Managing Sensing and Cooperation to Analyze PUE Attacks in Cognitive Radio Ad Hoc Networks

Julio Soto, **Saulo Queiroz** and **Michele Nogueira**
NR2 – Wireless and Advanced Networks Laboratory
Federal University of Paraná (UFPR), Brazil
Email: {jchsoto, sauloqueiroz, michele}@inf.ufpr.br

***Abstract*—In Cognitive Radio Ad Hoc Networks (CRAHNs), malicious Secondary Users can exploit CR (Cognitive Radio) capabilities to perform Primary User Emulation Attacks (PUEA). These attacks pretend the transmission of a Primary User (PU), giving to malicious users the priority of using licensed frequencies over well-behaved unlicensed Secondary Users (SU). Since CRAHNs are envisioned as a solution for the frequency spectrum underutilization, PUEA is a threat, compromising these networks operation and easily resulting in Denial of Services (DoS). While the state of the art has focused on evolving architectural design issues (i.e. centralized non-cooperative to decentralized cooperative schemes) another key design aspect was left behind: the decision criterion, which is typically assumed as unique metric (e.g. the received signal power). To fill this gap, we propose INCA, a novel multIple criteria scheme for the deceNtralized and Cooperative Analysis of the PUEA presence in CRAHNs. INCA follows two phases. On the first, each SU employs multiple criteria to define a hypothesis about the potential existence of attacks; whereas on the second, these hypotheses are exchanged among neighbors, and each SU employs the Bayes theorem to calculate the final probability of a PUEA. Simulation results show the improvement and effectiveness of the multi-criteria approach.**

I. Introduction

The Cognitive Radio (CR) technology enable the deployment of Cognitive Radio Ad Hoc Networks (CRAHNs) in which unlicensed Secondary Users (SUs) can improve spectrum efficiency by opportunistically using idle licensed frequency bands of Primary Users (PUs), *spectrum holes* or *white spaces*. In CRAHNs, SUs (nodes) are able to communicate among themselves in a multi-hop fashion by firstly *sensing* the spectrum in order to identify a spectrum hole; next, they can *decide* move to it by employing CR capabilities to change its radio configuration parameters (e.g. channel bandwidth). Such process, however, must cause no interference on PUs. Thus, whenever a SU senses a PU, it must perform a *spectrum handoff* to release the current frequency band and move to another available white space. During this process, SU might suffer from temporal interruptions until a new available channel is found [1], [2], [3].

CRAHNs allow to achieve a spectrum management efficiency thanks to the opportunistic use of spectrum holes. However, this efficiency can be exploited as a *new* security flaw in wireless networks. A notorious instance in this sense is the Primary User Emulation Attack (PUEA) and its variants [4], [5]. The PUEA can be performed by a "bad" (i.e. malicious or selfish) SU aiming at maximizing its own spectrum usage. In a PUEA, a bad SU (the attacker) emulates its radio configurations to pretend the behavior of a PU. Thus, it impairs the spectrum sharing opportunity of legitimate (i.e. neither malicious, nor selfish) SU and increases its own priority to access licensed bands.

The design of solutions to detect or mitigate bad SU effects constitutes a challenging security aspect in CRAHNs [5], [6], [7], [8]. Hence, we observe that prior works follow mostly two design approaches: *decentralized* (instead of centralized ones) and *cooperative* (evolved from non-cooperative ones). As those works focused on such design features, another very important aspect was left behind: the **decision criterion**, which is typically assumed as a single. This decision criterion allows schemes in the literature applying complex techniques to perform an analysis based on a single criterion (ex. received signal strength) in order to determine the presence of PUE attack. In fact, to the best of our knowledge no prior work concerned the design of a multiple criteria aware scheme to detect PUEAs. A multiple criteria analysis represents an opportunity to have more resources or information to properly achieve a consensus among all different criteria and yield a better result.

Hence, to fill this gap, in this work we propose INCA, a multIple criteria scheme for deceNtralized Cooperative Analysis of PUEAs in CRAHNs. INCA consists of two phases: **sensing** and **cooperation**. On the former, each node uses multiple criteria to determine individually a preliminary probability about the presence of a PUEA. On the latter, nodes exchange their detection hypothesis and then, each node employs Bayes Theorem over them to infer the definitive probability about the presence of a PUEA. Exhaustive simulations show that INCA improves the analysis of the presence of PUEA in all evaluated scenarios, mostly when both phases are applied.

This work proceeds as follow. In Section II, we present related work. In Section III, we detail INCA, the proposed scheme to infer the presence of PUEA in CRAHNs. In Section IV, we present the performance evaluation and results. Finally, in Section V, we conclude the paper and highlight future works.

II. Related Work

Prior works employ different strategies to detect PUEAs in cognitive radio networks. In this context, we verified that

978-3-901882-48-7

the state of art has evolved non-cooperative centralized PUEA detection or mitigation approaches to cooperative decentralized ones. First solutions rely on non-cooperative centralized models to detect PUEAs, e.g. [5], [6], [7], [9]. A weakness of such approach is the strong possibility of overloading the central base station, then it can suffer from high delay levels and a point of failure in the system.

Similarly, in spite of the fact that cooperative centralized approaches (e.g. [10], [11]) can cope with those delays, they also suffer from the overload weakness. This problem is definitely solved by non-cooperative distributed schemes (e.g. [8]). However, non-cooperative approaches enable each node to detect PUEAs by itself which can lead to both high false negative and high false positives rates.

Finally, the current evolution stage of the state of the art mitigates the high detection error rates of the non-cooperative solutions by relying on *cooperative distributed* schemes (e.g. [12]). However, as all previous proposals, they relay on a single-criterion to analyze the presence of attacks on the network. As we defend in this paper, such design choice leads them to miss the opportunity of improving the detection rate.

III. The INCA Scheme

This section describes the INCA scheme. INCA considers two well-defined phases: *sensing* and *cooperation*. On the first phase, each SU samples the considered criteria and associates them with specific weights to calculate a *preliminary probability* $P(A|B)$. $P(A|B)$ is just an initial estimative about the presence of a PUEA in the network, calculated during the first phase of INCA. On the second phase, SUs exchange their $P(A|B)$ among them in order to calculate the final PUEA probability $P(B|A)$ by means of the Bayes theorem.

In the next subsections, we consider the following notation for explaining these phases. N expresses the set of nodes in the network, N_P the set of PUs and N_S the set of SUs, i.e. $N = N_P \cup N_S$. In turn, $N_S = N_{SL} \cup N_{SB}$, in which N_{SL} is the set of legitimate SUs and N_{SB} is the set of bad SUs. c expresses the number of criteria considered for the PUEA analysis and the preliminary probability $P_i(A|B)$ of the i-th legitimate SU in the network is so that $1 \leq i \leq |N_{SL}|$. These criteria represent the characteristics of transmission used by the devices (nodes) in the spectrum to establish a communication. These features may be the received signal strength, transmission power, noise, signal to noise ratio (SNR), data rate, and others.

A. Sensing phase

In the first phase of INCA, the i-th legitimate SU basically calculates $P_i(A|B)$ upon the sets $\mathcal{S}$, $\mathcal{W}$, $\mathcal{M}in$ and $\mathcal{M}ax$. The whole process is performed by means of the NWAUF (*Normalized Weighted Additive Utility Function*) analysis, whose general steps are presented in Algorithm 1. In the algorithm, $\mathcal{S}$ consists in the set of the current samples for each one of the c criteria. Similarly, the sets $\mathcal{M}in$ and $\mathcal{M}ax$ stand for the minimum and maximal known values for each one of the c criteria. These sets are used by the NWAUF algorithm to normalize values in $\mathcal{S}$ and generate the corresponding normalized set $\overline{\mathcal{S}} = \{\overline{s} \mid 0 \leq \overline{s} \leq 1\}$ (Algorithm 1. Lines 8–9). Finally, the algorithm also relays on the input $\mathcal{W} = \{w_1, w_2, \ldots, w_c \mid \sum_{i=1}^{c} w_i = 1\}$, each weight is assigned to each criteria in $\overline{\mathcal{S}}$ to calculate $P_i(A|B)$. The values in $\mathcal{W}$ are determined by us, we used static values based on the relevance of each criterion for the preliminary indication about a PUEA.

Algorithm 1 NWAUF Analysis

1: **procedure** NWAUFAnalysis($\mathcal{S}, \mathcal{W}, \mathcal{M}in, \mathcal{M}ax$)
2: ▷ Initializing the preliminary probability and the set for the normalized values of $\mathcal{S}$
3: $P_i(A|B) \leftarrow 0$;
4: $\overline{\mathcal{S}} \leftarrow \emptyset$;
5: ▷ c is the total of criteria considered in the analysis of the PUEA
6: **for all** $i = 1 \rightarrow |c|$ **do**
7: ▷ In general, X_i stands for the sample x_i of the set X
8: $\overline{s_i} \leftarrow \frac{\mathcal{S}_i - \mathcal{M}in_i}{\mathcal{M}ax_i - \mathcal{M}in_i}$;
9: $\overline{\mathcal{S}} \leftarrow \overline{\mathcal{S}} \cup \{\overline{s}\}$;
10: ▷ Assign the weight W_i for each $\overline{s}_i$ and calculate $P_i(A|B)$
11: $P_i(A|B) \leftarrow P_i(A|B) + W_i \cdot \overline{s}_i$;
12: **end for**
13: **end procedure**

The per-node NWAUF analysis gives to each node a preliminary probability of the presence of a PUEA. Such result will be considered to take the final decision in the INCA's cooperation phase. Fig. 1(a) highlights each step of the multi-criteria NWAUF analysis in the first phase of $INCA$.

B. Cooperation phase

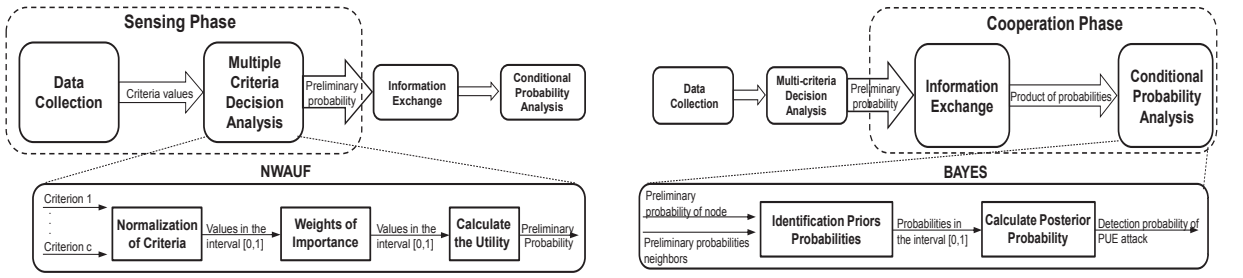
On the cooperation phase, the i-th legitimate SU in the network does not only share its $P_i(A|B)$, but also receives preliminary probabilities from its neighborhood (we consider as neighbor of a node, a SU within antenna range and a hop away from the node that exchanges probabilities). After receiving $k \leq |N_{SL}| - |\{i\}|$ preliminary probabilities from its neighborhood, the node $i \in N_{SL}$ calculates its own final probability $P_i(B|A)$ about the presence of a PUEA in the network. $P_i(B|A)$ is calculated by means of the Bayes theorem (Eq. 1) in which not only the prior preliminary probability $P_i(A|B)$ is considered but also the prior probabilities $P_j(A|B)$, $j = 1, \ldots, k$ from SUs neighbors. The relevance of the prior probability of the j-th neighbor has to $P_i(B|A)$ is denoted by $P_j(B) \in [0, 1]$. In particular, $P_i(B) \in [0, 1]$ denotes the relevance of $P_i(A|B)$ for $P_i(B|A)$.

$$P_i(B|A) = \frac{P_i(B).P_i(A|B)}{[P_i(B).P_i(A|B)] + [\sum_{j=1}^{k} P_j(B).P_j(A|B)]} \quad (1)$$

Fig. 1(b) highlights the steps performed by each SU node in the conditional probability analysis in order to determine the probability of the presence of a PUEA.

C. INCA Showcase

INCA is designed to support multiple different criteria in the analysis of a PUEA. In this Subsection, we select three



(a) Phase 1: Sensing

(b) Phase 2: Cooperation

Fig. 1. The Phases of the INCA Scheme

criteria and their corresponding models in order to explain INCA in action for a concrete case. The criteria we have chosen to illustrate INCA are: (i) *received signal strength*, (ii) *transmission power* and (iii) *distance*. Particularly, from the perspective of a legitimate SU node $i \in N_{SL}$, the strength of a signal it senses from an arbitrary node $j \in N - \{i\}$, at the instant t, is denoted by $P_R^{j \to i}(t)$. The transmission power of j is denoted by $P_T^j(t)$ and the distance between them by $d_j^i(t)$. With no loss of generality, next we explain the specific models we assumes for each one of these criteria.

Considering the models related to the $P_R^{j \to i}(t)$ criterion, the first consideration to be done concerns whether a transmission is taking place in the licensed spectrum or not, i.e. node i should properly sense the spectrum to differentiate noisy from real transmissions. Spectrum sensing in CRAHNs is usually modeled as a binary hypothesis-testing problem (e.g. [13]), as described in Eq. 2.

$$H = \begin{cases} H_0 : y_i(t) = & \eta(t), \\ H_1 : y_i(t) = & P_R^{j \to i}(t) + \eta(t) \end{cases} \quad (2)$$

In this sensing method, the H_1 hypothesis expresses that node j is using the licensed spectrum. In this case, the total power $y_i(t)$ perceived by i at the instant t is $P_R^{j \to i}(t)$ plus the signal received from other sources that, in this case, plays the role of a noisy $\eta(t)$. We assume $\eta(t)$ is the additive white Gaussian noise (AWGN). The hypothesis H_0 takes place when no transmission is sensed in the spectrum, i.e. $P_R^{j \to i}(t) = 0$.

In turn, assumes $P_R^{j \to i}(t)$ relates to both $P_T^j(t)$ and $d_j^i(t)$ by means of specific radio propagation models described in the Eq. 3. In particular, we assume the Free-Space model for the signal sensed by i if $j \in N_P$, i.e. if j is a PU (e.g. typically high TV tower); in turn, the Two-ray ground model takes place if $j \in N_S$, i.e. j is a bad or legitimate SU ([12], [14]). Finally, G_p^2 and G_s^2 model the shadowing loss factor in each aforementioned model, respectively.

$$P_R^{j \to i}(t) = \begin{cases} P_T^j(t)(d_j^i(t))^{-2} G_j^2, \text{ if } j \in N_P \\ P_T^j(t)(d_j^i(t))^{-4} G_j^2, \text{ if } j \in N_S \end{cases} \quad (3)$$

IV. Performance Evaluation and Analysis

In this section, we describe the simulation settings to evaluate the performance of INCA. Firstly, we describe the simulation environment and parameters, then we present our results and analysis.

A. Simulation Settings

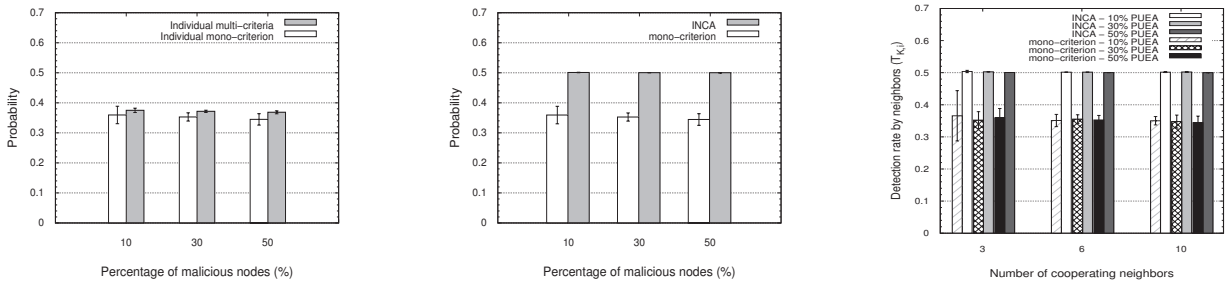
Our simulations are composed of $|N_P| = 2$ and $|N_S| = 50$ static nodes. $|N_{SL}|$ and $|N_{SB}|$ varies to reflect different rate of attackers in the network. Each SU is capable of sensing the spectrum and has the same transmission range. Whenever SUs intends to transmit, it performs a sensing procedure in order to detect an idle channel. Moreover, each PU accesses its licensed band following a random distribution. Similarly, each PUEA uses a random distribution to accesses different frequencies and generate the attack.

In the network, a node $p_1 \in N_P$ employs a private licensed channel to transmit to a node $p_2 \in N_P$. The transmission power $P_T^{p_1}(t)$ of p_1 can be easily determined by means of its underlying PHY (*Physical layer*) standard. In turn, assuming the location of p_1 is publicly known (e.g. a TV tower) any static node $i \in N_{SL}$ can know its distance $d_{p1}^i(t)$ from p_1. Thus, based on these knowledge, on the radio propagation model (Eq. 3) and on the measurements, i might increase the ability of differentiating transmission of PUs from transmission of attackers and improve its probability of detection of a PUEA. Simulations were performed in the NS-2.31 using the module for cognitive radio ad hoc networks developed by Di Felice et al. [15] with the parameters described in Table I.

TABLE I
Simulation parameters values

Simulation Parameter	Value
Secundary users (SUs)	50
Primary users (PUs)	2
Rate of PUE attackers	10%, 30%, 50%
Number of channels	11
Simulation time	500 seconds
SUs transmission range	250 m
PUs transmission range	1000 m
Attacker transmission range	250 to 1000 m
SUs transmission power	24.5 dBm
PUs transmission power	94 dBm (according to [16])
Attacker transmission power	24.5 to 94 dBm
Routing protocol	AODV
Area	1000x1000 m

The main evaluation metric employed to is the probability of the presence of a PUEA sensed by SUs. It is calculated



(a) Multi-criteria x mono-criterion (b) Comparing INCA and Mono-criterion (c) Varying the number of neighbors

Fig. 2. INCA's Evaluation

from the Bayesian theorem (Eq. 1) upon both the preliminary probability $P_i(A|B)$ calculated by the detecting node and the set of preliminary probabilities calculated and received from each cooperating neighbor. We also analyze the impact of the number k of SU neighbors (3, 6 and 10) on $P_i(B|A)$.

Further, we measure the detection rate $T_{k,i}$ of the node $i \in N_{SL}$ for different number k. $T_{k,i}$ is given by $T_i = \frac{\sum_{j=1}^{k} P_j(A|B)}{k}$, in which $P_j(A|B)$ is the preliminary probability shared by the j-th neighbor of i, and $0 \leq k \leq |N_{SL}| - |\{i\}|$ is the corresponding total of cooperating neighbors.

B. Results

In this subsection, we report the performance results of INCA using multiple criteria and compare them to a version of INCA using a single criterion, called *mono-criteria* (i.e. based only on the received signal power, which is the criterion widely used in the state of the art). Fig. 2(a) compares the probability of the presence of a PUEA given by the single-criterion approach against the probability taken from the first phase of INCA without cooperation (i.e. the multi-criteria based preliminary probability). We can observe that the performance of the single criterion analysis impairs as the rate of attackers increases in the network. Precisely, it presents the probabilities 35.96%, 35.30% and 34.48% for PUEA rates of 10%, 30% and 50%, respectively. Under these same conditions, the INCA's multi-criteria preliminary probabilities outperform the single criterion approach in 1.53%, 1.85% and 2.36%, respectively. Such improvements are solely explained by the multi-criteria design aspect since in the INCA's first phase the cooperative design aspect *does not* take place.

In turn, when the detection probability takes the cooperative phase into account *for both* INCA and the single criterion approaches, the improvements resulted from the multi-criteria design aspect in comparison to the single one are even greater (about 15.56%), as we can observe in the Fig. 2(b). This time, the cooperation works to enrich the detection analysis and provide an improvement of about 12.6% in comparison to the non-cooperative multi-criteria analysis. In spite of this, the benefits due to node cooperation can be dramatically impaired, if a multi-criterion approach does not take place. In fact, enabling cooperation for the single criterion approach presented a very slightly improvement of 0.02% in comparison to the non-cooperative single criterion approach.

Finally, Fig. 2(c) compares the detection rate $T_{k,i}$ under different number of cooperating neighbors k of a given SU i in both INCA and the single criterion approach. In the evaluation of the cooperation, we take into account the quantity of cooperating nodes and the percentage of attackers in the CRAHN. The single criterion approach presents a variation of 1.33% for the probability in the scenarios with 3, 6 and 10 cooperating nodes. In turn, $INCA$ presents a variation of 0.3% among the scenarios with different quantities of cooperating nodes. Further, we also verify that the low variation in the probabilities is due to the random access of the PUEA. In other words, this means that a SU will not necessarily use the channel under attack.

V. Conclusion and Future Works

In this work, we presented INCA, a novel multIple criteria scheme for deceNtralized Cooperative Analysis of PUEAs in CRAHNs. The INCA's design embodies not only state of the art design approaches, like decentralization and cooperation, but also an innovative approach to take into consideration multiple criteria in the process of detecting PUEAs. We evaluate INCA against its single criterion version as a way of representing the approach taken by current state of the art. Results obtained from exhaustive simulations, suggest that single criterion proposals (typically based on the received signal power) can present a very poor performance when attackers transmit at a power very similar to the primary users. In turn, INCA can handle such issue by relying on additional criteria like distance and transmission power. Thus, our results make a strong case for PUEA detection schemes that embody criteria to analyze primary user emulation attacks. An important issue inherent to the PUEA analysis based on multiple criteria schemes, as INCA, is the task of assigning weights to represent the importance and differentiate of criteria, i.e. level of relevance of each weight. In this work, we focused on demonstrating the feasibility and benefits of the multiple criteria approach instead of deeply studying the best set of weights for each criterion. In future work, we intend to design advanced algorithms to enable INCA to dynamically adjust the weights by itself.

REFERENCES

[1] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Pers. Comm.*, vol. 6, no. 4, pp. 13–18, Aug 1999.

[2] W.-Y. Lee and I. F. Akyldiz, "A spectrum decision framework for cognitive radio networks," *IEEE Trans. on Mobile Computing*, vol. 10, no. 2, pp. 161 –174, Feb. 2011.

[3] I. Akyildiz, W.-Y. Lee, M. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Comm. Mag.*, vol. 46, no. 4, pp. 40 –48, Apr. 2008.

[4] Y. Tan, K. Hong, S. Sengupta, and K. P. Subbalakshmi, "Using sybil identities for primary user emulation and byzantine attacks in DSA networks," pp. 1–5, Dec 2011.

[5] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," pp. 110 –119, Sep 2006.

[6] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Comm.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[7] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," pp. 2749 – 2753, Jun 2009.

[8] Z. Jin, S. Anand, and K. Subbalakshmi, "Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks," pp. 1–5, Dec 2010.

[9] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics," *IEEE Trans. on Wireless Comm.*, vol. 9, no. 11, pp. 3566 –3577, Nov 2010.

[10] A. Min, K.-H. Kim, and K. Shin, "Robust cooperative sensing via state estimation in cognitive radio networks," pp. 185 –196, May 2011.

[11] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Trans. on Wireless Comm.*, vol. 10, no. 7, pp. 2135 –2141, Jul 2011.

[12] S. A. Z. Jin and K. P. Subbalakshmi, "Neat: A neighbor assisted spectrum decision protocol for resilience against primary user emulation attacks," *Technical Report*, 2010.

[13] W. Zhang, R. Mallik, and K. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Trans. on Wireless Communications*, vol. 8, no. 12, pp. 5761 – 5766, Dec 2009.

[14] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," pp. 1–6, Oct 2008.

[15] M. D. Felice, K. Chowdhury, W. Kim, A. Kassler, and L. Bononi, "End-to-end protocols for cognitive radio ad hoc networks: An evaluation study," *Performance Evaluation*, vol. 68, no. 9, pp. 859 –875, 2011.

[16] C. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Comm. Magazine*, vol. 47, no. 1, pp. 130 –138, Jan 2009.