Incentive Attack Prevention for Collaborative Spectrum Sensing: A Peer-Prediction Method

Yu Gan*, Chunxiao Jiang*, Wei Zhang†, Norman C. Beaulieu‡, and Yong Ren*
*Department of Electronic Engineering, Tsinghua University, Beijing 100084, P. R. China
†School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney NSW 2052, Australia
‡Beijing University of Posts and Telecommunications, P. R. China

***Abstract*—Collaborative spectrum sensing is an effective method to improve the detection rate in cognitive radio. However, it is vulnerable to spectrum sensing data falsification attacks. In order to improve the robustness, numerous attack prevention schemes have been proposed to identify malicious secondary users (SUs). Nevertheless, most of them neglect to incentivize SUs to send truthful reports. Therefore, an incentive method based on Private-Prior Peer-Prediction with approximate subjective priors is proposed to identify malicious suspects and punish attackers when falsifying the sensing data simultaneously. The theoretical analysis and simulation results demonstrate that honest SUs are rewarded by accurate and truthful sensing results while malicious SUs receive heavy loss for making falsified sensing results. Moreover, a significant improvement of detection rates is demonstrated when there are a large number of malicious SUs conducting cooperative attacks compared to the pure majority rule scheme.**

I. Introduction

Frequency spectrum is becoming increasingly crowded as a consequence of the rapid development of wireless communications. However, it is utilized inefficiently because of the idle time of the licensed users (primary users, PUs). In order to solve this problem, cognitive radio networks (CRNs) have been proposed recently, allowing unlicensed users (secondary users, SUs) to utilize the spectrum without causing interfere to PUs [1], [2]. The essential step in CRNs is spectrum sensing, which aims to detect whether the spectrum is occupied by PUs and thus avoid interruption [3], [4]. However, single-user spectrum sensing is often unreliable because of the fading and shadowing in wireless channels. To improve the accuracy, collaborative spectrum sensing (CSS) has been proposed, which combines all SUs' observations to make the decision; this reduces the uncertainty in the system and improves reliability. Nevertheless, CSS is especially vulnerable to Spectrum Sensing Data Falsification (SSDF) attacks. In such attacks, malicious SUs send falsified local reports to the fusion center (FC) and mislead the overall decision in order to disturb the transmission of 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-proof mechanisms have been proposed in [5]–[11]. In [6], an outlier-detection scheme with partial prior knowledge of the PU has been proposed to identify malicious SUs whose results differ greatly from other SUs. In [7], an abnormality detection method has been proposed, which is able to recognize multiple malicious SUs without any prior information of attack strategies. In [8], Duan *et al.* have put forward a mechanism with direct and indirect penalties to SUs when the FC announces busy but collision happens to the PU. Considering various types of honest and malicious SUs, Soltanmohammadi and Naraghi-Pour in [9] have introduced an iterative expectation maximization based algorithm to identify malicious SUs.

However, most existing works mainly focus on the study of the algorithms to identify malicious SUs but ignore incentivizing SUs in CRNs to announce truthful local reports. Considering the fact that all SUs participating in CSS are naturally 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 the SU intends to send falsified sensing reports, if there is no mechanism to punish SUs when lying. 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 decision fusion as the number of malicious SUs increases. Furthermore, some of the previous schemes rely on accurate common prior knowledge of the activity of the PU, and assume each SU's private error rate of sensing is shared by all SUs, which are not realistic. Moreover, CSS networks are extremely vulnerable to heavy cooperative attacks by a high percentage of malicious SUs, but only a few previous works consider this extreme condition in their studies.

Therefore, in this paper, we propose a mechanism based on *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. The scheme merely requires the SU's approximate subjective estimation of the prior knowledge of the PU's activity. In [12], 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 [13] and [14]. This scheme is adequate for the circumstances where prior knowledge is subjective and private to each agent. The Peer-Prediction method has been utilized to collect truthful reports on website reviews, pollution detection [15] and private surveys [16], which is regarded as an effective way to elicit truthful feedback.

978-1-4799-5952-5/15/$31.00 ©2015 IEEE

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 in collaborative spectrum sensing in Section III. Simulation results are demonstrated in Section IV, and conclusions are drawn in Section V.

II. System Model

In our paper, we consider a CRN with one PU who has the license to transmit data in one channel and N SUs who conduct collaborative spectrum sensing independently, each making hard decisions, denoted by $D_i \in \{0,1\}$, on whether the channel is idle or busy by utilizing energy detection, and generating a binary sensing report, denoted by $S_i \in \{0,1\}$. The two different states of the channel are denoted by $\mathcal{H}_0$ and $\mathcal{H}_1$, which represent the channel is idle or busy, respectively. Among N SUs, there are M malicious SUs and they cannot be predominant in a normal CSS network, thus $M < \frac{1}{2}N$. All honest SUs report what they detect locally and are uninterested in the final fusion results, while malicious SUs report according to their attack strategies and desire to dominate the FC's final decision. In this paper, we primarily focus on protection against cooperative attacks, which means that all malicious SUs are able to contact each other and will conduct attacks together.

A total number of T time slots are considered in the process and in each time slot, every SU senses the channel and reports its detection to the FC only once. Each SU i has its own false alarm probability of sensing $P_{fa,i}$, missed detection probability of sensing $P_{md,i}$, false alarm probability of reporting $P_{f,i}$, missed detection probability of reporting $P_{m,i}$, and subjective prior belief in regard to the state of the channel $P_i(\mathcal{H}_1)$ which are implicit to the FC and other SUs. They remain constant in T time slots for simplicity. The SUs are assumed to be able to make an approximate estimation of $P(\mathcal{H}_1)$ based on the regularity of the PUs activity.

The FC fuses the decisions according to the fusion rule. In this paper, the final decision result will be based on majority rule, which generates a final result according to the decisions of most SUs in the decision pool. In addition, the FC will calculate a score (either rewards if it is positive, or penalties if it is negative) for each SU according to its reports in each time slot.

III. Peer-Prediction Method

In this section, we firstly introduce Private-Prior Peer-Prediction method for collecting truthful reports of SUs. With the utilization of 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 obtain. Lastly, we propose the uncertainty index and a method to enlarge the loss on scores of malicious SUs when conducting attacks based on the threshold to 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 feedback on online reviewing websites. 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 information and prediction reports and calculating the score of each agent by an appropriate scoring rule [13].

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:

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

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 $P^i_{att,md,j}$ and $P^i_{att,fa,j}$ 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 its respective subjective prior information according to

$$\begin{aligned} P^i_{f,j} &= (1 - P^i_{fa,j}) \cdot P^i_{att,fa,j} + P^i_{fa,j} \cdot (1 - P^i_{att,md,j}) \\ P^i_{m,j} &= (1 - P^i_{md,j}) \cdot P^i_{att,md,j} + P^i_{md,j} \cdot (1 - P^i_{att,fa,j}). \end{aligned} \tag{2}$$

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,

$$\begin{aligned} Y_{i,j} =& P_i(S_j = 1|D_i = d_i) \\ =& P_i(S_j = 1|\mathcal{H}_0) \cdot P_i(\mathcal{H}_0|D_i = d_i) \\ &+ P_i(S_j = 1|\mathcal{H}_1) \cdot P_i(\mathcal{H}_1|D_i = d_i). \end{aligned} \tag{3}$$

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

$$\begin{aligned} Y^0_{i,j} =& P_i(S_j = 1|D_i = 0) \\ =& \frac{P^i_{f,j} \cdot (1 - P_{fa,i}) \cdot P_i(\mathcal{H}_0) + (1 - P^i_{m,j}) \cdot P_{md,i} \cdot P_i(\mathcal{H}_1)}{P_{md,i} \cdot P_i(\mathcal{H}_1) + (1 - P_{fa,i}) P_i(\mathcal{H}_0)} \end{aligned} \tag{4}$$

$$\begin{aligned} Y^1_{i,j} =& P_i(S_j = 1|D_i = 1) \\ =& \frac{P^i_{f,j} \cdot P_{fa,i} \cdot P_i(\mathcal{H}_0) + (1 - P^i_{m,j}) \cdot (1 - P_{md,i}) \cdot P_i(\mathcal{H}_1)}{P_{fa,i} \cdot P_i(\mathcal{H}_0) + (1 - P_{md,i}) P_i(\mathcal{H}_1)}. \end{aligned} \tag{5}$$

The prediction report made by a well-functioning honest SU with low P_{fa} and P_{md} will not be 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 SU i and j, it holds that

$$P_i(S_j = 1|D_i = 1) > P_i(S_j = 1) > P_i(S_j = 1|D_i = 0). \tag{6}$$

Proof: For every SU 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 $P_f + P_m < 1$.

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

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

In our mechanism, to satisfy the condition of Proposition 1, the FC will restrict the SUs whose $P_f + P_m \geq 1$ and $P_{fa} + P_{md} \geq 1$ to participate in the CSS process. This is reasonable 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 speculated by the FC according to the following rule,

$$S_i = \begin{cases} 1 & Y_{i,j} > X_{i,j} \\ 0 & Y_{i,j} < X_{i,j}. \end{cases} \tag{7}$$

Note the fact that the accuracy of $P^i_{f,j}$ and $P^i_{m,j}$ are unnecessary for Proposition 1 to hold. It can be concluded that the imprecise estimation will have no influence on the accuracy of the judgement on SU i's decision using Eq. (7).

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,

$$U_i = \underbrace{\alpha \cdot R(X_{i,j}, S_j)}_{\text{Information Score}} + \underbrace{\beta \cdot R(Y_{i,j}, S_j)}_{\text{Prediction Score}} + \gamma \tag{8}$$

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

To maintain the average score in the whole system equal to zero, $\gamma = -\frac{1}{N}\sum_{i=1}^{N}\big[\alpha \cdot R(X_{i,j}, S_j) + \beta \cdot R(Y_{i,j}, S_j)\big]$. 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 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 accumulative scores are malicious. Thus, the FC sets an integer K and removes the decisions made by K SUs with lowest accumulative 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 [10] and [11] 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 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.

B. Scoring Rules

For a binary report $q \in \{0, 1\}$, a proper scoring rule $R(x, q)$ incentivizes the agents' accurate probabilistic predictions by

assigning different scores according to their reports x. And a strictly proper scoring rule maximizes the expectation of the scores if and only if the prediction reports equal the actual probabilities [17]. Furthermore, the binary quadratic scoring rule, according to Selten [18], is an incentive compatible strictly proper scoring rule. It is given by

$$\begin{aligned} R(x,0) &= 1-x^2 \\ R(x,1) &= 2x-x^2 \end{aligned} \tag{9}$$

for $x \in [0,1]$. Assuming p is probability of $q=1$, 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 can get a maximum when $x = p$ [13].

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 [12]. 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, 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 when it announces falsified report data.

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

Given the time slot index $t = 0$, the FC initializes the parameters α and β, the threshold θ 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 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. (7);
    Calculate uncertainty index $\phi_{i,j}$ utilizing Eq. (10);
    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 Eq. (8) and (9);
  Remove the decision 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

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 $Y^0_{i,j} = X_{i,j} - \varepsilon$ when $\mathcal{H}_1$ or $Y^1_{i,j} = X_{i,j} + \varepsilon$ when $\mathcal{H}_0$, 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}, $\frac{\partial Y^0}{\partial P_{md}} < 0$, $\frac{\partial Y^0}{\partial P_{fa}} < 0$, $\frac{\partial Y^1}{\partial P_{md}} > 0$ and $\frac{\partial Y^1}{\partial P_{fa}} > 0$. Thus, $Y^0(P_{md}, P_{fa})$ is a decreasing function while $Y^1(P_{md}, P_{fa})$ 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 $\widetilde{P}^j_{md,i}$ when observing $\mathcal{H}_0$ and so is the SU with low $\widetilde{P}^j_{fa,i}$ when observing $\mathcal{H}_1$. 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 of $\phi_{i,j}$ is then,

$$\phi_{i,j} = \begin{cases} \frac{(P_{f,j} - Y_{i,j})P(\mathcal{H}_0)}{\left[Y_{i,j} - (1-P_{m,j})\right]P(\mathcal{H}_1)} & \text{if } X_{i,j} > Y_{i,j} \\ \frac{\left[Y_{i,j} - (1-P_{m,j})\right]P(\mathcal{H}_1)}{(P_{f,j} - Y_{i,j})P(\mathcal{H}_0)} & \text{if } X_{i,j} < Y_{i,j}. \end{cases} \tag{10}$$

Eq. (10) above can be derived from Eq. (4) and (5) 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 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, decided 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, so 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 expectation of the prediction score.

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

IV. Simulation Results

In this section, we conduct several simulations to demonstrate the effectiveness of Algorithm 1 for collaborative spectrum sensing in cognitive radio. 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 $P_{fa,i} \in [0.05, 0.1]$. Besides, each SU has the subjective prior knowledge of the activity of the PU with an error up to $\pm 10\%$ 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 cooperative 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 majority fusion rule is adopted in our proposed scheme and we will compare our proposed scheme with the pure majority rule scheme.

A. 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. 1 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 accumulative 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

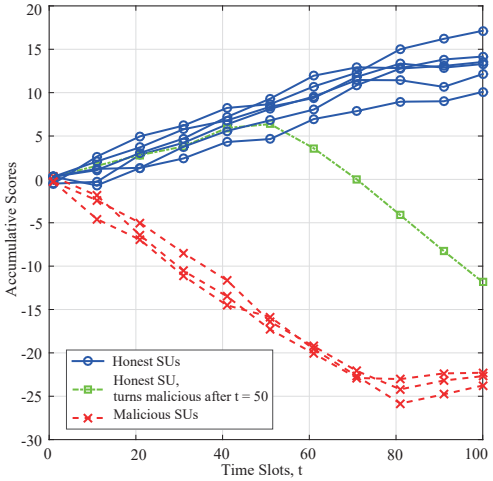

Fig. 1. Score variation under different types of SU behaviors.

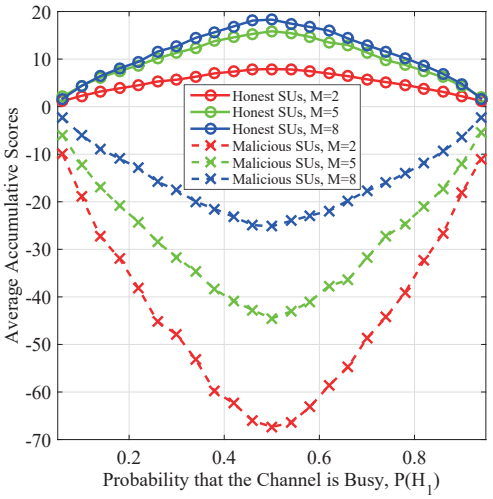

Fig. 2. Stability of scores for different proportions of malicious SUs and PU's activities.

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 other malicious SUs. Besides, as long as a malicious SU stops sending falsified reports, the accumulative score merely fluctuate slightly and the total penalty remains approximately constant. Moreover, it is noteworthy 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 halfway still decreases but the total income of the system has to remain zero.

B. 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. 2 that honest SUs always have higher average accumulative 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

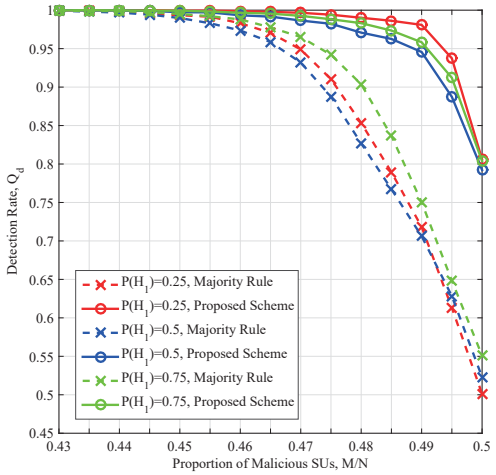

Fig. 3. Comparison of the detection rates for the proposed scheme and the majority rule under heavy cooperative attacks.

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.

C. Performance Evaluation

In this section, we set the number of SUs N as 200, 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. In this section, we do not consider the maximum loss that a malicious can afford. We demonstrate a better performance of our peer-prediction based mechanism than that of the pure majority rule. In Fig. 3, the majority rule removes the outliers accurately in hard decision and has excellent performance when the proportion of malicious users is relatively low. However, the accuracy decreases sharply when $\frac{M}{N} > 0.45$ because of heavy cooperative attacks conducted by malicious SUs. Our proposed scheme performs even better than the majority rule when the proportion of malicious SUs increases regardless of the variation of $P(\mathcal{H}_1)$. By removing the decisions of suspect attackers with low accumulative scores, the FC guarantees more reliable decisions in the decision pool. Therefore, the error rate of the proposed scheme reduces to one fifth of that of the majority rule scheme generally. If considering the rationality of malicious SUs and their tolerance of loss, they have to reduce their attacking rate or even are reluctant to attack, for they cannot expect a positive income when attacking.

V. Conclusion

In this paper, we proposed an incentive attack prevention method with approximate subjective priors for collaborative spectrum sensing in CRNs to motivate SUs to report truthful sensing results and identify malicious suspects based on Private-Prior Peer-Prediction. Each SU's local sensing decision was judged by comparing the relationship between the information report and the prediction report. Besides, the score of each SU was calculated by utilizing the binary quadratic scoring rule. In order to increase the loss incurred by malicious SUs, we introduced the threshold of the uncertainty index to constrain the value of the prediction reports. From the simulation results, we can observe distinct difference in scores between honest SUs and malicious SUs, and significant increase of detection rates compared with pure majority rule under heavy cooperative SSDF attacks.

References

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

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

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

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

[5] 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, 2013.

[6] 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, 2010.

[7] 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, 2010.

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

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

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

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

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

[13] J. Witkowski and D. C. Parkes, "Peer prediction without a common prior," in *Proc. of ACM Conference on Electronic Commerce*. ACM, 2012, pp. 964–981.

[14] D. C. Parkes and J. Witkowski, "A robust bayesian truth serum for small populations," in *Proc. of AAAI Conference on Artificial Intelligence 2012*. AAAI, 2012.

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

[16] A. Ghosh, K. Ligett, A. Roth, and G. Schoenebeck, "Buying private data without verification," in *Proc. of ACM conference on Economics and computation*. ACM, 2014, pp. 931–948.

[17] T. Gneiting and A. E. Raftery, "Strictly proper scoring rules, prediction, and estimation," *Journal of the American Statistical Association*, vol. 102, no. 477, pp. 359–378, 2007.

[18] R. Selten, "Axiomatic characterization of the quadratic scoring rule," *Experimental Economics*, vol. 1, no. 1, pp. 43–62, 1998.