compared to the proposed method for decision fusion the continuous private-prior peer-prediction method further improves the detection rate at the cost of little added complexity. From the simulation results, we can observe that the honest SUs obtain significantly higher scores than the malicious SUs and that the proposed schemes have higher detection probabilities compared with the ARC scheme and the methods without attack prevention under heavy SSDF attacks.

References

[1] K. B. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proc. IEEE*, vol. 97, no. 5, pp. 878–893, May 2009.

[2] C. Jiang, N. C. Beaulieu, L. Zhang, Y. Ren, M. Peng, and H.-H. Chen, "Cognitive radio networks with asynchronous spectrum sensing and access," *IEEE Netw.*, vol. 29, no. 3, pp. 88–95, May/Jun. 2016.

[3] J. Mitola and G. Q. Maguire, Jr., "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Apr. 1999.

[4] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[5] C. Jiang, Y. Chen, and K. J. R. Liu, "Multi-channel sensing and access game: Bayesian social learning with negative network externality," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2176–2188, Apr. 2014.

[6] C. Jiang, Y. Chen, Y. Gao, and K. J. R. Liu, "Joint spectrum sensing and access evolutionary game in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2470–2483, May 2013.

[7] C. Jiang, H. Zhang, Y. Ren, and H. Chen, "Energy-efficient non-cooperative cognitive radio networks: Micro, meso, and macro views," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 14–20, Jul. 2014.

[8] T. Yücek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, 1st Quart., 2009.

[9] F. Gao, J. Li, T. Jiang, and W. Chen, "Sensing and recognition when primary user has multiple transmit power levels," *IEEE Trans. Signal Process.*, vol. 63, no. 10, pp. 2704–2717, May 2015.

[10] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE DySPAN*, Nov. 2005, pp. 131–136.

[11] R. Tandra and A. Sahai, "Fundamental limits on detection in low SNR under noise uncertainty," in *Proc. IEEE IWCMC*, vol. 1. Jun. 2005, pp. 464–469.

[12] Z. Chen and F. Gao, "Cooperative-generalized-sensing-based spectrum sharing approach for centralized cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3760–3764, May 2016.

[13] H. Zhang, C. Jiang, X. Mao, and H. H. Chen, "Interference-limited resource optimization in cognitive femtocells with fairness and imperfect spectrum sensing," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1761–1771, Mar. 2016.

[14] J. Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4502–4507, Nov. 2008.

[15] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 1st Quart., 2013.

[16] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2488–2497, Aug. 2010.

[17] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3554–3565, Nov. 2010.

[18] L. Duan, A. W. Min, J. Huang, and K. G. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1658–1665, Oct. 2012.

[19] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Countering Byzantine attacks in cognitive radio networks," in *Proc. IEEE ICASSP*, Mar. 2010, pp. 3098–3101.

[20] H. Chen, X. Jin, and L. Xie, "Reputation-based collaborative spectrum sensing algorithm in cognitive radio networks," in *Proc. IEEE PIMRC*, Sep. 2009, pp. 582–587.

[21] E. Soltanmohammadi and M. Naraghi-Pour, "Fast detection of malicious behavior in cooperative spectrum sensing," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 3, pp. 377–386, Mar. 2014.

[22] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1707–1719, Aug. 2014.

[23] D. R. Pauluzzi and N. C. Beaulieu, "A comparison of SNR estimation techniques for the AWGN channel," *IEEE Trans. Commun.*, vol. 48, no. 10, pp. 1681–1691, Oct. 2000.

[24] N. Miller, P. Resnick, and R. Zeckhauser, "Eliciting informative feedback: The peer-prediction method," *Manage. Sci.*, vol. 51, no. 9, pp. 1359–1373, 2005.

[25] J. Witkowski and D. C. Parkes, "Peer prediction without a common prior," in *Proc. ACM Conf. Electron. Commerce*, 2012, pp. 964–981.

[26] B. Faltings, J. J. Li, and R. Jurca, "Incentive mechanisms for community sensing," *IEEE Trans. Comput.*, vol. 63, no. 1, pp. 115–128, Jan. 2014.

[27] A. Ghosh, K. Ligett, A. Roth, and G. Schoenebeck, "Buying private data without verification," in *Proc. ACM Conf. Econ. Comput.*, 2014, pp. 931–948.

[28] G. Radanovic and B. Faltings, "Incentives for truthful information elicitation of continuous signals," in *Proc. AAAI Conf. Artif. Intell.*, 2014, pp. 770–776.

[29] P. Zhang and Y. Chen, "Elicitability and knowledge-free elicitation with peer prediction," in *Proc. AAMAS*, Richland, SC, USA, 2014, pp. 245–252.

[30] W. Zhang, R. K. Mallik, and K. B. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5761–5766, Dec. 2009.

[31] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions* (Applied Mathematics Series), vol. 55. New York, NY, USA: Dover, 1966, p. 62.

[32] T. Gneiting and A. E. Raftery, "Strictly proper scoring rules, prediction, and estimation," *J. Amer. Statist. Assoc.*, vol. 102, no. 477, pp. 359–378, 2007.

[33] R. Selten, "Axiomatic characterization of the quadratic scoring rule," *Experim. Econ.*, vol. 1, no. 1, pp. 43–62, 1998.

[34] J. E. Matheson and R. L. Winkler, "Scoring rules for continuous probability distributions," *Manage. Sci.*, vol. 22, no. 10, pp. 1087–1096, 1976.

Yu Gan received the B.E. degree in electronic engineering from Tsinghua University, Beijing, China, in 2016. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Cornell University, Ithaca, NY, USA. His research interests include wireless communications and computer systems.

Chunxiao Jiang (S'09–M'13–SM'15) received the B.S. degree (Hons.) in information engineering from Beihang University, Beijing, in 2008, and the Ph.D. degree (Hons.) in electronic engineering from Tsinghua University, Beijing, in 2013. From 2011 to 2014, he visited the Signals and Information Group with the Department of Electrical and Computer Engineering, University of Maryland, College Park, sponsored by China Scholarship Council. He is currently an Assistant Research Fellow with the Tsinghua Space Center, Tsinghua University. His research interests include application of game theory, optimization, and statistical theories to communication, networking, signal processing, and resource allocation problems, in particular space information networks, heterogeneous networks, social networks, and big data privacy. He has authored or co-authored over 100 technical papers in renowned international journals and conferences, including over 50 renowned the IEEE journal papers. He has been actively involved in organizing and chairing sessions, and has served as a member of the Technical Program Committee and the Symposium/Workshop Chair for a number of international conferences. He is currently an Editor of the *Wiley Wireless Communications and Mobile Computing*, *Wiley Security and Communications Networks*, and *International Journal of Big Data Intelligence*, and a Guest Editor of the *ACM/Springer Mobile Networks & Applications* Special Issue on Game Theory for 5G Wireless Networks. He was a recipient of the best paper award from the IEEE Globecom in 2013, the Best Student Paper Award from the IEEE GlobalSIP in 2015, the Distinguished Dissertation Award from Chinese Association for Artificial Intelligence in 2014, and the Tsinghua Outstanding Postdoc Fellow Award (only ten winners each year) in 2015. He is a Senior Member of the IEEE Communication Society.

Norman C. Beaulieu (S'82–M'86–SM'89–F'99) received the B.A.Sc., M.A.Sc., and Ph.D. degrees from the University of British Columbia, Vancouver, Canada. He was subsequently a Queen's Nation Scholar Professor with Queen's University, Kingston, Canada, and an Alberta Informatics Circle of Research Excellence and a Canada Research Chair Professor with the University of Alberta, Edmonton, Canada. He is currently a Thousand Talents Professor with the Beijing University of Posts and Telecommunications, Beijing, China.

He has authored or co-authored over 342 journal papers, and over 428 conference papers. His current research interests are the statistical modeling of wireless channels, cognitive radio, cooperative communications, massive multiple-input multiple-output systems, wideband wireless communications, signal processing in communications, and impulse radio.

Dr. Beaulieu was the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS for four years, and has been a Special Editor, a Senior Editor, and an Associate Editor of a number of the IEEE and non-IEEE journals, and serving on the Editorial Board of The Proceedings of the IEEE. He has served as the Technical Program Chair, or the Symposium Chair of multiple international conferences, as well as on a number of awards and funding committees in multiple countries and organizations. He is a fellow of the Royal Society of Canada, the IET, the EIC, the CAE, and an NSERC E.W.R. Steacie Memorial Fellow. He is the only person in the world to hold both the IEEE Edwin Howard Armstrong Technical Achievement Award, named for the inventor of FM, and the IEEE Reginald Aubrey Fessenden Medal for Technical Achievement, named for the inventor of AM. In 2016, he was awarded the title State Specially Recruited Experts bestowed upon him by the Minister of Human Resources and Social Insurance and the Vice Minister of the Organization Department, Y. Weimin.

Jian Wang (M'12) received the Ph.D. degree in electronic engineering from Tsinghua University in 2006. In 2006, he joined the Faculty of Tsinghua University, where he is currently an Associate Professor with the Department of Electronic Engineering. His research interests include wireless security, embedded device security, privacy-enhancing technology, and signal processing in the encrypted domain and cognitive radio networks.

Yong Ren (SM'16) received the B.S., M.S., and Ph.D. degrees from the Harbin Institute of Technology, China, in 1984, 1987, and 1994, respectively, all in electronic engineering. He held a post-doctoral position with the Department of Electronic Engineering, Tsinghua University, China, from 1995 to 1997. He is currently a Professor with the Department of Electronic Engineering and the Director of the Complexity Engineered Systems Laboratory with Tsinghua University. He holds 12 patents, and has authored or co-authored over 100 technical papers in the behavior of computer network, P2P network, and cognitive networks. He serves as a Reviewer of *IEICE Transactions on Communications*, *Digital Signal Processing*, *Chinese Physics Letters*, *Chinese Journal of Electronics*, *Chinese Journal of Computer Science & Technology*, and *Chinese Journal of Aeronautics*. His current research interests include complex systems theory and its applications to the optimization and information sharing of the Internet, Internet of Things, and ubiquitous network, cognitive networks, and cyber-physical systems.