Computer Communications 172 (2021) 25–34

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

AdS: An adaptive spectrum sensing technique for survivability under jamming attack in Cognitive Radio Networks

Muhammad Faisal Amjad [a,*], Hammad Afzal [a], Haider Abbas [a], Abdul B. Subhani [b]

[a] National University of Sciences and Technology, Pakistan
[b] Centex Technologies, USA

ARTICLE INFO

Keywords:
Cognitive Radio Network
Intelligent spectrum sensing
Survivability
Minimal Denial of Service

ABSTRACT

IEEE 802.22 Cognitive Radio Network (CRN) allows sharing of geographically unused spectrum allocated to the television broadcast service, on a non-interfering basis. CRNs make use of Dynamic Spectrum Access (DSA) which is a two-stage mechanism comprising *fast sensing*, which is mandatory and *fine sensing* which is optional. However, the two-stage spectrum sensing mechanism suits malicious nodes in the CRN which intend to deny the use of vacant spectrum to the CRN by jamming its communication while at the same time, minimizing the amount of power expended on jamming. Such *Minimal Denial of Service* (MDoS) jamming attack can be launched by the malicious nodes by transmitting a very short jamming signal during the mandatory fast sensing stage which will in turn force the CRN to carry out the otherwise optional, fine sensing. MDoS jamming attack results in wastage of spectrum opportunities for the rest of the CRN to the extent which can jeopardize its survivability. In this paper we present ***AdS***: an Intelligent ***Ad***aptive spectrum ***S***ensing technique which, not only minimizes the effects of MDoS jamming attack but can also reduce the effects of noise during the spectrum sensing stages of DSA. The adaptive nature of AdS improves spectrum utilization by CRNs by up to 90% through adaptive tuning of the fine sensing threshold which is based on an estimate of PU's activity and the severity of MDoS jamming attack.

1. Introduction

Wireless communications account for a far greater part of modern data communication than it once used to be. However, spectrum is a scarce resource and numerous techniques are aimed at its efficient utilization and sharing. Cognitive Radio Networks based on IEEE 802.22 standard [1,2] employ Cognitive Radio communication [3–6] techniques to provide Internet access by utilizing the analog TV white spaces (TVWS) in an opportunistic, yet non-interfering manner. To minimize wastage of precious spectrum resources, TVWS have been opened up by the Federal Communication Commission (FCC) for unlicensed and opportunistic use [4] by CRNs. These TVWS fall in the 54–862 MHz frequency range. On one hand, to achieve DSA on a non-interference basis, CRNs are mandated to continuously sense the spectrum, use it for its own communication only if found un-occupied and vacate it as soon as the incumbent PU is detected to be on-air. To ensure high Quality of Service for its users on the other hand, the CRN must make use of the vacant spectrum to its maximum. Evidently, these two are conflicting goals and to strike a balance between the two, CRNs carry out spectrum sensing in two stages during every superframe. These two stages are called *fast sensing* and *fine sensing* [1]. As the name suggests, fast sensing typically takes between 9 and 20 microseconds based on the underlying technique used [7]. The most common of the fast sensing techniques is called *energy detection* which can only determine if any signal is found on the channel but cannot ascertain the type of signal currently being received. Fine sensing stage of DSA employs much more sophisticated techniques to determine the type(s) of signals being received on the channel and can take the entire length of a superframe i.e., up to 160 msec [8] and is also known as the Channel Detection Time (CDT) slot [1,2].

CRNs based on the IEEE 802.22 standard have long transmission range from 35 to 100 km which makes the task of spectrum sensing quite challenging. These CRNs therefore depend on collaborative and distributed spectrum sensing for accurate determination of the channels' state. The CRN base station (BS) calculates its spectrum decision based on spectrum sensing reports from the secondary users (SU) that may be scattered across the CRN in addition to its own spectrum sensing. To perform collaborative spectrum sensing, SU devices in a CRN need to be synchronized and must thereafter carry out the mandatory fast sensing stage of every CDT slot. After the fast sensing has been completed by all SUs, the results are reported to the CRN BS. Based

* Corresponding author.
E-mail addresses: faisal@nust.edu.pk (M.F. Amjad), hammad.afzal@mcs.edu.pk (H. Afzal), haider@mcs.edu.pk (H. Abbas), asubhani@centextech.com (A.B. Subhani).

https://doi.org/10.1016/j.comcom.2021.03.001
Received 15 September 2020; Received in revised form 25 January 2021; Accepted 1 March 2021
Available online 6 March 2021
0140-3664/

on the fast sensing results, the BS must decide whether fine sensing is required for a detailed examination of the spectrum's state. To ensure that SUs taking part in the collaborative spectrum sensing listen for the PU's signals and not their own, the quiet periods for spectrum sensing must be synchronized. As per the IEEE 802.22 standard, the CRNs are required to *always* conduct fine sensing when the result of the fast sensing stage concludes that there is a signal present on the spectrum [1] which needs to be further investigated through fine sensing. As we demonstrate in the subsequent sections, the static nature of fine sensing decisions can be exploited by attacker(s) in the CRN to launch Minimal Denial of Service (MDoS) jamming attacks. In this paper, we propose AdS: an adaptive spectrum sensing technique which is meant to modify the static nature of the IEEE 802.22 standard's fine sensing decision strategy, as explained below.

In the context of DSA, spectrum opportunity is the state when the channel is idle and the PU is OFF-air. Malicious secondary users in the CRN can exploit spectrum vacancy to launch a Denial of Service (DoS) attack by transmitting a jamming signal on the channel which is being used by CRN at a given time. This kind of jamming would need to be done for the entire duration of a CDT. Such an attack however has a couple of disadvantages: first, it will render the jammed channel unusable by the attacker and second, it would require a lot of transmission power to be successful. There is however another approach available to the attacker with which it would be able to deny the use of channel to honest SUs, expend much less transmission power while at the same time keeping the jammed channel available for its use. This can be achieved by transmission of a very short duration jamming signal coinciding with the fast sensing stage of DSA. We call this a minimal denial of service (MDoS) jamming attack. Because the fast sensing stage is much shorter in duration in comparison with the CDT, a MDoS jamming attack would intuitively consume much less energy of the attacker than jamming the full CDT slot. Discovering a short jamming signal during fast sensing stage will force the CRN to conduct fine sensing during the rest of the CDT. During resultant fine sensing time, spectrum opportunity would be wasted for the CRN while at the same time making it available for the attackers' own communications. Therefore, to thwart MDoS attacks and optimize spectrum opportunity utilization, we propose in this paper, an adaptive spectrum sensing technique called ***AdS***.

Motivation: To protect the incumbent licensed PU's communications, the IEEE 802.22 standard has set an upper limit on the maximum allowed time during which, its presence must be detected by the CRN and its channels must be vacated. This upper limit for PU detection is called Maximum Detection Time (MDT) [1,5,9,10] and is specified to be equal to 2 s. To defend against MDoS jamming attacks, we leverage the MDT constraint to adaptively decide whether or not fine sensing must be carried out if a signal is detected during fast sensing stage. We call this technique AdS: Adaptive Spectrum Sensing. The difference between AdS and the fine sensing decision criterion of the IEEE 802.22 standard is: when fast sensing reports from the SUs in CRN indicate the presence of *some* signal on the channel, the IEEE 802.22 standard would carry out fine sensing while our proposed AdS technique would dynamically adjust its threshold for carrying out fine sensing based on a few parameters while enforcing the MDT constraint. As explained subsequently in Section 4, the dynamic threshold is calculated with the help of a cost minimization function, the CRN's estimate of MDoS jamming attack severity as well as the prediction of PU's presence or absence on the channel. Without the protection afforded by our proposed adaptive defense technique, secondary users of the CRN would struggle to communicate and the malicious nodes would be able to jam the entire communications of the CRN with minimal expenditure of their energy.

The rest of this paper is organized as follows: An overview of the latest related work for optimum spectrum utilization and defense against jamming attacks is presented in Section 2. The underlying assumptions of the AdS technique and the system model are presented in Section 3. The inner workings of the AdS technique are presented in Section 4 while the evaluation and its discussion are presented in Section 5. Conclusions and future work are presented in Section 6.

2. Related work

CRNs rely on collaborative sensing and opportunistic access to the spectrum. This form of communication makes them vulnerable to attacks from users which may disrupt their operation either because of selfish behavior or merely for malicious purpose. Security of DSA in CRNs as well as protecting the communication rights of the incumbent PUs has therefore attracted the attention of many research efforts. In this section, we present the state of the art in the research work in this domain and also highlight how the work proposed in this paper differs from them. A summary of the related work is presented in Table 1.

An anti-jamming communication mechanism for CRNs based on a two-dimensional Q-network algorithm is proposed in [11]. The authors have applied a deep convolution neural network to accelerate the learning process of the CRN with which it can decide whether to stay in the current channel or move to another channel which might not have been jammed by the attacker. Similarly, authors of [12] propose to use Q-learning to learn the behavior of the jammer to avoid jammed channels pro-actively by hopping over to other channels. Our proposed technique is different from both of these since it tries to mitigate the effects MDoS jamming attack while staying in the channel being jammed.

Authors of [13] consider the situation in which malicious users may intentionally falsify spectrum sensing reports as well as Byzantine failure in CRNs. They have proposed a defensive mechanism against such attacks with the help of weighted sequential probability ratio test (WSPRT) which is used to filter out spectrum reports which are considered as suspicious. Instead of such a passive attack on spectrum sensing reports, in this paper we consider an active jamming attack by a malicious SU.

Ad hoc CRNs sometimes rely on a Common Control Channel (CCC) which may be attacked by a malicious user to disrupt its normal operation. Authors of [14] have considered the possibility of jamming the CCC either through individual action by the attackers or through collusion. They have proposed two separate techniques to deal with the two scenarios i.e., relying on channel hopping and the encrypted dissemination of the hop sequence to the nodes in the CRN through the CCC. Our work on the other hand, deals with securing the spectrum sensing itself instead of securing the dissemination means of spectrum sensing reports.

Authors of [15] propose a spectrum sensing mechanism by collaborating SUs which defines two parameters to represent the trust scores of SUs. These parameters are called 'Malicious Intent' and 'Location Reliability' calculated based on the famous 'Dempster-Shafer theory of evidence'. Both of these parameters represent the overall trust score of any SU of the CRN. Collectively, the two parameters are used to decide whether or not a SU's spectrum sensing report is used in deciding the current state of the channel. As with the previous case, this approach also focuses on the accuracy of spectrum sensing reports and does not consider active jamming by the attackers or malicious SUs in the CRN.

To thwart jamming and disruption of DSA in CRNs, various game theoretic solutions have been proposed in [16–20]. The focus of all of these approaches is to continuously look out for jamming attack on the spectrum and at the same time maintaining a clear picture of the vacant channels that may be hopped on to by the CRN if jamming is detected in the current channel. On the other hand, the attack model which we have considered consists of an attacker who does not want to jam the channel in its entirety so that it remains available for the attacker's own use while also minimizing the amount of energy spent on jamming. Furthermore, our proposed technique defends against jamming attack while staying in the channel which is currently being jammed.

Authors of [21] present a similar defensive technique in which the SUs collaborate to mitigate the effects of jamming in which the attackers collude to jam the entire spectrum band. As a defense mechanism, SUs form a system of proxies based on temporal as well as spatial diversity for continued communication in the presence of sweep jamming

Table 1
A summary of the related work.

Reference	Attack type	Description	Defense mechanism	Defend while staying in the same channel?
[11]	Jamming	Anti-jamming communication mechanism for CRNs based on a two-dimensional Q-network algorithm	Channel hopping	No
[12]	Jamming	Q-learning to learn the behavior of the jammer to avoid jammed channels	Channel hopping	No
[13]	False spectrum reports	weighted sequential probability ratio test (WSPRT) to filter out suspicious spectrum reports	Trust score	No
[14]	Common Control Channel	Encrypted dissemination of the hop sequence	Channel hopping	No
[15]	False spectrum reports	Dempster-Shafer theory to determine trust score of SU's spectrum reports	Trust score	No
[16–20]	Jamming	Use game theoretic approaches to look out for jamming attack on the spectrum	Channel hopping	No
[21]	Sweep jamming	Formation of a system of proxies based on temporal as well as spatial diversity	Channel hopping	No
[22]	Jamming	Use Markov Decision Process and Maximum Likelihood Estimation to learn channel state	Channel hopping	No

attack. As is the case with previously discussed defense mechanisms, the attackers do not seek to conserve the power which may be expended on jamming the channels and they also do not consider keeping the jammed channels available for their own use. Intuitively, the defense strategy relies on hopping on to a different channel instead of staying in the channel currently being jammed.

An optimal strategy is developed by the Authors of [22] to defend against jamming in CRNs using the 'Markov Decision Process'. Based on this strategy, the SUs decide whether or not to hop to a different channel if jamming is encountered in the current channel. Based on a record of observations made in the past, combined with 'Maximum Likelihood Estimation', the authors have also formulated a learning technique for the SUs to determine prevalent network state and to optimize their channel selection decisions. As in other solutions, if jamming is encountered, the CRN's response is to hop on to another channel. Authors of [23] consider various levels of SNR in the network and have proposed a technique which optimizes the duration for which spectrum sensing must be carried out. This work caters for variations in network conditions which are considered natural and does not consider the existence of attackers.

Contributions: *AdS*, our proposed adaptive spectrum sensing technique, is aimed at thwarting the jamming attacks carried out by malicious secondary users of the CRN. To that end, in this paper we have made the following contributions:

- We have demonstrated that the static fine sensing decision mechanism can be exploited by attackers to maximize their spectrum opportunity while denying the same to benign secondary users.
- Carried out an analysis of the impact of MDoS jamming attack on DSA within a CRN.[1]
- Proposed AdS: a novel adaptive spectrum sensing technique with which the CRN can overcome and mitigate the effects of MDoS jamming attacks.
- AdS offers additional advantage of improving spectrum opportunity utilization by the CRN under noisy conditions.
- We have also carried out a detailed evaluation of the proposed AdS technique and demonstrated that it enhances spectrum opportunity utilization as compared with the IEEE 802.22 standard under MDoS jamming attack.

To the best of our knowledge, our proposed technique AdS is the first solution which not only defends against MDoS jamming attack in IEEE 802.22 CRNs but also minimizes the wastage of spectrum opportunities while staying in the channel currently being jammed and does not rely on hopping to a different vacant channel.

3. System model, attack model and assumptions

System Model: Due to large transmission range, IEEE 802.22 based CRNs rely on cooperative spectrum sensing by SUs spread across the network to ensure that the PU's communication is protected regardless of its location. For this paper, we assume the same setup of network entities. For accurate identification of PU's communications, all SUs have synchronized quiet periods with each other and the BS. Every CDT slot begins with a mandatory fast sensing stage the results of which, are aggregated at the BS. If the fast sensing stage determines the channel to be vacant then regular communication of the CRN can be undertaken. However, if the fast sensing stage indicates the presence of *some* signal on the channel, then the BS decides to carry out fine sensing which may take the remainder of current CDT slot.

The IEEE 802.22 standard defines a parameter called **Maximum Detection Time (MDT)** which is the time limit during which presence of a PU's signal must be detected by a CRN. The current value of MDT is set to 2 s [5,9]. On the other hand, one superframe/CDT spans 160 msec [1]. Therefore, when a PU comes on-air, the CRN has a total of τ CDT slots to detect it and immediately vacate the channel, given by the following equation.

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

[1] We use the terms Opportunistic Spectrum Utilization/Access and Dynamic Spectrum Access (DSA), interchangeably.

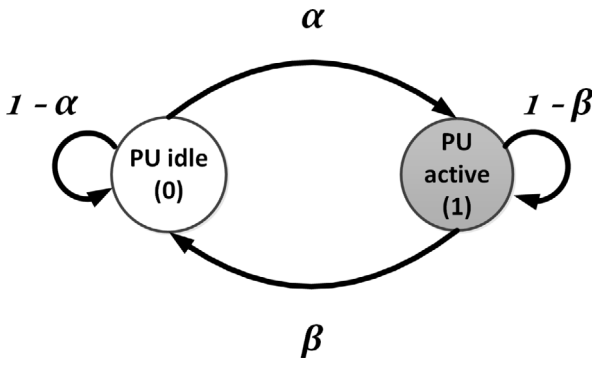


Fig. 1. Markov ON/OFF model for Primary User.

This is where our proposed AdS technique differs from the way IEEE 802.22 standard handles the detection of some signal during fast sensing stage. IEEE 802.22 requires the CRN to *always* resort to fine sensing, the situation where an attacker can launch a MDoS attack because transmission of a very short jamming signal during fast signal will render the rest of the CDT slot unusable for the CRN since it would be busy conducting fine sensing. During the same time, the attacker would have the channel to itself. Making use of the MDT requirement, AdS on the hand adaptively delays going into fine sensing until the expiry of MDT because it considers the possibility of experiencing a MDoS attack in addition to the PU's signal or the usual noise on the channel. AdS uses a cost minimization function to calculate how much time it can delay until resorting to fine sensing, the inner working of which is explained Section 4. Table 2 lists down the notations used in this paper along with their descriptions.

Attack Model: The attack model considered in this paper has the following aspects:

- The attacker intends to deny the use of spectrum to the CRN alone, and not the PU.
- The CRN is denied the use of spectrum by launching a Minimal Denial of Service (MDoS) jamming attack by transmitting a short signal during the fast sensing stage of DSA.
- MDoS jamming attack is intended to force the CRN to enter into fine sensing.
- The MDoS jamming attack consumes much less transmission power than jamming the entire CDT slot and it keeps the spectrum band being jammed, available for use by the attacker.

Assumptions: Our proposed AdS technique for DSA is based on the following assumptions:

- ***PU's Spectrum Usage:*** As shown in Fig. 1, the PU's communication on the its licensed spectrum is assumed to follow the Markov ON/OFF process [24,25]. Transitioning of the PU from state 0 (idle or OFF state) to 1 (active or ON state) is represented as α whereas its transitioning from state 1 to 0 is represented as β.
- ***Spectrum Sensing's Detection Rate:*** We assume that the spectrum is noisy causing high false positive rate for fast sensing. Fine sensing on the other hand, has no false negatives since it employs sophisticated techniques for spectrum sensing and would not miss the detection of PU if it was active.
- ***Duration of Fast and Fine sensing:*** Depending on the technique used, fast sensing can take from 9 to 20 microseconds whereas fine sensing may take up to 160 ms i.e., the duration of entire CDT slot [7,8].

Spectrum measurements carried out in Chicago metropolitan area [26] have shown that the TVWS bands are occupied 30% of the time in long term whereas the short term average of their occupancy is less than 14%. We can therefore, add the following about PU's communication pattern to our set of assumptions (see Table 2):

Table 2
Notations & acronyms.

Notation	Description
α	PU's prob. to transition from idle to active state
β	PU's prob. to transition from active to idle state
P_k	Probability that PU is active after being idle for k CDT slots
p_t	CRN's prob. of conducting fine sensing after fast sensing alert
τ	Number of time slots in MDT (12 according to IEEE 802.22 standard)
t	Current time
k	CDT slots since PU was last active
π_1	Primary User's spectrum usage (%)
γ_{kt}	Cost of missing PU's presence on channel
ϕ_t	Cost of spectrum opportunity wastage
p_t^*	Optimal decision for fine sensing
J_t	AdS's cost minimization function
c	Sensitivity towards deferring fine sensing
v_t	Attack Severity estimate
CDT	Channel Detection Time (i.e., 1 superframe)
MDT	Maximum (Primary User) Detection Time (2 s)
CRN	Cognitive Radio Network
SU	Secondary User (CRN client)
PU	Primary User (Channel license holder)
BS	Base Station (of CRN)

- ***Time spent in Active state:*** The PU stays idle more than it stays active on the spectrum.
- ***Time spent in Current state:*** Because the license holders of the TVWS are primarily TV broadcast stations, they stay in their current (idle or active) state longer than one CDT slot i.e., 160 ms.

4. AdS: An adaptive spectrum sensing technique

4.1. Main idea behind AdS

Based on our assumptions, the PU stays in its current (ON or OFF) state for much longer time than one CDT slot. Therefore, as soon as the channel is sensed to be idle, it is safe for the BS to assume that the PU will *stay* in the idle state for a few more superframes' duration. During this time, the AdS technique would allow the CRN BS to skip going into fine sensing if the fast sensing detects some signal. This would not be possible according to the IEEE 802.22 standard resulting in wastage of numerous spectrum opportunities because of lesser probability of PU being active soon after going off-air and greater probability of noise or MDoS attack. Calculation of these probabilities is given in next subsection. The main idea behind AdS therefore, is delaying the conduct of fine sensing adaptively based on a certain threshold, while staying within the IEEE 802.22 standard's MDT constraint [1,5,9].

4.2. Modeling PU activity as Markov ON/OFF process

The state transition of a PU on its licensed channel is often represented according to the Markov ON/OFF model [25] and the same has been assumed in this paper. Since the attacker does not affect the PU's communication and is interested only in denying the use of channel to the CRN, AdS performs adaptive spectrum sensing as soon as the PU becomes idle. Let $X \in (1, 2, 3, \ldots)$. represent a random variable, which is the number of CDT slots during which the PU stays in idle state. It follows a geometric distribution with α representing the PU's transition probability from idle to active state. Let P_k represent the probability of PU to transition to active state at time $t = k$ given that it was in idle state at time $t = 0$ i.e., i.e., $P_k \equiv P(X \leq k)$ is given by:

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

which is the cumulative distribution function of the geometric distribution.

The impact of parameter α on the probability P_k of PU to transition to active state at time k is shown in Fig. 2. It shows that as soon as

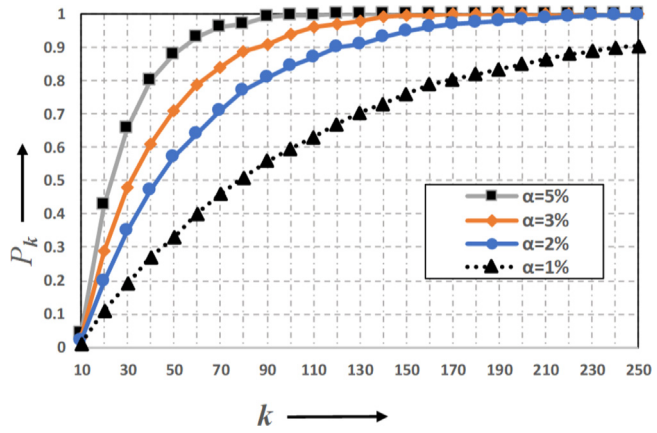


Fig. 2. Effect of α (state transition probability) on P_k.

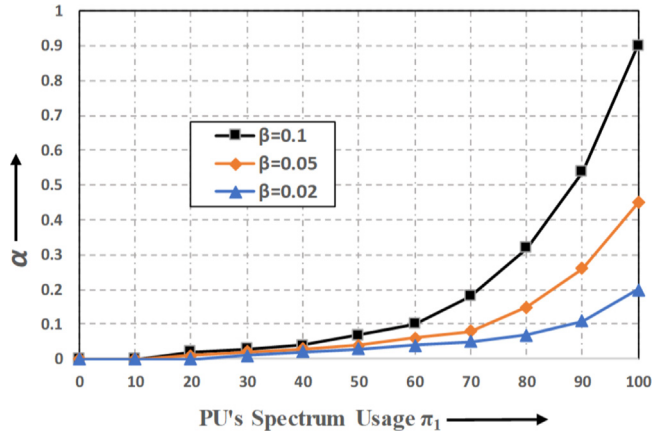


Fig. 3. Relationship between α, β and PU's spectrum usage (π_1).

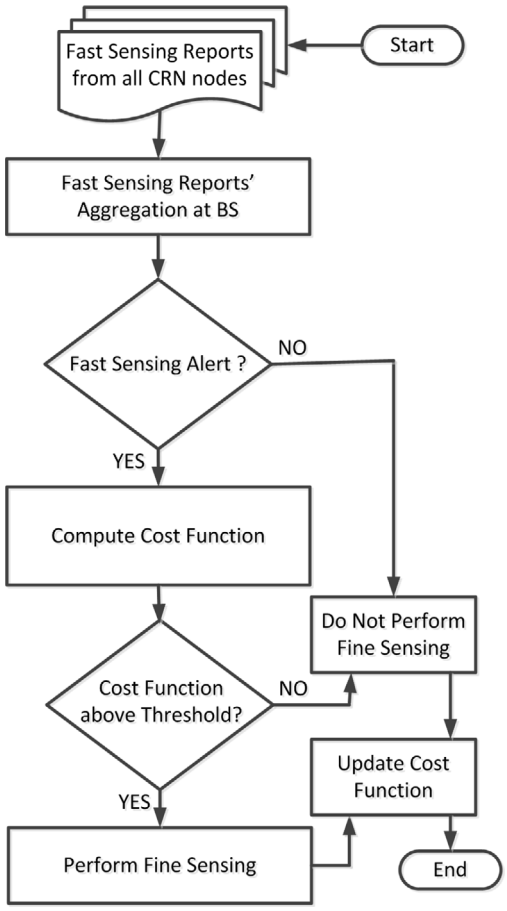


Fig. 4. One cycle of the AdS technique.

the PU goes into idle state at time $t = 0$, its probability to transition back to active state at time $t = k$ increases at a rate depending on α. Therefore, the value of P_k from Eq. (2) represents AdS's prediction of PU's spectrum usage and is used in the cost minimization function presented in the next subsection.

According to the Markov ON/OFF process, the time taken to stay in a given state has 'memory-less' characteristic i.e., given that a PU is idle during a particular CDT slot s, then its probability to become active on the channel at CDT slot $s+k$ remains P_k where k represents the number of CDT slots since the time the result of last fine sensing concluded that PU was in an idle state. Conversely, if fine sensing determines the PU to be active then DSA would be carried out statically in next CDT slots as per the IEEE 802.22 standard and not adaptively by AdS.

Let π_0 and π_1 represent the steady state probabilities of the PU to be in idle or active states respectively, where $\pi_0 + \pi_1 = 1$. Let PU's spectrum utilization be defined as the amount of time the PU remains in the active state then PU's spectrum usage would be equal to pi_1. The relation between PU's state transition probabilities α and β and its spectrum usage pi_1 are shown in Fig. 3. Because the random variable X is geometrically distributed, we can determine the average time $E[X]$ while the PU stays in idle state based on data from past observations i.e., $E[X] = 1/\alpha$.

4.3. The AdS technique

AdS implements a cost minimization function which considers two costs to implement its adaptive spectrum sensing. It also has a mechanism with which the CRN BS can estimate the severity of MDoS jamming attack at any given time. Furthermore, it defines a parameter called sensitivity which is the amount of BS's inclination to delay fine sensing during adaptive spectrum sensing. Appropriate values for the sensitivity parameter enable AdS to work just as the original IEEE 802.22 standard. Fig. 4 shows the flow diagram of AdS. In the subsequent paragraphs, we discuss the components of AdS which enable it to minimize the effects of MDoS jamming while maximizing spectrum opportunity utilization.

Calculation of MDoS Attack Severity: To be aware of the intensity with which the attacker launches MDoS attack at any given time, AdS needs to measure it first. To that end, we define ***attack severity*** (υ_t), a parameter which represents the amount of time the CRN experiences MDoS jamming attack. The results of past N CDT slots's fast sensing reports' aggregations are recorded in a sliding window to guarantee that the calculation of attack severity is based on the recent past alone. Its value at a given CDT slot is calculated as:

$$\upsilon_t = \frac{\sum_{i=1}^{N} n_i}{N}, \forall n_i \in (0,1), \forall i \in N \text{ and } N \neq 0 \tag{3}$$

where n_i is the ith entry in the sliding window, $n_i = 0$ represents that the channel was reported as idle whereas $n_i = 1$ means it was reported to be occupied during the CDT slot. An *occupied* report can mean any of the following: the channel was being used by the PU, it was under MDoS jamming attack or the channel had noise on it. Whatever the case may be, fine sensing is carried out as a result of fast sensing alert, and if it finds the alert to be a false alarm then in retrospect, all sliding window records of $n_i = 1$ are considered as MDoS jamming attacks and the attack severity is calculated as Eq. (3).

Cost Minimization Function: Our proposed AdS technique implements a cost minimization function designed to minimize the *cost* of adaptive spectrum sensing. These costs are:

- The cost of causing interference to the PU which may happen because the fast sensing gave an alert but AdS decided to delay carrying out fine sensing.
- The cost of spectrum opportunity getting wasted which may happen because the fast sensing gave an alert and AdS decided to carry out fine sensing because the adaptive fine sensing threshold was above certain level due to a combination of reasons explained subsequently.

These situations along with MDoS jamming attack and AdS's approach to deal with them are discussed in detail in Section 5 and are represented in Fig. 5. It is to be noted that AdS treats MDoS jamming attack as well as noise on channel, in the same way.

When there is high level of noise on the channel or when the there is more MDoS jamming attack (Fig. 5c), the number of fast sensing alerts are expected to increase, thereby raising the current estimate of attack severity υ_t. Therefore, it needs to be a part of the cost minimization function so that fewer spectrum opportunities are wasted and the CRN carries out fine sensing, more conservatively.

Let us define p_t to denote the probability with which the CRN chooses to conduct fine sensing during the CDT slot t. From Eq. (2), we know that the probability of the PU being active on the channel is given by P_k. Then, $P_k(1-p_t)$ represents the probability that interference would be caused to the PU when it is active and the CRN decides not to carry out fine sensing after a fast sensing alert. Similarly, $p_t(1-P_k)$ represents cost and also the probability of a spectrum opportunity being wasted since the PU was idle while the CRN decided to carryout fine sensing as a result of fast sensing alert, initiated due to a MDoS jamming attack. Let J_t denote the total cost of adaptive spectrum sensing by AdS at any given time t, then it is given as the total weighted sum of the two costs mentioned above and is given as:

$$J_t = \gamma_{kt} P_k (1 - p_t) + \upsilon_t \phi_t p_t (1 - P_k) \tag{4}$$

where γ_{kt} denotes the cost of interference being caused to the PU at time t, ϕ_t denotes the cost of spectrum opportunity being wasted at time t wasting the current CDT slot, the number of CDT slots passed since the last fine sensing concluded the PU to be in idle state is represented as k and υ_t represents attack severity at time t. As the CRN decides to carry out or skip fine sensing due to a fast sensing alert, the change in AdS's cost can be represented as the derivative of Eq. (4) as follows:

$$\frac{dJ_t}{dp_t} = \upsilon_t \phi_t (1 - P_k) - \gamma_{kt} P_k \tag{5}$$

It is reasonable to consider that the cost of causing interference to the PU should be significantly greater than the cost of wasting a spectrum opportunity. Therefore, the cost of spectrum opportunity wastage ϕ_t is treated as a constant while the same cannot be said about cost of causing interference to the PU γ_{kt} because it can have a direct impact on the PU's communication. Furthermore, the delaying of fine sensing as a result of fast sensing alert must never be allowed to exceed the MDT constraint. To determine the cost of interference to PU, we use the following relation (which is used in calculating the adaptive fine sensing threshold which we present subsequently):

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

where c represents the *sensitivity* of the CRN for the detection of the PU. With larger values of c, the CRN would be more sensitive towards fast sensing alerts. The sensitivity parameter and its effects are discussed further in the following subsection.

The optimum value for the probability with which the CRN must carry out fine sensing after a fast sensing alert is based on Eq. (5) as well as Eq. (6) and is given as p_t^* as follows:

$$p_t^* = \begin{cases} 0, & \text{if } dJ_t/dp_t > 0 \\ \frac{1}{2}, & \text{if } dJ_t/dp_t = 0 \\ 1, & \text{if } dJ_t/dp_t < 0 \end{cases} \tag{7}$$

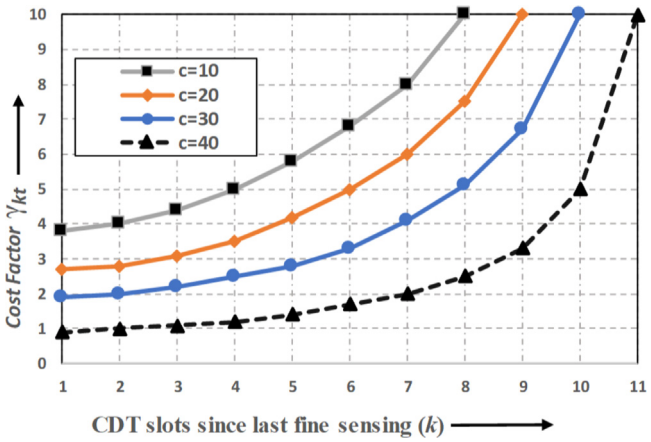


Fig. 5. Effect of Sensitivity towards delaying PU's detection (c) on the cost of interfering with the PU (γ_{kt}).

Algorithm 1: The AdS Technique

Data: $c, \upsilon_t, \tau, k, t$
Result: Adaptive fine sensing decision.
Initialization: $\tau \leftarrow \lfloor MDT/CDT \rfloor, k \leftarrow 0, t \leftarrow time$;

$s \leftarrow$ time when PU's state became idle;
for *every CDT slot* t **do**
  if *PU state was idle at time* $t-1$ **then**
    if *fast sensing result gives an alert* **then**
      $k \leftarrow t - s$;
      $P_k \equiv P(X \leq k) \leftarrow 1 - (1-\alpha)^k$;
      if $k < \tau$ **then**
        $\gamma_{kt} \leftarrow \frac{c}{\tau - k}$;
      else
        $\gamma_{kt} \leftarrow \infty$;
      end
      $J_t \leftarrow \gamma_{kt} P_k (1 - p_t) + \upsilon_t \phi_t p_t (1 - P_k)$;
      $\frac{dJ_t}{dp_t} \leftarrow \upsilon_t \phi_t (1 - P_k) - \gamma_{kt} P_k$;
      if $\frac{dJ_t}{dp_t} < 0$ **then**
        $p_t^* \leftarrow 1$;
        $k \leftarrow 0$;
      else
        if $\frac{dJ_t}{dp_t} = 0$ **then**
          $p_t^* \leftarrow 1/2$;
        else
          $p_t^* \leftarrow 0$;
        end
      end
    else
      Do not perform fine sensing
    end
  else
    perform fine sensing statically according to IEEE 802.22 standard;
    $s \leftarrow t$;
  end
end

Adaptive Fine Sensing Threshold: $\upsilon_t \phi_t (1 - P_k)$, which is part of Eq. (5), represents AdS's adaptive fine sensing threshold to decide whether or not fine sensing is carried out in a given CDT slot, since it contains parameters to denote PU's current state on the channel as well as a measure of current attack severity by the attacker. If the PU

has a higher probability P_k of currently being active then the adaptive fine sensing threshold will have a smaller value and the CRN would be less likely to skip fine sensing when fast sensing gives an alert. On the contrary, if the measure of attack severity υ_t has a higher value then AdS's adaptive fine sensing threshold will have a higher value and the CRN would be less likely to carry out fine sensing in response to fast sensing alert. AdS's adaptive fine sensing threshold is shown as a dotted blue horizontal line and the combined cost of causing interference to the PU and wasting a spectrum opportunity $\gamma_{kt} P_k$ is shown as solid red plot in Fig. 8. A detailed discussion on how AdS handles MDoS attacks, PU activity and different channel conditions is provided in the next section and depicted in Figs. 8(a)–8(c).

Sensitivity towards Delaying Primary User's Detection: The effects of varying degrees of sensitivity c on the cost factor γ_{kt} are shown in Fig. 5. The cost associated with the CRN's decision to skip carrying out fine sensing after fast sensing alerts for k consecutive CDT slots increases (reaches infinity) much rapidly as the value of sensitivity is raised. E.g., cost factor approaches infinity at CDT slot number 11 when $c = 10$. Whereas, it approaches infinity much faster at CDT slot number 8 when $c = 40$. This indicates another advantage of having the sensitivity parameter included in AdS's adaptive fine sensing threshold: AdS can be made to behave exactly according to the IEEE 802.22 standard's static decision for fine sensing by having a sufficiently large value for c. AdS's adaptive fine sensing technique is summarized in algorithm 1.

5. Performance evaluation

This section first presents the setup for simulations that we have performed to evaluate the performance of AdS followed by the results as compared with the IEEE 802.22 standard. Finally, we provide a detailed discussion on how AdS performs under MDoS jamming attack and PU's activity on the channel as well varying channel conditions.

5.1. Simulation setup

A time slot which is also called the CDT slot, is the same as specified by the IEEE 802.22 standard's superframe and is equal to 160 ms. The maximum amount of time available for detecting the presence of a PU on the channel is equal to 2 s or equivalently, 12 CDT slots [1]. Using this constraint, AdS has the option to defer carrying out fine sensing when fast sensing gives an alert, based on its cost minimization function. The IEEE 802.22 standard on the other hand, always carries out fine sensing when an alert is received from the fast sensing stage. Whenever fine sensing is conducted, it consumes the rest of CDT slot. The state when the PU is idle, is called *spectrum opportunity* whereas, the amount of time when the PU is active on the channel is termed as *PU's spectrum utilization (%)*. An attacker launches the MDoS attack with some probability during the fast sensing stage only, by sending a very short jamming signal. The plots in graphs presented in this section represent the average of 100 simulation runs, each.

5.2. Simulation results

A comparison of spectrum opportunity utilization by AdS technique and the IEEE 802.22 standard is presented in Fig. 6(a). It shows that the amount of spectrum opportunity utilization by IEEE 802.22 standard is proportional to the severity of MDoS jamming attack whereas AdS improves it significantly and stays above 90% even when the MDoS jamming is done in every CDT slot, a situation in which the IEEE 802.22 standard results in the complete shut down of CRN operation. The results of Fig. 6 were taken with PU's spectrum usage $\pi_1 = 30\%$ and sensitivity $c = 10$. The effects of varying these parameters on AdS's performance are presented in subsequent figures.

Fig. 6(b) demonstrates how AdS upholds the fundamental requirement of CRNs' operation by the IEEE 802.22 standard as well as the

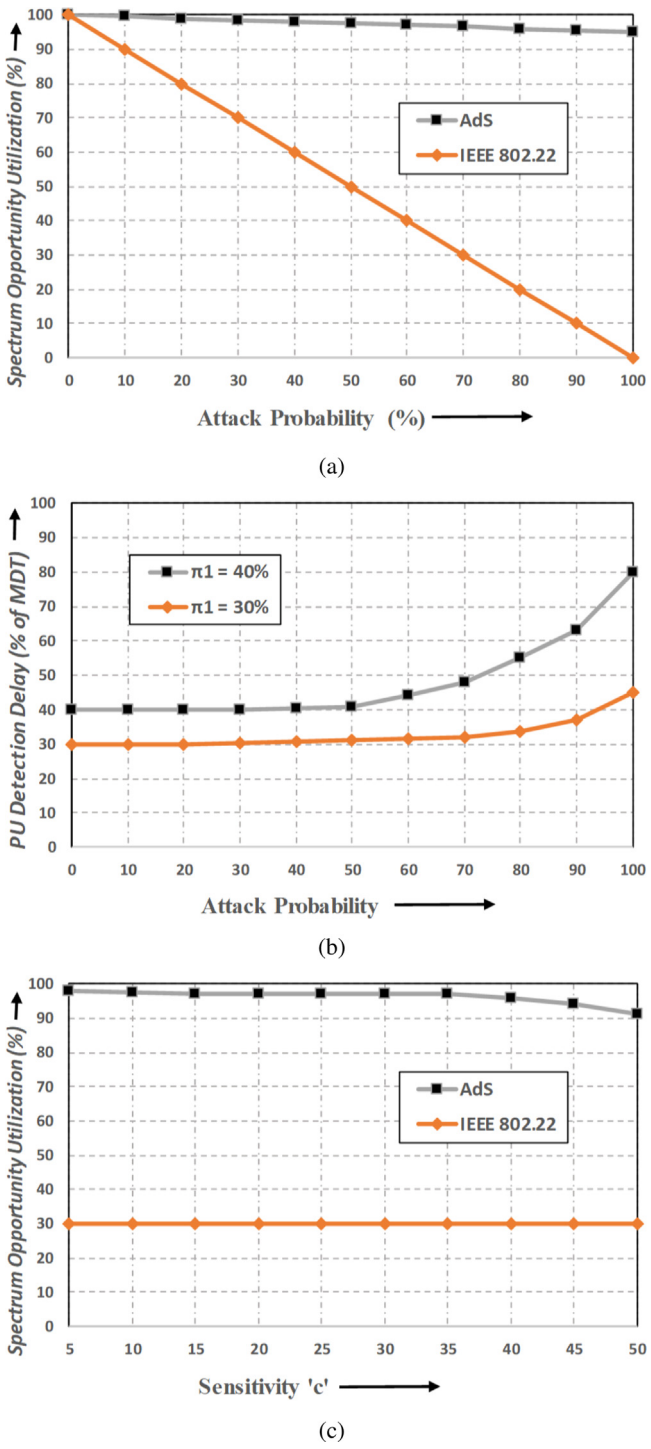
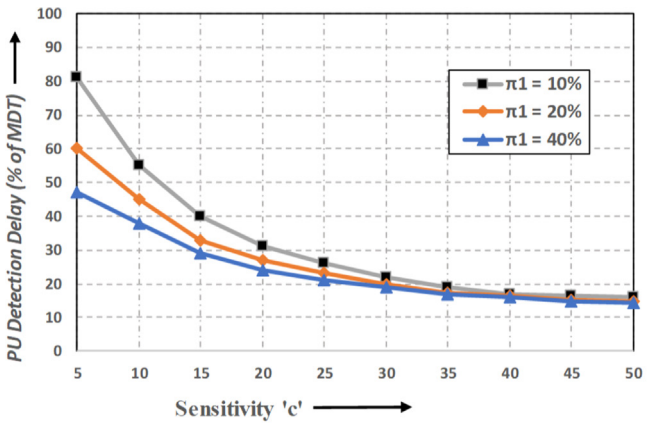
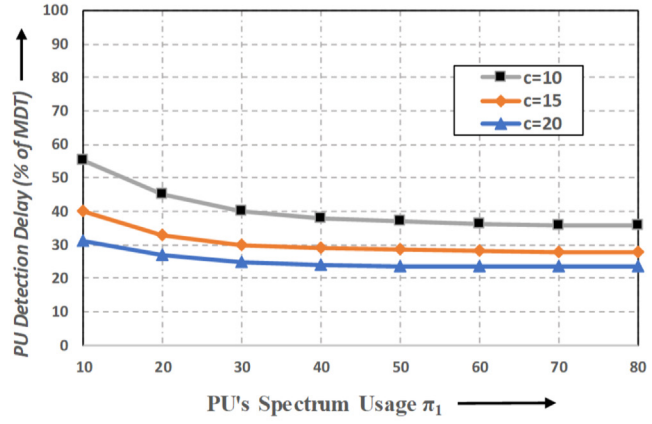


Fig. 6. Effect of various parameters on AdS's performance, (a) Spectrum opportunity utilization with varying attack probability (b) Delay in detection of PU with varying attack probability, (c) effect of sensitivity towards PU detection delay on spectrum opportunity utilization.

FCC, of non-interference with the PU's communications. AdS is very effective in dealing with MDoS jamming attack and it never allows for the delay in detecting PU's presence on the channel to exceed the MDT constraint. PU detection delay stays below 40% when the MDoS jamming attack rate is below 50% and increases to 60% of the MDT when the attack severity is at its maximum (100% of the time) when the PU;s spectrum usage is kept constant at 30%. Delay in the detection



(a)



(b)

Fig. 7. Effect of various parameters on AdS's performance, (a) effect of sensitivity on PU detection delay (b) effect of PU activity on spectrum opportunity utilization (c) Effect of PU's spectrum usage on the delay in detecting PU.

of the PU increases within the MDT constraint with the increase in PU's spectrum usage to 40%.

Due to its static nature of deciding to carry out fine sensing, spectrum opportunities are wasted by the IEEE 802.22 standard proportional to the amount of MDoS jamming attacks. As evident from Fig. 6(c), at a constant MDoS jamming attack rate of 70%, spectrum opportunity utilization by IEEE 802.22 stays at a constant 30%. However, AdS's spectrum opportunity utilization rate is far greater. The effect of varying its sensitivity c on spectrum opportunity utilization can be seen in this figure as well. A higher value of sensitivity would mean that the cost factor has a higher value and the CRN would be more likely to carry out fine sensing instead of deferring it to a later CDT slot. Its effect on PU detection delay and the MDT constraint are shown in Fig. 7(a). By having a sufficiently large value of sensitivity, AdS can be made to perform just as the IEEE 802.22 standard which would have a minimum delay of 1 CDT slot to confirm the presence of the PU on the channel, giving a theoretical minimum delay of 8% of MDT constraint while achieving much greater spectrum opportunity utilization under MDoS jamming attack.

When the PU increases its use of the spectrum, it has a similar effect on the CRN's operation as an increase in MDoS jamming attack i.e., there would be a proportional increase in the fast sensing alerts. This in turn would have a similar response by both the IEEE 802.22 standard as well as AdS. As expected, IEEE 802.22 would result in a proportional decrease in spectrum utilization as there would be fewer spectrum opportunities. Increased spectrum usage by the PU would have no effect on the IEEE 802.22 standard's detection of PU however, it *does* have an effect on AdS as shown in Fig. 7(b). As the spectrum usage by the PU increases, MDoS jamming attack would decrease proportionally thereby increasing the cost of PU's detection being missed. Resultantly, when the PU's presence on the channel increases, it would be detected much faster.

5.3. Discussion

In this subsection, we provide a discussion on AdS's handling and performance under varying network conditions including noise and MDoS jamming attack. AdS, on one hand, provides security against MDoS jamming attack while on the other hand mitigates the effects of noise on the channel and improves spectrum opportunity utilization. Its strength lies in its adaptability to changing channel conditions by utilizing its optimization approach. It becomes more aware of channel conditions by including in its objective function, an estimate of noise as well as MDoS jamming attack severity. Various channel conditions along with AdS's handling of them are depicted in Fig. 8.

Low Primary User's Activity: The state when the PU is idle on the channel is shown in Fig. 8(a). The lower half of the figure shows channel state, IEEE 802.22 standard's handling of the state and also AdS's response to it. The upper half of the figure shows two aspects of AdS: the changes in its cost factor $\gamma_{kt}P_k$ at any given CDT slot (shown in solid red plot) and the adaptive fine sensing threshold (shown in dotted blue horizontal line). The cost factor increases with respect to the number of CDT slots since last fine sensing and approaches infinity near the MDT constraint.

The cost factor γ_{kt} in the optimization objective function of Eq. (4), assumes its values depending on the value of k as per Eq. (6). The value of k is the number of CDT slots since the result of last fine sensing carried out by the CRN, was that the PU is in idle state. Therefore, when the CRN is not under MDoS jamming attack or noise, and the PU is also idle, then fast sensing is unlikely to raise an alert. Therefore, when fast sensing *does* raise an alert (meaning that the PU has become active), then $k > \tau$ and $\gamma_{kt} = \infty$ making it greater than adaptive fine sensing threshold and will force AdS's cost minimization function to conduct fine sensing since the optimal fine sensing decision would be $p_t^* = 1$ as per Eq. (7). This shows that under normal channel state, fine sensing will always be carried out similar to the IEEE 802.22 standard as soon as the fast sensing gives an alert and PU's detection will never be deferred.

High Primary User's Activity: High level of PU's usage of the channel is depicted in Fig. 8(b). Although the PU is more active and as a result, there are more fast sensing alerts, AdS defers carrying out fine sensing for the first 3 CDT slots because during that time, the cost factor $\gamma_{kt}P_k$ remains below the adaptive fine sensing threshold. It is worth noting that the IEEE 802.22 standard carries out fine sensing during every CDT slot that has a fast sensing alert.

It is evident that the deferment of fine sensing by AdS causes interference to PU's communication during the CDT slots when the cost factor $\gamma_{kt}P_k$ was below the fine sensing threshold. However, this delay and subsequent detection of PU's signal on the channel is well within the MDT constraint. Once PU's signal has been detected, the associated cost of deferring PU's detection stays above the threshold for adaptive fine sensing during subsequent CDT slots due to which, whenever there is fast sensing alert, the CRN always carries out fine sensing until the PU goes off-air again. The amount of interference with PU's signals can be adjusted by having the sensitivity tuned to an appropriate value in Eq. (6).

MDoS Jamming Attack and Noisy Channel:

Fig. 8(c) represents the situation when the attacker launches the MDoS attack on the CRN during the CDT slots when the PU is in inactive state. Assuming that the fast sensing alerts are received in every CDT slot, IEEE 802.22 standard responds by carrying out fine sensing after every alert. On the contrary, AdS responds by calculating the cost factor $\gamma_{kt}P_k$ during every CDT slot and comparing it with the

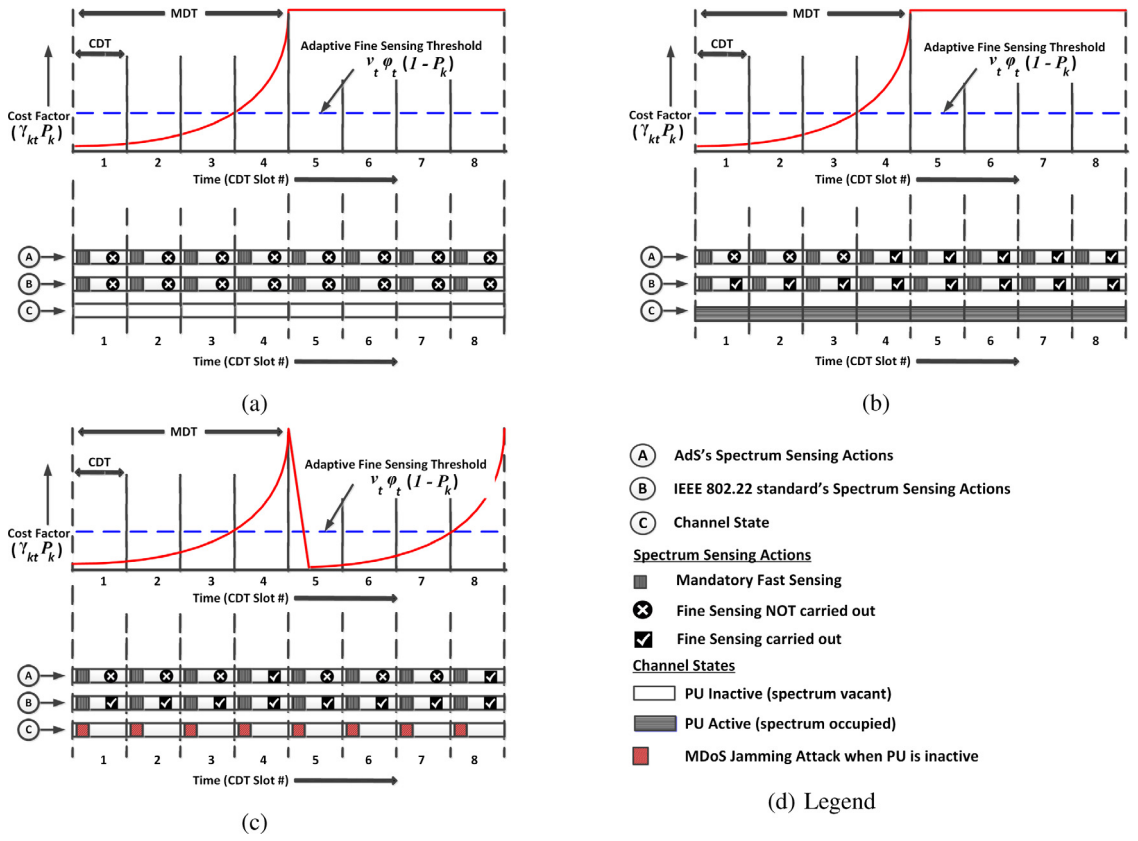


Fig. 8. Comparison of AdS with IEEE 802.22 under various conditions (a) Low Primary User's activity. (b) High Primary User's Activity and (c) Under MDoS jamming attack and noisy channel. The lower part of the figures shows channel state and spectrum sensing actions by the IEEE 802.22 standard and AdS whereas the upper part of the figures shows the cost minimization function's value at every CDT slot. As evident, AdS performs fine sensing due to fast sensing alert only when the cost factor $\gamma_{kt} P_k$ is greater than the adaptive fine sensing threshold. MDT is set at 4 CDT slots in this figure, instead of 12 CDT slots specified by the standard because of limited space.

adaptive fine sensing threshold. It decides to carryout fine sensing after fast sensing alert is received, only when the cost factor becomes more than the threshold while staying within the MDT constraint.

As evident from Fig. 8(c), IEEE 802.22 standard's static nature of response to fast sensing alerts causes all spectrum opportunities to be wasted. However, as the cost factor remains below the adaptive fine sensing threshold, AdS ignores fast sensing alerts until CDT slot number 3. As soon as the cost factor becomes greater than the threshold at CDT slot number 4, AdS decides to carry out fine sensing and finds out that the alert was due to MDoS jamming attack or noise and not due to PU's signals. This resets AdS's cost factor to its lowest value for next CDT slot. Although the attacker launched MDoS jamming attack in all vacant CDT slots, AdS was able to defeat the attack and utilize the opportunity 75% of the time. Simulations with actual values for MDT and CDT have shown that AdS achieved much higher values of spectrum opportunity utilization. Adaptive spectrum sensing enables the CRN to utilize spectrum opportunities to the maximum and will mitigate the effects of noise and MDoS jamming attacks.

6. Conclusion

In this paper, we have shown that the two-stage spectrum sensing mechanism in IEEE 802.22 standard suits malicious nodes in the CRN which intend to deny the use of vacant spectrum to the CRN by jamming its communication while at the same time minimizing the amount of power expended on jamming. Such Minimal Denial of Service (MDoS) jamming attack can be launched by the malicious nodes by transmitting a very short jamming signal during the mandatory fast sensing stage which will in turn force the CRN to carry out the otherwise optional, fine sensing. MDoS jamming attack results in wastage of spectrum opportunities for the rest of the CRN to the extent which can jeopardize its survivability. As a countermeasure for such attacks, we have proposed AdS, a novel adaptive spectrum sensing technique which has the ability to thwart MDoS jamming attack as well as mitigate the effects of noise on the spectrum sensing in DSA. It enhances spectrum opportunity utilization through adaptive fine sensing decisions. AdS utilizes the *Maximum Detection Time or MDT* constraint of the amount of delay allowed before the primary user of the spectrum must be detected and its licensed channel must be vacated by the CRN. It achieves up to 90% improvement in spectrum opportunity utilization and when required, can also be tuned to behave exactly as the IEEE 802.22 standard.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] IEEE 802.22-2011 - IEEE standard for local and metropolitan area networks - Specific requirements - Part 22: Cognitive wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV bands.

[2] C. Cordeiro, K. Challapali, D. Birru, S. Shankar, IEEE 802.22: the first worldwide wireless standard based on cognitive radios, New Front. Dyn. Spectr. Access Netw., (DySPAN) (2005).

[3] J. Mitola, G.Q. Maguire Jr., Cognitive radio: making software radios more personal, IEEE Pers. Commun. 6 (4) (1999) 13–18.

[4] U S. FCC, ET Docket 04- 186, notice of proposed rule making, in the matter of unlicensed operation in the TV broadcast bands, May 25, 2004.

[5] C. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. Shellhammer, W. Caldwell, IEEE 802.22: The first cognitive radio wireless regional area network standard, IEEE Commun. Mag. 47 (2009) 130–138.

[6] I.F. Akyildiz, W. Lee, K.R. Chowdhury, CRAHNs: Cognitive radio ad hoc networks, Ad Hoc Netw. (2009).
[7] T. Yucek, H. Arslan, A survey of spectrum sensing algorithms for cognitive radio applications, IEEE Commun. Surv. Tutor. 11 (2009) 116–130.
[8] K. Kim, I.A. Akbar, K.K. Bae, Um. Jung-Sun, C.M. Spooner, J.H. Reed, Cyclostationary approaches to signal detection and classification in cognitive radio, in: IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2007.
[9] S.J. Shellhammer, Spectrum sensing in IEEE 802.22, in: IAPR Workshop on Cognitive Information Processing (CIP), 2008.
[10] M. Faisal Amjad, B. Aslam, C.C. Zou, DS3: A dynamic and smart spectrum sensing technique for cognitive radio networks under denial of service attack, in: IEEE Global Communication Conference (Globecom), Atlanta USA, Dec. (2013) pp. 9-13.
[11] G. Han, L. Xiao, H. Vincent Poor, Two dimensional anti-jamming communication based on deep reinforcement learning, in: The 42nd IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017.
[12] F. Slimeni, B. Scheers, Z. Chtourou, V. Le Nir, Jamming mitigation in cognitive radio networks using a modified Q-learning algorithm, in: IEEE International Conference on Military Communications and Information Systems (ICMCIS), Cracow, 2015.
[13] Chen Ruiliang, Jerry Park Jung-Min, Bian Kaigui, Robustness against Byzantine failures in distributed spectrum sensing, Elsevier Comput. Commun. (2012).
[14] S. Liu, L. Lazos, M. Krunz, Thwarting control-channel jamming attacks from inside jammers, IEEE Trans. Mob. Comput. 11 (9) (2012) 1545–1558.
[15] S. Jana, et al., Trusted collaborative spectrum sensing for mobile cognitive radio networks, in: 32nd IEEE International Conference on Computer Communications, INFOCOM, 2012.
[16] Q. Wang, K. Ren, P. Ning, Anti-jamming communication in cognitive radio networks with unknown channel statistics, in: 19th IEEE International Conference on Network Protocols (ICNP), 2011.
[17] B. Wang, Y. Wu, K.J.R. Liu, T.C. Clancy, An anti-jamming stochastic game for cognitive radio networks, IEEE J. Sel. Areas Commun. (JSAC) 29 (4) (2011) 877–889.
[18] H. Li, Z. Han, Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems, in: IEEE Global Telecommunications Conference (GLOBECOM), 2009.
[19] S. Sodagari, T.C. Clancy, An anti-jamming strategy for channel access in cognitive radio networks, in: 2nd international conference on Decision and Game Theory for Security (GameSec), 2011.
[20] C. Chen, M. Song, C. Xin, J. Backens, A game-theoretical anti-jamming scheme for cognitive radio networks, IEEE Netw. 27 (2013).
[21] W. Wenjing, M. Chatterjee, K. Kwiat, Collaborative jamming and collaborative defense in cognitive radio networks, in: IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011.
[22] Y. Wu, B. Wang, K.J.R. Liu, Optimal defense against jamming attacks in cognitive radio networks using the Markov decision process approach, in: IEEE Global Telecommunications Conference (GLOBECOM), 2010.
[23] X. Zhang, Q. Wu, J. Wang, Optimization of sensing time in multichannel sequential sensing for cognitive radio, Internat. J. Comm. Syst. (2013) http://dx.doi.org/10.1002/dac.1341.
[24] C. Ghosh, Carlos Cordeiro, D.P. Agrawal, M.B. Rao, Markov chain existence and hidden Markov models in spectrum sensing, in: IEEE International Conference on Pervasive Computing and Communications, (PerCom), 2009.
[25] Li Xiaoyuan, Wang Dexiang, Mao Xiang, J. McNair, On the accuracy of maximum likelihood estimation for primary user behavior in cognitive radio networks, IEEE Commun. Lett. 17 (5) (2013) 888–891.
[26] T.M. Taher, et al., Long-term spectral occupancy findings in Chicago, New Front. Dyn. Spectr. Access Netw. (IEEE DySPAN) (2011).