Defense against Spectrum Sensing Data Falsification Attacks in Mobile Ad Hoc Networks with Cognitive Radios

F. Richard Yu[†], Helen Tang[§], Minyi Huang[‡], Zhiqiang Li[†] and Peter C. Mason[§]
[†]Depart. of Systems and Computer Engin., [‡]Sch. of Math. and Statistics, Carleton University, Ottawa, ON, Canada
[§]Defense R&D Canada - Ottawa, ON, Canada
Email: richard_yu@carleton.ca; helen.tang@drdc-rddc.gc.ca; mhuang@math.carleton.ca; zlia@sce.carleton.ca; peter.mason@drdc-rddc.gc.ca

Abstract - Cognitive radios (CRs) have been considered for use in mobile ad hoc networks (MANETs). The area of security in Cognitive Radio MANETs (CR-MANETs) has yet to receive much attention. However, some distinct characteristics of CRs introduce new, non-trivial security risks to CR-MANETs. In this paper, we study spectrum sensing data falsification (SSDF) attacks to CR-MANETs, in which intruders send false local spectrum sensing results in cooperative spectrum sensing, and SSDF may result in incorrect spectrum sensing decisions by CRs. We present a consensus-based cooperative spectrum sensing scheme to counter SSDF attacks in CR-MANETs. Our scheme is based on recent advances in consensus algorithms that have taken inspiration from self-organizing behavior of animal groups such as fish. Unlike the existing schemes, there is no need for a common receiver to do the data fusion for reaching the final decision to counter SSDF attacks. Simulation results are presented to show the effectiveness of the proposed scheme.

I. Introduction

The trend in wireless communications is such that advances demand ever increasing, and more efficient, use of limited spectrum resources. Regulatory agencies, such as the Federal Communication Commission (FCC), are considering opening up licensed (primary) bands to unlicensed (secondary) operations on a non-interference basis to licensed users. One way to realize this is to adopt the idea of Cognitive Radio (CR) [1], which is capable of sensing its surrounding environment and adapting its internal states by making corresponding changes in certain operating parameters [2]. CR technologies have been considered in mobile ad hoc networks (MANETs) [3], which enable wireless devices to dynamically establish networks without necessarily using a fixed infrastructure. In such a self-organized network, each node can pass information and control packets from one neighbor to another. MANETs are gaining importance with the increasing number of potential applications, such as military battle field communications, disaster relief, and autonomous vehicular communications.

Since primary user networks have no requirement to change their infrastructure for spectrum sharing, the task falls upon CRs as secondary users in MANETs to detect the presence of primary users through continuous spectrum sensing. Spectrum sensing by CRs can be conducted either individually or cooperatively. Recently, the efficacy of cooperative spectrum sensing has garnered a great deal of attention. There are several advantages offered by cooperative spectrum sensing over non-cooperative methods [4]–[8].

Although some security work has been done in CR technologies, the area of security in CR-MANETs has received relatively little attention [3], [9]. Compared to wired networks, MANETs are inherently less secure because of the lack of any central authority. Certainly, threats to non-cognitive wireless networks in general are still of interest in the CR paradigm. However, some distinct characteristics of CRs introduce new non-trivial security risks to CR-MANETs. For example, locally-collected and exchanged spectrum sensing information is used to construct a perceived environment that will impact CR behavior. This opens opportunities to malicious attackers. Two known security threats in CRs are Incumbent Emulation (IE) and Spectrum Sensing Data Falsification (SSDF) [9]. In an IE attack, intruders emulate signals with the characteristics of incumbent primary users to fool other secondary users. IE attacks can severely interfere with the spectrum sensing process and significantly reduce the channel resources available to authentic secondary users. A transmitter verification scheme is proposed in [10] to identify such IE attacks. In an SSDF attack, intruders send false local spectrum sensing results, which will result in suspect spectrum sensing decisions by CRs. Authors in [9] suggest several

978-1-4244-5239-2/09/$26.00 ©2009 IEEE

approaches for countering SSDF attacks using a common receiver for data fusion. However, no further development is reported for MANETs where a central data fusion center may not be practical.

In this paper, we present a consensus-based cooperative spectrum sensing scheme to counter SSDF attacks in CR-MANETs. Recently, bio-inspired mechanisms have become important approaches to handle complex communication networks [11], [12]. Our scheme is based on recent advances in bio-inspired consensus algorithms [13]. Collective animal behavior has motivated many effective yet simple control algorithms for the coordination of multi-agent systems in engineering. Recently, consensus problems have played a crucial role in spacial distributed control models [14], wireless sensor networks [15], and stochastic consensus seeking with noise measurement [16]. Since these algorithms are usually constructed based on local communication of neighboring agents, they have low implementational complexity and good robustness, and the overall system may still function when local failure occurs. Concerning our secure spectrum sensing models, the basic requirement is for the secondary users to collectively filter out falsified data inserted by SSDF attacks and make the correct decision about the presence of primary users, which can be viewed as a typical multi-agent coordination situation. The contributions of this work are as follows.

Extensive simulation results illustrate the effectiveness of the proposed scheme by showing significant improvement in identifying and preventing SSDF attacks. It can also assure that both miss detection probability and false alarm probability are kept below desired levels.

The rest of the paper is organized as follows. Section II presents spectrum sensing and SSDF attack models. In Section III, the consensus-based scheme is presented to counter SSDF attacks. Some simulation results are given in Section IV. Finally, we conclude this study in Section V.

II. Spectrum Sensing and SSDF Attack Models

In this section, we first present the spectrum sensing and SSDF attack models. Then we introduce the network model and consensus notations used in this paper.

A. Spectrum Sensing Model

For many years radio spectrum has been assigned to licensed (primary) users. Most of the time, some frequency bands in the radio spectrum remain largely unoccupied by primary users. Spectrum usage measurements by the FCC show that at any given time and location, most of the spectrum is actually idle. That is, the spectrum shortage results from the spectrum management policy rather than a paucity of usable spectrum. CR is considered an enabling technology that allows unlicensed (secondary) users to operate in the licensed spectrum bands. One important application of CR is spectrum overlay dynamic spectrum access (DSA), where secondary users operate in the licensed band while limiting interference with primary users. Spectrum opportunities are detected and used by secondary users in the time and frequency domain [17]. Three kinds of methods are widely used for spectrum sensing [18]. The first, *matched filter* is optimal theoretically, but it needs prior knowledge of the primary system, which means higher complexity and cost to develop adaptive sensing circuits for different primary wireless systems. A second method, *energy detection* is suboptimal, but it is simple to implement and does not rely on the position of primary users. Finally, *cyclostationary feature detection* can detect signals with very low signal-to-noise ratio (SNR), but it still requires some prior knowledge of the primary user [19].

In this paper, we consider a modeling scenario where their is no prior knowledge of the primary user. For implementation simplicity, an energy detection spectrum sensing method [8] is used. Fig. 1 shows the block-diagram of an energy detector. The input bandpass filter selects the center frequency f_s and the bandwidth of interest W. This filter is followed by a squaring device to measure the received energy and an integrator that determines the observation interval T. Finally, the output of the integrator Y is compared with a threshold λ to decide if the primary user signal is present. The goal of spectrum sensing is to decide between the following two hypotheses,

$$x(t) = \begin{cases} n(t), & H_0 \\ h \cdot s(t) + n(t), & H_1 \end{cases} \tag{1}$$

where $x(t)$ is the signal received by secondary user, $s(t)$ is primary user's transmitted signal, $n(t)$ is the additive white Gaussian noise (AWGN) and h is the amplitude gain of the channel. We also denote by γ the SNR. The output of integrator in Fig. 1 is Y, which serves as the decision statistic. Following the work of [20], Y can be shown to have the following distribution,

$$Y = \begin{cases} X^2_{2TW}, & H_0 \\ X^2_{2TW}(2\gamma), & H_1 \end{cases} \tag{2}$$

where X^2_{2TW} and $X^2_{2TW}(2\gamma)$ denote random variables with central and non-central chi-square distributions, respectively, each with $2TW$ degrees of freedom and a non-centrality parameter of 2γ for the latter distribution. For simplicity we assume that time-bandwidth product, TW, is an integer number, which is denoted by m.

Under Rayleigh fading, γ would have an exponential distribution, so in this case the average SNR ($\overline{\gamma}$) is used instead. In addition, h is not deterministic. Therefore,

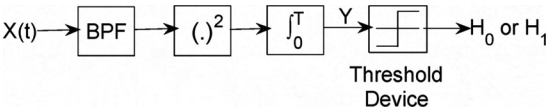

Fig. 1. Block diagram of an energy detector.

according to [21],

$$Y = \begin{cases} X^2_{2TW}, & H_0 \\ X^2_{(2TW-2)} + e_{(2\overline{\gamma}+2)}, & H_1 \end{cases} \quad (3)$$

where $e_{(2\overline{\gamma}+2)}$ is a random variable having the exponential distribution with parameter $(2\overline{\gamma}+2)$ and $X^2_{(2TW-2)}$ is a random variable with non-central chi-square distribution with $(2TW-2)$ degree of freedom.

As a summary, after T, each secondary user i detects the energy and gets the estimated energy level $Y_i \in \mathbb{R}^+$.

B. SSDF Attack Models in Cooperative Spectrum Sensing

In cooperative spectrum sensing, a group of secondary users perform spectrum sensing by collaboratively exchanging locally-collected information. Malicious secondary users may take advantage of the cooperative spectrum sensing and launch SSDF attacks by sending false local spectrum sensing results to others, resulting in a wrong spectrum sensing decision. Three attack models are presented as follows.

In the first attack model, a malicious secondary user reports the existence of a relatively high primary user energy so that other secondary users conclude that primary users are present and they will not use the spectrum. The intention of the malicious secondary user is to gain the exclusive access to the target spectrum. We denote this kind of attack a *Selfish SSDF*. In the second attack model, a malicious secondary user falsely reports a relatively low primary user energy. In this case, other secondary users wrongly conclude that there is no primary user and they will use the spectrum. The intention of the malicious secondary user is either to cause interference to primary users or inhibit the communication of other secondary users. We denote this attack as an *Interference SSDF*. In the third attack model, a malicious secondary user reports at random a true or false value for the primary user energy. That is, sometimes, it sends out a correct primary user energy; sometimes, it sends out a false value. The intention of the malicious secondary user is to confuse other secondary users so that consensus can be reached. We denote this attack as a *Confusing SSDF*.

As an important line of defense, an authentication scheme can be used to help protect CR-MANETs in cooperative spectrum sensing. However, the experience in security of traditional wireless networks indicates that there are always weak points in the system that are hard to predict, no matter what is used for authentication. Therefore, it would be prudent to emply multi-level protection mechanisms for CR-MANETs, especially considering the low physical security of mobile devices. To mitigate these SSDF attacks, we will apply recent advances in consensus algorithms in cooperative spectrum sensing. The network model and consensus notions will be introduced as follows.

C. The Network Model and Consensus Notions

In our spectrum sensing scheme, secondary users establish communication links with their neighbors to locally exchange information among them. The network formed by the secondary users can be described by a standard graph model. For simplicity, this can be represented by an undirected graph (to be simply called a graph) $\boldsymbol{G} = (\mathcal{N}, \mathcal{E})$ [22], [23] consisting of a set of nodes $\{i = 1, 2, \cdots, n\}$ and a set of edges $\mathcal{E} \subset \mathcal{N} \times \mathcal{N}$. Denote each edge as an unordered pair (i, j). Thus, if two secondary users are connected by an edge, it means they can mutually exchange information. A path in $\boldsymbol{G}$ consists of a sequence of nodes $i_1, i_2, \cdots, i_l,\ l \geq 2$, such that $(i_m, i_{m+1}) \in \mathcal{E}$ for all $1 \leq m \leq l-1$. The graph $\boldsymbol{G}$ is connected if any two distinct nodes in $\boldsymbol{G}$ are connected by a path. For convenience of exposition, we often refer node i as secondary user i. The two names, secondary user and node, will be used alternatively. The secondary user j (resp., node j) is a neighbor of user i (resp., node i) if $(j, i) \in \mathcal{E}$ where $j \neq i$. Denote the neighbors of node i by $\mathcal{N}_i = \{j | (j, i) \in \mathcal{E}\} \subset \mathcal{N}$. The number of elements in $\mathcal{N}_i$ is denoted by $|\mathcal{N}_i|$. In a similar manner, a directed graph $\boldsymbol{G}$ is specified by a pair $(\mathcal{N}, \mathcal{E})$ where $\mathcal{E}$ consists of a set of directed edges each denoted by an ordered pair (i, j). A directed path in $\boldsymbol{G}$ consists of a sequence of nodes $i_1, i_2, \cdots, i_l,\ l \geq 2$, such that $(i_m, i_{m+1}) \in \mathcal{E}$ for all $1 \leq m \leq l-1$, and $\boldsymbol{G}$ is called strongly connected if there exists a directed path from each node to any other node.

The Laplacian of the undirected graph $\boldsymbol{G}$ is defined as $\boldsymbol{L} = (l_{ij})_{n \times n}$, where

$$l_{ij} = \begin{cases} |\mathcal{N}_i|, & \text{if } j = i \\ -1, & \text{if } j \in \mathcal{N}_i \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

The matrix $\boldsymbol{L}$ defined by (4) is positive semi-definite. Further, if $\boldsymbol{G}$ is a connected undirected graph, then $\text{rank}(\boldsymbol{G}) = n - 1$ (see, e.g., [24]).

Since the cooperative spectrum sensing problem is viewed as a consensus problem where the users locally exchange information regarding their individual detection outcomes before reaching an agreement, we give the formal mathematical definition of consensus as follows.

The n secondary users, distributed according to the graph model $\boldsymbol{G}$, are assigned a set of state variables x_i, $i \in \mathcal{N}$ (the initial estimated energy level Y_i mentioned previously). Each x_i will be called a consensus variable, and in the cooperative spectrum sensing context, it is essentially used by node i for its estimate of the detected energy. By reaching consensus, we mean the individual states x_i asymptotically converge to a common value x^*, i.e.,

$$x_i(k) \to x^* \quad \text{as } k \to \infty, \tag{5}$$

for each $i \in \mathcal{N}$, where k is the discrete time instant, $k = 0, 1, 2, \cdots$, and $x_i(k)$ is updated based on the previous states of node i and its neighbors.

The special cases with $x^* = \text{Ave}(x) = (\frac{1}{n})\sum_{i=1}^{n} x_i(0)$, $x^* = \max_{i=1}^{n} x_i(0)$ and $x^* = \min_{i=1}^{n} x_i(0)$ are called average-consensus, max-consensus, and min-consensus, respectively.

III. Consensus-based Spectrum Sensing Scheme

In this section, we propose a consensus-based spectrum sensing scheme to counter SSDF attacks. The convergence performance of this scheme is also presented.

A. Consensus-based Spectrum Sensing

Let us assume secondary users have established duplex wireless connections with their desired neighbors, and the connections remain working until the consensus is reached. The network topology can then be modeled by a fixed graph. Note that the attackers are included as some nodes in the graph and they will provide falsified information to authentic secondary users. Based on this assumption, the proposed consensus-based spectrum sensing scheme will consist of the following steps.

1) In the first stage, all the secondary users individually sense the target spectrum band based on the spectrum sensing models, and obtain the local estimated energy level denoted by Y_i.
2) In the second stage, all users establish wireless communication links with their neighbors, and then begin to exchange the local updated estimated energy level from time instant $k \in \mathbb{Z}+$. This process is done in iterations. We denote for user i, its measurement Y_i at time instant $k = 0$ by $x_i(0) = Y_i \in \mathbb{R}^+$. The state update of the consensus variable for each secondary user occurs at discrete time instant $k = 0, 1, 2, \cdots$, which is associated with a given sampling period. In each time instant k, having received the updated estimated energy level $x_j(k)$ from neighbors, each user i first uses a selection criterion to exclude a neighbor that is more likely to be an attacker. The procedure then generates a subset of neighbors whose data will be used in updating the state of user i.
3) After the local update computation, each user i sends out its updated estimated energy level $x_i(k+1)$ to its neighbors. Then the above neighbor selection and state updating procedure are repeated at the individual nodes until all the estimated energy levels $x_i(k)$ converge to a common value x^* within a prescribed error.

Finally, by comparing the average consensus result x^* with a pre-defined threshold λ based on Fig. 1, every secondary user i gets the final fused data locally:

$$\textit{Decision } \boldsymbol{H} = \begin{cases} 1, & x^* > \lambda \\ 0, & otherwise \end{cases} \tag{6}$$

We now describe the selection rule in detail. Consider $k \geqslant 1$ and we assume $|\mathcal{N}_i| > 2$. The procedure below is applied by each authentic secondary user.

1) First, user i gets the local mean value at time instant $k-1$

$$\mu_i(k-1) = \frac{x_i(k-1) + \sum\limits_{j \in \mathcal{N}_i} x_j(k-1)}{1 + |\mathcal{N}_i|}. \tag{7}$$

2) Secondly, user i identifies the neighbor with the maximum deviation from the value $\mu_i(k-1)$:

$$\hat{j} = \arg\max_{j \in \mathcal{N}_i} |x_j(k) - \mu_i(k-1)|. \tag{8}$$

3) Thirdly, user i forms a set $\widehat{\mathcal{N}}_i(k)$ of neighbors that are regarded as authentic users:

$$\hat{\mathcal{N}}_i(k) = \mathcal{N}_i \backslash \{\hat{j}\}. \tag{9}$$

When $k = 0$ or $|\mathcal{N}_i| \leqslant 2$, we set $\hat{\mathcal{N}}_i(k) = \mathcal{N}_i$. The reason why $k = 0$ is an exception is apparent.

Next, we present the consensus algorithm incorporating neighbor selection. From $k = 0, 1, 2, \cdots$, the iterative form of the consensus algorithm can be stated as follows:

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in \widehat{\mathcal{N}}_i(k)} (x_j(k) - x_i(k)), \tag{10}$$

where

$$0 < \epsilon < (\max_i |\mathcal{N}_i|)^{-1} \triangleq \Delta^{-1}. \tag{11}$$

The number Δ is called the maximum degree of the network.

This algorithm can be written in the vector form:

$$\boldsymbol{x}(k+1) = \boldsymbol{P}\boldsymbol{x}(k), \tag{12}$$

where $\boldsymbol{P} = \boldsymbol{I} - \epsilon \boldsymbol{L}$. Notice that the upper bound in (11) for ϵ ensures that $\boldsymbol{P}$ is a stochastic matrix, and in fact one can further show that $\boldsymbol{P}$ is ergodic when $\boldsymbol{G}$ is connected Since $\boldsymbol{G}$ is an undirected graph, all row sums and column sums

of $\boldsymbol{L}$ are equal to zero. Hence $\boldsymbol{P}$ is a doubly stochastic matrix (i.e.,$\boldsymbol{P}$ is a nonnegative matrix and all of its row sums and column sums are equal to one).

If the basic algorithm (where $\widehat{\mathcal{N}}_i(k)$ is always set as $\mathcal{N}_i$ in (10)); see, e.g., [24]) is applied and there are no attackers, then an average-consensus is ensured and the final common value $x^* = (\frac{1}{n})\sum_{i=1}^{n} x_i(0)$ will be the average of the initial vector $\boldsymbol{x(0)}$, or equivalently, the average of $\boldsymbol{Y^T} = \{Y_1, Y_2, \cdots, Y_n\}$ will be obtained in the end of the previous energy detection section.

If there are no attackers and we choose ϵ such that $0 < \epsilon < \frac{1}{\Delta}$, then an average-consensus will be ensured and the final common value $x^* = (\frac{1}{n})\sum_{i=1}^{n} x_i(0)$ will be the average of the initial vector $\boldsymbol{x(0)}$, or equivalently, the average of $\boldsymbol{Y^T} = \{Y_1, Y_2, \cdots, Y_n\}$ will be obtained in the end of the previous energy detection section. It can be further shown that the above algorithm can achieve an exponential convergence rate. In practical implementations, the exponent δ depends on the network topology and the parameter ϵ.

However, when attackers are present, the nature of the basic consensus algorithm is changed in that the neighborhood of each authentic user must be determined on-line according to the information it has received so that the user most likely to be an attacker is rejected. Moreover, due to the neighbor selection procedure applied by the authentic users, it is possible that secondary user A accepts secondary user B as a neighbor but the latter does not accept the former. This may result in unidirectional information exchange along certain edges of the graph $\boldsymbol{G}$. Hence, the algorithm (10) is essentially associated with a sequence of directed graphs $\mathbf{G}_t = (\mathcal{N}_a, \mathcal{E}_t)$, where $\mathcal{N}_a$ corresponds to the set of authentic secondary users. In this case, since the coefficient matrix in the algorithm is in general not doubly stochastic, one cannot expect convergence to the average value of the initial states. Also, the convergence of the algorithm with presence of attackers depends on the structure of the sequence of directed graphs $\boldsymbol{G}_t$. Indeed, if there is a large constant T such that for any time window $[k, k+T]$, the union $\cup_{t=k}^{k+T} \boldsymbol{G}_t$, as the directed graph formed by putting all edges of $\boldsymbol{G}_t$ together, is strongly connected, then convergence of the algorithm is guaranteed [14]; such a joint connectivity of $\boldsymbol{G}_t$ means that any two authentic secondary users can always directly or indirectly exchange information on a sufficiently long time window.

IV. Simulation Results and Discussions

In this section, we present simulation results to show the performance of the proposed schemes.

A. Defense against SSDF Attacks

In the first part of the simulations, we intend to demonstrate how the proposed consensus-based scheme works to counter SSDF attacks. The simulations are based on a CR-MANET shown in Fig. 2, where 11 secondary users are doing cooperative spectrum sensing to check whether or not there is a primary user. There are 10 authentic secondary users. The sensed energy from the nodes is distributed according to (3) with an average SNR of 10. There is an attacker in the MANET. Fig. 3 shows the estimated primary user energy with and without the Selfish SSDF. If there is no malicious attack, although the initially sensed energy varies greatly due to variable wireless channel conditions, a consensus will be reached that the energy is very low and there is no primary user. With the Selfish SSDF attack, node 11 keeps sending falsified data $x_{11}(k) = 20$. An incorrect conclusion will be made in the CR network that there is a primary user. Fig. 4 illustrates that when using our consensus-based scheme to filter out the attack data, all the authentic users can reach the consensus and make the correct decision that there is no primary user.

B. False Alarm Probabilities

In the second part of the simulations, we focus on the performance in terms of false alarm probabilities.

We compare the performance of the proposed scheme with that of the centralized decision fusion scheme [9]. In the centralized decision fusion scheme, each sensing terminal senses the spectrum and makes a local decision by comparing the sensed energy against a predefined energy threshold λ. Then, all sensing terminals send the local decisions to a common receiver, which sums all of the collected local spectrum sensing results. A threshold value is defined. If the sum of local decisions is equal to or greater than the threshold value, then the final result is the presence of primary users; Otherwise, the band is free. In our simulations, the threshold value is set to two in the centralized fusion scheme. To make a fair comparison, we need to determine the threshold λ, under which the centralized decision fusion scheme and the proposed consensus-based scheme have the best performance, when there is no malicious attack. In the simulations, we find that the best performance occurs when we set the local threshold $\lambda = 14.2$dB for the centralized decision fusion, and $\lambda = 11.4$dB gives the best performance for the proposed scheme. This shows the proposed consensus-based scheme has significant improvement in terms of the required average SNR for detection. The proposed scheme can make a better detection than the centralized decision when secondary users experience worse channel fading (low average SNR). We will use these threshold values in the following simulations.

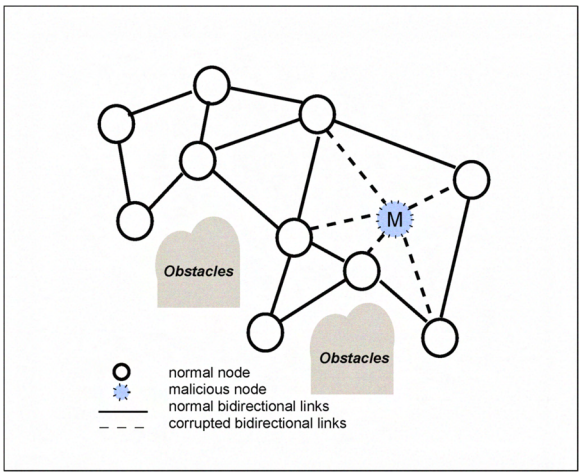

Fig. 2. A 11-node MANET with one SSDF attack.

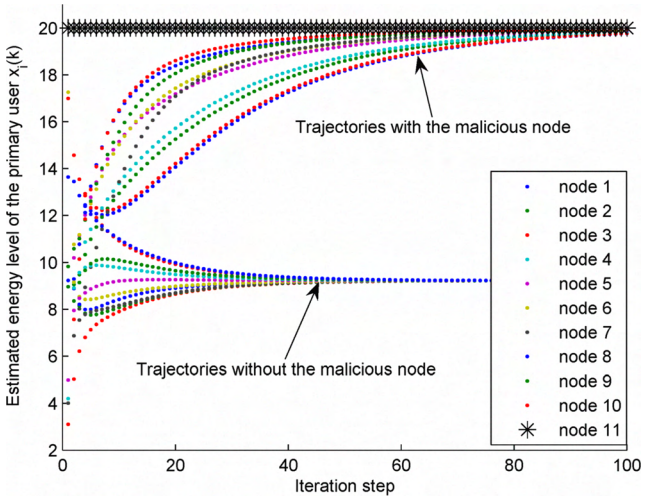

Fig. 3. Estimated primary user energy with and without Selfish SSDF attacks.

Two Selfish SSDF attacks are conducted. In the first attack, a user is compromised and sends out falsified detected energy level data 20. In the second attack, two users are compromised, they send out falsified data 20 and 15, respectively. Fig. 5 shows the results in terms of false alarm probabilities. From Fig. 5, we can see that the consensus-based scheme is more robust than the existing centralized fusion scheme. When $\lambda = 11.4$dB, the false alarm probability in the consensus-based scheme is lower than that in the centralized scheme in all of the following three cases: no attack, one attacker and two attackers. The centralized scheme is very vulnerable to the Selfish SSDF attacks, particularly in the two attacker case, where the false alarm probability is 1. This will result in severe performance degradation of the MANET. The spectrum utilization will be very low since false alarms increase the number of missed opportunities (white space). When the false alarm probability is 1, the CR-MANET cannot find any spectrum opportunities.

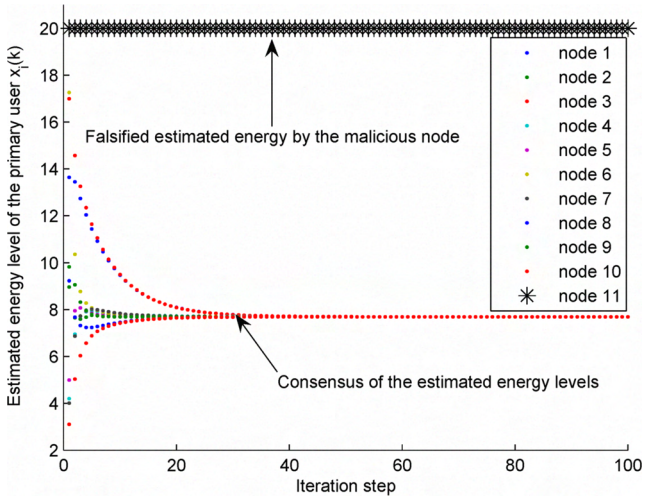

Fig. 4. Estimated primary user energy in the proposed consensus-based scheme to mitigate Selfish SSDF attacks. (Attacker node 11 is filtered out.)

V. Conclusions and Future Work

Security is an important issue in CR-MANETs. Malicious CRs can send false local spectrum sensing results in cooperative spectrum sensing. In this paper, we have presented a consensus-based spectrum sensing scheme to counter SSDF attacks in CR-MANETs. Using the consensus of secondary users, the proposed scheme can differentiate the trustworthiness of spectrum sensing terminals, which makes it is robust against SSDF attacks. Moreover, a common receiver is not needed for the final decision in the proposed scheme. Simulation results have been presented to illustrate the effectiveness of the proposed schemes.

Future work is in progress to use other bio-inspired algorithms to improve the quality of service and security in CR-MANETs.

References

[1] J. Mitola, *Cognitive radio: An integrated agent architecture for software defined radio*. Doctor of Technology, Royal Inst. Technol. (KTH), Stockholm, Sweden, 2000.

[2] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, pp. 201–220, Feb. 2005.

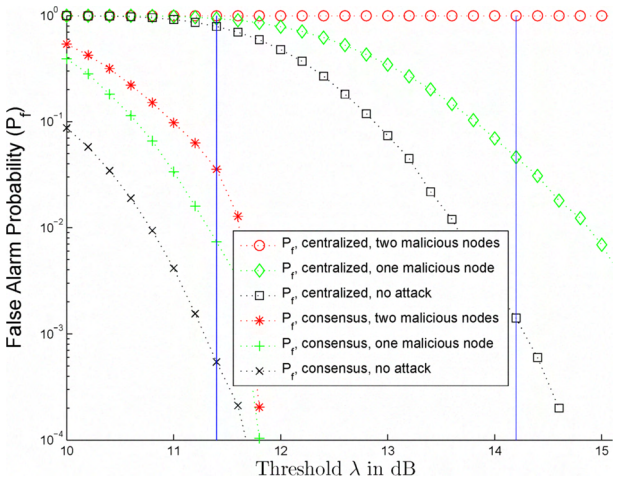

Fig. 5. False alarm probability comparison between the centralized decision fusion scheme and the consensus-based scheme.

[3] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *Elsevier Ad Hoc Networks*, vol. 7, pp. 810–836, July 2009.

[4] A. Ghasemi and E. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE DySPAN 2005*, (Baltimore, Maryland), Nov. 2005.

[5] E. Peh and Y.-C. Liang, "Optimization for cooperative sensing in cognitive radio networks," in *Proc. IEEE WCNC'07*, (Hong Kong, P.R. China), Mar. 2007.

[6] J. Unnikrishnan and V. V. Veeravalli, "Cooperative sensing for primary detection in cognitive radio," *IEEE J. Sel. Topics Signal Proc.*, vol. 2, pp. 18–27, Feb. 2008.

[7] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics Signal Proc.*, vol. 2, pp. 28–40, Feb. 2008.

[8] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Veh. Tech.*, vol. 7, pp. 1326–1337, Apr. 2008.

[9] R. Chen, J.-M. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Comm. Mag.*, vol. 46, pp. 50–55, Apr. 2008.

[10] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, pp. 25–37, Jan. 2008.

[11] I. Carreras, I. Chlamtac, F. D. Pellegrini, and D. Miorandi, "Bionets: Bio-inspired networking for pervasive communication environments," *IEEE Trans. Veh. Tech.*, vol. 56, pp. 218–229, Jan. 2007.

[12] F. Dressler, Ö. B. Akan, and A. Ngom, "Guest Editorial - Special Issue on Biological and Biologically-inspired Communication," *Springer Trans. on Computational Systems Biology (TCSB)*, vol. LNBI 5410, Dec. 2008.

[13] W. Ren, R. Beard, and E. Atkins, "A survey of consensus problems in multi-agent coordination," in *Proc. American Control Conference'05*, (Portland, OR), June 2005.

[14] W. Ren and R. W. Beard, "Consensus seeking in multiagent systems under dynamically changing interaction topologies," *IEEE Trans. Auto. Control*, vol. 50, pp. 655–661, May 2005.

[15] L. Xiao, S. Boyd, and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in *Proc. Fourth International Symposium on Information Processing in Sensor Networks IPSN 2005*, pp. 63–70, 2005.

[16] M. Huang and J. Manton, "Stochastic consensus seeking with measurement noise: convergence and asymptotic normality," in *Proc. American Control Conference'08*, (Seattle, WA), June 2008.

[17] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Proc. Mag.*, vol. 24, pp. 79–89, May 2007.

[18] D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proc. Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, vol. 1, pp. 772–776, 2004.

[19] C. Sun, W. Zhang, and K. B. Letaief, "Cluster-based cooperative spectrum sensing in cognitive radio systems," in *Proc. IEEE ICC'07*, (Glasgow, UK), pp. 2511–2515, June 2007.

[20] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, pp. 523–531, Apr. 1967.

[21] V. Kostylev, "Energy detection of a signal with random amplitude," in *IEEE Proc. ICC'02*, (New York, NY), Apr. 2002.

[22] M. Huang and J. H. Manton, "Stochastic lyapunov analysis for consensus algorithms with noisy measurements," in *Proc. American Control Conference'07*, (New York, NY), July 2007.

[23] M. Huang and J. H. Manton, "Coordination and consensus of networked agents with noisy measurements: stochastic algorithms and asymptotic behavior," *SIAM J. Control and Optimization*, vol. 48, no. 1, pp. 134–161, 2009.

[24] R. Olfati-Saber, J. Fax, and R. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, pp. 215–233, Jan. 2007.