DS3: A Dynamic and Smart Spectrum Sensing Technique for Cognitive Radio Networks Under Denial of Service Attack

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

***Abstract* – IEEE 802.22 Cognitive Radio Networks (CRN) employ a two-stage quiet period mechanism based on a mandatory *Fast Sensing* and an optional *Fine Sensing* stage for Dynamic Spectrum Access (DSA) during every super frame. However, the two-stage spectrum sensing approach presents an opportunity to malicious users where they can launch a smart Denial of Service (DoS) attack by transmitting a very short jamming signal during the fast sensing stage and thus forcing the CRN to carry out fine sensing, thereby wasting spectrum opportunities for honest Secondary Users (SU). In this paper, we present *'DS3'*: A *Dynamic* and *Smart Spectrum Sensing* algorithm, which minimizes the effects of jamming as well as noise on the fast sensing phase of DSA. It improves system's efficiency by striking a balance between spectrum utilization by SUs and delay in the detection of Primary Users' (PU) presence on the spectrum, using a dynamic fine sensing decision algorithm with minimal overhead.**

I. INTRODUCTION

IEEE 802.22 based CRNs are Wireless Regional Area Networks (WRAN) that are intended to provide Internet access to under-served areas by opportunistically accessing the analog TV bands made available by FCC for unlicensed use [1]. Devices in a CRN are required to sense the spectrum periodically and vacate the spectrum band if they detect the presence of incumbent PU. Therefore, CRNs employ a two-stage spectrum sensing approach: the stages called fast sensing and fine sensing [1]. Fast sensing typically takes a few microseconds and uses simple techniques such as energy detection, and therefore can only report the presence or absence of a signal on the spectrum band. On the other hand fine sensing employs sophisticated techniques for identification of signal types on the spectrum and may take up to 160 msec i.e. the entire duration of a super frame also called the Channel Detection Time (CDT) [1]. This two stage mechanism is meant to strike a balance between the conflicting goals of proper protection of incumbent PU's signals and optimum QoS for CRN's SUs.

Devices in a CRN carry out the mandatory fast sensing during every CDT slot. The result of fast sensing is reported by all SUs to the CRN base station (BS) which then decides if fine sensing needs to be carried out. To ensure that everyone in the CRN senses PU's signals and not their own, quiet period for spectrum sensing are synchronized. Present IEEE 802.22 draft standard mandates the CRN to *always* carry out fine sensing when the fast sensing stage reports presence of any signal on the spectrum [1]. Therefore, at the time when PU is not using the spectrum, called *spectrum opportunity* for DSA, malicious users in the CRN can take advantage of the fixed nature of the two stage spectrum sensing mechanism by transmitting a small jamming signal during the fast sensing stage. We call this kind of an attack as a *smart jamming attack.* A smart jamming attack would consume far less energy than for jamming the entire CDT slot and will force the rest of the CRN to carry out fine sensing denying them the spectrum opportunity with an additional benefit of utilizing it for their own communications.

The IEEE 802.22 draft standard imposes an upper bound of 2 seconds called *Maximum Detection Time* or *MDT*, on the maximum delay allowed for the detection of incumbent PU's signal [1], [2]. In order to mitigate the effects of smart jamming attacks on spectrum opportunity utilization, a dynamic spectrum sensing technique is needed. We leverage the MDT constraint along with a cost minimization function to propose Dynamic and Smart Spectrum Sensing algorithm 'DS3'. With DS3, based on the cost factor at every CDT slot, the BS decides whether or not to conduct fine sensing if the fast sensing stage reports presence of any signal on the spectrum band. Specifically, we have made the following contributions in this paper:

- Carried out an analysis of the impact of smart jamming/DoS attack on CRN's dynamic spectrum access.
- Proposed a novel spectrum sensing algorithm called DS3 that allows the CRN base station to dynamically decide if fine sensing should be carried out.
- Carried out simulation experiments of the proposed algorithm and presented the results.

The rest of this paper is organized as follows: Section II presents an overview of the related research work aimed at optimizing DSA and its protection against DoS attacks. Section III lays out our assumptions and the system model for this paper. Section IV presents DS3, our proposed dynamic and smart spectrum sensing algorithm while section V provides a discussion on performance evaluation of DS3. Section VI concludes this paper.

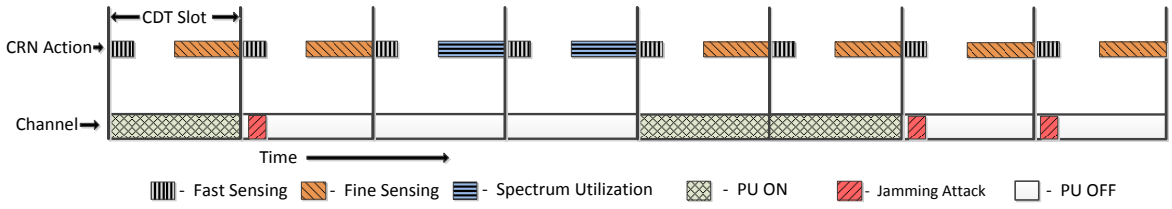

Figure 1: CRN's Dynamic Spectrum Access under Smart Jamming Attack

II. Related Work

Opportunistic spectrum access in CRNs makes them an easy target for attackers that may jeopardize its operation for their individual gains or merely because of malicious intent. Therefore, security of DSA in CRNs has been the focus of attention for many research efforts lately. This section provides an overview of related work and provides an insight as to how these studies differ from the work presented in this paper.

Measures to prevent the jamming of Common Control Channel (CCC) in an ad hoc CRN are presented in [4]. It assumes that the jammers are aware of the protocol specifics as well as cryptographic quantities used to secure network operations. The authors propose two techniques to identify malicious nodes that act independently and those that collude to jam the CCC. They also propose generation and secure dissemination of hopping sequences for the CRN to elude jammers. This however is primarily aimed at defending against jamming the CCC through which spectrum sensing and other control data are shared. On the other hand, our work addresses defense against jamming of spectrum sensing itself.

In [5], authors consider an ad hoc CRN in which they introduce various types of jammers: jammers that jam a fixed channel, a random selection of channels and channels that are predicted to be used next in subsequent time slots. An algorithm is proposed with which senders and receivers learn the jammers' channel access pattern and can evade jamming by hopping to jamming-free channels. Our proposed DS3 algorithm does not resort to channel hopping and evades jamming while staying on the same channel.

A collaborative defense technique is presented in [6] where the SUs in a CRN defend against a collaborative DoS attack launched by sweeping and jamming the channels in the entire spectrum. The SUs make use of spatial and temporal diversity to form proxies in order to continue communicating. This work however does not consider that the jammer may seek to conserve its jamming power budget and jam only the fast sensing stage and the main defense against jamming attack is for the CRN to hop to another channel.

Authors in [7] present a game theoretic approach to defend against jamming attacks in CRNs. They derive an optimal strategy for the SUs to decide whether to remain in the current band or to hop to another band by employing a Markov Decision Process approach. The authors propose a learning process through which SUs estimate current network conditions based on past observations using the maximum likelihood estimation technique. This work also does not consider the two-stage spectrum sensing that is employed in the current IEEE 802.22 WRAN draft standard, and the defense against jamming is for CRN to hop to another channel.

To the best of our knowledge, this is the first attempt to address a smart jamming attack by malicious users and to make maximum utilization of spectrum opportunities while staying in the spectrum band that is being jammed and not hopping away from it.

III. Sytem Model and Assumptions

System Model: We consider an IEEE 802.22 based Cognitive Radio Network in which the SUs are synchronized and carry out the mandatory fast sensing during every super frame (CDT). A CDT slot spans 160 msec [1] whereas the MDT is 2 seconds [3], giving the base station a maximum of

$$\tau = \lfloor MDT / CDT \rfloor \qquad (1)$$

discrete time slots to detect the presence of a PU on the spectrum. During every CDT slot, SUs send their fast sensing report to the BS which after executing our proposed DS3 algorithm, decides if fine sensing is needed in current CDT slot. Malicious users in the CRN launch a smart jamming DoS attack with some probability, by transmitting a short jamming signal during the fast sensing stage in order to force the CRN to conduct fine sensing at every CDT slot.

As shown in figure 1, a malicious user transmits a short jamming signal as compared to the overall length of a CDT slot, synchronized with the fast sensing stage of DSA but it is enough to deny the CRN a spectrum opportunity that may arise due to the absence of the PU from its spectrum band. This is a *smart* jamming attack since it denies the use of spectrum to the CRN while consuming very little energy as compared with jamming the whole CDT slot and at the same time allows the malicious nodes to utilize rest of the CDT slot for their own communications.

Assumptions: Our proposed DS3 algorithm runs at the BS only, and is aimed to replace the existing static fine sensing decision criterion with a dynamic one. The PU's use of spectrum is modeled as a Markov ON/OFF process [8-10] as shown in figure 2, with α being the probability that the PU will transition from state 0 to 1 and β being the transition probability from state 1 to 0. State 0 represents OFF and 1 represents ON state of the PU. Fast

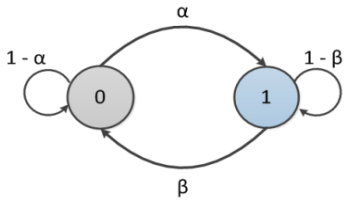

Figure 2: Markov ON/OFF model for PU's Spectrum Usage

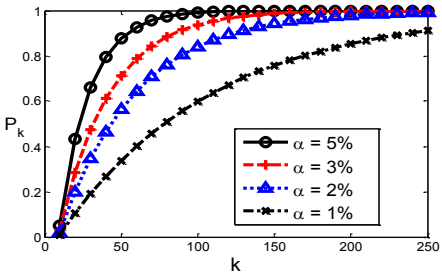

Figure 3: Effect of α on P_k

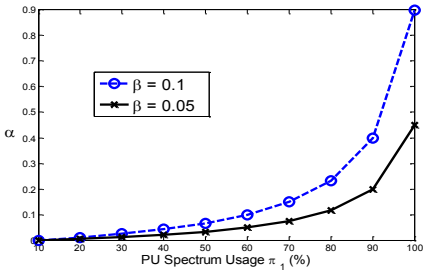

Figure 4: Relationship between α, β and π_1

sensing stage is assumed to have high false positive under large noise or smart jamming attack, but has no false negative to miss the detection of PU. Fine sensing may consume a whole CDT slot i.e. 160 msec whereas fast sensing lasts for a few micro seconds [1]. Fine sensing has no false negative, i.e., it will not miss the detection of PU if it is present on the spectrum.

IV. DS3: DYNAMIC AND SMART SPECTRUM SENSING SCHEME

A. Markov ON/OFF model for PU activity

In this section, we formulate our proposed dynamic and smart spectrum sensing algorithm DS3. Experimental data recorded in the Chicago city area shows that the TV spectrum is severely under-utilized and the average spectrum occupancy of the TV spectrum is close to 30% [11]. Research has shown that PU's spectrum usage follows the Markov ON/OFF model [8-10] and therefore, in this paper we have the same assumption that PU's spectrum usage follows the Markov ON/OFF model. In our model, every discrete time interval corresponds to one super-frame i.e. one CDT time slot.

In this paper, we mainly focus on the spectrum sensing during PU's OFF period i.e. in state 0. After transitioning to OFF state, let X denote the number of CDT slots the PU stays in that state until it jumps back to the ON state (state 1), where $X \in \{1,2,3,\dots\}$. This random variable X follows a geometric distribution with parameter α. Let P_k denote the probability that given the PU is in the OFF state at time 0, the PU transitions to ON state by time interval k, i.e., $P_k \equiv P(X \leq k)$. Thus the formula for P_k is the cumulative distribution function of the geometric distribution given by:

$$P_k \equiv P(X \leq k) = 1 - (1 - \alpha)^k \qquad (2)$$

Figure 3 shows the impact of α on P_k. Physically, it means that as time goes on, the PU initially in the OFF state at time $k = 0$ has more and more chance to become active again and transition to ON state.

In the Markov ON/OFF model, the staying time at each state before transitioning to the other state has the memory-less characteristic. That is to say, given that at the discrete CDT slot s, we know the PU is in OFF state, the probability that the PU will transition back to ON state at interval $s + k$ will still be equal to P_k. Based on our assumption, a fine sensing carried out at a time slot s will tell us whether or not the PU is in OFF state at that time slot. Thus the variable k in the notation P_k represents how many discrete time units have passed since the last fine sensing which concluded that the PU is OFF. On the other hand, if the last fine sensing concluded that the PU is ON, then DS3 will carry out fine sensing statically and continuously for subsequent CDT slots according to the original IEEE 802.22 draft standard.

From the Markov ON/OFF model, the probability of PU being in state 0 or 1 is represented as the steady state probability π_0 and π_1 respectively, where $\pi_0 + \pi_1 = 1$. It is clear that if we define *PU spectrum usage* as the fraction of time PU utilizes the spectrum under consideration, then PU spectrum usage is equal to π_1. Figure 4 shows the relationship between α, β and PU spectrum usage π_1.

Based on past observation data of PU spectrum usage, we can know the average amount of time PU stays in OFF state, i.e., we know the value of $E[X]$. Since the geometrically distributed r.v. X is given by $E[X] = 1/\alpha$, thus we can calculate the value of α from observed data as:

$$\alpha = 1/E[X] \qquad (3)$$

B. The Core idea for Dynamic Smart Spectrum Sensing

Because the duration of PU being either in ON state or OFF state is much larger than the protocol defined Channel Detection Time i.e. 160 milliseconds [3], when PU just turns OFF, or turns OFF for a short time, the base station of SU has the option to dynamically decide whether or not to go for fine sensing at each CDT, even if the fast sensing stage reports presence of some signal on the spectrum. The original IEEE 802.22 CRN protocol carries out fine sensing every time when fast sensing gives alert, which could waste a lot of spectrum resource when there is very low chance of PU being active right after it turns OFF. The central idea of our proposed approach is to dynamically determine when to conduct fine sensing in order to save spectrum resource for SU usage, and at the same time not to delay detection of PU's presence on the spectrum for more than the MDT [3].

C. Proposed DS3 Scheme

Our proposed scheme for DS3 is based on an optimization function with the goal of minimizing the

overall "cost". There are two possible costs that we consider related to our fine sensing decision:

1) The cost of delaying PU's detection when the PU is actually using the spectrum while we choose to skip fine sensing.
2) The cost of wasting opportunity when PU is OFF but we choose to carry out fine sensing in response to a fast sensing alert.

In the first scenario, the cost represents interference caused to the PU when the CRN misses detecting PU's activity in the current CDT time slot. In the current IEEE 802.22 CRN standard, the short-term interference is acceptable as long as it is less than the Maximum Detection Time (MDT), which is 2 seconds [1], [3]. Meanwhile, the second scenario happens when we waste

Notation	Definition
k	# of CDT slots passed since the last fine sensing which concluded that the PU is OFF
P_k	Probability PU is ON after it stays in OFF state for k consecutive CDT slots
τ	# of CDT slots in MDT (12 slots)
π_1	PU's spectrum usage
γ_{kt}	Cost Factor for dynamic spectrum sensing
p_t^*	Optimal spectrum sensing decision
J_t	DS3's cost optimization function
c	Sensitivity
α	Prob. of PU to transition from state 0 to state 1
β	Prob. of PU to transition from state 1 to state 0
CDT	Channel Detection Time / super frame (160 msec)
MDT	Maximum Detection Time (2 seconds)

Table 1: List of Notations

the CDT slot by conducting fine sensing as the fast sensing produces alert, i.e., we encounter either a smart jamming attack, or noise on the spectrum band.

Let the probability of the base station choosing to carry out fine sensing at the discrete CDT slot *t,* be represented as p_t. Then the total cost J_t associated with dynamically deciding whether or not to conduct fine sensing after receiving an alert from fast sensing at time *t* is given by:

$$J_t = \gamma_{kt} P_k (1 - p_t) + \varphi_t p_t (1 - P_k) \quad (4)$$

$$\frac{dJ_t}{dp_t} = \varphi_t (1 - P_k) - \gamma_{kt} P_k \quad (5)$$

where γ_{kt} represents the cost factor for missing the detection of PU and causing interference to the PU, and φ_t represents the cost factor for carrying out fine sensing under smart jamming attack and thereby wasting the current CDT slot, k is the number of CDT slots passed since the last fine sensing telling us that PU is in OFF state. Equation (4) represents the two costs discussed

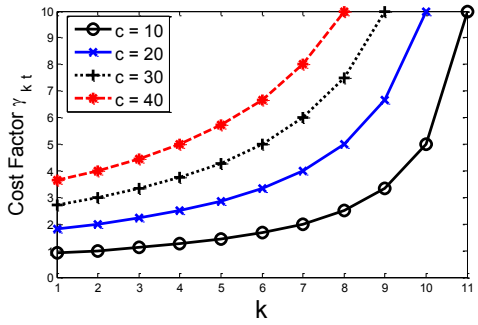

Figure 5: Effect of Sensitivity constant '*c*' on cost factor γ_{kt}

above respectively, where $P_k(1 - p_t)$ is the probability of the first scenario happening and $p_t(1 - P_k)$ is the probability of the second scenario.

Intuitively, the cost of wasting spectrum resource for SU should increase linearly according to the amount of time wasted, thus the second cost factor, φ_t , can be treated as a constant value. However, this is not true for the first cost factor γ_{kt} . Intuitively, the potential interference caused to PU's spectrum usage should increase significantly when the PU detection delay becomes longer. In addition, we should never allow a PU detection time to be longer than the maximum detection time (MDT) specified in the standard. For this reason, the cost factor γ_{kt} should not be a constant value. In our proposed scheme, we use the following formula to determine current cost factor:

$$\gamma_{kt} = \begin{cases} \frac{c}{\tau - k} & when\ k < \tau \\ \infty & when\ k \geq \tau \end{cases} \quad (6)$$

where c is a constant representing the "sensitivity" of the BS towards PU detection. The larger the value of c, the more sensitive (or aggressive) the BS will be towards fast sensing stage's alert reports.

Figure 5 shows how the sensitivity 'c' (6) affects the cost factor γ_{kt}. As the sensitivity increases, the cost for not carrying out fine sensing after k consecutive CDT slots reaches infinity much faster e.g. in figure 5, for c = 10 the cost factor reaches infinity for not carrying out fine sensing at CDT slot 11 while for c = 40, it reaches infinity for not carrying out fine sensing at CDT slot 8. Therefore, by increasing the value of sensitivity to a sufficiently large value, we can make DS3 to function as the original static fine sensing decision algorithm of IEEE 802.22 CRNs. Based on Equation (5), we can find the optimum value for dynamic fine sensing decision p_t^*, which is given by:

$$p_t^* = \begin{cases} 0 & if\ \frac{dJ_t}{dp_t} > 0 \\ 1/2 & if\ \frac{dJ_t}{dp_t} = 0 \\ 1 & if\ \frac{dJ_t}{dp_t} < 0 \end{cases} \quad (7)$$

Initializations:
1: c = Sensitivity, $\tau = \lfloor MDT / CDT \rfloor$, $k = 0$
2: π_1 and $E[X]$ based on past observations

DS3 Algorithm:
3: for every CDT slot t
4: if PU was OFF in previous CDT slot
5: if fast sensing gives an alert
6: s = CDT slot when last fine sensing reported PU's absence
7: t = current CDT slot
8: $k = t - s$
9: Calculate P_k as:
10: $P_k \equiv P(X \leq k) = 1 - (1 - \alpha)^k$ and
11: if k < τ
12: Cost Factor $\gamma_{kt} = \frac{c}{\tau - k}$
13: else
14: Cost Factor $\gamma_{kt} = \infty$
15: end if
16: $\frac{dJ_t}{dp_t} = \varphi_t(1 - P_k) - \gamma_{kt}(P_k)$
17: Calculate Cost Function J_t based on γ_{kt} (4)
18: if $\frac{dJ_t}{dp_t} < 0$
19: conduct fine sensing
20: else if $\frac{dJ_t}{dp_t} = 0$
21: conduct fine sensing with prob. 1/2
22: else
23: do not conduct fine sensing
24: end if
25: end if
26: else do not conduct fine sensing
27: end if
28: end for

Table 2: DS3 Algorithm

In summary, Table 2 shows the pseudo-code of the proposed dynamic and smart spectrum sensing scheme DS3.

V. Performance Evaluation

A. Simulation Setup

A CDT slot in simulations is 160 milliseconds long [1] and the maximum time available to the CRN for detection of a PU's signal is 2 seconds or 12 CDT slots, therefore based on the current cost function of DS3, the BS may defer fine sensing even when fast sensing reports presence of some signal on the spectrum. Without DS3, the CRN *always* conducts fine sensing whenever fast sensing gives an alert, and fine sensing always consumes the whole CDT slot. The overall fraction of time that the PU is ON is called *PU's Spectrum Usage*. The absence of PU on the spectrum is called *Spectrum Opportunity* for CRN. A malicious user in the CRN launches a DoS attack in spectrum opportunity by transmitting a jamming signal

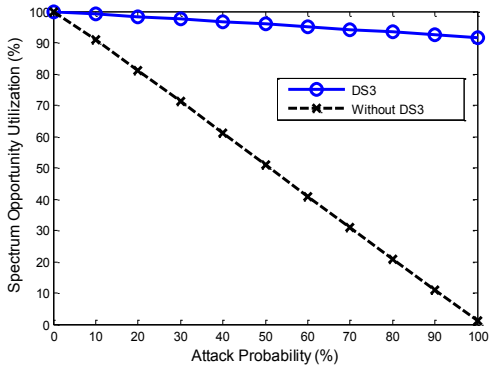

Figure 6: Effect of Jamming Attack Probability on Spectrum Opportunity Utilization

during the fast sensing stage of the CDT slot with some probability. Every data point shown in figures 6 through 10 corresponds to the average of 100 simulation runs.

B. Performance Evaluation

Figure 6 shows the improvement in spectrum Opportunity Utilization achieved by DS3. Without DS3, spectrum opportunity utilization decreases proportional to the increase in jamming attacks whereas with DS3, the decrease is at a much slower rate and remains close to 90% even when the malicious users jam every possible spectrum opportunity. The results shown in figure 6 were recorded while keeping the sensitivity to its minimum value of 10 and PU Spectrum Usage at 30%.

Figure 7 shows the performance of the DS3 algorithm by varying the sensitivity from 10 to 50 at a fixed jamming attack rate of 70%. Without DS3, spectrum opportunity utilization remains close to 30% whereas it decreases from 94% to 71% with increasing sensitivity. A lower sensitivity to detect PU's signal means that the cost factor has a lower value and the BS is inclined more towards deferring fine sensing to a later CDT slot.

Figure 8 shows DS3's performance with respect to varying PU spectrum usage at jamming attack probabilities 40% and 90% as compared with spectrum opportunity utilization without DS3. It shows that PU's spectrum usage also has very little impact on spectrum opportunity utilization of DS3 and that too at higher values of π_{1t} .When the DS3 algorithm of CRN's BS defers carrying out fine sensing even though fast sensing reports presence of some signal on the spectrum band, it is clear that some of the time, the fast sensing stage would detect a PU's signal but the BS disregards it because the cost factor would not be high enough to warrant carrying out fine sensing

Figure 9 shows the overhead caused due to additional delay in the detection of PU's signal. Notice however that the additional delay caused due to deferred fine sensing does not increase more that 50% of the MDT required by FCC and the PU is detected within the specified time limit. It is also worth noting that if we increase DS3's sensitivity to a large enough value, the PU detection delay

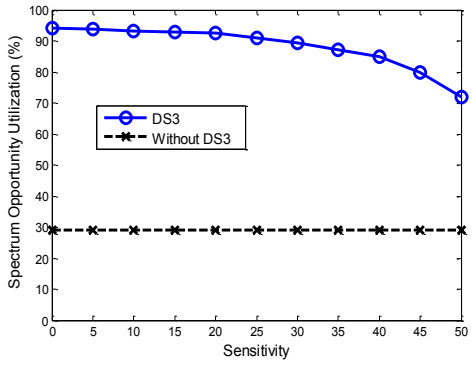

Figure 7: Effect of Sensitivity 'c' on Spectrum Opportunity Utilization

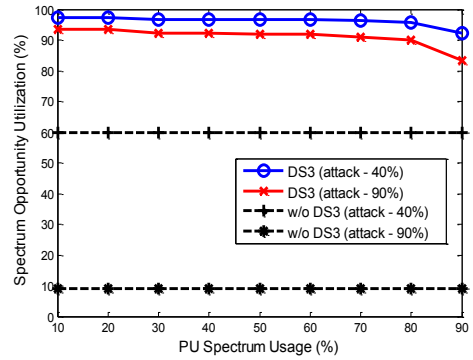

Figure 8: Effect of PU's Spectrum Usage π_{1t} on Spectrum Opportunity Utilization

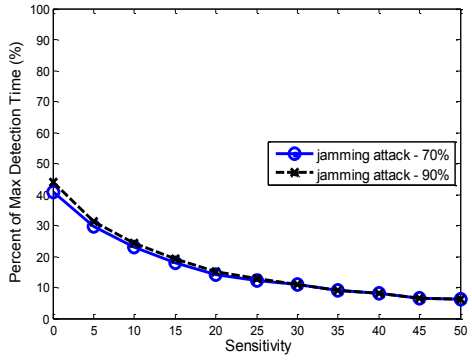

Figure 9: Effect of Sensitivity on PU detection time

approaches the time taken by the conventional algorithm of IEEE 802.22.

Figure 10 shows the effect of PU's spectrum usage π_{1t} on PU detection time for the DS3 algorithm. As π_{1t} increases, it causes a corresponding increase in α_t which increases the DS3's probability of PU to turn back ON p_t, at a much faster rate. With higher values of p_t, the cost function increases at faster rate forcing the BS to carry out fine sensing earlier.

VI. Conclusion

In this paper we presented a novel algorithm DS3, which minimizes the effects of smart jamming as well as noise on the fast sensing phase of DSA and improves

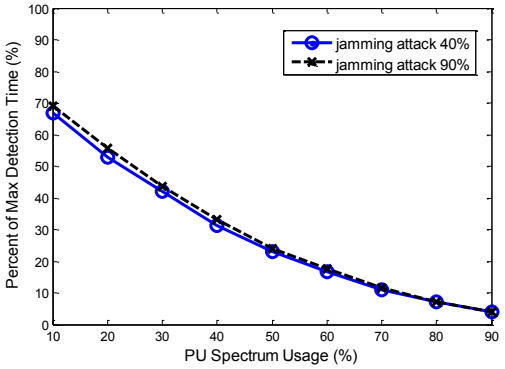

Figure 10: Effect of PU Spectrum Usage π_{1t} on PU detection

spectrum utilization through dynamic fine sensing decision algorithm with minimal increase in the overhead caused due to additional delay in the detection of PU's presence on the spectrum. DS3 achieves up to 90% improvement in spectrum utilization under jamming attack while keeping the PU detection delay to less than 50% of the maximum allowed PU detection delay.

VII. References

[1] IEEE 802.22-2011 ™ standard, Members only Documents of the IEEE 802.22 Working Group.

[2] Stevenson, C, Chouinard, G, Zhongding Lei, Wendong Hu, Shellhammer, S, Caldwell, W, "*IEEE 802.22: The first cognitive radio wireless regional area network standard*," IEEE Communications Magazine, vol.47, pp.130-138, 2009.

[3] Shellhammer, S. J.; "Spectrum Sensing in IEEE 802.22," *IAPR Workshop on Cognitive Information Processing (CIP), 2008*.

[4] Liu, S.; Lazos, L.; Krunz, M., "Thwarting Control-Channel Jamming Attacks from Inside Jammers," *IEEE Transactions on Mobile Computing,* vol.11, no.9, pp.1545,1558, Sept. 2012.

[5] Su, H.; Wang, Q.; Ren, K.; Xing, k.; "Jamming-Resilient Dynamic Spectrum Access for Cognitive Radio Networks," *IEEE International Conference on Communications (ICC), 2011.*

[6] Wenjing W.; Chatterjee, M.; Kwiat, K., "Collaborative jamming and collaborative defense in Cognitive Radio Networks," *IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011* .

[7] Wu Y.; Wang B.; Liu, K.J.R., "Optimal Defense against Jamming Attacks in Cognitive Radio Networks Using the Markov Decision Process Approach," *IEEE Global Telecommunications Conference (GLOBECOM) 2010.*

[8] Ghosh, C.; Cordeiro, Carlos; Agrawal, D.P.; Rao, M.B., "Markov chain existence and Hidden Markov models in spectrum sensing," *IEEE International Conference on Pervasive Computing and Communications, (PerCom) 2009.*

[9] Rondeau, T.W.; Rieser, C.J.; Gallagher, T.M.; Bostian, C.W., "Online modeling of wireless channels with hidden Markov models and channel impulse responses for cognitive radios," *IEEE Microwave Symposium Digest MTT-S, pp.739,742 Vol.2, June 2004.*

[10] Kyouwoong Kim; Akbar, I.A.; Bae, K.K.; Jung-Sun Um; Spooner, C.M.; Reed, J.H., "Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio," *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2007.*

[11] Taher, T.M.; Bacchus, R.B.; Zdunek, K.J.; Roberson, D.A., "Long-term spectral occupancy findings in Chicago," *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011.*