sensors

MDPI

Article

Reputation-Based Spectrum Sensing Strategy Selection in Cognitive Radio Ad Hoc Networks

Zhiguo Sun, Zhenyu Xu, Zengmao Chen, Xiaoyan Ning * and Lili Guo

College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China; sunzhiguo@hrbeu.edu.cn (Z.S.); xuzhenyuaichiyu@hrbeu.edu.cn (Z.X.); chenzengmao@hrbeu.edu.cn (Z.C.); guolili@hrbeu.edu.cn (L.G.)

* Correspondence: ningxiaoyan@hrbeu.edu.cn; Tel.: +86-137-9660-8901

Received: 8 November 2018; Accepted: 6 December 2018; Published: 11 December 2018

Abstract: Spectrum sensing plays an essential role in the detection of unused spectrum whole in cognitive radio networks, including cooperative spectrum sensing (CSS) and independent spectrum sensing. In cognitive radio ad hoc networks (CRAHNs), CSS enhances the sensing performance of cognitive nodes by exploring the spectrum partial homogeneity and fully utilizing the knowledge of neighboring nodes, e.g., sensing results and topological information. However, CSS may also open a door for malicious nodes, i.e., spectrum sensing data falsification (SSDF) attackers, which report fake sensing results to deteriorate the performance of CSS. Generally, the performance of CSS has an inverse relationship with the fraction of SSDF attackers. On the contrary, independent spectrum sensing is robust to SSDF attacks. Therefore, it is desirable to choose a proper sensing strategy between independent sensing and collaborative sensing for CRAHNs coexisting with various fractions of SSDF attackers. In this paper, a novel algorithm called Spectrum Sensing Strategy Selection (4S) is proposed to select better sensing strategies either in a collaborative or in an independent manner. To derive the maximum a posteriori estimation of nodes' spectrum status, we investigated the graph cut-based CSS method, through which the topological information cost function and the sensing results cost function were constructed. Moreover, the reputation value was applied to evaluate the performance of CSS and independent sensing. The reputation threshold was theoretically analyzed to minimize the probability of choosing the sensing manner with worse performance. Simulations were carried out to verify the viability and the efficiency of the proposed algorithm.

Keywords: CRAHNs; collaborative spectrum sensing; SSDF; spectrum sensing strategy selection

1. Introduction

With the rapid development of radio communication, radio systems tend to provide higher speed, have denser deployment, and occupy wider bandwidth, which can cause the radio spectrum to become overcrowded, i.e., spectrum scarcity. However, many studies have shown that under the current radio communication strategy, spectrum resources have not been fully utilized [1]. This provides a possibility to resolve the contradiction between limited spectrum and the increasing requirement of radio communication bandwidth. To address the problem of spectrum scarcity and improve spectrum utilization, cognitive radio has been proposed and widely studied as a promising technology [2].

In cognitive radio networks, the primary users (PUs) are licensed to occupy the authorized frequency band. To avoid interfering with the PU, the secondary users (SUs) can opportunistically access the frequency band, which is not fully utilized by the PUs, i.e., the spectrum white holes [3]. When PUs are active, spectrum resources are not available for SUs; SUs can access the spectrum opportunistically through spectrum sensing when PUs are mute. Therefore, spectrum sensing is

essential for cognitive radio to exploit spectrum holes. To avoid interfering with the PU, the spectrum sensing algorithm should be able to detect white holes efficiently and effectively.

Due to the spacious coverage of ad hoc networks, each SU may receive varying PU signal powers and thus undergo diverse spectral status in cognitive radio ad hoc networks (CRAHNs). However, neighboring SUs are spatially close and prefer to experience identical spectral status. This characteristic of ad hoc networks is called spectrum partial homogeneity [4]. Cooperative spectrum sensing (CSS) takes full advantage of this prior information to improve the performance of malfunctioning SUs with poor wireless propagation characteristics, such as those nodes experiencing deep shading. It is unlikely that all SUs undergo severe fading. Therefore, it is feasible for SUs to exploit sensing performance gain from adjacent nodes through cooperation. In the first step of collaborative sensing, each SU reports the local independent spectrum sensing decision to the data fusion center through control channels. Then, the data fusion center generalizes the cooperation of the local decision according to given rules, such as Majority criteria, Or criteria, And criteria, Bayes criterion, and so on [5]. The decision results are broadcast back to each SU node via the control channels.

On one hand, introducing cooperation during sensing provides CRAHNs with enormous performance improvement; on the other hand, it also opens the door to spectrum sensing data falsification (SSDF) attackers, which aim to undermine the sensing performance of CRAHNs. Moreover, ad hoc networks are more likely to sustain SSDF attack due to the openness and dynamics of CRAHNs. Hence, it is crucial to design robust collaborative sensing algorithms to suppress SSDF attackers. The issue of how to eliminate the interference of SSDF attackers in cognitive radio has attracted the attention of many researchers [6–10]. Reputation value theory (RVT)-based algorithms against SSDF attacks are commonly applied in cognitive radio networks to detect and remove malicious nodes [11,12]. However, existing RVT algorithms cannot detect all malicious SUs and even regard honest SUs as malicious nodes by mistake. Residual malicious nodes and mis-detected honest nodes will inevitably degrade the sensing performance. In Reference [13], the maximum likelihood estimation method is combined with reputation theory to eliminate SSDF attackers. The performance of independent sensing is compared with the performance of CSS under SSDF attack in Reference [14]. Unfortunately, the independent sensing results, which perform better when the fraction of SSDF attackers is high, are not used in the proposed algorithm [14]. Different from previous researches, this paper mainly concentrates on the problem of choosing the sensing strategy between either independent spectrum sensing or CSS from the view of honest Sus, rather than how to reject malicious nodes from the view of the data fusion center.

The contributions of this article are as follows:

- The theoretical deduction of the maximum posterior probability estimation based on image segmentation in CRAHNs is introduced.
- This paper proposes a spectrum sensing strategy selection algorithm based on the reputation value theory. Moreover, the theoretical derivation and simulation verification of the optimal threshold value are completed.

The arrangement of this paper is as follows: Section 2 establishes the system model of a cognitive radio network. Section 3 introduces the spectrum sensing methods in cognitive radio networks, and Section 4 proposes the selection strategy of spectrum sensing methods. Section 5 investigates the optimal threshold for the spectrum sensing strategy selection algorithm. Simulation results are given, and conclusions are drawn in Section 6. Finally, Section 7 discusses the potential future works that may be needed.

2. System Model

This paper considers a centralized CRAHN model, consisting of a PU, a fusion center (FC), and N SUs with $N - M$ Honest Secondary Users (HSUs) and M malicious secondary users (MSUs). As shown in Figure 1, parts of the secondary users are affected by severe fading and uncertain noise, resulting in

false sensing decisions. Thereby, we exploit the prior information of the spectral state consistency of CRAHNs to improve the performance of these fading nodes via cooperation. Although the cognitive nodes of different location may experience different spectrum status, topologically adjacent nodes tend to be in the same spectrum occupancy status. In other words, CRAHNs are composed of several 'same spectrum status' patches. Therefore, malfunctioning SUs under deep fading can cooperate with neighboring nodes to rectify the local erroneous spectrum sensing results.

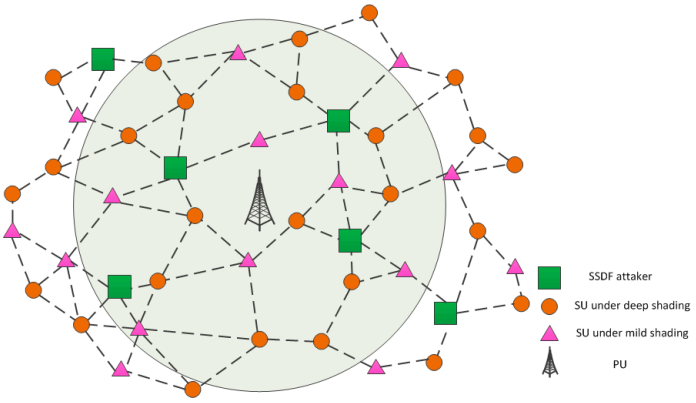


Figure 1. This figure shows a centralized cognitive radio ad hoc network (CRAHN) contaminated by some spectrum sensing data falsification (SSDF) attackers. The gray circle around the primary user (PU) indicates the coverage of PU. Inside the circle, the secondary user (SU) should not access the spectrum while SUs outside the circle have this opportunities.

In the first step of CSS, the SUs carry out independent spectrum sensing, and then send the local sensing decisions to the FC through the ideal control channels. In ad hoc networks, the topology information is relatively easy to acquire. Based on the accepted local sensing results and known topology information, the FC makes a final decision, and then broadcasts the sensing decisions to all SUs.

At each cognitive node, independent spectrum sensing can be considered as a binary hypothesis testing problem defined as:

$$\begin{cases} \mathrm{H}_1: & \textit{the spectrum is occupied} \\ \mathrm{H}_0: & \textit{the spectrum is idle} \end{cases}$$

The power of the PU signal received at the cognitive node not only depends on the distance between the PU and the SU, but also relates to other wireless propagation characteristics, such as shadow fading, multipath, and noise. According to References [15,16], the formulation among the level of fading and the related parameters at SUs is as follows:

$$PL(d)[\mathrm{dB}] = \overline{PL}(d) + X_\sigma = \overline{PL}(d_0) + 10n \log \frac{d}{d_0} + X_\sigma. \tag{1}$$

Path loss $PL(d)$ is a function of d, which denotes the distance between the PU and the SU. X_σ is subject to Gaussian distribution with a mean value of 0 and a variance of σ, i.e., $X_\sigma \sim \mathcal{N}(0, \sigma^2)$. d_0 and n represent the reference distance and the path loss factor, respectively.

Assuming that P_t denotes the transmission power of the primary user, when the PU is present, the power received at the i-th SU can be expressed as $P_r^i(d_i) = P_t - PL(d_i)$. When the PU is absent, $P_r^i(d_i) = W_i$, where W_i follows Gaussian distribution with $\mathcal{N}(\overline{PL}(d_i), \sigma_0^2)$.

Assume that SUs detect the PUs based on energy detection with a threshold λ. Hence, the probability of detection of the i-th SU can be formulated as:

$$\begin{array}{l} P_d^i = P\left(P_r^i > \lambda \middle| H_1\right) = P\left(X_\sigma < P_t - \overline{PL}(d_i) - \lambda\right) \\ = Q\left(\frac{\lambda - P_t + \overline{PL}(d_i)}{\sigma}\right) \end{array}, \tag{2}$$

where $Q(z) = 1/\sqrt{2\pi}\int_z^\infty \exp\left(-x^2/2\right)\mathrm{d}x$ denotes the complementary distribution function of standard normal distribution. Similarly, the probability of a false alarm of the i-th SU can be expressed as:

$$P_f^i = Q\left(\frac{\lambda - \overline{PL}(d_i)}{\sigma_0}\right). \tag{3}$$

Although CSS may improve the sensing performance, it also provides SSDF attackers with the opportunity to undermine the sensing performance due to its nature of openness. SSDF attackers can mislead the FC and deteriorate the CSS performance by means of reporting false sensing results. Thereby, the CSS algorithm must be robust to SSDF attacks. Although some algorithms can detect malicious nodes [11], the residual malicious nodes will still affect the spectrum sensing performance. As the fraction of malicious nodes rises in cognitive radio networks, the probability of CSS detection decreases. Meanwhile, the probability of CSS false alarm ascends. Therefore, different sensing strategies are needed under different fractions of malicious nodes.

3. Collaborative Spectrum Sensing in CRAHNs

In this section, the graph cut algorithm used regularly in computer vision is introduced into CSS, where the graph cut-based maximum a posteriori estimation of spectrum occupancy states is realized. In the field of computer vision, graph cut algorithms are often used to derive the minimum energy of an image [17,18], and divide this image into 'foreground' and 'background'. Similarly, in CSS, all SUs nodes are expected to decide whether the PU is 'absent' or 'present' at each node.

Based on the spectrum state of each node in CRAHNs, a graph of spectrum occupancy status is constructed in this section. Each SU is regarded as a graph pixel and links (v_i, v_j) between neighboring nodes i and j are established based on their topology information. Hence, an undirected graph of spectrum occupancy status (GSOS) can be built. In computer vision, two terminals (source and sink) are added to the image, and each node in the image relates to two terminals [17]. Similarly, source node O, denoting spectrum occupied, and terminal node U, denoting spectrum unoccupied, and the connection between each node and two endpoints $l(v_o, v_j)$, $l(v_j, v_u)$ are added in the GSOS. In this way, dividing SU status in CSS is equivalent to image segmentation in computer vision, and can be further processed by existing graph cut algorithms.

3.1. Maximum a Posteriori Probability of CSS

Given the spectrum state of the i-th secondary user x_i, where $\{x_i = 1, 0\}$ meaning that its spectrum is occupied or vacant, respectively, the PU signal energy y_i received at the i-th secondary user is conditionally dependent on x_i, and the conditional probability density function is $f\{y_i|x_i\}$. Therefore, considering a cognitive radio network with N SU nodes with spectrum state $x = \{x_1, x_2, \ldots, x_N\}$, the power density function of the signal power received by each SU node is denoted as:

$$p(y|x) = \prod_{i=1}^{N} f(y_i|x_i) = \prod_{i=1}^{N} f(y_i|x_i = 1)^{x_i} f(y_i|x_i = 0)^{1-x_i}. \tag{4}$$

where $y = \{y_1, y_2, \ldots, y_N\}$. In cognitive radio networks, the prior distribution of SU nodes can be considered as a conditional Markov random field (MRF) [19], which is a commonly used model

for location scenes with numerable patches having the same spectrum status. Thereby, the prior distribution of each node state $p(x)$ can be expressed as follows [19]:

$$p(x) \propto \exp\left\{\frac{1}{2}\sum_{i=1}^{N}\sum_{i=1}^{N}\beta_{ij}\left[x_i x_j + (1-x_i)(1-x_j)\right]\right\}, \tag{5}$$

where β_{ij} stands for the relationship between two SU nodes. When the i-th secondary user and j-th secondary user are adjacent nodes, we have $\beta_{ij} = \beta_{ji} = \beta$, where β is constant; otherwise, $\beta_{ij} = \beta_{ji} = 0$.

According to the Bayes criterion, the posterior probabilities of the spectrum state of the network nodes $p(x|y)$ can be written as:

$$p(x|y) = \frac{p(x,y)}{p(y)} = \frac{p(x)p(y|x)}{p(y)}. \tag{6}$$

Namely, the logarithm of the posterior probability, $\ln p(x|y)$, can be formulated as:

$$L(x) = \sum_{i=1}^{N} x_i \ln\frac{f(y_i|x_i=1)}{f(y_i|x_i=0)} + \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left(x_i x_j + (1-x_i)(1-x_j)\right) + \mathrm{K}, \tag{7}$$

where $\frac{f(y_i|x_i=1)}{f(y_i|x_i=0)}$ represents the likelihood ratio of the SUs. The constant K, which is independent of the spectrum states, can be expressed as:

$$\mathrm{K} = \sum_{i=1}^{N} p(y_i|x_i=0) - \ln y. \tag{8}$$

3.2. Parameter Setting of the Graph Cut

The minimum energy of the graph according to the maximum flow/minimum cut algorithm [18] can be written as [20]:

$$E(L) = \sum_{p\in P} D_p(L_p) + \sum_{(p,q)\in\phi} V_{p,q}(L_p, L_q), \tag{9}$$

where $L = \{L_p, p \in P\}$, $D_p(\cdot)$, $V_{p,q}(\cdot)$, and ϕ denote the value of each pixel of the penalty function for each node's value, the interaction function between the pixels p and q, and the set of all adjacent nodes, respectively.

This paper makes some adoptions to build the connection between the results of graph cut and the maximum a posteriori estimation of the SUs' spectrum status in CSS. Similarly with the penalty function $D_p(\cdot)$ and the interaction function $V_{p,q}(\cdot)$ in the graph cut, the sensing result cost functions $c(v_i, v_o)$, $c(v_u, v_i)$ and the topological information cost function $c(v_i, v_j)$ are introduced, respectively.

1. Sensing results cost function:

$$c(v_i, v_o) = \ln\left(\frac{f(y_i|x_i=1)}{f(y_i|x_i=0)}\right) = \lambda_i, \tag{10}$$

$$c(v_u, v_i) = \ln\eta, \tag{11}$$

where η is set to 1, and thus $c(v_u, v_i) = 0$. From Equations (10) and (11), we can derive that when $c(v_i, v_o) > c(v_u, v_i)$, the i-th node prefers to decide that the spectrum status at the i-th node is idle, which is equal to the decision of the independent spectrum sensing.

When it comes to making a hard decision, $c'(v_i, v_o) = 1$ and $c'(v_u, v_i) = 0$ when the likelihood ratio function is greater than 1; otherwise, $c'(v_i, v_o) = 0$ and $c'(v_u, v_i) = 1$. Thus, the cognitive node reports this 1-bit hard decision data to the FC.

2. Topological information cost function:

$$c(v_i, v_j) = \begin{cases} \beta, & i \text{ and } j \text{ are neighbors} \\ 0, & \text{otherwise} \end{cases}. \tag{12}$$

The topological information cost function denotes the correlation of the spectrum status between two nodes. The topological information cost function $c(v_i, v_j)$ is equal to β when the i-th node and j-th node are neighbors to each other topologically. It is reasonable that adjacent nodes prefer to undergo the same spectrum status and thus $\beta > 0$.

Based on the aforementioned cost functions, the energy function of GSOS can be written as:

$$C(x) = \sum_{i=1}^{N} x_i c(v_i, v_o) + \sum_{i=1}^{N} (1 - x_i) c(v_u, v_i) + \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} c(v_i, v_j) (x_i - x_j)^2, \tag{13}$$

which differs from the negative part of the posterior probability function $-L(x)$ by a constant K. Suppose that minimum of $C(x)$ is taken at $x = x_0$, it is obvious that $L(x_0)$ is the maximum of $L(x)$. In other words, graph cut algorithms minimize the energy function of an image, $C(x)$, and consequently derive the maximum a posteriori estimation in CSS.

4. Spectrum Sensing Strategy Selection Based on Reputation Value

In the field of CSS, reputation value theory is often applied to distinguish HSUs from SSDF attackers [21,22]. In this section, reputation value theory is innovatively adopted to a select sensing strategy between CSS and independent sensing.

Massive MSUs in CRAHNs will deteriorate the performance of CSS dramatically, which contradicts the belief that CSS should improve the sensing performance. Different from CSS, independent sensing ensures the independence of each node's sensing results, which means that MSUs have no chance to interfere with HSUs in independent sensing. Therefore, it is advisable to select independent spectrum sensing when enormous malicious nodes exist, and vice versa. However, the fraction of MSUs in CRAHNs is not easy to determine.

Though the fraction of MSUs is unknown for each SU, local sensing data and CCS results can be easily obtained at an HSU without additional hardware costs. This information can be further exploited to evaluate the performance of independent spectrum sensing and CSS. At each SU node, the performance of independent sensing is compared with that of CSS. When the results of the former are the same as those of the latter, the reputation value is increased by 1; when they are different, the reputation value is reduced by 1. Therefore, collaborative sensing results are trustworthy when the reputation value is high. Likewise, independent sensing decisions are reliable when the reputation value is low. Thereby, a specific reputation threshold should be investigated. CSS results are selected when the reputation value exceeds the reputation threshold, and independent sensing results are chosen when the reputation value is below the threshold.

To elaborate upon the sensing strategies selection, the reputation value is analyzed at an honest node. Assuming that the sensing result at moment t is denoted as u_t with detection probability P_d^{I} and false alarm probability P_f^{I}, g_t represents the CSS result at moment t with P_d^{C} and P_f^{C} representing the detection probability and false alarm probability, respectively. Let e_t denote the comparison between the sensing result of the FC and the sensing result of the cognitive node.

It is assumed that the result of independent spectrum sensing is equals to that of CSS at moment t, denoted as:

$$e_t = \begin{cases} 1, u_t = g_t \\ 0, u_t \neq g_t \end{cases}. \tag{14}$$

$P\{e_t = 1\} = p$ represents the probability that the CSS result will be identical to the independent spectrum sensing result, and it can be written as follows:

$$\begin{aligned} p &= \sum_{j\in\{0,1\}} P\{Q_j\}\left(P\{g_t = 1, u_t = 1|Q_j\} + P\{g_t = 0, u_t = 0|Q_j\}\right) \\ &= \sum_{j\in\{0,1\}} P\{Q_j\}\left(P\{g_t = 1|Q_j\}\cdot P\{u_t = 1|Q_j\} + P\{g_t = 0|Q_j\}\cdot P\{u_t = 0|Q_j\}\right) \\ &= P\{Q_1\}\left(P_d^{\mathrm{I}}P_d^{\mathrm{C}} + (1-P_d^{\mathrm{I}})(1-P_d^{\mathrm{C}})\right) + P\{Q_0\}\left(P_f^{\mathrm{I}}P_f^{\mathrm{C}} + \left(1-P_f^{\mathrm{I}}\right)\left(1-P_f^{\mathrm{C}}\right)\right) \\ &= 1 - P\{Q_1\}\left(P_d^{\mathrm{I}} + P_d^{\mathrm{C}} - 2P_d^{\mathrm{I}}P_d^{\mathrm{C}}\right) - P\{Q_0\}\left(P_f^{\mathrm{I}} + P_f^{\mathrm{C}} - 2P_f^{\mathrm{I}}P_f^{\mathrm{C}}\right) \end{aligned}, \tag{15}$$

$P\{e_t = 0\} = q$ denotes the probability that the CSS result will be different from the independent spectrum sensing result, and it can be formulated as follows:

$$\begin{aligned} q &= 1 - p \\ &= P\{Q_1\}\left(P_d^{\mathrm{I}} + P_d^{\mathrm{C}} - 2P_d^{\mathrm{I}}P_d^{\mathrm{C}}\right) + P\{Q_0\}\left(P_f^{\mathrm{I}} + P_f^{\mathrm{C}} - 2P_f^{\mathrm{I}}P_f^{\mathrm{C}}\right) \end{aligned}, \tag{16}$$

The partial derivative of p on P_d^{C} and P_f^{C} can be expressed as:

$$\frac{\partial p}{\partial P_d^{\mathrm{C}}} = -P\left\{Q_1^A\right\}\left(1 - 2P_d^{\mathrm{I}}\right), \tag{17}$$

$$\frac{\partial p}{\partial P_f^{\mathrm{C}}} = -P\{Q_0\}\left(1 - 2P_f^{\mathrm{I}}\right), \tag{18}$$

where it is reasonably assumed that $1 > P_d^{\mathrm{I}} > \frac{1}{2} > P_f^{\mathrm{I}} > 1$ and $1 > P_d^{\mathrm{C}} > \frac{1}{2} > P_f^{\mathrm{C}} > 1$. Thus, $\frac{\partial p}{\partial P_d^{\mathrm{C}}} > 0$ and $\frac{\partial p}{\partial P_f^{\mathrm{C}}} < 0$ hold true. p decreases with the increase of P_d^{C} at interval $[0.5, 1]$. Likewise, p increases with the increase of P_f^{C} at interval $[0.5, 1]$. When $\left(P_d^{\mathrm{C}}, P_f^{\mathrm{C}}\right) = (0.5, 0.5)$, p achieves the minimum $P_{\min}$, which can be denoted as:

$$P_{\min} = 1 - 0.5(P\{Q_1\} + P\{Q_0\}) = 0.5, \tag{19}$$

When $\left(P_d^{\mathrm{C}}, P_f^{\mathrm{C}}\right) = \left(P_d^A, P_f^A\right)$, P_{thr} is derived as:

$$P_{thr} = 1 - P\{Q_1\}2P_d^{\mathrm{I}}\left(1 - P_d^{\mathrm{I}}\right) - P\{Q_0\}2P_f^{\mathrm{I}}\left(1 - P_f^{\mathrm{I}}\right), \tag{20}$$

When $\left(P_d^{\mathrm{C}}, P_f^{\mathrm{C}}\right) = (1, 0)$, the maximum of p is formulated as:

$$\begin{aligned} P_{\max} &= 1 - P\{Q_1\}\left(P_d^{\mathrm{I}} + 1 - 2P_d^{\mathrm{I}}\right) - P\{Q_0\}P_f^{\mathrm{I}} \\ &= 1 - P\{Q_1\}\left(1 - P_d^{\mathrm{I}}\right) - P\{Q_0\}P_f^{\mathrm{I}} \end{aligned}, \tag{21}$$

Obviously, $p \geq P_{Thr}$ is obtained when $P_d^{\mathrm{C}} \geq P_d^{\mathrm{I}}$, $P_f^{\mathrm{C}} \leq P_f^{\mathrm{I}}$; $p < P_{Thr}$ is obtained when $P_d^{\mathrm{C}} < P_d^{\mathrm{I}}$, $P_f^{\mathrm{C}} > P_f^{\mathrm{I}}$. Therefore, p can be used as a performance metric to compare the performance of CSS and that of independent spectrum sensing. When $p \geq P_{Thr}$, CSS outperforms independent sensing; when $p < P_{Thr}$, independent spectrum sensing outperforms CSS. To achieve better sensing performance, the CSS results rather than the independent sensing results are chosen as the final decision when $p \geq P_{Thr}$; meanwhile, the independent spectrum sensing results are selected when $p < P_{Thr}$. The abovementioned procedure is termed the spectrum sensing strategies selection (4S) algorithm.

5. Selection of Reputation Value Threshold

For the purpose of obtaining optimal sensing results, the 4S algorithm is expected to select the CSS results when the results of CSS are excellent; the independent spectrum sensing decision is deemed as the final decision in the 4S algorithm when independent sensing outperforms CSS. The first type of sensing error P_{e1} and the second type of sensing error P_{e2} are defined as the choice of the independent spectrum sensing results when the CSS decisions are optimal and should be selected, and the selection of the CSS results when the performance of the independent sensing is better than that of CSS, respectively. To reduce the sum of the first type of strategy selection error and second type of strategy selection error for the i-th SU, i.e., $P_e^i = P_{e1} + P_{e2}$, an optimal reputation value threshold can be designed as follows.

Definition 1. *The reputation value of the i-th SU—E is recorded by comparing the sensing results of the FC with the local sensing results, i.e., e_t over a limited time window from t_0 to $t_0 + T$.*

$$E = \sum_{t=t_0}^{t_0+T} e_t, \tag{22}$$

where e_t follows the Bernoulli distribution with the parameter ρ. Therefore, E is subject to the binomial distribution. According to Reference [23], when T, $P\{e_t = 1\} = p$, and $P\{e_t = 0\} = q$ satisfy the following condition,

$$\left| \frac{1}{\sqrt{T}} \left(\sqrt{\frac{q}{p}} - \sqrt{\frac{p}{q}} \right) \right| < 0.3, \tag{23}$$

E approximately follows a normal distribution, i.e., $E \sim \mathcal{N}(Tp, Tpq)$. The probability density functions of E can be formulated as:

$$f(E) = \frac{1}{\sqrt{2\pi Tpq}} \exp\left(-\frac{(E - Tp)^2}{2Tpq} \right). \tag{24}$$

Considering that $p \gg q$, it's reasonable to assume that $\sqrt{q/p} \approx 0$. Thus, the formula (23) can be simplified as

$$T > \frac{p}{0.09q} \approx 11\frac{p}{q}, \tag{25}$$

Under the condition from Equation (25), an appropriate reputation value threshold can be derived to minimize the probability of total strategy selection error.

For the i-th SU, when $p > P_{Thr}$, the CSS results are optimal, and the detection probability of CSS the false alarm probability of independent sensing are greater than the detection probability of independent sensing and the false alarm probability of CSS, respectively, i.e., $P_d^C > P_d^I$ and $P_f^C < P_f^I$; conversely, the independent spectrum sensing performance is better and $P_d^C < P_d^I$, $P_f^C > P_f^I$. A proper reputation value threshold is η investigated for E, and the cooperative spectrum sensing results are chosen when $E > \eta$; conversely, the independent spectrum sensing results should be selected when $E < \eta$. Thus another definition of the first type of sensing error can be expressed as the probability of $E > \eta$ when p is less than a given threshold P_{Thr}, i.e., $P\{E > \eta | p < P_{Thr}\}$; the second type of sensing error can be denoted as the probability of $E < \eta$ when $p > P_{Thr}$, i.e., $P\{E < \eta | p > P_{Thr}\}$.

The probability of the first type of sensing error, $P\{E > \eta | p < P_{Thr}\}$ can be formulated as:

$$P\{E > \eta | p < P_{Thr}\} = \int_{\eta}^{+\infty} f(E)\mathrm{d}E = \int_{\eta}^{+\infty} \frac{1}{\sqrt{2\pi Tpq}} \exp\left(-\frac{(E - Tp)^2}{2Tpq} \right) \mathrm{d}E, \tag{26}$$

The probability of the second type of sensing error, $P\{E < \eta | p > P_{Thr}\}$ can be formed as:

$$P\{E < \eta | p > P_{Thr}\} = \int_0^{\eta} f(E)\mathrm{d}E = \int_0^{\eta} \frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(E-Tp)^2}{2Tp(1-p)}\right)\mathrm{d}E. \tag{27}$$

Let us assume that the cognitive radio network has a massive amount of honest cognitive nodes, thus $\left(P_d^C\right)_{\max} \approx 1$ and $\left(P_f^C\right)_{\min} \approx 0$ according to Reference [24]. In accordance with Reference [16], under the best SSDF attack, the performance of the cognitive radio network is at its worst with $\left(P_d^C\right)_{\min} = 0.5$ and $\left(P_f^C\right)_{\max} = 0.5$.

Given that $\theta(p)$ represents the probability density function of $P\{e_t = 1\} = p$, it is assumed that p is subject to uniform distribution at $[P_{\min}, P_{\max}]$ under the attack of malicious nodes; that is:

$$\theta(p) = \begin{cases} \frac{1}{P_{\max}-P_{\min}}, & P_{\min} \le p \le P_{\max} \\ 0, & others \end{cases}. \tag{28}$$

Therefore, the total strategy selection error probability for the i-th SU P_e^i can be written as:

$$\begin{aligned} P_e^i &= \int_{0.5}^{P_{thr}} \theta(p) \cdot \int_{\eta}^{+\infty} f(E)\mathrm{d}E\mathrm{d}\theta + \int_{P_{thr}}^{1} p(\theta) \cdot \int_{0}^{\eta} f(E)\mathrm{d}E\mathrm{d}p \\ &= \int_{0.5}^{P_{thr}} \theta(p) \cdot \int_{\eta}^{+\infty} f\left(\frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(E-Tp)^2}{2Tp(1-p)}\right)\right)\mathrm{d}E\mathrm{d}p \\ &+ \int_{P_{thr}}^{1} \theta(p) \cdot \int_{0}^{\eta} f\left(\frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(E-Tp)^2}{2Tp(1-p)}\right)\right)\mathrm{d}E\mathrm{d}p \end{aligned}, \tag{29}$$

The partial derivative of the total strategy selection error probability over the reputation value threshold η can be computed as:

$$\begin{aligned} \frac{\partial P_e^i}{\partial \eta} &= \frac{\partial\left(\int_{P_{\min}}^{P_{thr}} \theta(p) \cdot \int_{\eta}^{+\infty} f(E)\mathrm{d}E\mathrm{d}p + \int_{P_{thr}}^{P_{\max}} \theta(p) \cdot \int_{0}^{\eta} f(E)\mathrm{d}E\mathrm{d}p\right)}{\partial \eta} \\ &= -\int_{P_{\min}}^{P_{thr}} \theta(p) \cdot f(\eta)\mathrm{d}p + \int_{P_{thr}}^{P_{\max}} \theta(p) \cdot f(\eta)\mathrm{d}p \\ &= \frac{1}{P_{\max}-P_{\min}}\left(\int_{P_{\min}}^{P_{thr}} -\frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right)\mathrm{d}p \right. \\ &\left. + \int_{P_{thr}}^{P_{\max}} \frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right)\mathrm{d}p\right) \end{aligned}. \tag{30}$$

Proposition 1. *The solution for the optimal reputation value exists.*

Proof. See Appendix A. □

According to Proposition 1, the solution of $\frac{\partial P_e^i}{\partial \eta} = 0$ exists, and $\frac{\partial P_e^i}{\partial \eta} = 0$ can be expressed as:

$$\begin{aligned} &\frac{1}{P_{\max}-P_{\min}}\left(\int_{P_{\min}}^{P_{thr}} -\frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right)\mathrm{d}p \right. \\ &\left. + \int_{P_{thr}}^{P_{\max}} \frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right)\mathrm{d}p\right) = 0 \end{aligned}. \tag{31}$$

The solution of the above equation is the optimal reputation threshold of the 4S algorithm. To reduce the computational complexity, an error function is applied to approximate the formula $\frac{\partial P_e^i}{\partial \eta} = 0$ as follows (see Appendix B):

$$\frac{\partial P_e^i}{\partial \eta} = \frac{1}{2(P_{\max} - P_{\min})} \left(\operatorname{erf}\left(\frac{P_{\max}}{\sqrt{2T\eta(1-\eta)}} \right) + \operatorname{erf}\left(\frac{P_{\min}}{\sqrt{2T\eta(1-\eta)}} \right) - 2\operatorname{erf}\left(\frac{P_{\text{thr}}}{\sqrt{2T\eta(1-\eta)}} \right) \right), \tag{32}$$

where $\operatorname{erf}(x)$ is the error function. We define optimal threshold function $h(\eta)$ as:

$$h(\eta) = \operatorname{erf}\left(\frac{P_{\max}}{\sqrt{2T\eta(1-\eta)}} \right) + \operatorname{erf}\left(\frac{P_{\min}}{\sqrt{2T\eta(1-\eta)}} \right) - 2\operatorname{erf}\left(\frac{P_{\text{thr}}}{\sqrt{2T\eta(1-\eta)}} \right). \tag{33}$$

It can be seen that $h(\eta)$ is equal to zero when $\eta = \eta_0$, $\frac{\partial P_e^i}{\partial \eta} < 0$ when $\eta < \eta_0$, and $\frac{\partial P_e^i}{\partial \eta} > 0$ when $\eta > \eta_0$. Namely, the total strategy selection error probability monotonically decreases at interval $(0.5, \eta_0)$ and ascends at interval $(\eta_0, 1)$. Accordingly, the total strategy selection error probability for the i-th SU reaches its minimum at $\eta = \eta_0$.

6. Performance Analysis

This section analyzes and investigates the performances of independent spectrum sensing, CSS, and the proposed 4S algorithm in CRAHNs under various SSDF attack strategies.

6.1. Parameter Setting

In this section, a centralized cognitive radio network is considered, where three sensing algorithms are applied and simulated. The PU is assumed to be located at the center of the cognitive radio network, and accesses the licensed band with a probability of 0.5. The power and the bandwidth of the PU emitted to the cognitive radio network reaches 20 watts and 900 MHz, respectively. All of the SUs' locations, including HSUs and MSUs, are subject to a Poisson point process with a density of $8 \times 10^{-5}/\text{m}^2$. Wireless channel propagation is modeled as Rayleigh distribution with mean of 1, and the path loss factor is 4. Background noise $n(t)$ follows normal distribution with $N(0, 10^{-14})$. Prior information about partial spectrum homogeneity, β, is equal to 0.4.

6.2. SSDF Attack Strategies

At first, spectrum sensing is implemented at each node. Afterwards, SSDF attackers resolve their report data based on their sensing results and attacking strategies. SSDF attacking strategies can be divided into four ways [25], listed as follows.

1. "Always occupied" attack: To access spectrum resources alone, MSUs send reports of being occupied by the PU to force the FC to regard the spectrum status as always occupied. Thus, SUs have no privilege to access the spectrum band. Therefore, the total spectrum utilization efficiency is reduced.

2. "Always idle" attack: When the spectrum status is occupied, malicious nodes send 'idle' reports to deliberately mislead the FC to allocate spectrum resources to SUs. As a result, the quality of communication is worsened.

3. "Always false" attack: Sensing data reported to the FC by MSUs is always completely contrary to the sensing results. That is, when the malicious user detects the existence of the PU, the malicious user sends an 'idle' report to the FC; if the malicious user finds that the spectrum status is idle, the malicious user sends an 'occupied' report to the FC.

4. Possible attack: To avoid being detected and eliminated by the FC, the malicious user reports not only false results but also true results under a specific probability.

6.3. Simulation Results

Considering the goal of minimizing the average total strategy selection error probability for all HSUs, $\overline{P_e}$, we employ the probability of correctness for HSUs as a performance metric, which is given by:

$$P_c = 1 - \overline{P_e} = 1 - \frac{\sum_{i=1}^{N-M} \kappa^i Pb_C^i + (1-\kappa^i) Pb_I^i}{N-M}, \tag{34}$$

where Pb_C^i and Pb_I^i denote the sensing error of CSS and the sensing error of independent sensing, respectively; $\kappa^i = 0$ and $\kappa^i = 1$ indicate that the CSS results are selected and that the independent sensing results are selected for i-th SU, respectively.

Assuming that the sensing method with better performance is always chosen in the 4S algorithm, we can derive the upper bound of the probability of correctness, $\widehat{P_c}$, which is given by:

$$\widehat{P_c} = 1 - \frac{\sum_{i=1}^{N-M} \min\left\{Pb_C^i, Pb_I^i\right\}}{N}. \tag{35}$$

When the number of SUs, N, is constant, the fraction of SSDF attackers is denoted as:

$$\alpha = \frac{\text{number of SSDF attackers}}{\text{number of honest SUs } + \text{ number of SSDF attackers}}. \tag{36}$$

Figure 2 shows that independent spectrum sensing is not affected by the fraction of MSUs at all and that CSS is sensitive to the fraction of MSUs and performs worse when it comes to a high fraction of MSUs. Moreover, 'always occupied' attacks have greatest impacts on CSS and 'always idle' attacks have the lowest effects on CSS. This is mainly due to the large coverage area of CRAHNs, which means that most cognitive nodes are out of the PU's coverage and may fall into an 'idle' status. MSUs out of the PU's coverage, which adopt an 'always idle' strategy, report errorless data to the FC, and vice versa. In Figure 2a, when the fraction of SSDF attackers is high, the performance of CSS is low and thus independent sensing is selected as the final decision of the 4S algorithm. Therefore, the performance of the 4S algorithm converges with the performance of independent sensing. In Figure 2b, the flattening of the plots is caused because SUs out of the PU's coverage report errorless data to the FC. The convergence value depends on the ratio of the number of SUs out of the PU's coverage to the number of SUs in the PU's coverage.

It also can be seen from Figure 2 that there is a gap between the performance of the 4S algorithm and the upper bound of the 4S algorithm. Firstly, we assume that $\left(P_d^C\right)_{\max} \approx 1$ and $\left(P_f^C\right)_{\min} \approx 0$; when these are not perfectly satisfied, the threshold selection is not optimal. Secondly, in the above discussion, the total strategy selection error P_e^i reaches a minimum value, which is equal to 0. This means that there are still some cases in which SUs make the wrong choice in strategy selection. Therefore, the upper bound of the 4S algorithm cannot be reached.

Overall, Figure 2 proves that the 4S algorithm performs much better than CSS when the fraction of MSUs is high and slightly worse than CSS in the case of a limited fraction of MSUs. Moreover, the 4S algorithm is almost always superior to independent spectrum sensing, except in the case of moderate to high fractions of MSUs under an "always occupied" attack.

Figures 3 and 4 show the influence of probabilistic attacks on the performance of three sensing algorithms with a hard decision and with a soft decision [4], respectively. It was demonstrated that CSS with a soft decision is vulnerable to malicious attacks and the performance of CSS with a soft decision is worse than that of CSS with a hard decision. This is mainly due to the robustness of the hard decision topological information cost function. Compared with the soft decision topological information function, the hard one causes information losses to MSUs, which results in the poor performance of MSUs. Therefore, CSS with a hard decision perform better than CSS with a soft

decision under a high fraction of MSUs. Although the performance of the 4S algorithm decays as a result of the decline of the CSS performance as the fraction of MSUs rises, the former still outperforms CSS and independent spectrum sensing. As the probability of attack increases, the curve of the 4S algorithm merges with that of independent sensing, which means that the 4S algorithm selects the independent sensing results when the CSS results are deeply affected by malicious nodes.

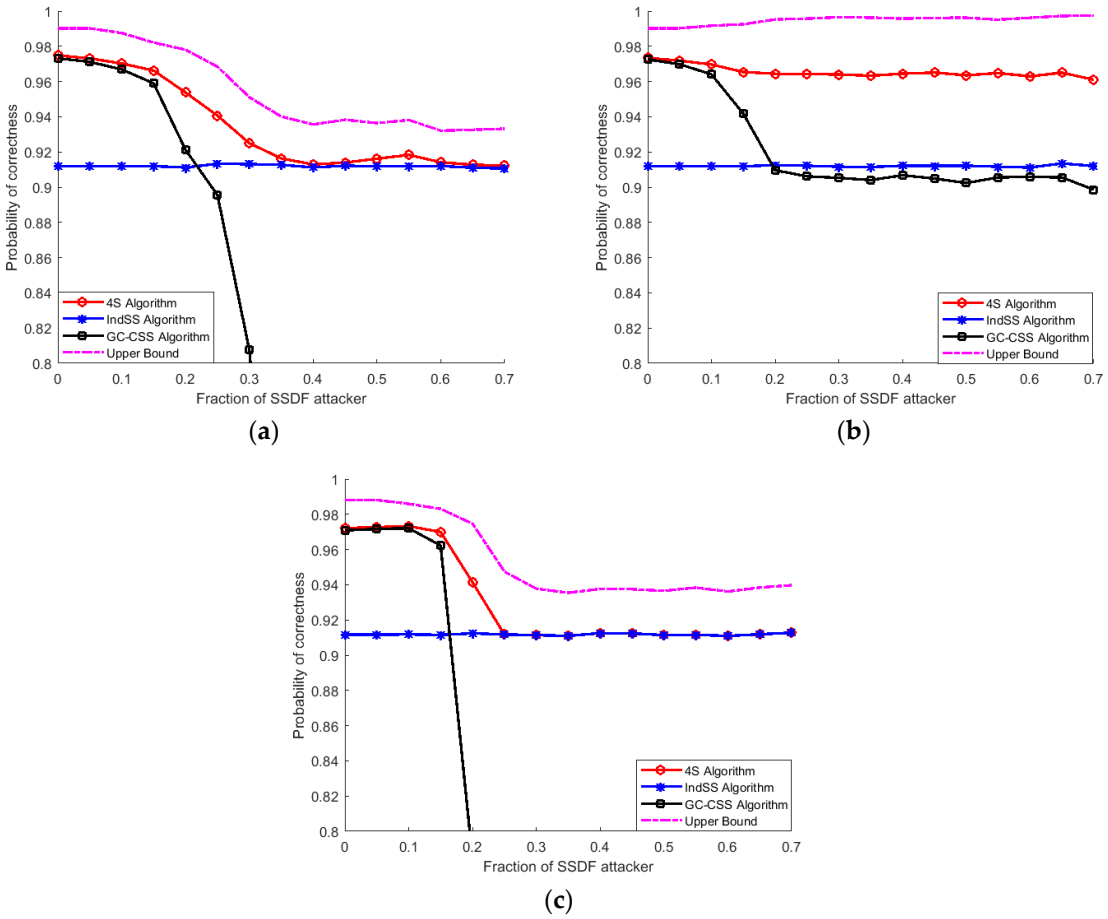


Figure 2. Comparison of three sensing strategies under various attack strategies. (**a**) "Always false" attack; (**b**) "always idle" attack; (**c**) "always occupied" attack.

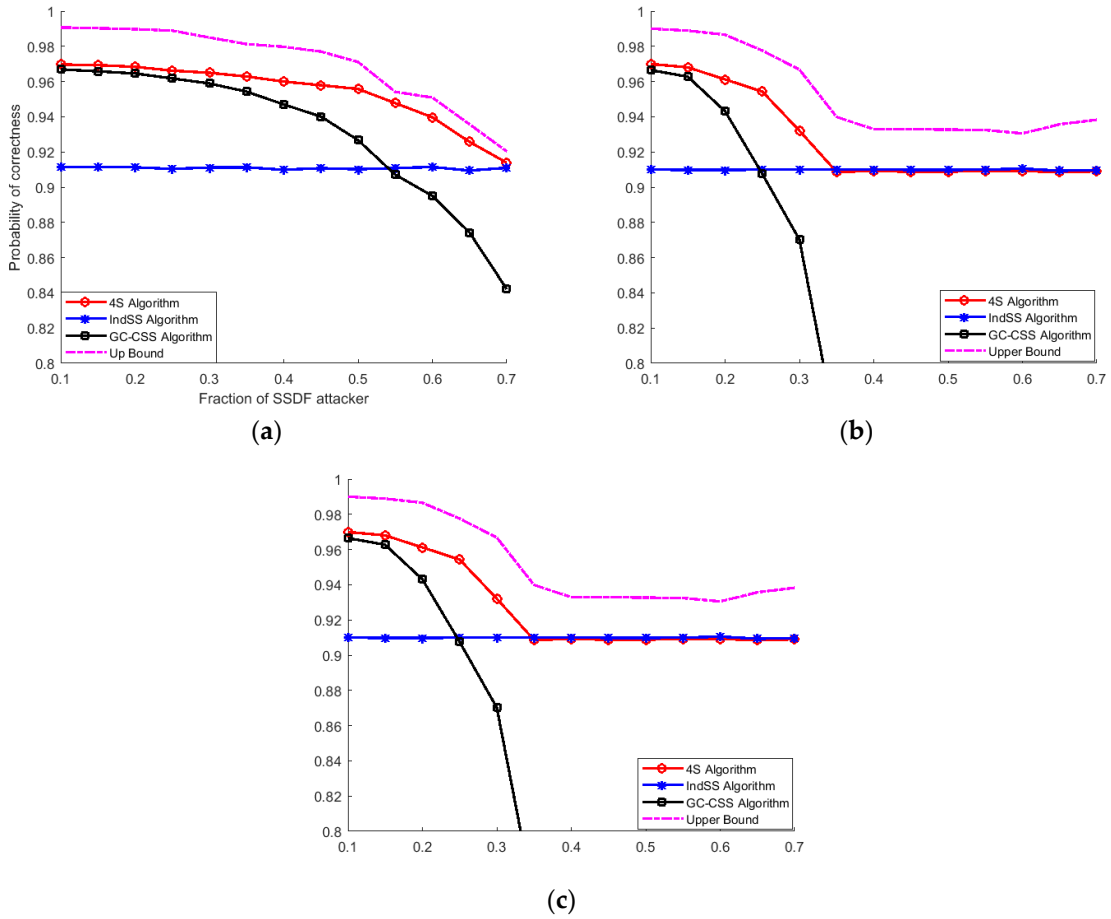


Figure 3. Comparison of three sensing strategies under possible attack with a hard decision. (**a**) Possible attack with probability = 0.2; (**b**) possible attack with probability = 0.5; (**c**) possible attack with probability = 0.8.

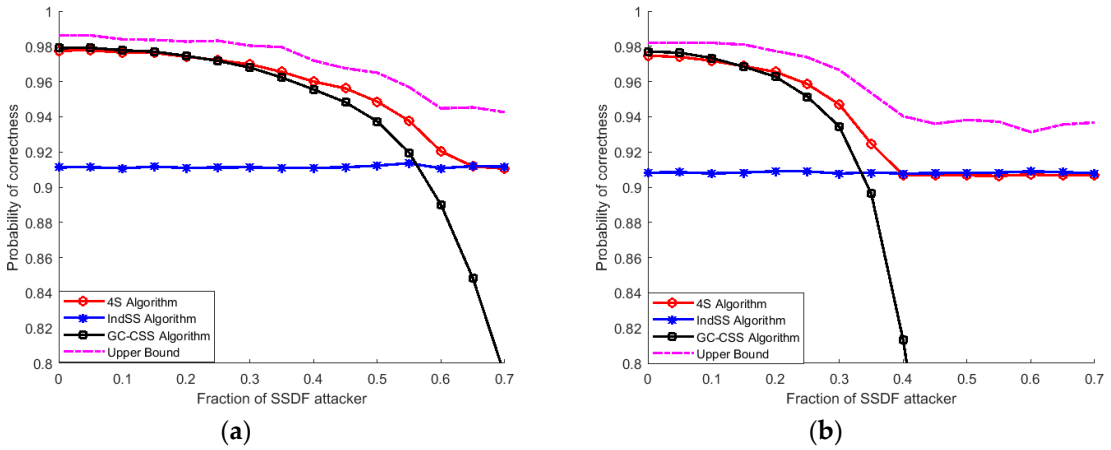
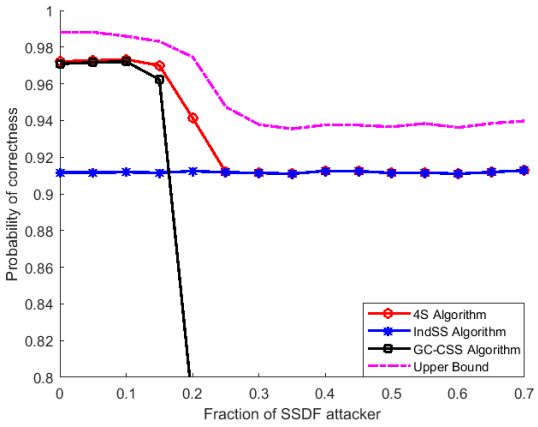


Figure 4. *Cont.*



(**c**)

Figure 4. Comparison of three sensing strategies under possible attack with a soft decision. (**a**) possible attack with probability = 0.2; (**b**) possible attack with probability = 0.5; (**c**) possible attack with probability = 0.8.

Owing to spectrum heterogeneity in CRAHNs and various fractions of MSUs, the performance of CSS and independent sensing among cognitive nodes differs. In the 4S algorithm, when the fraction of MSUs is relatively low in networks, the majority of SUs tend to select the CSS results as the final decision; thus, the performance of the 4S algorithm is roughly the same as that of CSS. When the number of MSUs increases, the performance of CSS gets worse. Therefore, it is reasonable for the 4S algorithm to select the insensitive independent sensing results as the final decision rather than the CSS results. To sum up, the 4S algorithm shows robustness under SSDF attack.

7. Conclusions

In this paper, we developed an adaptive deciding mechanism against SSDF attacks. Independent sensing and CSS have different sensitivities to the fraction of malicious nodes. We proposed the 4S algorithm, in which spectrum sensing is designed to adaptively select the better results between CSS and independent sensing under various attacking fractions of MSUs. The algorithm evaluates the performance of CSS and independent sensing through comparing reputation values. The simulation results clearly verified the effectiveness of the proposed 4S algorithm under varying malicious node attack strategies. The performance of the 4S algorithm is comparable ti that of CSS when the fraction of MSUs is high and it outperforms CSS when there is a low fraction of malicious nodes.

Author Contributions: Conceptualization, Z.S.; Formal analysis, Z.X.; Funding acquisition, Z.S.; Investigation, X.N.; Software, Z.X.; Supervision, X.N. and L.G.; Writing—original draft, Z.X.; Writing—review and editing, Z.C.

Funding: This research was funded by the National Natural Science Foundation of China (Grant No. 61401196) and the Natural Science Foundation of Jiangsu Province (Grant No. BK20140954).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

By substituting $p = \frac{P_{\max}-P_{\text{thr}}}{P_{\text{thr}}-P_{\min}}(\omega - P_{\min})$ in $\int_{P_{thr}}^{P_{\max}} \frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right) \mathrm{d}p$, we obtain

$$\int_{P_{\min}}^{P_{\text{thr}}} \frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right) \cdot \frac{P_{\max}-P_{\text{thr}}}{P_{\text{thr}}-P_{\min}} \mathrm{d}\omega. \tag{A1}$$

To prove that solution of $\frac{\partial P_e^i}{\partial \eta} = 0$ exists, we first prove that $\frac{\partial P_e^i}{\partial \eta} < 0$ when $\eta = P_{\min}$ and $\frac{\partial P_e^i}{\partial \eta} > 0$ when $\eta = P_{\max}$. Then $\frac{\partial P_e^i}{\partial \eta}\Big|_{\eta=P_{\max}} \geq 0$ needs to be proved. Accordingly, we obtain

$$\int_{P_{\min}}^{P_{\text{thr}}} \frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right) \cdot \frac{P_{\max}-P_{\text{thr}}}{P_{\text{thr}}-P_{\min}} \mathrm{d}\omega \geq \int_{P_{\min}}^{P_{\text{thr}}} \frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right) \mathrm{d}p. \tag{A2}$$

Thus, the above inequation is proven if the following inequation is proved to be true:

$$\frac{1}{\sqrt{2\pi T\theta(1-\theta)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right) \cdot \frac{P_{\max}-P_{\text{thr}}}{P_{\text{thr}}-P_{\min}} \geq \frac{1}{\sqrt{2\pi T\omega(1-\omega)}} \exp\left(-\frac{(\eta-T\omega)^2}{2T\omega(1-\omega)}\right), \tag{A3}$$

where $p = \frac{P_{\max}-P_{\text{thr}}}{P_{\text{thr}}-P_{\min}}(\omega - P_{\min})$.

That is,

$$\exp\left(\frac{(\eta-T\omega)^2}{2T\omega(1-\omega)} - \frac{(\eta-Tp)^2}{2Tp(1-p)}\right) \geq \frac{\sqrt{2\pi Tp(1-p)}}{\sqrt{2\pi T\omega(1-\omega)}} \cdot \frac{P_{\text{thr}}-P_{\min}}{P_{\max}-P_{\text{thr}}}. \tag{A4}$$

From the above equation, we can obtain:

$$\mathrm{T} \geq \frac{1}{\frac{(\eta/T-\omega)^2}{2\omega(1-\omega)} - \frac{(\eta/T-p)^2}{2p(1-p)}} \log\left(\frac{\sqrt{2\pi Tp(1-p)}}{\sqrt{2\pi T\omega(1-\omega)}} \cdot \frac{P_{\text{thr}}-P_{\min}}{P_{\max}-P_{\text{thr}}}\right). \tag{A5}$$

It is assumed that T is large enough, thus $\frac{\partial P_e^i}{\partial \eta}\Big|_{\eta=P_{\max}} \geq 0$.

Similarly, $\frac{\partial P_e^i}{\partial \eta} \leq 0$ when $\eta = P_{\min}$ can be proved.

Appendix B

It is difficult to solve Equation (31), hence we derive an approximation of Equation (31) with a sufficiently large T.

At first, $f(x)$ and $g(x)$ are defined as follows:

$$f(x) = \frac{1}{\sqrt{2\pi Tx(1-x)}} \exp\left(-\frac{(\eta-Tx)^2}{2Tx(1-x)}\right), \tag{A6}$$

$$g(x) = x(1-x). \tag{A7}$$

At interval $[\eta-\Delta, \eta+\Delta]$, we have $g(\eta+\Delta) - g(\eta-\Delta) = 2\Delta(1-2\eta)$. Therefore, $g(x)$ can be regarded as a constant $g(\eta)$ at interval $[\eta-\Delta, \eta+\Delta]$ if we ignore $2\Delta(1-2\eta)$. Then we obtain:

$$\begin{aligned} \frac{\partial P_e^i}{\partial \eta} &= \int_{P_{\text{thr}}}^{P_{\max}} \frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right) \mathrm{d}p - \int_{P_{\min}}^{P_{\text{thr}}} \frac{1}{\sqrt{2\pi Tp(1-p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tp(1-p)}\right) \mathrm{d}p \\ &= \int_{\Omega_1} \frac{1}{\sqrt{2\pi Tg(\eta)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tg(\eta)}\right) \mathrm{d}p + \varepsilon_1 - \int_{\Omega_2} \frac{1}{\sqrt{2\pi Tg(\eta)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tg(\eta)}\right) \mathrm{d}p - \varepsilon_2 \end{aligned}, \tag{A8}$$

where ε_1 and ε_2 are given by:

$$\begin{cases} \varepsilon_1 = \int_{\Omega_3} \frac{1}{\sqrt{2\pi Tg(p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tg(p)}\right) \mathrm{d}p \\ \varepsilon_2 = \int_{\Omega_4} \frac{1}{\sqrt{2\pi Tg(p)}} \exp\left(-\frac{(\eta-Tp)^2}{2Tg(p)}\right) \mathrm{d}p \end{cases}, \tag{A9}$$

and

$$\begin{cases} \Omega_1 = [P_{\text{thr}}, P_{\max}] \cap [\eta - \Delta, \eta + \Delta] \\ \Omega_2 = [P_{\min}, P_{\text{thr}}] \cap [\eta - \Delta, \eta + \Delta] \\ \Omega_3 = [P_{\text{thr}}, P_{\max}] - [\eta - \Delta, \eta + \Delta] \\ \Omega_4 = [P_{\min}, P_{\text{thr}}] - [\eta - \Delta, \eta + \Delta] \end{cases}. \tag{A10}$$

Consider that ξ is sufficiently small, this satisfies $\max\{f(\theta), \theta \in \Omega_3 \cup \Omega_4\} \leq \xi$, i.e.,

$$\frac{1}{\sqrt{2\pi T g(p)}} \exp\left(-\frac{(\eta - Tp)^2}{2Tg(p)}\right) \leq \xi. \tag{A11}$$

Noting that T is sufficiently large, Equation (A11) holds, thus we obtain:

$$\max\{f(\eta - \Delta), f(\eta + \Delta)\} \leq \xi. \tag{A12}$$

Namely,

$$\varepsilon_1 = \int_{\Omega_3} \frac{1}{\sqrt{g(p)}} \exp\left(-\frac{(\eta - Tp)^2}{2g(p)/\mathrm{T}}\right) \mathrm{d}p \leq \int_{\Omega_3} \xi \mathrm{d}p. \tag{A13}$$

When ξ is sufficiently small, ε_1 can be neglected. Similarly, ε_1 is sufficiently small and is neglected. Thus, we obtain:

$$\begin{aligned} \frac{\partial P_e^i}{\partial \eta} &\approx \int_{\Omega_1} \frac{1}{\sqrt{2\pi T g(\eta)}} \exp\left(-\frac{(\eta - Tp)^2}{2Tg(\eta)}\right) \mathrm{d}p + \zeta_1 \\ &- \int_{\Omega_2} \frac{1}{\sqrt{2\pi T g(\eta)}} \exp\left(-\frac{(\eta - \theta)^2}{2Tg(\eta)}\right) \mathrm{d}p - \zeta_2 \\ &= \int_{P_{\text{thr}}}^{P_{\max}} \frac{1}{\sqrt{2\pi T g(\eta)}} \exp\left(-\frac{(\eta - \theta)^2}{2Tg(\eta)}\right) \mathrm{d}p - \int_{P_{\min}}^{P_{\text{thr}}} \frac{1}{\sqrt{2Tg(\eta)}} \exp\left(-\frac{(\eta - \theta)^2}{2Tg(\eta)}\right) \mathrm{d}p \\ &= \frac{1}{2(P_{\max} - P_{\min})} \left(erf\left(\frac{P_{\max}}{\sqrt{2Tg(\eta)}}\right) + erf\left(\frac{P_{\min}}{\sqrt{2Tg(\eta)}}\right) - 2erf\left(\frac{P_{\text{thr}}}{\sqrt{2Tg(\eta)}}\right)\right) \end{aligned}. \tag{A14}$$

References

1. Federal Communications Commission. Spectrum Policy Task Force. Rep. ET Docket no. 02-135; 2002. Available online: https://fcc.gov/sptf/files/SEWGFinalReport_1.pdf (accessed on 10 December 2018).
2. Mitola, J.; Maguire, G.Q. Cognitive radio: Making software radios more personal. *IEEE Pers. Commun.* **1999**, *6*, 13–18. [CrossRef]
3. Yucek, T.; Arslan, H.A. survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 116–130. [CrossRef]
4. Wu, K.; Tang, M.; Tellambura, C.; Ma, D. Cooperative Spectrum Sensing as Image Segmentation: A New Data Fusion Scheme. *IEEE Commun. Mag.* **2018**, *56*, 142–148. [CrossRef]
5. Kailkhura, B.; Han, Y.S.; Brahma, S.; Varshney, P.K. Distributed Bayesian Detection in the Presence of Byzantine Data. *IEEE Trans. Signal Process.* **2015**, *63*, 5250–5263. [CrossRef]
6. Azer, M.A.; El-Kassas, S.M.; Hassan, A.W.F.; El-Soudani, M.S. A survey on trust and reputation schemes in ad hoc networks. In Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, Barcelona, Spain, 4–7 March 2008; pp. 881–886.
7. Feng, J.; Zhang, M.; Xiao, Y.; Yue, H. Securing Cooperative Spectrum Sensing Against Collusive SSDF Attack using XOR Distance Analysis in Cognitive Radio Networks. *Sensors* **2018**, *18*, 370. [CrossRef] [PubMed]
8. Feng, J.; Li, S.; Lv, S.; Wang, H.; Fu, A. Securing Cooperative Spectrum Sensing against Collusive False Feedback Attack in Cognitive Radio Networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 8276–8287. [CrossRef]
9. Qin, Z.; Li, Q.; Hsieh, G. Defending against cooperative attacks in cooperative spectrum sensing. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 2680–2687. [CrossRef]
10. Nguyen-Thanh, N.; Koo, I. An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context. *IEEE Commun. Lett.* **2009**, *13*, 492–494. [CrossRef]

11. Hyder, C.S.; Grebur, B.; Xiao, L.; Ellison, M. ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks. *IEEE Trans. Mob. Comput.* **2014**, *13*, 1707–1719. [CrossRef]
12. Zeng, K.; Pawelczak, P.; Cabric, D. Reputation-based cooperative spectrum sensing with trusted nodes assistance. *IEEE Commun. Lett.* **2010**, *14*, 226–228. [CrossRef]
13. Wang, P.; Chen, C.; Zhu, S.; Lyu, L.; Zhang, W.; Guan, X. An optimal reputation-based detection against SSDF attacks in industrial cognitive radio network. In Proceedings of the 2017 13th IEEE International Conference on Control & Automation (ICCA), Ohrid, Macedonia, 3–6 July 2017.
14. Ren, J.; Zhang, Y.; Ye, Q.; Yang, K.; Zhang, K.; Shen, X.S. Exploiting Secure and Energy Efficient Collaborative Spectrum Sensing for Cognitive Radio Sensor Networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 6813–6827. [CrossRef]
15. Rawat, A.S.; Anand, P.; Chen, H.; Varshney, P.K. Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks. *IEEE Trans. Signal Process.* **2011**, *59*, 774–786. [CrossRef]
16. Min, A.W.; Kim, K.; Shin, K.G. Robust Cooperative Sensing via State Estimation in Cognitive Radio Networks. In Proceedings of the 2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Aachen, Germany, 3–6 May 2011.
17. Boykov, Y.; Kolmogorov, V. An experimental comparison of min-cut/max-flow algorithms for energy minimization in vision. *IEEE Trans. Pattern Anal. Mach. Intell.* **2004**, *26*, 1124–1137. [CrossRef] [PubMed]
18. Kolmogorov, V.; Boykov, Y.; Rother, C. Applications of parametric maxflow in computer vision. In Proceedings of the 2007 IEEE 11th International Conference on Computer Vision, Rio de Janeiro, Brazil, 14–21 October 2007; pp. 1–8.
19. Greig, D.M.; Porteous, B.T.; Seheult, A.H. Exact maximum a posteriori estimation for binary images. *J. R. Stat. Soc.* **1989**, *51*, 271–279. [CrossRef]
20. Boykov, Y.; Kolmogorov, V. An experimental comparison of min-cut/max-flow algorithms for energy minimization in vision. In *International Workshop on Energy Minimization Methods in Computer Vision and Pattern Recognition*; Springer: Heidelberg/Berlin, Germany, 2001; pp. 359–374.
21. Wang, J.; Guo, Q.; Zheng, W.X.; Wu, Q. Robust Cooperative Spectrum Sensing Based on Adaptive Reputation and Evidential Reasoning Theory in Cognitive Radio Network. *Circuits Syst. Signal Process.* **2018**, *37*, 1–27. [CrossRef]
22. Mousavifar, S.A.; Leung, C. Energy efficient collaborative spectrum sensing based on trust management in cognitive radio networks. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 1927–1939. [CrossRef]
23. Box, G.E.P.; Hunter, W.G.; Hunter, J.S. *Statistics for Experimenters*; Wiley Interscience: Hoboken, NJ, USA, 2005; pp. 51–53.
24. Ma, L.; Xiang, Y.; Pei, Q.; Xiang, Y.; Zhu, H. Robust reputation-based cooperative spectrum sensing via imperfect common control channel. *IEEE Trans. Veh. Technol.* **2018**, *67*, 3950–3963. [CrossRef]
25. Wang, J.; Chen, R.; Tsai, J.J.P. Trust-based mechanism design for cooperative spectrum sensing in cognitive radio networks. *Comput. Commun.* **2018**, *116*, 90–100. [CrossRef]