2011 International Conference on Computer Communication and Management
Proc .of CSIT vol.5 (2011) © (2011) IACSIT Press, Singapore

A Fuzzy Secure Spectrum Sensing (F3S) Scheme for Cognitive Radios in Adversarial Environment

Ehsan MoeenTaghavi [1], Bahman Abolhassani [2]

School of electrical engineering, Iran University of science and technology, Tehran 16846, Iran
[1] emtaghavi@elec.iust.ac.ir, [2] abolhassani@iust.ac.ir

Abstract. Most existing schemes for cooperative spectrum sensing are typically vulnerable to attacks made by malicious users who transmit false sensing data. To nullify this effect, we propose a Fuzzy Secure Spectrum Sensing (F3S) scheme in which fuzzy logic is employed to identify malicious users. We further propose a Fuzzy Trust Level and Suspicious Level of each user based on fuzzy logic. Sensing information from secondary users is incorporated into cooperative sensing based on their fuzzy trust level, which increases robustness of cooperative sensing. Simulation results verify the effectiveness of our proposed scheme.

Keywords: Cognitive radio, secure spectrum sensing, Fuzzy logic, Fuzzy trust level.

1. Introduction

Traditionally, spectrum bands have been assigned to a specific service for a long time in geographical regions. This policy has led to inefficient spectrum usage. This inefficiency and the limited availability of spectrum caused cognitive radio networks to be proposed [1]. In cognitive radio networks, secondary (unlicensed) users can use licensed spectrum bands when it is idle and make the bands vacant as soon as primary (licensed) user returns. Spectrum sensing is essential for identifying vacant spectrum and for prompt evacuation of spectrum as soon as a primary user returns.

Spectrum sensing techniques include energy detection, cyclostationary feature detection and matched filter detection. Among them, energy based detection is the most popular due to less complexity [2]. It is shown that the received signal strength could be seriously weakened due to multi path fading or shadowing effect. Cooperative spectrum sensing aims at achieving a higher performance than that of a single user sensing [3]. However, in cooperative sensing, due to imperfect channel between a primary user (PU) and a secondary user (SU) or dishonestly of a SU, a user might send false sensing results to the fusion center (FC). So, the performance of the system degrades severely. To overcome this problem, secure spectrum sensing has been proposed.

The authors in [4] 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 [6], a defence scheme that computes suspicious level and trust value of the users is proposed. In [7], a robust secure spectrum sensing based on reliability evaluation stage from previous performance of each user is proposed. In our previous work [8], malicious user detection based on outlier energy detection techniques is proposed and a filtering based on statistical parameters of sensing results is used to eliminate the effects of malicious users. In this paper, we propose using fuzzy logic in cooperative sensing to dedicate both suspicious level and trust level to users based on their past and present sensing results. To eliminate the effects of malicious users, we propose a weighted combining method to make final decision in the fusion center. The weighting of each user is based on its Fuzzy trust level. Simulation results show that our propose method outperforms the existing one when the ratio of malicious users increases with less complexity.

The rest of the paper is organized as follows: Section 2 introduces system model and gives a background about fuzzy logic. In Section 3, our new technique to nullify malicious users using fuzzy logic is proposed. Simulation results are illustrated in Section 4. Finally, a conclusion is drawn in Section 5.

2. System Description

2.1. System model

We discuss a cognitive radio network composed of one primary user and a group of N secondary users. An independent and identically distributed (i.i.d) lognormal shadowing fading channel between a primary user and each secondary user is assumed. Variation in path loss is neglected. Each SU conducts energy detection and transmits the received signal power in perfect control channel to fusion center. Based on combination of the sensing results from different SU, the fusion center makes the final decision regarding the presence or absence of the PU.

If $e_n[k]$ for $n=1,2,...,N$ represents the received signal power of n^{th} SU at time instant k and hypotheses H_1 and H_0 denote the presence and absence of a primary signal respectively, then the signal power received by n^{th} SU is given by:

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

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

Cooperative spectrum sensing in adversarial environments where a malicious user sends false sensing data, degrade the performance of the system severely. In adversarial environments, different kinds of malicious user can affect the 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. Another kind of malicious users is the one which always send data indicating the absence of the primary user ("Always no" malicious users). This kind of malicious users causes the interference among primary and secondary user's signal [9]. In this paper, we propose a Fuzzy secure spectrum sensing (F3S) scheme to dedicate each user a Fuzzy trust level based on their trust level. In the proposed scheme, users more reliable are assigned with a higher trust level. This scheme also detects those users who are suspicious to be malicious with their corresponding suspicious levels using fuzzy logic.

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 scheme integrates fuzzy logic with spectrum sensing in order to better detect malicious users.

Fuzzy logic provides a simple way to get definite conclusion and solution based on Fuzzy input information. 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 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 [10]. In the next section, we present details of the fuzzy logic that we use in F3S scheme.

3. Proposed F3S Scheme

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 1 shows the 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 2. 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.

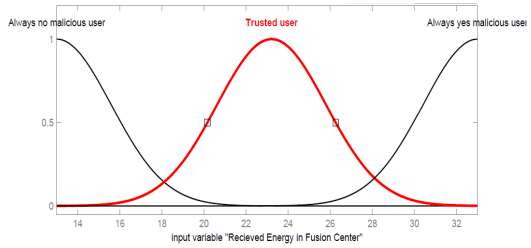

Figure 1. Membership functions of an input parameter

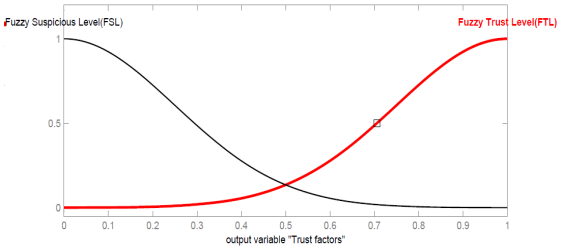

Figure 2. Membership functions of output

The output of the system shows the trust and suspicious levels of each user. These users whose their sensing results are near the median of the sensing results are assigned with higher trust levels and those users whose their 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 follow:

$$FTL_n[k] = \frac{FTL'_n[k]}{\sum_{n=1}^{N} FTL'_n[k]}. \qquad (2)$$

where N denotes the number of users.

Then, the final decision is computed using FTLs of all N users as follows:

$$\sum_{n=1}^{N} FTL_n[k]e_n[k] \underset{H_0}{\overset{H_1}{>}} e_T. \qquad (3)$$

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 scheme, the suspicious users who are malicious or their sensing results are affected by fading are assigned with lower fuzzy trust levels, so their effects in the final decision are not considered.

To achieve a better performance, the sensing results of each user over a certain period L 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:

$$FTL_n[k] = \sum_{l=0}^{L-1} (L-l)FTL'_n[k-l). \qquad (4)$$

Finally, these weighted fuzzy trust levels are normalized according to equation (2).

By considering previous and present behaviours 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

We consider a group of N=50 secondary users. The mean received SNR of the channel between primary user and each of secondary users is 2 dB. Independent and identically distributed small scale fading channels are considered between any secondary user and the primary user, and the path loss is neglected.

In Fig. 3, 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 F3S scheme, we compare probability of detection (P_d) and probability of false alarm (P_f) of our F3S scheme 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 Fig. 3 we can see that using the F3S scheme, 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. It is notable that the P_f of our proposed F3S scheme is about zero for e_T values larger that 18, while the P_f of no malicious user case is always worse than that of our F3S. This is due to alleviating the fading channel in our F3S scheme in addition to detecting malicious users.

In Fig. 4, unlike Fig. 3, we consider a sensing system in which 10 users always announce the presence of the primary user to the fusion center. From Fig. 4 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.

In Fig. 5, we observe the probability of detection according to the number of "Always no" malicious users. From the figure, we can see that our proposed scheme is more robust than traditional ones. This scheme is robust until 50% of the secondary users become malicious and has a better performance compared to that of [5].

In Fig. 6, the effect of "Always yes" malicious users is also considered. Similar to previous cases, our scheme with effective malicious user detection can achieve an acceptable performance.

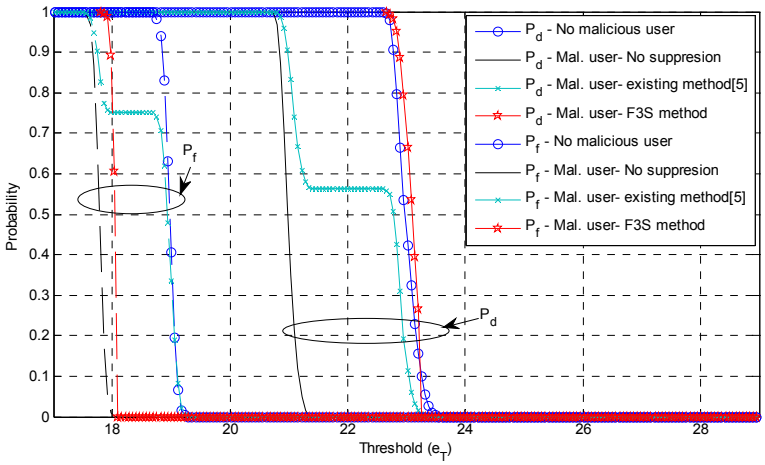

Figure 3. Probability of detection and false alarm in adversarial environment with 10 "Always no" malicious users.

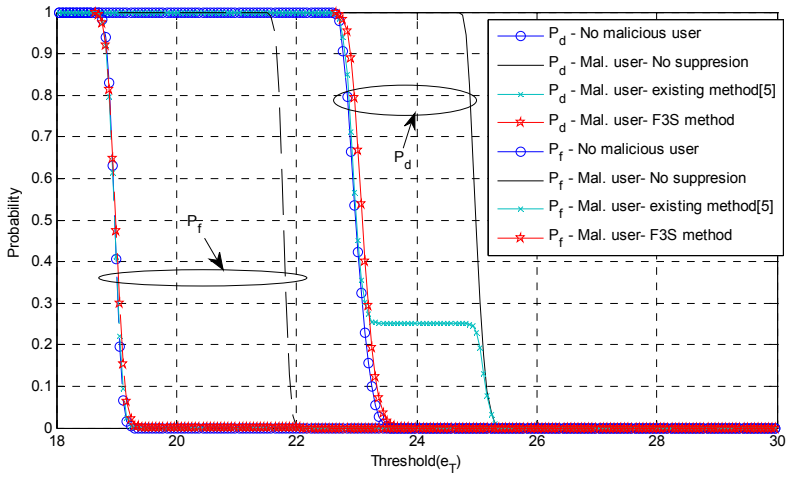

Figure 4. Probability of detection and false alarm in adversarial environment with 10 “Always yes” malicious users.

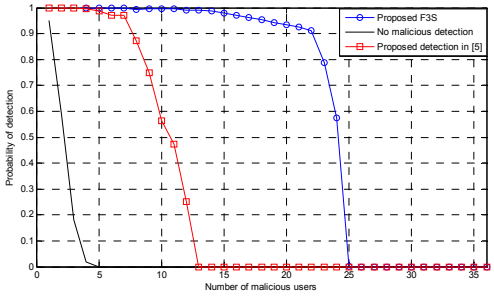

Figure 5. Probability of detection with varying the number of “Always no" malicious users.

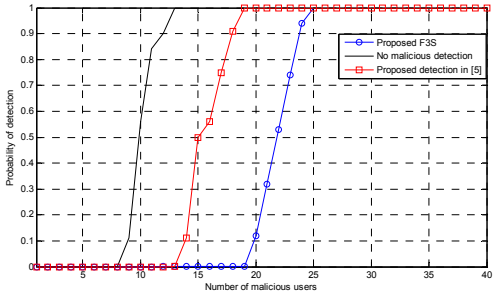

Figure 6. Probability of false alarm with varying the number of "Always yes" malicious users.

5. Conclusion

In this paper, a new cooperative secure spectrum sensing for malicious user detection in cognitive radio networks based on fuzzy logic was proposed. In our proposed F3S scheme, based on the sensing results, 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 scheme can significantly nullify the effects of malicious users. Moreover, it can alleviate the effect of fading channels. Furthermore, the complexity of our proposed scheme is much lower than those of existing ones. In future work, we will develop the F3S scheme for the case of using cyclostationary detectors (rather than energy detectors used in this paper) and for more complex scenarios.

6. Acknowledgements

This research is partially funded by the Iranian Institute of information and Communication Technology (the former ITRC).

7. References

[1] S. Anand, Z. Jin, and K.P. Subbalakshmi,” Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing “, ACM SIGMOBILE Mobile Computing and Communications Review, Volume 13, pp. 74-85, 2009.

[2] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, “NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey,” Elsevier Jl. on Computer Networks, vol. 50, no. 13, pp. 2127–2159, 2006.

[3] A. Ghasemi, E. S. Sousa. "Collaborative spectrum sensing for opportunistic access in fading environment", IEEE International Symposia on New Frontiers in Dynamic Spectrum Access Networks, pp. 131–136, 2005.

[4] S. Xu, Y. Shang, H. Wang, “Double thresholds based cooperative spectrum sensing against untrusted secondary users in cognitive radio networks”, IEEE Int. Vehicular Technology Conference, pp. 1-5, 2009.

[5] P. Kaligineedi, M. Khabbazian, V.K. Bhargava, “Secure cooperative sensing techniques for cognitive radio system”, IEEE Int. Conf. Commun. (ICC), pp. 3406-3410, 2008.

[6] W. Wang, H. Li, Y. Sun, Z. Han, “Attack-Proof collaborative spectrum sensing in cognitive radio networks”, IEEE Annual Conf. on Information Sciences and Systems (CISS), pp. 130-134, 2009.

[7] N. Nhan, I. Koo, “ A secure distributed spectrum sensing scheme in cognitive radio”, Springer-Verlag Berlin Heidelber, volume 5755, pp. 698-707, 2009.

[8] E. MoeenTaghavi, B. Abolhassani, “Trustworthy node detection in cognitive radio in hostile environments”, International Conference on Communication and Electronics Information, Vol. 2, pp. 258-262, 2011.

[9] P. Kaligineedi, M. Khabbazian, V.K. Bhargava, “Malicious user detection in a cognitive radio cooperative sensing system”, IEEE Trans. on wireless communications, Vol. 9, No. 8, pp. 2488-2497, 2010.

[10] El-Hajj, W.; Aloul, F.; Trabelsi, Z.; Zaki, N. ,” On Detecting Port Scanning using Fuzzy Based Intrusion Detection System “,International Conference on wireless Communications and Mobile Computing, pp. 105-110, 2008.