Int. J. Communications, Network and System Sciences, **2011, 4, 507-513**
doi:10.4236/ijcns.2011.48062 Published Online August 2011 (http://www.SciRP.org/journal/ijcns)

A Two Step Secure Spectrum Sensing Algorithm Using Fuzzy Logic for Cognitive Radio Networks

Ehsan MoeenTaghavi, Bahman Abolhassani
School of Electrical Engineering, Iran University of Science and Technology (*IUST*), *Tehran, Iran*
E-mail: *emtaghavi@elec.iust.ac.ir*, *Abolhassani@iust.ac.ir*
Received June 5, 2011; *revised July* 9, 2011; *accepted July* 18, 2011

Abstract

In this paper, a two step secure spectrum sensing algorithm is proposed for cognitive radio networks. In this algorithm, the sensing results of secondary users are pre-filtered and applying fuzzy logic, so, the overall sensing performance of the network is improved. To determine pre-filter parameters, statistical parameters of the sensing results are used to remove those sensing results which are far from the majority sensing results. However, to obtain a better performance in the spectrum sensing, we propose a fuzzy logic to nullify the effects of malicious users who transmit false sensing data to the fusion center. We further propose a Fuzzy Trust Level for each user as to weight the sensing result of the corresponding user before combining all sensing results in the fusion center. Simulation results demonstrate that our proposed algorithm yield significant improvement in the performance of the spectrum sensing and identifying malicious users.

Keywords: Cognitive Radio, Cooperative Spectrum Sensing, Energy Detection, Malicious User Detection, Pre-filtering, Fuzzy Logic

1. Introduction

Traditionally, fixed spectrum bands have been assigned to specific services for a long time. This policy has led to inefficient spectrum usage, and caused cognitive radio networks were proposed. In these networks, cognitive radios, which are called secondary (unlicensed) users are allowed to use the primary (licensed) users' bands when such bands are unoccupied by primary users (Pus). However, the secondary users (SUs) must make the band vacant immediately after a PU starts transmitting in the corresponding band [1]. Therefore, the most important task of a cognitive radio is spectrum sensing. Spectrum sensing techniques include energy detection, cyclostatioary feature detection and matched filter detection [2-4]. The performance of a spectrum sensing is determined by two probabilities: probability of detection (P_d) and probability of false alarm (P_f). P_d is the probability of declaring the channel is occupied while the PU is present. P_f is the probability of declaring the channel is occupied by a PU while the PU has no transmission. Among different spectrum sensing schemes for reliably identifying the licensed spectrum status, the energy detector scheme incurs a very low implementation cost and therefore is widely used. It serves as the optimal method to detect the signal transmitted by a PU whose location is unknown, and the detector only knows the power of the received signal [6]. The problem of this scheme is that the received signal power can be seriously weakened at a particular geographical location due to multipath fading and shadowing effects [7]. In these circumstances, it is difficult for a single sensing user to distinguish between an idle band and a deep faded one. In order to overcome this problem, cooperative spectrum sensing schemes have been proposed [5,8,9]. However, in cooperative sensing, due to imperfect channel between a primary user and a secondary user (SU) or dishonestly behavior of a SU, a user might send false sensing result to the fusion center. So, the performance of the system degrades severely. To overcome this problem, secure spectrum sensing has been proposed.

In [8], a spectrum sensing data falsification problem was solved by weighted sequential probability ratio test (WSPRT), which gives a good performance. However, this method requires the knowledge of locations of sensing terminals and position of PU for obtaining some required prior probabilities. This is inappropriate for mobile cognitive radios and for systems in which the location of the primary user is completely unknown. In [10], a robust secure distributed spectrum sensing scheme is

proposed that uses robust statistics to approximate the distribution for both hypotheses of all users, discriminatingly, based on their past data report. The authors in [11] propose the majority rule in the fusion center to nullify the effects of the malicious users. In [5], an effective weighted combining method is proposed to reduce the impact of false information. In [12], a defense scheme is proposed that computes suspicious levels and trust values of the users. In our previous work [13], malicious user detection based on outlier energy detection techniques is proposed and a filtering method is used based on statistical parameters of sensing results to eliminate the effects of malicious users. In this paper, we propose a two step secure spectrum sensing algorithm. At first, based on the statistical parameters of SUs sensing results, a pre-filter is designed to remove the sensing results of the secondary users which are far from the others. Then, trust weighted values are assigned to the users whose sensing results are passed from the filter based on the fuzzy logic. Finally, a weighted combining method is proposed to make final decision in the fusion center.

The rest of the paper is organized as follows: In Section 2, the system model is described and a brief background about fuzzy logic is presented. In Section 3, our new algorithm to nullify the effects of malicious users is proposed. Simulation results are carried and analyzed in Section 4, and conclusions are drawn in Section 5.

2. System Description

2.1. System Model

We discuss a cognitive radio network consist of one PU and a group of N SUs. A cooperative spectrum sensing is considered in which channels between a primary user and each secondary user have independent and identically distributed (i.i.d) Rayleigh distributions. Variation in path-loss is neglected. Each SU conducts energy detection and transmits the measured value of received signal energy in a perfect (*i.e.* error free) control channel to the fusion center. By combining the sensing results received from different SUs, the fusion center makes the final decision regarding the presence or absence of the primary user. If $e_n[k]$ for n=1,2, ⋯, N represents the received signal energy of n^{th} SU at time instant k, hypotheses H_1 and H_0 denote the presence and absence of the primary signal, respectively. Then, the signal energy received by n^{th} SU is given by:

$$e_n[k]=\begin{cases}\int_{T_k}^{T_k+T-1}\left|h_n(t)s(t)+z_n(t)\right|^2\mathrm{d}t, & H_1\\ \int_{T_k}^{T_k+T-1}\left|z_n(t)\right|^2\mathrm{d}t, & H_0\end{cases} \quad (1)$$

where T represents the time interval of sensing, $s(t)$ is the primary signal, $h_n(t)$ denotes the channel gain between the primary user and the n^{th} secondary user, and $z_n(t)$ is the additive white Gaussian noise (AWGN).

A threat to cooperative spectrum sensing is transmission of false results by attackers to the fusion center, which leads to make a wrong decision (SSDF[1] attack). So, cooperative spectrum sensing in adversarial environments where a malicious user sends false data degrades the performance of the system severely. In adversarial environments, different kinds of malicious users can affect the spectrum sensing system. They may send data indicating the presence of the PU to the fusion center ("Always Yes" malicious users). These malicious users cause the fusion center to erroneously decide that the PU is present. Then, malicious users selfishly use the entire free spectrum band and also probability of false alarm is increased. Another kind of malicious are those who always send data indicating the absence of the primary user ("Always No" malicious users). This kind of malicious users causes the interference among the primary and secondary user's signal and decrease probability of detection [14]. Therefore, the fusion scheme must be robust enough. In this paper, we propose a two step algorithm for secure spectrum sensing. In step 1, the sensing results in the data collector are pre-filtered and in step 2, we assign each user a Fuzzy Trust Level using fuzzy logic. In our proposed algorithm, more reliable users are assigned with higher trust levels. This algorithm also detects suspicious users with their corresponding suspicious levels using fuzzy logic. Finally, the sensing results are combined together based on their Fuzzy Trust Levels in the fusion center.

2.2. Overview of Fuzzy Logic

In this section, we present a brief background on fuzzy logic. The reason for that is because our proposed algorithm integrates fuzzy logic with spectrum sensing in order to better detect malicious user.

Fuzzy logic was introduced by Dr. Lotfi Zadeh of UC/Berkeley in the 1960's as a mean to model the uncertainty of natural language. fuzzy logic, a widely deployed technology for developing sophisticated control systems [15,16], provides a simple way to get definite precise conclusion and solution based on unclear, imprecise, ambiguous or missing input information. **Figure 1** shows the steps that fuzzy logic controller is composed of. The steps of a fuzzy logic can be summarized as follows: 1) receiving input values representing measurements of the parameters to be analyzed; 2) subjecting the input value to if-then fuzzy rules; 3) averaging and

[1]Spectrum Sensing Data Falsification Attack.

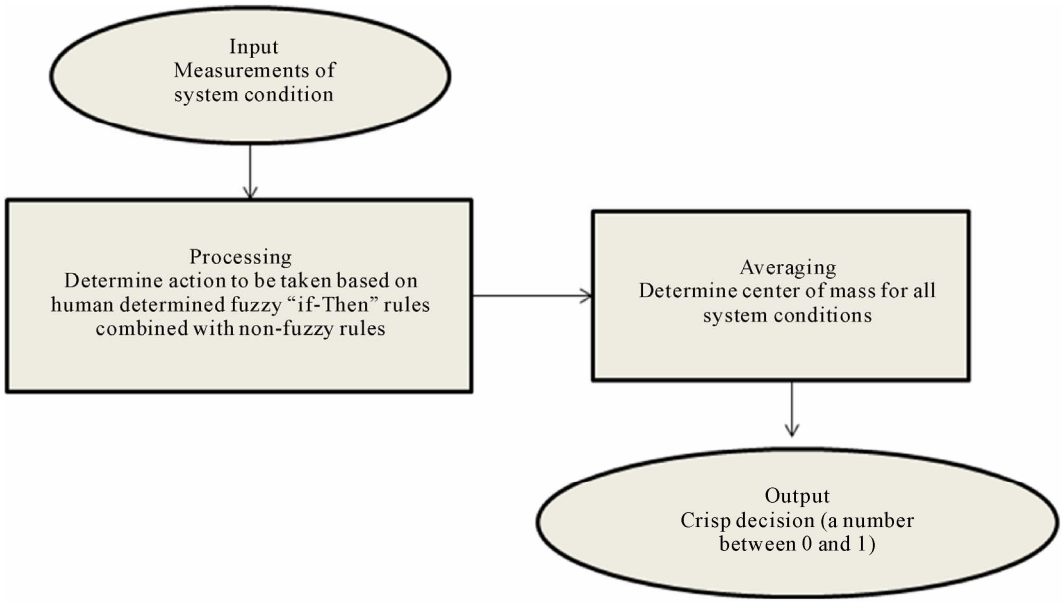

Figure 1. Components of the fuzzy logic controller [17].

weighting the results from all individual rules into one single output decision; 4) defuzzification of output to get a value between 0 and 1. To develop a fuzzy logic controller, two major components are required: 1) definition of a membership function for each input/output parameter; 2) designing the fuzzy rules. The membership function is a graphical representation of the magnitude of participation of each input. The fuzzy logic rules use the input membership values as weighting factors to determine their influence on the output sets [17].

For several reasons, fuzzy logic is very appropriate for using on secure spectrum sensing. One reason is that there is no clear boundary between normal and anomaly users. The use of fuzziness of fuzzy logic helps to smooth the abrupt separation of normality and abnormality. Another reason is the reduction of miss detection and false alarm probabilities. In the next section, we present details of the fuzzy logic that we use in our secure spectrum sensing algorithm.

3. Secure Spectrum Sensing Algorithm

By filtering and removing sensing results of malicious users, performance of the system can be compensated to some extent. First, the sensing results are passed through a pre-filter. In our proposed algorithm, those sensing results that are numerically distant from the rest of the results are not considered in the final decision. We propose to use the median (med[*k*]) and standard deviation ($\sigma[k]$) of energy values of sensing results in the computation of upper and lower bounds of the filtering, at time instant *k*, as follows:

$$\begin{cases} e_u[k] = \text{med}[k] + 1.5\sigma[k], \\ e_l[k] = \text{med}[k] - 1.5\sigma[k]. \end{cases} \quad (2)$$

Considering the number of malicious users is much less than the total number of users, the median is less vulnerable to the presence of the malicious users. So, the filtering removes most of the malicious users.

Although filtering removes most malicious users, some sensing results, which have been affected by fading or by malicious users, might pass through filtering. The performance of the system will degrade in these two cases. To prevent this performance degradation, we propose to dedicate a trust factor (*TF*) to each user who passed through filtering. The users, which have been affected by fading or are malicious, are assigned with lower trust factors. The users, which have a good channel condition or aren't suspicious to be malicious are assigned with higher trust factors. Trust factors are determined and normalized so that their summation becomes one, *i.e.*

$$\sum_{n=1}^{N} TF_n[k] = 1. \quad (3)$$

In this paper we propose to use fuzzy logic to dedicate each user a Trust Factor. As mentioned before, the fuzzy logic is composed of membership functions for each the input/output variables and fuzzy values. We select spectrum sensing results as input parameters to the fuzzy controller in order to detect malicious users. For an input parameter, three Gaussian membership functions are designed: 1) always no malicious users; 2) trusted users; and 3) always yes malicious users. **Figure 2** shows the

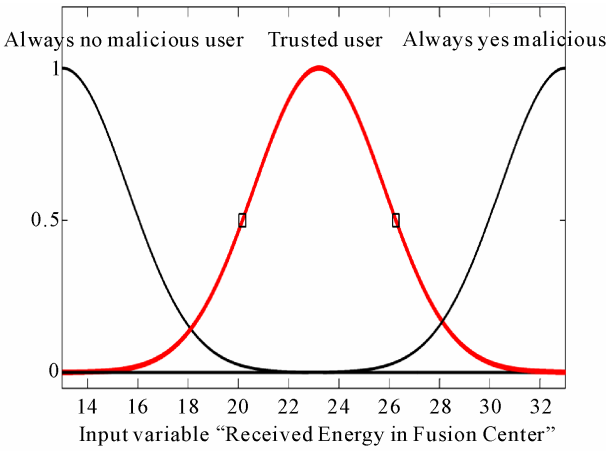

Figure 2. Membership functions of an input parameter.

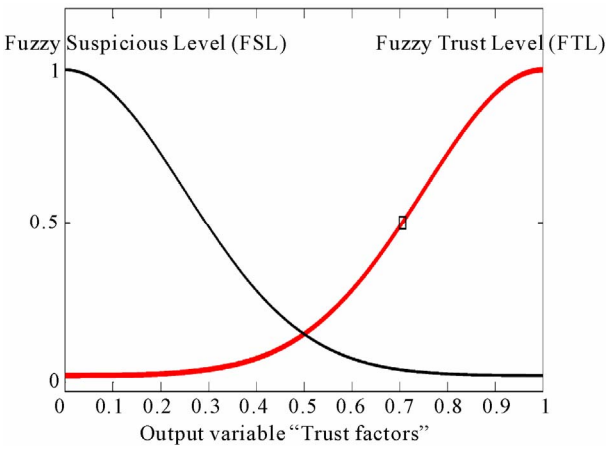

Figure 3. Membership functions of the output.

three Gaussian membership functions for an input parameter. The output parameter also has two Gaussian membership functions distributed in the range [0, 1] as shown in **Figure 3**. These two membership functions are called Fuzzy Trust Level (FTL) and Fuzzy Suspicious Level (FSL). After defining the input parameters, the fuzzy logic rules are designed. These rules are written depending on the knowledge of secure spectrum sensing. We discuss these rules in the following:

1) If (the sensing result is Trusted user) then (output is FTL). This rule presents the sensing result of this user is an expected value, so this user is normal and participates in final decision in the fusion center;

2) If (the sensing result is always no malicious user) or (the sensing result is always yes malicious user) then (output is FSL), this rule presents the sensing result of this user is an unexpected value, so this user is malicious and takes no part in final decision.

The output of the system shows the trust and suspicious levels of each user. Those users whose sensing results are near the median of the sensing results are assigned with higher trust levels and other users whose sensing results are far from the median are assigned with higher suspicious levels in the fuzzy logic. After Defuzzification for each user, we have a value for FTL and a value for FSL in the range [0, 1]. The FTL shows the degree of being a normal user and the FSL shows how much malicious the user might be. In final decision, to eliminate the effects of malicious users, we propose to combine each sensing result, considering its fuzzy trust level (FTL). First, we normalize fuzzy trust level of user n at time instant k as follows:

$$\mathrm{FTL}_n[k] = \frac{\mathrm{FTL}'_n[k]}{\sum_{n=1}^{N} \mathrm{FTL}'_n[k]}, \tag{4}$$

where N denotes the number of users which have been passed through filtering. Then, the final decision is computed using FTLs of all N users as follows:

$$\sum_{n=1}^{N} \mathrm{FTL}_n[k]\mathrm{e}_n[k] \underset{H_0}{\overset{H_1}{\gtrless}} \mathrm{e}_T. \tag{5}$$

If the value obtained in the left side of the above equation is greater than a given threshold (e_T), the fusion center will announce the presence of the primary signal. In our proposed algorithm, the suspicious users who are malicious or their sensing results are affected by fading are assigned with lower fuzzy trust levels, so their effects on the final decision are insignificant.

To achieve a better performance, the sensing results of each user over a given number of (say L) measurements are considered to obtain the final fuzzy trust level for each user. In the computation of a fuzzy trust level, we assign higher weights to those FTLs which are closer to the present time, *k*, *i.e.*:

$$\mathrm{FTL}_n[k] = \sum_{l=0}^{L-1} (L-l)\,\mathrm{FTL}'_n[k-l). \tag{6}$$

Finally, these weighted fuzzy trust levels are normalized according to Equation (4).

By considering previous and present behaviors of each user in computation of the final fuzzy trust level, the users which behave maliciously for a period of time and behave normally the rest of time, are detected and assigned with lower Fuzzy Trust Levels.

4. Simulation Results

In this section, the proposed secure spectrum sensing algorithm is evaluated by simulations. The basic parameters are fixed and considered as a group of N = 50 secondary users. The mean received SNR of the channel between the primary user and each of secondary users is 2 dB. Independent and identically distributed small scale

fading channels are considered between any SU and the PU, and the path loss is neglected.

In **Figure 4**, we assume a cooperative system with 10 "Always No" malicious users, each giving a value indicating the absence of the primary user. To evaluate our secure sensing algorithm, we compare probability of detection (P_d) and probability of false alarm (P_f) of our algorithm and three other cases, which are: 1) cooperative spectrum sensing with no malicious user; 2) spectrum sensing with malicious users with no suppression; and 3) secure spectrum sensing proposed in [5]. From **Figure 4** we can see that using our secure sensing algorithm, the "Always No" malicious users are assigned with low fuzzy trust levels and can not affect the performance of the system. So, the probability of detection (P_d) of the system would be close to that of cooperative sensing with no malicious user.

In **Figure 5**, unlike **Figure 4**, we consider a sensing system in which 10 users always announce the presence of the primary user to the fusion center. From **Figure 5** we can see that our proposed scheme can nullify the effects of malicious users in the final decision and has better performance compared to those of previous works. It's notable that in the secure sensing, which was pro-

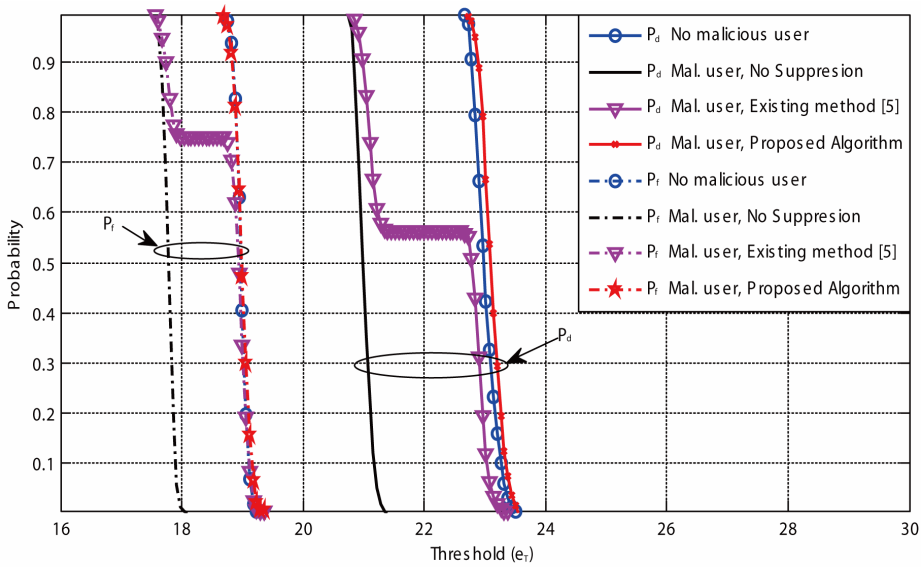

Figure 4. Probability of detection and false alarm in adversarial environment with 10 "Always No" malicious users.

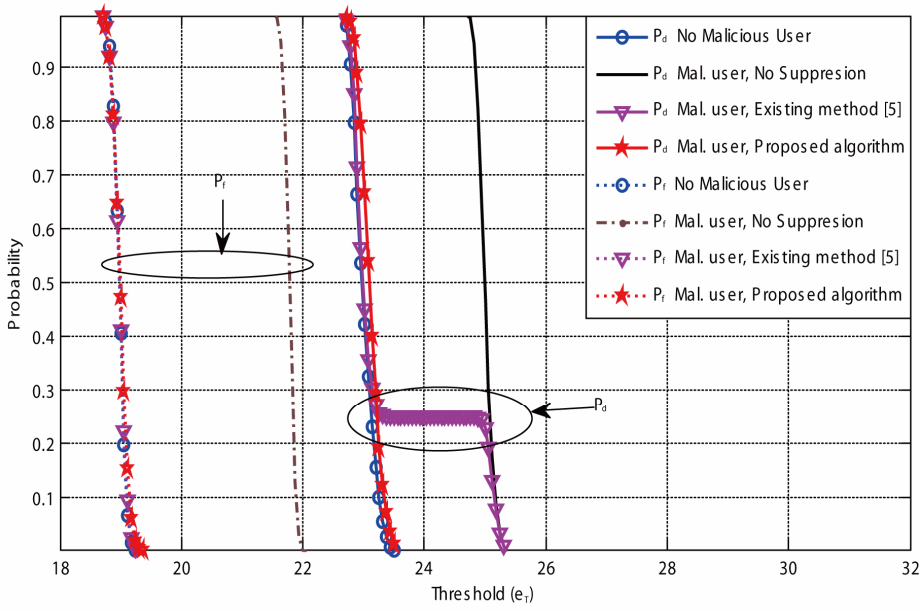

Figure 5. Probability of detection and false alarm in adversarial environment with 10 "Always Yes" malicious users.

posed in [5], the fading channel is not considered. By applying the fading effects to this scheme, due to its filtering structure, some malicious users affect the final decision.

In **Figure 6**, we observe the probability of detection according to the number of "Always No" malicious users. From this figure, we can see that our proposed algorithm is more robust than traditional ones. Our algorithm is robust until 50% of the secondary users become malicious and has a better performance compared to that of [5].

In **Figure 7**, we observe the probability of false alarm with varying the number of "Always Yes" malicious users. As shown in the figure, our algorithm with effective malicious user detection can achieve an acceptable performance.

5. Conclusions

In this paper, a new cooperative secure spectrum sensing

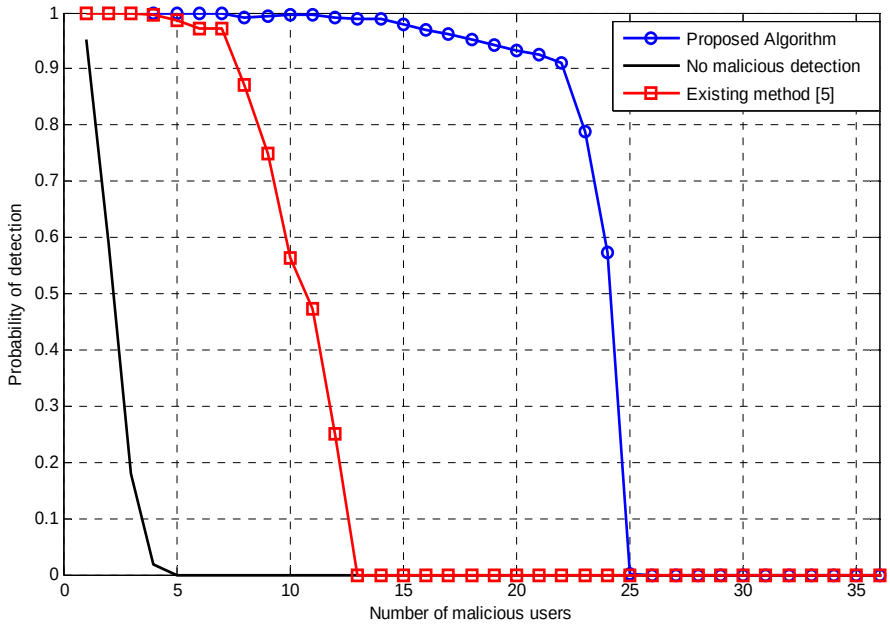

Figure 6. Probability of Detection with varying the number of "Always No" malicious users.

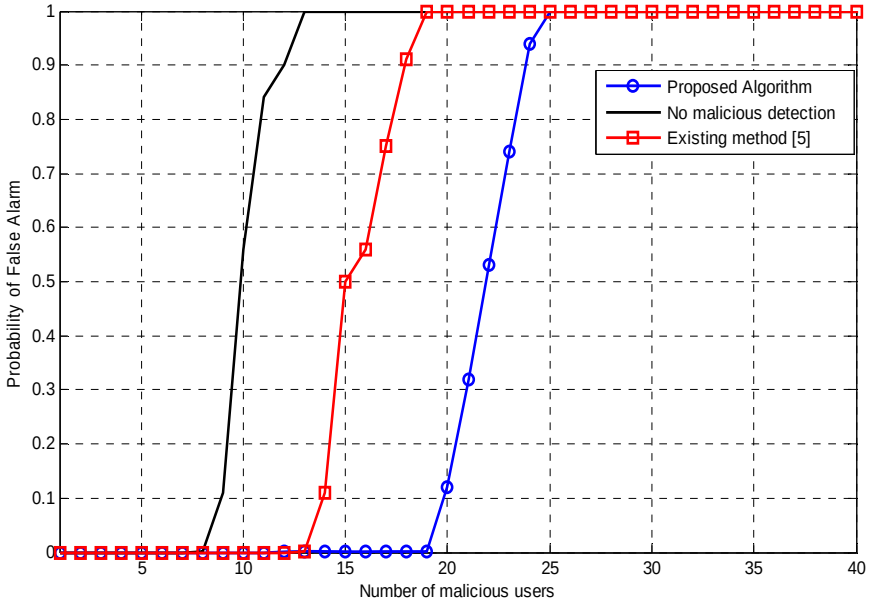

Figure 7. Probability of False Alarm with varying the number of "Always Yes" malicious users.

algorithm for malicious user detection in cognitive radio networks based on fuzzy logic was proposed. In our proposed secure sensing algorithm, first a pre-filtering is designed to prevent the users, whose sensing results are far from the others, take effect on final decision. Then, based on the results of the filter output, the fuzzy parameters are obtained, and then according to fuzzy parameters, a fuzzy trust level is assigned to each user. Finally, the sensing results are combined in the fusion center based on their fuzzy trust levels. Simulation results show that our proposed algorithm can significantly nullify the effects of malicious users. Moreover, it can alleviate the effect of fading channels. Furthermore, the complexity of our proposed algorithm is much lower than those of existing ones. In future work, we will develop our secure spectrum sensing algorithm for the case of using cyclostationary detectors (rather than energy detectors used in this paper) and for more complex scenarios.

6. Acknowledgements

The authors would like to thank the Iranian Institute of information and Communication Technology (the former ITRC) for the financial support of this work.

7. References

[1] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 2, 2005, pp. 201-220. doi:10.1109/JSAC.2004.839380

[2] S. M. Kay, "Fundamentals of Statistical Signal Processing: Detection Theory," Prentice Hall, Upper Saddle River, 1998.

[3] H. V. Poor, "An Introduction to Signal Detection and Estimation," Springer-Verlag, New York, 1994.

[4] S. Enserink and D. Cochran, "A Cyclostationary Feature Detector," *Proceedings of the* 28*th Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, 31 October-2 November 1994, pp. 806-810. doi:10.1109/ACSSC.1994.471573

[5] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio System," *IEEE International Conference on Communications*, Beijing, 19-23 May 2008, pp. 3406-3410.

[6] B. Shen and K. S. Kwak, "Soft Combination Schemes for Cooperative Spectrum Sensing in Cognitive Radio Networks," *ETRI Journal*, Vol. 31, No. 3, 2009, pp. 263-270. doi:10.4218/etrij.09.0108.0501

[7] D. Cabric, S. M. Mishra and R. W. Brodersen, "Implementation Issues in Spectrum Sensing for Cognitive Radios," *Proceedings of* 38*th Asilomar Conference on Signals, Systems, Computers*, Pacific Grove, 7-10 November 2004, pp. 772-776.

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

[9] K. J. Peng and Z. H. Tsai, "A Distributed Spectrum Sensing Scheme Based on Credibility and Evidence Theory in Cognitive Radio," *Proceedings of the* 17*th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Helsinki, 11-14 September 2006, pp. 1-5. doi:10.1109/PIMRC.2006.254089

[10] N.-T. Nhan and I. Koo, "A Secure Distributed Spectrum Sensing Scheme in Cognitive Radio," *Proceedings of the Intelligent Computing* 5*th International Conference on Emerging Intelligent Computing Technology and Applications*, Vol. 5755, 2009, pp. 698-707.

[11] S. Y. Xu, Y. L. Shang and H. M. Wang, "Double Thresholds Based Cooperative Spectrum Sensing against Untrusted Secondary Users in Cognitive Radio Networks," *IEEE International Vehicular Technology Conference*, Barcelona, 26-29 April 2009, pp. 1-5.

[12] W. K. Wang, H. S. Li, Y. Sun and Z. Han, "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks," *IEEE Annual Conference on Information Sciences and Systems*, Baltimore, 18-20 March 2009, pp. 130-134.

[13] E. MoeenTaghavi and B. Abolhassani, "Trustworthy Node Detection in Cognitive Radio in Hostile Environments," *International Conference on Communication and Electronics Information*, Vol. 2, 2011, pp. 258-262.

[14] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Malicious User Detection in a Cognitive Radio Cooperative Sensing System," *IEEE Transaction on Wireless Communications*, Vol. 9, No. 8, 2010, pp. 2488-2497.

[15] L. A. ZADEH, "Fuzzy Sets," *Information and Control*, Vol. 8, No. 3, 1965, pp. 338-353. doi:10.1016/S0019-9958(65)90241-X

[16] L. A. ZADEH, "Fuzzy Algorithms," *Information and Control*, Vol. 12, 1968, pp. 94-102. doi:10.1016/S0019-9958(68)90211-8

[17] W. El-Hajj, F. Aloul, Z. Trabelsi and N. Zaki, "On Detecting Port Scanning Using Fuzzy Based Intrusion Detection System," *International Conference on Wireless Communications and Mobile Computing*, Crete Island, 6-8 August 2008, pp. 105-110.

