Int. J. Communications, Network and System Sciences, **2013, 6, 60-65**
http://dx.doi.org/10.4236/ijcns.2013.61007 Published Online January 2013 (http://www.scirp.org/journal/ijcns)

A New Method for Sensing Cognitive Radio Network under Malicious Attacker

Shaahin Tabatabaee, Vahid Tabataba Vakili
Department of Telecommunication, School of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran
Email: shaahin_tabatabaee@elec.iust.ac.ir, vakily@iust.ac.ir

Received November 4, 2012; revised December 3, 2012; accepted December 17, 2012

ABSTRACT

Cognitive radio has been designed for solving the problem of spectrum scarcity by using the spectrum of primary users who don't use their spectrum on that time. For sensing the spectrum, collaborative spectrum sensing has been utilized because of robustness. In this paper, a new collaborative spectrum method is proposed based on Least Mean Square (LMS) algorithm. In this scheme, the weights of secondary users were updated in time and finally the sensing results were combined in the fusion center based on their trusted weights. Simulation results show that the proposed scheme can significantly reduce the effects of Spectrum Sensing Data Falsification (SSDF) attackers, when they are smart malicious, and even percentage of malicious users are more than trusted users.

Keywords: Cognitive Radio; LMS Algorithm; Fusion Center; Malicious User; SSDF Attack

1. Introduction

The cognitive radio is a network to alleviate spectrum scarcity; cognitive radios (CRs) have attracted intensive research attention recently. In this network beside the licensed users (primary) who exclusively have frequency bands, CR users (secondary) are allowed to opportunistically access temporarily unused licensed bands ("white spaces"), but if the PUs come back to their frequency bands, Secondary Users (SU) have to leave the band to prevent from interference.

One of the most important challenges in cognitive radio is reliable spectrum sensing. It has attracted far-reaching attention recently. Spectrum sensing procedure can be accomplished individually or cooperatively. If spectrum sensing procedure is used by cooperative decision, it could be more reliable because there might happen something to several users and they couldn't sense the spectrum well and their local decisions don't be true.

In [1], a survey of spectrum sensing methodologies for cognitive radio is presented. Various aspects of spectrum sensing problem are studied through cognitive radio perspective; and multi-dimensional spectrum sensing concept is introduced. There are many methods for spectrum sensing such as energy detection, matched filter detection [1], cyclostationary feature detection [2], wavelet detection [3] and covariance detection [4]. Like other networks, CR networks have security problem in each layer, and because of spectrum sensing in physical layer, it needs more attention and research. In [5], the special characteristics of cognitive radio are described, and the current and potential security threats that are due to their characteristics are analyzed. In [6], the architecture of cognitive radio networks is analyzed and the various possible DoS attacks in cognitive radio networks in different protocol layers are discussed. A specific threat to spectrum sensing that is called primary user emulation (PUE) attacks is identified in [7], where a malicious user emulates characteristics of a primary user's signal in order to reduce channel resources available to secondary users. In [8] *Spectrum Sensing Data Falsification* (SSDF) attacks have been defined; under SSDF attack some of the secondary users send false sensing information into the FC to make the final decision unclear regardless of the presence or absence of the PU.

In this paper, we only consider SSDF attack. A weighted decision fusion algorithm is proposed based on LMS algorithm. Using this scheme, the reliability of each secondary user is estimated when there no priori knowledge about secondary users. The performance of the collaborative spectrum sensing in fading environment is quantified by employing LMS algorithm.

The rest of the paper is organized as follows. In Section 2, the system model will be described. The proposed scheme is introduced in Section 3, and the numerical results are depicted in Section 4. Section 5 concludes the remarks.

2. System Model

2.1. Collaborative Spectrum Sensing

SUs may sense white space while the PU is present; it could happen because of fading and shadowing on environment, where SUs could experience deep fading or shadowing. In this system making an individual decision may cause interference with primary user in network, thus collaborative spectrum sensing is applied to make the decision more reliable. In collaborative spectrum sensing two methods could be used, data fusion or decision fusion. In data fusion method, secondary users send their sensing information such as power and then data fusion processes this information by using schemes like Maximum Ratio Combining (MRC) and after all final decision is made [9]. In decision fusion, secondary users sense the channel in each time slot and make local decision and send their reports to the fusion center in a way that one bit is used by control channel [10]. In fusion center final decision is made by using different methods such as OR, AND, M out of N, Majority and etc. **Figure 1** demonstrates a typical network of cognitive radio using collaborate spectrum sensing.

Several types of spectrum sensing are utilized, in this paper, for simplicity, we use energy detection and also we assume that all users experience independent and identically distributed (i.i.d) fading with the same average Signal to Noise Ratio (SNR), and all users have the probability of false alarm P_f and probability of missed detection P_m. In [11], the relation between this probability and threshold of energy detection is provided.

We assume to have N secondary users, each of SUs sense the channel at the beginning of each slot and report their decisions to FC by one bit, $H_1(=1)$ and $H_0(=0)$ denote the presence and absence of a primary signal respectively. The signal power received by i_{th} SU is given by:

$$e_i[t] = \begin{cases} \int \left|H_i(t)s_i(t) + n_i(t)\right|^2 \mathrm{d}t : H_1 \\ \int \left|n_i(t)\right|^2 \mathrm{d}t : H_0 \end{cases} \tag{1}$$

and,

$$e_i[t] \underset{H_0}{\overset{H_1}{\gtrless}} \lambda \tag{2}$$

where $S_i(t)$ is a primary signal, $H_i(t)$ is a channel coefficient that is multiplied by signal and $n_i(t)$ is Additive White Gaussian Noise (AWGN). The threshold that is denoted by λ in Equation (2) can be defined by [11],

$$\frac{\lambda}{\sigma_n^2} = 2u + 2\sqrt{u}Q^{-1}\left(P_f\right) \tag{3}$$

where P_f is the detection probability of false alarm in wireless environment, u is time-bandwidth product and σ_n^2 is a variance of noise.

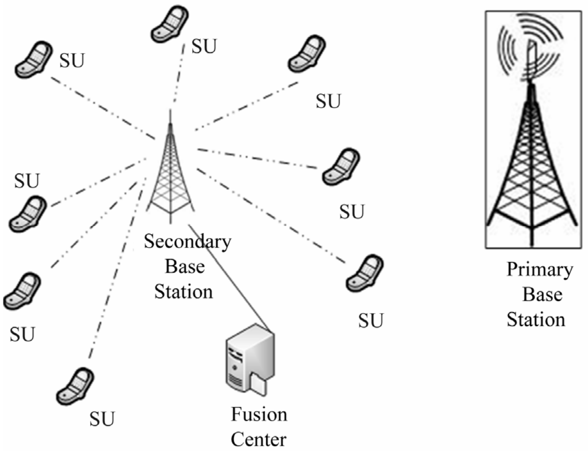


Figure 1. A typical collaborate spectrum sensing in cognitive radio network.

2.2. SSDF Attack

Beside all the advantages of collaborative spectrum sensing, it has few disadvantages, like, It needs an station for gathering all information of SUs and some nodes could send false sensing data to FC and cause some problem. For these purposes these nodes send false data, first, they could send the false sensing data to make an interference with PUs, and second, they might make Denial of Service (DoS) attack and also use the idle spectrum as selfish users.

We assume that we have 3 types of malicious users in our system:

- *Smart Malicious*: These type of attackers sense the channel in each time slots and if the channel is occupied "1" they send "0" and vice versa.
- "*Always Yes*" *Malicious*: These malicious always send "1" to FC and they aren't as smart as the first type. They don't sense the channel and without any attention to the state of channel, always send H_1. The purpose of these malicious is DoS attack.
- "*Always No*" *Malicious*: They are like always yes nodes and always send "0" to FC. The purpose of this type is to make interference with primary user in occupied bands.

2.3. Learning Algorithm

Learning algorithm which is used by neural network is explained in this section. Neural network is a pattern of human mind. Neurons in neural network mimic the properties of biological neurons in human mind. These neurons have interconnection with each other. Statistical estimation, optimization and control theory get benefit from neural network [12,13].

Neural network is used in different part of cognitive radio, such as dynamic channel selection, channel sensing, spectrum prediction, learning and etc. In this paper the Least Mean Square algorithm is used as learning algorithm. The LMS algorithm was formulated by Widrow and Hoff for using in switching circuits, but, it was developed to adaptive equalization, adaptive signal detection, adaptive signal processing and etc. The LMS algorithm operates with a single linear neuron model. The design of the LMS algorithm is very simple [14], **Figure 2**, is a simple form of this algorithm.

In **Figure 2**, obviously each input $(x_i, i = 1, \cdots, p)$ has a special weight $(w_i, i = 1, \cdots, p)$ to participate in system. After each input that is multiplied by special weight, all of the results add with each other to compute the output.

3. Proposed Scheme

As it was mentioned in section 2, LMS algorithm has weight for any of inputs. We assume that each of these inputs is once spectrum sensing report of SUs in each time slots in CR network and also the Weights are trust value of each SUs. These trusted weights will be updated in each time slot. In **Figure 3** the operation of LMS algorithm has been illustrated.

By using Wiener-Hopf equation, we can calculate the output.

$$O(k) = \sum_{i=0}^{n} w_{\mathrm{i}}(k) R_i(k) \tag{4}$$

The error of the system can be easily defined,

$$d(k) = t(k) - O(k) \tag{5}$$

and,

$$J(k) = \frac{1}{2} E\left[d^2(k)\right] \tag{6}$$

where $R_i(k)$ and $w_i(k)$ are the k_{th} report and weight of i_{th} SU, $t(k)$ is a desire target of k_{th} slot, $d(k)$ is a error of k_{th} slot and $J(k)$ is a mean square error of k_{th} slot.

By substituting Equations (4) and (5), Equation (6) can be rewritten as:

$$\begin{aligned} J = {} & \frac{1}{2} E\left[d^2(k)\right] + \sum_{i=1}^{n} w_i(k) E\left[R_i(k) t(k)\right] \\ & + \frac{1}{2} \sum_{j=1}^{n} \sum_{i=1}^{n} w_i(k) w_j(k) E\left[R_i(k) R_j(k)\right] \end{aligned} \tag{7}$$

The updated weight can be computed by:

$$w_i(k+1) = w_i(k) - \eta \nabla_{w_i} J(k) \tag{8}$$

where $\nabla_{w_i} J(k)$ is a gradient of each weight, $w_i(k+1)$ stands for updated weights and η is a positive constant called the learning rate parameter.

In Equation (7) we need to compute the correlation of SUs report and also the cross-correlation between SUs report and desire target, but we don't have any expression to compute these parameters. Using instantaneous estimation leads us to compute these parameters, where

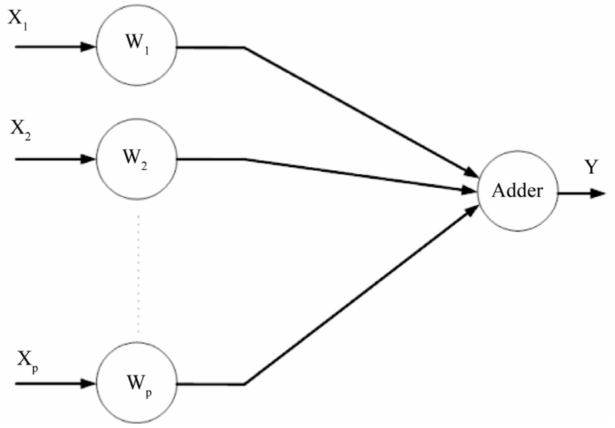


Figure 2. Simple form of LMS algorithm.

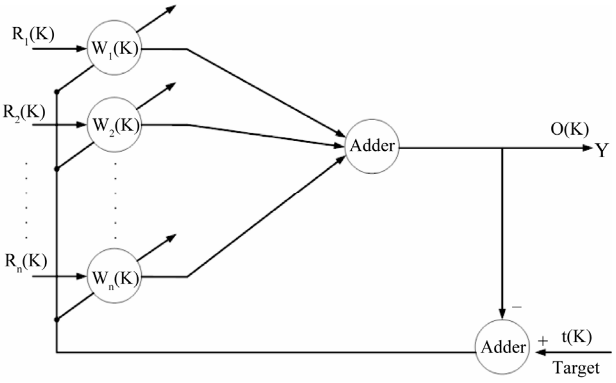


Figure 3. Cognitive radio sensors use LMS algorithm.

$$E\left[R_i(k) t(k)\right] = R_i(k) t(k) \tag{9}$$

and,

$$E\left[R_i(k) R_j(k)\right] = R_i(k) R_j(k) \tag{10}$$

Thus, Equation (8) can be rewritten,

$$\hat{w}_i(k+1) = \hat{w}_i(k) + \eta d(k) R_i(k) \tag{11}$$

where $\hat{w}_i(k)$ is a estimated weight of $w_i(k)$.

For our goal this algorithm needs to be modified, because by using this algorithm when $R_i(k)$ is H_0 (=0), the updated weight corresponded with the last weight, thus if the report is H_1, one is the input number and if the report is H_0, minus one is the input number of the algorithm.

$$R_i(k) = 2r_i(k) - 1 \tag{12}$$

where $R_i(k)$ are the mapped-reports of the real report $r_i(k)$. But, with this mapping if the primary user is absent and a report of each secondary user is H_0, the weight of this secondary user may be decreased. To solve this problem Equation (11) can be modified as:

$$\hat{w}_i(k+1)=\begin{cases}\hat{w}_i(k)+\left|\eta d(k)R_i(k)\right| & : r_i(k)=t(k)\\ \hat{w}_i(k)-\left|\eta d(k)R_i(k)\right| & : r_i(k)\neq t(k)\end{cases} \tag{13}$$

We limit the weights between 0 and 1, because by increasing the iteration, our weights tend to infinity.

About “Always no” and “Always yes” users, they depend on the primary users pattern of usage, if the primary user occupies its spectrum more than 50%, the update weights of “Always no” users tend to zero, but the weight of “Always yes” users tend almost to one and vice versa. To solve this problem we can add a provision to our algorithm proposed in **Algorithm 1**, where P_e is probability of error in AWGN channel between secondary users and fusion center.

4. Simulation Results

We consider a group of $N = 50$ secondary users that cooperate together to sense primary user. The channel between primary users and secondary users is assumed to be small scale Rayleigh fading and the channel between secondary users and fusion center is assumed to be Additive White Gaussian Noise (AWGN) channel. Received mean SNR at the secondary users is considered to be 5 *dBm*. The probability of false alarm is determined 0.1 and time bandwidth product is assumed 5. The initial weights are set in 0.5 and η = 0.025. We assume that 20 percent of the secondary users are Smart Malicious, also 20 percent are “Always yes” users and 20 percent of the users are “Always no” users. We compare our algorithm with the majority of the decisions in the figures.

In **Figure 4**, the update weights of 5 samples of secondary users are given. Obviously, we can see that the weights of trusted users, during the number of slot, are increased and the weights of smart Malicious users are decreased. It could be seen that the weights of trusted users are not same, because they encounter different fading channel during time slots. It should be mentioned that this simulation is obtained after using **Algorithm 1**.

The effect of using algorithm 1 is illustrated in **Figure 5**, where the weights of both “Always no” and “Always

Algorithm 1. Weights correction.

Parameters:

r_i(k) The report of i_{th} secondary user in slot k
R_i(k) The mapped report of i_{th} secondary user in slot k
T(k) The estate of primary user’s channel in slot k
Eta Learning rate parameter
W_i(k) The weight of i_{th} secondary user in slot k
Pe The probability of error in AWGN channel
D_W(k) The amount of update weight in each slot

Main:

```
for Number of Slots (k)
    $Y(k)=\sum R_i(k)W_i(k)$
    D_W(k)=Eta*(T(k)-Y(k))
    for Number of secondary user (i)
        z= k.Pe
        x= k-(k.Pe)
        if $\sum_k r_i(k)\geq x$
            $W_i(k+1)=W_i(k)-\left|D\_W(k)\cdot R_i(k)\right|$
        end if
        if $\sum_k r_i(k)\leq z$
            $W_i(k+1)=W_i(k)-\left|D\_W(k)\cdot R_i(k)\right|$
        end if
    end for
end for
```

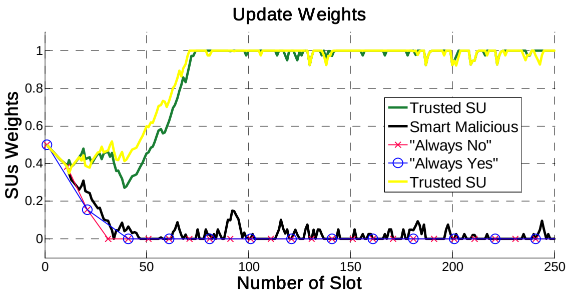
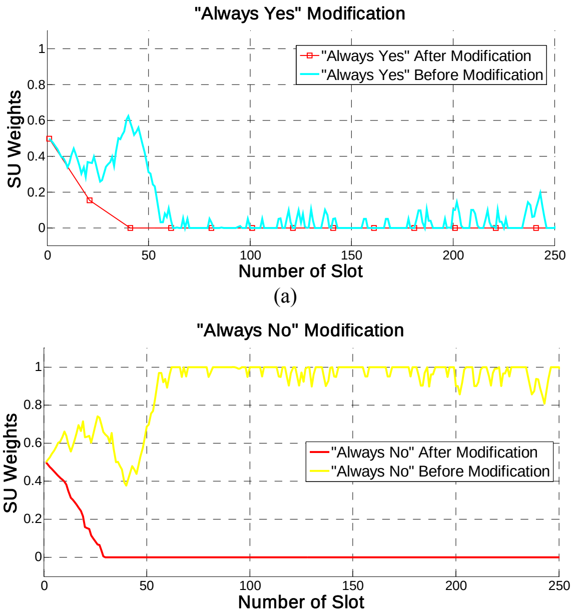


Figure 4. Update weight of 5 sample of users.



(a)

(b)

Figure 5. Malicious users modification. (a) “Always yes” users; (b) “Always no” users.

yes" tend to zero after several slots. If the **Algorithm 1** is not applied to LMS algorithm, the weight of "Always no" or "Always yes", depending on the pattern of primary user, will tend to 1.

Figure 6 shows the probability of correct sense during slots. You can see that the probability of correct sense using LMS algorithm after several slots is more than the probability of correct sense using majority decision (the reason for our simulations is the weights of secondary users, where after several slots, secondary user's weights are optimized). For **Figure 6** we apply Monte Carlo algorithm for 1000 iterations.

In **Figure 7** the percentage of false sense, False alarm and missed detection are plotted. It is obvious that with LMS algorithm the probability of errors decrease.

The LMS algorithm is very simple and it doesn't take time to compute updated weights. The number of calculations by increasing the number of secondary users grows with O(n) [15].

5. Conclusion

In this paper, a new cooperative spectrum sensing for cognitive radio based on LMS algorithm was proposed. In our proposed scheme the weights of secondary users were updated in time and finally the sensing results were combined in the fusion center based on their trusted weights. Simulation results show that our proposed scheme can significantly reduce the effects of SSDF attackers, even when they are Smart malicious, and the percentage of malicious users are more than trusted users. Moreover the effect of fading channels can decrease by using our algorithm. The complexity of our algorithm is low and it can be operated in each time slot.

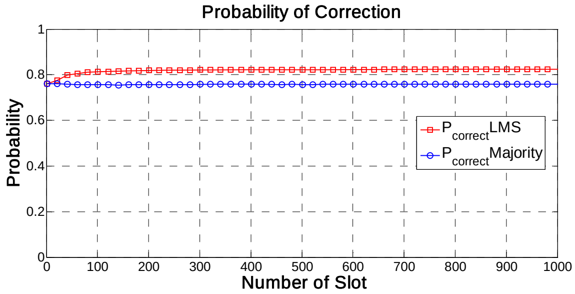


Figure 6. Probability of correct sense.

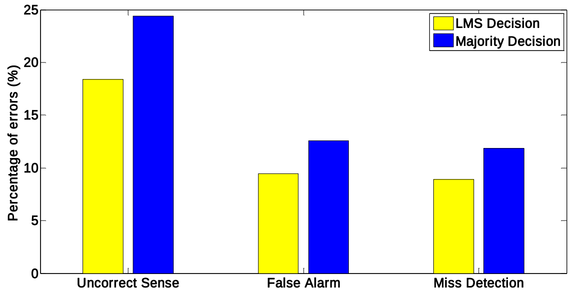


Figure 7. Probability of incorrect sense, false alarm and missed detection.

REFERENCES

[1] T. Yűcek and H. Arslan, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications," *IEEE Communications Surveys & Tutorials*, Vol. 11, No. 1, 2009, pp. 116-130. doi:10.1109/SURV.2009.090109

[2] S. Y. Xu, Z. J. Zhao and J. Shang, "Spectrum Sensing Based on Cyclostationary," *IEEE Workshop on Power Electronics and Intelligent Transportation System*, 2-3 August 2008, pp. 171-174. doi:10.1109/PEITS.2008.41

[3] S. Chantaraskul and K. Moessner, "Implementation of Wavelet Analysis for Spectrum Opportunity Detection," *IEEE 20th International Symposium on Personal*, *Indoor and Mobile Radio Communications*, Tokyo, 13-16 September 2009, pp. 2310-2314.

[4] Y. Zeng and Y.-C. Liang, "Covariance Based Signal Detections for Cognitive Radio," 2*nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, 17-20 April 2007, pp. 202-207.

[5] Y. Zhang, G. C. Xu and X. Z. Geng, "Security Threats in Cognitive Radio Networks," 10*th IEEE International Conference on High Performance Computing and Communications*, Dalian, 25-27 September 2008, pp. 1036-1041. doi:10.1109/HPCC.2008.21

[6] W. F. Wang "Denial of Service Attacks in Cognitive Radio Networks," 2010 *International Conference on Environmental Science and Information Application Technology* (*ESIAT*), Wuhan, 17-18 July 2010, pp. 530-535.

[7] R. Chen, J. M. Park and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, Vol. 26, No. 1, 2008, pp. 25-37. doi:10.1109/JSAC.2008.080104

[8] R. Chen, J.-M. Park and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," *IEEE Proceedings of the* 27*th Conference on Computer Communications*, 13-18 April 2008, pp. 1876-1884.

[9] J. Ma, G. Zhao and Y. Li, "Soft Combination and Detection for Cooperative Spectrum Sensing in Cognitive Radio Networks," *IEEE Transactions on Wireless Communications*, Vol. 7, No. 11, 2008, pp. 4502-4507. doi:10.1109/T-WC.2008.070941

[10] Y. Zeng, Y. Liang, A. Hoang and R. Zhang, "A Review on Spectrum Sensing for Cognitive Radio: Challenges and Solutions," *EURASIP Journal on Advances in Signal Processing*, Vol. 2010, 2010, p. 2. doi:10.1155/2010/381465

[11] S. Ciftci and M. Torlak, "A Comparison of Energy Detectability Models for Cognitive Radios in Fading Environments," *Wireless Personal Communications*, Vol. 68, No. 3, 2013, pp. 553-574.

[12] Wikipedia, "Neural Network and Multilayer Perceptron," 2012. http://en.wikipedia.org/wiki

[13] X. Dong, Y. Li, Ch. Wu and Y. Cai, "A Leaner Based on

Neural Network for Cognitive Radio," *IEEE International Conference on Communication Technology* (*ICCT*), Nanjing, 11-14 November 2010, pp. 893-896. doi:10.1109/ICCT.2010.5688723

[14] S. Haykin, "Neural Network a Comprehensive Foundation," Prentice Hall, Upper Saddle River, 1999.

[15] T. S. Rappaport, "Wireless Communications Principle and Practice," 2nd Edition, Prentice Hall, Upper Saddle River, 2001.