Reputation Aware Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks

Muhammad Faisal Amjad[†], Baber Aslam[‡], Cliff C. Zou[†]
[†]Department of Electrical Engineering and Computer Science, University of Central Florida, USA
[‡] National University of Sciences & Technology, Pakistan
[†]{faisal, czou}@cs.ucf.edu [‡]baber-mcs@nust.edu.pk

Abstract – **The task of spectrum sensing for Dynamic Spectrum Access in Cognitive Radio Networks (CRNs) is very challenging in the presence of malicious secondary users that may launch Spectrum Sensing Data Falsification (SSDF) attacks. Existing solutions to detect such malicious behaviors cannot be utilized in scenarios where the transmission range of primary users is limited within a small sub-region of the CRN, such as low-power primary user devices like wireless microphones or emergency warning systems for vehicles. In this paper, we present a reputation system that works in the scenarios described above in conjunction with a semi-supervised spatio-spectral anomaly/outlier detection system. This system guarantees protection of incumbent primary users' communication rights while at the same time making optimal use of the spectrum when it is not used by primary users. Simulation of our proposed scheme under typical network conditions and SSDF attack shows that spectrum decision error rate is reduced to be less than 2% and detection rate of malicious secondary users is up to 95%.**

I. INTRODUCTION

Cognitive Radio Network (CRN) is a natural development in wireless communications to increase the utilization of a scarce spectrum resource, especially in greatly under-utilized licensed spectrum bands such as TV broadcast. Interest in the development of CRNs is a direct consequence of numerous studies such as [1]. These studies demonstrate severe under-utilization of spectrum bands by the incumbent *Primary Users* (PUs) that have the license to use them, and an ever-increasing demand for unlicensed spectrum for a variety of new mobile and wireless applications. The essence of Cognitive Radio (CR) operation is the opportunistic utilization of licensed spectrum bands by the *Secondary Users* (SUs) that collectively form the CRN, without causing any disruption to PUs' communications.

Collaborative spectrum sensing is essential in situations where the PUs' transmission range is much smaller than the size of the CRN e.g. a wireless microphone, since PU's signal may only be received by a small subset of the SU nodes. In such situations, the Fusion Center (FC) *has to* rely on spectrum sensing reports from SUs spread across the CRN. However, collaborative spectrum sensing can also be very favorable to malicious nodes in the network, which may launch SSDF attack [2]. Such an attack may adversely affect spectrum sensing decisions, which in turn, may cause harmful interference to the PUs or deny the use of the vacant spectrum bands. An SSDF attack may be aimed at gaining spectrum opportunities for the malicious nodes' own advantage or to disrupt CRN operation. As shown in the next section, efforts have been made to defend against SSDF attacks in CRNs, few have attempted to deal with the situation where PUs are mobile and their transmission range is small as compared with the overall CRN size.

A CRN is vulnerable to selfish or malicious behavior because if left unchecked, the SSDF attacks may result in disruption of its operation to an extent that may even jeopardize its existence. Reputation systems have frequently been used in computer networks to guard against malicious behavior from their entities. Reputation score typically represents an entity's long term contribution in a network's operation. The reputation scores are usually derived from some form of a voting mechanism and are used as weights in the system's decision making process. However, any reputation system based on voting from *all* of network's nodes will not work in situations where a PU's transmission can be received by only a small subset of nodes in the CRN.

In this paper, we present a novel reputation-aware collaborative spectrum sensing framework for ad hoc cognitive radio networks based on spatio-spectral anomaly detection. It can reliably detect malicious SUs and make the correct spectrum sensing decisions under SSDF attack. It is especially suited for situations where PUs have a smaller transmission range compared to the coverage area of the CRN. Simulation of our proposed scheme shows that spectrum sensing decision error rate can be reduced to less than 2% and accuracy of detecting malicious SUs increased up to 95%.

Specifically, we have made following contributions:

- Identified limitations of existing CRN spectrum sensing and reputation systems in dealing with short-range PUs.
- Developed spectral map construction system and formulated spatio-spectral anomaly/outlier detection for CRNs with short-range PUs.
- Proposed a novel reputation system to defend against SSDF attacks through spatio-spectral anomaly/outlier detection.

II. RELATED WORK

The idea of using Beta Reputation System as reputation evaluation system has been proposed in [3] in which a node's confidence in its spectrum sensing report is used as a weight during calculation of spectrum decisions. This work assumes that the PU's transmission range is large enough to be received by all nodes in the CRN including the SU base station (SUBS), the controlling entity of the CRN. It also assumes that the PU can communicate with SUBS, wherein a PU may complain to the SUBS regarding any interference caused by CRN operation. Since this work assumes that the PU cannot sell its unused spectrum bands, therefore there is no incentive for it to communicate with the CRN. This communication may cost a PU, additional hardware and/or system complexity, just to inform the CRN regarding interference caused to its communications. Furthermore,

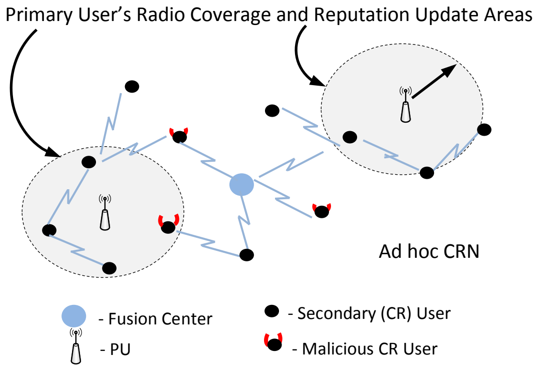

Figure-1: Ad hoc CRN with malicious nodes. Spectrum sensing reports only in PU's coverage area should be considered for spectrum decisions, and only those SUs' reputation scores will be updated.

the FCC requires that the CRN may use vacant spectrum bands in a non-interfering basis without the need for any changes to the incumbent PU. This work also does not deal with any mobility by SUs or PUs.

A collaborative spectrum sensing scheme is presented in [4] which introduces Location Reliability and Malicious intent as trust parameters. The authors employ the Dempster-Shafer theory of evidence to evaluate trustworthiness of reporting secondary user nodes. The proposed scheme assigns trust values to different cells in the network which may receive abnormal levels of PU's signal due to the effects of multi-path, signal fading and other factors in the radio environment. Equal emphasis is given to the spectrum sensing reports from SUs using Equal Gain Combining while using trust values of the cells from where these reports were received as weights for data aggregation. This approach also assumes that the PU's communication range is large enough to be received by the entire CRN and uses the spectrum sensing reports of all CRN nodes to reach the final spectrum decision.

Authors in [5] and [6] assume that the transmission range of PU is large enough to be received in the entire CRN. [5] proposes pre-filtering to remove extreme spectrum sensing reports and a simple average combining scheme to calculate spectrum sensing decisions while considering all reports that pass the pre-filtering phase. [6] characterizes the spectrum sensing problem as an M-ary hypotheses testing problem and considers a cluster-based CRN where cluster heads receive and process raw spectrum sensing data before forwarding to the fusion center. Since PU's transmission range is assumed to be large enough to be received by every node in the network, both approaches cannot be adopted for a CRN in which a PU has smaller transmission range than the size of CRN.

III. Assumptions and System Model

We model the Ad hoc CRN (Figure-1) as a region in which the PUs and SUs are mobile under the Random Waypoint mobility model [7]. There can be one or more PUs operating within the CRN at any given time. With techniques such as Radio Frequency Fingerprinting (RFF) [8], devices in the CRN can be uniquely identified. Therefore, in this paper, we treat it as a black box and assume that nodes in the CRN as well as the FC are capable of performing RFF and uniquely identifying other nodes and PUs. A Spectrum band is considered to be *vacant* when it is not being used by a PU, and *occupied* otherwise. After every Channel Detection Time (CDT) slot, which is also the reputation update cycle, SUs report their sensed Received Signal Strength (RSS) to the FC, which is a SU in the CRN, selected to aggregate spectrum sensing data from SUs and make spectrum sensing decisions. Selection of FC may be carried out in a similar manner as cluster heads are selected in various kinds of networks [9-10]. However, selection of FC is out of the scope of this paper and is assumed to be achieved by other protocols. It is also assumed that SUs have an on-board GPS device, know their location at all times and include this information in every spectrum sensing report.

Let $P_{r,i,k}$ denote the received signal strength at secondary user i at time k, which can be calculated according to [11]:

$$P_{r,i,k} = G_{r,i}.P_t.G_t.\left(\frac{\lambda}{4\pi S_{i,k}}\right)^2 \qquad (1)$$

where $G_{r,i}$ is the antenna gain of node i, P_t is the transmitted power of the PU and G_t is antenna gain of the PU, λ is PU signal's wavelength and $S_{i,k}$ is distance between the PU and receiving SU i at time k. From Equation (1), we define RSS levels as discrete annular regions with γ_m as width of a region for a given RSS level m (see Figure-2). A node i, whose reported RSS satisfies the condition $m \leq P_{r,i,k} < m+1$, belongs to RSS level m.

After every CDT slot k, each SU i sends its spectrum sensing report to the FC, which includes the RSS value $P_{r,i,k}$ and its location $l_{i,k}$. This is essential for the FC to construct a spatio-spectral map of the entire CRN which is then utilized to calculate spectrum occupancy decision. We also define a *Detection Threshold* τ, which corresponds to the RSS level below which a PU's signal is not considered to have been detected.

Because of the limited transmission range of a PU, it is possible that the FC does not receive PU's signal directly when the PU is far away. For a robust system design, we assume that the FC always relies on the reports from the SUs to construct the spatio-spectral map of the CRN. However, with the presence of malicious nodes in the CRN, which may provide false spectrum sensing information to the FC, the accuracy of the spectrum sensing decisions could be severely degraded thereby jeopardizing the operation of the CRN. Presence of malfunctioning nodes i.e. *Byzantine Failure,* is also considered as a SSDF attack, in this paper.

IV. Reputation Aware Spectrum Sensing Framework

Spectrum sensing reports from SUs for detecting a PU can vary a lot because of (1) small communication range of PUs relative to the size of CRN, and (2) mobility of both SUs and PUs. This situation is, however, very suitable for malicious nodes to launch SSDF attack and cause errors in spectrum decisions. It is therefore vital for the FC to identify malicious nodes and prevent them from inducing spectrum decision errors. To detect malicious nodes and guard against SSDF attacks, our proposed reputation aware spectrum sensing framework has three components: 1) Spatio-spectral anomaly detection, 2)

Spectrum sensing data aggregation, and 3) Reputation management.

A. Semi-Supervised Spatio-Spectral Anomaly Detection

The first phase of our spectrum sensing framework has three steps: (1) Gathering of spectrum sensing reports from the SUs at the FC; (2) Construction of the CRN's spectral map; (3) Detecting of anomalies in these reports for current CDT slot. Step 1 is conducted by using existing routing protocols, which is not the focus of this paper. In this section we introduce the second and third steps as follows.

Spectral Map Construction: In order to calculate the location of the PU and construct its spectral map, we employ the *Kåsa method* of circular regression, which is an algebraic fitting algorithm whose implementation details can be found in [12]. On a two-dimensional plane, we want to find a circle that best fits the given set of points that represent reporting SUs locations in a sense of least squares approximation. The fitted circle is assumed to have the center point *(a, b)* and a radius of *R*. The observed set of n points that represent n reporting SUs' locations is given by $\{(x_i, y_i),\ i \in 1,2,\cdots,n\}$.

The calculated center of the annular region is the result of n SUs reporting the same RSS level, and with increasing n, the accuracy of PU location calculation also increases. We carry out the same process of circular regression with each of the K RSS levels for which the number of reporting SUs is at least 3. Calculation of PU's location with K RSS levels is done as follows: Let $(a_k,\ b_k)$ be the center of the annular region, calculated for RSS level k, where $k \in (1,2,\dots,K)$. If n_k is the number of SUs that reported RSS level k, then the final location (a^F, b^F) of the PU, is calculated as a weighted average of K points as:

$$a^F = \frac{\sum a_k \,.\, n_k}{\sum n_k}, \quad b^F = \frac{\sum b_k \,.\, n_k}{\sum n_k}$$

Anomaly/Outlier Detection: A report from a SU has the RSS as well as the node's current location. Both of them can be falsely reported by malicious nodes. Based on the RSS values calculated at different ranges for a particular kind of PU transmitter and the constructed spatio-spectral map of the CRN, we define the normal behavior for reporting SUs in the form of lower and upper bounds on the distance between a given pair of RSS levels. These lower and upper bounds on normal behavior are formulated as matrices φ and ψ respectively, where the elements of these behavior matrices are derived as:

$$\varphi_{i,j} = \begin{cases} \sum_{m=i+1}^{j-1} \gamma_m & if\ \ j-i > 1 \\ 0 & if\ \ |i-j| \le 1 \\ \sum_{m=j+1}^{i-1} \gamma_m & if\ \ j-i < -1 \end{cases} \tag{2}$$

$$\psi_{i,j} = \sum_{m=1}^{i} \gamma_m + \sum_{m=1}^{j} \gamma_m \tag{3}$$

where the element $\varphi_{i,j}$ is the *minimum* distance and the element $\psi_{i,j}$ is the *maximum* distance between RSS levels i and j.

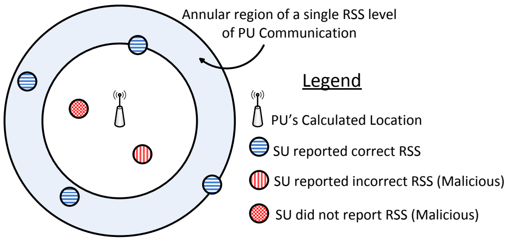
Annular region of a single RSS level of PU Communication
Legend
PU's Calculated Location
SU reported correct RSS
SU reported incorrect RSS (Malicious)
SU did not report RSS (Malicious)

Figure-2: After estimation of PU's location/spectral map, SUs are classified as malicious/normal through outlier detection. In this figure one malicious node is calculated as within PU's coverage area but did not report PU's presence while the other malicious node reported false RSS level.

After gathering all reports from the SUs, the FC compares every reported RSS level with all other reported RSS levels, and classifies the distance between the nodes whose RSS levels are being compared, as either a normal or abnormal distance. This classification is performed by comparing the distance with both the minimum as well as maximum distance matrices. At the end of distance classification, the number of normal and abnormal distances of a given node from all other reporting nodes is compared. If majority of a node's distances are normal then the node is considered honest in the current CDT slot, otherwise it is treated as a malicious node and its reputation score is decremented by the reputation management system as follows: Consider the set of spectrum sensing reports S in a given CDT slot, to be

$$S = \{s_1\,(l_1,\, r_1),\ s_2\,(l_2,\, r_2),\ \ldots\ldots\ s_m\,(l_m,\, r_m)\}$$

where l_m is the location and r_m is the reported RSS level of node m. Distance between nodes i and j is given by $\delta_{i,j}$ which can be calculated from their reported location information. Classification of a distance between a pair of nodes j and k, denoted by $C_{i,j}$, is given as:

$$C_{i,j} = \begin{cases} 1 & if \quad \varphi_{r_i,r_j} \le \delta_{i,j} \le \psi_{r_i,r_j} \\ -1 & \quad otherwise \end{cases} \tag{4}$$

where $C_{i,j} = 1$ represents that the distance is within normal range and -1 means that the distance does not match with the respective location information of the nodes and therefore classified as abnormal. The final classification of a node as an outlier, denoted by $\Theta_{j,k}$, is done as:

$$\Theta_{j,k} = \begin{cases} 0 & if\ \sum_{j=1}^{m} C_{j,k} \ge 0 \\ 1 & otherwise \end{cases} \tag{5}$$

where $\Theta_{j,k} = 0$ represents that node j is a normal node at time slot k, and 1 represents an outlier node (abnormal node) at CDT slot k.

B. Spectrum Sensing Data Aggregation and Spectrum Decision

Typically, spectrum sensing reports are aggregated using voting mechanisms based on either the majority rule, the AND rule or the OR rule [13]. As evident from Figure-1, these aggregation rules cannot be applied in situations where PU's transmission range is much smaller as compared with the overall size of the CRN. This is because even in the absence of malicious nodes, the number of nodes receiving PU's signal is expected to be much less than the total number of nodes in the CRN. Therefore, our proposed spectrum data aggregation technique determines the presence or absence of PU within an area of CRN that is equal to the PU's transmission range. When all spectrum reports are collected at FC, each node is classified as behaving normally or abnormally, in every CDT slot. This node classification at each CDT slot can be viewed as a node's instantaneous reputation; however, the reputation score of every node used in our proposed system is accumulated by every node with the passage of time and can be viewed as its long-term reputation.

For the purpose of data aggregation, we use *soft-combining* technique where, instead of its spectrum sensing decision, a CRN node reports its RSS level to the FC. Then the FC aggregates these reports to calculate its final spectrum sensing decision. Nodes, whose spectrum sensing reports were considered anomalous in current CDT slot, are classified as outliers and their reputation scores are decremented. Spectrum sensing reports that pass the anomaly detection phase are next processed in data aggregation phase to determine if they can be used in spectrum decision calculation. In our reputation-aware spectrum sensing framework, a node has to have a minimum reputation score to be considered honest at the current CDT slot, for its report to be included in calculation of spectrum decision. Calculation of reputation score and classification of a node as either honest or malicious is explained in the next section. The two-stage approach for behavior classification mentioned above, is used because a malicious node may report correct spectrum sensing results in some of the CDT slots to hide its SSDF attacks with a few correct reports, as well as to improve its reputation score.

A node once labeled as *malicious* may regain an *honest* status by providing correct spectrum sensing reputation, however, the rate of reputation improvement is much slower than its decline. This difference in the rate of reputation change ensures that the malicious nodes cannot easily manipulate their reputation scores to their advantage.

In a CDT slot k, if no honest SU reported presence of a PU's signal then the spectrum decision D_k , is *'vacant'*. If there were some reports from honest nodes that indicated presence of PU's signal on the spectrum band, then a majority vote is conducted based on a *Detection Threshold* τ, to determine the spectrum sensing decision:

$$D_{j,k} = \begin{cases} 1 & if \quad r_{j,k} > \tau \\ -1 & if \quad 0 < r_{j,k} \leq \tau \end{cases} \tag{6}$$

$$D_k^F = \begin{cases} 1 & if \quad \sum_{j=1}^{m} D_{j,k} \geq 0 \\ 0 & \quad otherwise \end{cases} \tag{7}$$

where $D_{j,k}$ is the spectrum sensing decision (*occupied* = 1, *vacant* = -1) from report $r_{j,k}$ of node j and D_k^F is the final spectrum sensing decision (*occupied* = 1, *vacant* = 0) of the CRN for CDT slot k.

C. Reputation Management

Reputation management is undertaken by the FC in two phases, each after the execution of the two modules presented in sections IV-A and IV-B above, i.e. after the spatio-spectral anomaly detection phase and spectrum sensing data aggregation and decision phase.

A reputation table is implemented as a two-tiered sliding window for every node in the CRN, as shown in Figure-3. Implementation of the reputation table as a sliding window serves two purposes: first, it represents the latest behavior of a node and prevents malicious nodes from taking advantage of their reputation score from distant past, and second, it gives a chance to falsely-labeled nodes to improve their standing in the CRN by having a forgetting characteristic of the sliding window. The two-tiered implementation of reputation table is used to normalize the difference between the speed of a node's mobility and the frequency of its spectrum sensing reports. Once the lower tier of the reputation table is filled, a corresponding entry based on majority rule, is placed in the upper tier. After placing an entry in the upper tier, the lower tier is reset and the upper tier is slid forward one space.

Reputation Update Phase-1: When a node has been classified as behaving either normally or abnormally according to Equation (5), a corresponding entry R_j is added in the lower tier of the reputation table, where an *outlier* entry corresponds to $R_j = 1$ and a *normal* entry corresponds to $R_j = 0$.

Reputation Update Phase-2: When the final spectrum sensing decision D_k^F has been made, SUs whose spectrum sensing reports contributed positively towards reaching the final decision are rewarded and the SUs whose reports contributed negatively towards reaching the final spectrum sensing reports are punished by the reputation update module, by adding relevant *malicious / honest* entries R_j in the lower tier of their reputation tables. However, the second phase of reputation update is slightly more complex than the first phase, as follows: After the anomaly detection phase is over and all abnormal reports have been filtered out, rest of the reports are aggregated to reach a spectrum decision, which can have two outcomes: spectrum 'vacant' or 'occupied' by a PU. The reputation system takes different courses of action for the two spectrum decisions: If the spectrum decision was 'vacant', then all nodes that reported presence of PU's signal are punished by adding a malicious entry R_j=1 in the lower tier of the reputation table. However, if the spectrum decision was 'occupied' then the FC has to first determine the location of the PU in order to reward or punish the nodes in PU's coverage area only, as shown in Figure-1.

The FC carries out circular regression [12] based on the reported locations and RSS levels of the honest nodes demonstrating normal behavior only, and determines the estimated location of PU. Estimation of PU's location and its coverage area with the help of circular regression is reasonable due to the PU's very short transmission range, i.e., 100 - 200m. Based on the same spectrum reports, the FC then constructs a spectral map of the PU and calculates the expected spectrum sensing reports. For a given CRN node, if reported and expected spectrum sensing reports do not match, then a malicious entry R_j=1 is added in the lower tier of the node's reputation table. Otherwise, an

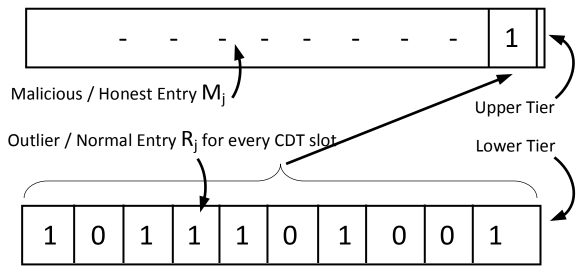
- - - - - - - - -
1
Malicious / Honest Entry M_j
Upper Tier
Outlier / Normal Entry R_j for every CDT slot
Lower Tier
1 0 1 1 1 0 1 0 0 1

Figure-3: The two-tiered sliding window reputation table

'honest' entry R_j=0 is added. Classification of a CRN node j to be malicious or otherwise at CDT slot k is represented by the upper tier reputation table entry M_j and is done based on the following:

$$R_j = \begin{cases} 0 & if \quad normal\ behavior \\ 1 & \quad\quad outlier \end{cases}$$

$$M_j = \begin{cases} 0 & if \quad \sum_{l=1}^{N} R_{j,l} \le T \\ 1 & \quad\quad otherwise \end{cases}$$

where R_j is the reputation table entry for node j and N is the size of lower tier of the reputation table. T is the threshold for a node's reputation score to be considered malicious or honest. In this manner, the decision to reward or to punish a node is reached by the reputation system by determining if the node contributed towards or against the final spectrum sensing decision.

V. Performance Evaluation

In this section we present an evaluation of our proposed reputation aware collaborative spectrum sensing framework to defend against SSDF attack. For the purpose of our simulations, we define SSDF attack as follows: A SSDF attack refers to malicious nodes reporting absence of PUs from the spectrum band, which in fact, are currently using the spectrum. The purpose of this attack is to trick the CRN into believing that the spectrum is vacant and "induce" transmission by SUs thereby causing interference to the PUs. We refer to such an attack as an *Induction* attack and use the term Induction attack and SSDF attack interchangeably. This attack can have devastating and far reaching effect on the CRN, as it can cause harmful interference to PU's signal and can jeopardize the existence of the CRN.

A. Simulation Setup

For the purpose of evaluating our proposed framework for defending against aforementioned SSDF attack, we have considered an ad hoc CRN with the dimension of 1000m x 1000m, in which there exists a single PU and many SU nodes. Both the PU and the SUs are mobile under the Random waypoint mobility model [5], with their speed varying between 0 and 4m/s and maximum transmission ranges for both the PU and the SUs is 200 meters. We have conducted simulations with multiple PUs operating within the CRN's area, however, we do not present those results here due to space limitation. We have carried out simulations for both dense (100 SU nodes) and sparse (50 SU nodes) network configurations.

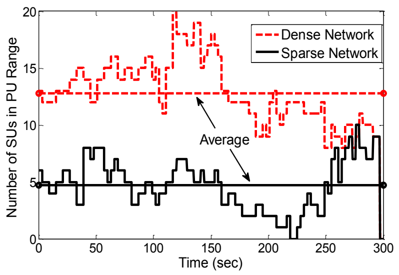

Figure-4: Average number of SUs in PU's range at various time intervals

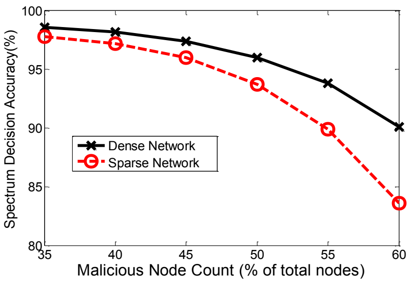

Figure-5: Spectrum Decision Accuracy under Induction Attack in Dense and Sparse

Figure-4 shows the number of SUs within PU's transmission range at a given point in time during a simulation run, with the mean of 4.7 and variance 5.1 for a sparse network and a mean of 12.7 and variance 9.2 for a dense network. The threshold T for a node to be considered as malicious was studied for 3, 9 and 15 malicious entries in the reputation window with the total reputation window size of N=*20*. However, due to space limitations, the malicious threshold value considered for this paper is kept at T=*3*. Spectrum sensing reports are generated by the SUs in every CDT slot, which equals 100 msec. These sensing reports are then aggregated by the FC to reach the final spectrum sensing decision M_j for the current CDT slot. All the graphs represent results that are averaged over 100 simulation runs each.

B. Simulation Results

Spectrum sensing accuracy is the most important metric with regards to the collaborative spectrum sensing because the existence of the CRN depends on accurate spectrum sensing decisions. Performance of our proposed reputation aware collaborative spectrum sensing framework with respect to spectrum sensing accuracy is shown in Figure-5. As the number of malicious users in the CRN grows, it will have a negative impact on the overall spectrum sensing decisions. Our proposed framework successfully detects malicious behavior and reaches correct spectrum sensing decisions up to 99.3% of the time when malicious nodes are 10% of the entire SUs, which is a fairly large number of malicious nodes. Spectrum decision accuracy of our proposed framework drops to 97% with malicious node count of 35%, which is a highly unlikely number of malicious nodes in a network.

In order to launch a successful Induction attack in a CRN, a malicious node has to report the absence of the PU in the spectrum band when it is actually been used by a PU. The honest nodes in the vicinity of a malicious node will, however, report the presence of the PU and the attempted attack on the CRN will fail. This makes the

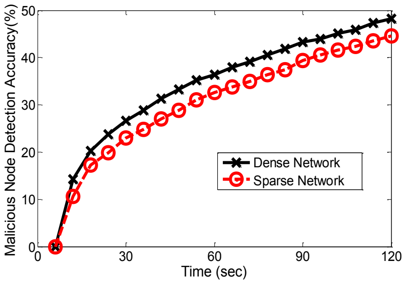

Figure-6 Malicious Node Detection Accuracy under SSDF attack

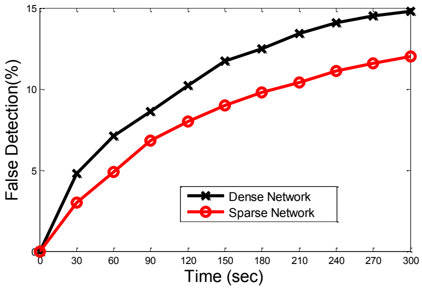

Figure-7: Percent of Honest nodes falsely labeled as Malicious

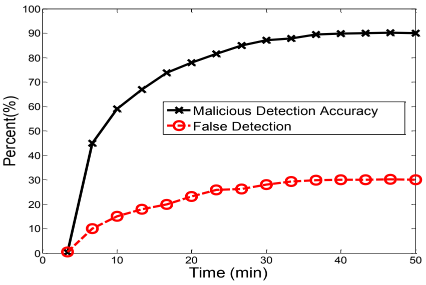

Figure-8: Time to achieve steady state for detecting malicious nodes under SSDF Attack

Induction attack difficult to launch successfully. In order to find out exactly how difficult it is to launch an Induction attack, we increased the malicious node probability to 60% of the total nodes in the CRN as shown in Figure-5, which shows that the attack's success rate was around 6% for a sparse network and our reputation framework was able to achieve a spectrum decision accuracy of 90% for a dense network.

Figure-6 shows the speed and accuracy of our proposed framework to detect malicious nodes in dense as well as sparse networks under the SSDF attack. As discussed earlier, the Induction attack is difficult to launch successfully; on the other hand, it is also difficult to detect malicious nodes launching an Induction attack. To accurately identify a malicious node launching an Induction attack, PU localization has to be perfect. However, since PU localization will always have some degree of error, if a node did not report the presence of a PU, we can never be absolutely certain whether the node really did not sense the PU since it is out of the PU's transmission range, or it was launching an Induction attack. Once an estimated PU location is calculated, if the number of nodes in its transmission range that did not report presence of PU is more than the number of nodes that reported PU's presence, then this condition is considered to have been caused due to PU localization error and nodes suspected of providing false spectrum sensing reports are not punished. In this manner, the reputation framework is very careful so as not to punish honest nodes on which the system relies for future spectrum decisions. This careful handling of induction attack by the reputation framework results in slower detection of malicious nodes.

Figure-7 shows the error rate of categorizing an honest node as a malicious node by our proposed reputation framework under SSDF attacks. For the duration of every simulation run i.e. 300 sec, false detection percentage is less than 15%. Figure-8 shows the long term dynamic for malicious detection accuracy under Induction attack as well as false detection percentage.

VI. Conclusion and Future Work

In this paper we have proposed a novel reputation aware collaborative spectrum sensing framework based on spatio-spectral anomaly detection. Our proposed system is well suited for situations where the PU's communication range is limited within a sub-region of the CRN. Simulations of our system show that it is robust against SSDF attacks and can detect malicious behavior up to 99.3 percent of the time when malicious node density is within a reasonable range and is still very effective when the number malicious nodes is even greater. Our proposed system is also flexible enough to be used where PU's communication range spans the entire CRN. We are studying other kinds of SSDF attacks in similar settings and will present the results in a future work.

References

[1] Taher, T.M, et al., "*Long-term spectral occupancy findings in Chicago*," New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2011.

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

[3] Qin, T., et al., "Towards a trust aware cognitive radio architecture," SIGMOBILE Mobile Computational Communication Reviews 2009, pp. 86–95.

[4] Jana, S., et al., "Trusted collaborative spectrum sensing for mobile cognitive radio networks," 32nd IEEE International Conference on Computer Communications, INFOCOM 2012.

[5] P. Kaligineedi., et al., "Secure Cooperative Sensing Techniques for Cognitive Radio Systems", International Conference on Communications, ICC 2008.

[6] Jin Wei., et al., "Two-Tier Optimal-Cooperation Based Secure Distributed Spectrum Sensing for Wireless Cognitive Radio Networks," IEEE INFOCOM 2010

[7] J. Broch et al., "A performance comparison of multi-hop wireless ad hoc network routing protocols", Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking(Mobicom98), October 1998.

[8] C. C. Loh et al., "Identifying unique devices through wireless fingerprinting," in Proc. of the first ACM conference on Wireless network security, Mar. 2008, pp. 46–55.

[9] I. F. Akyildiz,W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Netowrks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug 2002.

[10] A. Amis, R. Prakash, T. Vuong, and D. Huynh, "Max-Min D-Cluster Formation in Wireless Ad Hoc Networks," IEEE INFOCOM, March 2000.

[11] C. A. Balanis., "Antenna Theory: Analysis and Design," 2nd Edition, John Wiley and Sons, Inc. 1997.

[12] N. Chernov., "Circular and linear regression: Fitting circles and lines by least squares", Chapman & Hall/CRC June 2010.

[13] Xu, S., et al. "Double thresholds based cooperative spectrum sensing against untrusted secondary users in cognitive radio networks." IEEE VTC 2009.