Robust Collaborative Spectrum Sensing in the Presence of Deleterious Users

Kamran Arshad[†] and Klaus Moessner[‡],

[†]School of Engineering, University of Greenwich, United Kingdom

[‡]Centre for Communication Systems Research, University of Surrey, United Kingdom

Email: k.arshad@greenwich.ac.uk, k.moessner@surrey.ac.uk

Abstract

Collaborative spectrum sensing has attracted significant research attention in the last few years and is widely accepted as a viable approach to improve spectrum sensing reliability. Fusing data from multiple opportunistic users (OUs) in order to produce reliable sensing results implies a reliance on the OU to provide correct information. In the presence of malfunctioning or selfish users, performance of collaborative spectrum sensing deteriorates significantly. In this article, we propose mechanisms for the detection and suppression of such deleterious opportunistic users (DOUs) for hard and soft decision fusion. More specifically, a credibility based mechanism for hard decision fusion using a beta reputation system (HDC-BR) is introduced. Our proposed method does not require knowledge of the total number of deleterious users in advance. In HDC-BR, the fusion center assigns and updates weights to each user's decisions based on an individual user credibility score which is calculated using the beta reputation system. The presence of DOUs in soft decision based collaborative spectrum sensing has even more adverse effects on system performance. We also propose a scheme for the case of soft decision fusion to detect and eliminate falsified user observations at the fusion centre using a Modified Grubbs Test; we refer to it as SDC-MG. We compare the performance of the proposed methods with malicious user detection schemes proposed in the literature as well as with the case where no DOU suppression scheme is implemented, and conclude that SDC-MG performs much better than HDC-BR in a low Signal to Noise Ratio (SNR) regime.

Index Terms

Cognitive Radio, Collaborative Spectrum Sensing, Reputation Systems

I. Introduction

Opportunistic users operation relies on radio environment knowledge provided by geo-location databases or by spectrum sensing [1]. One most crucial task of an OU is to identify the presence of Incumbent Users (IUs) with high reliability over a wide spectrum. In a 2010 FCC ruling [1], a geo-location database based query mechanism was proposed for the protection of IU's, eliminating the need for spectrum sensing, initially required, back in 2008 [2]. However, spectrum regulators, including the Ofcom in UK and FCC in USA, still encourage researchers to continue research on spectrum sensing [3].

Several local and collaborative spectrum sensing schemes are available in the literature and a comprehensive survey has published in [4]. In *collaborative* or *centralised* spectrum sensing, a central entity controls the overall sensing operation, referred to as the fusion centre in remainder of this article. Opportunistic users taking part in collaborative spectrum sensing may send a soft decision (i.e. local observation) or hard decision (i.e. 1-bit decision) to the fusion centre, termed SDC and HDC respectively. In this article, we use energy detection for local spectrum sensing and consider both HDC and SDC based collaborative spectrum sensing. It should be noted that energy detection based sensing is used for simplicity and the proposed mechanisms are applicable in the case of any other sensing technique.

Most current collaborative spectrum sensing schemes assume that all OUs are honest, trustworthy and without any hardware faults [5]–[8]. An opportunistic user may be malign and send false information to the fusion centre e.g. due to device malfunctioning or selfish reasons. For instance, a selfish user may send sensing information to the fusion centre that an incumbent signal is present so that the fusion centre makes a wrong decision, allowing the selfish user to transmit its own signal on the free channel. A user may also send wrong information unintentionally due to defects or faults in its hardware. Identification of such users is a challenging task. In this article, such users are referred as DOUs and we assume that they send wrong sensing data because of aforementioned reasons. It has been shown in the literature that the presence of even a single DOU can severely degrade the performance of collaborative spectrum sensing [9].

There is limited literature that addresses collaborative spectrum sensing in the presence of DOUs. In [9], a simple approach was proposed in which opportunistic users report *yes* or *no* that indicates either IU present or absent, respectively. If there are k DOUs then the fusion centre declares *yes* only if at least $k+1$ users report *yes*. This approach has many disadvantages e.g. it requires the exact number of DOUs to be known in advance and the approach cannot be applied if users report soft information to the fusion centre. In [10], the credibility of users is taken into consideration, based on each users detection and false alarm rate, but this approach does not consider potential cheating behavior. Similarly, the approach proposed in [11] can differentiate between honest and deleterious users when there is a single deleterious user but the scheme cannot be applied when there are multiple DOUs. In [12], an approach based on reporting histories of opportunistic users has been presented for the detection of compromised nodes in collaborative spectrum sensing. The approach presented in [12] requires that the fusion centre have prior knowledge of the attackers policy, which is difficult to obtain in practice. Secure collaborative spectrum sensing based on outlier detection techniques has been proposed in [13], but assumes partial knowledge of incumbent user activity and proposed a malicious user detection scheme.

In this article, we investigate the effects of DOUs on collaborative spectrum sensing and consider both soft and hard decision combining at the fusion centre. We consider a centralised system in which all opportunistic users may send either soft or hard decisions to the fusion centre. The fusion centre makes a final decision using a weighted approach where weights are calculated using proposed schemes (i.e. HDC-BR and SDC-MG). We assume that the number of DOUs is unknown to the fusion centre. For the case of HDC, a robust credibility based collaborative detection scheme to alleviate the vicious effects of deleterious users is proposed. In our approach (HDC-BR), the fusion center calculates a credibility score of all OUs using a Bayesian formulation, more specifically a Beta Reputation (BR) system. The credibility score of each user is used to calculate a weight coefficient for the corresponding sensing result of that user at the fusion center. Initially, all users are considered as reliable. User credibility is updated at each sensing interval by checking consistency between global and local sensing decisions. Based on the credibility score, user information is weighted at the fusion centre and hence less credible users have less effect on the global decision.

We also propose a DOU detection scheme based on a Modified Grubbs Test (SDC-MG) for the case of SDC. The Grubbs test is used to detect a single outlier in normally distributed data. The modified Grubbs test, which is used in this article can be implemented for the detection of any number of deleterious users. The fusion centre identifies DOUs using the SDC-MG test and deletes observations from these users to nullify the effects of falsified information. Furthermore, both proposed schemes are able to detect if a good user suddenly turns bad and vice versa.

The rest of this article is organised as follows: In section II we describe the collaborative spectrum sensing model. In section III we provide an overview of the beta reputation system and explain the proposed credibility based collaborative spectrum sensing mechanism for HDC. We describe the modified Grubbs test based collaborative spectrum sensing scheme in section IV. Section V discusses the system parameters and simulation results and, finally, conclusions are drawn in section VI. Boldface notation is used to represent vectors and $[.]^{\mathrm{T}}$ represents their transpose.

II. System Model

We consider an incumbent user in a frequency band W and a group of K opportunistic users each equipped with an energy detector, let the set of users be represented as $\Omega = \{1, 2, 3, \cdots, K\}$. In addition, lets assume that there are M DOUs in the system such that $M < K$. The OUs perform spectrum sensing during a sensing interval T when instructed by the fusion centre and send their hard or soft decisions to the fusion centre through control channels. We also assume error free control channels for the transmission of sensing information.

A. Local Spectrum Sensing

Spectrum sensing can be formulated as a binary hypothesis testing problem as follows [8],

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

where $i \in \Omega$, $\mathcal{H}_0$ represents the null hypothesis that only noise is present, $\mathcal{H}_1$ represents the alternate hypothesis that both IU signal and noise is present. In equation (1), $s(t)$ is the IU signal and is assumed to be an independent and identically distributed (i.i.d.) Gaussian random variable with zero mean and variance σ_s^2. For the i^{th} OU, the receiver noise is modelled as $n_i(t)$ which is also assumed to be an i.i.d. Gaussian random process with zero mean and variance σ_n^2 and h_i is the complex gain of the channel between the IU and the i^{th} OU. Further, it is assumed that $s(t)$ and $n(t)$ are independent of each other. The received SNR at the i^{th} OU is given as,

$$\gamma_i \triangleq \frac{\mathbb{E}[|h_i|^2]\sigma_s^2}{\sigma_n^2}, \tag{2}$$

where $\mathbb{E}[.]$ represents the expectation operator.

Assume the sensing time-bandwidth product is always close to an integer and is denoted by $N = T \times W$. With energy detection, if T_i is the test statistics of an i^{th} user, the local decision rule can be written as [14],

$$T_i \triangleq \sum_{j=1}^{N} \left| x_i\left(\frac{j}{W}\right) \right|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \lambda_i, \tag{3}$$

where λ_i is the decision threshold at the i^{th} user. For large values of N (practically when $N \geq 10$ [15]), distribution of T_i converges to a normal distribution with statistics given by,

$$\mathbb{E}\left[T_i \mid \mathcal{H}_0\right] = N\sigma_n^2 \qquad \mathbb{E}\left[T_i \mid \mathcal{H}_1\right] = \left(N + \gamma_i\right)\sigma_n^2 \tag{4}$$

$$\text{Var}\left[T_i \mid \mathcal{H}_0\right] = 2N\sigma_n^4 \qquad \text{Var}\left[T_i \mid \mathcal{H}_1\right] = 2\left(N + 2\gamma_i\right)\sigma_n^4, \tag{5}$$

where Var[.] represents the variance operator. Hence the probability of false alarm $P_f^i = \Pr(\mathcal{H}_1 \mid \mathcal{H}_0)$ and detection $P_d^i = \Pr(\mathcal{H}_1 \mid \mathcal{H}_1)$ for an i^{th} user can be written as,

$$P_f^i = \mathrm{Q}\left(\frac{\lambda_i - N\sigma_n^2}{\sqrt{2N}\sigma_n^2}\right) \tag{6}$$

$$P_d^i = \mathrm{Q}\left(\frac{\lambda_i - (N + \gamma_i)\sigma_n^2}{\sqrt{2(N + 2\gamma_i)}\sigma_n^2}\right), \tag{7}$$

where Q(.) is the right tail probability of the standard normal distribution.

B. Hard Decision Combining - HDC

In hard decision fusion, each OU makes a local decision and sends this 1-bit information to the fusion centre via the common control channel in an orthogonal manner. Let $d_i \in \{0, 1\}$ represents i^{th} user decision i.e.,

$$d_i = \begin{cases} 1 & \text{if} \quad T_i \geq \lambda_i \\ 0. & \text{otherwise} \end{cases} \tag{8}$$

The fusion center combines decisions from all users and makes a global decision D as,

$$D = \mathfrak{g}\left(\mathbf{w}^h, \mathbf{d}\right), \tag{9}$$

where $\mathbf{d} = \left[d_1, d_2, \cdots, d_K\right]^{\mathrm{T}}$, $\mathbf{w}^h = \left[w_1^h, w_2^h, \cdots, w_K^h\right]^{\mathrm{T}}$ is the weight vector for HDC and $\mathfrak{g}$ is the fusion rule. According to the Neyman-Pearson criteria, approaches based on the Likelihood Ratio Test (LRT) provide optimal performance, hence an optimal combining scheme at the fusion centre results in following counting rule [16],

$$\sum_{j=1}^{K} d_j \log_e \left[\frac{P_d^j\left(1 - P_f^j\right)}{\left(1 - P_d^j\right)P_f^j}\right] \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \lambda^*, \tag{10}$$

where λ^* is the optimal threshold determined by the target global false alarm probability. To compute λ^* under the Neyman-Pearson criteria is mathematically untractable and generally the fusion centre is not aware of local detection and false alarm probabilities, hence one must use suboptimal solutions [17]. In this article, we select the counting based fusion rule, $\mathfrak{g}$, defined as follows [18],

$$D = \mathfrak{g}\left(\mathbf{w}^h, \mathbf{d}\right) = \begin{cases} 1 & [\mathbf{w}^h]^{\mathrm{T}}\mathbf{d} \geq \lceil \frac{K}{2} \rceil \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

where $\mathbf{w}^h$ is calculated using HDC-BR, discussed in section III-B.

C. Soft Decision Combining - SDC

In SDC, instead of sending 1-bit information, each user transmits T_i to the fusion centre. The fusion centre combine observations as,

$$y_s = \left[\mathbf{w}^s\right]^{\mathrm{T}} \mathcal{T} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \lambda^{**} \tag{12}$$

where $\mathbf{w}^s = \left[w_1^s, w_2^s, \cdots, w_K^s\right]^{\mathrm{T}}$ is the weight vector for SDC, $\mathcal{T} = \left[T_1, T_2, \cdots, T_K\right]^{\mathrm{T}}$ is the observation vector and λ^{**} again denotes the threshold based on the desired probability of false alarm. Depending on the outcome of SDC-MG, w_i^s is either 0 (ith user is identified as DOU) or 1 (ith user is not identified as DOU), i.e.

$$w_i^s = \begin{cases} 1 & \text{Reject hypothesis that } i^{\text{th}} \text{ user is DOU} \\ 0 & \text{Cannot reject hypothesis that } i^{\text{th}} \text{ user is DOU} \end{cases} \tag{13}$$

and is determined by SDC-MG. From equation (12) the distribution of y_s at the fusion centre can be written as,

$$\mathbb{E}\left[y_s \mid \mathcal{H}_0\right] = N\sigma_n^2 \sum_{i\in\Omega} w_i^s \qquad \mathbb{E}\left[y_s \mid \mathcal{H}_1\right] = \sum_{i\in\Omega} \left[w_i^s \left(N + \gamma_i\right)\right] \sigma_n^2 \tag{14}$$

$$\mathrm{Var}\left[y_s \mid \mathcal{H}_0\right] = 2N\sigma_n^4 \sum_{i\in\Omega} \left(w_i^s\right)^2 \qquad \mathrm{Var}\left[y_s \mid \mathcal{H}_1\right] = 2\sum_{i\in\Omega} \left[\left(N + 2\gamma_i\right)\left(w_s^i\right)^2\right] \sigma_n^4. \tag{15}$$

Hence, threshold λ^{**} as defined in (12) can be calculated as,

$$\lambda^{**} = N\sigma_n^2 \sum_{i\in\Omega} w_i^s + \mathrm{Q}^{-1}\left(\overline{P_f}\right) \sigma_n^2 \sqrt{2N \sum_{i\in\Omega} \left(w_i^s\right)^2}, \tag{16}$$

where $\left(\overline{P_f}\right)$ is the desired probability of false alarm.

III. Proposed Reputation based Collaborative Spectrum Sensing - HDC

This section provides an overview of the beta reputation system and then describes how the credibility of each user is built and updated in the HDC-BR scheme.

A. Beta Reputation System

Reputation systems are used to foster good behavior by providing incentives for honest users and to help some entity to make decisions about whom to trust. Reputation systems have been widely used in several domains e.g. e-commerce [19], Internet [20], ad-hoc Networks [21] etc. In human society, the credibility of an individual is established based on his/her interactions with others over the time. Our intent is to develop a similar mechanism in collaborative spectrum sensing to judge the credibility of each user based on how consistently a users opinion agrees with rest of the group. In a cognitive radio network, a fusion centre can employ a reputation system to identify deleterious users quickly and to minimise their contributions in global decision making by assigning appropriate weights, $\mathbf{w}^h$, to the users. A reputation system, CONFIDENT, was introduced in [22] in which nodes warn each other about deleterious nodes but the system is vulnerable to false accusations. There are other reputation systems that allow dissimilation of positive information only [23]. In such reputation systems, the information can still be falsely praised, resulting in a good reputation for deleterious users.

In cognitive radio networks, the requirements are different, as the focus is on the quick isolation of deleterious users. In this article, we apply the Bayesian approach for reputation updates and propose the use of beta reputation systems. The beta reputation system models the behavior of each OU in each iteration as a binary event modelled by the beta distribution. Beta distribution provides a sound mathematical basis for combining decisions from distributed users and for expressing the credibility of each user [24]. Since the true probability of an OU user to act deleteriously, say $\widetilde{p}$ is unknown, we estimate a credibility factor (i.e. ς) from the data obtained at the fusion centre. We take probability of $\widetilde{p}$ i.e. Prob($\widetilde{p}$) from the beta family, whose probability function is given by,

$$f(\widetilde{p} \mid \alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} \widetilde{p}^{\alpha-1} \left(1-\widetilde{p}\right)^{\beta-1}, \qquad 0 \leq \widetilde{p} \leq 1,\ \alpha \geq 0,\ \beta \geq 0 \tag{17}$$

with the restriction that $\widetilde{p} \neq 0$ if $\alpha < 1$ and $\widetilde{p} \neq 1$ if $\beta < 1$ [24]. The first order statistics of the beta distribution is given as,

$$\mathbb{E}[\widetilde{p}] = \frac{\alpha}{\alpha+\beta} \tag{18}$$

$$\text{Var}[\widetilde{p}] = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}. \tag{19}$$

The advantage of the beta reputation system is that it only needs two parameters (i.e. α and β) that are continually updated as decisions are reported to the fusion centre. Further, beta distribution is a suitable option because of its flexibility and ability to peak at any value in $[0, 1]$ with arbitrarily small variance.

In HDC, the fusion centre has two possible outcomes for each user in each sensing interval; the fusion centre either categorises d_i as *positive rating* or *negative rating*. Let $\zeta_{i,t}$ represent the total number of *positive ratings* and $\eta_{i,t}$ represent the total number of *negative ratings* in the t^{th} sensing interval where $t = 1, 2, \cdots$. The probability density function of the outcome that the i^{th} user has a *positive rating* in the t^{th} sensing interval is obtained by setting $\zeta_{i,t} = \alpha + 1$ and $\eta_{i,t} = \beta + 1$ i.e. [24],

$$f(\widetilde{p}) = \frac{\Gamma(\zeta_{i,t}+\eta_{i,t}+2)}{\Gamma(\zeta_{i,t}+1)\Gamma(\eta_{i,t}+1)} \widetilde{p}^{\zeta_{i,t}} \left(1-\widetilde{p}\right)^{\eta_{i,t}} \qquad \zeta_{i,t}, \eta_{i,t}\ \geq 0. \tag{20}$$

The probability expectation value is defined as $\mathbb{E}[\widetilde{p}]$ which is interpreted as the most likely value of $f(\widetilde{p})$.

B. Reputation based mechanism at Fusion Centre - HDC-BR

An opportunistic or cognitive radio user can be classified either as reputable or deleterious based on its current decision d_i and the global decision D, calculated from equation (8) and (9). A reputable OU is always honest i.e. transmitting its actual spectrum sensing observation or decision to the fusion centre, while a DOU is the one who may be dishonest (as explained in section 1) or honest but its sensing decisions are falsified. In order to achieve a high credibility score i.e. ς value, an OU needs to be honest and able to provide accurate sensing observations. The credibility score of each OU is updated at the fusion centre in each sensing interval. The overall process of implementing HDC-BR can be summarised as follows: All collaborative opportunistic users perform spectrum sensing in each sensing interval and send their reports to the fusion centre. After receiving sensing reports from the users, the fusion centre first calculates D using (9) or (11) and then decides if the i^{th} user is collaborative or not. The fusion centre then update the values of ζ_j and η_j by incorporating new observation d_i as follows:

$$\zeta_{i,t} = \zeta_{i,t-1} + \tau_i^{*}, \quad \eta_{i,t} = \eta_{i,t-1} + \tau_i^{**}, \tag{21}$$

where

$$\tau_i^* = \begin{cases} 1 & \text{if } \; d_i(t) = D(t) \\ 0 & \text{otherwise} \end{cases} \tag{22}$$

$$\tau_i^{**} = \begin{cases} 1 & \text{if } \; d_i(t) \neq D(t) \\ 0 & \text{otherwise} \end{cases} \tag{23}$$

Hence, based on equations (18) to (23), the credibility score ς_i of i^{th} user can be written as

$$\varsigma_i(t) \triangleq \mathbb{E}[\widetilde{p}] = \frac{\zeta_{i,t}+1}{\zeta_{i,t}+\eta_{i,t}+2}. \tag{24}$$

Finally, the weighting coefficients for the observations of each OU are defined as,

$$\mathbf{w}^h(t) = \frac{\boldsymbol{\varsigma}_t}{\sum_{i\in\Omega}\varsigma_{i,t}}, \tag{25}$$

where $\boldsymbol{\varsigma}_t = [\varsigma_{1,t}, \varsigma_{2,t}, \cdots, \varsigma_{K,t}]^{\text{T}}$. The weight vector defined in equation (25) is updated in each sensing interval and once a CR user is regarded as unreliable, their observations have less effect on the global decision because of the users low credibility score. The calculated $\{w_i^h \mid i \in \Omega\}$ is used in the next sensing interval and a final decision D is calculated using equation (11). It is noted here that the calculation of $\mathbf{w}^h$ can be performed between two consecutive sensing intervals hence the computational complexity of the proposed method is low.

IV. Identification of DOUs in Collaborative Spectrum Sensing - SDC

To defend collaborative spectrum sensing against deleterious users when users send their soft decisions to the fusion centre, we propose an outlier detection approach based on a Modified Grubbs test (SDC-MG). In SDC-MG, the fusion centre receives soft decisions from all K users and evaluates the credibility of each user based on Grubbs test. Unlike the HDC-BR approach discussed in section III, credibility is not building in successive sensing iterations rather fusion centre assigns tags (0 or 1) with each user observation i.e. deleterious users are detected immediately and completely eliminated in collaborative spectrum sensing.

A. Modified Grubbs Test for the detection of DOUs

The Grubbs test is one of the most commonly used tests for the detection of a single outlier in univariate data [25]. It is based on the assumption of normality and in this application soft decisions at the fusion centre can be reasonably approximated by normal distribution. According to the central limit theorem, for a large number of samples, the distribution of local sensing observations is approximately Gaussian [26]. For the detection of multiple DOUs, we implemented a “multiple-outlier” version of the Grubbs test, i.e. we removed one DOU at a time, reiterating until no DOU remains. Define,

$$\mathcal{H}_n : \quad \text{No DOUs in the received sensing observations} \tag{26}$$

$$\mathcal{H}_y : \quad \text{At least one DOU in the received sensing observations} \tag{27}$$

To detect a DOU, the fusion centre first calculates SDC-MG test statistics i.e. $\{\Re_k \mid k = 1, 2, \cdots, l\}$ and corresponding thresholds $\{e_k \mid k = 1, 2, \cdots, l\}$ where l is an initial estimate of the number of DOUs (e.g. it can be $K/2$ in the beginning) from the data set containing all K users observations, say $\mathcal{T}_K = \{T_1, T_2, \cdots, T_K\}$.

If all of the $\Re_k \leq e_k$ where $k \leq l$ then hypothesis $\mathcal{H}_n$ can not be rejected and there is no DOU in the data set $\mathcal{T}_K$ and we can assign $\{w_i^s = 1 \mid i \in \Omega\}$. If some $\Re_k > e_k$ then define $j = \max\{k : \Re_k > e_k\}$, and declare $T^{(0)}, T^{(1)}, \cdots, T^{(j-1)}$ as the DOU corresponds to the most extreme observations in the successively reduced data set. In the rest of this section, we explain how test statistics and critical values i.e. $\Re_i$ and e_i can be calculated by the fusion centre.

1) Test Statistics - SDC-MG: Statistic $\Re_k$ is the extreme studentised deviate completed from the data set $n - k + 1$. More specifically, the first statistic $\Re_1$ is given by,

$$\Re_1 = \frac{\max\left(T_i - \mathbb{E}[\mathcal{T}_K]\right)^2}{\mathrm{S}_{\mathcal{T}}}, \quad i \in \Omega \tag{28}$$

where $\mathbb{E}[\mathcal{T}_K]$ and $\mathrm{S}_{\mathcal{T}}$ is the mean and standard deviation of the data set $\mathcal{T}_K$.

$$\mathbb{E}[\mathcal{T}_K] = \frac{1}{K}\sum_{i\in\Omega} T_i \tag{29}$$

$$\mathrm{S}_{\mathcal{T}} = \frac{1}{K-1}\sum_{i\in\Omega}\left(T_i - \mathbb{E}[\mathcal{T}_K]\right)^2, \tag{30}$$

Similarly, $\Re_2$ is computed but with a reduced sample size of $K-1$ obtained by removing the sensing observation corresponding to $\max \mid T_i - \mathbb{E}[\mathcal{T}_K] \mid$ user from the full set $\mathcal{T}_K$ and similarly calculate $\Re_3$, $\Re_4$ and so on.

2) Calculation of Critical values: As described, $\Re_i$ has to be compared with the critical value e_i to decide if the i^{th} user is a deleterious user. In our scheme for the simultaneous detection of several DOU at the same time, critical values $e_i \mid i \in \Omega$ can be obtained from,

$$\Pr\left\{\bigcup_{i=\phi+1}^{l}\left(\Re_i > e_i \mid \mathcal{H}_y\right)\right\} = \widetilde{\alpha}, \quad \text{for} \quad \phi = 0, 1, \cdots, l-1 \tag{31}$$

where $\widetilde{\alpha}$ is the significance level to reject hypothesis $\mathcal{H}_n$. Using simulation, critical values can be calculated from equation (31), however such an approach is not suitable in our case as it requires a table of estimated percentiles for $\{\Re_k \mid k = 1, 2, \cdots, l\}$ [27]. An alternative approach is to approximate critical values from the t-distribution. For the calculation of critical values we adopt the approximate method proposed by Quesenberry et. al. [28].

$$e_{k+1} = \frac{t_{K-\phi-2,\bar{p}}\left(K-\phi-1\right)}{\left\{\left[K-\phi-2+t^2_{K-\phi-2,\bar{p}}\right](K-\phi)\right\}^{2}}, \quad \phi = 0, 1, 2, \cdots, l-1 \tag{32}$$

where $\bar{p} = 1 - [(\tilde{\alpha}/2)(K-\phi)]$ and $t_{a,b}$ represents the b^{th} percentile of a t-distribution with a degrees of freedom.

V. Simulation Results and Discussion

In this section, we present the simulation results of our proposed credibility based collaborative spectrum sensing schemes, HDC-BR and SDC-MG. For the simulations, we consider $K = 20$ opportunistic users in a cognitive radio network randomly distributed in a certain area such that the mean SNR of the users is uniformly distributed in the range of -15 to 5dB unless stated otherwise. Each user samples the received signal, $N = 10$ times and processes N received samples to generate test statistic T_i as defined in equation (3). We assume that the noise variance σ_n^2 is known to each user and is equal to 1. In our simulations, DOUs do not perform spectrum sensing but rather send random data to the fusion centre.

For the case of HDC-BR, we initially consider all as trusted users and initialise a weight vector $\mathbf{w}^h$ as a vector of all ones. To estimate values of probability of false alarm and probability of detection we considered $100,000$ iterations. From extensive simulation, we observed that the weight of all users converges after $10-12$ sensing intervals if the channel and user credibility conditions remain constant. If the sensing channel conditions change slowly then the proposed method will still work. However, if the sensing channel conditions change quickly, the HDC-BR method becomes invalid and this case is outside the scope of this article.

Similarly for SDC-MG, we initialise $w_i^s = 1$ for all values of $i \in \Omega$. The fusion centre receives sensing observations from the nodes and assigns appropriate values to w_i^s in each sensing interval. Both schemes assign weighting factors to the user contributions that help nullify the effect of false information in order to enhance the collaborative spectrum sensing performance in the presence of deleterious users.

In Fig. 1 and 2 we consider a collaborative spectrum sensing system having either no DOU, 10% DOU and 20% DOU and study the impact of deleterious users on the performance of collaborative spectrum sensing. Deleterious users are selected randomly in our simulations. We plot Receiver Operating Characteristics (ROC) curves for performance evaluation i.e. the probability of miss detection versus the probability of false alarm [8]. It is clear from Fig. 1 and 2 that presence of deleterious users significantly affects the performance of collaborative spectrum sensing. For example, with 20 collaborative users and false alarm rates equal to 50%, the presence of 10% and 20% DOUs can decrease detection rates to 32% and 50% respectively in SDC, while in HDC detection rates decreases up to 17% with 20% deleterious users. From the simulation results it is clear that DOUs badly affect the soft decision combining based collaborative spectrum sensing compared to hard decision combining. This is intuitively clear, since in SDC all users send their sensing observations to the fusion centre and performance depends on the overall magnitude of false readings.

In our simulation results, we compare the ROC curves for the case in which no deleterious user suppression scheme using SDC is used and we refer it as DOU-NC. In this case, all users contribute equally in the global decision making regarding the existence of incumbent users. Further, we compare the performance of our algorithms with another malicious user detection scheme recently proposed in literature [29]. In [29], authors propose a novel technique to eliminate DOU in cognitive networks, which they call Statistical Moment Deviation Detection (SMDD). In SMDD, DOU are detected by detecting variations in the statistical moment of sensing observations, for details refer to [29]. The proposed schemes i.e. HDC-BR and SDC-MG, are based on the credibility score of each user, where user observations or decisions are weighted at the fusion centre in order to nullify the effect of false information.

In Fig. 3 we plot miss detection probability versus false alarm probability when all opportunistic users receives higher mean SNR values. In particular, we assume that each user receives a mean SNR of $\gamma = 0$dB with 10% DOUs. Compared to DOU-NS and SMDD in the presence of deleterious users, the proposed schemes demonstrate significant gains in detection probability which is achieved by eliminating the effects of misbehaved users. Moreover, when the mean SNR of users is high, HDC-BR performs better than the SDC-MG scheme. Figure 4 shows the ROC curves with 10% deleterious opportunistic users with very low received SNR for all opportunistic users. Here, we assume received SNR at each user terminal is -10dB. With very low SNR, the SDC-MG scheme performs much better than HDC-BR. Hence, we conclude here that in low SNR regimes SDC-MG is better than HDC-BR while with high received SNR, the performance of HDC-BR is superior to

SDC-MG. To further substantiate these conclusions, miss detection probability was plotted versus received SNR for a given probability of false alarm in Fig. 5. The value of P_f was fixed to 0.5 and number of DOUs as 10%. It is clear from Fig. 5 that with SDC-MG, 20 users can detect a signal with average received SNR as low as -15dB with detection probability of 81.4% while with DOC-NC and HDC-BR such a low SNR signal can be detected with detection probability of 39.6% and 39.2% respectively.

In Fig. 6 we consider a scenario in which received mean SNR at the receiving terminals of OUs is low and uniformly distributed in the range of -15 to 5dB. We assumed there are 10% DOC which are randomly choosen from $K = 20$ users. From Fig. 6 it is clear that in low SNR regimes, performance of SHC-MG is significantly better than the HDC-BR and the scheme is able to detect and eliminate all 20% deleterious users. Hence, we can draw the conclusion that for higher received SNR the preferred scheme is HDC-BR, which also incurs less communication overhead. However for the case of low SNR, SDC-MG is able to reliably detect and isolate mischievous users.

In order to estimate the number of users that our proposed schemes are able to detect, we further plotted the probability of detection versus the number of deleterious opportunistic users for a fixed SNR of -5dB and for a given probability of false alarm, $P_f = 0.5$ (Fig. 7). The main conclusion that can be drawn from Fig. 7 is that, to a certain extent, both schemes can provide better performance if the number of deleterious users does not exceed $K/2$, i.e 50%. If more than half of the users are deleterious users than the proposed schemes do not improve detection performance. This result is consistent with the logical argument that if there are more deleterious users, then a global decision may be wrong and neither HDC-BR nor SDC-MG schemes are able to detect deleterious opportunistic users.

VI. Conclusions

In this article, collaborative spectrum sensing schemes that are able to detect deleterious users in cognitive radio networks have been proposed. We considered collaborative spectrum sensing scenarios where a user can either send a 1-bit decision or energy detector output to a central control (i.e. fusion centre) in order to determine the presence of incumbent users. In each case, a scheme to assign weights to individual users contributions for each sensing interval has been proposed. The procedure to identify deleterious users and reduce their impact on the overall global decision making at the fusion centre has been described. The proposed schemes do not require any feedback from the incumbent system and do not need any assistance from a trusted node. Further, our schemes do not require an exact number of deleterious opportunistic users to work. However, the inherent assumption is that there are more trusted users than deleterious users in the network. We analysed the performance of the proposed schemes with comprehensive simulations, and compared the simulation results with existing malicious user detection scheme available in the literature. The proposed schemes show significant advantages, primarily that they can identify deleterious users and eliminate their impact on the decision making. Our main conclusion is that if the average received SNR at users is high then HDC-BR performs better than SDC-MG while in the low SNR case, SDC-MG outperforms HDC-BR.

Acknowledgment

The research leading to these results was derived partially from the European Community's Seventh Framework Programme (FP7) under Grant Agreement number 248454 (QoSMOS) and partially from the University of Greenwich Research & Enterprise Investment Programme grant under agreement number RAE-ENG-04/12.

REFERENCES

[1] "Federal Communications Commission: Second Memorandum Opinion and Order," 2010. [Online] http://transition.fcc.gov/oet/dockets/et93-62/, accessed 30 July 2011.

[2] Federal Communications Commission Auctions, March 2008. [Online] http://www.wireless.fcc.gov/, accessed 30 July 2011.

[3] V. Goncalves and S. Pollin, "The value of sensing for tv white spaces," in *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on*, pp. 231 –241, may 2011.

[4] T. Yucek and H. Arslan, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[5] A. Ghasemi and E. S. Sousa, "Opportunistic Spectrum Access in Fading Channels through Collaborative Sensing," *IEEE Journal of Communications*, vol. 2, pp. 71–81, March 2007.

[6] J.-H. Lee, J.-H. Baek, and S.-H. Hwang, "Collaborative Spectrum Sensing using Energy Detector in Multiple Antenna System," in *10th International Conference on Advanced Communication Technology, ICACT'08*, vol. 1, pp. 427–430, Feb. 2008.

[7] K. Arshad and K. Moessner, "Collaborative Spectrum Sensing for Cognitive Radio," in *IEEE International Conference on Communications Workshops, 2009*, pp. 1–5, June 2009.

[8] K. Arshad, M. A. Imran, and K. Moessner, "Collaborative Spectrum Sensing Optimisation Algorithms for Cognitive Radio Networks," *International Journal of Digital Multimedia Broadcasting*, vol. 2010, no. 424036, 2010.

[9] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative Sensing among Cognitive Radios," in *IEEE International Conference on Communications, ICC'06*, vol. 4, pp. 1658–1663, June 2006.

[10] Y. Wendong, C. Yueming, and X. Youyun, "A Fuzzy Collaborative Spectrum Sensing Scheme in Cognitive Radio," *International Symposium on Intelligent Signal Processing and Communication Systems*, pp. 566–569, 2007.

[11] H. Wang, E.-H. Yang, Z. Zhao, and W. Zhang, "Spectrum Sensing in Cognitive Radio using Goodness of Fit testing," *IEEE Transactions on Wireless Communications*, vol. 8, pp. 5427–5430, November 2009.

[12] W. Wang, H. Li, Y. Sun, and Z. Han, "Securing Collaborative Spectrum Sensing Against Untrustworthy Secondary Users in Cognitive Radio Networks," *EURASIP J. Adv. Signal Process*, vol. 2010, pp. 4:4–4:4, Jan. 2010.

[13] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious User Detection in a Cognitive Radio Cooperative Sensing System," *IEEE Transactions on Wireless Communications*, vol. 9, pp. 2488 –2497, august 2010.

[14] H. Urkowitz, "Energy detection of unknown deterministic signals," *IEEE Proceedings*, vol. 55, pp. 523–531, April 1967.

[15] P. K. Varshney, *Distributed Detection and Data Fusion*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1996.

[16] G. Strang, *Introduction to Linear Algebra*. Wellesley-Cambridge Press, 2003.

[17] J. N. Tsitsiklis and M. Athans, "On the Complexity of Decentralized Decision Making and Detection Problems," in *The 23rd IEEE Conference on Decision and Control*, vol. 23, pp. 1638 –1641, dec. 1984.

[18] Z. Khan, J. Lehtomaki, K. Umebayashi, and J. Vartiainen, "On the selection of the best detection performance sensors for cognitive radio networks," *Signal Processing Letters, IEEE*, vol. 17, pp. 359 –362, april 2010.

[19] A. Gutowska and K. Buckley, "Computing reputation metric in multi-agent e-commerce reputation system," in *Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on*, pp. 255 –260, june 2008.

[20] T. Kaszuba, A. Hupa, and A. Wierzbicki, "Advanced Feedback Management for Internet Auction Reputation Systems," *IEEE Internet Computing*, vol. 14, pp. 31 –37, sept.-oct. 2010.

[21] Y. Liu and Y. Yang, "Reputation Propagation and Agreement in Mobile Ad-hoc Networks," in *IEEE Wireless Communications and Networking*, vol. 3, pp. 1510 –1515 vol.3, march 2003.

[22] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '02, (New York, NY, USA), pp. 226–236, ACM, 2002.

[23] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in *Proceedings of the 2nd ACM conference on Electronic commerce*, EC '00, (New York, NY, USA), pp. 150–157, ACM, 2000.

[24] A. Jøsang and R. Ismail, "The Beta Reputation System," in *Proceedings of the 15th Bled Electronic Commerce Conference*, 2002.

[25] V. Barnett and T. Lewis, *Outliers in Statistical Data*. Wiley, 3rd ed., February Feb 1994.

[26] Z. Quan, S. Cui, and A. Sayed, "Optimal Linear Cooperation for Spectrum Sensing in Cognitive Radio Networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, pp. 28–40, Feb. 2008.

[27] P. Prescott, "Critical Values for a Sequential Test for Many Outliers," *Journal of the Royal Statistical Society*, 1979.

[28] C. P. Quesenberry and H. A. David, "Some Tests for Outliers," *Biometrika*, vol. 48, no. 3/4, pp. 379–390, 1961.

[29] A. Javied, S. Rajasegarar, K. Arshad, and K. Moessner;, "A Statistical Moment Deviation Approach to Identify Outliers in Collaborative Spectrum Sensing for Cognitive Radio," in *Future Network and Mobile Summit 2012*, pp. 1–5, 4-6 July, 2012.

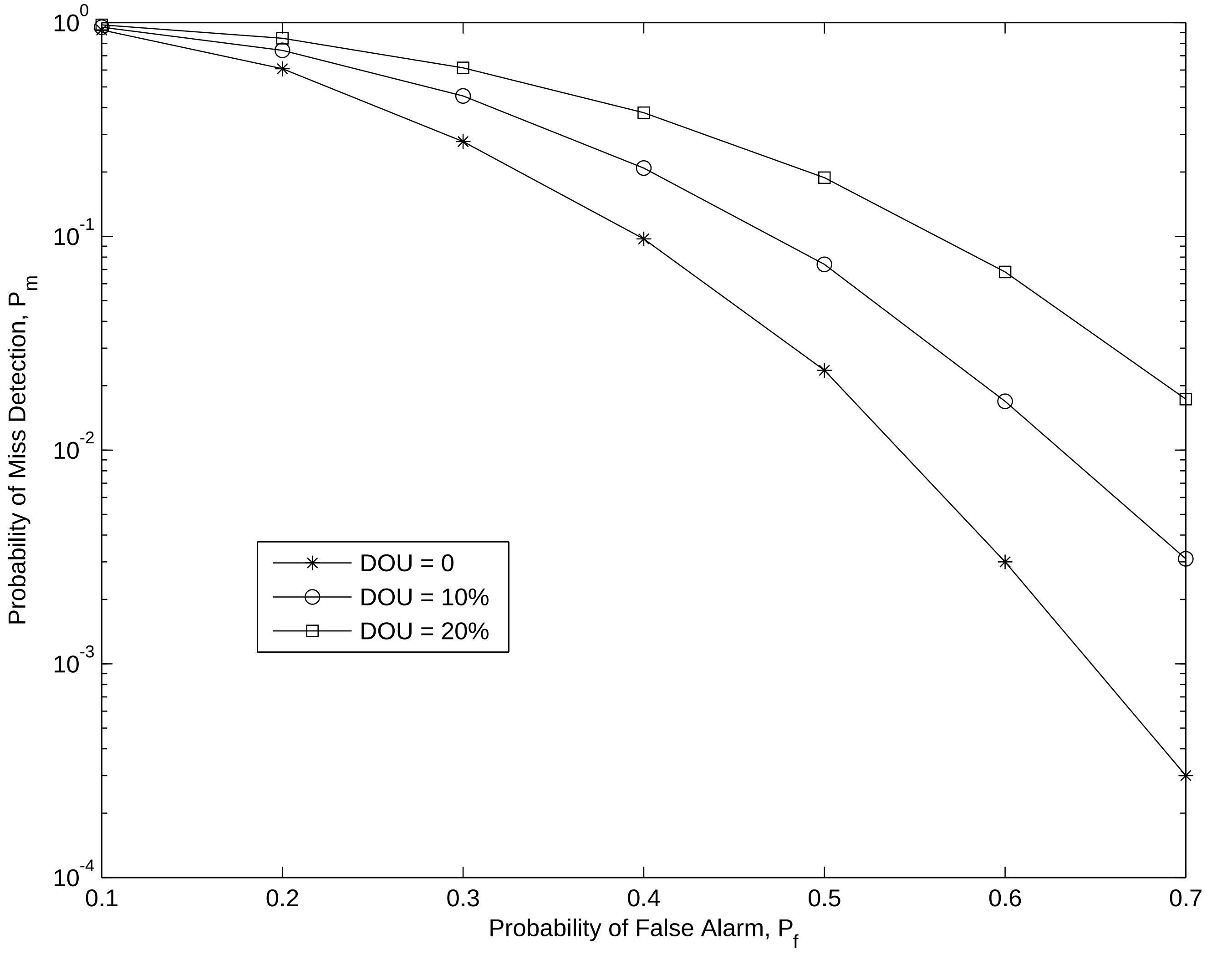

Fig. 1. Effect of Deleterious users on the performance of collaborative spectrum sensing in HDC, $N = 10$, $K = 20$ and $\gamma_i = -15$ to 5dB uniformly distributed

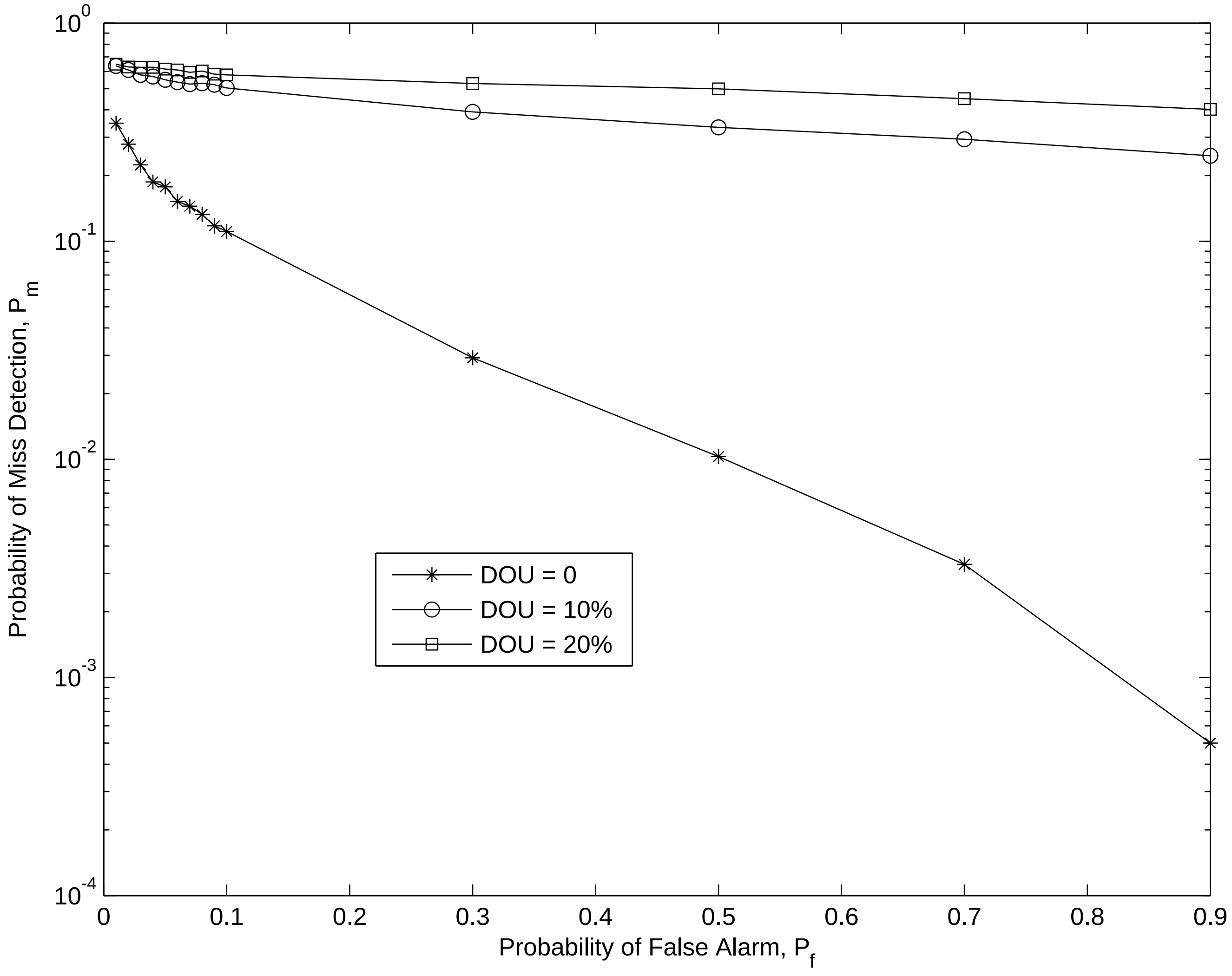

Fig. 2. Effect of Deleterious users on the performance of collaborative spectrum sensing in SDC, $N = 10$, $K = 20$ and $\gamma_i = -15$ to 5dB uniformly distributed

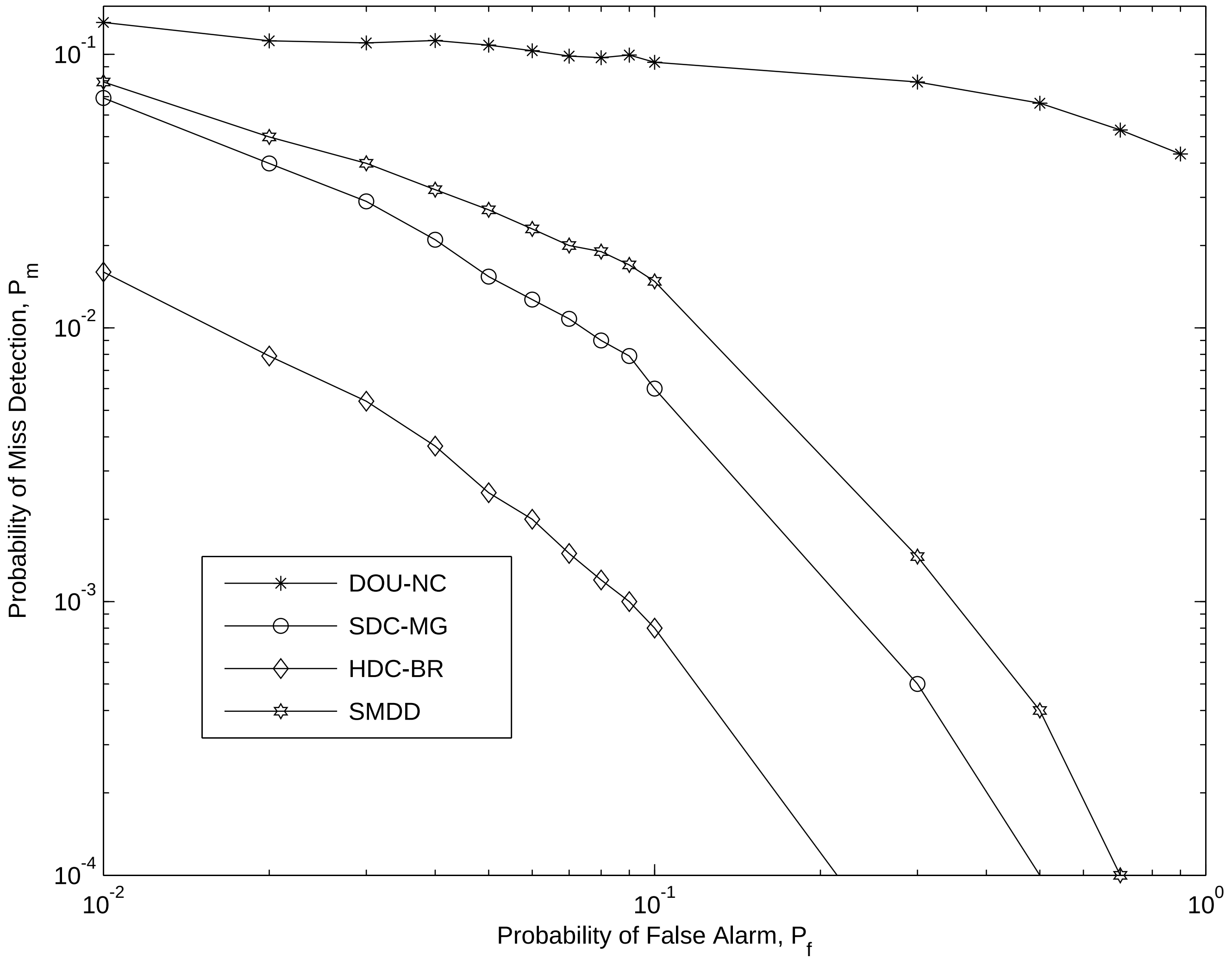

Fig. 3. Probability of miss detection versus false alarm probability in the presence of 10% Deleterious Opportunistic Users, $N = 10$, $K = 20$ and $\gamma_i = 0$dB

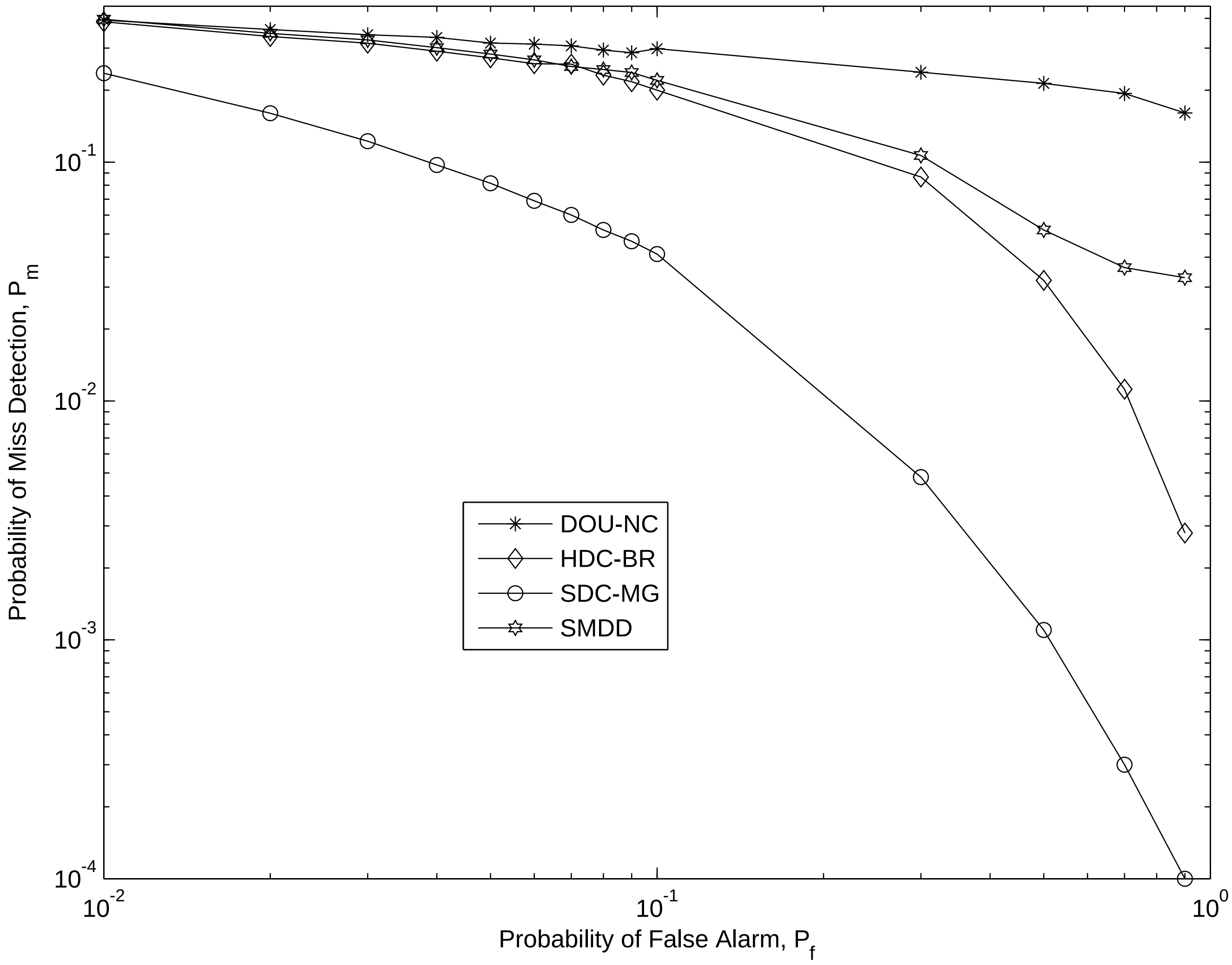

Fig. 4. Probability of miss detection versus false alarm probability in the presence of 10% Deleterious Opportunistic Users, $N = 10$, $K = 20$ and $\gamma_i = -10$dB

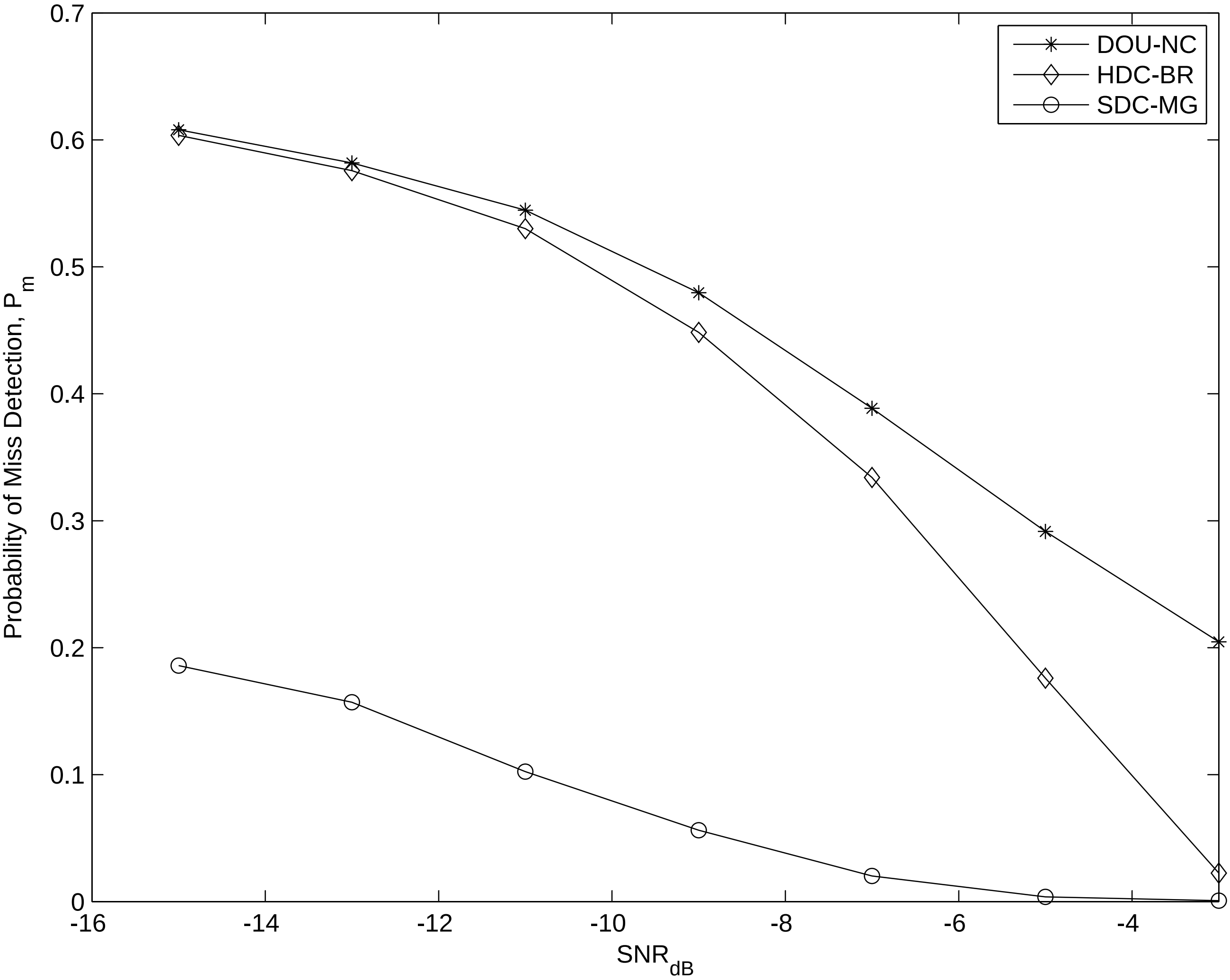

Fig. 5. Miss detection probability versus SNR with 10% Deleterious Opportunistic Users, N=10, K=20 and $P_f = 0.5$

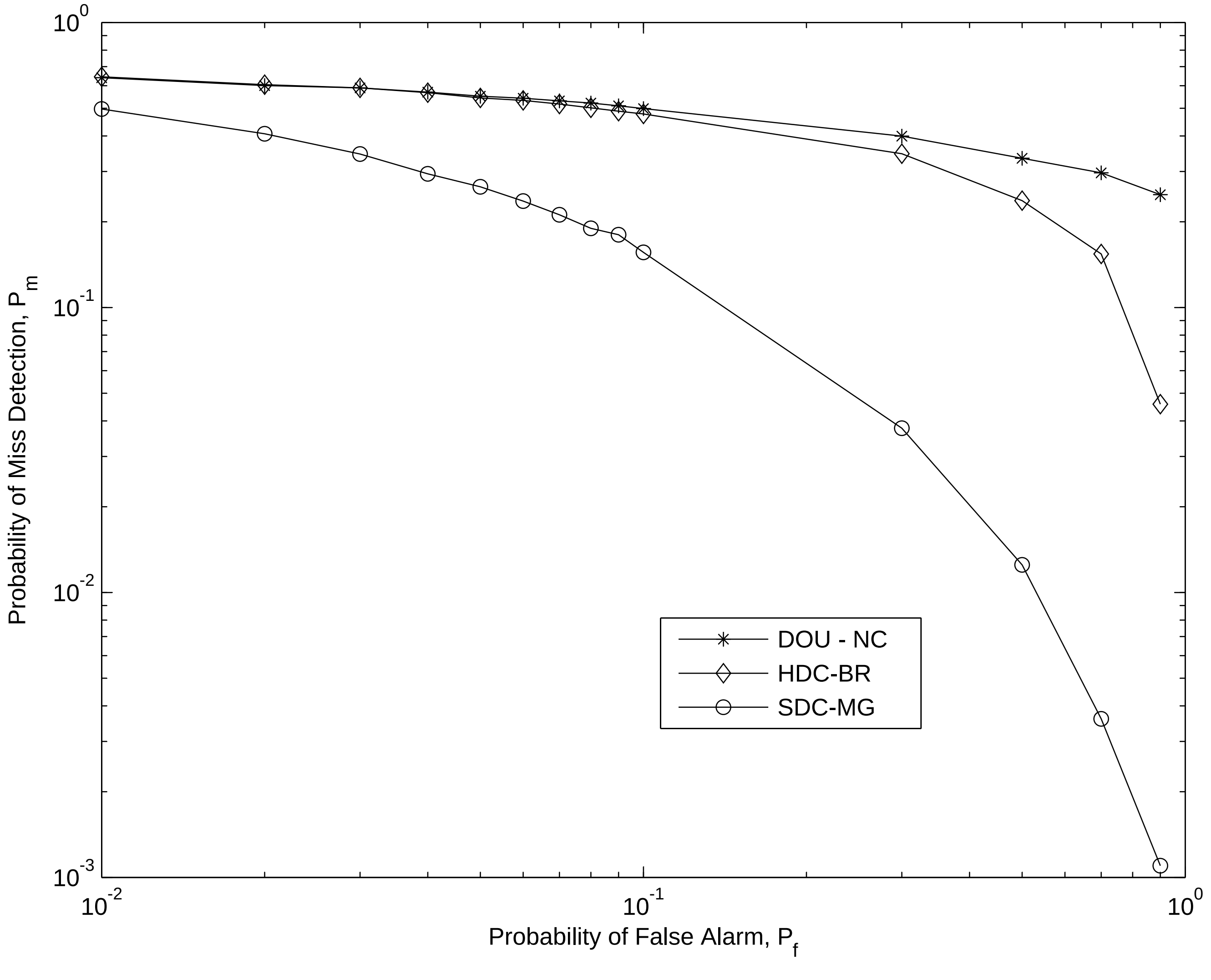

Fig. 6. ROC Curves with 10% Deleterious Opportunistic Users, $N = 10$, $K = 20$ and $\gamma_i = -15$ to 5dB uniformly distributed

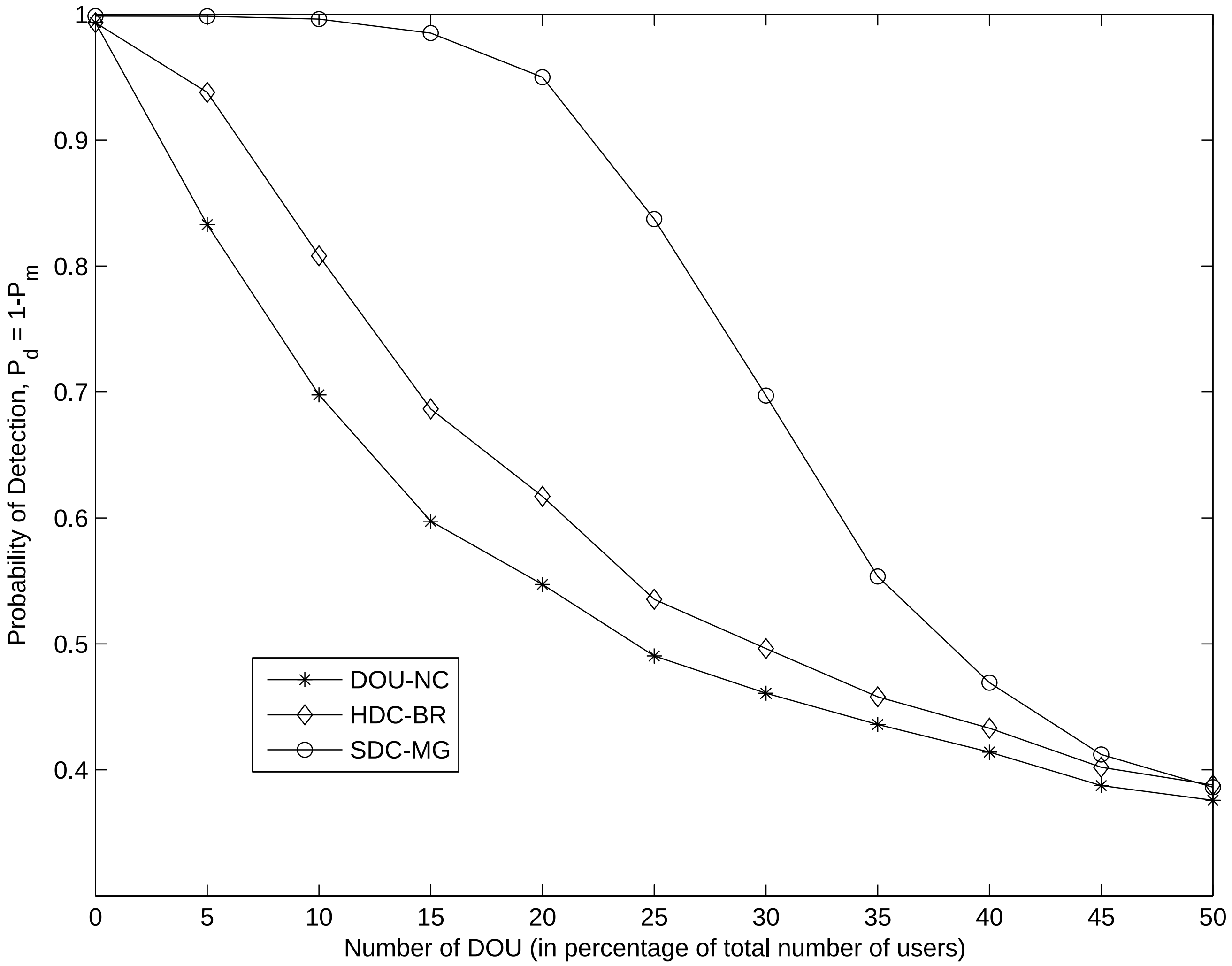

Fig. 7. Probability of Detection versus number of deleterious opportunistic users with $N = 10$, $K = 20$, $P_f = 0.5$ and $\gamma = -5$dB