Quickest Detection of Denial-of-Service Attacks in Cognitive Wireless Networks

CaLynna Sorrells[1] and Lijun Qian[2]

(Corresponding author: Lijun Qian)

Corporate Quality Network, Intel Corporation, Hillsboro, OR 97124, USA[1]
Department of Electrical and Computer Engineering, Prairie View A&M University[2]
Prairie View, TX 77446, USA
(Email: liqian@pvamu.edu)

(Received Aug. 11, 2012; revised and accepted July 17, 2013)

Abstract

Many denial-of-service (DOS) attacks in wireless networks, such as jamming, will cause significant performance degradation to the network and thus need to be detected quickly. This becomes more important in a cognitive wireless network employing dynamic spectrum access (DSA), where it is easier for the attackers to launch DOS attacks. For instance, the attackers may pretend to be a licensed primary user, and carry out the primary user emulation (PUE) attacks. The attackers may also explore the spectrum themselves, and conduct smart jamming. These attacks usually happen at unknown time and are unpredictable due to the lack of prior knowledge of the attackers. It is also observed that the statistical property of the resulted paths from multipath routing will have abrupt change when the attack happens. Hence, in this paper, we formulate the detection of DOS attacks as a quickest detection problem, i.e., detect the abrupt changes in distributions of certain observables at the network layer with minimum detection delay, while maintaining a given low false alarm probability. Specifically, we propose a non-parametric version of the Pages cumulative sum (CUSUM) algorithm to minimize the detection delay so that a network manager may react to the event as soon as possible to mitigate the effect of the attacks. Simulation results using a Spectrum-Aware Split Multipath Routing with dynamic channel assignment as a baseline routing protocol demonstrate the effectiveness of the proposed approach.

Keywords: Cognitive radio, denial-of-service attacks, quickest detection

1 Introduction

Many denial-of-service (DOS) attacks in wireless networks, such as jamming, will cause significant performance degradation to the network and thus need to be detected quickly.

This becomes more important in a cognitive radio (CR) wireless network employing dynamic spectrum access (DSA), where CR users will have the capability to adaptively sense a wide range of frequencies and to opportunistically use the unused spectrum in a heterogeneous environment. This is because it becomes easier for the attackers to launch sophisticated DOS attacks in CR networks. For instance, the attackers may pretend to be a licensed primary user, and carry out the primary user emulation (PUE) attacks [1]. The attackers may also explore the spectrum themselves, and conduct smart jamming [21]. A common characteristic of these attacks is that they cause anomalous spectrum usage and disrupt the dynamic spectrum access, thus we termed them "Anomalous Spectrum Usage Attacks" (ASUAs) in the context of CR wireless networks [18].

In light of the new types of attacks specific to CR networks, we observe that a common characteristic of the attacks in both examples is that they cause Anomalous Spectrum Usage Attacks" (ASUAs) in the context of CR wireless networks. Anomalous Spectrum Usage Attacks are extremely difficult to detect, especially for many mission-critical applications and such as in emergency response where an infrastructure may not exist or function. Denial of Service (DoS) attack is a specific type of ASUA that can cause severe performance degradation in the context of CR networks because of the ability to make the spectrum resource unavailable which can subsequently disable CRs attempting to establish communication with each other. This new type of security attacks in CR is not well researched and should be investigated further if CR technology is to be deployed successfully.

Network intrusions due to ASUAs or DoS attacks happen at an unknown time and are usually unpredictable due to the lack of knowledge of the attackers. It is also observed that the statistical property of a certain random process will have an abrupt change when the attack happens. For example, ASUAs will cause the availability of the spectrum to suddenly decrease. Quickest Detection (QD) has been used to detect distribution changes of a sequence of observations as quickly as possible with the constraint of false alarm or detection probability. Common methods of QD include sequential detection, Bayesian detection, and CUSUM test [13]. In many existing works in the literature, such as [2, 5, 7, 8, 9], quickest detection has been applied to detect emerging primary users (PUs) so that the CR users could vacate the spectrum quickly and avoid harmful interference to the PUs. In this work, we dedicate our effort on a new topic, namely detecting special cases of ASUAs, DoS attacks in CR ad hoc networks.

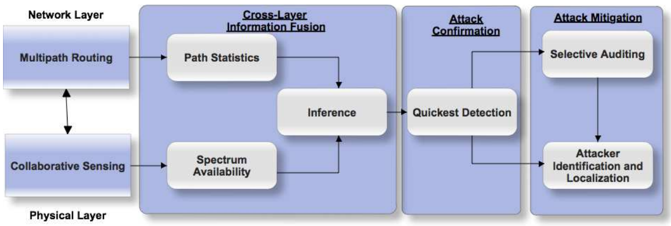

Figure 1: Block diagram of the proposed cross-layer approach for detection of Denial-of-Service Attacks in cognitive radio networks.

In this paper, we are interested in a specific type of smart jamming where the jammer is assumed to have similar capabilities of a CR user, i.e., the jammer is able to monitor the spectrum and observe other users' activities. In addition, a smart jammer only start jamming after a legitimate transmission is detected, and it will stop jamming as soon as the legitimate transmission stops. As a result, its activity will not be picked up by the popular energy detection based spectrum sensing at the physical layer because the smart jammer will stop transmission during the quiet period when the CR users perform spectrum sensing. However, it was shown in our preliminary work that this type of smart jamming will cause change at the network layer, specifically it will cause changes in the distribution of the obtained multiple paths from routing [18]. Hence, in this paper, we formulate a quickest detection problem to catch such smart jammers, i.e., detect the changes in distributions of certain observables at the network layer with minimum delay, while maintaining a given low false alarm probability. Specifically, we employ a Spectrum-Aware Split Multipath Routing (SA-SMR) as a baseline multipath routing protocol to provide necessary network layer observables (obtained multiple paths). According to the obtained paths along time, a non-parametric version of the Page's cumulative sum (CUSUM) test [12] is proposed to detect change in distribution of the obtained paths, subject to a maximum allowable false alarm rate. Then comparing to physical-layer spectrum sensing results, the smart jammer can be identified and located. A block diagram is shown in Figure 1 to illustrate our idea. Extensive simulations have been performed to demonstrate the feasibility of the proposed scheme and the receiver operating characteristic (ROC) curve are plotted to quantify the effectiveness of the proposed method. The tradeoff between the average detection delay and false alarm probability is also shown.

The rest of this paper is organized as follows. The proposed Spectrum-Aware Split Multipath Routing (SA-SMR) is introduced in Section 2. Background on quickest detection is provided in Section 3. The quickest detection problem for jamming attack is formulated in Section 4, with proposed solution. Simulation studies and our findings of these experiments are given in Section 5. Comparisons with existing related works on quickest detection for CR networks are given in Section 6. Section 7 contains the concluding remarks and future work.

2 Spectrum-Aware Split Multipath Routing (SA-SMR)

In a cognitive wireless ad hoc network, the links among CR users may be highly unreliable due to the activities of the PUs. A backup could be set up in the frequency spectrum, say, preparing backup channels for each CR user [10]. When PU emerges, the affected CR user can scan for another idle channel for transmission. However, such an approach may incur significant overhead since finding a new idle channel may be time-consuming. Furthermore, if the PU occupies all available channels, the traffic path will no longer work, thus causing a serious performance degradation. A promising solution would be using multipath routing, where the end-to-end throughput is resilient to the dynamic behavior of the PUs [22]. In addition, multipath routing is an effective solution against jamming attacks [4].

In this section, a novel spectrum-aware multipath routing protocol, Spectrum-Aware Split Multipath Routing (SA-SMR), is introduced as a baseline routing protocol for cognitive wireless ad hoc networks. Routing protocols for cognitive ad hoc networks need to be spectrum aware, such that the performance of such protocols would be robust and efficient in a dynamic spectrum access network [16]. Since the objective here is not designing an optimal routing protocol, but to explore the effects of PUs' activities and spectrum sensing by the CR users on the resulted paths, we use a generic spectrum-aware multipath routing protocol by modifying Split Multi-path Routing [6] with dynamic channel assignment. This protocol serves as a baseline spectrum-aware multipath routing protocol for performance evaluation.

Split Multi-path Routing (SMR), introduced by Lee and Gerla [6], is an on-demand routing protocol that constructs maximally disjoint paths. SMR is based on DSR [3] but uses a different packet forwarding mechanism. While DSR discards duplicate routing request (RREQ), SMR allows intermediate nodes to forward certain duplicate RREQ in order to find more disjoint paths. In SMR, intermediate nodes forward the duplicate RREQ that traversed through a different incoming link than the link from which the first RREQ is received, and whose hop count is not larger than that of the first received RREQ. Here we choose SMR as a starting point because it constructs maximally disjoint paths that provide much needed backup paths in cognitive wireless ad hoc networks where PUs' activities may constantly disrupt CR users' traffic. In order to use SMR in a dynamic spectrum access network, we modify SMR in two respects:

1) Dynamic channel assignment is added since each pair of neighbors along the route must have at least one available (data) channel in common to be used for the data traffic. However, to make the protocol generic and to avoid overhead for complicated distributed scheduling to minimize the intra-flow and inter-flow interferences, we do not optimize the channel assignment procedure and simply let the pair of neighboring nodes to uniformly randomly choose a channel from the set of their common available channels.

2) Two additional fields on channel availability and traffic load (in unit of channel) are added to RREQ.

Note that collecting all the physical layer spectrum sensing results to a central node to perform collaborative spectrum sensing in a large CR ad hoc network requires a lot of overhead, both in terms of sensing a wide spectrum by each individual CR user and the bandwidth and delay incurred by reporting the results to the central node. On the contrary, using multipath routing in a CR ad hoc network covering a large geographical area is necessary to provide robustness and thus quality-of-service to CR users. Hence, the proposed SA-SMR will not incur much overhead (except two additional fields on channel availability and load) if a multipath routing approach is needed and implemented for the robust operation of the network. Furthermore, the information provided by the physical layer spectrum sensing results and from the proposed quickest detection using the resulted paths from multipath routing usually complement each other and it can be used for cross examination to distinguish jammers from legitimate PUs.

3 Background on Quickest Detection

Detecting abrupt changes in a probability distribution of a time series or a stochastic process during data acquisition is referred to as quickest detection. In general, quickest detection can be referred to as statistical change detection, change-point detection or disorder detection. Quickest detection is a well-known approach that dates back to the 1930s in monitoring the quality of manufacturing processes. Quickest detection has recently gained popularity in fields such as econometrics, finance, network security and remote sensing. Quickest detection has to deal with detecting whether or not a change has occurred at an unknown time and determining when that change occurred while maintaining an acceptable probability of false alarm and minimizing the average detection delay. There are two types of quickest detection methods: parametric and nonparametric. Parametric quickest detection occurs when the pre-change and post-change distributions is known beforehand. Nonparametric quickest detection is different in that the distributions are unknown beforehand. In this paper, the pre-change and the post-change distribution is not known beforehand, thus nonparametric quickest detection is applied. In this section, an overview of subcategories of quickest detection is given.

3.1 Sequential Detection Overview

Sequential detection is a classical problem which can be formulated as an optimal stopping problem. The error probabilities are optimized over a fixed decision time which is how this problem becomes an optimal stopping problem. The goal in this formulation is to create an optimal decision rule between two hypothesis (or statistical models) after a minimum average number of experiments. The tradeoff in this method is between the probability of error and the decision time. Intuitively, to obtain more accuracy in a decision, a longer decision time is needed. Conversely, a smaller decision time will lead to a less accurate decision. Performance indices of interest are the probability of error and the decision time which are penalized for optimization purposes. Sequential detection is advantageous in that as soon as a decision is made, the observations stop. An overview of popular sequential detection methods is given in the following sections.

3.1.1 Bayesian Quickest Detection

Kolmogorov and Shiryaev [17] presented the first formal quickest detection method in the early 1960s. This formulation assumes that a prior distribution is known which is given as a geometric distribution. The goal is to detect an abrupt change in distribution along a random sequence of observations as quickly as possible. This approach uses a log-likeliood ratio (LLR) to determine the hypotheses that a change occurred or that no change occurred [19]. Two types of performance indices are of importance in this formulation, the mean delay until detection and the probability of false alarm. The changepoint is decided once the posterior probability crosses a predefined threshold based on current and past observations [13]. There are several approaches to the Bayesian formulation including the Shiryaev problem, the Bojdecki's problem and the Ritov's problem. The disadvantage is that the assumption of a known prior distribution is sometimes unrealistic in a practical scenario.

3.1.2 Non-Bayesian Quickest Detection

Lorden first proposed a non-Bayesian quickest detection approach in which a pre-existing statistical model of the changepoint is given. This type of model is beneficial in scenarios in which the assumption of a known prior distribution is unrealistic is not desired. In this type of scenario, mean detection delay and false alarm probability are not useful since there can be numerous distributions for the observations. Lorden's formulation optimizes the worst case delay and places a constraint of the rate of false alarms. The rate of false alarms is quantified by the mean time between false alarms. A lower bound is placed on the mean time between false alarms to control the false alarms. The disadvantage of this approach is that the pre-change distribution and the post-change distribution should be known beforehand [13].

3.1.3 CUSUM Test

The CUSUM (cumulative sum) test is a sequential analysis technique proposed by E.S. Page [12] and is used to monitor change detection. It is intuitively sequential since analysis is performed as a result of each sum. Thresholding of a statistic, S is sequentially summed until the value S passes a threshold value. Upon the first crossing of this threshold, a stopping time has been reached which infers that a change has occurred. Similar to the Shiryaev test, the CUSUM test also uses the LLR for testing the hypotheses that a change occurred or that a change did not occur. However, the CUSUM does not necessarily require the use of the LLR depending on the application. In this case, an appropriate score function should be selected to replace the LLR. Probability of false alarm and probability of detection are two common performance indices, however the average run length (ARL) time is an additional metric to consider when applying the CUSUM test.

We presented here a general overview of quickest detection. Depending on the application needed change point detection analysis will determine which method of quickest detection that will be applied. We choose to use a nonparametric version of the CUSUM method of quickest detection because it is proven to be optimal when the post distributions are unknown beforehand.

4 Quickest Detection of Smart Jamming

The effect of location-dependent channel availability is significant in a CR ad hoc network which requires multihop communications for traffic sessions. As a result, certain statistics of resulted paths from multipath routing can reveal potential "troubled" areas in the network, which provide ground for further investigation of potential jamming attacks.

4.1 CUSUM Algorithm

In this study, because the prior knowledge of the attack on the network is usually not available, we apply the non-parametric version of the sequential detection algorithm. Let Y_n be a sequence of observations from monitoring the network. Assuming that the probability distribution before change is p_0, and the probability distribution after change is p_1, and the change occurs at an unknown point in time, say at n^*. Thus the conditional probability density function (PDF) before change is $p_0(Y_n|Y_1, Y_2, \cdots, y_{n-1})$ when $n < n^*$, while the conditional PDF after change is $p_1(Y_n|Y_1, Y_2, \cdots, y_{n-1})$ when $n \geq n^*$. Denote the time of detection, i.e., at which point it is declared that a change has occurred, as n_d, then the detection delay is $r = n_d - n^*$. Define two average run lengths (ARL) [13] to measure the performance of the quickest detection as follows

$$\bar{T_1} = ess\ sup\ E_1[r|n_d \geq n^*], \tag{1}$$

$$\bar{T_0} = E_0[n_d], \tag{2}$$

where E_1 denotes the expectation under the assumption that the change happens at time n^*, E_0 is the expectation under the assumption that the change never happens. Note that the esssup in $\bar{T_1}$ means the worst-case delay. For quickest detection, we need to obtain a small $\bar{T_1}$ and a large $\bar{T_0}$.

4.2 Sequential Detection Algorithm

Anomalous Spectrum Usage Attacks (ASUAs) [18] are a subtle type of Denial of Service (DoS) attack that can cause severe damage in CR networks. This characteristic renders these types of attacks difficult to detect. If these types of attacks are not detected quickly, spectrum shortage will result. Thus, quick detection approaches such as sequential detection and batch-sequential detection should be implemented. These types of approaches analyze statistics of a distribution before an attack and after the attack. In order to obtain good performance, an observable needs to be carefully selected such that before an attack, the distribution of the observable remains normal, and an attack will result in sharp change of statistics of the observable with high probability. There are two common approaches used to detect this type of change: sequential detection and batch-sequential detection [19]. Sequential detection is used here, because the statistics of the observations are calculated on-line during data acquisition which is advantageous.

In this work, we propose to use "the frequency of a node (secondary user) appearing in the resulted paths from routing" as a metric to categorize nodes. This is based on our preliminary result [18] that the Probability Mass Function (PMF) of this frequency changes dramatically when under ASUAs. Define N_P as the number of obtained paths, m_i as the number of times that node n_i appearing in those paths, then the percentage of n_i appearing in the resulted paths is given by

$$f_i = \frac{m_i}{N_P}\ . \tag{3}$$

If a node never appear in any path, then $f_i = 0$ for this node. On the contrary, if a node appears in every path, then $f_i = 1$. We use this observable f_i as the metric to put the nodes in different "bins", i.e., according to the percentage of that node appearing in the resulted paths from routing. Suppose there are total B bins, and a node n_i will be put in bin j iff $\underline{b}_j \leq f_i \leq \overline{b}_j$, where $\underline{b}_j$ and $\overline{b}_j$ are the lower and upper bound of bin j, respectively[1], then the percentage of nodes belonging to bin j is given by

$$g_j = \frac{h_j}{\sum_{j=1}^{B} h_j} \ , \tag{4}$$

where h_j represents the number of nodes in bin j.

Ideally, the distribution before attack and after the attack are known a priori and the probability of the log likelihood ratio (LLR) can be used. However, an ASUA occurs at a random time and its effect on the distribution can vary. Thus the distribution after the attack is unpredictable and unknown. Therefore, only the distribution before attack can be assumed as known. Thus, we use a nonparametric approach. Specifically, it is appropriate to use a score function, v instead of using the LLR to detect changes in multiple bins [19]. The size of each bin is generally based on the set of obtained paths. We evaluate the mean value of g_j, $\mu_j = E[g_j]$, in the before and after attack distribution. The score function, v is selected so that it can indicate the changes of μ after an attack. The mean value, $\mu_j = E_0[(A_{1,j}, \cdots, A_{t,j})]$, can be estimated during each t-th time interval, where $A_{t,j}$, is the total percentage of nodes in the t-th time interval in the j-th bin. The score function is defined as:

$$v_j\left(A_{1,j}, \cdots, A_{t,j}\right) = A_{t,j} - \mu_j \ . \tag{5}$$

Once the attack occurs, the CUSUM-type statistic becomes

$$C_{n,j} = \underset{1 \leq n^* \leq n}{max} \sum_{t=n^*}^{n} v_j\left(A_{1,j}, \cdots, A_{t,j}\right) \tag{6}$$

for the j-th bin, where n^* is the change-point. Then the decision rule is

$$\begin{cases} \text{Attack is not presented;} & \text{if } C_{n,j} < \theta \\ \text{Attack is presented;} & \text{if } C_{n,j} \geq \theta \end{cases} , \tag{7}$$

where θ is a pre-determined threshold. θ has to be carefully determined and it will have significant effect on the performance of the QD algorithm, as we will see in the numerical results later. Similarly, which bin should be the observable for QD should be also carefully chosen. Suppose a specific bin is selected, say the jth bin, the declaration time for the jamming attack is obtained by the following stopping rule:

$$\hat{n}_d = \min\{n : \quad C_{n,j} \geq \theta\}. \tag{8}$$

It can be shown that the average detection delay is related to the detection threshold in the following manner

$$E_1[r|n_d \geq n^*] \approx \frac{\theta}{E[v_j]} = \frac{\theta}{E[A_{t,j}] - \mu_j} \tag{9}$$

4.3 Cross-Layer Examination

Recall in Figure 1, a cross-layer examination is needed after the dramatic change in resulted paths from routing is detected in order to distinguish between legitimate PU activities and a smart jammer. The physical-layer spectrum sensing results are obtained from the additional fields on channel availability of the routing requests. The proposed scheme for spectrum congestion detection consists of the following three steps:

1) Perform statistical analysis of the paths/nodes obtained from route discovery using SA-SMR. If anomalous patterns occur, go to the next step. Otherwise, choose several candidate paths and feedback to the source node.

2) Passive checking: Cross check the anomalous pattern in the resulted paths with physical layer spectrum sensing results and the traffic load information, as well as any prior knowledge on PUs from empirical data to detect potential spectrum congestion.

3) Active checking: In order to confirm a spectrum congestion, perform active checking by selectively injecting controlled traffic to the potential congested area and collect measurements such as the packet delivery ratio.

In step 1, exactly how many routes will be chosen for statistical analysis is a design parameter in multi-path routing protocols. It depends on the multi-path data delivery strategy and specific applications, with maximum disjoint paths preferred. The passive checking in step 2 and the active checking in step 3 progressively confirm whether the suspicious area is indeed under spectrum congestion. Since the focus of this paper is on the QD of network layer changes, tests of the cross-layer examination procedures are performed in our future work.

5 Simulation Results and Analysis

In this section, we present the numerical simulations to demonstrate the performance of the proposed scheme. We analyze how parameters such as the detection threshold will impact the average detection delay (ADD), probability of false alarm, and probability of detection. The simulation results are obtained in a 2500mx2500m square area in which there are 10 licensed channels. One PU is present that randomly turns on and transmits on a number of randomly distributed (uniformly from 1 to 10) contiguous channels during an on-period. The PU has a circular interference range of 500m and the SUs located within this area cannot access those channels occupied by the PU. There exists 50 SUs which are randomly deployed in the network in which each user has a sensing range of 300m. The smart jammer is randomly located in the network and has a circular interference range of 300m and occupies *all* of the channels within its range. An example

[1] A node will be put in bin j if $f_i = \overline{b}_j$, or equivalently, we assume that $\underline{b}_{j+1} = \overline{b}_j + \delta$, where δ is infinitesimal.

scenario is shown in Figure 2 in which 68 paths were discovered in the presence of a jammer and a PU. The nodes in the interference range of the jammer do not have any available channels to use since the jammer uses all of the channels. However, some paths are created within the interference range of the PU because there are still a few channels available.

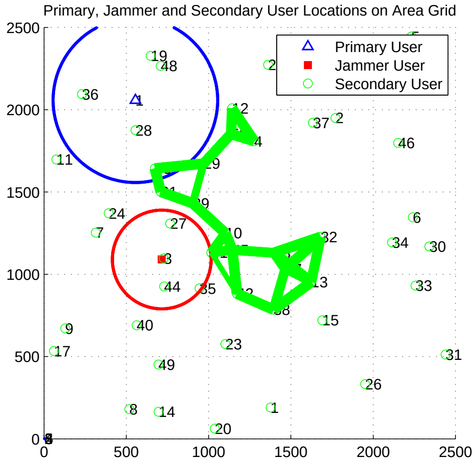

Figure 2: Typical routing result from node 12 to node 47.

We created 200 time series of routing events, with each series containing 20 time slots. During each time slot, a source-destination pair is randomly selected and Spectrum-Aware Split Multipath Routing (SA-SMR, see Section 2) is used to obtain the paths. We select the bins according to a 10% interval, i.e., $\overline{b}_j - \underline{b}_j = 10\%$, for $j = 1, \cdots, 12$. For instance, a node n_i never appear in any path ($f_i = 0$) belongs to bin1, a node appears in 8% of the paths belongs to bin2, while a node contained in every path ($f_i = 1$) is in bin12. We are particularly interested in the statistics of bin1 and bin12, because an attack would push more nodes to these 2 bins. In other words, under an Anomalous Spectrum Usage Attack, the nodes under the influence of the attacker would not participate in the routing process, thus they belong to bin1; similarly, the attack will also create choking point such that it will force many paths go through the same nodes, thus increase the number of nodes in bin12. Hence, we choose bin12 in this simulation study.

In the following experiments, we assume that we have no knowledge whether the PU is on or off when performing QD. As a result, the mean before an attack, μ_j, is estimated using mixed cases with half with PU on and half with PU off. In order to examine the effect of the threshold value for QD, we vary the threshold value from 0.1 to 0.5 and plot the probability of false alarm in Figure 3 and the average detection delay in Figure 4, respectively. It is observed that the average detection delay increases, while the probability of false alarm decreases, when the detection threshold increasing, as expected.

The results show that when the detection threshold equals to 0.5, there will be very few false alarm, but the average detection delay would be more than 5 time units. The tradeoff between the probability of false alarm and the average detection delay can be observed in Figure 5. A good compromise would be setting the detection threshold to 0.3, where the probability of false alarm is less than 2% (with PU off) and less than 7% (with PU on), while the average detection delay is merely 3.25 time units.

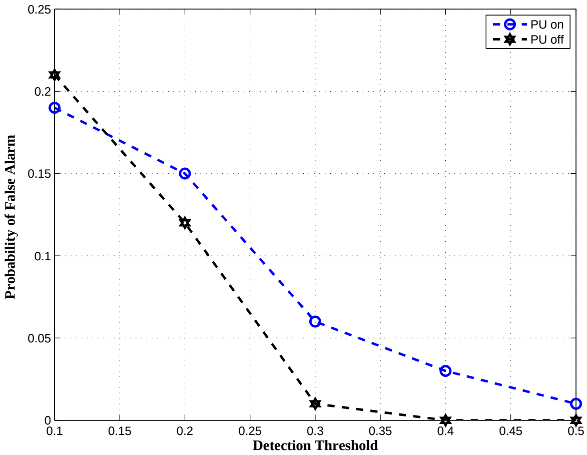

Figure 3: Probability of false alarm vs. the threshold values.

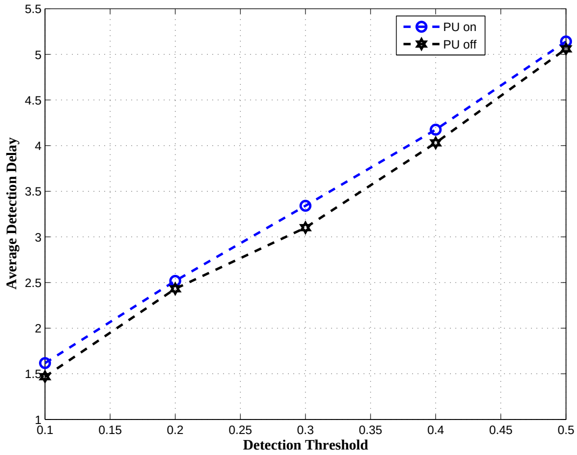

Figure 4: Average detection delay vs. the threshold values.

It is also observed that with PU on, both the probability of false alarm and the average detection delay increase, due to the fact that PU will occupy certain number of channels that would affect the routing of the SUs. However, it is interesting to notice that when the PUs behave inherently different from the smart jammers, such as a PU usually does not occupy all the available channels and block all the routing requests from its transmission range, then the proposed QD algorithm performs very well at identifying the smart jammers from legitimate PUs. Indeed, under the current parameter setting, the probability of false alarm and the average detection delay only increase slightly when the PU is on. Of course, if the PU would occupy all channels and block all the SU's paths in its interference range, we cannot make decisions based solely on QD using obtained paths, and cross-layer examination becomes necessary (see Section 4.3).

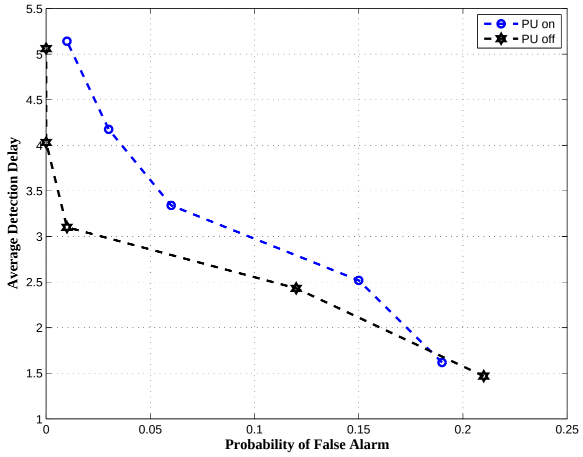

Figure 5: Average detection delay vs. the probability of false alarm.

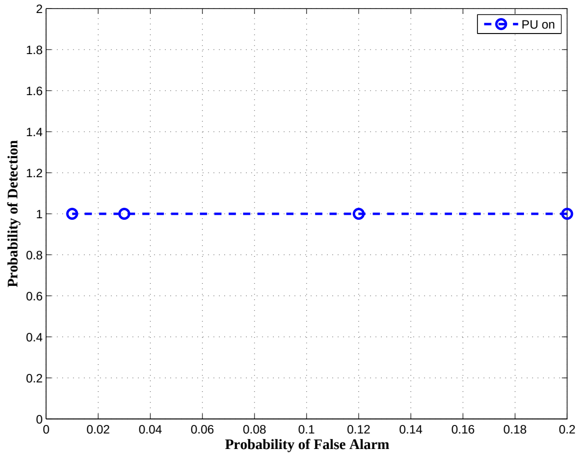

Figure 6: ROC curve when PU is on.

Under the current parameter setting, we do not have any miss during the detection process. In other words, the ROC curve is flat, see Figure 6. This is due to the ideal assumption that the destination node would be able to collect all the paths, thus the waiting time is long. In realistic implementation, the destination may only wait for a limited amount of time and only obtain a portion of the paths. It would be interesting to investigate how that would affect the ROC curve and this is one of our future works.

6 Related Works and Disucssions

6.1 Quickest Detection in Cognitive Radio Networks

In [9], quickest spectrum sensing is used to detect the change in frequency distribution by employing a successive refinement algorithm which combines generalized likelihood ratio (GLR) and the parallel CUSUM test. It is shown that most secondary nodes achieve good performance (1.5%) while a small portion of nodes perform much worse (3.5%) due to bad signal-to-noise ratio.

A sequential change detection framework was presented [5] to characterize the detection delay of certain detection algorithms. Detection schemes that minimize the detection delay while maintaining false alarm at a given level were developed.

The collaborative quickest detection approach proposed in [8] is based on a threshold broadcast scheme. This scheme is employed without a centralized coordinating entity and the local observations are broadcast in a random time slot. It is demonstrated that the proposed threshold broadcast scheme can achieve substantial performance gain (less than 60% in detection delay for the same false alarm rate) over schemes of random broadcast without regulation and single-user spectrum sensing.

The authors in [2] combine the Hidden Markov Model (HMM) and quickest detection for spectrum detection. Spectrum recognition is achieved via frequency sweeping in which samples of the power spectral density become the input for the HMM and forward variables derived from the HMM are sequentially observed to create the decision statistic.

Quickest Detection has been also applied to spectrum detection in CR networks employing cyclostationary feature detection [7]. A multi-thread competition based algorithm was applied which indicates a change when a thread reaches a limit in the cyclic structure. Thread truncation was used minimize the computational cost.

It is clear from the reviews and discussions that the existing works of quickest detection in cognitive radio network context are focusing on detection of abrupt changes in distribution of spectrum usage, while the proposed work applied quickest detection for Denial-of-Service attacks by detecting abrupt changes in statistics of routing paths. The authors believe that this is the first of such work that applying quickest detection for identifying Denial-of-Service attacks in cognitive radio networks.

6.2 Anomaly Detection in Computer Networks and Sensor Networks

It is noticeable that quickest detection methods have been used for anomaly and attack detection in computer networks and distributed sensor networks, such as in [11, 14, 15, 19, 20], just to name a few. Adaptive sequential and batch-sequential methods are used in [19] for an early detection of attacks in computer networks that lead to changes in network traffic, such as denial-of-service attacks, worm-based attacks, portscanning, and man-in-the-middle attacks. These methods employ a statistical analysis of data from multiple layers of the network protocol to detect very subtle traffic changes. Results of the experimental study with a network simulator testbed as well as real-life testing for TCP SYN flooding attacks show the effectiveness of the methods.

In [20], a decentralized formulation of the quickest detection problem is studied, where the distributions of the observations at all of the sensors in the system change at the time of disruption, and the sensors communicate with a common fusion center. An optimal solution to the problem is derived when a priori knowledge of the change time distribution is available. It is further relaxed to include the case where this information is not known.

Quickest change detection in the multisensor setting where the change propagates across the sensors was considered in [15]. A dynamic programming framework was proposed and an optimal stopping rule was derived. Under a certain condition on the Kullback-Leibler (K-L) divergence between the post- and the pre-change densities, it is established in [15] that the threshold test is asymptotically optimal.

In [11], the quickest detection problem was studied in a general context of monitoring a large number of data streams in sensor networks when the trigger event may affect different sensors differently. Motivated by censoring sensor networks, scalable detection schemes were developed based on the sum of those local CUSUM statistics that are large under either hard thresholding or top-r thresholding rules or both. The proposed schemes are shown to possess certain asymptotic optimality properties.

A sleep/wake scheduling algorithm is proposed in [14] for quickest detection of an intrusion using a sensor network, while keeping only a minimal number of sensors active to maximize energy efficiency. The intrusion detection problem was modeled as a Markov decision process (MDP).

In this paper, we adopted a non-parametric version of the cumulative sum (CUSUM) method. The challenge is to find an appropriate statistical metric and the corresponding score function that can capture the Denial-of-Service attacks in cognitive radio networks due to smart jamming. As a result, the focus of this paper is on applying quickest detection method to identify Denial-of-Service attacks in cognitive radio networks by developing an appropriate non-parametric version of the cumulative sum (CUSUM) method, rather than trying to invent a new quickest detection method.

7 Conclusions and Future Work

In this paper, we proposed a non-parametric version of the Pages cumulative sum (CUSUM) algorithm to detect spectrum congestion in cognitive wireless ad hoc networks. Placing within a cross-layer framework, the proposed algorithm is capable of detecting DOS attacks with minimum delay while maintaining desired false alarm rate. It is demonstrated that as long as the primary users will not occupy all channels and aggressively block all the routing packets of the SU, i.e., primary user behaves differently from the jammers, then the proposed quickest detection algorithm is rather robust whether primary user is on or off. It worth pointing out that the aim of the proposed Spectrum-Aware Split Multipath Routing (SA-SMR) is *not* to optimize a routing protocol, but simply use it as a base-line routing protocol, and a vehicle to carry critical information, both spectrum sensing information and traffic load information, to fulfill the needs for cross-layer detection. Since the focus of this paper is on the quickest detection of network layer changes, tests of the cross-layer examination procedures are not performed, and this is one of our future research topics.

Acknowledgments

The first author is supported by the HBGI Scholarship. This research work is supported in part by NSF under CNS-1040207 and the US Army Research Office under Cooperative Agreement W911NF-12-1-0054.

References

[1] R. Chen, J. M. Park, and J. H. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25–37, Jan. 2008.

[2] Z. Chen, Z. Hu, and R. C. Qiu, “Quickest spectrum detection using hidden markov model for cognitive radio,” in *Proceedings of IEEE Military Communications Conference*, pp. 1–7, Oct. 2009.

[3] D. Johnson, Y. Hu, and D. Maltz. “The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4,”. in *RFC 4728*. IETF, 2007.

[4] M. Kim and K. Chae, “Dmp: Detouring using multiple paths against jamming attack for ubiquitous networking system,” *Sensors*, vol. 10, no. 4, pp. 3626–3640, 2010.

[5] L. Lai, Y. Fan, and H. V. Poor, “Quickest detection in cognitive radio: A sequential change detection framework,” in *Proceedings of IEEE Global Telecommunications Conference*, pp. 1–5, Dec. 2008.

[6] S. Lee and M. Gerla, “Split multipath routing with maximally disjoint paths in ad hoc networks,” in *Proceeding of IEEE ICC*, pp. 3201–3205, 2001.

[7] H. Li, “Cyclostationary feature based quickest spectrum sensing in cognitive radio systems,” in *Proceedings of IEEE 72nd Vehicular Technology Conference Fall (VTC 2010-Fall)*, pp. 1 –5, Sep. 2010.

[8] H. Li, H. Dai, and C. Li, “Collaborative quickest spectrum sensing via random broadcast in cognitive radio systems,” in *Proceedings of IEEE Global Telecommunications Conference*, pp. 1–6, Dec. 2009.

[9] H. Li, C. Li, and H. Dai, "Quickest spectrum sensing in cognitive radio," in *Proceedings of 42nd Annual Conference on Information Sciences and Systems*, pp. 203–208, Mar. 2008.

[10] H. Li and L. Qian, "Enhancing the reliability of cognitive radio networks via channel assignment: Risk analysis and redundancy allocation," in *Proceedings of 44th Annual Conference on Information Sciences and Systems*, 2010.

[11] Y. Mei, "Quickest detection in censoring sensor networks," in *Proceedings of IEEE International Symposium onInformation Theory Proceedings (ISIT)*, pp. 2148–2152, 2011.

[12] E. Page, "Continuous inspection schemes," *Biometrika*, vol. 41, pp. 100–115, Jun. 1954.

[13] V. Poor and O. Hadjiliadis, *Quickest Detection*. Cambridge University Press, 2009.

[14] K. Premkumar and A. Kumar, "Optimal sleep-wake scheduling for quickest intrusion detection using wireless sensor networks," in *Proceedings of IEEE INFOCOM*, pp. 1400–1408, 2008.

[15] V. Raghavan and V. V. Veeravalli, "Quickest change detection of a markov process across a sensor array," *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1961–1981, 2010.

[16] A. Sampath, L. Yang, L. Cao, H. Zheng, and B. Y. Zhao, "High throughput spectrum-aware routing for cognitive radio networks," 2010.

[17] A. N. Shiryaev, "On optimum methods in quickest detection problems," *Theory of Probability and its Applications*, no. 1, pp. 22–46.

[18] C. Sorrells, P. Potier, L. Qian, and X. Li, "Anomalous spectrum usage attack detection in cognitive radio wireless networks," in *Proceedings of IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 384–389, Nov. 2011.

[19] A. G. Tartakovsky, B. L. Rozovskii, R. B. Blazek, and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods," *IEEE Transactions on Signal Processing*, vol. 54, pp. 3372–3382, Sep. 2006.

[20] V. V. Veeravalli, "Decentralized quickest change detection," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1657–1665, 2001.

[21] L. Wang and A. M. Wyglinski, "A combined approach for distinguishing different types of jamming attacks against wireless networks," in *Proceedings of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PacRim)*, pp. 809–814, Aug. 2011.

[22] X. Wang, T. T. Kwon, and Y. Choi, "A multipath routing and spectrum access (mrsa) framework for cognitive radio systems in multi-radio mesh networks," in *Proceedings of the 2009 ACM workshop on Cognitive radio networks*, pp. 55–60, New York, NY, USA, 2009.

CaLynna Sorrells obtained her PhD in Electrical Engineering from Prairie View A&M University in Prairie View, Texas in 2012. Her research is on The Detection and Mitigation of Security Attacks in Cognitive Radio Ad Hoc Networks. She obtained her MS and BS from Tuskegee University in Tuskegee, AL in Electrical Engineering. Her thesis was on Call Admission Control (CAC) in mobile ad hoc networks. She has held several internships and research assistantships in the Army Research Laboratory (ARL) spanning security threats, vulnerabilities and risks in mobile ad hoc networks. She is now a component design engineer for the Intel Corporation in Hillsboro, OR in the Corporate Quality Network (CQN), where she drives new methodologies and quality system solutions for Security Quality and performs RF Modeling for performance and quality optimizations. Her research interests include cognitive radio ad hoc networks and network security.

Lijun Qian received BS degree from Tsinghua University, Beijing, China, in 1993, MS from Technion-Israel Institute of Technology, Haifa, Israel, in 1996, and PhD from Rutgers University, NJ, USA, in 2001. He is currently an Associate Professor in the Department of Electrical and Computer Engineering at Prairie View A&M University (PVAMU), a member of the Texas A&M University System. He is also the director of the Wireless Communications Lab (WiComLab). Dr. Qian's research is supported by the US National Science Foundation (NSF) and the US Army Research Office (ARO), and he is the recipient of the NSF Research Initiation Award in 2012. Before joining PVAMU, he was a MTS in the Networks and Systems Research Department of Bell-Labs at Murray Hill, NJ. He is a visiting professor at Aalto University, Finland. His research interests are wireless communications and mobile networks, network security, and systems biology.