PAPER

Robust Detection of Incumbents in Cognitive Radio Networks Using Groups

Helena RIFÀ-POUS[†], ***Member***, **Mercedes JIMÉNEZ BLASCO**[†], ***and*** **José MUT ROJAS**[†], ***Nonmembers***

SUMMARY Cognitive radio is a wireless technology aimed at improving the efficiency use of the radio-electric spectrum, thus facilitating a reduction in the load on the free frequency bands. Cognitive radio networks can scan the spectrum and adapt their parameters to operate in the unoccupied bands. To avoid interfering with licensed users operating on a given channel, the networks need to be highly sensitive, which is achieved by using cooperative sensing methods. Current cooperative sensing methods are not robust enough against occasional or continuous attacks. This article outlines a Group Fusion method that takes into account the behavior of users over the short and long term. On fusing the data, the method is based on giving more weight to user groups that are more unanimous in their decisions. Simulations have been performed in a dynamic environment with interferences. Results prove that when attackers are present (both reiterative or sporadic), the proposed Group Fusion method has superior sensing capability than other methods.

key words: *cooperative sensing, hard data fusion, robustness, malicious attacks*

1. Introduction

The large amount of wireless network services available today has led to an increase in the demand for the radio-electric spectrum. The spectrum's resources are limited and controlled by government agencies that grant licenses for their utilization. Only a small part of the spectrum is available for unlicensed use, and this band is becoming increasingly overloaded. In contrast, the use of the other frequencies does not exceed 15%. Thus, as stated by the Federal Communications Commission (FCC) [1], the current distribution and use of the spectrum is inefficient.

Cognitive radio networks are emerging as a key technology for optimizing the management of the available bandwidth [2]. They are characterized to have the capability to observe, learn, optimize, and change the transmission parameters according to the ambient radio environment. Thus, the frequency spectrum can be shared among primary or incumbent users (i.e., licensed) and secondary users (i.e., unlicensed) to improve spectrum utilization while avoiding interferences.

The main requirement for cognitive radio systems is to avoid interfering with incumbents. However, this is a complicated task owing to the nature of the wireless medium. The signals can suffer deep fade due to the multipath effect or because they cross a medium with severe shadowing. This effect can cause the hidden terminal problem in which a secondary node fails to detect a primary signal. To avoid errors, cognitive radio systems must be significantly more sensitive than primary receivers. Developing sensors that individually guarantee the sensitivity requirements needed for a cognitive radio system is very costly. Thus, the solutions that are usually adopted make use of a different strategy: cooperative sensing [3].

Cooperative sensing techniques combine the results of the spectrum monitoring carried out individually by several secondary users and obtain a final decision on the presence of a primary user in the operating band. As the multipath effect and shadowing are local factors that degrade the detection of only some network nodes, cooperative sensing schemes can mitigate these effects in the final decision, thus leading to an increase in the probability of primary user detection. This paradigm, however, entails security risks as the nodes can report false data that alters the final decision on the spectrum status.

Although several proposals for cooperative sensing methods can be found in the literature (see the reviews [4] and [5]), few of them take into account the presence of malicious users in the network that send erroneous data on purpose. Those that do, generally require *a priori* information on the conditions of the environment, whether that be the profile of the system nodes, the characteristics of the signal and the noise, the occupation frequency of the channels, etc.

This article introduces a new cooperative sensing fusion method for cognitive radio systems that does not assume the prior knowledge of the context and is robust against malicious attacks. The proposed algorithm uses the local decisions of multiple nodes and classifies them into four groups according to the node's hit rate, which takes into account the results obtained both over the short and long term. The groups make a decision based on the sensing report of the majority of its members. Lastly, the group decisions are fused, taking into account the global reputation of the group and the unanimity of its decision.

The rest of the article is structured as follows: In section 2, general aspects on the cooperative sensing of primary signals and on basic cooperative fusion methods are described. The group data fusion method proposed is explained in section 3. In section 4, the results of the simulations verify the operation of the proposed method compared with basic methods. The conclusions of the article are outlined in section 5.

[†]The author is with the Internet Interdisciplinary Institute, Universitat Oberta de Catalunya, 08018-Barcelona, Spain

2. Cooperative Sensing Techniques

This section first outlines the general aspects on the cooperative sensing techniques and then describes the most-used basic cooperative fusion methods.

A cognitive radio network comprises a group of secondary users that scan their radio-electric environment periodically to detect the presence of incumbents. The secondary users are found under different conditions of attenuation.

Most cooperative sensing techniques use a fusion center that collects data sent by secondary nodes on the results of their local sensing. The fusion center executes a given fusion method on the data to obtain the final decision.

The fusion methods used by the fusion center can be classified into two types: soft-combining data fusion methods and hard-combining data fusion methods. The first type of methods fuses data on the measurement taken by each node. The fusion provides very accurate information but the nodes are required to send a very high volume of data to the fusion centre. By contrast, hard decision combining methods fuse the local decisions on whether primary users are present. All the local decisions are sent to the fusion center in binary format. The main advantage of these methods is that they reduce the amount of data sent.

The methods outlined in this article use hard decision combining. Before presenting the different methods proposed for implementing cooperative sensing, two important parameters for assessing the data fusion techniques are described.

The first parameter is detection probability, which is defined as the probability of correctly detecting a primary user. This probability indicates how good a method is at avoiding interferences with primary users. When detection probability is high, a high level of primary-signal protection is achieved. The second parameter is false-alarm probability, which is the probability of detecting a primary user when there is actually no primary user. The lower the false-alarm probability is, the more efficient the use of the free channels.

2.1 Hard-Combining Data Fusion Methods

This section describes the main hard-decision combining techniques for cooperative sensing.

The OR, AND and Majority rules are the most basic data fusion methods and can be adapted to any situation [6]. These techniques decide on channel occupation by summing each of the decisions of N system nodes (u_i) and comparing the result with a threshold. The value of the decision threshold value determines whether it is a case of the AND, OR or Majority rule.

The OR rule declares that the primary user is present if at least one of the nodes detects the primary user:

$$\text{If} \begin{cases} \sum_{i=1}^{N} u_i \geq 1 & \Rightarrow \text{ primary signal present} \\ \text{else;} & \Rightarrow \text{ primary signal absent} \end{cases}$$

With the AND rule, the decision threshold for declaring there is a primary user is the total of N nodes:

$$\text{If} \begin{cases} \sum_{i=1}^{N} u_i = N & \Rightarrow \text{ primary signal present} \\ \text{else;} & \Rightarrow \text{ primary signal absent} \end{cases}$$

With the Majority fusion rule, a channel is declared occupied when at least half the nodes detect the primary user:

$$\text{If} \begin{cases} \sum_{i=1}^{N} u_i \geq \frac{1}{2}N & \Rightarrow \text{ primary signal present} \\ \text{else;} & \Rightarrow \text{ primary signal absent} \end{cases}$$

Another way of fusing the spectrum analysis data is by performing the Likelihood Ratio Test (LRT) to obtain an optimum final decision. On modeling the fusion process as a probabilistic problem, it is necessary to have additional information as well as to know the local decisions of the nodes. In particular, the knowledge of the *a priori* conditional probabilities of u_i's when u is zero or one are required. LRT is calculated using the following expression:

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

where H_0 is the hypothesis that the channel is free; H_1, that it is busy. The result of the LRT is compared with threshold λ to obtain the final decision (H_0 or H_1). Bayesian detection and Neyman-Pearson test [7] provide two mechanisms to compute the threshold. These methods are particularly good for static environments where certain system parameters are known.

In general, cooperative sensing facilitates obtaining a more accurate analysis of free frequency bands than by using one local sensing source. However, the correct operation of these methods can be affected by the following problems.

First, the signals received by the secondary nodes may be severely attenuated or simply may happen that the secondary terminal is not working correctly, thus performing erroneous spectrum analyses. These causes lead to mistakes in the node's decision on sensing the primary signal. Secondly, the system may contain malicious users. Malicious nodes send false sensing data to the fusion center in order to alter the final decision. This type of attack leads to mistakes when the data fusion algorithm is performed. This can produce effects such as false alarm and miss detection errors. False alarms reduce system performance. Miss detections, however, have more serious consequences as they can cause interferences to primary users.

As a result of these problems, recent research has been

done on new fusion methods that implement countermeasures to reduce the effects of data falsification attacks and of faulty units that unwittingly send incorrect results.

Lim et al. proposed a binary data fusion method that uses confidence vectors and reputations [8]. The confidence vector is an index assigned by the node based on the confidence that it has in the accuracy of the sensing result. The reputation is the accuracy of a node with respect to the final decisions in its sensing history.

Firstly, a node senses the spectrum, makes a decision on channel occupation and determines the confidence value. The node then adds a positive sign to the value of the confidence vector if the node decided that the channel was occupied; it adds a negative sign if it decided it was not.

Next, the nodes send their new confidence value to the fusion center. The fusion center groups all the results using a weighted majority fusion rule to obtain the final decision. Weights are assigned based on the reputations of the nodes; heavier weightings are given to the most reliable nodes. As a result, the decisions of these nodes have a bigger influence in the final decision.

The final decision u is obtained using the following expression:

$$u = \begin{cases} 1, & \text{si} \quad \sum_i c_i w_i \geq 0 \\ 0, & \text{si} \quad \sum_i c_i w_i < 0 \end{cases}$$

where c_i is the confidence vector for user i, and w_i is the reputation factor.

Other cooperative and binary fusion methods have been proposed for reducing the effects of malicious nodes ([9]–[11]), but they are not so generally applicable as they require knowledge of certain data on the environment.

3. Proposed Group Fusion Method

Up until now, the proposed hard-combining data fusion methods have been designed for very-static wireless environments in which there is a limited attacker presence. They only assume the presence of ALWAYS-YES (always declare the presence of a primary user in the network, even if they do not sense it) and ALWAYS-NO (always deny the presence of a primary user) attackers. However, nodes that normally provide the community with reliable sensing of spectrum channels can provide a skewed view of the system when they themselves need a communication channel. A selfish node can manipulate the system and say a channel is busy when it is actually free so as to be able to use this channel without having to share it with the other nodes in the community. A malicious node may also report that a channel is free when it is busy just to cause interference and the denial of service to primary nodes.

The main contribution of this paper is that it deals with any typology of false responses, from long term attacks, to punctual and sudden changes of behavior from some good reputed users. To achieve this, nodes are classified in groups based on their past behavior. The groups make a decision based on the sensing of the majority of its members. Lastly, the group decisions are fused giving heavier weightings to user groups that have higher past-detection hit-rates and that are more unanimous in their voting on the current decision. A first approximation to this strategy was presented in [12].

3.1 Crediting the Nodes

The reputation of a node is a value that measures correct detection decisions over the long term, i.e., when the node's local decision and the system's global decision coincide. Reputation $r_i \in [0, 1]$ of node i is:

$$r_i = \frac{\sum_{k=1}^{N_i} a_i(k)}{N_i}$$

where $a_i(k)$ is a function that returns 0 or 1 when node i in period k fails to detect or correctly detects the primary node, respectively, and N_i is the total number of sensing processes that a node i has performed. Thus, t_i is a global rating of node i during its lifetime.

Node stability is a value that illustrates the contextual or behavioral changes of a node over a brief period. Stability e_i is calculated using the latest four sensing operations of node i. Using this short time frame, the system can have and updated and precise view on how node's are developing their sensing tasks in a particular moment.

$$e_i = \frac{\sum_{k=N_i-3}^{N_i} a_i(k)}{4}$$

Reputation r_i and stability e_i are used to get the incidence factor $w_i \in [0, 1]$ for node i in a particular time:

$$w_i = r_i \cdot e_i$$

3.2 Classifying the Nodes

The fusion center classifies the nodes in the network in four groups (G_1, G_2, G_3 and G_4) according to their incidence factor, a value that quantifies the confidence in these nodes' reports. The nodes in the first group, G_1, are the ones with the highest marks, while the nodes in G_4 have the lowest. The cut-off values between groups are determined by the elements at positions 25%, 50% and 75% of a decending ordered list of the nodes' incidence factors. Thus, the nodes are classified into groups in the following manner:

$$\text{If} \begin{cases} 0 \leq w_i \leq \lambda_{34}; & \Rightarrow \quad u_i \in G_4 \\ \lambda_{34} < w_i \leq \lambda_{23}; & \Rightarrow \quad u_i \in G_3 \\ \lambda_{23} < w_i \leq \lambda_{12}; & \Rightarrow \quad u_i \in G_2 \\ \lambda_{12} < w_i \leq 1; & \Rightarrow \quad u_i \in G_1 \end{cases}$$

with $\lambda_{12} = olw(\lfloor 0,25 \cdot n \rfloor)$, $\lambda_{23} = olw(\lfloor 0,5 \cdot n \rfloor)$, $\lambda_{12} = olw(\lfloor 0,75 \cdot n \rfloor)$, and $olw(x)$ a function that returns the element in the x position of a descending ordered list of the incidence factors w of the n active nodes of a CR network.

After this first categorization of nodes, the fusion center verifies whether the groups meet two conditions: (1) any

non-empty group has at least 10% of the total number of nodes, (2) groups are structured in a pyramidal way; i.e. groups with higher incident factors must have less or the same number of nodes than lower groups. The fusion centre forces these conditions moving the nodes of a group to the next lower group when required. These conditions prevent the system from making decisions based on the view of too few nodes, and that a small group of malicious nodes can have a greater effect on the system than that of a good large group.

3.3 Decision Algorithm

Nodes sense the spectrum and send their local decisions $d_i = \{-1, 1\}$ to the fusion center to indicate that the band is free (-1) or occupied (1). The proposed fusion algorithm is based on the Majority fusion rule, but instead of treating the decisions of all the nodes as equal, the system weighs them according to the incidence factor of the nodes and the decision's degree of unanimity.

The fusion center adds the data reported by the nodes in the following manner:

$$\gamma = \overline{G_1} + (1 - \left|\overline{G_1}\right|)\overline{G_2} + (1 - \left|\overline{G_1}\right|)(1 - \left|\overline{G_2}\right|)\overline{G_3} + (1 - \left|\overline{G_1}\right|)(1 - \left|\overline{G_2}\right|)(1 - \left|\overline{G_3}\right|)\overline{G_4} \quad (1)$$

being $\overline{G_x}$ the average of the local decisions received by group G_x. Hence, $\overline{G_x}$ can take values between -1 and 1. $\left|\overline{G_x}\right| = 1$ when the decision of all nodes in G_x is unanimous; $\left|\overline{G_x}\right| = 0$ when the disparity of the decisions between the nodes of the group G_x is maximum, i.e., half of the nodes decide that the spectrum band on which the sensing is done is free and the other half decide that it is occupied.

The decision algorithm primarily takes into account the decisions of the nodes that are in group G_1 to make a final decision as these nodes have greater reputations and stabilities in the system. However, when the decisions in this group are very different (i.e., the absolute value of the data average is low), the weighting given to this group drops and the decisions of groups G_2, G_3 and G_4 become more important. As done with G_1, the uniformity of the decisions of each group G_x is analyzed and the incidence of this group in the final decision is weighted accordingly.

The global decision is made based on the resulting value γ (1).

$$\text{If} \begin{cases} \gamma \geq 1 & \Rightarrow \text{ primary signal present} \\ \gamma < 0 & \Rightarrow \text{ primary signal absent} \end{cases}$$

Once the fusion center has made a decision on channel occupation, the reputations and stabilities of system nodes can be updated. When reports of nodes are heterogeneous, the value of $|\gamma|$ is low, so final decision is not very confident. Contrarily, when reports are homogeneous, the value of $|\gamma|$ is high and final decision is reliable. The system only updates the reputation and stability of the nodes when the final decision has a certain degree of confidence, in particular, when $|\gamma| \geq 0.5$.

During the initial period of a user in a CR network its reputation is not calculated, a neutral value its used. Only when a node has accumulated some actions (e.g. 50) it can be profiled and put in a high reputed group.

4. Simulations

This section illustrates the results of the simulations carried out with the proposed schema using the ROC curves. The ROC curves plot detection probability (sensitivity) versus false alarm probability for different decision thresholds. The detection capability for different cooperative sensing methods for general use -those that do not require *a priori* knowledge on the application context- is analyzed.

The simulations were performed using ns-2. The test scenario is comprised of 50 secondary users spread randomly over an area of $500m$ x $500m$. Users move at a speed of $4km/h$ and hold an antenna at the ground level. The fusion center is a static node located in the middle of secondary users' squared area. Both secondary users and the fusion center have a transmitter power of $0,4W$. All the antennas have a gain of 1dB. The medium is exposed to white and colored noise of -70dB.

The primary user is located $5km$ away from the secondaries, and is transmitting at $0,8W$ using an antenna $10m$ above the ground. We use a shadowing propagation model with a standard deviation of 6, 8dB and a path loss exponent of 2, 7. The propagation model is modified using an asymmetric propagation [13] that simulates the effects of obstacles in the medium.

All the secondary nodes use energy detectors to monitor the spectrum. Therefore, users receive different SNRs and, consequently, their sensing capabilities differ. They take a local decision an report it to the fusion center, whether positive or negative. We assume the reporting is error free. Finally, the fusion center uses one of the fusion methods described in sections 2 and 3 to reach a final decision.

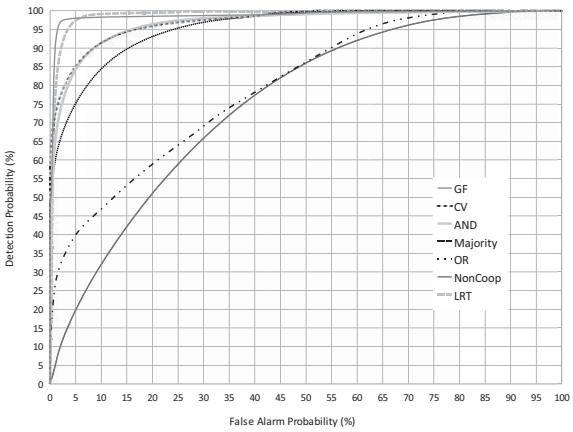

Fig. 1 ROC curve. Cooperative Detection with 50 users

We have simulated the scenarios for a period of 5000 iterations, with each iteration comprising a sensing period of 20ms.

In figure 1, the different fusion methods are compared: the proposed Group Fusion method (referred to as GF), the Confidence Vector method (referred to as CV), the AND rule (referred to as AND), the Majority fusion rule (referred to as Majority), the OR rule (referred to as OR), and the Neyman-Pearson Likelihood Ratio Test (referred to as LRT). Additionally, a non-cooperative method (referred to as Non-Coop) is defined. In this algorithm the probability of detection of individual nodes on the sensing process is measured and the average of these probabilities on each iteration is obtained.

The ROC curve shows that the detection probability increases at the expense of the false alarm probability and vice versa, which means that a compromise between these two concepts must be sought when selecting the local thresholds of decision. To achieve a minimum quality of service (QoS), the requirements for sensitivity (Pd) and false alarm probability (Pfa) should be respectively, greater than 90% and less than 10%.

The algorithms GF, LRT, CV and AND, can meet the minimum QoS requirements in the considered scenario. However, the results evidence that the proposed method outperforms the conventional data fusion algorithms; the area enclosed below the ROC curve and the axis of Pd=90% and Pfa=10% is greater for the GF algorithms than the others. For a false alarm probability of 10%, this schema achieves a detection probability 14% greater than the Majority fusion rule.

The second analyzed simulation scenario has the same network characteristics as the first, except that ALWAYS-NO or ALWAYS-YES malicious users that repeatedly attack the system are added. Simulations are carried out with each one of these type of attacks separately. Firstly, the simulation with ALWAYS-NO malicious users is shown in Figure 2. Secondly, Figure 3 represents results of the simulation subject to ALWAYS-YES attacks. To assess the behavior of each method, for each algorithm, a local detection threshold that maximizes both the detection probability and false-alarm probability in an attacker-free scenario is set (this threshold is the same for the GF, CV, LRT, Majority and Non-Coop algorithms). From here, the system's detection probability and false alarm probability are analyzed as ALWAYS-NO or ALWAYS-YES attackers are added to the network, respectively.

Figure 2 illustrates that the AND rule is the least robust method against ALWAYS-NO attacks as it experiences the greatest decrease. By contrast, OR provides the best results for this kind of attack but, as we will see next, if has a very poor perfomance against ALWAYS-YES assaults. LRT and the proposed method GF meet the minimum QoS requirements when the network has up to 36% of attackers. GF is even a little better than LRT since taking into account the operative range when detection probabilities are over 90%, this method provides better results.

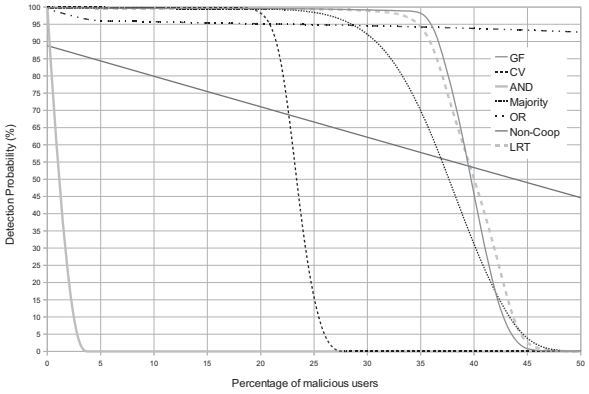

Fig. 2 Detection Probability of the system vs. Percentage of ALWAYS-NO attackers

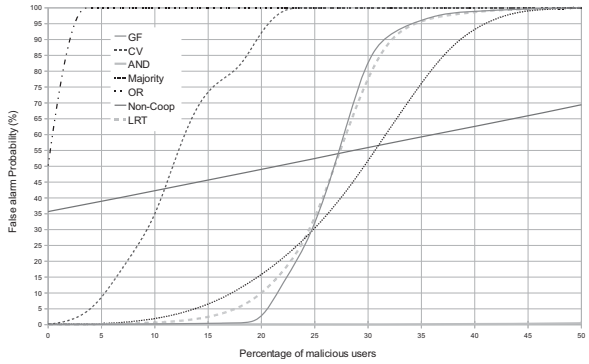

Fig. 3 False Alarm Probability of the system vs. Percentage of ALWAYS-YES attackers

Regarding the detection probabilities for the CV, Majority and Non-cooperative methods, they decrease slightly as malicious users are introduced in the system. Nevertheless the Majority fusion rule cannot assure a detection probability over 90% when there are more than 30% attackers in the CR network, the CV for more than 21% attackers, and the Non-cooperative for any case. The CV method has the best performance of all when the attackers are very low (less than 15%) but when more malicious nodes are introduced in the system, its performance decreses very fast.

Figure 3 shows that the OR rule is the least robust method against ALWAYS-YES attacks as it experiences the greatest increase in the false alarm probability. The AND rule has a good performance with this type of attack. However, as mentioned before, it can not counteract ALWAYS-NO attacks.

Focusing on the results with a false alarm probability below 10%, the best algorithm is the proposed GF scheme that can handle up to 21% of attackers. The Majority rule also presents interesting results since the slope of false alarm probability increase under attacks is very smooth. However, we seek algorithms that can maintain minimum error probabilities for as much as attackers as possible, and so, the GF

Fusion	10% Attacks		20% Attacks		40% Attacks	
Algorithm	Al.No	Burst	Al.No	Burst	Al.No	Burst
GF	99,6	99,2	99,6	98,8	35,9	65,5
CV	99,9	97,1	99,6	48,2	0,0	0,0
AND	0,0	0,0	0,0	0,0	0,0	0,0
Maj.	99,6	99,6	99,5	99,5	30,7	30,7
OR	95,8	95,8	95,2	95,2	93,8	93,8
NCoop.	79,9	79,9	71,0	71,0	53,4	53,4
LRT	99,6	99,6	99,5	98,5	50,4	20,2

Table 1 Detection Probability with different attacks

is the best.

The proposed GF scheme is effective under less than 21% of ALWAYS-NO and ALWAYS-YES attackers. As seen before, the Group Fusion scheme counteracts a greater proportion of ALWAYS-NO attackers than ALWAYS-YES. This performance is positive since the ALWAYS-NO attacks produce miss detection failures which are more harmful to the system than false alarm situations.

Lastly, the results of the system under burst attacks are analyzed. The simulation scenario is composed of nodes that, in general, are well-behaved and so, they enjoy a good reputation. However, they can occasionally attack the system when they believe that a successful attack may benefit them. Table 1 illustrates the detection probabilities of the algorithms for different percentages of attackers: 10%, 20% and 40%. Columns labelled *Al.No* show the results under ALWAYS-NO attacks, while columns labelled *Burst* indicate the detection probability under burst attacks. As expected, results show that the fusion schemes without memory, such as the OR, AND, Majority and Non-cooperative methods, behave in the same way when they get the sensing reports from occasional attackers or reiterative ones. In contrast, methods that have memory and learn from nodes' past actions are in general more vulnerable to burst attacks because the fusion center takes the reports sent by usually good nodes as correct. The least robust algorithm of our analysis is the CV. In CV nodes report the sensing result as well as the confidence level they have in this result, which is used to weight user's contributions. Thus, sporadic attackers can influence a lot the final decision and are a real threat to the network.

The proposed method GF performs better than the rest of the algorithms under burst attacks. In particular, for 10% and 20% of attackers, the GF reacts correctly, maintaining a detection probability around 99%. When the percentage of attackers is high (40%) the detection probability is around 60%, whereas for the same percentage of reiterative attackers, the method cannot detect the primary user.

Under reiterative attacks, GF and LRT are the best algorithms with quite similar results. Yet, under burst attacks the difference is outstanding, being the GF the most robust method.

5. Conclusions

In this study, a cooperative sensing by groups schema (GF) is described with the aim of improving the sensitivity and robustness of cognitive radio networks. The protocol is light and efficient since it is based on hard-decision combining techniques and so, few information has to traverse the network. The proposal is analyzed using simulations and compared with other common hard-decision techniques in order to evaluate its performance. The results demonstrate that the GF provides better detection probabilities than the others. The strength of GF is that it can handle attacks from both permanent and sporadic malicious users, and it is robust even in presence of 20% of any kind of attackers.

Acknowledgments

This work was partially supported by the Spanish Ministry of Science and Education under grants TSI2007-65406-C03-03 E-AEGIS and CONSOLIDER CSD2007-00004 ARES.

References

[1] S. Force, "Spectrum policy task force report," Federal Communications Commission ET Docket 02, vol.135, 2002.

[2] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," Computer Networks, vol.50, no.13, pp.2127–2159, 2006.

[3] A. Ghasemi and E. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," Journal of Communications, vol.2, no.2, p.71, 2007.

[4] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," Communications Surveys Tutorials, IEEE, vol.11, no.1, pp.116–130, 2009.

[5] R. Chen, J.M. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," Communications Magazine, IEEE, vol.46, no.4, pp.50–55, apr. 2008.

[6] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of tv transmissions in support of dynamic spectrum sharing," IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)., pp.338–345, Nov. 2005.

[7] P. Varshney and C. Burrus, Distributed detection and data fusion, Springer Verlag, 1997.

[8] S. Lim, H. Jung, and M.S. Song, "Cooperative spectrum sensing for ieee 802.22 wran system," Proceedings of 18th Internatonal Conference on Computer Communications and Networks (ICCCN)., pp.1–5, Aug. 2009.

[9] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," SIGMOBILE Mob. Comput. Commun. Rev., vol.13, no.2, pp.86–95, 2009.

[10] R. Chen, J.M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," INFOCOM. The 27th Conference on Computer Communications. IEEE, pp.1876–1884, April 2008.

[11] W. Wang, W. Zou, Z. Zhou, and Y. Ye, "Detection fusion by hierarchy rule for cognitive radio," Cognitive Radio Oriented Wireless Networks and Communications. CrownCom. 3rd International Conference on, pp.1–5, May 2008.

[12] M.J. Blasco, J. Mut, and H. Rifà-Pous, "Detección robusta en grupos de señales primarias en redes de radio cognitiva," Actas de la XI Reunión Española sobre Criptología y Seguridad de la Información (XI - RECSI), pp.371–376, Sep. 2010.

[13] I. of Telematics, "Asymmetric propagation proxy." Website, 2008. https://wiki.ti5.tu-harburg.de/wsn/ns2/asymmetric_propagation.