Trustworthy Node Detection in Cognitive Radio in Hostile Environments

Ehsan Moeen Taghavi and Bahman Abolhassani

Abstract—**The most important challenge in cognitive radio networks is detection of primary user signal. Cooperation among secondary users increases the performance of the system significantly. In cooperative sensing in hostile environments, intruder nodes send false sensing results to the fusion center and make the fusion center erroneously decides about the presence of the primary user. Several detection methods have been proposed to nullify effects of malicious nodes. But in most of these scenarios, the fading effects are not considered. In this paper, we propose a method to identify trustworthy nodes in hostile environments, considering fading effects. We introduce a modified filtering method to reduce the effects of malicious nodes. We also propose new trust factors to be assigned to the nodes for increasing the effects of trustworthy nodes in the final decision.**

Index Terms—**Cognitive radio, cooperative spectrum sensing, energy detector, trustworthy nodes detection.**

I. Introduction

With increasing demand for wireless communications, efficient utilization of spectrum becomes very important. Cognitive radio is a new approach for improving the spectrum utilization by making it possible for secondary (unlicensed) users to access spectrum bands when primary (licensed) user is absent [1].

In cognitive radio networks (CRNs), secondary users sense spectrum continuously and as soon as find an occupied band, it starts transmitting in this band, and by finding a primary signal, to prevent interference, make spectrum vacant. So, the most important challenge in CRNs is primary user detection, which is performed by spectrum sensing. Popular sensing techniques include matched filter, energy detection, cyclostationary detection and wavelet detection. Among them, energy detection method requires the minimum prior knowledge on primary user signal and it's optimal for detecting independent identically distributed (i.i.d) signals [2]. In spectrum sensing, two probabilities are considered: probability of miss detection (Pmiss) and the probability of false alarm (Pf). Pmiss is the probability of declaring that the channel is vacant while the primary user is present. Pf is the probability of declaring the channel is occupied by a primary user while the primary user has no transmission.

A sensing device could send false sensing results due to fading channel or shadowing, which cause increasing miss detection probability and degrading performance of the system. To solve this problem and to increase performance of the system, cooperation among secondary nodes (users) in spectrum sensing is used. In cooperative sensing, each user sends its sensing result to a fusion center. Based on the sensing results received from different nodes, the fusion center makes final decision about the presence or absence of the primary user.

Presences of malicious nodes which intentionally send false sensing results to the fusion center degrade considerably performance of the system. In [2-8], different methods for malicious node detection have been proposed. The author in [2], proposed the majority rule in the fusion center to reduce effects of malicious nodes. In [3], a scheme for identifying malicious users based on outlier detection techniques employing energy detection was proposed. But fading effect was ignored. A defense scheme that computes suspicious level and trust values of the nodes was proposed in [4]. In [5], a robust distributed spectrum sensing to degrade effects of malicious nodes was proposed. In [6], a local decision is made by each secondary user and in the fusion center these local decisions are combined with weighted combining method based on their reliabilities. In this paper, we investigate a technique to degrade the effects of malicious user in cooperative spectrum sensing considering fading effects. In our proposed method, with increasing the number of malicious users, the performance still remains in an acceptable level.

The rest of this paper is organized as follows: in Section II, system model is defined. In Section III, our new technique for detecting and nullifying malicious users is proposed. Simulation results are presented in Section IV. Finally, conclusions are drawn in Section V.

II. System Model

We consider a group of N secondary users in the presence of a primary transmitter. We assume independent log-normal shadowing and fading for the channel between the primary transmitter and each secondary user. Variation in the path-loss is neglected. All secondary nodes use energy detectors. We assume that the sensing device can distinguish the signal of the primary user from the others. The secondary users send their sensing data to the fusion center through control channels, which assumed to be perfect. Based on the sensing results received from different secondary users, the fusion center makes a decision regarding the presence of the primary user.

If $e_n[k]$ for $n=1,2,\ldots,N$ represents the output of energy detector of n^{th} secondary user at time instant k, and

Manuscript received August 15, 2012; revised October 12, 2012.

The authors are with the the School of electrical engineering Iran University of science and technology, Tehran 16846, Iran (e-mail: emtaghavi@Elec.iust.ac.ir, abolhassanii@iust.ac.ir).

hypotheses H_1 and H_0 denote the presence and absence of primary signal, respectively, then the output of energy detector for n^{th} user is given by:

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

where T denotes the length of the sensing interval, $s(t)$ is the primary transmitted signal, $h_n(t)$ represents the channel voltage gain between the primary transmitter and the n^{th} secondary user, $z_n(t)$ is the additive white Gaussian noise (AWGN) with one-sided power spectral density N_0.

The presence of malicious users affects the performance of the system severely. A user might be malicious for selfish reasons. For example, a malicious user might detect the primary signal is absent; nevertheless, it might send false data that show the presence of primary signal to the fusion center (FC). So, the FC erroneously decides that the primary signal is present. Then the malicious user selfishly uses entire free spectrum band.

Different kinds of malicious nodes can affect sensing system. They may always send data indicating the presence of the primary signal to the FC ("always yes" nodes). These kind of malicious nodes increase false alarm probability (P_f) and cause the FC prohibits other secondary users from accessing the vacant spectrum. So, the performance of the system is degraded. Another kind of malicious nodes is the one in which they always send data indicating the absence of the primary signal ("always no" nodes). These malicious users degrade performance of the system and cause the interference among primary and secondary user's signal [9]. In our proposed method, malicious nodes which their sensing results are much different from the others are detected and their sensing results are removed before making the final decision.

III. Proposed Method for Malicious Node Detection

By filtering and removing sensing results of malicious nodes, performance of the system can be compensated to some extent. In our proposed method, the sensing results which are numerically distant from the rest of the results are not considered in the final decision. By removing them before making the final decision the author in [3], have filtered the sensing data. The upper bound ($e_u[k]$) and lower bound ($e_l[k]$) of the filtering are as follows:

$$\begin{cases}e_u[k]=e_{3/4}[k]+3e_{iq}[k],\\ e_l[k]=e_{1/4}[k]-3e_{iq}[k],\end{cases} \quad (2)$$

where $e_{iq}[k]=e_{3/4}[k]-e_{1/4}[k]$ and $e_{1/4}[k]$ and $e_{3/4}[k]$ represent the first and third quartile of values $e_n[k]$.

If a particular value of $e_n[k]$ is in the interval $[e_l[k],e_u[k]]$, the n^{th} secondary user will be considered as a non-malicious node. As mentioned, fading effects were ignored in [3]. If we consider fading effects, the sensing results will numerically distant from each other. So $e_{iq}[k]$ would become larger. Therefore, despite of filtering, some malicious users affect final decision. To solve this problem, we propose new upper and lower bounds in filtering so that malicious nodes will be removed. If we use the median ($med[k]$) and standard deviation ($\sigma[k]$) of energy value of sensing results in the computation of upper and lower bounds, at time instant k, we will have less vulnerable sensing method to fading effects and malicious nodes in filtering. In this paper, we evaluate upper and lower bounds for values $e_n[k]$ as follow:

$$\begin{cases}e_u[k]=med[k]+1.5\sigma[k],\\ e_l[k]=med[k]-1.5\sigma[k].\end{cases} \quad (3)$$

In our proposed outlier detection technique, by increasing the number of malicious nodes, unlike proposed method in [3], the performance still remains acceptable.

A. Trust Factor Computation

Although filtering removes most malicious nodes, some sensing results, which have been affected by fading or by malicious users' results, 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 node. The nodes, which have been affected by fading or are malicious, are assigned with lower trust factors. The nodes, which have a good channel condition or aren't suspicious, are assigned with higher trust factors. Trust factors are determined and normalized so that their summation becomes one, i.e.

$$\sum_{n=1}^{N} TF_n[k]=1. \quad (4)$$

Those nodes, whose sensing results are larger than the upper bound or less than the lower bound, are detected as malicious users and their trust factors are assigned to be zero, i.e.

$$If \quad \{e_n[k]<e_l[k] \,||\, e_n[k]>e_u[u]\}, \quad Then\{TF_n[k]=0\}.$$

Trust factors of the users whose sensing results are between the upper and lower bounds can be determined in different methods. The least complexity method to assign trust factor is to dedicate an equal amount of to all users where M denotes the number of users which have passed through filtering. To improve the performance of the system, trust factor of each user should be computed separately. The users with better channel conditions must be assigned higher trust factors. In this paper, we propose trust factors as follows:

$$TF_n'[k]=\begin{cases}e^{-|med[k]-e_n[k]|} & :e_l[k]<e_n[k]<e_u[k],\\ 0 & :\text{Otherwise},\end{cases} \quad (5)$$

where med[k] denotes the median of the sensing results which have passed through filtering. By increasing distant of

sensing results from the median, trust factor decreases exponentially. Finally, the trust factors are normalized.

$$TF_n[k] = \frac{TF'_n[k]}{\sum_{n=1}^{N} TF'_n[k]}. \quad (6)$$

The final decision is computed using the trust factors as follows:

$$\sum_{n=1}^{N} TF_n[k]e_n[k] \underset{H_0}{\overset{H_1}{>}} e_T. \quad (7)$$

If the value obtained in the left side of the above equation is greater than the threshold (e_T), the fusion center will announce the presence of the primary user signal.

With our proposed method, the nodes whose energy sensing results are low ("always no" nodes) or are high ("always yes" nodes), are not considered in the final decision.

For achieving a better performance, we consider sensing results of each node over a certain period L to obtain final trust factors for nodes. In computation of final trust factors, we assign more weight to those TFs which are closer to the present time, k, i.e.

$$\lambda'_n[k] = \sum_{l=0}^{L-1} (L-l)TF_n[k-l]. \quad (8)$$

Finally, these weighted trust factors, $\lambda'_n[k]$, are normalized so that the normalized weighted trust factors, $\lambda_n[k]$, is given by:

$$\lambda_n[k] = \frac{\lambda'_n[k]}{\sum_{n=1}^{N} \lambda'_n[k]}. \quad (9)$$

A larger value of L could be used to identify the nodes which have hostile behavior regularly and a smaller value of L would help to identify the nodes which behave maliciously over short periods of time.

IV. Simulation Results

We consider a cooperative sensing system with N=50 secondary users. The mean received SNR of the cognitive radio users is 2 dB. Independent and identically distributed small scale Rayleigh fading is assumed at each node. The sensing period at each node is 40 bits.simulation parameters and their values are given in Table I.

In Fig. 1, we assume a cooperative system in which 10 users are "always no" nodes, each giving a value lower than the threshold. We present the probability of miss detection (P_{miss}) and probability of false alarm (P_f) in for different cases, in case 1, there is no malicious node in the system, in the case 2, there are 10 malicious nodes but there is no way to detect them, in case 3, there is a malicious node detection which was proposed in [3] and finally in case 4, our proposed malicious detection is used. From Fig. 1-a, we can see that using our proposed malicious node detection scheme, most of "always no" nodes would be identified easily. So, the probability of miss detection (P_{miss}) of the system would be close to that of cooperative sensing of the system without any malicious node. At the same time, from Fig. 1-b, the probability of false alarm (P_f) remains close to that of cooperative sensing system without a malicious node. In addition, while the threshold varies from 20.5 to 22.5, P_{miss} of the proposed method is much better than P_{miss} of the proposed method in [3].

TABLE I: Important Simulation Parameters and Their Values

Number of secondary users	50 users
Mean received SNR	2 dB
Channel conditions	i.i.d small scale Rayleigh fading

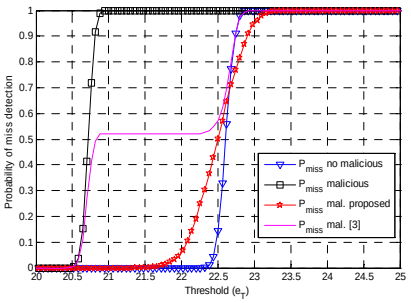

Fig. 1-a. Probability of miss detection for the case in which no malicious node in the system (P miss no malicious), 10 always no malicious nodes with no malicious detection scheme (P miss malicious), malicious node detection which was proposed in [3](P miss mal. [3]) and for the case in which our proposed malicious detection is used (P miss mal. proposed).

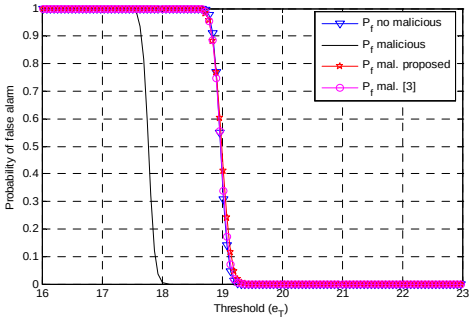

Fig. 1-b. Probability of false alarm for the case in which no malicious node in the system (Pf no malicious), 10 always no malicious nodes with no malicious detection scheme (Pf malicious), malicious node detection which was proposed in [3](Pf mal. [3]) and for the case in which our proposed malicious detection is used (Pf mal. proposed).

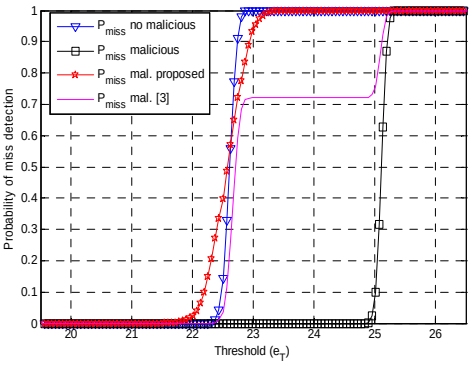

Fig. 2-a. Probability of miss detection for the case in which no malicious node in the system (P_{miss} no malicious), 10 always yes malicious nodes with no malicious detection scheme (P_{miss} malicious), malicious node detection which was proposed in [3](P_{miss} mal. [3]) and for the case in which our proposed malicious detection is used (P_{miss} mal. proposed).

In Fig. 2, unlike Fig. 1, we consider a system in which 10 users are "always yes" nodes so, they announce the presence

of the primary user signal to the FC. From Fig. 2, we can see that our proposed scheme successfully identifies most malicious nodes and nullify their effects on final decision.

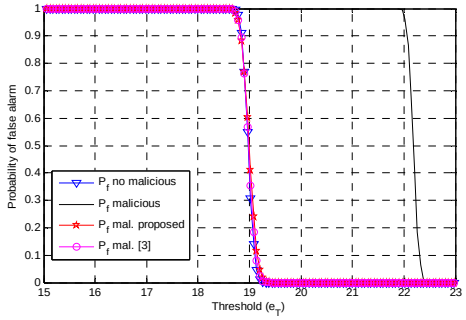

Fig. 2-b. Probability of false alarm for the case in which no malicious node in the system (P_f no malicious), 10 always yes malicious nodes with no malicious detection scheme (P_f malicious), malicious node detection which was proposed in [3](P_f mal. [3]) and for the case in which our proposed malicious detection is used (P_f mal. proposed).

In Fig. 3, we observe the probability of miss detection as we vary the number of "always no" malicious nodes from 5 to 20 with step size 5. From Fig. 3, we can see that as opposed to the results derived in [3], by increasing the number of malicious nodes the performance of the system is still acceptable.

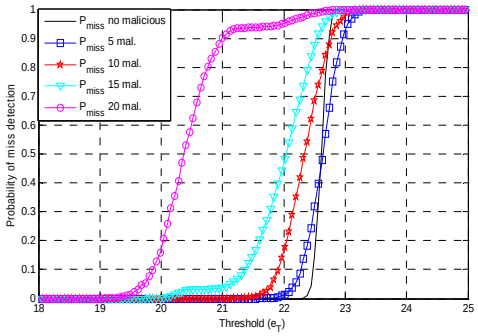

Fig. 3. Probability of miss detection of our proposed method for the case in which no malicious node in the system, and for the cases of 5,10,15,20 always no malicious nodes.

In Fig. 4, we observe the performance of the system as we vary the number of "always yes" malicious nodes from 5 to 20 with step size 5. We can see that the performance of the system doesn't degrade so much by increasing the number of malicious nodes which shows robustness of our proposed method.

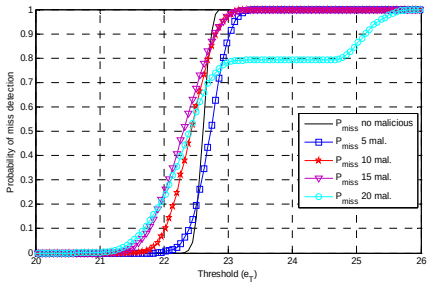

Fig. 4-a. Probability of miss detection of our proposed method for the case in which no malicious node in the system, and for the cases of 5,10,15,20 always yes malicious nodes.

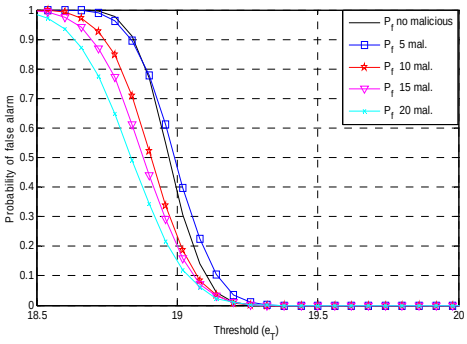

Fig. 4-b. Probability of false alarm of our proposed method for the case in which no malicious node in the system and for the cases of 5,10,15,20 always no malicious nodes.

V. Conclusions

In this paper, we proposed a method to identify and nullify the effects of malicious users for the case of spectrum sensing based on energy detectors. In our proposed method, we assign trust factors to nodes based on their channel conditions and their suspicious level of being a malicious user. In this method, the nodes with low or high value sensing results obtained from the energy detector are not considered in the final decision. In our future work, we will develop trustworthy node detection considering more complex scenarios and using intelligent algorithms for assignment of trust factors.

References

[1] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Toward a trust aware cognitive radio architecture," *ACM. Mobile Computing and Communications Review*, vol. 13, no. 2, pp. 86-95, 2009.

[2] S. Xu, Y. Shang, and 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.

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

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

[5] R. Chen, J. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," *IEEE Int. Conf. on Computer and Communications (INFOCOM)*, pp. 1876-1884, 2008.

[6] T. Zhao and Y. Zhao, "A news cooperative detection technique with malicious user suppression," *IEEE Int. Conf. Commun. (ICC)*, pp. 1-5, 2009.

[7] R. Chen, J. Park, Y.T. Hou, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Communication Magazines*, vol. 46, no. 4, pp. 50-55, 2008.

[8] F. R. Yu, H. Tang, M. Haung, Z. Lee, and P. C. Mason, "Defence against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," *IEEE Military Communications Conf. (MILCOM)*, pp. 1-7, 2009.

[9] P. Kaligineedi, M. Khabbazian, and 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.