Catch Me If You Can – A Proposal Mechanism Against the Cooperative Attacks in Cognitive Radio Networks

Mr. Hari Haran V PG Scholar, Embedded System Technologies harivjkumar@gmail.com
Ms. Jeyapiriya K Assistant Professor jeyapiriya.ece@sairam.edu.in
Department of ECE Sri Sai Ram Engineering College
Tambaram,Chennai,India

Abstract*—With today's increase in the usage of wireless devices and spectrum allocation, radio spectrum is becoming scarce and it is used partially. This has evolved a concept called the Cognitive radio to exploit the presence of these spectrum holes which utilizes cooperative spectrum sensing concept for primary user detection. This spectrum sensing concept has a drawback that an intruder can capture these sensors and manipulates the sensing reports. Therefore, an attack model is considered and we propose a revised COI (combinatorial optimization identification) algorithm to defend against such attacks. Finally, spectrum allocation to secondary users is made based on the uncompromised sensing reports by filtering out the compromised sensing reports.

Keywords – **Spectrum allocation, cognitive radio, cooperative spectrum sensing, combinatorial optimization, compromised sensing reports, uncompromised sensing reports.**

I. INTRODUCTION

With the advancements and rapid use of wireless devices and consequent spectrum allocation, the radio spectrum is becoming scarce for new applications. The studies have revealed that the spectrum allocated to the authorized users have not been utilized for large periods of time. These authorized users are called the primary users (PU) who have exclusive access to specific services over the spectrum band. Also, no violation from unlicensed users called the secondary users (SU) is allowed. Due to this, the spectrum is greatly under-utilized temporally or spatially. To overcome this problem, an intelligent radio network called the cognitive radio network has evolved which grants spectrum access to secondary users to opportunistically use the licensed spectrum by using the spectrum sensing methods.

For primary user detection, the cooperative spectrum sensing method gives more accurate results when compared with other methods involved in the primary user detection. In cooperative spectrum sensing method, a group of secondary users sense the spectrum and share the sensing results with each other to make a cooperative decision whether the primary user is active or inactive. This concept leads to a problem that, an intruder makes his/her way to compromise one or a group of secondary user sensors to inject false data and he/she compromises the sensing reports to make a false detection decision opposite to that of the original decision. This type of attack is called the *cooperative attack*.

In this paper, an attack model is considered in which an attacker injects self-consistent false data (all injected data are based on a single power level which is inconsistent with the real value). A key challenge is identifying compromised sensing reports under attack and making a detection decision only with uncompromised sensing reports. We hence propose a revised COI algorithm to overcome such attacks and to make an allocation based on uncompromised sensing reports. We have evaluated our algorithm with simulation results. Also, we have estimated the accuracy of primary user detection and the performance of the algorithm.

II. PRELIMINARY CONCEPTS

In this section, we will discuss about the concepts that are involved and related to this paper.

A. Cooperative Spectrum Sensing

In cognitive radio network, the secondary users who are located in the same geographical area with the primary users, share the licensed spectrum in an opportunistic manner. This spectrum sharing can be done continuously with the help of spectrum sensing methods. Among spectrum sensing methods, cooperative spectrum sensing has shown good performance in detecting the presence of primary user. In cooperative spectrum sensing, several secondary users share the sensing results with each other to detect whether the primary user is present/absent. In this paper we consider a centralized cooperative spectrum sensing model in which, a group of secondary users share their sensing reports to a center node. This center node will make a detection decision based on the sensing reports.

Fig. 1 represents the model of a cooperative spectrum sensing concept. During each sensing period, sensors measure primary user's signals and then send them to the center node using a dedicated control channel. A primary transmitter's signal is sensed by N secondary user sensors and these sensing reports are given to a center node. This center node

reads all the sensing reports and then makes a final decision regarding allocation to all the sensors.

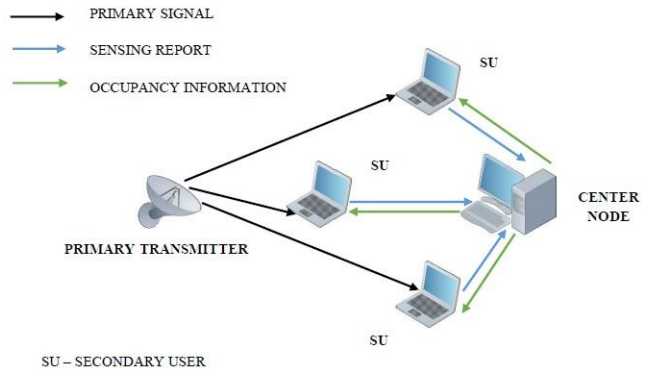

Fig. 1. The centralized model of cooperative spectrum sensing

B .Cooperative Attack

In cooperative spectrum sensing, an intruder can capture one or more secondary sensors either physically or remotely. By doing so, he/she reads all the sensing reports and injects self-consistent false data to the sensor and thus manipulates the sensing reports given to a center node. This kind of attack is called the *cooperative attack*.

The major aim of the attacker is to make the center node to take a wrong decision irrespective of the original decision. That is, the attacker when the primary user is present, the attacker will inject false data as if the primary user is absent and if the primary user is absent, the attacker will inject false data as if the primary user is present. Therefore, the main objective is to make the center node in identifying the compromised sensing reports and thus making the detection decision only with the uncompromised (normal) sensing reports.

III.STATISTICAL EVALUATION

Let each secondary user S_i is located at a distance d_i from the primary transmitter. Then, the received signal strength of the primary user at each secondary user, P_i can be calculated using the equation,

$$P_i = P_o + \alpha 10log_{10}(do/di) + \epsilon_i,\ i \in [1,N] \qquad (1)$$

where P_o is the received power at the reference distance d_o, α is the path-loss exponent and ϵ_i is the measurement error of sensor *i*.

C. Problem Formulation

We denote the set of all N sensors in a cognitive radio network by $S = \{S_1,S_2,,...,S_N\}$. During a sensing period, we assume that the sensing reports are $P = [P_1,P_2,\ldots P_N]^T$ before any attack, where T is the matrix transpose operator. Now an attacker has compromise a set of N_{com} sensors, denoted by S', where $S' \subset S$. Without loss of generality, we assume that the compromised sensors are the first N_{com} sensors in S to simplify the description. Based on the sensing reports of $[P_1,P_2,\ldots P_{Ncom}]^T$, the attacker conducts a linear fitting and obtains the primary transmission power P_o and the path-loss exponent α. Then the attacker will inject false data into the N_{com} compromised sensors as if the two values of P'_o and α', where P'_o tells a scenario opposite to the real one and α' can be any normal value. Suppose that the compromised sensing reports are $P' = [P'_1,P'_2,\ldots P'_{Ncom}]^T$. The remaining sensing reports, $P_r = [P_{Ncom+1},\ldots,P_N]^T$, are intact. Then on the control node side, the collected sensing reports are $P_\alpha = P' \cup P_r = [P'_1, P'_2,\ldots, P'_{Ncom}, P_{Ncom+1},\ldots,P_N]^T$. Our problem is to obtain the real transmission power P_o from $P\alpha$.

D. Revised COI Algorithm

The original *COI* is an approach for identifying multiple instances of bad data in power system state estimation. The essential idea is to construct a partial decision tree using the branch-and-bound method to obtain a feasible solution with the minimum number of bad data. We borrow this idea and make two modifications to fit our problem.

As mentioned above, there may be more than one feasible solution. Therefore, our first modification is to find all feasible solutions instead of only the one with the minimum number of bad data. The second modification is setting a time threshold to meet the time requirement in cooperative spectrum sensing. For instance, in IEEE WRANs, the center node must make a detection decision once every 2 seconds. We will run the branch-and-bound method with increasing bound until hitting the time threshold.

In state estimation, the state variables are P_o and α and it is denoted by vector **x**:

$$\boldsymbol{x} = [P_o \ \ \alpha]^T \qquad (2)$$

Note that $\mathbf{P} = [P_1, P_2, ..., P_N]^T$ is the vector of the primary transmitter's signal strength received by *N* sensors. The normalized residuals are defined as;

$$r_N = D^{-1/2}r \qquad (3)$$

State Estimator can be defined as;

$$x = (H^T WH)^{-1} H^T WP \qquad (4)$$

where, $D = diag(W^{-1} - H(H^T WH)^{-1} H^T)$
$r = P - Hx$
$H = log_{10}(d_0/d_i)$ and
w = diagonal matrix with elements σ_i^{-2}

We first illustrate the branch-and-bound strategy, and then present the complete algorithm. The branch-and-bound method will construct a partial decision tree. Since the data with the largest normalized residual is usually more likely to

be compromised, after each state estimation run, we pick the sensor with the largest normalized residual as the target node. Each target node has two branches, the right branch representing the case that the sensor is compromised and its left branch representing the other case that the sensor is good as shown in Fig. 2.

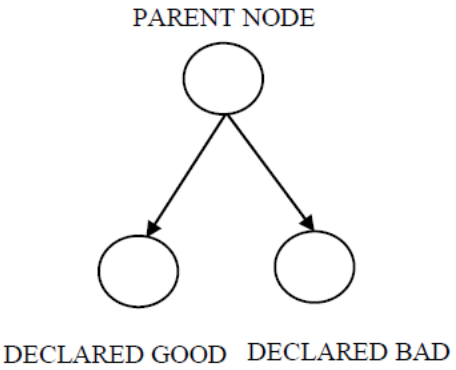

Fig. 2. Successors of a node

The state estimation is conducted at each target node assuming that all undeclared sensors are good. The next sensor to target is the one whose sensing report has the largest normalized residual among all the undeclared sensors.

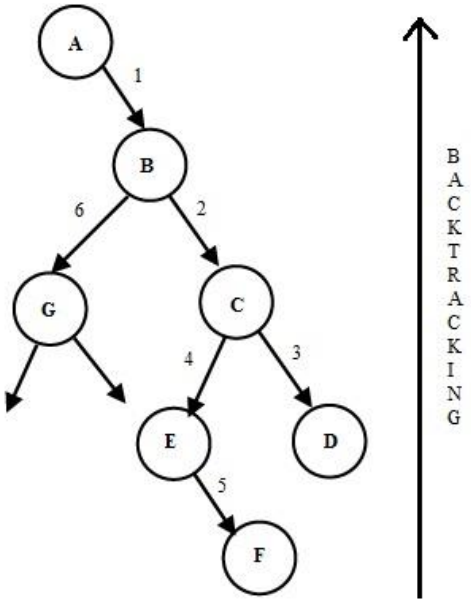

Fig. 3. Branch strategy in the decision tree

In Fig. 2, the b-successor will be the sensor with the largest residual among all undeclared sensors assuming the parent node is compromised, and the g-successor will be the sensor with the largest residual among all undeclared sensors assuming the parent node is good. The key strategy of the tree construction is to first move down towards the right until feasible solutions is reached, and then backtrack to find better solutions. In backtracking, the algorithm stays as far as possible to the right. Let us use an example to illustrate this strategy. As shown in Fig. 3, the tree is constructed in the following order:

(1) at the beginning, sensor A has the largest normalized residual, and it becomes the root of the tree; with node A declared bad, run state estimation and node B emerges to have the largest normalized residual; then node B becomes the b-successor of node A;
(2) with node B declared bad, run state estimation and node C has the largest normalized residual; then node C becomes the b-successor of node B;
(3) similar to step (2), construct node D; suppose a feasible solution is found;
(4) backtrack to node C, assume node C is good and run state estimation; node E becomes the g-successor of node C;
(5) construct node F; suppose another feasible solution is found;
(6) backtrack to node B and construct nod G.

The above construction only shows branching. The bounding is taken care of by a heuristic parameter h. In the tree, a g-successor means that one refuses to make a decision that the data with largest normalized residual is compromised, and instead asks for more information about the remaining data. During tree construction, the algorithm keeps a record on how many times a candidate solution takes a g-successor. If a node already has h g-branches between itself and the root, no more g-branches are considered for itself and its successors.

After running the algorithm, we get set F, which contains sets of feasible measurements. Since all of them are feasible, we cannot favor some over others without further information. In practice, we can estimate the attacker's capability, i.e., the maximum number of sensors he can compromise.

The problem in this paper is purely combinatorial. Our revised COI does not scan the decision tree thoroughly, while it scans the partial tree that most likely contains most of the feasible solutions. To Fig. out all feasible solutions, one has to use the brute-force search method, which takes too much computational time.

IV. RESULTS

This section shows the evaluations of the algorithm. The transmission power P_o at the reference distance d_o is 5dB. The radius of the secondary network is about 1km and the distance between the secondary network and the primary transmitter is 5km. There are eight sensors, whose distances away from the primary transmitter are listed in Table I. When there is no measurement error and the primary user is active, sensors will get perfect reports, which are marked as *perfect* in Table I. The column with *noise* shows the reports with some random noise. Now suppose an attacker has compromised three

sensors, sensors 5, 6 and 7 and changed their values to those listed in column *compromised* in Table I.

TABLE I. THE MEASUREMENTS FROM SENSORS BEFORE AND AFTER THE ATTACK

Sensor *i*	Distance d_i	*perfect*	*with noise*	*compromised*
1	4.46	-113.01	-112.81	no change
2	4.62	-113.62	-113.27	no change
3	4.90	-114.64	-114.42	no change
4	5.08	-115.27	-114.94	no change
5	5.20	-115.68	-115.36	-120.18
6	5.44	-116.46	-116.23	-120.96
7	5.72	-117.33	-117.23	-121.83
8	5.88	-117.81	-117.55	no change

The algorithm uses b_i to denote three states of sensor i, declared bad, declared good and undeclared with 0, 1, -1 respectively. We use a vector to represent a candidate problem *v = [b1, b2, ..., bN]*, in which, the candidate problem is v = [1, 1,…, 1], i.e., all the sensors are undeclared initially. Therefore, after running our algorithm, a set of feasible solutions is obtained containing the states of all the sensors which is given in Table II. Thus, secondary user allocation is made based on the original and uncompromised sensing reports which are obtained from the feasible solutions after running the algorithm.

TABLE II. FEASIBLE SOLUTIONS FROM REVISED COI

S_i	1	2	3	4	5	6	7	8
b	-1	-1	-1	1	0	0	0	-1

After obtaining all the results, the primary user detection accuracy and processing time of algorithm is computed. We consider a network with *N* = 40 sensors. The radius of the secondary network is about 2km, and the nodes are randomly distributed inside the circle. The distance between the secondary network and the primary transmitter is 8km. Before any attack, we introduce some random noise to all sensing reports; the noise for each sensing report is less than 1% of the original sensing report. Then we randomly compromise *ncom* of *N* sensors and inject cooperative bad sensing reports. *ncom* varies from 1 to 20. For each value of *ncom*, we run the simulation *n* = 1000 times and we estimate the count *n*1, the number of times that our algorithm gets the nearly correct P_o. If the resulting power is within the range of [0.9, 1.1] of the real P_o, then it is a correct detection. Therefore, P_o detection accuracy is represented in Fig. 4 which can be estimated as *n1/n*.

Fig. 5 shows the processing time of the algorithm for *N = 40* sensors. Our simulation are run on an Intel Core2Duo CPU at 1.80GHz with MATLAB.

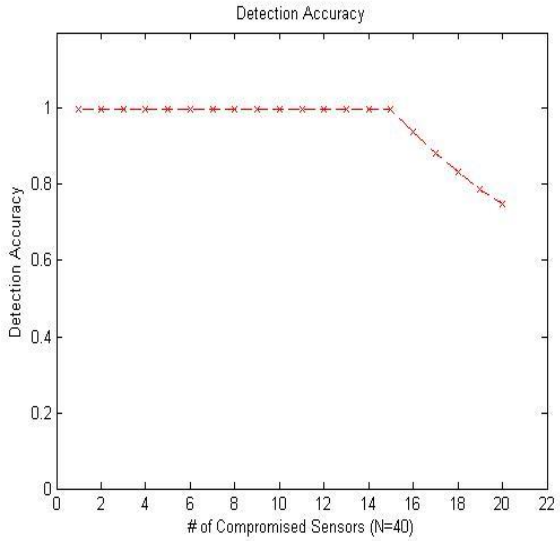

Fig. 4. P_o detection accuracy

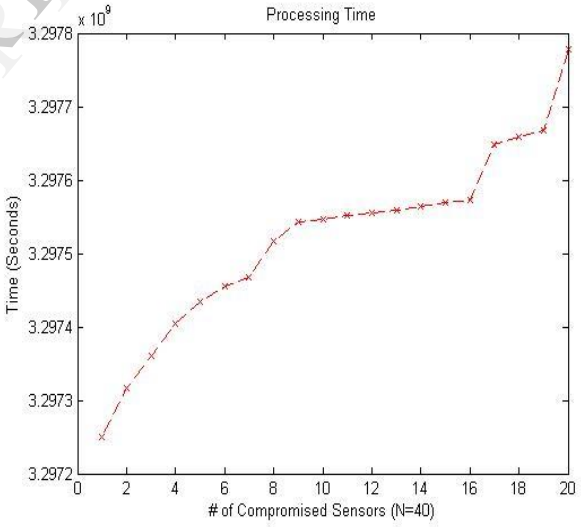

Fig. 5. Processing time

V. CONCLUSION

In this paper, we aim to defend against cooperative attacks in cooperative spectrum sensing. We propose a revised COI algorithm to improve spectrum sensing performance. Our algorithm can be flexibly adjusted to meet the time delay requirement. We intensively evaluate our algorithm with simulations, and the results show that our algorithm is well suited for these kind of attacks.

REFERENCES

[1] Z.Qin, Q.Li and G.Hsieh, "Defending against cooperative attacks in cooperative spectrum sensing," IEEE Trans on Wirless Commun., vol.12,no.6, 2013.

[2] J. Mitola III and G. Maguire Jr., "Cognitive radio: making software
radios more personal," *IEEE Personal Commun.*, vol. 6, pp. 13–18, 1999.

[3] T. Jing, X. Chen, Y. Huo, and X. Cheng, "Achievable transmission capacity of cognitive mesh networks with different media access control," in *Proc. 2012 IEEE INFOCOM*, pp. 1764–1772.

[4] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms
for cognitive radio applications," *IEEE Commun. Surveys & Tutorials*,
vol. 11, pp. 116–130, 2009.

[5] J. Hillenbrand, T. A. Weiss, and F. K. Jondral, "Calculation of detection
and false alarm probabilities in spectrum pooling systems," *IEEE Communications Letters*, Vol. 9(4), Apr. 2005, pp. 349–351.

[6] A. Taherpour *et al.*, "Asymptotically optimum detection of primary user in cognitive radio networks," *Communications, IET*, vol. 1, pp. 1138–1145, Dec. 2007.

[7] C. Xin, M. Song, L. Ma, and C.-C. Shen, "Performance analysis of a control-free dynamic spectrum access scheme," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 4316–4323, 2011.

[8] Y. Zhao, M. Song, C. Xin, and M. Wadhwa, "Spectrum sensing based on three-state model to accomplish all-level fairness for co-existing multiple cognitive radio networks," in *IEEE Proc. 2012 INFOCOM*, pp. 1782–1790.

[9] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," in *Proc. 2005 IEEE DySPAN*, pp. 137–143.

[10] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. 2006 IEEE International Conf. Commun.*, vol. 4, pp. 1658–1663.

[11] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power Apparatus Syst.*, vol. 94, pp. 329–337, 1975.

[12] Federal Communications Commission, "Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz in the 3GHz band," *ET Docket No. 04-186*, May 2004.

[13] P. Kaligineed i, M. Khabbazian, and V. Bhargava, "Malicious user
detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.*, vol. 9, pp. 2488–2497, 2010.