ANALYSIS OF SNIFFER CHANNEL ASSIGNMENT FOR COGNITIVE RADIO NETWORKS

Adithya G S Kumar[#1], Kiran W S[#2]
.[#1] *M.E graduate, Electronics and Communication Engineering,*
.[#2]*AP, ECE Department, Sivaji College of Engineering and Technology*
ws.kiran@gmail.com, adithyagskumar@gmail.com

***Abstract*: This paper mainly concentrates on the security aspects of cognitive radio systems. CR devices have become more exposed to both internal and external attackers and hence they are vulnerable to malicious behavior. Sniffer channel assignment (SCA) is a fundamental building block for wireless data capture, which is essential for traffic monitoring and network forensics. Most of the existing SCA approaches for cognitive radio networks (CRNs) adopt optimization-based methods and rely on the prior knowledge of the secondary user (SU) activities. To relax this constraint, learning-based methods have been recently developed; however, there is still insufficient theoretical understanding within the learning framework for SCA. In the proposed model, it aims to maximize the total amount of the captured SU traffic, and formulate the SCA problem as a non-stochastic/adversarial multi-armed bandit problem. Moreover, the inherent error in wireless capturing, i.e. imperfect monitoring, is considered in our model. It proposes two online learning algorithms for the SCA scenarios with and without channel switching costs, respectively, and their regret performances are proven uniformly sub linear in time and polynomial in the number of channels. The numerical evaluation shows, in addition to their robust regret performances, the proposed algorithms greatly outperform the existing SCA approaches in the amount of effectively captured SU traffic. The proposed solution has a strong theoretical performance guarantee in terms of the amount of effectively captured traffic, without prior knowledge of the SU activities.**

***Keywords*: Cognitive Radio, Sniffers, Sniffer Channel Assignment, Non Stochastic Muti-armed Bandit Problem**

I. INTRODUCTION

Cognitive radio network (CRN) is a promising paradigm to solve the contradiction between the limited wireless spectrum resources and the growing number of mobile applications. By exploiting the spectrum in an opportunistic fashion, CRNs allow the secondary users (SUs) to use the licensed bands without generating excessive interference to primary users (Pus).In the last several years, the spectrum sharing (SS) systems have been widely studied due to their advantage in solving the spectrum demand.

Several attack patterns and their counter measures have been investigated, including spectrum sensing data falsification, primary user emulation attack, jamming attack and etc. Moreover, the potential infringements of the licensed spectrum call for the research of network forensics in CRNs. To deal with all these security threats, various network management applications, such as traffic monitoring and network forensics, have to be developed for CRNs. As a result, wireless data capture, which is a fundamental building block of those applications, attracts increasing research attention. Typically, the task of wireless data capture is implemented by deploying passive sniffers.

- ***Sniffers***

Sniffers are a family of dedicated hardware devices, which can gather wireless signals and decode the PHY/MAC information within. They are used to avoid traffic in file sharing applications. A wireless sniffer is a type of packet analyzer. A packet analyzer (also known as a packet sniffer) is a piece of software or hardware designed to intercept data as it is transmitted over a network and decode the data into a format that is readable for humans. Wireless sniffers are packet analyzers specifically created for capturing data on wireless networks. It is a piece of software that grabs all traffic flowing into and out of the computer network.

Uses of Sniffers

- Analyze network problems
- Detect network intrusion attempts

© Journal - ICON All Rights Reserved

- Detect network misuse by internal and external users
- Documenting regulatory compliance through logging all perimeter and endpoint traffic
- Gain information for effecting a network intrusion
- Isolate exploited systems
- Monitor WAN bandwidth utilization
- Diagnosing and investigating network problems
- Monitoring network usage, ability and security
- Discovering network misuse, attack attempts, malware and vulnerabilities
- Filtering network traffic
- Identifying configuration issues and network bottlenecks.

➢ ***Sniffer Channel Assignment***

A sniffer usually has a limited special range and spectrum bandwidth of monitoring, which gives rise to the problem of sniffer channel assignment (SCA) in broadband multi-channel wireless networks. In essence, the SCA problem asks for the optimal matching, in some sense, between sniffers and channels. In the previous research, the working channels of sniffers are often assigned in a static manner, aiming to maximize the total amount of collected information. The SCA problem stacks a new dimension of challenge, i.e., the opportunistic access behaviors of SUs. Most of the existing optimization-based approaches rely on the assumption that, the user activities can be described by some known distribution or be inferred by continuous channel scanning. However, there are various factors with unknown nature affecting the SU activities, such as the channel access patterns of PUs, data arrival processes at SUs, the spectrum sharing strategy/regulation and etc, and furthermore, malicious or misbehaving SUs potentially exist.

Hence, it is unrealistic to build up the prior knowledge of SU activities more often than not. To relax the strong knowledge constraint in modeling, some learning-based approaches have been proposed in the literature, where the knowledge of the SU activities is acquired over time via observations.

➢ ***Multi-armed Bandit Problem***

The multi-armed bandit, or simply the bandit problem, models the sequential decision process of a decision-maker under uncertainty in the rewards associated with a set of actions. As a gambler in face of a collection of slot machines, once selecting an action or a particular machine, a corresponding reward that is unknown a priori will be generated for the decision-maker. The objective of the bandit problem is to figure out the best sequence of arm pulls so as to maximize the sum of rewards. There is a crucial trade-off between "exploitation" (i.e., to utilize the machine that is likely to yield the highest reward) and "exploration" (i.e., to get more information about the expected rewards of the other machines).

Based on the assumptions on the underlying reward, the bandit problems can be categorized into two families, namely the stochastic versus the non-stochastic/adversarial. In stochastic MAB, the reward of each arm is assumed to be given by a stochastic process with possibly unknown parameters. In the non-stochastic bandit problems, the rewards of arms are not endowed with probabilistic models, but are rather assumed deterministic, yet unknown, or even chosen by an adversary given the decision-maker past actions. This formulation essentially considers the bandit problem from a sample path perspective. Comparing to the (non-stationary) stochastic MAB, the solutions of non-stochastic MAB generally target a worst-case performance guarantee that applies to any particular sequence of rewards.

II. EXISTING SYSTEM

Due to the highly dynamic nature of the CR network architecture, legitimate CR devices become exposed to both internal as well as to external attackers and hence they are extremely vulnerable to malicious behavior. For example, an illegitimate user may intentionally impose interference (i.e. jamming) for the sake of artificially contaminating the CR environment. Hence, the CR users fail to accurately characterize

© Journal - ICON All Rights Reserved

their surrounding radio environment and may become misled or compromised, which leads to a malfunction. Alternatively, an illegitimate user may attempt to tap the communications of authorized CR users by eaves dropping, to intercept confidential information. Clearly, CR networks face diverse security threats during both spectrum sensing as well as spectrum sharing, spectrum mobility and spectrum management. Extensive studies have been carried out for protecting CR networks both against primary user emulation (PUE) and against denial of- service (DoS) attacks.

In addition to PUE and DoS attacks, eavesdropping is another main concern in protecting the data confidentiality, although it has received less attention in the literature on CR network security. Traditionally, cryptographic techniques are employed for guaranteeing transmission confidentiality against an eavesdropping attack. However, this introduces a significant computational overhead as well as imposing additional system complexity in terms of the secret key management. Furthermore, the existing cryptographic approaches are not perfectly secure and can still be decrypted by an eavesdropper (E), provided that it has the capacity to carry out exhaustive key search with the aid of brute-force attack.

To combat the fading effects, multiple-input multiple-output (MIMO) schemes as well as cooperative relaying and beam forming techniques were investigated for the sake of enhancing the achievable wireless secrecy capacity. In contrast to conventional non-cognitive wireless networks, the physical-layer security of CR networks has to consider diverse additional challenges, including the protection of the primary user's QoS and the mitigation of the mutual interference between the primary and secondary transmissions. The notion of the SRT in wireless physical layer security was introduced and examined in, where the security and reliability was characterized in terms of the intercept probability and outage probability, respectively. In contrast to the conventional non-cognitive wireless networks studied in, the SRT analysis of CR networks presented in this work additionally takes into account the mutual interference between the primary user (PU) and secondary user (SU).

The relay selection has been used in the previous survey where there is SRS and MRS strategy which compares with the classical direct transmission and artificial noise based methods. The paper shows that the MRS scheme outperforms the other schemes when the intercept probability is plotted against the outage probability.

A. Disadvantages of Existing System

- Computational overhead as well as imposing additional system complexity in terms of the secret key management
- Eavesdropper can easily crack the message by using Brute force attack.
- SNR is low
- Data rate is low.
- Some optimization problem.

III. PROPOSED SYSTEM

This paper aims to maximize the total amount of the sniffed or effectively monitored SU traffic, and formulate the SCA problem as a non-stochastic/adversarial multi-armed bandit (MAB) problem. The inherent error in wireless capturing, i.e. imperfect monitoring, is also considered in our model. A family of online learning algorithms was proposed for the SCA problem in which the channel switching may not be negligible. The proposed solution has a strong theoretical performance guarantee in terms of the amount of effectively captured traffic, without prior knowledge of the SU activities.

The main contributions include:

* In light of the volatile characteristics of SU activities, we formulate the SCA problem as a non-stochastic/adversarial MAB problem, without probabilistic models of the SU activities. Imperfect monitoring and channel switching costs, often non-negligible in realistic data capture applications, are incorporated in our model, which is applicable when the unreliability in monitoring is time-varying.

© Journal - ICON All Rights Reserved

* A family of learning-based algorithms was proposed as the solution to the above SCA problem, and we theoretically prove the performance bound of the proposed algorithms.
* The performance of the proposed solution was numerically validated, and empirically shows that our solution significantly outperforms existing ones in the literature.

A. Advantages of Proposed system

- Complexity is low.
- Utilises low power compared to other techniques.
- Reduced transmitter and receiver complexities.

IV. STSTEM MODEL AND PROBLEM FORMULATION

A) SYSTEM MODEL

An independent data capture system deployed in a CRN. The system objective is to capture as much SU traffic as possible, so as to support applications like network monitoring and network forensics.

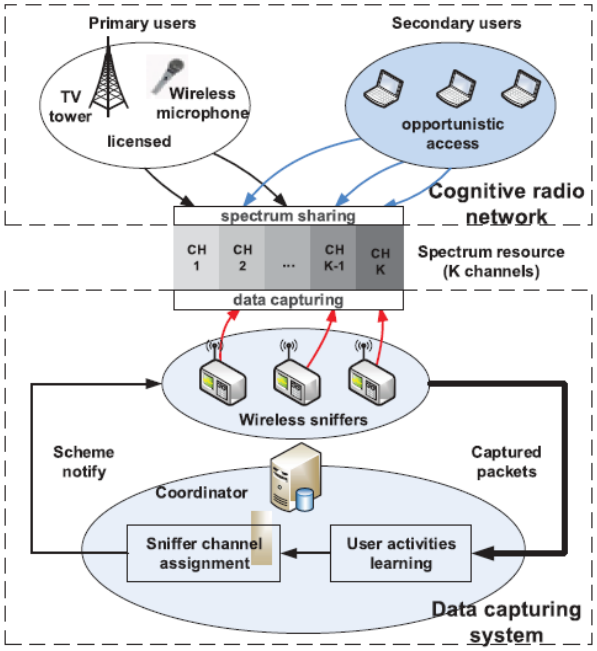


Fig1: Application of wireless data capture system for cognitive radio networks

The main assumptions and key components in this scenario are as follows, assuming the system operates in discrete-time units, called time slots.

• ***Spectrum resource*:** The spectrum resource is partitioned to K channel. They are licensed to the PUs, and can be utilized by the SUs subject to application-specific spectrum sharing regulations.

• ***Target cognitive radio network*:** The target CRN consists of a number of PUs and SUs. The SUs are allowed to opportunistically access the channels in each time slot. There is no information known a priori about the SUs. They can be either regular or misbehaving users, and their traffic characteristics are unknown.

• ***Data capture system*:** This system consists of S distributed sniffers ($S < K$) and one coordinator server. Each sniffer can be assigned to monitor any of the K channels, and communicate with the coordinator via a dedicated control channel. In each time slot, the sniffers report their monitoring results to the coordinator. The latter learns the SUs activities, determines the sniffer-channel assignment, and then notifies the sniffers for the next time slot.

Two specific issues that often arise in practice are considered in this system:

– ***Imperfect monitoring*:** The monitoring and capture of traffic by sniffers is unreliable. The packets of SUs are successfully captured with certain probability, which we call the *capture probability*. It can be time-varying due to channel fading and etc. In this paper, it is assumed that there is a known range for this capture probability, which can be estimated via measurement conducted in controlled propagation environment.

– ***Channel switching cost*:** A sniffer is able to operate on only one channel in each time slot. If the target channel in the next time slot is different from the current one, the sniffer has to switch channel, and a non-negligible channel switching cost will be incurred. This cost may relate to the time delay or the energy consumption of each frequency tuning1. In this paper, the possible miss in monitoring of traffic caused by such switching delay will be considered.

© Journal - ICON All Rights Reserved

B) PROBLEM FORMULATION

The SCA problem faces the classic "exploitation-exploration" dilemma that can be modeled by multi-armed bandit problem, that is, to deploy the sniffers on the channels that have been observed with higher reward, or to deploy the sniffers on those under-utilized channels that can bring potentially higher reward in the future. Provided the uncertainty in a CRN that we have previously discussed, we formulate the SCA problem as a non-stochastic bandit problem.

We denote by $\boldsymbol{a}$ an admissible sniffer channel assignment scheme where $\boldsymbol{a} = (a1, a2, \ldots, aS)$ and $ai = j$ if sniffer i is assigned to monitor channel j for any $i \in [S] := \{1, 2, \ldots, S\}$ and $j \in [K] := \{1, 2, \ldots, K\}$. Given any $\boldsymbol{a}$, there exists an equivalent matrix representation A such that $Ai\ j = 1$ if $ai = j$ and $Ai\ j = 0$ otherwise. For example, consider 4 channels and 2 sniffers (i.e., $K = 4$ and $S = 2$). An admissible scheme $\boldsymbol{a} = (1\ 4)$ can be alternatively denoted by 1 for a detailed study on this issue,

In the rest of this paper, $\boldsymbol{a}$ represent a sniffer channel assignment scheme in either format whenever there is no ambiguity in the context. Also, when $\boldsymbol{a}$ is in the matrix form, ai, j denotes its (i, j)th entry. The capture probability matrix is denoted by Pc, of which the (i, j)th entry $Pc(i, j) \in (0, 1]$ represents the probability that an SU packet on channel j is successfully captured by sniffer i, if the sniffer is deployed on this channel when the packet is transmitted. For the time being, Pc is time-invariant and known a priori via measurement. Let A be the set of admissible sniffer channel assignment schemes and _A be the set of all probability distributions over A.

The performance of policy is then measured by the notion of regret, which is the difference between the rewards of one given policy and that of a reference policy. We shall adopt the optimal static policy as the reference one: assuming a genie with prior knowledge on the sequence of SU activities, the optimal static policy is then the one that plays persistently the "best" arm, i.e., to deploy the S sniffers on the S most SU-active channels in hindsight among the K channels, which generates the highest reward. This is in fact a highly non-trivial reference to compete and infeasible to implement in our setup without genie knowledge. In this case, the regret is also termed weak regret or external regret in the online learning literature.

In the next section, a family of algorithms is proposed that generate policies for the SCA problem with sub linear regret over time. That is, the proposed solution performs no worse than the optimal static policy on average asymptotically.

V. ONLINE SNIFFER CHANNEL ASSIGNMENT POLICY

In this section, presents online sniffer channel assignment algorithms that achieve order-optimal sub linear regrets. Firstly describe an algorithm for the case when there is no switching cost, which will be used as a building block when we incorporate the switching costs in the second part.

A) SNIFFER CHANNEL ASSIGNMENT WITHOUT SWITCHING COSTS

A straightforward solution to the SCA problem with imperfect monitoring is to treat each SCA scheme as an arm, and to invoke the classic Exp3 algorithm. Though sub linear in time, the regret of the Exp3 algorithm typically scales in polynomials. A naive conversion of a combinatorial problem to the classic bandit setting, as aforementioned, will result in an exponentially large action space, and the regret performance is rather unsatisfactory for most applications. We note that our problem is in essence a bipartite matching problem. For a balanced bipartite graph, a perfect matching is the one in which every vertex of the graph is incident to exactly one edge, and each matching can be expressed as a permutation.

The problem setup for the ExpMatch algorithm is closely related to our formulation, and we provide a brief overview in the following to help highlight our generalization later.

For each round $t = 1, 2, \ldots, T$:

1) The decision-maker chooses a perfect matching between two sets of vertices, each with the size of n and denoted by U and V.

© Journal - ICON All Rights Reserved

2) An adversary assigns an individual loss $li, j \in [0, 1]$ for each matched pair (i, j), where $i \in U$ and $j \in V$.
3) The decision-maker perfectly observes the loss of the chosen matching and suffers an aggregate loss as the sum of all individual losses. The matching decision process proceeds to the next round.

The reward yi, j in our formulation is hence given by a random variable with an arbitrarily assigned mean (depending on the value of $xt\ j$), whereas li, j in the above framework is a deterministic though arbitrary value.

The adapted ExpMatch algorithm, detailed in Algorithm 1, inherits two fundamental ideas of the well-known Exp3 algorithm: single-sample unbiased estimation of the reward and randomization with exponential weights, which are the key ingredients to ensure a sub linear regret uniformly in time.
Moreover, instead of regarding each matching as an arm in the bandit problem and maintaining a weight for each matching, the algorithm keeps individual weights for sniffer channel pairs, and uses the total $S \times K$ weights, in the form of a weight matrix, to generate a distribution over exponentially many matching. This is the key to reduce the dependence of regret on S and K to a polynomial order instead of an exponential one. This method is feasible due to the Birkhoff-von Neumann theorem and the Sinkhorn-Knopp algorithm.

The former states that any doubly stochastic matrix can be decomposed as a convex combination of permutation matrices and the coefficient can be interpreted as the probability of choosing a matching represented by a permutation matrix. The latter provides an efficient approach to convert any non-negative matrix to a doubly stochastic matrix by using the Kullback-Liebler projection.

The algorithm maintains two matrices: the weight matrix $\boldsymbol{W}$ and the doubly stochastic matrix $\boldsymbol{D}$. In each time slot, the coordinator assigns probability masses to sniffer channel assignment schemes by decomposing the doubly stochastic matrix $\boldsymbol{D}$ (Step 2) using the subroutine Decompose, and the generated distribution over A has a support of size less than $S \times K + 1$.

A sniffer channel assignment scheme is then realized per the mixture of this distribution and the uniform distribution (Step 3). At the end of a time slot, the observation from each monitored channel is reported to the coordinator, and the gathered information is then used to estimate the true reward (the number of SU packets) on each channel (Step 4). Finally, the weight matrix is updated (Step 5) and a corresponding doubly stochastic matrix is constructed for the next slot (Step 6) using Sinkhorn-Knopp. We note that the non-negligible overhead can be modeled in the cost term C in the reward, with slight abuse of the name of channel switching costs.

B) SNIFFER CHANNEL ASSIGNMENT WITH SWITCHING COSTS

When there is no switching cost associated with each pair of consecutive actions by the coordinator, the SU traffic can be regarded in aggregate as an "oblivious" adversary who determines the reward at time t solely based on the current sniffer channel assignment scheme. In other words, the adversary is unaware of the coordinator's past deployment decisions. With the introduction of switching costs, the adversary can be regarded as "non-oblivious" with one unit of memory for the coordinator's action in the last step, and exerts an additional cost $C(\boldsymbol{at}\,|\boldsymbol{at}-1)$ at time t. Online learning problems with a non-oblivious adversary have attracted considerable attention in recent years with various learning algorithms proposed. The main idea is to divide time slots to mini-batches and the actions in each mini-batch of slots are static so as to neutralize the effect of bounded memory of the adversary. Based on the meta algorithm proposed in, we introduce a new algorithm using the adapted ExpMatch introduced.

VI. REGRET ANALYSIS

- ***Regret of Algorithm 1***

ExpMatch and its prototype for non-combinatorial bandit problems, i.e., Exp3, are both online learning algorithms in the family of exponential weight

© Journal - ICON All Rights Reserved

algorithms and particularly designed for the partial observation case, in which only the rewards of the played arms/matching pairs are observed. The key of ExpMatch and Exp3 to tackle partial observation is to maintain a single-sample unbiased estimator of reward on each arm/matching pair at any time, even though it may not be played in a realization. In Algorithm 1, $\tilde{y}t\ i, j$ also provides an unbiased estimation for the average reward when assigning sniffer i to channel j in our problem, where the data capture is subject to uncertainty characterized by the capture probability $Pc(i, j)$. The expected regret of Algorithm 1, given any realization of SU traffic, is upper bounded the regret of the bipartite matching problem with full information establishes lower bound on the regret for the partial and unreliable observation case as our SCA problem. Thus, we conclude that Algorithm 1 enjoys an order-optimal sub linear regret.

- ***Regret for Algorithm 2***

With the regret bound for the adapted algorithm, the regret of Algorithm 2 follows from the meta algorithmic analysis. In the above result, the value of τ explicitly depends on T, which is in general not given a priori in practice. This dependence in fact can be removed by using the standard "doubling trick". The idea is to partition the time into periods of exponentially increasing lengths and to parameterize the algorithm for each period with a fixed length, so as to achieve a horizon independent bound on the same logarithmic order

VII. RESULTS AND DISCUSSIONS

The numerical results from Matlab simulations are used to evaluate the proposed algorithms.

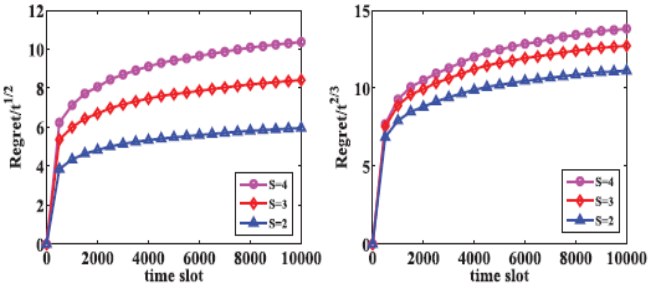
A. Setup and Performance Metrics

The total numbers K and S of channels and sniffers are respectively randomly selected from [6, 12] and [2, $\_K/2\_$]. The capture probabilities are randomly generated in the range of $(0, 1]$.

1) ***Synthetic PU Traces:*** Without loss of generality, consider the case that each channel is licensed by one PU. Assume that the activities of PU evolve as a Markovian process over time with two states (present and not present in a channel), and generate each PU trace with a randomly produced transition probability matrix.

2) ***Synthetic SU Traces:*** The number of SUs is randomly chosen in the range of [6, 20]. Generate Poisson time series to emulate the packet arrivals of each SU. For a given SU, if it has packets in the current time slot, it accesses one of the channels according to a predefined pattern, which we will elaborate later. If the channel is occupied in the pre-generated PU traces, the SU then evacuates from this channel. When a channel is selected by multiple SUs in the same slot, one SU is chosen uniformly and randomly, and the others back off. In both of the previous cases, the SUs that have no access to a channel defer their transmission to the next time slot. Four types of access patterns are implemented in our simulations:

- ***Static pattern:*** The SU persistently attempts to access the same channel during the entire simulation.
- ***Hopping pattern:*** The SU actively switches to the neighboring channel in the case of access failure, i.e., a round robin manner to choose the next channel in the ascending order.
- ***Random pattern:*** The SU randomly selects a candidate channel in every attempt.
- ***MAB pattern*:** The SU adopts the sensing and access strategy that proposed in which the channel with the highest "free" probability will be selected based on the historical statistics of channel idle states.



(a) Algorithm 1 (b) Algorithm 2

Fig. 2. Regret of our proposed policies under various sniffer number (K = 8)

© Journal - ICON All Rights Reserved

In addition to the proposed algorithms in this paper, it also implements two SCA policies for comparison.

• ***Random policy.*** The operating channels of the sniffers are randomly assigned at each time slot.

• ***SVR policy*** . The channels are indexed by the estimated arrival time of the next SU packet, which is predicted by the SVR (Support Vector Regression) method for each channel. The channels with the closest future packet arrivals are assigned to the sniffers. Once the sniffer finds a prediction miss on current channel, it will adhere to explore it and revise the prediction result.

*3) **Performance Metrics:*** Consider the optimal static policy in hindsight as the benchmark or reference, and evaluate the performance of an algorithm using the following two metrics.

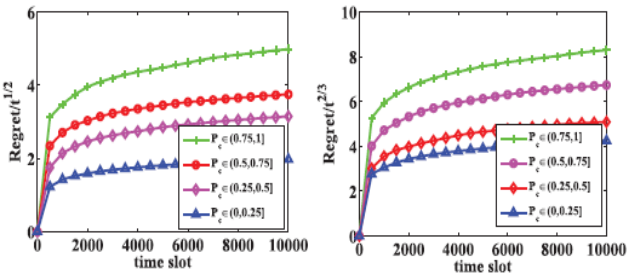
• ***Regret:*** This is the performance metric considered throughout this paper, which is the difference in total rewards between the candidate SCA algorithm and the optimal static policy.

• ***Normalized reward ratio (NRR):*** This is defined as the total rewards achieved by the candidate SCA algorithm. It is normalized by that of the optimal static policy. *NRR* = 1 denotes the rewards of optimal static SCA policy, while *NRR* = 0 is the worst case (i.e., no packet is captured).

B. Regret

In the first group of simulations, we numerically validate the regret bound of Algorithm 1 and Algorithm 2 under various settings. The simulation for each scenario is repeated for 1000 times, and we report the sample means of metrics. The time horizon of the simulation is $T = 104$ slots. Based on the configuration parameters, we classify these experiments into three cases:

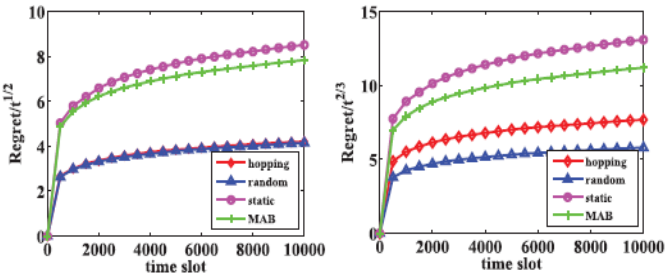
*1) **Varying the Number of Sniffers:*** It investigates the impact of sniffer number on regret bound. Some representative results are provided in Fig. 2. Note that the vertical axis represents the regret divided by different scales (T 1/2 for Algorithm 1 and T 2/3 for Algorithm 2). In each figure, the regrets of two algorithms with various numbers of sniffers are plotted. As shown in both figures, all regret curves tend to flatten over time. This is consistent with Theorem 1 and 2, that is, the upper regret bounds of our proposed policies are polynomial in the number of deployed sniffers.



(a) Algorithm 1 (b) Algorithm 2

Fig 3: Regret of proposed policies with various capture uncertainty ($K = 7$, $S = 3$)

*2) **Varying the Capture Probabilities:*** Studies the impact of capture probabilities on regret bound. Similar as the above simulation setup, the entries of capture probability matrix under certain channel number and sniffer number are randomly generated in the range of (0,0.25], (0.25,0.5], (0.5,0.75], (0.75,1], respectively. One set of representative results ($K = 7$, $S = 3$) is shown in Fig. 3, and it shows the convergency of the proposed algorithms.



(a) Algorithm 1 (b) Algorithm 2

Fig 4: Regret of proposed policies with various capture uncertainty ($K = 6$, $S = 2$)

3) Different Access Patterns: Examines the impact of SU access patterns. Different from the previous setup, we design a simple scenario where all the SUs access the channels following one of the four access patterns (static, hopping, random and MAB). The results are presented in Fig. 4, which validate the effectiveness of the proposed solutions with respect to various access patterns.

© Journal - ICON All Rights Reserved

C. Normalized Reward Ratio

This part, compares the performances of Algorithm 1 and Algorithm 2 with the random and SVR policies in terms of NRR. The simulations are conducted for 1000 runs in the scenario of 10 channels and 4 sniffers. Since the switching costs are not considered in the SVR policy, to compare fairly, we emulate the channel switching costs by a penalty in the calculation of reward, which introduces 20% loss of the captured packets.

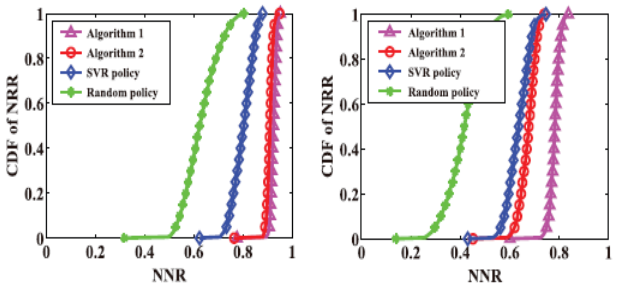


Fig:5 Normalized Reward Ratio

The cumulative distribution function (CDF) of rewards without and with switching costs are shown in Fig. 5(a) and Fig. 5(b), respectively. As shown in Fig. 5(a), when switching costs are not considered, the random and the SVR policies are significantly worse than Algorithm 1 and 2. It is also worth noting that Algorithm 1 performs slightly better between the proposed algorithms. Since Algorithm 2 adopts a relatively conservative manner in updating so as to reduce switching costs, it does not adjust the channel assignments as frequently as Algorithm 1. On the other hand, as can be seen in Fig. 5(b), when switching costs are presented and nontrivial, Algorithm 2 greatly outperforms the others.

VIII. CONCLUSION

This paper studied the sniffer channel assignment problem for data capture in cognitive radio networks. Without the assumption of prior knowledge of the SU behavioral patterns, we formulate the problem as a non-stochastic multi-armed bandit problem. Also, we introduced (time-varying) capture probabilities to model the imperfect monitoring in applications. Moreover, by incorporating channel switching costs, we proposed a family of algorithms using existing online learning techniques, which enjoy an order-optimal sub linear regret in performance. It numerically validated the performance of the proposed solution, and empirically showed that our solution significantly outperforms existing ones. As to the future work, validating the proposed solution on real-world data can be very interesting for applications. Also, the computational complexity of the proposed solution can be non-trivial for very large scale networks, and extending the presented techniques to this case is an ongoing research project.

REFERENCES

[1] Akyildiz,W.-Y. Lee, M. C. Vuran, and S. Mohanty,"A survey on spectrum management in cognitive radio networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 40–48, Apr. 2008.

[2] Baldini, T. Sturman, A. R. Biswas, and R. Leschhorn, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 355–379,May 2012.

[3] Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities
and protection countermeasures: A multi-dimensional analysis and assessment," in Proc. 2nd Int. Conf. CROWNCOM, Orlando, FL, USA, Aug. 2007, pp. 456–464.

[4] Cabric,S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in Proc. 38th Asil. Conf. Signal, Syst. Comput., Pacific Grove, CA, USA, Nov. 2004, pp. 772–776.

[5] Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," IEEE Trans Wireless Commun., vol. 6, no. 2,pp. 649–658, Feb. 2007.

[6] Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in Proc. 28th ICDCS, Beijing, China, Jun. 2008, pp. 19–27

[7] Li, "Cooperative spectrum sensing via belief propagation in spectrum heterogeneous
cognitive radio systems," in Proc. IEEE WCNC, Sydney, N.S.W., Australia, Apr. 2010, pp. 1–6.

[8] Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems part I: Known channel statistics," IEEE Trans. Wireless Commun., vol. 9, no. 11, pp. 3566–3577,Nov. 2010.

[9] Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," IEEE Trans. Wireless Commun., vol. 7, no. 11, pp. 4502–4507, Nov. 2008.

[10] Southwell, J. Huang, and X. Liu, "Spectrum mobility games," in Proc.31st INFOCOM, Orlando, FL, USA, Mar. 2012, pp. 37–45.

© Journal - ICON All Rights Reserved