Improvement of a Fully Distributed Cooperative Spectrum Sensing Protocol for Cognitive Radio Networks

Juliana Arévalo
Universitat Oberta de Catalunya, Barcelona, Spain.
jarevalo0@uoc.edu

***Abstract*—Spectrum sensing is a key process in the context of Cognitive Radio Networks because the system requires finding white-spaces (portions of spectrum free of their rightful user). Collaborative spectrum sensing provides good performance in fading and shadowing environment, but it also opens up the possibility for malicious users to try to get the system into wrong decisions about the spectrum. They falsify the reports in order to use the spectrum selfishly or cause unavailability. To avoid this, the system requires a secure protocol that merges the information sent by all nodes to get to a final decision about the presence of the rightful user. In this paper, it is analyzed a protocol that allows merging the reports without a static, trusted node, that is difficult to find in CRN and become a single point of failure. It also requires low processing for cryptographic functions. An improvement of this protocol is presented; it reduces the overhead produced by the collaborative spectrum sensing.**

***Index Terms*—Security, Collaborative spectrum sensing, Cognitive radio networks, Authentication of sensing reports, SSDF.**

I. Introduction

Cognitive radio networks (CRN) are a new alternative for the problem of spectrum shortage in the current environment, particularly because most of the bands are destined to licensed users. In this context, ad hoc wireless users may not have enough space to transmit. However, a relevant segment of the licensed spectrum remains free [1] since the rightful users do not occupy the spectrum all the time or the band may be without any owner.

CRN propose that users without the actual license (Secondary users or nodes) use the spectrum as long as the owner (Primary user) does not occupy the band. This situation might occur during a short time window or a long period. It will depend on the P.U. application.

CRN come along with many challenges such as control channels, configurable radios definition of protocols and architectures [2] and many others.

One of the principal concerns of CRN researchers is the detection of a primary user in the spectrum or instead, finding *white spaces*, that is the availability of a band during a period. It is a key part on the communication process because it allows selecting the right bands for secondary users to transmit. This process is known as Spectrum Sensing.

For a better performance in Spectrum Sensing, it is a good approach the use of several collaborative nodes that sense the spectrum locally and then share the result with the rest of the nodes. In this way, the final decision is better informed. This method is more efficient since it considers fading, shadowing [3] and allows to use lower sensitivity sensors, keeping an accurate result.

This paper presents an improvement proposal for a secure, Fully Distributed Collaborative Spectrum Sensing protocol. The main features of the protocol, defined in [4], are presented. It also proposes an alternative to reduce the amount of data sent as control information to perform the collaborative spectrum sensing and the data fusion.

The following section presents the main aspects of the spectrum sensing process, section II presents the key features of the protocol to improve and sections III and IV present an improvement proposal and conclusions, respectively.

II. Background

A. Spectrum Sensing Process

For any spectrum sensing technique, the objective is to determine if the primary user of a certain frequency is present or if this band of the spectrum can be used opportunistically by secondary users. It also has the characteristics of any wireless network, including hidden terminal problem effect on the result because path loss, fading and any environmental situation, etc, so there is a probability that the actual state of the band will not be sensed.

For the local spectrum sensing process, there are several approaches, in [5] there is a classification on 3 schemes, (1) Transmitter detector, (2) Cooperative detection and (3) Interference based detection.

In Collaborative schemes, each node carries on with the local sensing process and then, takes place the fusion of individual reports about the spectrum. Those are sent by secondary users to a central authority that takes the final decision. Alternatively, the secondary users broadcast the reports so each node can decide by itself. Collaborative spectrum sensing has better performance in fading, shadowing environments [3] since it reduces uncertainty and allows the use of less powerful sensing devices.

However, CRN require additional considerations as they have special features not present in other wireless networks [4]:

- Nodes create CRN in ad hoc fashion without previous knowledge.
- Nodes are mobile and change over time, so the network is highly dynamic.

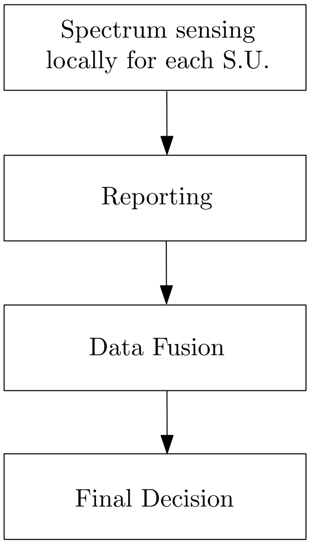

Fig. 1. Collaborating spectrum sensing phases

- Not all nodes have Internet connection, and they cannot access a Public Key Infrastructure.

In addition, it is possible that one or more nodes performing the collaborative spectrum sensing have a malfunction or is malicious and introduces false information regarding the presence of a P.U.

There are 3 distinct phases on collaborative sensing before getting the final decision. Figure 1 presents the phases: (1) Spectrum Sensing locally for each node, (2) Reporting, (3) Data fusion.

The first step is local, individual detection, where each device is responsible for sensing and deciding if there is a P.U. present. On this category, the main techniques: matched filter detection, energy detection and cyclostationary feature detection. Energy detection is the most used method because it is easy to implement and it has low computational cost.

Reporting is the process of sharing the acquired information by the previous step with the central authority (if it is centralized sensing) or the rest of the nodes (if the decision is made in a distributed manner). The reports are sent using a Common Control Channel (CCC) as proposed in [6], [5], [4]. This CCC is often modeled as error free [7], [3] and its description is out of the scope of this paper.

Data fusion is the process of combining the information from reporting to get to a final decision about the existence of a P.U. in the spectrum band evaluated. Later, it is presented a description of the effect of malicious nodes sending false information of spectrum sensing reports in the network.

1) Countermeasures to SSDF: Many collaborative spectrum sensing methods do not consider any malicious user; however not all of the nodes can be trusted, because they can try to attack the network, either to create unavailability or to use selfishly the spectrum. This attack consists of falsify the sensing data sent to the decision-makers, whether it is a central node or the rest of the nodes. The name for this attack is Spectrum Sensing Data Falsification or SSDF.

For these, not completely trusted environment, there are two approaches for merge the data received by the nodes according to the possibility that some of them are sending false information [8], (1) Reputation and (2) Correlation. However, there is still the possibility of Sybil attacks, in which a single user sends several reports with different identities. As a countermeasure, the spectrum sensing reports should be authenticated, so all nodes identify themselves.

Using the former approach, [4] presents a protocol to perform a Fully Distributed Collaborative Spectrum Sensing in a secure way. It proposes to authenticate all reports and do not have a static fusion center, instead, the center role will rotate between all members in the network.

The next section presents the main aspects of the protocol and specifically the procedure for sharing the reports result from the sensing process.

III. Fully Distributed Cooperative Spectrum Sensing for Cognitive Radio Networks

In [4], the authors present a design to perform a Fully Distributed Cooperative Spectrum Sensing from constrain devices, using hash functions, symmetric keys and a fusion center node that is called *coordinator node*. The coordinator verifies the identity of each secondary user by validating its public key certificate. This will require that a node, with a connection to Internet, plays the role of the coordinator in order to access a Certification Authority. Since this connection is not necessarily stable, a different node may act as a coordinator. The election is performed using the protocol defined in [9], based on a simple majority according to a vote from each node. All nodes send their vote selecting the candidate with the highest reputation in their own reputation table.

The final sensing decision is made by the coordinator according to method selected to merge the data [10], only using the information from nodes that the coordinator confirmed to have a valid public certificate. However, all nodes use the algorithm to confirm the coordinator's decision.

The procedures for reputation calculation use the WSPRT method defined in [10]. The protocol messages are sent through a CCC.

A. Protocol procedures

The protocol defines 3 procedures as shown in figure 2:

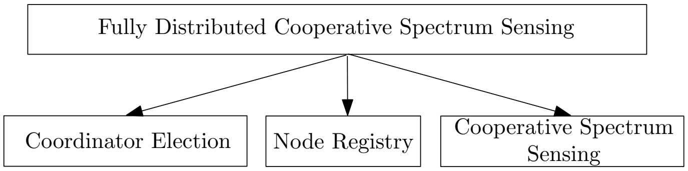
Fully Distributed Cooperative Spectrum Sensing
Coordinator Election
Node Registry
Cooperative Spectrum Sensing

Fig. 2. Procedures for the Fully Distributed Collaborative Spectrum Sensing protocol [4]

- Node registry: Each node prepares a hash chain, which is a sequence of keys applying a hash function iteratively. This method was originally proposed in [11]. The length of the chain will depend on the node's memory constrains. It will send the top value, signed with its public certificate, to register in the network. The rest of the keys in the hash chain will act as one-time keys to generate HMACs to authenticate the reports. The coordinator is in charge of validate the signature and broadcast to other nodes so the registering node can be authenticated.

- Electing a coordinator node: The protocol considers the fusion center is not static, so after a period the network selects a new fusion center, called coordinator node. It must have Internet connection and good reputation, so other nodes accept it. The election follows the method described in [9].
- Cooperative spectrum sensing: It is the most important part of the protocol; in this procedure, the nodes share and process the information related to authentication and reputation.

For the purpose of this paper, the main focus will be the third process: Cooperative Spectrum Sensing. Figure 3 shows the steps of this procedure.

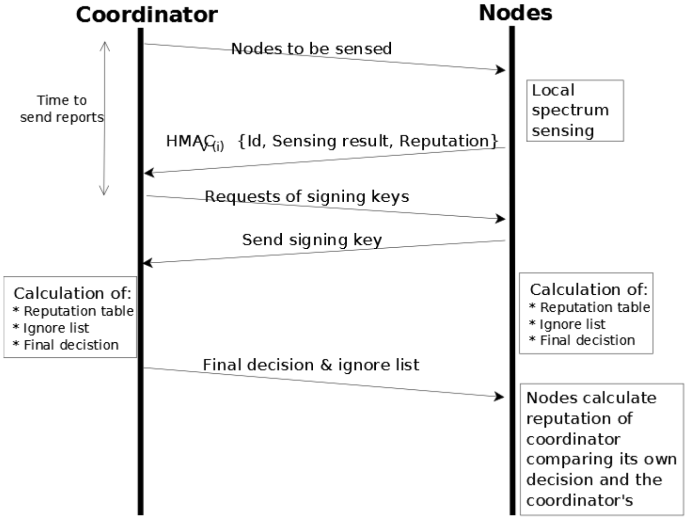

Fig. 3. Process of Cooperative Spectrum Sensing in [4]

The procedure has 11 steps, and it involves sharing information in several of them:

1) The coordinator informs which bands must be sensed.
2) Each node reports the results, along with its ID, reputation and HMAC sign.
3) The coordinator requests the keys to verify the HMAC signatures.
4) Each node sends its signing key.
5) *Only for nodes that just join the network:* New nodes create their reputation tables.
6) Each node creates a list of nodes to ignore, *Ignore List*. The reasons for a node to be in the ignore list are:
    - the HMAC signature verification has failed
    - the reputation reported by the node is different from that stored by node
    - there is no evidence of the node having registered to the network
    - no sensing result has been received
7) Each node calculates the final decision
8) Each node updates its reputation table using the final decision and the information sent by other nodes.
9) The coordinator sends its final decision and its Ignore List
10) *Only for nodes that just join the network:* New nodes update their reputation tables.
11) Nodes update its reputation table about coordinator and other nodes

This procedure is the one that requires the biggest bandwidth for the protocol. The steps with more use of the available bandwidth are, in order, 2 (spectrum sensing reports), 3 (HMAC keys) and 9 (final decision and ignore list).

B. Protocol contributions

The most notable contributions of this protocol are:

- It authenticates sensing reports for Cooperative Spectrum Sensing.
- It reduces overhead and has small bandwidth use.
- It removes the single point of failure since the coordinator node can always be replaced.

These aspects of the protocol make it suitable in CRN, taking into account that they have some difficult features, such as:

- Users may be mobile, constrain devices that create the network in and ad hoc manner, without previous knowledge of the other members.
- The transmission time and bands are limited and highly dynamical since it depends on the absence of a primary user.
- As any wireless network, the medium is a shared resource and communications are vulnerable to attackers that may want to produce unavailability or want to use the spectrum selfishly.

C. Bandwidth use

As it was mentioned before, this paper will focus on the cooperative spectrum sensing procedure, which is the one with highest bandwidth use and the most recurrent one.

Steps 5 to 8, 10 and 11 of the protocol do not transmit any data. For the others steps, the transmitted data are:

$$Step\,1 : D_tx = Sa_l$$

$$Step\,2 : D_tx = N \cdot (R_l + Id_l + SensRes_l + HMAC_l)$$

$$Step\,3 : D_tx = KeyReq_l$$

$$Step\,4 : D_tx = N \cdot (Key_l)$$

$$Step\,9 : D_tx = Z_o \cdot (Id_l + R_l) + FinalDecision_l$$

Where D_tx is the total transmitted data, Sa_l is the length in bits of the announcement of the bands that must be sensed, N is the total amount of nodes that send the reports, R_l is the length in bits of the reputation, Id_l is the length in bits of the Id, $SensRes_l$ is the length in bits of the sensing result, $HMAC_l$ is the length in bits of the HMAC code, $KeyReq_l$ is the length in bits of the hash key to calculate the HMAC,

Z_o is the number of nodes included in the ignore list and $FinalDecision_l$ is the length in bits of the final decision about the spectrum occupancy.

The actual values of these variables will depend on the amount of nodes, type of devices and their processing capacity.

The next section presents the improvement proposal for this protocol, based on the reduction of the number of transmitted reports.

IV. Improvement Proposal

Considering that, in a CRN, the channels may be available only for short periods, it is vital to optimize the protocol in order to have the minimum possible overhead [4]. It is possible to reduce the transmitted information if it is considered that some reports will not be used during the fusion data process.

The protocol is designed to collect information about the spectrum from many sources. However, most of this data remains unused because only the nodes that have registered in the networks and that have a high reputation will be considered. Since all this information was, anyway, sent to the nodes, the bandwidth was misused.

To optimize the use of the available bandwidth, the proposal is to restrict some network nodes to send reports

There are two criteria for selecting the nodes that will be banned:

- Nodes that inform a very low reputation value for themselves in the previous cycle.
- Nodes that have been included in the ignore list for a number of cycles.

To specify which nodes are disabled, the coordinator sends a list of IDs, along with the list of channels, to be sensed during the current session on the first step of the spectrum sensing procedure. Each ID will be together with a counter parameter that will decrease on each cycle until the node is no longer banned. Sharing the counter will allow the coordinator's role to move from one node to another without the necessity of sending additional information. This information will be the *Banned list*.

Since there are a number of disabled nodes, during the second stage of the spectrum sensing procedure will be less data transmitted, at the cost of more use during the first step. The procedure to restrict the nodes will depend on the media access control.

This change in the protocol affects the transmitted data for steps 1 to 4 of the original protocol, as described below:

1) Transmitted data increases in the size of the ID and the counter by the factor of disabled nodes

   $$D_t x = N_i \cdot (Id_l + Count_l)$$

   Where $Count_l$ is the decremental counter.
2) Transmitted data decreases in
   $R_d = (N - N_i) \cdot (Id_l + SensRes_l + R_l)$
   Where R_d is the total reduced data and N_i is the total number of disabled nodes in the cycle.
3) There are no changes in this step.
4) Transmitted data decreces in
   $R_d = (N - N_i) \cdot (V[i]_l)$
   Where $(V[i]_l)$ is the length in bits of the signing key for the HMAC signature.

Totally, the transmitted data will reduce in:

$$TotalR_d = N_i \cdot (Id_l + SensRes_l + R_l + HMAC_l + V[i]_l) - N_b \cdot (Id_l + Count_l)$$

Where N_b is the number of banned nodes and $Count_l$ is the length in bits of the decreasing counter that indicates how many cycles the node will be banned.

This restriction to the nodes can only take place after a given number of sensing cycles, because it requires historical reports to determine which nodes meet the criteria.

A. Additional Considerations

Other considerations for the protocol are:

- The method used for data fusion, the WSPRT, requires an increased number of reports to obtain accurate results compared to other methods [10]. For this reason, it is necessary to establish rules, so the banned nodes are able to send reports again; to achieved this, the protocol must limit the amount of sensing cycles that a node will be disabled to send the sensing reports. This is the purpose of the *counter* but the amount of cycles of any node will depend on the behavior of the nodes.

  As an example, a node gathers a low reputation over the cycles due to a poor position relative to the principal node; this node will send low reputation for itself. Using the last rule, this node could send reports again after it has moved to a more convenient location and the number of banned cycles has passed. Other node can send an invalid signature, and for that reason it will be placed in the ignore list. In this case, it is more probable that the node is malicious, and the number of banned cycles, should be larger.
- A responsibility for the coordinator is to ensure that the WSPRT method has enough reports, however it may be the case where there is a small quantity of trusted, not banned nodes. If this is the situation and there are too many mistakes in detecting the P.U, the coordinator can change the fusion method for another that allows fewer reports. It will also start to relax the rules to ban the nodes in order to get more reports and start working with the WSPRT as soon as possible.
- The nodes must process all the reports to calculate the reputation of each node. If the number of nodes reduces, then the nodes will require less processing capacity.
- Since CRN are highly dynamic, the number banned cycles for a node should be small, close to the quantity of nodes in the network.
- The decision about the banned nodes is taken by the coordinator, so the nodes must be able to use this information to update the coordinator's reputation. It will have lower weight than the actual difference between each node's final decision and the coordinator's one.

Applying the proposed changes and the considerations described before, the Fully Distributed Cooperative Spectrum Sensing protocol will reduce the required bandwidth. The next section presents a comparison between the bandwidth usages in the two schemes.

V. Bandwidth use comparison

Section III presented the bandwidth use in the original protocol. For the modified protocol, the next expressions present the transmitted data on each step.

$$Step\,1: D_tx = Sa_l + N_b \cdot (Id_l + Count_l)$$

$$Step2: D_tx = (N - N_b) \cdot (R_l + Id_l + SensRes_l + HMAC_l)$$

$$Step\,3: D_tx = KeyReq_l$$

$$Step\,4: D_tx = (N - N_b) \cdot (Key_l)$$

$$Step\,9: D_tx = Z_b(Id_l + R_l) + FinalDecision_l$$

Where Z_b is the number of nodes in the ignore lists.

Related to the original protocol, the only step that did not change was step 3. Making some assumptions, it is possible to prove that the data sent in the modified protocol is less than in the original one. The next expressions show the transmitted information with the original protocol and the modified one.

Original protocol:

$$D_tx = Sa_l + N \cdot (R_l + Id_l + SensRes_l + HMAC_l) + KeyReq_l + N \cdot (Key_l) + N \cdot (Key_l) + Z_o \cdot (Id_l + R_l) + FinalDecision_l$$

Modified protocol:

$$D_tx = Sa_l + N_b \cdot (Id_l + Count_l) + (N - N_b) \cdot (R_l + Id_l + SensRes_l + HMAC_l) + KeyReq_l + (N - N_b) \cdot (Key_l) + N \cdot (Key_l) + Z_b \cdot (Id_l + R_l) + FinalDecision_l$$

Considering that some nodes, that must be ignored, are already in the initial banned list, it is possible to assume that $Z_o > Z_b$. Also we can consider that the length of the counter $Count$ is very small compared to the sensing result, HMAC code and Key $SensRes_l, HMAC, Key_l$.

According to this, the modified protocol uses less bandwidth since it reduces the amount of sensing reports and their authentication.

VI. Conclusion

Cognitive Radio Networks require optimal protocols due to their particular conditions such as reduced bandwidth and transmission time. An important part of the CRN are the spectrum sensing mechanisms to detect the primary user in a given band. For this purpose, the best approach is to implement a collaborative scheme in a secure form. Authenticating the sensing reports from many nodes, it is possible to obtain accurate, secure results in a spectrum sensing scheme; this approach is presented in [4] as a Fully Distributed Cooperative Spectrum Sensing protocol for CRN. In this paper, an improvement of the protocol was presented. The main advantage is the reduction in the amount of broadcast data to share the spectrum sensing reports. An additional gain is that every node requires less processing resources to merge the sensing reports since the total number of reports are less than with the original protocol.

The next step on the research is to simulate the protocol and define the requirements for the protocol in lower layers.

References

[1] Peter Steenkiste, Douglas Sicker, Gary Minden, and Dipankar Raychaudhuri. Future Directions in Cognitive Radio Network Research NSF Workshop Report. In *Network*, number June, pages 1–40. 2009.

[2] Markus Mueck, Infineon Technologies, Merouane Debbah, Thomas Haustein, Fraunhofer Heinrich-hertz institute, Jens Gebert, Alcatel-lucent Deutschland Ag, Benoist Deschamps, Paul Bender, Michael Street, and Nato C Agency. COGNITIVE RADIO NETWORKS ETSI Reconfigurable Radio Systems : Status and Future Directions on Software Defined Radio and Cognitive Radio Standards. *IEEE Communications Magazine*, (September):78–86, 2010.

[3] A Ghasemi and E.S. Sousa. Collaborative spectrum sensing for opportunistic access in fading environments. *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pages 131–136, 2005.

[4] Carles Garrigues, Helena Rifà-Pous, and Guillermo Navarro-Arribas. Fully Distributed Cooperative Spectrum Sensing for Cognitive Radio Networks. In *Actas de la XII Reunión Española sobre Criptología y Seguridad de la Información.*, pages 327–332., 2012.

[5] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks*, 50(13):2127–2159, September 2006.

[6] Lingjie Duan and AW Min. Attack Prevention for Collaborative Spectrum Sensing in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications*, 30(9):1658–1665, 2012.

[7] Praveen Kaligineedi, Majid Khabbazian, and Vijay K Bhargava. Secure Cooperative Sensing Techniques for Cognitive Radio Systems. *Communications Society*, pages 3406–3410, 2008.

[8] Helena Rifà-Pous, Mercedes Jiménez Blasco, and Carles Garrigues. Review of Robust Cooperative Spectrum Sensing Techniques for Cognitive Radio Networks. *Wireless Personal Communications*, 67(2):175–198, August 2011.

[9] Helena Rifà-Pous and Jordi Herrera-Joancomartí. A Fair and Secure Cluster Formation Process for Ad Hoc Networks. *Wireless Personal Communications*, 56(3):625–636, April 2010.

[10] Ruiliang Chen, JM Park, and Kaigui Bian. Robust distributed spectrum sensing in cognitive radio networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 1876– 1884, 2008.

[11] Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11), 1981.