International Journal of MC Square Scientific Research Vol.7, No.1 Nov 2015

# IMPROVED DISTRIBUTED COOPERATIVE SPECTRUM SENSING (DCSS) FOR COGNITIVE RADIO ADHOC NETWORK

*Rajesh. D,*
*Assistant Professor, Department of Computer Science and Engineering,*
*Universal College of Engineering and Technology, Vallioor, Tamil Nadu, India*
*Email- rajeshd936@gmail.com*

**Abstract—** Cooperation among cognitive radios for spectrum sensing is deemed essential for environments with deep shadows. In this paper, we study cooperative spectrum sensing for cognitive radio ad hoc networks where there is no fusion center to aggregate the information from various secondary users. We propose a novel consensus-inspired cooperative sensing scheme based on linear iterations that is fully distributed and low-cost. In addition, the trade-offs on the number of consensus iterations are explored for scenarios with different shadow fading characteristics. Furthermore, we model Insistent Spectrum Sensing Data Falsification (ISSDF) attack aimed at consensus-based iterative schemes and show its destructive effect on the cooperation performance which accordingly results in reduced spectrum efficiency and increased interference with primary users. We propose a trust management scheme to mitigate these attacks and evaluate the performance improvement through extensive Monte Carlo simulations for large-scale cognitive radio ad hoc networks in TV white space. Our proposed trust management reduces the harm of a set of collusive ISSDF attackers up to two orders of magnitude in terms of missed-detection and false alarm error rates. Moreover, in a hostile environment, integration of trust management into cooperative schemes considerably relaxes the sensitivity requirements on the cognitive radio devices.

**Keywords—** Dynamic spectrum access, Cognitive radio ad hoc networks, Distributed consensus-based cooperative spectrum sensing, Trust management, Insistent spectrum sensing data falsification attack

## I. INTRODUCTION

The radio frequency spectrum shortage problem is originated from the static assignment of the frequency bands to the primary users (PUs or licensees) of the bands. The non-adaptive spectrum assignment leaves a significant portion of RF spectrum underutilized [1]. Dynamic spectrum access (DSA), enabled by cognitive radios, introduces an adaptive approach for spectrum use that facilitates more flexibility by allowing secondary users (SUs) to use licensed spectrum bands on an opportunistic non-interference basis. As a result, DSA offers a better utilization of the spectrum and is essential for solving the spectrum shortage problem. Cognitive

radios that sense and dynamically share the spectrum empower today's smart technologies such as cognitive Internet of Things [2] and heterogeneous networks with cognitive Femtocells [3]. Spectrum sensing is an important step for DSA. However, when an SU senses the spectrum, it is possible that it does not detect the PU due to a deep shadow and this in turn increases the risk of interference to the PU. In order to improve the SUs' detection accuracy cooperative spectrum sensing has been proposed. In this approach, a set of SUs cooperate by sharing their sensing information with each other and collectively deciding on the presence or absence of the PU [4]. In a centralized cognitive radio network (e.g. IEEE 802.22 [5]), the final decision is made by a fusion center that aggregates the sensing data from all of the SUs in the network. In contrast, in a decentralized network (e.g. a cognitive radio ad hoc network or CRAHN), the nodes must perform a distributed cooperation. Distributed cooperative spectrum sensing (DCSS) is preferred to a centralized scheme because a distributed scheme is scalable, fault-tolerant and more efficient. DCSS is performed by exploiting existing distributed consensus algorithms that have been previously used for applications such as sensor fusion [6] or Peer-to-Peer systems [7]. These consensus algorithms are based on iterative diffusion and aggregation of data through linear iteration-based or gossip-based schemes [8] and involve communication with direct neighbors in the network graph. However, the consensus based DCSS schemes that have been proposed previously are not practical for ad hoc networks as they require the individual nodes to have knowledge about the topology of the network. Another known issue with cooperative schemes is that in a realistic potentially hostile environment, malicious secondary users can broadcast falsified sensing data to their neighbors in order to mislead them and compromise the spectrum sharing in the cognitive radio network. This attack is called Spectrum Sensing Data Falsification (SSDF) [9] attack.

A more serious and less studied attack particularly aimed at consensus-based schemes is an iterative attack that we call Insistent SSDF (ISSDF). The ISSDF attacker not only falsifies its own initial data but it also broadcasts the falsified value in every iteration of the consensus and refrains from performing updates according to the protocol. The ISSDF attack compromises the cooperation significantly and it may cause divergence from the correct consensus. In order to address the above-mentioned problems, in this paper, we introduce a trust-aware consensus inspired DCSS scheme which is low-overhead and resilient to ISSDF attacks. Our contributions can be summarized as following: We propose a practical distributed scheme for cooperative spectrum sensing in cognitive radio ad hoc networks that is inspired by a linear iterative average consensus algorithm and uses an equal-weighting update strategy that does not require any topology knowledge by SUs. Through extensive simulations for realistic large-scale mobile networks in outdoor environments with correlated shadow fading, we show that our proposed scheme offers the same level of performance compared to the existing more complex consensus-based schemes. We analyze the performance-complexity trade-offs on the number of consensus iterations for a typical simulated network under different shadowing severities. We show the

significant potential of the collusive ISSDF attackers in crippling the consensus-based schemes. We propose a trust management scheme that can be integrated with any consensus-based DCSS scheme to mitigate the ISSDF attacks. We show that our proposed trustaware DCSS scheme is robust even in the presence of a large set of ISSDF attackers that act in harmony and simultaneously. In addition, we propose a trust-aided outlier detection technique that when combined with the proposed trust scheme can effectively mitigate dynamic attackers. We analyze the impact of malicious attacks and trust management mitigations on the sensitivity requirements of cognitive radio devices which has direct relationship with the system's cost and flexibility.

## II. BACKGROUND AND RELATED WORK

Recently, average consensus algorithms [8] including gossip-based protocols [7] and linear iteration- ased schemes [6] [10] have been exploited for the DCSS applications [11] [12] [13] [14]. However, all of the existing consensus-based DCSS schemes require the individual SUs to have some type of knowledge about the network topology. For instance, some of these schemes require the nodes to know the maximum degree in the network (or at least an upper bound), while others require the nodes to know the degree of the neighbor nodes (e.g. Metropolis weighting) [6]. These limitations make the existing DCSS schemes impractical for cognitive radio ad hoc networks. In this paper, we propose a consensus-inspired DCSS scheme that is practical for a dynamic network because the SUs are completely topology-agnostic. The other significant issue in the current cooperative spectrum sensing schemes is ensuring the robustness of the cooperation against malicious SSDF [9] attackers that broadcast falsified sensing data. Moreover, in the context of iterative consensus-based DCSS schemes, ISSDF attackers, that do not follow the consensus update protocol and broadcast falsified data in every iteration, are much more destructive than the conventional SSDF attackers. In addition, a set of collusive ISSDF attackers can amplify the effect of each-other. Sundaram et. al. prove that a set of conspiring malicious nodes, who do not follow the update protocol, are able to prevent the network from converging to the correct answer [15] [16]. ISSDF attackers are in a sense similar to the stubborn agents [17] that have been studied in the context of opinion propagation and convergence. It is shown that the stubborn agents can cause the network to converge to their opinions. Moreover, the optimal selection and placement of stubborn agents for maximized impact on a fixed network is investigated [17] [18] [19]. In contrast, in this paper, we consider a mobile network of SU nodes, where a random subset of nodes are ISSDF attackers and they move randomly similar to the normal nodes.

We do not make any assumption that ISSDF attackers collude to move in a way to maximize their effect on the network. This may be an interesting scenario for further research. The conventional SSDF attacks and mitigation approaches against them have been well-studied in the literature for the centralized schemes [9] [20] [21] [22]; however, the problem of coping with ISSDF attacks in the consensus-based DCSS schemes is hardly explored. A proposed approach to mitigate the effect of ISSDF attackers in consensus-based DCSS schemes is adaptive outlier detection [23] [24] which is based on detecting the nodes that broadcast values that are deviated from the the rest of the neighbors. This approach is distributed however, it requires

every node to compute a deviation threshold at each consensus iteration which imposes a significant computational overhead on each SU. As will be described in the following sections, in our proposed scheme the SUs update the trust scores only once the consensus iterations are completed and therefore the computational overhead is low. Zhang et. al. propose a weighted average consensus scheme to count for channel conditions and multi-path fading in DCSS, however, they do not address the ISSDF attacks nor the impact of correlated shadow fading. In this paper, we introduce trust scores as weights for the average consensus update rule to mitigate ISSDF attacks. Liu et. al. [25] propose a trust scheme using trust propagation and a set of pre trusted nodes to mitigate the effect of Byzantine adversaries in linear iterative consensus in sensor networks. However, trust propagation is costly and generally there are no pre-trusted nodes in an ad hoc network. A trust-aware DCSS based on single neighbor gossip has been proposed in [12] which can mitigate SSDF attacks; however, due to the nature of wireless networks, this model is less efficient compared to a broadcast model which we consider in this paper. In addition [12] considers sharing of binary decisions only. In this paper, we consider the model where the SU nodes share raw PU power values. In this paper, we extend our previous work [26] by analyzing our proposed trust-aware consensus-inspired DCSS scheme for a mobile CRAHN in realistic environments with correlated shadow fading of various severity. In addition, we study the trade-offs that determine the best choice for number of consensus iterations. Moreovesr, we analyze the operating characteristics of a CRAHN under various detection thresholds in the presence of ISSDF attackers and show the significant improvement through trust management. Our trust management scheme does not depend on pre-trusted nodes and only requires the nodes to perform a single local trust evaluation per sensing round for each direct neighbor. These features make our proposed trust-aware DCSS scheme practical and low-cost for CRAHNs

## III. SYSTEM MODEL

Our model consists of a network of n SUs that form a CRAHN in a square location area which is far away from a PU transmitter. The PU transmitter is assumed to have a high transmission power (e.g. a TV station), therefore the whole SU network is within the transmission range of the PU transmitter. A network of PU receivers are also collocated in the same area. See Figure 1 for the system overview. SU nodes are initially uniformly spread throughout the location area and during the time of simulation, they move randomly. The neighbor set of the SU node i, denoted by Ni, consists of all of the SUs that are located within the communication range of SU node i. Obviously, the neighbor sets are always changing due to the mobility of the nodes; however, we assume the SU network topology remains unchanged during one sensing period. When node i broadcasts a message, all of its one-hop neighbors will receive that message. Here we assume perfect communication between the SUs via a common control channel. The detection of a PU is modeled as a binary hypothesis testing problem as follows: H0 if PU is absent and H1 if PU is present. Each SU node is equipped with a power detector for sensing the received power from the PU. When the PU is inactive, the sensed power at an SU will essentially be equal to the received noise power.

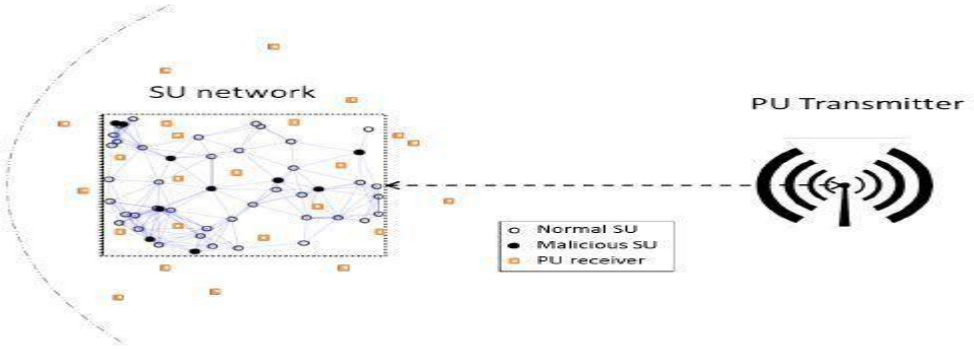


Fig. 1. System Overview

**A. Path loss and shadow fading model**

A radio propagation model (analytical or empirical), provides an average path loss for a given transmitter-receiver distance. In our model, we apply Hata path loss model (suburban areas variant) [31]. The IEEE 802.22 working group recommends the Hata model for spectrum sensing modeling in wireless regional area networks (WRAN) operating in TV whitespace.

In addition, a signal transmitted through a wireless link naturally experiences random variations due to obstacles in the path. As a result, two receivers at two different locations with equal distance from a transmitter will not be affected by the same path loss despite the fact that the average path loss is the same at both locations. The random variation about the average path loss due to blockage of objects in the signal path such as buildings and trees is called shadow fading. It is safe to assume that shadow fading remains constant at a single location over time since normally there is no significant change in the terrain such as the surrounding buildings or trees (a space-time correlated shadow fading model [32] may be used if the shadows are not constant over time.) Obviously, the reception of the mobile radio nodes changes when they move in and out of shadows over time. The loss due to shadow fading is commonly modeled by a random variable with lognormal distribution [31]. That is the shadow fading loss in dB

## IV. DISTRIBUTED AVERAGE CONSENSUS-BASED COOPERATIVE SPECTRUM SENSING

In an average consensus-based DCSS scheme, the SUs aim at estimating the average of the received power by all of the SUs. At each sensing round, each SU first measures its own received power as its initial value; then it participates in a series of broadcast and update iterations. In each iteration, the SUs broadcast their current values and update their average estimates based on the received values from neighbors. Finally, each node independently compares its estimate of the average power with a threshold and makes its final decision about the PU presence. In this section, we briefly describe two categories of average-consensus algorithms: gossip-based and weighted linear iteration-based, that are used for DCSS application. We will compare our proposed DSCC scheme against these schemes.

**A. Weighted linear iteration-based**

In the weighted linear iteration scheme, the nodes in the network follow a weighted linear combination update strategy at each iteration in order to converge to a consensus about the global average [6]. The value of node i at consensus iteration c is denoted by vi(c). At each

sensing round, each node i is initialized with vi(0) = received power at node i. In order to converge to the global average, at each consensus iteration c, each node i updates its value with a weighted linear combination of its own value and the received values from its neighbors [6
Obviously, for the distributed linear iterations to asymptotically converge to the global average, the graph must be connected; otherwise, the convergence can only be reached for each isolated subgraph. Optimal and heuristic approaches have been proposed to realize the weight matrix that satisfies the convergence condition as described above. The optimal solution [10] is not a distributed solution and therefore is not practical for our purpose. Two heuristic weight choices that satisfy the convergence condition and therefore guarantee asymptotic convergence to the global average are [6]:

**B. Gossip-based**

We also compare our proposed scheme against DCSS schemes based on Push-Sum protocol [7] which is a gossipbased solution for the average consensus problem. In Push- Sum algorithm, each node maintains a sum, which is initialized to be the received PU power at this node; it also maintains a gossip weight which is initialized to 1. At each consensus iteration, each node sends a fraction of its sum and weight to one or more randomly chosen neighbor(s). We will compare our proposed DCSS scheme against the following two variants of the Push-Sum scheme: 1) One-neighbor gossip, where at each iteration, each node picks one of its neighbors at random and sends half of its sum and weight to it [12]. 2) Flooding gossip, where at each iteration, each node distributes its sum and weight values uniformly among all of its neighbors [26]. See [7] for details of the Push-Sum algorithm.

**C. Neighbor discovery overhead**

The existing average consensus-based DCSS schemes that are described above impose overhead related to neighbor discovery at each sensing round. In the Metropolis linear iteration-based scheme, the weights are calculated based on the larger degree in each pair of nodes. Therefore, the nodes must first discover their neighborhood sizes (degrees) and then broadcast their degrees to others. As a result, this scheme requires the nodes to perform neighbor discovery that needs to be updated every sensing round which imposes significant overhead. In addition to that overhead, each node also needs to broadcast its degree to the other nodes at each sensing round. Note that in a mobile network the neighborhoods are changing all the time and therefore the number of neighbors of a node is different from one sensing round to the next. As a result using the perceived number of neighbors based on the broadcasts received in the immediately previous sensing round introduces error in convergence. Similarly, for the maximum-degree variant, determining the maximum degree is not trivial in a distributed ad hoc network where nodes only have local views of the network. In the gossip-based DCSS scheme, each node needs to know the number of its active neighbors in advance to calculate the fraction to broadcast in the current sensing round (or to pick one random neighbor in the case of one-neighbor gossip). As mentioned above, using the perceived number of neighbors based on the previous round introduces error (leakage of some fractions of values in this case). Therefore, a neighbor discovery phase is necessary at each sensing round. Neighbor discovery in mobile ad hoc networks is a non-trivial task and an active area of research. The determination of the direct neighboring nodes is generally done using hello protocols where each node periodically broadcasts a hello message. Each node considers another node as a direct one-hop neighbor only if it receives at least one hello message from it [33] [34]. The random access discovery schemes require the nodes to be randomly in a “listen” or “transmit” mode in each time slot so that each

node receives the hello message from every neighbor at least once in a predefined time period. These algorithms generally require a large number of time slots to reliably discover all neighbors [35] [36]. Therefore, neighbor discovery imposes a significant time overhead in particular for mobile networks with changing topologies. As we will show next, our proposed equally-weighted DCSS scheme is considerably more efficient than the existing schemes because it does not require the neighbor discovery phase and thus completely eliminates the associated overhead.

## V. PROPOSED EQUALLY-WEIGHTED LINEAR ITERATION-BASED DCSS

We introduce a novel DCSS scheme based on iterative linear combinations with equal weight assignment. At each iteration, each node simply broadcasts its value and then updates its value as an equally-weighted average of its own value and all of the received values in this iteration. Our proposed equallywighted approach offers significantly lower overhead compared with the existing schemes due to the elimination of neighbor discovery. Note that if every neighbor broadcasts its value to node i, then Ri will be essentially equal to Ni (the neighbor set), therefore translating the proposed scheme back to Equation (7), the equal weights that node i assigns to any neighbor j and to itself will be equal to 1 1+jNij and a weight of zero is assigned to the other nodes. 10-2 Equally-weighted Metropolis Max Degree While the average consensus algorithms are originally designed to asymptoticly converge to the exact global average for sufficient number of iterations (e.g. in sensor fusion applications), in DCSS applications the nodes do not need to converge to the exact average as the estimated average is solely used for comparison against a detection threshold. Therefore, the accuracy of estimation can be relaxed. Obviously with more consensus iterations the accuracy of the estimated average improves, however the consensus overhead also increases. As a result there is a cost-performance trade-off and the number of iterations must be kept as few as possible for the required performance. The corresponding weight matrix of this approximate approach does not necessarily satisfy the condition for asymptotic convergence to the exact global average as described in Equation (8); however, we show with Monte Carlo experiments, that this scheme results in an approximate convergence with a small error offset and it converges faster compared to the Metropolis and maximum-degree heuristics (See Figure 3). In addition, we will show in the next sections that the small convergence error does not degrade the performance of DCSS. This is because in the DCSS applications, an exact convergence is not necessary; instead, a practical solution is desired where the nodes estimate the average power within only a few iterations to quickly arrive at binary decisions about the PU presence. Since for asymptotic convergence weights must satisfy Equation (8), we define the n _ n weight error matrix _ as a metric to evaluate the convergence for any number of iterations, c:= Wc (1N )11T (10) We evaluate the convergence of Wc in different schemes through Monte Carlo simulations. In each Monte Carlo run, we consider a different random network topology which corresponds to a different weight matrix W for each of the schemes . Then we average that over the many random network topologies in the Monte Carlo simulations.the convergence of the three different schemes in terms of weight error convergence. All of the random topologies include a graph of 50 nodes in a 300 m _ 300 m area. All of the three schemes almost converge within around 6 iterations. As expected, for the proposed equally-weighted scheme, there is an associated error offset in the convergence; however, the weight errors drop faster than the other two schemes. As a result, the convergence errors of the equally-weighted scheme are smaller in the first few

iterations. This faster convergence of weights in the equally-weighted scheme directly translates to a faster convergence of nodes' values towards the global average. Note that fast convergence in a few iterations is vital for a practical DCSS scheme whereas higher number of iterations might not be affordable anyway. In Section VI, we present our performance results in terms of PU detection error rates which confirm that our proposed equal-weighting scheme performs as well as other more complex schemes. In addition, as discussed above, it is the most practical choice for DCSS due to its simplicity.

## VI. PERFORMANCE ANALYSIS OF CONSENSUS-BASED DCSS SCHEMES

### A. Simulation Setup

We study a cognitive radio ad hoc network with 50 SU mobile nodes spread and moving in a 300 m_300 m square, according to a random way point model [37], operating in a TV whitespace channel of 6 MHz bandwidth with 615 MHz center frequency. SU network is at a 15 km distance from the PU transmitter (TV station). We assume a 54 dBm transmit power for PU transmitter. Using the Hata path loss model, the nominal loss only due to distance is about 138 dB. In addition to path loss, we consider log-normal shadow fading with dB spread of 4; 8; 12 dB. We analyze the performance of different schemes in different scenarios through Monte Carlo simulations, where at each run, the network is randomly initialized. PFA and PMD of the network are derived as the average fraction of the honest nodes in the network that make a false alarm and missed-detection error in a sensing round, respectively. The simulation parameters listed in Table I, will be used for the experiments presented in the rest of the paper.

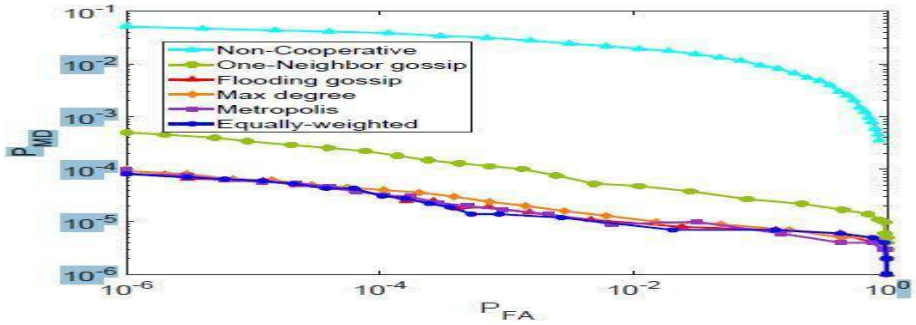


Fig. 2. ROC for consensus-based DCSS schemes. Number of consensus iterations = 8, dB = 8 dB

### B. Comparison results

In this section, we evaluate and compare the performance of the distributed consensus schemes that were described earlier using complementary Receiver Operating Characteristics (ROC) curves plotting missed-detection rate versus false alarm rate for various values of detection threshold.We have picked a wide range of detection thresholds ranging from 96 dBm to 82 dBm that result in very high to very low missed-detection and false alarm error rates. Figure 4 shows ROC curves for all of the schemes that were described in the previous sections, for 8 consensus iterations. The results show that the proposed equally-weighted linear scheme performs as well as the other consensus more complex schemes.

### C. Performance-complexity trade-offs on the number of consensus iterations

Cooperative spectrum sensing is deployed to overcome thecorrelated shadow fading by exploiting the spatial diversity among the cooperating nodes with the hope that different nodes at

various locations experience different shadow severity. Therefore, the nodes that enjoy a better reception can help the other nodes who may suffer from a deep shadow. As discussed in Section III, the decorrelation distance associated with an environment determines the size of the shadows (see Figure 2 for example). When decorrelation distance is large (shadows are large), in order to better exploit the existing spatial diversity, nodes must cooperate within larger areas (i.e. with nodes that are multiple hops away.) For example, if SUs consult with their direct neighbors only (i.e. only 1 iteration), the cooperation will be ineffective. The reason is that the neighboring nodes are under the effect of the same shadow and their sensing data is highly correlated. As a result, a "local averaging" scheme is not effective particularly for scenarios with large decorrelation distances. On the other hand, the communication and computational overhead of the consensus-based DCSS schemes is directly related to the number of consensus iterations. If C denotes the number of consensus iterations, the communication overhead of consensus for each node will be C packets per sensing round. In addition, if we denote the average number of neighbors of a node at any given time by B, the computational overhead is of the order of O(C _ B). Therefore, in order to keep the consensus overhead affordable for DCSS application, the number of iterations must be as small as possible. In a nutshell, there is an important complexity-performance tradeoff in determining the optimal number of iterations. Figure 5 compares the missed-detection rates of the equallyweighted scheme with only 1 consensus iteration versus the same scheme with 4 and 8 iterations. On the horizontal axis the decorrelation distance is increased from 25 m up to 100 m. For large decorrelation distances, in particular, a local cooperation (# Iterations = 1) is not sufficient; higher number of iterations is required to better use the spatial diversity. The gap is even more significant for the case of higher dB spread as seen in Figure 5(c) with _ dB = 12 dB. Figure 6 shows ROC plots for our proposed equally-weighted consensus-based DCSS scheme with 1, 4, and 8 iterations. With only 1 consensusn iteration, each node receives information solely from direct neighbors. 4 iterations is significantly better than 1 iteration, however the performance resulting from 8 iterations is very close to 4 iterations. For the rest of the paper we fix the number of consensus iterations to 4.

## VII. INSISTENT SPECTRUM SENSING DATA FALSIFICATION

In iterative average consensus-based DCSS schemes, in all of the iterations, all of the nodes must follow a predefined update strategy.

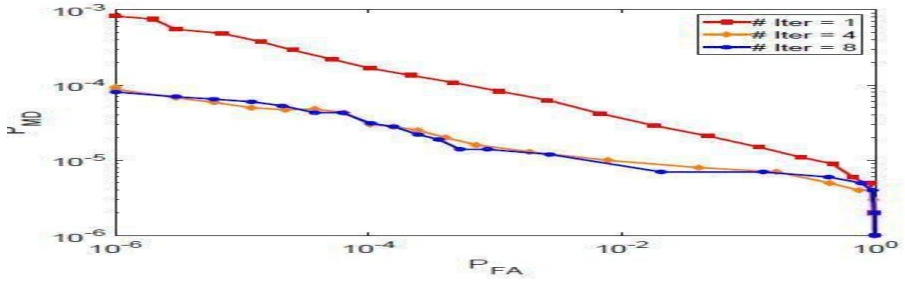


Fig. 3. ROC for the proposed equally-weighted DCSS with different number of consensus iterations, _ dB = 8 dB

We call this attack Insistent SSDF or ISSDF. Since the falsified data is repeatedly fed into the consensus process, an ISSDF attack is significantly more destructive than the conventional SSDF. We will show that ISSDF attacks make the honest (non-malicious) nodes, diverge from the correct average. In the case of SSDF attack, if the number of attackers is sufficiently small, the malicious effect may be neutralized by the honest nodes in the network

by only using simple cooperation. In contrast, as we will show in our experiments, even a very small set of ISSDF attackers can have much larger impact which makes trust management a necessity.

## VIII. PROPOSED TRUST MANAGEMENT SCHEME

Our trust management works based on trust scores that the nodes assign to each other based on their previous interactions. The trust score that node i assigns to node j at time step (sensing round) t is a value in the interval [0; 1] and is denoted by _ij(t). This score can be interpreted as the estimated probability of j being honest from the viewpoint of node i. In order to make the DCSS schemes resilient to data falsifying attacks, each node must be aware of the level of trustworthiness of its neighbors before relying on the received values from them.

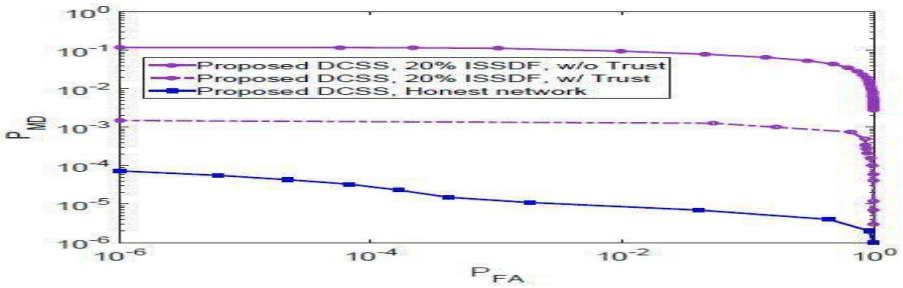


Fig.4. ISSDF attack and mitigation with trust management for our proposed trust-aware DCSS scheme

### A. Analysis on node agreement probability

The trust score is essentially a quantization of the probability of agreement between the two nodes in the recent interactions. In this section, we analyze the trust score that an honest node assigns to a fabricating ISSDF attacker. A fabricating attacker always reports the opposite of the truthabout the PU activity. Therefore, when an honest node i makes an observation from a fabricating node a, node i is able to detect the conflict and tag the observations as negative. There are two conditions where the two nodes agree: 1) if H0, then a's report indicates the PU is present; therefore, if i makes a false-alarm error, the two node agree, 2) if H1, then a's report indicates the PU is absent; thus, i agrees with a in case of a missed-detection error. Equation (13) shows the agreement rate which is directly translated to the trust score that a typical honest node assigns to a fabricating attacker.

. As we will show in the results, the integration of trust management with the proposed DCSS significantly improves the error rate performance in the presence of fabricating attackers.

### B. Trust integration

We incorporate the trust management into the linear iterations of our proposed equally-weighted DCSS scheme by using the trust scores as weights associated with received values from different nodes. Denoting the number of consensus iterations by C and average number of neighbors by B, the computational overhead of incorporating the trust scores is on the order of O(C _ B). This overhead is reasonably low for realistic scenarios with a bounded number of consensus iterations (e.g. 4 iterations) and typical neighborhood sizes (e.g. 8 to 10 neighbors).

### C. Discussion on trust initialization strategy

Our proposed trust assignment strategy is conservative which means each node must

perform a minimum number of observations (Omin) from a neighbor before it assigns a non-zero trust score to it (i.e. _ij = 0 if jOij j < Omin). As a result, a node builds up a sufficient record of observations,from a new neighbor before considering the neighbor's sensing reports in its decisions. As a result, we choose the more conservative strategy for trust assignment.

**D. Mitigating dynamic attackers**

In this section, we consider a more complex attack scenario where a subset of the honest nodes become malicious while the network is in operation. The main complication of this dynamic behavior is that a node which has been honest and therefore has already built up high trust in the viewpoint of the other honest nodes, suddenly starts to broadcast falsified data. This type of attack is harder to mitigate because the dynamic attackers abuse their initial high trust score to influence the final decision of the honest nodes to be in agreement with them which in turn makes the honest nodes continue to trust the dynamic attackers. In order to mitigate the dynamic attacks, we introduce an outlier detection technique as another layer of defense in our proposed trust management scheme. Note that, the trust score update is performed without any change as before; therefore, the trust score of a dynamic attacker will be decreased gradually during the following sensing rounds as its reports are repeatedly in conflict with the honest nodes.

**E. Simulation results**

The ROC curves for the scenario where 20% of the nodes are ISSDF with and without trust enabled. The ROC curve for an honest network (no attackers) is also shown for comparison. For a fixed false alarm rate, enabling trust management improves the missed-detection rate by as much as two orders of magnitude. From right to left of the plots, the detection threshold is increased. We analyze various levels of attack severity and the trust improvements in those scenarios in Figure 9. Our proposed trust-aware scheme outperforms the schemes that are not trustenabled in all of the scenarios including the case where the majority of the SUs are malicious (See the ROC curve corresponding to 60% ISSDF).

**1) Operating regions and sensitivity requirements:** The ROC curves are perfect tools for determining the system requirements for a desired operating region in terms of misseddetection and false alarm rates. As a result, using the proposed trust scheme enables us to relax the sensitivity requirements on the cognitive radio devices and potentially reduce the cost. The presented results confirm the significance of integration of the proposed trust system into cooperative spectrum sensing.−96 −94 −92 −90 −88 −86 −84 −82.

**2) Dynamic attackers:** We analyze the performance of our proposed trust scheme with trust-aided outlier detection in mitigating dynamic attackers. We assume that at the beginning of each Monte Carlo simulation 10% of the nodes are malicious ISSDF attackers and during the time of the simulation another 10% of the nodes become malicious. Therefore, at the end of a Monte Carlo simulation, in total 20% of the nodes are malicious. Figure 11 shows that our trust scheme can effectively mitigate dynamic ISSDF attackers who become malicious when the network is in operation.

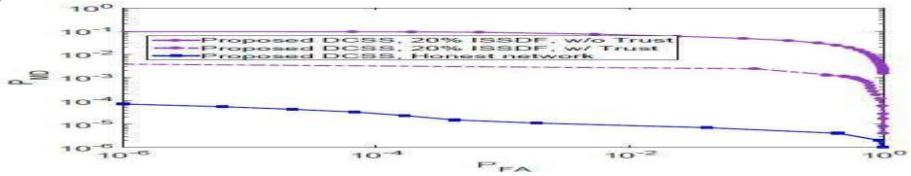


Fig. 5. Dynamic ISSDF attack and mitigation with trust management

## IX. CONCLUSION

In this paper we present a novel trust-aware consensusinspired scheme for distributed cooperative spectrum sensing that is robust against malicious Insistent Spectrum Sensing Data Falsification (ISSDF) attacks. The proposed equallyweighted linear iteration-based scheme is a practical methodfor ad hoc networks because it does not require the nodes to have any topology knowledge. We compare the performance of the proposed scheme against other more complex consensusbased methods and show that despite the simplicity, the performance enhancement through cooperation is as effective as the other schemes. We evaluate our proposed trust management scheme in the presence of collusive fabricating ISSDF attackers with various severity levels through extensive Monte Carlo simulations. We show that integration of our trust management with the proposed equally-weighted consensusbased scheme improves the performance in terms of misseddetection and false alarm error rates by as much as two orders of magnitude. Furthermore, we present an analysis of the operating characteristic curves and the desired operating regions and we show that adopting the proposed trust scheme increases the dynamic range of the supported sensitivity thresholds of the cognitive radio devices and therefore can reduce the cost and enhance the flexibility of the cooperative system.

## REFERENCES

[1] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in IEEE International Conference on Communications (ICC), vol. 4, 2006, pp. 1658–1663.

[2] Q. Wu, G. Ding, Y. Xu, S. Feng, Z. Du, J. Wang, and K. Long, "Cognitive internet of things: A new paradigm beyond connection," Internet of Things Journal, IEEE, vol. 1, no. 2, pp. 129–143, 2014.

[3] H. ElSawy and E. Hossain, "Two-tier hetnets with cognitive femtocells: Downlink performance modeling and analysis in a multichannel environment," Mobile Computing, IEEE Transactions on, vol. 13, no. 3, pp. 649–663, March 2014.

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

[5] "Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands," IEEE Standard 802.22, 2011.

[6] L. Xiao, S. Boyd, and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks. IEEE Press, 2005.

[7] D. Kempe, A. Dobra, and J. Gehrke, "Gossip-based computation of aggregate information," in 44th Annual IEEE Symposium on Foundations of Computer Science Proceedings, Oct 2003, pp. 482–491.

[8] R. Olfati-Saber, J. Fax, and R. Murray, "Consensus and cooperation in networked multi-agent systems," Proceedings of the IEEE, vol. 95, no. 1, pp. 215–233, Jan 2007.

[9] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in INFOCOM. The 27th Conference on Computer Communications, April 2008, pp. 31–35.

[10] L. Xiao and S. Boyd, "Fast linear iterations for distributed averaging," in 42nd IEEE Conference on Decision and Control, vol. 5, Dec 2003, pp. 4997–5002.

[11] N. Ahmed, D. Hadaller, and S. Keshav, "Guess: Gossiping updates for efficient spectrum

sensing," in Proceedings of the 1st International Workshop on Decentralized Resource Sharing in Mobile Computing and Networking. New York, NY, USA: ACM, 2006, pp. 12–17.
[12] A. Vosoughi, J. Cavallaro, and A. Marshall, "A cooperative spectrum sensing scheme for cognitive radio ad hoc networks based on gossip and trust," in 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Dec 2014, pp. 1175–1179.
[13] Z. Li, F. R. Yu, and M. Huang, "A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios," IEEE Transactions on Vehicular Technology, vol. 59, no. 1, pp. 383–393, 2010.
[14] W. Zhang, Y. Guo, H. Liu, Y. Chen, Z. Wang, and J. Mitola, "Distributed consensus-based weight design for cooperative spectrum sensing," Parallel and Distributed Systems, IEEE Transactions on, vol. 26, no. 1, pp.
54–64, Jan 2015.
[15] S. Sundaram and C. Hadjicostis, "Distributed function calculation via linear iterations in the presence of malicious agents - part I: Attacking the network," in American Control Conference, June 2008, pp. 1350– 1355.
[16] H. Zhang and S. Sundaram, "Robustness of complex networks with implications for consensus and contagion," in Decision and Control (CDC), 2012 IEEE 51st Annual Conference on, Dec 2012, pp. 3426– 3432.
[17] E. Yildiz, D. Acemoglu, A. E. Ozdaglar, A. Saberi, and A. Scaglione, "Discrete opinion dynamics with stubborn agents," Available at SSRN: http://ssrn.com/abstract=1744113, Jan 2011.
[18] M. Pirani and S. Sundaram, "Spectral properties of the grounded laplacian matrix with applications to consensus in the presence of stubborn agents," in American Control Conference (ACC), 2014, June 2014, pp. 2160–2165.
[19] J. Ghaderi and R. Srikant, "Opinion dynamics in social networks: A local interaction game with stubborn agents," in American Control Conference (ACC), 2013, June 2013, pp. 1982–1987.
[20] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," SIGMOBILE Mob. Comput. Commun. Rev., vol. 13, no. 2, pp. 86–95, Sep. 2009.
[21] R. Zhang, J. Zhang, Y. Zhang, and C. Zhang, "Secure crowdsourcingbased cooperative spectrum sensing," in INFOCOM, 2013 Proceedings IEEE, April 2013, pp. 2526–2534.
[22] S. Kalamkar, P. Singh, and A. Banerjee, "Block outlier methods for malicious user detection in cooperative spectrum sensing," in Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th, May 2014, pp. 1–5.
[23] S. Liu, H. Zhu, S. Li, X. Li, C. Chen, and X. Guan, "An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum sensing," in Global Communications Conference (GLOBECOM), 2012 IEEE, Dec 2012, pp. 603–608.
[24] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. Hou, "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks," in INFOCOM, 2012 Proceedings IEEE, March 2012, pp. 900–908.