Review of Robust Cooperative Spectrum Sensing Techniques for Cognitive Radio Networks

Helena Rifà-Pous · Mercedes Jiménez Blasco · Carles Garrigues

Abstract Cognitive radio networks sense spectrum occupancy and manage themselves to operate in unused bands without disturbing licensed users. The detection capability of a radio system can be enhanced if the sensing process is performed jointly by a group of nodes so that the effects of wireless fading and shadowing can be minimized. However, taking a collaborative approach poses new security threats to the system as nodes can report false sensing data to reach a wrong decision. This paper makes a review of secure cooperative spectrum sensing in cognitive radio networks. The main objective of these protocols is to provide an accurate resolution about the availability of some spectrum channels, ensuring the contribution from incapable users as well as malicious ones is discarded. Issues, advantages and disadvantages of such protocols are investigated and summarized.

Keywords Cognitive radio · Cooperative sensing · Data fusion · Reputation · Security

1 Introduction

The growing number of wireless services available nowadays has significantly increased the demand of radio spectrum resources. This has given rise to a worrying shortage of spectrum. Moreover, the Federal Communications Commission (FCC) has reported that most of the spectrum allocated to licensed users is largely under-utilized [5], and spectrum utilization is discontinuous across time and space.

In order to increase the efficiency in spectrum utilization, a solution has been proposed which is based on opportunistic spectrum sharing. In this approach, unlicensed users, which are referred to as secondary users (SU), are allowed to opportunistically access spectrum as long as they do not cause harmful interference with licensed users. Licensed users are referred to as primary users (PU), and they always have usage priority.

H. Rifà-Pous (✉) · M. J. Blasco · C. Garrigues
Internet Interdisciplinary Institute, Universitat Oberta de Catalunya, Barcelona, Spain
e-mail: hrifa@uoc.edu

Cognitive Radio (CR) [1] is the technology that has been proposed to implement opportunistic sharing. A cognitive radio is a system capable of sensing several spectrum bands, determine if there are unused portions, and adapt to operate in the vacant bands. The spectrum sensing mechanisms implemented by CRs should reliably detect the presence and absence of primary signals in real time. Once cognitive radios detect the presence of a primary user in their operating band, they must vacate the band immediately. Hence, accurate spectrum sensing is an essential feature of CR systems.

However, the effect of fading and shadowing on the spectrum sensing process can be very negative. These two problems can result in a secondary user failing to detect a primary signal, which is known as the hidden node problem. In order to avoid this problem, cognitive radio systems must be significantly more sensitive in detecting the primary transmissions than the primary receivers.

In order to reduce the individual sensitivity requirements of CRs, the technique that has been most frequently used is Cooperative Spectrum Sensing [15]. Cooperative Spectrum Sensing is based on combining the sensing results of multiple cognitive radio nodes to reach the final decision. By merging the local observations of different secondary users, we are exploiting the spatial diversity of independently fading signals, and thus we are enhancing our probability of successful detection.

The IEEE 802.22 is an example of network architecture based on cognitive radios [4]. The IEEE 802.22 is a standard developed for Wireless Regional Area Networks (WRANs) and utilizes UHF/VHF TV bands. The main application of 802.22 is wireless broadband access in rural and remote areas. The base-station of the system manages its own cell and several secondary users allocated into the cell, which are known as consumer premise equipments (CPEs).

In this paper, we will present a review of the cooperative spectrum sensing methods that have been proposed so far. In order to do so, Sect. 2 describes the main features of the local spectrum sensing performed by individual radios; Sect. 3 provides a description of the basic types of data fusion techniques that are used to reach a sensing decision collaboratively; and Sect. 4 discusses the security issues associated with the cooperative sensing process. Then, the paper describes the methods that are devised to allow cognitive radios to perform cooperative sensing securely. These methods are divided into two categories: First, those based on reputations, which are presented in Sect. 5, and those based on cross-correlation, which are described in Sect. 6. Section 7 provides an analysis of the reviewed secure cooperative sensing methods. Finally, Sect. 8 presents the conclusions of the paper and points out future directions.

2 Local Spectrum Sensing

In this section, we will present the methods used by cognitive radios to perform local spectrum sensing. The methods proposed in the literature are based on three different techniques: energy detection, cyclostationary feature detection or matched filter [2].

The first technique, energy detection, is based on measuring the energy received over an observation interval. The received signal on the secondary terminal passes through a bandpass filter and it is integrated over the time of observation. The output signal is the test statistic and is compared with a threshold. This method cannot discriminate between the primary signal and noise, and hence makes it difficult to set the threshold used for primary user detection, specially at low SNR. However, energy detectors are widely used because of their simplicity.

The second technique, cyclostationary feature detection, takes advantage of the fact that most of the primary user signals have built-in periodicities. Thus, this embedded redundancy can be used for detection of cyclostationary signals in a background of noise using a spectral correlation function. This method is free of noise interference. However this method requires long observation times.

The third method is based on using a matched filter, and it provides an optimal detection technique when the cognitive radio has a priori knowledge of the primary user signal. The match filter detection is based on correlating the known primary signal with the observed signal. The problem of this method is that it is difficult to have an a priori knowledge of the primary signal. The matched filter detection requires short time for sensing, even though its complexity is high when operating with different types of primary user systems.

From these three techniques, the one most frequently adopted is energy detection. The test statistic of the energy detection is equivalent to an estimation of the average received signal strength (RSS). Energy detection is the test of two hypotheses: H_0, which is the null hypothesis and represents the absence of a primary user, and H_1 which is the alternative hypothesis and represents that there exist some primary user signal. Under H_0, the received data at the secondary user is noise alone. Under H_1, the data is the signal transmitted by primary user plus noise.

3 Cooperative Sensing Techniques

In this section, we will explore the different methods proposed in the literature to date to implement cooperative sensing.

First of all, we can find methods based on a distributed or a centralized approach [6]. In a distributed approach, all secondary nodes exchange their sensing results and then each node combines the results of its neighbors to make the final decision individually [26]. On the other hand, centralized methods use a base station or fusion center that collects the results of all secondary users and executes the data fusion to reach the final decision. The recent work on cooperative sensing has generally adopted the centralized approach, due to its greater simplicity. In particular, the secure cooperative sensing proposals that we analyze in this paper have a centralized architecture, with a fusion center that performs the data fusion.

As shown in Fig. 1, a cognitive radio network is composed of a group of secondary users which may suffer from shadowing and multipath fading. Each secondary user performs spectrum sensing and reports its results to the fusion center. Upon receiving the sensing results from all secondary users, the fusion center integrates the results (and optionally its own measurements) to reach the final decision.

Cooperative sensing techniques can also be grouped according to which kind of information is forwarded to the fusion center. In soft-decision schemes, cognitive radios exchange their test statistics calculated from their local observations. On the other hand, hard-decision schemes only exchange their individual 1-bit decisions. Before exploring these two approaches in detail, we will describe two parameters that are associated with the performance of the data fusion process.

The first parameter is the probability of detection, which is the probability of successful detection of the primary user signal. This probability indicates how well interfering with primary users is avoided. The second parameter is the probability of false alarm, which represents the probability of the sensor detecting a primary signal when in fact it is absent. A high level of protection of the primary signal is reached when the probability of detection is

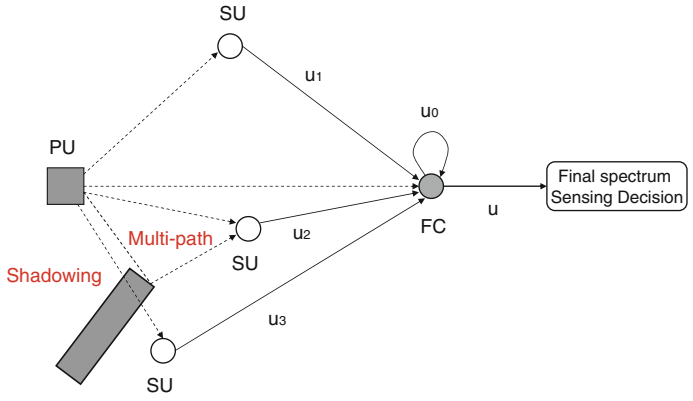

Fig. 1 Modeling cooperative spectrum sensing network

high. On the other hand, the lower the probability of false alarm is, the better the channel is used when it is available.

In the following sections, we will see the relation of these parameters with the soft-decision and the hard-decision schemes.

3.1 Soft-decision Combining Data Fusion Schemes

In soft-combining algorithms, nodes deliver their measured energies to the fusion center, providing high level of information, but increasing the volume of communication data.

To combine the observed energy, algorithms such as Maximal Ratio Combining (MRC) or Equal Gain Combining (EGC) can be adopted [12]. In both cases, the observed energies from N cooperative users are scaled by weight factor and added up. The decision statistic is the result of the weighted sum and is given by

$$Y = \sum_{i=1}^{N} w_i Y_i$$

where Y_j is the observed energy of the ith user and w_i denotes the weight factor corresponding to the ith user.

The resulting decision statistic is compared to a decision threshold T to decide between H_1 (the channel is occupied) and H_0 (the channel is idle)

$$\begin{cases} Y > T \Rightarrow accept\ H_1 \\ Y < T \Rightarrow accept\ H_0 \end{cases}$$

The threshold is defined so as to achieve the desired probability of false alarm or miss detection.

The difference between MRC and EGC schemes is the evaluation of the weights:

– MRC soft combination scheme defines weight coefficients as

$$w_{MRCi} = \frac{\gamma_i}{\sqrt{\sum_{k=1}^{N} \gamma_k^2}}, \quad 1 \leq i \leq N$$

where γ_i represents the instantaneous SNR of the ith cognitive radio user. MRC obtains the normalized weight assigned to each node. Nodes with strong signals are further ampli-

fied, while weak signals are attenuated. Despite the optimal performance of this scheme, it is rarely used because it requires an estimation of the channel gains.

– On the other hand, the weights of EGC soft combination scheme are calculated as

$$w_{EGCi} = \frac{1}{\sqrt{N}}, \quad 1 \leq i \leq N.$$

Sensors have identical assigned weights which depend on the number of cooperative users N. EGC is a near-optimal scheme and does not require channel estimation.

3.2 Hard-decision Combining Data Fusion Schemes

When employing hard combining algorithms, the final decision is reached by taking only into consideration the individual decisions reported by each cognitive radio. The main advantage of this method is the reduction of the communication overhead.

Decision Fusion [22]: The fusion center adds up all local reports and compares the outcome with a threshold in order to decide whether there is a primary signal present or not. This method is the simplest one. Depending on the threshold value, we can have different variants:

A. OR Rule: declares signal presence when at least one user reports that the channel is occupied. The threshold value is 1.
B. Majority Rule: declares signal presence when more than a half of the secondary users declare that the channel is occupied.
C. AND Rule: the decision threshold is the total number of reporting users. This implies that all users must report that the channel is occupied in order for the final decision to be occupied.

3.3 Data Fusion Schemes Allowing for Soft and Hard-decision

In this section, we describe four data fusion mechanisms which enable both hard and soft decision approaches. In order to simplify the explanations, we will introduce some notation first: u is the final sensing decision, and u_i is the sensing result of the ith secondary user. $P(u_i \mid H_0)$ is the a priory probability of u_i when u is zero, and $P(u_i \mid H_1)$ is the a priory probability of u_i when u is one.

Bayesian Detection [21]: This method is based on calculating the cost of the decisions taken by the secondary users. All possible decisions are considered: $u = 0$ when the band is occupied, $u = 1$ when the band is free, $u = 0$ when the band is free, and $u = 1$ when the band is occupied. In the first two cases, the final decision is incorrect, and thus a high cost is associated with these decisions. In the last two cases, the final decision is correct, and thus the associated cost is zero. The overall cost is the sum of the four costs weighted by the probabilities of the corresponding cases. The Bayesian detection is based on calculating the likelihood ratio test [21] and using the overall cost as the threshold. This test can be represented by the following expression:

$$\prod_i \frac{p(u_i \mid H_1)}{p(u_i \mid H_0)} \underset{H_0}{\overset{H_1}{>}} \frac{P_0 (C_{10} - C_{00})}{P_1 (C_{01} - C_{11})}$$

where the a priori probabilities of both hypotheses (H_0 and H_1) are represented by P_0 and P_1, respectively. The main problem of this method is that it requires these a priori probabilities to be known in advance.

Neyman–Pearson Detection [21]: The objective of the Neyman–Pearson test is to guarantee a target false alarm probability while minimizing the miss detection probability or vice versa. This method is based on calculating the likelihood ratio test and comparing the result with a threshold, as shown in the following expression:

$$\prod_i \frac{p\,(u_i \mid H_1)}{p\,(u_i \mid H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda$$

The threshold is calculated from the predefined probabilities of false alarm or miss detection. Unfortunately, in cognitive radio networks where the signal reception conditions are different for each node, thresholds cannot be obtained analytically and their numerical evaluation is an NP-complete problem. In contrast to Bayesian, this method does not require the a priori probabilities of the testing hypotheses. However, it still requires the knowledge of a priori probabilities of u_i's when u is zero or one.

Sequential Probability Ratio Test [21]: This method is based on performing several sensing rounds so that the final decision is taken after merging a variable number of sensing results. The protocol assumes that the number of sensing results can be increased and adjusted as necessary, so it guarantees both a bounded false alarm probability, P_{01}, and a bounded miss detection probability, P_{10}. This sequential detection scheme applies the likelihood ratio test as follows:

$$S_n = \prod_{i=0}^{n} \frac{p\,(u_i \mid H_1)}{p\,(u_i \mid H_0)}\,,$$

where n is the number of samples and can be different from the total number of secondary users. The fusion center decides whether or not the band is occupied based on the following conditions:

$$\begin{cases} S_n \geq \eta_1 & \Rightarrow \quad accept\ H_1 \\ S_n \leq \eta_0 & \Rightarrow \quad accept\ H_0 \\ \eta_0 < S_n < \eta_1 & \Rightarrow take\ another\ observation \end{cases}$$

Threshold values η_1 and η_0 are calculated as follows:

$$\eta_0 = \frac{1 - P_{01}}{P_{10}} \quad \text{and} \quad \eta_1 = \frac{P_{01}}{1 - P_{10}}.$$

Dempster-Shafer Evidence Theory [20]: Dempster-Shafer (DS) is an alternative model to the traditional Bayesian probabilistic theory for the mathematical representation of uncertainty. It offers a way to combine evidence from multiple observers without the need to know about a priori or conditional probabilities as in the likelihood ratio test approaches. However, it needs to determine the initial estimates of nodes' trustworthiness.

DS theory defines a set of hypothesis $A \in \Theta$ for which evidence can be provided, and a density function m, called the Basic Probability Assignment (BPA), that represents the belief that one is willing to commit exactly to A, given a certain piece of evidence. BPA fulfills two conditions: $m(\emptyset) = 0$ and $\sum_{A \subset \Theta} m(A) = 1$.

BPAs from different information sources can be combined with Dempster's orthogonal rule to get a new joint distribution. The compound BPA can be calculated as follows:

$$\begin{cases} m(C) = \frac{1}{1-k} \sum\limits_{\substack{i,j \\ A_i \cap B_j = C}} m_1(A_i) m_2(B_j) \\ m(\emptyset) = 0 \end{cases}$$

where $k = \sum\limits_{\substack{i,j \\ A_i \cap B_j = \emptyset}} m_1(A_i) m_2(B_j)$. The coefficient $\frac{1}{1-k}$ is called normalization factor and is used to avoid non zero mass from being assigned to the empty set after combination. It has the effect of attributing any mass associated with conflict to the null set.

The combination of m is only possible if m_1 and m_2 are two BPAs induced from two independent evidence sources, and the following condition is met:

$$\sum_{\substack{i,j \\ A_i \cap B_j = \emptyset}} m_1(A_i) m_2(B_j) < 1$$

The decision strategy of DS evidence theory is supported by BPAs. The hypothesis that maximizes the density function m is selected.

4 Security Issues

Cooperative sensing can significantly improve the accuracy of individual sensing approaches [15]. However, the performance of the collaborative approach can also be reduced by the following problems:

Firstly, nodes may fail to detect the primary signal because they suffer from severe fading, or simply because they use malfunctioning sensing terminals.

Secondly, nodes may send false sensing information to the fusion center in order to alter the final decision. This problem is known as the spectrum sensing data falsification (SSDF) attack. In this case, secondary users intentionally manipulate the sensing reports, thus leading the data fusion algorithms to make the wrong decision. A survey of the effects of this kind of attacks can be found in [16].

SSDF attackers can be classified according to the way they send false sensing reports. This classification leads to three different types of attackers:

- The first type of attacker is the one who always reports the same sensing result. An Always-Yes attacker always declares that the primary user is active. On the other hand, an Always-No attacker always reports an absence of primary signal.
- The second type of attacker is the one who always reports the opposite of its local spectrum sensing result.
- The third type is the one who occasionally reports extreme false values. Thus, they mislead the system once in a while, but they behave correctly during the rest of the time.

As a result of all these problems, cooperative data fusion techniques must implement countermeasures to mitigate the risk of SSDF attacks and the effects of false reports sent by malfunctioning devices unintentionally. The solutions proposed for these problems are based on the following strategies:

- *Reputations*: the fusion center keeps track of the reporting history of a sensing terminal. Nodes that usually send false reports have low reputation and their sensing data have low or no impact on the final sensing decision.

– *Cross-correlation*: despite the heterogeneity of devices, node locations, fadings, etc., the SNR reported from different sensing terminals must be consistent. This fact can be exploited to identify outliers and discard false reports.

In the next sections, we will review the main proposals based on both reputation and cross-correlation schemes.

5 Reputation-based Algorithms of Decision

Reputation-based algorithms detect malicious secondary users from the accumulation of failures on their sensing reports. Figure 2 shows the overall protocol scheme. In each sensing round, nodes sense the spectrum and compose a report with information about the received power or their decision on the channel occupancy. Reports are sent to the fusion center, which processes them to achieve a final decision. In order to counteract the impact of malicious users' reports, different operations can be applied to the sensing decision procedure:

1. *Pre-filtering*: Nodes whose sensing results significantly deviate from that of others, or nodes with low reputation, are filtered out from the data fusion module. Only consistent reports remain in order to make a more reliable decision.
2. *Data Fusion*: A data fusion rule is applied to make a global decision about the presence of primary users in the sensed spectrum band. User's contributions to the final decision can be weighted based on their reputation parameters.
3. *Reputation Update*: Reputation values need to be adjusted for the next sensing round. Update of node's reputation is based on either the global decision or others node's reports. Several computational reputation models can be applied.

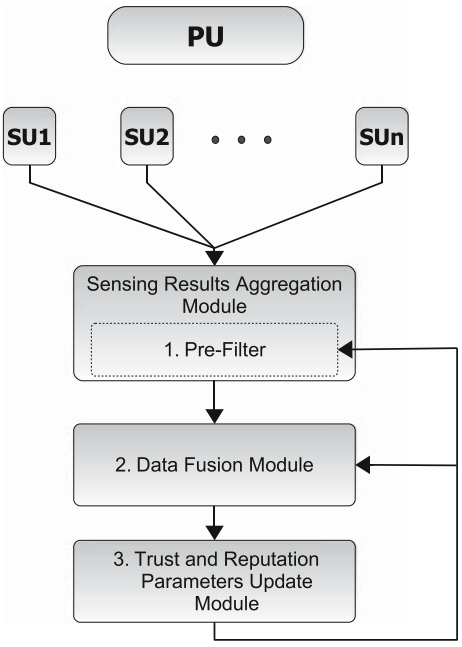

Fig. 2 Overall architecture of the trust and reputation model

A cooperative sensing scheme is qualified by its Data Fusion method. Therefore, the data fusion method defines the main features of the Pre-filtering and Reputation Update modules. The data fusion module incorporates weights on the conventional data fusion approaches. Weights are based on trust or reputation of nodes. On each sensing process round, trust and reputation parameters should be updated by means of a computational reputation model. Reputation update makes nodes reputation accurate and improves robustness of scheme.

5.1 Weighted Data Fusion Techniques

In a weighted collaborative scheme each node has its own weight in the data fusion process. Weights represent the behaviour of past sensing for each secondary node. They also give different node's contributions on the final decision. When scheme incorporates pre-filtering only nodes that pass through the filter are authorized to participate in the decision process.

A Trust-Weighted Aggregation Scheme: Qin et al. [19] introduce the notion of self-confidence and trust. Self-confidence is a rate supplied by a sensing terminal of its own confidence on the accuracy of its sensing results. Trust is a measure of reputation, and represents the historical accuracy of terminals' sensing reports. Specifically, the trust factor of the scheme is computed using the generic de-centralized reputation evaluation model BRS (Beta Reputation System) [9] with the particularity that each user has a different score for each possible sensing context (e.g. geographical location, sensing band, etc.). Besides, a forgetting factor under each context is used to gradually decrease the influence of older ratings. Thus, the trust factor τ_{ip} of a user i in the context (or sensing band) p, can be computed as follows:

$$\tau_{ip} = \frac{\sum_{j=0}^{N-1} \rho_{ip}^{N-1-j} \alpha_{jip}}{\sum_{j=0}^{N-1} \rho_{ip}^{N-1-j} (\alpha_{jip} + \beta_{jip})}$$

where N is the accumulated number of ratings that user i has been given in the past, $\rho_{ip} (0 \leq \rho_{ip} \leq 1)$ is the forgetting factor of i in the context p, α_{jip} is the jth positive behavior score of i in the context p, and β_{jip} is the jth negative behavior score of i in the context p.

The scheme defines a pre-filter that discards nodes which trust factor is below a threshold. Then, the contributions of secondary users are merged using a majority fusion rule approach that weights nodes' decisions based on their trust factor.

In the proposed system the fusion center is itself a sensing node. The fusion center as well as the secondary nodes of the network sense the spectrum and rate their binary sensing decisions based on the received power and the channel gain between the transmitter and themselves. In order to take a final decision, the fusion center complements its decision with data from other sensors. The more it trusts in its own decision, the less weight the secondary users have. The aggregated sensing result R_p for the particular context p is calculated as:

$$R_p = \theta \Gamma_{fp} + (1 - \theta) \frac{\sum_{i=1}^{M} \tau_{ip} \Gamma_{ip}}{\sum_{i=1}^{M} \tau_{ip}}$$

where θ is the confidence level of the fusion center, Γ_{fp} is the sensing result of the fusion center in the context p, Γ_{ip} is the sensing result of user i in the context p, τ_{ip} is the trust factor of user i in the context p, and M is the number of users whose sensing results have passed the pre-filter.

After the final decision is taken, nodes' trust factors are updated. Nodes that agree with the overall decision are added a point to its positive behavior score, while those who disagree are

added a point to its negative score. Besides, nodes whose sensing result has caused a complaint from a primary user are punished with N negative points, being N the total number of ratings that a user has been given in the past.

A Weighted Sequential Probability Ratio Test (WSPRT): Chen et al. present a new weighted fusion approach [3] based on the Sequential Probability Ratio Test (SPRT). The a priori probabilities of the likelihood ratio test are raised to the power of a weight w, which is a function of the node's trust factor. The decision variable is

$$W_n = \prod_{i=0}^{n} \left(\frac{P[u_i|H_1]}{P[u_i|H_0]} \right)^{w_i}$$

with $w_i \in [0, 1]$ the weight factor of user i.

The reputation update module evaluates the consistency of nodes' reports with respect to the overall decision over a past period. If a node i has agreed with the final decision, its trust factor r_i is incremented by one; otherwise it is decremented by one. Based on the new computed trust factor, the weight of a node w_i is obtained using the following function:

$$w_i = f(r_i) = \begin{cases} 0, & r_i \leq -g \\ \frac{r_i+g}{max(r_i)+g}, & r_i > -g \end{cases}$$

The variable $g(< 0)$ is used to obviate penalizations in case of short-term randomness or temporary interferences, and to avoid that some punctual incorrect reports negatively effect the system's performance.

This scheme presents a trade-off between data collection overhead and robust performance. As the primary signal strength or nodes' density decreases, the average number of samples required to keep an accurate performance raises.

Like other algorithms based on the likelihood ration test, WSPRT requires the a priori probabilities of nodes' decisions under the hypothesis of the test. The authors introduce a procedure to calculate them based on the physical location of the nodes and the path loss of the environment.

A Weighted Data Fusion Scheme with Confidence Vector: Lim et al. also deal with reputation and self-confidence factors on node's reports [11] like the trust-weighted aggregation scheme of Qin et al. [19].

Nodes rate the confidence they have with their binary sensing results using a real number between 0 and 1, where 0 means no confidence and 1 stands for complete assurance. Then, they reassign the confidence value with a positive sign if their sensing decision is that the spectrum band is occupied, and with a negative sign otherwise. The signed confidence factor is sent to the fusion center as a sensing report.

The fusion center merges nodes' sensing reports using a weighted majority fusion rule that gives a higher contribution to nodes with a high reputation. The resultant final decision $u(n)$ is computed as follows:

$$u(n) = \begin{cases} 1, & \sum_i c_i w_i \geq 0 \\ 0, & \sum_i c_i w_i < 0 \end{cases}$$

with c_i the confidence factor of user i, and w_i the trust factor of user i.

Trust factors are timely updated and represent the successful detection ratio of a node with respect to the overall decision in its past sensing history. Thus, higher weights are assigned to reliable nodes which make correct local detections.

A Weighted-Collaborative Scheme: In contrast to the protocols seen so far, Huang et al. first considered a weighted collaborative scheme over soft-decision [7]. They consider nodes evaluate the spectrum using an energy detection model. Then data is merged through a product fusion rule adjusting user's contributions with a weight factor. Weights represent the reputation of a node. Reputation decreases when a node is under deep fading thereby reducing node's influence on the final decision. The weight factor assigned to the ith user in the nth sensing process is defined as

$$W_i(n+1) = W_i(n) P_{d\,i}(n) / \overline{W(n) P_d(n)}$$

where,

$$\overline{W(n) P_d(n)} = \frac{1}{N} \sum_{i=1}^{N} W_i(n) P_{d\,i}(n)$$

$P_{d\,i}$ is the detection probability of the ith user, which is based on the node's received SNR level, and N is the total number of secondary users. Authors assume the environmental conditions of a site are known and thus the probability distribution functions can be obtained to calculate detection probabilities.

Matsui et al. designed a similar weighted cooperative scheme [13]. The difference is that the reputation is a value inversely proportional to the distance between the fusion center and the cognitive radio node. The further the node is, the lower the reputation becomes. They assume that the fusion center exactly knows the location of secondary users and system stations, which are stationary.

An Average Combination Scheme: Kaligineedi et al. apply a weighted collaborative data fusion over a soft-decision model [10].

Nodes sense the spectrum using energy detectors and send the received energy level to the fusion center. The scheme first applies a pre-filter that discards the extreme outliers of the acquired data distribution, i.e. the reports which are numerically distant from the rest of the data. The thresholds are computed as follows:

$$b_l(k) = b_1(k) + 3b_{iqr}(k)$$
$$b_u(k) = b_3(k) + 3b_{iqr}(k)$$

The lower bound, $b_l(k)$, is a linear combination of the value in the cut-off position of the first quartile, $b_1(k)$, and the interquartile range value, $b_{iqr}(k)$. The interquartile range value is the difference between the value in the cut-off position of third quartile and the value in the cut-off position of first quartile. Then, the upper bound, $b_u(k)$, is computed as a linear combination of the value in the cut-off position of third quartile, $b_3(k)$, and the interquartile range value.

After pre-filtering, the fusion center combines the remaining sensing reports using a weighted majority fusion rule that gives a higher contribution to nodes with a good reputation, i.e., nodes with a high trust factor. The final decision is computed as follows:

$$u(n) = \begin{cases} 1, & \sum_i \lambda_i(k) e_i(k) \geq e_T \\ 0, & \sum_i \lambda_i(k) e_i(k) < e_T \end{cases}$$

where $\lambda_i(k)$ is the trust factor of user i at instant k, $e_i(k)$ is the energy value reported by user i at the instant k, and e_T is the threshold level. The threshold is obtained empirically by Monte Carlo simulations to meet the required probability of detection.

Finally, the scheme updates nodes' trust factors. The trust factor gives a measure of reliability of a particular user. It is based on the past and present sensing data sent by the user as well as the sensing data sent by other users. To evaluate the trust factors, the fusion center computes the nodes' instant trust penalties d_i at each sensing iteration k using the following formula:

$$d_i(k) = \frac{|e_i(k) - \mu(k)|}{\sigma(k)}$$

where $\mu(k)$ and $\sigma(k)$ are, respectively, the mean and the variance of the sensing data that has passed the initial filter of the protocol at the instant k. Then, instant trust penalties are summed over a certain period of time L to obtain $D_i(k)$:

$$D_i(k) = \sum_{k'=k-L+1}^{k} d_i(k')$$

Comparing the $D_i(k)$ values of different users would give a clear idea of which sensing nodes are deviating.

The authors propose two approaches for computing nodes' trust factors based on $D_i(k)$. The first one is by identification of mild outliers among $D(k)$ in a analogous way to what the initial filtering module does. A node's trust factor is set to one if its $D_i(k)$ lies between the defined thresholds; otherwise, the assigned trust factor is zero. The second approach assigns trust factors such that they are exponentially decreasing according to the distance from $D_i(k)$ to the median $m_D(k)$: $\lambda_i(k) = e^{-|m_D(k)-D_i(k)|}$

Trust factors are a mean to identify malicious nodes. Depending on the characteristics of the environment the time frame L used to compute the trust factors has to be adjusted. Small time frame values are useful for identifying nodes which behave maliciously over short periods of time, while large values help identifying long-term attacks.

Multiple Malicious User Detection by Onion-Peeling Approach: Focusing on performing an accurate pre-filtering, Wang et al. present a soft-decision reporting scheme [23] that is robust against malicious users. The protocol can be used with any of the existing collaborative data fusion algorithms, either based on hard or soft combining. The contribution of the authors is in the design of a powerful pre-filter based on the users' report histories.

The authors define an heuristic approach to iteratively identify malicious nodes, batch by batch. Initially all nodes are presumed to be honest. For every node, the fusion center computes a suspicious level, i.e., the *a posteriori* probability that it is an attacker. To calculate a node's suspicious level, the scheme needs to know both the honest node and malicious node report probabilities. These probabilities are estimated assuming that the fusion center knows the position of the nodes and the attackers' policy. Moreover, the primary user is assumed to be static.

When the suspicious level of a node goes beyond a threshold it is discarded from the final decision process and moved into a malicious user set. After applying this filtering procedure to all the nodes, the way to calculate the suspicious level is updated. The protocol starts a new filtering iteration, in which new malicious users will be identified. The process is repeated until no more malicious nodes can be found. Eventually the reports from honest users are fused to make the final decision.

A Dempster-Shafer Theory of Evidence Data Fusion Scheme: Qihang et al. designed a soft-decision data fusion scheme [18] that uses the DS theory of evidence. They estimate the nodes' trustworthiness from their channel condition and their distance to the primary node. Specifically, when local sensing is performed with an energy detection model, the trustworthiness is computed from the cumulated power of their received signal. Based of these parameters, the commitment of a node to a certain hypothesis is established in the form of BPAs. Finally, the Fusion Center combines the BPAs of all individual nodes using the Dempster's orthogonal rule. It selects the hypothesis associated with the mass function whose credibility is higher:

$$H_1 : m(H_1) < m(H_0)$$
$$H_0 : m(H_0) < m(H_1)$$

Using the same basic DS scheme as [18], in [17] Nguyen-Thanh and Koo estimate the DS hypothesis applying the Hubber's robust statistics method [8]. Robust statistics are more resistant to wireless network failures and attacks than classical statistical estimators such as mean and standard deviation. Moreover, they can be obtained using the available past sensing node's received power data; no other information about the context is required.

Hence, the Nguyen-Thanh and Koo scheme first estimates the distribution of both hypotheses H_0 and H_1 of each user and filters the users with abnormal statistics data. The BPA values of the remaining users are combined using the Demptser's combining rule. The novelty introduced by Nguyen-Thanh and Koo in the data fusion process is that they weight the nodes' BPAs using a normalized trust factor. The fusion center maintains four counters to evaluate the reliability of each network node i: $n_{00_i}(n)$, $n_{01_i}(n)$, $n_{10_i}(n)$, $n_{11_i}(n)$, where $n_{ab_i}(n)$ means the number of times the local decision of user i is a and the global one is b over n decisions. Then, the trust factor of a node is:

$$r_i = \frac{n_{11_i}(n)}{n_{11_i}(n) + n_{10_i}(n)} \cdot \frac{n_{00_i}(n)}{n_{00_i}(n) + n_{01_i}(n)}$$

and the BPAs of each user are adjusted with a weight w_i as follows:

$$m_i'(H) = \frac{r_i(n)}{max_i(r_i(n))} \cdot m_i(H)$$

Simulation results indicate the scheme presents a good performance even when 70% of users are malicious or affected by fading or deep shadowing.

6 Cross-correlation Based Algorithms of Decision

In order to mitigate the effect of malicious users, cross-correlation based algorithms gather sensing nodes into sets according to the similarity of some of their sensing characteristics such as location, fading environment, etc. The data fusion process in usually performed in several steps. First, reports from nodes in a set are merged to obtain an overall group report. Then, group reports are combined to get the final decision.

The overall architecture of cross-correlation based schemes is the same than those based in reputations (see Fig. 2). Nevertheless, there is a difference in the order in which operations

are performed. In cross-correlation based schemes, the calibration of the users' weights is made before executing the data fusion. This is due in these schemes, users are weight according to the deviation of their sensing reports compared with the others, and no information about which is the final decision is required. On the contrary, reputation based schemes need to know if the local decision of a user agrees with with final one to be able to update the user's weight in the system.

Next, three different data fusion schemes are revised. They group nodes according different features such as the received signal strength or the location.

A Decision Fusion Scheme by Hierarchy Configuration: Wang et al. propose to classify nodes according to their SNR level and then merge node's reports using a hierarchal rule [24]. The scheme can be both employed in a decentralized and a centralized (with a fusion center) cognitive radio network. However, since the performance of the first approach is more limited, we will focus on the decentralized configuration.

Users sense the spectrum through an energy detector and estimate the received SNR from the expected value of the signal energy under H_0 and H_1 hypotheses. Users send the SNR to the fusion center, which analyzes them and creates groups of nodes that have a similar SNR value. The data fusion is started merging the reports of the group whose SNR is the lowest. The combining rule used in this first fusion level is the majority rule since it is nearly optimal when the sensing capabilities of nodes are very similar. In this case, the detection and false alarm probabilities of the nodes are approximately equal.

Then, the result of the lowest SNR group is inserted in the immediately above group. This hierarchical process is performed throughout all the groups. The data fusion rule employed in each case is the OR rule if the group has up to two values, and the majority rule otherwise. Each group set the threshold of the majority rule according to its members reports and the received value from the lower group.

A Double Thresholds based Cooperative Spectrum Sensing Scheme: Xu et al. propose a double-threshold energy detector combined with a two-level decision fusion rule in order to counteract both Always-Yes and Always-No attacks [25].

The scheme defines two thresholds that are employed during the local sensing to classify the nodes into three groups, namely $G1$, $G2$ and $G3$; depending on the energy level they receive from the analyzed spectrum band, they are set in a group or another. Nodes in $G1$ and $G2$ groups are meant to send a binary sensing report to the fusion center, while $G3$ members send their observed multi-bit energy value. Thus, the local decision of ith user can be expressed as:

$$d_i = \begin{cases} 1, & \text{if } y_i > \lambda_2; \quad (u_i \in G1) \\ y_i, & \text{if } \lambda_1 \leq y_i \leq \lambda_2; \quad (u_i \in G3) \\ 0, & \text{if } y_i < \lambda_1; \quad (u_i \in G2) \end{cases}$$

with y_i the received energy by node i.

The fusion center starts the data fusion process combining the energy values from $G3$ nodes using either the Maximal Ratio Combining (MRC) or Equal Gain Combining (EGC) rule. The output decision of $G3$ is then mixed with the binary decisions from $G1$ and $G2$ using a revised version of the conventional OR, AND or Majority fusion rules, to get a final decision D.

$$D = \begin{cases} 1, \begin{cases} \text{If } \sum_{i=1}^{N_1+N_2+1} d_i \geq 1 + num & (a) \\ \text{If } \sum_{i=1}^{N_1+N_2+1} d_i = N_1 + N_2 + 1 - num & (b) \\ \text{If } \sum_{i=1}^{N_1+N_2+1} d_i \geq \frac{1}{2}(N_1 + N_2 + 1 + num) & (c) \end{cases} \\ 0, \text{ Otherwise} \end{cases}$$

where *num* represents the number of untrusted users and it is the minimum between N_1 and N_2; N_1 and N_2 are respectively the number of users in $G1$ and $G2$. All users in $G3$ are considered trusted. In the equation, a decision of $D = 1$ denotes the primary user is present, and $D = 0$ means primary user is absent. Besides, the rule described by equation (a) is the Revised OR rule, (b) is the Revised AND rule and (c) is the Revised Majority rule.

An Attack-Tolerant Distributed Sensing Protocol (ADSP): Min et al. introduce a novel cluster-based distributed sensing that exploits shadow fading correlation for the detection of malfunctioning sensors or malicious nodes [14]. The scheme is based on local energy detection and employs the fact that nearby nodes are subject to similar environmental conditions, and so, their received signal strengths must be alike.

Nodes sense the spectrum and report their energy detector's output as well as their location to the fusion center. The fusion center first groups nodes in close proximity into a cluster and performs a pre-filtering that consists on making a cross-correlation between the reports of all available pair of nodes in a cluster. For each node, the fusion center counts the number of cross-correlations which output lies outside the thresholds. Thresholds are set differently for each pair of neighboring nodes as they depend on nodes' relative distance and measured energy. The final value of the counter provides a measure to filter abnormal nodes using the following rule:

$$IsNormal_i = \begin{cases} true; & counter_i > \beta \cdot |N_i| \\ false; & counter_i \leq \beta \cdot |N_i| \end{cases}$$

with $\beta \in [0, 1]$, and N_i the set of neighbors of node i (the members of its cluster)

After filtering abnormal nodes, the fusion center merges the remaining sensing reports using a variation of the Equal Gain Combining (EGC) rule named Weighted Gain Combining (WGC). The authors propose to weight the nodes' sensing reports using a factor that states the statistical significance of the report in terms of its correlation with the others. Thus, the protocol can further improves its attack-tolerance. The weights in WGC are defined as:

$$w_i = \frac{\sum_{j \in N_v(i)} w_{ij}}{|N_v(i)|}, \quad \text{where } w_{ij} = 1 - 2|F_{R_i|R_j}(r_i|rj) - 0.5|$$

with $N_v(i)$ the set of valid neighbors of node i, and $F_{R_i|R_j}(r_i|rj)$ the cumulative distribution function of node i's report (r_i) given node j's report (r_j).

To obtain the final decision, the result of the WGC is compared with a threshold which is derived from desired probability of false alarm. As with other fusion rules, there is a trade-off in determining the value of the threshold; the lower the probability of false alarm, the higher the mis-detection rate.

7 Analysis of Secure Data Fusion Schemes

The aim of this section is to analyze and compare the performance and the limitations of cooperative sensing protocols. A comparison of the secure cooperative sensing protocols discussed in this paper is presented in Table 1. The following paragraphs describe the information shown in this table.

The first two columns contain the type of protocol (reputation or cross-correlation based) and the method's name.

The third column (Required information from the CR network) points out the information required to carry out the data fusion process. Some schemes assume that the system is able to provide this information, and others require additional systems to provide the necessary data (such as positioning devices).

The 'Fusion Approach' column indicates whether the protocol is based on hard-decision or soft-decision combining.

The 'Pre-filter' column shows which methods apply pre-filtering over the received reports and what parameter is used to discard the reports.

The 'Weighted Data Fusion' column indicates whether the data fusion method scales the nodes' contributions with a weight factor, and points out what is the basic algorithm used for data fusion. As the column shows, some protocols apply new fusion techniques to scale the different contributions.

The 'Cost overhead' column contains the potential overhead in the response time or the amount of data transmissions resulting from the fact that the protocol requires a high number of secondary users or iterations.

The 'Rob.' column provides an evaluation of the protocols' robustness. Because different types of malicious users can be involved in the attack to a cooperative sensing process, we can define different levels of robustness for each protocol. Schemes that provide high protection against multiple types of attacks and under a high number of attackers are given the maximum robustness grade. On the other hand, schemes that are robust only under some assumptions or a low number of attackers are given a low robustness grade.

The 'Adap.' column provides an evaluation of the protocols' adaptability. The adaptability depends on whether the protocols are able to adapt dynamically to system parameter changes or, instead, they are not flexible against context changes and require different configurations depending on the situation. In order to obtain the robustness and adaptability measures, simulations of the different protocols have been used.

The '802.22 standard' column indicates whether the protocol complies with the IEEE 802.22 standard. The IEEE 802.22 WRAN standard specifies a maximum false alarm probability of 10% and a minimum detection probability of 90%. The required probabilities must be reached with a SNR of -22 dB. Few of the studied schemes are consistent with the specifications of the IEEE 802.22 standard.

Now that we have described the different parameters used in our comparison, we will discuss the most relevant features of the protocols explored in this paper.

Two of the methods reviewed provide a high level of protection against malicious users: the Onion-peeling approach [23] and the D-S theory of evidence data fusion [17]. Both of them are soft-combining schemes and demonstrate high adaptability. These schemes perform efficiently both when nodes dynamically change their attack behavior (their reputations change dynamically) and when nodes occasionally report extreme false values (their reputations recovers rapidly). However, their implementation is complex and leads to an overhead in decision time because they are iterative. As the number of iterations increases, the

Table 1 Comparison of schemes for robust cooperative spectrum sensing

Class	Method	Required information from the CR network	Fusion approach	Pre-filter	Weighted data fusion	Cost overhead	Rob.	Adap.	802.22 Standard
Reputation-based algorithms	Trust-weighted aggregation scheme	Confidence levels and history of successful decisions	Hard-decision	Yes, based on reputation scores	Yes, majority rule	No	+	−	NA
	WSPRT	SU's locations, history of successful decisions and tolerated false alarm and miss detection probabilities	Hard-decision	No	Yes, sequential detection	High, trade-off with good performance	+	+	NA
	Data fusion with weighted confidence vector	Confidence vectors and history of successful decisions	Hard-decision	No	Yes, majority rule	Low	−−	−	Yes
	WCS	Signal and noise probability distribution function or SU's locations	Soft-decision	No	Yes, product fusion rule	Low, 8 users are enough	−−	−	No
	Average combination scheme	History of received energy levels and tolerated false alarm and miss detection probabilities	Soft-decision	Yes, based on deviation from users reports distribution	Yes, majority rule	Low	−	−	Yes (SNR −10 dB)

Table 1 continued

Class	Method	Required information from the CR network	Fusion approach	Pre-filter	Weighted data fusion	Cost overhead	Rob.	Adap.	802.22 Standard
	Onion-peeling approach	SU's locations, path loss model and history of sensed energy	Soft-decision	Yes, based on reputations scores	Proposed approach can be combined with many data fusion scheme	Calculation of a threshold for each sensing round.	++	+	NA
	D-S theory data fusion	History of received power data, channel condition and SU's distances to PU	Soft-decision	Yes, based on users abnormal estimated parameters	Yes,D-S theory of evidence data fusion	Yes, update of robust statistics estimation for each user on every sensing round	++	+	Yes (SNR −10dB), no for Rayleigh fading
Cross-correlation based algorithms	Detection fusion by hierarchy rule	Channel condition, SU's distance to PU and probability of false alarm and detection	Hard-decision	No	No, majority rule with threshold set according to previous group decision	Yes, due to performing serial data fusion with several groups	−−	++	No

Table 1 continued

Class	Method	Required information from the CR network	Fusion approach	Pre-filter	Weighted data fusion	Cost overhead	Rob.	Adap.	802.22 Standard
	Double thresholds based scheme	Attack probabilities of malicious nodes	Soft-decision and hard-decision	No	No, revised decision fusion rules adjusted to nodes partition	Low, local sensing made with two thresholds	−	−	No
	ADSP	SU's locations, cumulative distribution function of received signals and tolerated probability of false alarm	Soft-decision	Yes, based on correlation analysis with nodes on same cluster	Yes, based on EGC adjusts weights to mitigate unfiltered attacks	Low	+	−	NA

++ maximum −− minimum

efficiency of the protocols improves. These schemes show good performance under low SNR levels.

The Onion-Peeling approach [23] used for multiple malicious user detection provides an accurate pre-filtering stage. This scheme uses a sophisticated iterative algorithm to identify malicious nodes. The simulations show that the scheme achieves high probability of detection at low probabilities of false alarm when 30% of the users are malicious and have high attack probability.

The D-S data fusion method [17] provides two separate distributions which allow to make an accurate identification of different types of malicious nodes and to obtain reliable reputations. The protocol yields good results in scenarios with a 50% of malicious users, and considering many different types of attacks. The method used for estimating the parameters provides robust statistics that are based on the sensing reports obtained after a certain number of iterations.

The other protocols studied do not appear so robust, but they are still efficient against malicious users. Trust Weighted Aggregation Scheme, Weighted Sequential Probability Ratio Test and Attack-Tolerant Distributed Sensing Protocol would be in this category. The first and the second are hard-combining schemes, and the third is a soft-combining one.

The Trust weighted aggregation protocol [19] introduces concepts such as the confidence level or the forgetting factor, which contribute to a more accurate data fusion. The confidence level allows users to rate themselves on the reliability of their sensing reports, and it is suitable for filtering users. However, the confidence level has not proven to be useful when secondary users are malicious. By adjusting the protocol parameters, such as the forgetting factor or the threshold, this protocol can be applied to different environments. However, this scheme does not provide dynamic adaptability since the history of behaviors and forgetting factors are specific for each environment and channel.

The Weighted sequential probability ratio test [3] achieves robustness of the data fusion process at the cost of increasing the number of samples from the sensing nodes. This fact produces an overhead in the amount of data communications. This method is also robust under different network conditions by adjusting the number of samples. Additionally, reputations are computed in such a way that they can be easily recovered when nodes make occasional wrong decisions. However, this scheme is complex because it must obtain nodes' locations.

The key feature of the Attack-tolerant distributed sensing protocol [14] is that it groups nodes that are in close proximity. The protocol takes advantage of the nodes' reports correlation and uses it to pre-filter abnormal behaviors. This scheme provides good results even under low SNR environments. However, it is not robust when attacks do not exhibit significant deviations to be detected. In addition, the protocol presents low adaptability because the threshold of the final decision is fixed, since it is based on the tolerated probability of false alarm.

Other protocols, such as Average combination scheme and Double Threshold based scheme, also have low robustness, but they are simple and have low cost overhead.

The Average combination protocol [10] provides a pre-filter to detect attackers whose results deviate from those of other users. The detection technique does not adapt to dynamic changes on attacker's behavior. Besides, the threshold of the final decision is fixed throughout the sensing process. From the simulations carried out, the protocol has proven to be not robust neither under low SNR environments nor when the number of malicious users is higher than 20%.

The Double threshold protocol [25] proposes an energy detector with two thresholds to detect two different types of attacks. As it does not use pre-filtering or weight factors, robust-

ness only depends on the definition of the threshold values. The adaptability of this protocol is low because the threshold values are fixed. Finding accurate thresholds is a difficult task since these depend on the probability of each type of attack.

Finally, some protocols assume that sensing measurements suffer from different fading but their simulations do not consider SSDF attacks. Schemes like a Weighted data fusion scheme with confidence vectors, a Weighted-collaborative scheme or a Decision fusion scheme by hierarchy rule assign different contributions to nodes according to the reliability of their sensing reports.

The Weighted data fusion protocol with confidence vectors [11] makes an accurate final decision introducing confidence vectors and weights into the sensing results. However, the adaptability to new environment conditions is low because the reputation of nodes is computed considering their historic reports. Thus, the adaptation of the scheme depends on the number of previous samples used to calculate the weights.

The Weighted-collaborative protocol [7] introduces weights by assuming fading environments to make an accurate sensing decision. This scheme has low adaptability because the reputation depends on past probabilities of detection. However, this protocol is worse than the Weighted data fusion with confidence vectors protocol because it uses all the previous samples to compute the reputations. Thus, when the environment changes, the reputations have the contribution of the past weights and probabilities of detection. The scheme performance improves when increasing either the number of users or the number of sensing iterations.

The Decision fusion scheme by hierarchy rule [24] proposes a combination of serial and parallel configurations to make the final decision. The SNR levels are taken into account to group the nodes. Thus, this protocol achieves adaptation to new environments rapidly. The abnormalities of the received reports can be detected because they are compared with those from neighboring nodes. However, the implementation of this scheme is complex.

In conclusion, there is no optimal scheme. If robustness is the most important characteristic, then the D-S theory of evidence data fusion scheme provides the highest protection against attacks. On the other hand, if flexibility and dynamic adaptability are more important, then cross-correlation based schemes, and in particular the Detection fusion by hierarchy rule protocol, is the most suitable.

8 Conclusions

Cooperative sensing protocols for cognitive radio networks have been a subject of quite a number of investigations in recent years. Most of these investigations have been motivated by the need to design an efficient and reliable data fusion scheme that can deal with inaccuracies and false reports. To ensure right decisions, protocols based on reputations and cross-correlation issues have been proposed. This paper reviewed the main cooperative sensing protocols that assume the existence of malicious nodes in the network and try to nullify their effects. Different strategies have been presented along with their limitations and advantages. It has been shown that most robust protocols require the knowledge of prior context variables (noise distribution, channel gain, probability of malicious users,…). More research is required along the lines introduced in this review to create a cognitive radio network that can really learn from the environment and improve its sensing accordingly to cope with all the security attacks that threaten the network.

References

1. Akyildiz, I. F., Lee, W. Y., Vuran, M. C., & Mohanty, S. (2006). Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks, 50*(13), 2127–2159.
2. Cabric, D., Mishra, S. M., & Brodersen, R. W. (November, 2004). Implementation issues in spectrum sensing for cognitive radios. In *Conference record of the thirty-eighth asilomar conference on signals, systems and computers* (Vol. 1, pp. 772–776).
3. Chen, R., Park, J.-M., & Bian, K. (April, 2008). Robust distributed spectrum sensing in cognitive radio networks. In *INFOCOM. The 27th conference on computer communications* (pp. 1876–1884). IEEE.
4. Cordeiro, C., Challapali, K., Birru, D., & Sai Shankar, N. (November, 2005). IEEE 802.22: The first worldwide wireless standard based on cognitive radios. In *First IEEE international symposium on new frontiers in dynamic spectrum access networks (DySPAN)* (pp. 328–337).
5. Force, S. P. T. (2002). *Spectrum policy task force report*. Federal Communications Commission ET Docket 02 135.
6. Ganesan, G., & Li, Y. (November, 2005). Cooperative spectrum sensing in cognitive radio networks. In *IEEE international symposium on new frontiers in dynamic spectrum access networks (DySPAN)* (pp. 137–143).
7. Huang, X., Han, N., Zheng, G., Sohn, S., & Kim, J. (August, 2007). Weighted-collaborative spectrum sensing in cognitive radio. In *CHINACOM. Second international conference on communications and networking in China* (pp. 110–114).
8. Huber, P. J., & Ronchetti, E. M. (2009). *Robust statistics*. Oxford: Wiley-Blackwell.
9. Jøsang, A., & Ismail, R. (June, 2002). The beta reputation system. In *Proceedings of the 15th Bled electronic commerce conference* (pp. 324–337). Bled, Slovenia.
10. Kaligineedi, P., Khabbazian, M., & Bhargava, V. K. (May, 2008). Secure cooperative sensing techniques for cognitive radio systems. In *ICC. IEEE international conference on communications* (pp. 3406–3410).
11. Lim, S., Jung, H., & Song, M. S. (August, 2009). Cooperative spectrum sensing for ieee 802.22 wran system. In *Proceedings of 18th internatonal conference on computer communications and networks (ICCCN)* (pp. 1–5).
12. Ma, J., Li, Y. (November, 2007). Soft combination and detection for cooperative spectrum sensing in cognitive radio networks. In *IEEE global telecommunications conference* (pp. 3139–3143).
13. Matsui, M., Shiba, H., Akabane, K., & Uehara, K. (September, 2007). A novel cooperative sensing technique for cognitive radio. In *IEEE 18th international symposium on personal, indoor and mobile radio communications (PIMRC)* (pp. 1–5).
14. Min, A. W., Shin, K. G., & Hu, X. (October, 2009). Attack-tolerant distributed sensing for dynamic spectrum access networks. In *IEEE international conference on network protocols (ICNP)* (pp. 294–303).
15. Mishra, S. M., Sahai, A., & Brodersen, R. W. (2006). Cooperative sensing among cognitive radios. In *Proceedings of the IEEE international conference on communications (ICC)*. Citeseer.
16. Mishra, S. M., Sahai, A., & Brodersen, R. W. (June, 2006). Cooperative sensing among cognitive radios. In *ICC. IEEE international conference on communications* (Vol. 4, pp. 1658–1663).
17. Nguyen-Thanh, N., & Koo, I. (2009). A robust secure cooperative spectrum sensing scheme based on evidence theory and robust statistics in cognitive radio. *IEICE Transactions on Communications, 92*(12), 3644–3652.
18. Qihang, P., Kun, Z., Jun, W., & Shaoqian, L. (September, 2006). A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context. In *IEEE 17th international symposium on personal, indoor and mobile radio communications* (pp. 1–5).
19. Qin, T., Yu, H., Leung, C., Shen, Z., & Miao, C. (2009). Towards a trust aware cognitive radio architecture. *SIGMOBILE Mobile Computational Communication Reviews, 13*(2), 86–95.
20. Shafer, G. (1997). *A mathematical theory of evidence*. Princeton, NJ: Princeton University Press.
21. Varshney, P. K., & Burrus, C. S. (1997). *Distributed detection and data fusion*. Berlin: Springer.
22. Visotsky, E., Kuffner, S., & Peterson, R. (November, 2005). On collaborative detection of tv transmissions in support of dynamic spectrum sharing. In *IEEE international symposium on new frontiers in dynamic spectrum access networks (DySPAN)* (pp. 338–345).
23. Wang, W., Li, H., Sun, Y. L., & Han, Z. (2009). Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks. *Eurasip Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing for Cognitive Radio Networks* (accepted).

24. Wang, W., Zou, W., Zhou, Z., & Ye, Y. (May, 2008). Detection fusion by hierarchy rule for cognitive radio. In *Cognitive radio oriented wireless networks and communications. 3rd international conference on CrownCom* (pp. 1–5).
25. Xu, S., Shang, Y., & Wang, H. (April, 2009). Double thresholds based cooperative spectrum sensing against untrusted secondary users in cognitive radio networks. In *VTC spring. IEEE 69th vehicular technology conference* (pp. 1–5).
26. Zhao, J., Zheng, H., & Yang, G.-H. (November, 2005). Distributed coordination in dynamic spectrum allocation networks. In *IEEE international symposium on new frontiers in dynamic spectrum access networks (DySPAN)* (pp. 259–268).

Author Biographies

Helena Rifà-Pous is an associate professor in the Department of Computer Science at the Universitat Oberta de Catalunya from 2007. She received a graduate degree and a Ph.D. degree in Telecommunications Engineering from the Universitat Politècnica de Catalunya in 2001 and 2008, respectively. From 2000 to 2007, she was with Safelayer Secure Communications as a research project manager, focused on PKI projects mainly for the public administration. Her research interests include information hiding, network security, key management and mobile networks.

Mercedes Jiménez Blasco is a research assistant in the K-ryptography and Information Security for Open Networks (KISON) group at the Universitat Oberta de Cataluna from 2009. She received a graduate degree in Technical Telecommunications Engineering from the Universitat Autònoma de Barcelona in 2007 and she is currently pursing her M.E. degree. Her research interests include network security and next generation wireless communication systems.

Carles Garrigues received his Ph.D. in Computer Science from Universitat Autònoma de Barcelona in 2008. He is an associate professor in the Department of Computer Science at the Universitat Oberta de Catalunya, where he teaches in subjects related to Free Software, Information Systems Auditing and Information Security Management Systems. Since October 2009, he is the director of the UOC's Master's degree in Free Software. He is also a member of the K-riptography and Information Security for Open Networks (KISON) research group, and his main research interests include mobile agent security and cognitive radio networks.