Anomaly Spectrum Usage Detection in Multihop Cognitive Radio Networks: A Cross-Layer Approach

Lijun Qian[1], Xiangfang Li[2], and Shuangqing Wei[3]
[1] Department of Electrical and Computer Engineering, Prairie View A&M University, Prairie View, Texas 77446, USA
[2] Department of Electrical and Computer Engineering, Texas A&M University, College Station, Texas 77843, USA
[3] Department of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA 70803, USA
Email: liqian@pvamu.edu, xiangfangli@ieee.org, swei@ece.lsu.edu

Abstract — **The introduction of cognitive radio enables system's awareness of their environment and internal state, fulfills the need of dynamic spectrum access for higher spectrum utilization. However, at the same time, the use of cognitive radios further complicates the security problems in wireless networks and introduces additional challenges for a counter measure. Due to the intelligence of the attackers, many of the attacks may be stealthy by nature, such as the anomalous spectrum usage attacks, which usually cannot be detected only using information from one layer of the protocol stack. In this paper, we propose a cross-layer model for anomalous spectrum usage attacks detection with stealthy jammer as a prime example. Quickest detection technique is adopted and embedded in the proposed framework since the attacks usually happen at unknown time and are unpredictable due to the lack of prior knowledge of the attackers. A case study is performed by combining physical layer spectrum sensing with multipath routing at the network layer. The results demonstrate the effectiveness of the proposed approach.**

Index Terms—**cognitive radio, anomaly detection, cross-layer**

I. Introduction

Radio spectrum is a very valuable resource and it has been determined that allocated spectrum bands are sometimes lightly used. With the increase of traffic demands in wireless communication systems and the shortage of available spectrum below 3GHz, Cognitive Radio (CR) [1] based on Software-defined Radio (SDR) is developed in recent years as the enabling technology for dynamic spectrum access, which is a promising scheme for improving spectrum utilization. From the policy side, as the proliferation of wireless devices have crowded the unlicensed spectrum bands, regulatory bodies such as the U.S. Federal Communications Commission (FCC) have begun to open additional bands for use by unlicensed devices. Many emerging standards such as the IEEE 802.22 [2] and the IEEE 802.11af [3] help transfer cognitive radio research to practical implementation.

While cognitive radio introduces more flexibility of using the spectrum and optimizing the efficiency for coexistence of multiple radio systems, it also introduces many new challenges in network security. Specifically, because the capability of sensing and exploring a wide range of frequencies and opportunistic usage of spectrum become common in cognitive radio networks, it is easier for the attackers to launch sophisticated attacks in such networks. For instance, the attackers may pretend to be a licensed primary user, and carry out the primary user emulation (PUE) attacks [4]. The attackers may also explore the spectrum themselves, and conduct smart jamming [5], [6]. 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 cognitive radio networks [7].

Because of the "stealthy" nature of anomalous spectrum usage attacks, detection of such attacks often requires advanced methods that leverage on information from multiple layers of the protocol stack. For example, in the case of PUE attacks, a recent study show that comparing clustered information from spectrum sensing at the physical layer and MAC addresses can identify the attacker [8]. If location information is used for detection of PUE attacks, then topology control information from the MAC layer is useful, although localization using Received Signal Strength (RSS) may be difficult in reality due to the volatility of RSS.

Another prime example is stealthy jamming attacks. In this case, the jammer is assumed to have similar capabilities of a CR user and it is able to monitor the spectrum and observe other users' activities. A stealthy jammer only start jamming after a legitimate transmission is detected, and it will stop jamming as soon as the legitimate transmission stops. In most spectrum sensing algorithms, the CRs will sense the spectrum during a quiet period [9], i.e., the CRs do not transmit during spectrum sensing. As a result, the jamming activities will not be picked up by the popular spectrum sensing methods such as energy detection at the physical layer because the stealthy jammer will be silent during the spectrum sensing. However, it was shown in our preliminary work that this type of jamming will cause change at the network layer, specifically it will cause changes in the distribution of the obtained multiple paths from routing [7]. If the stealthy jammer targets channels selectively, say the common control channel (CCC), it is even harder to detect using only information at the physical layer,

Manuscript received March 15, 2013; revised April 7, 2013; accepted April 18, 2013.
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. An earlier version of this paper was published in ICNC 2013.
doi:10.12720/jcm. 8.4.259-266

but with collision monitoring at the MAC layer, a strong RSS and high collision rate indicate a potentially jammed CCC.

Based on the above discussions, we propose a cross-layer approach to detect anomalous spectrum usage attacks in cognitive radio networks. We firstly provide a general framework, with detailed guideline on how to apply this framework to PUE attacks and stealthy jammers. Since the PUE attack has been studied extensively, e.g., see [10] for a survey, we concentrate our attention to other anomalous spectrum usage attacks such as stealthy jammers, and provide a detailed case study. Stealthy jammer can be considered as an intelligent reactive jammer [6]. It is shown in [11] that single type of measurements fail to detect such jammers, and thus two consistency checks were proposed. The attacks by stealthy jammers can become more sophisticated in cognitive radio networks, and further improvement on detection technique is desired.

In this paper, a general framework is firstly introduced in Section II. Then a case study for detection of stealth jammers is examined in detail in Section III. Related works are discussed in Section IV. Section V contains the concluding remarks.

II. Framework

In this section, we firstly specify the model of the cognitive radio network and the attacker. Then the cross-layer detection framework is illustrated.

A. Model

In this study, we consider a cognitive radio network covering a large geographical area such that the spectrum availability is location dependent[1]. Each CR user i has an average transmission range of r_i^{tx} and an average detection range of r_i^d, and $r_i^d > r_i^{tx}$. These ranges depend on the path loss and shadow factor. The CR users rely on multi-hop paths for communications. It is assumed that the topology of the CR network would not change dramatically during one routing cycle or one data transport session. This assumption covers many important real world applications, such as fixed wireless networks, or network with low mobility or group mobility. It is assumed that the attacker has similar capability of the CR users, i.e., the attacker has similar transmission range and power as the CR users and it is able to monitor the spectrum and observe other users' activities. Only anomalous spectrum usage attacks are considered in this work, other attacks not specific to CR networks such as eavesdropping and traditional routing attacks are out of the scope of this paper. An example of the multi-hop CR network under stealthy jamming is shown in Fig.1, where node S and D are the source and destination, respectively, and primary users are not drawn for simplicity of presentation. Suppose the stealthy jammer is intelligent and selectively jam important packets such as the routing packets, the resulted paths will be affected dramatically.

[1]The case where all CR users have the same spectrum situation is a special case of the proposed model.

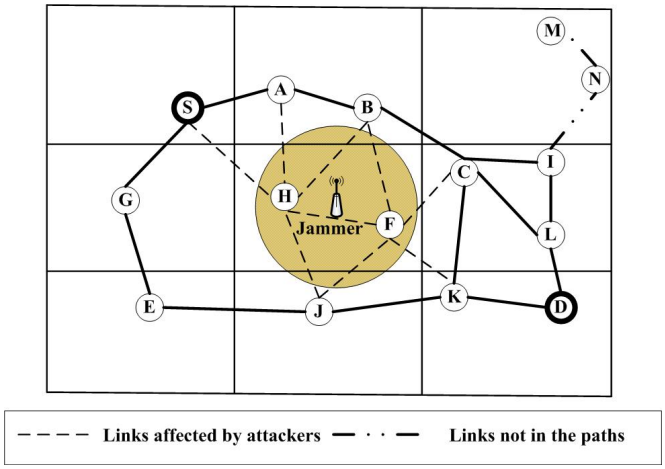

Figure. 1. An example of the multi-hop CR network under stealthy jamming.

B. Information Acquisition

It is assumed that the CR nodes perform periodic spectrum sensing. There exist many algorithms for spectrum sensing and the proposed method does not require any specific algorithm to be used by the CR nodes. Each CR node determine whether there is enough channel available for the traffic demand based on its perceived spectrum situation. As the spectrum availability is location dependent, the coverage of the network is assumed to contain G areas with at least one CR node in each area. For instance, there are 9 areas in Fig.1. A MAC layer module may keep monitoring the collision rate for each area. However, due to hardware limitations, each node can only monitor one channel at any given time. Similarly, the packet delivery ratio (PDR) can also be monitored at each node.

Although many studies proposed to use various information from multiple layers and from different users/nodes in the network, the proper method for collecting those information is not discussed. Note that collecting all the physical layer spectrum sensing results to a central node to perform collaborative spectrum sensing in a large multi-hop CR 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 multi-hop CR network covering a large geographical area is necessary to provide robustness and thus quality-of-service to CR users, where the end-to-end throughput is resilient to the dynamic behavior of the PUs [12]. Hence, an information collection mechanism is proposed here using Spectrum-Aware Split Multipath Routing (SA-SMR) [7] as a delivery vehicle for the purpose of data collection.

It is beneficial in cognitive radio networks since routing redundancy is desired to provide robustness against dynamic interruption from PUs. The proposed SA-SMR will not incur much overhead (except two additional fields on channel availability and load). 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.

C. Cross-layer Detection

The goal of this work is to lay out the framework for the detection of Anomalous Spectrum Usage Attacks in cognitive radio networks using a cross-layer approach. A three-step procedure is proposed. In step 1, after information from multiple layers is gathered, statistical analysis is performed. Then a discrepancy search is carried out to identify potential "troubles" in step 2, where results from multiple layers are compared, and potential attacks are identified. Based on the findings in step 2, further checking may be needed in step 3 to conclude a specific attack based on additional characteristics of the attack.

A flow chart of the proposed cross-layer detection procedure is given in Fig. 2. Only Spectrum sensing and routing modules are drawn for simplicity. This can be extended to include modules from other layers.

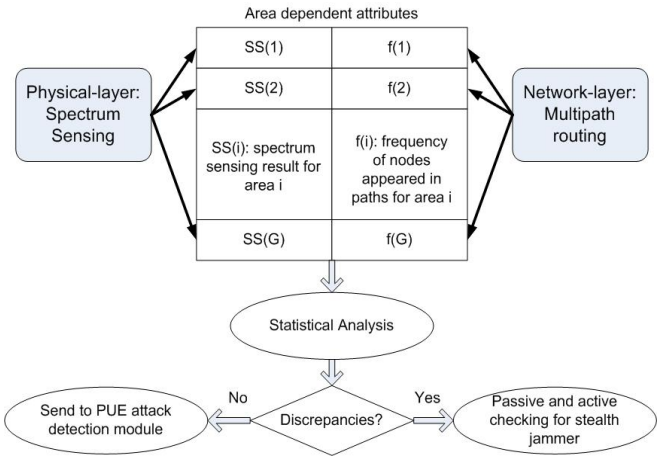

Figure. 2. Flow chart ofcross-layerdetection.

As an example, during a stealthy jamming attack, $SS(i)$ at the physical layer may report no spectrum activities in area i the whole time, while the $f(i)$ from the routing module at the network layer may experience significant change during consecutive routing events. Thus, after collecting all the information and obtaining statistics in the first step, it is suspected that there may be a stealthy jammer in area i by performing discrepancy search in the second step. Then an audit may be placed in area i in the third step, for instance, monitoring the packet drop rate at the MAC layer in area i.

For PUE attacks, information from other layers, such as the MAC layer, may be collected during step 1. In addition, specific audit of the suspected area may be performed by selectively injecting controlled interference to the potential attacker and subsequently observing its reaction. For many legitimate PUs, such as a cellular system, closed-loop power control is implemented for ensured quality-of-service. When the interference level is up due to the injected transmissions, the PU receiver would experience lower signal-to-interference-plus-noise ratio (SINR) and feedback this information to the PU transmitter. Then the PU transmitter would increase its transmission power to compensate for the interference. On the contrary, a PUE attacker would not have a corresponding receiver and thus would not respond to the interfering signal the same way as the legitimate PU does. There may be cases where the PU system is a broadcasting system and does not have the closed-loop mechanism, such as in TV systems. However, in those cases, the data of location, transmission power and effective receiving range of TV stations are publicly available.

With the general framework outlined, the details of statistical analysis are given below, and the emphasis is on statistical analysis using time series data.

1) Statistical analysis using snapshot data: When only snapshot of data available from the physical layer and the network layer, simple statistical measures can be used to determine whether there exists discrepancies among the data from different layers. As an example, if the physical layer report abundant amount of available channels in an area, yet the nodes within that area hardly appear in the resulted paths, then a potential jamming may occur. However, this may be due to other reasons such as the area is not on the path of the source destination pair, such as nodes M and N in Fig.1. Since only snapshot data is available, this detection may have high false alarm rate because lack of comparison to historic data. Thus, we focus on the case where time series data is used for statistical analysis.

2) Statistical analysis using time series data: Contrary to the static case, here we take advantage of the time series measurements of certain observables from multiple layers. This is motivated by the fact that the probability distribution of appropriately chosen observables will change when attack happens. Since the time of the attacks are unpredictable, we may apply quickest detection methods [13] to detect the changes in distributions of certain observables at each layer of the protocol stack. The proposed multi-layer quickest detection will minimize the average detection delay while maintaining acceptable false alarm probability.

It is assumed that the data from different layers are mutually independent. However, the observations in each layer are not i.i.d. before and after the change. Let Y_n^i be a sequence of observations from the i^{th} layer. Assuming that the probability distribution before change is p_0^i, and the probability distribution after change is p_1^i, and the change occurs at an unknown point in time, say at n^{i*}. Thus the conditional probability density function (PDF) before change (Hypothesis 0, H_0^i) is $p_0^i(Y_n^i|Y_1^i, Y_2^i, \cdots, y_{n-1}^i)$ when $n < n^{i*}$, while the conditional PDF after change (Hypothesis 1, H_1^i) is $p_1^i(Y_n^i|Y_1^i, Y_2^i, \cdots, y_{n-1}^i)$ when $n \geq n^{i*}$. Then the log-likelihood ratio (LLR) is given by

$$Z^i(n^{i*}, T) = \sum_{n=n^{i*}}^{T} \frac{p_1^i(Y_n^i|Y_1^i, Y_2^i, \cdots, y_{n-1}^i)}{p_0^i(Y_n^i|Y_1^i, Y_2^i, \cdots, y_{n-1}^i)}. \quad (1)$$

If the Page's cumulative sum (CUSUM) test [14] is adopted, the following iteration can be used for statistics $U^i(T) = max_{0 \leq n^{i*} \leq T} Z^i(n^{i*}, T)$,

$$U^i(T) = max\left\{0, U^i(T-1) + Z^i(T,T)\right\}, \quad (2)$$

with initial condition $U^i(0) = 0$. Denote the time of detection, i.e., at which point it is declared that a change has occurred,

as n_d^i, which is given by

$$n_d^i = \inf\left\{T \geq 1:\ U^i(T) \geq \theta^i\right\}, \tag{3}$$

where θ^i is a pre-determined threshold and has to be carefully chosen. It will have significant effect on the performance of the algorithm, as we will see in the case study later. Then the detection delay is $r^i = n_d^i - n^{i*}$. Define two average run lengths (ARL) [13] to measure the performance of the quickest detection as follows

$$\bar{D_1^i} = ess\ sup\ E_1^i[r^i | n_d^i \geq n^{i*}], \tag{4}$$

$$\bar{D_0^i} = E_0^i[n_d^i], \tag{5}$$

where E_1^i denotes the expectation under the assumption that the change happens at time n^{i*}, E_0^i is the expectation under the assumption that the change never happens. Note that the esssup in $\bar{D_1^i}$ means the worst-case delay. For quickest detection, we need to obtain a small $\bar{D_1^i}$ and a large D_0^i. Note that when the statistical knowledge of the observables prior to and after the attack on the network is not available, or very hard to estimate, non-parametric version of the sequential detection algorithm is suggested. When the detection from multiple layers are collaborative, then the detection can happen at

$$n_d = \inf\left\{T \geq 1:\ \max_i U^i(T) \geq \theta^i\right\}. \tag{6}$$

III. Case study: Joint physical and network layer quickest detection of stealthy jammer

In this case study, we apply the proposed cross-layer framework to detect stealthy jammers in a multi-hop CR network by leveraging information from physical layer spectrum sensing results and the obtained paths from routing. We formulate a quickest detection problem to catch such smart jammers. Specifically, according to the obtained paths from multipath routing along time, a non-parametric version of the Page's cumulative sum (CUSUM) test [14] 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. Quickest Detection Algorithm

The effect of location-dependent channel availability is significant in a multi-hop CR network which requires multi-hop 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 cross-layer examination. 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 [15]. 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 [7] 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

$$f_i = \frac{m_i}{N_P}\ . \tag{7}$$

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 $\underline{b}_j \leq f_i \leq \bar{b}_j$, where $\underline{b}_j$ and $\bar{b}_j$ are the lower and upper bound of bin j, respectively[2], then the percentage of nodes belonging to bin j is given by

$$g_j = \frac{h_j}{\sum_{j=1}^{B} h_j}\ , \tag{8}$$

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 [15]. 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:

$$v_j\left(A_{1,j}, \cdots, A_{t,j}\right) = A_{t,j} - \mu_j\ . \tag{9}$$

Once the attack occurs, the CUSUM-type statistic becomes

$$C_{n,j} = \underset{1 \leq n^* \leq n}{max} \sum_{t=n^*}^{n} v_j\left(A_{1,j}, \cdots, A_{t,j}\right) \tag{10}$$

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

$$\begin{cases} \text{Attack is not presented;} & \text{if } C_{n,j} < \theta \\ \text{Attack is presented;} & \text{if } C_{n,j} \geq \theta \end{cases}, \tag{11}$$

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

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

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:

$$\hat{n}_d = \min\{n : \quad C_{n,j} \geq \theta\}. \tag{12}$$

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

$$E_1[r|n_d \geq n^*] \approx \frac{\theta}{E[v_j]} = \frac{\theta}{E[A_{t,j}] - \mu_j} \tag{13}$$

B. 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. It is assumed the jammer will block all routing packets.

An example scenario is shown in Fig. 3 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.

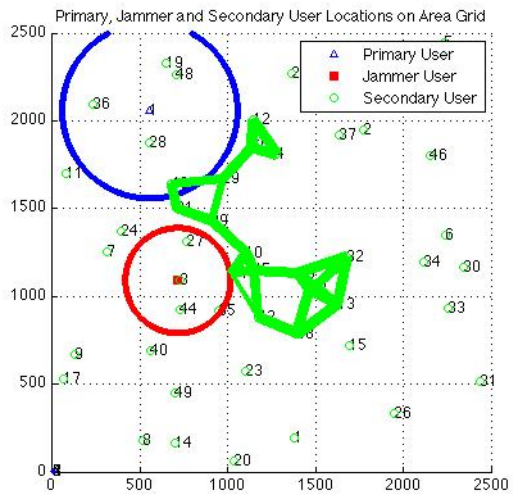

Figure. 3. Typical routing result from node 12 to node 47.

We created 200 time series of routing events, with each series containing 20 time intervals. During each time interval, a source-destination pair is randomly selected and Spectrum-Aware Split Multipath Routing is used to obtain the paths. We select the bins according to a 10% spacing, i.e., $\bar{b}_j - \underline{b}_j = 10\%$, 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.

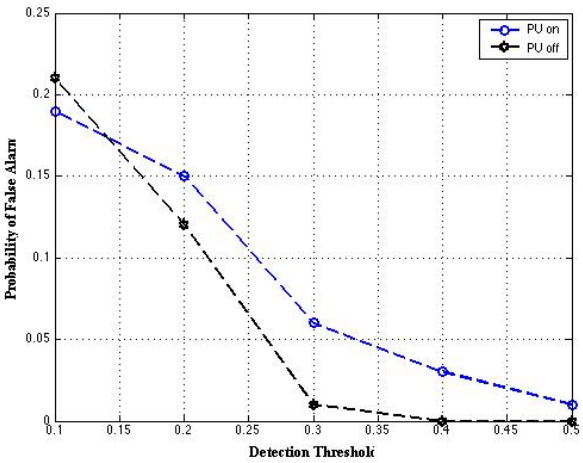

Figure. 4. Probability of false alarm vs. the threshold values.

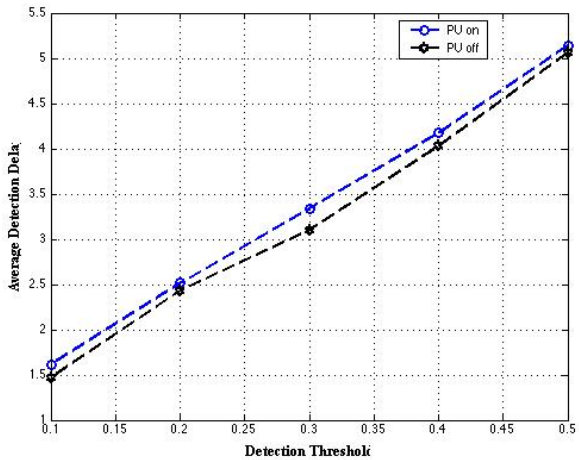

Figure. 5. Average detection delay vs. the threshold values.

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.

We plot the probability of false alarm in Fig. 4 and the average detection delay in Fig. 5, 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 intervals.

The tradeoff between the probability of false alarm and the average detection delay can be observed in Fig. 6. 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 intervals. It is also observed that with

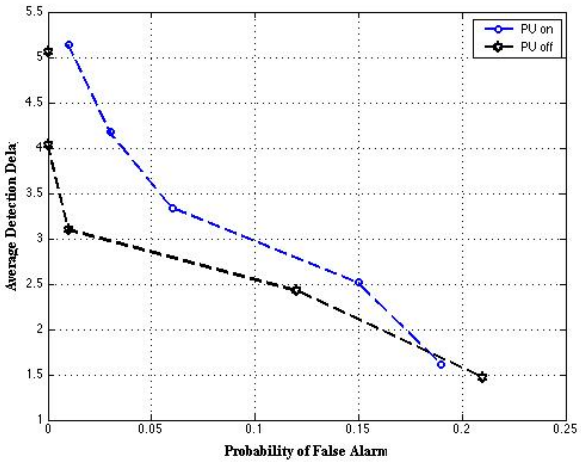

Figure. 6. Average detection delay vs. the probability of false alarm.

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.

When the PU would occupy more channels and thus block more the SU's paths in its interference range, (this happens due to lack of channels to assignment, not jamming routing packets in out-of-band CCC, as the jammer does), the ROC curve in Fig.7 shows that we cannot make decisions based solely on QD using obtained paths, and cross-layer examination becomes necessary. The ROC curve is flat at 100% detection rate when cross-layer fusion is performed. Similar results can be obtained when SUs use in-band channels for routing.

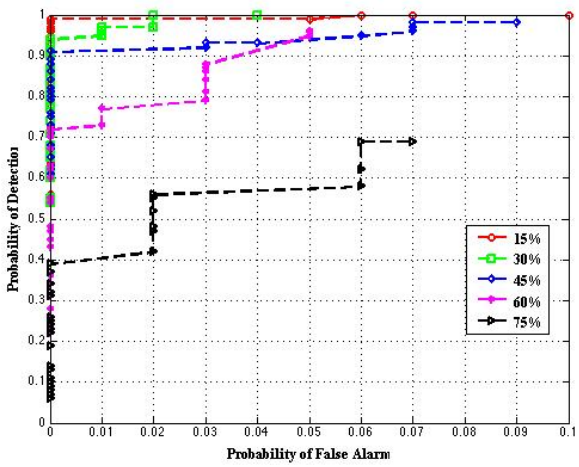

Figure. 7. ROC curve when the percentage of SU's paths blocked by PU increases.

IV. Related Works and Discussions

Anomaly detection systems, unlike typical signature based intrusion detection systems, model the normal network behavior which enables them to be extremely effective in finding and foiling both known and unknown attacks. An overview of recent anomaly detection techniques was given in [16]. As pointed out in that study, one of the challenges faced by anomaly detection system is high false alarm rate. In this work, we have taken into account the tradeoff between detection delay and false alarm rate using the quickest detection technique.

Sequential detection procedure for multichannel sensor systems was developed in [17]. Specifically, nonparametric version of the Page's CUSUM test was proposed for multichannel detection of a wide variety of attacks such as denial-of-service attacks and worm-based attacks. These methods formed grounds for the quickest detection scheme proposed in this paper.

The authors in [18] proposed detection methods of anomalous transmissions in cognitive radio networks. They presented a network structure for dynamic spectrum access and formulate the anomalous usage detection problem using statistical significance testing. Their proposed methods make use of the characteristics of radio propagation. Cross-layer approach was not considered.

Anomaly detection was studied by Thottan and Ji for IP networks [19]. Specifically, statistical analysis was applied to Simple Network Management Protocol (SNMP) management information base (MIB) variables. These variables contain information pertaining to the different functions performed by the network devices. Abrupt changes are detected by comparing the variance of the residuals obtained from two adjacent windows of data. The authors concluded that reliable detection can only be made by combining measurements from different MIB variables.

Lightweight methods for detection of spoofing and anomalous traffic in wireless networks was considered by Li and Trappe [20]. The authors proposed noncryptographic mechanisms that do not depend on cryptographic authentication, such

as a sequence number monotonicity detector and a joint traffic load and interarrival time detector. A multilevel classifier was also defined for practical implementation. Again, it is suggested that observations of multiple variables, such as the packet interarrival time and the background traffic, have to be made so that the detection can be effective.

Anomaly detection using cross-layer approach was proposed for broadcast networks by Chiang and Hu [21]. Cross-layer detection of jamming for wireless ad hoc networks was considered in [22]. The authors of [23] studied a cross-layer method for detecting routing attacks in mobile ad hoc networks. Similarly, a cross-layer approach was proposed for joint MAC and routing attack in multihop wireless networks [24]. However, none of the above works addressed the specific anomalous spectrum usage attacks in cognitive radio networks.

The above studies together with many other works on detection of anomalous behaviors in cognitive radio networks (e.g., see works reviewed in [25]) motivate us to consider a cross-layer detection scheme of anomalous spectrum usage attacks in cognitive radio networks. Furthermore, quickest detection method is adopted here to address the tradeoff between detection delay and false alarm rate.

V. Conclusions

In this paper, we proposed a framework for cross-layer detection of a type of stealthy denial-of-service attacks in multi-hop cognitive radio networks. Placing within a cross-layer framework, the proposed quickest detection algorithm is capable of detecting distribution changes at different layers with minimum delay while maintaining desired false alarm rate. It is demonstrated that cross-layer examination is critical when the effects of PU's behavior get close to those caused by the attackers. We plan to investigate the joint probability distribution of variables from different protocol layers and integrate multiple inputs from cross-layer variables into one representative statistic for detection in our future work.

VI. ACKNOWLEDGMENT

The authors would like to thank Dr. CaLynna Sorrells for performing some of the simulations in this study.

References

[1] J. Mitola III and G. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13 –18, Aug. 1999.

[2] C. Cordeiro, K. Challapali, D. Birru, and N. Sai Shankar, "Ieee 802.22: the first worldwide wireless standard based on cognitive radios," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, nov. 2005, pp. 328 –337.

[3] "Ieee p802.11af/d1.02 draft standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 3: Tv white spaces operation u.s." 1999.

[4] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25 –37, jan. 2008.

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

[6] K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications Surveys &Tutorials*, vol. 13, no. 2, pp. 245 –257, quarter 2011.

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

[8] N. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric bayesian classification," *Signal Processing, IEEE Transactions on*, vol. 60, no. 3, pp. 1432 –1445, march 2012.

[9] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys &Tutorials*, vol. 11, no. 1, pp. 116–130, quarter 2009.

[10] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys &Tutorials*, vol. PP, no. 99, pp. 1 –18, 2012.

[11] W. Xu, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *In ACM MOBIHOC*, 2005, pp. 46–57.

[12] 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*, ser. CoRoNet '09. New York, NY, USA: ACM, 2009, pp. 55–60. [Online]. Available: http://doi.acm.org/10.1145/1614235.1614249

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

[14] E. Page, "Continuous inspection schemes," *Biometrika*, vol. 41, no. 1/2, pp. 100 –115, Jun. 1954.

[15] A. Tartakovsky, B. Rozovskii, R. Blazek, and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods," *Signal Processing, IEEE Transactions on*, vol. 54, no. 9, pp. 3372 –3382, sept. 2006.

[16] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer Networks*, vol. 51, no. 12, pp. 3448 – 3470, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912860700062X

[17] A. G. Tartakovsky, B. L. Rozovskii, R. B. Blaek, and H. Kim, "Detection of intrusions in information systems by sequential change-point methods," *Statistical Methodology*, vol. 3, no. 3, pp. 252 – 293, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1572312705000493

[18] S. Liu, Y. Chen, W. Trappe, and L. Greenstein, "Aldo: An anomaly detection framework for dynamic spectrum access networks," in *INFOCOM 2009, IEEE*, 2009, pp. 675 –683.

[19] M. Thottan and C. Ji, "Anomaly detection in ip networks," *IEEE Transactions onSignal Processing*, vol. 51, no. 8, pp. 2191–2204, Aug. 2003.

[20] Q. Li and W. Trappe, "Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 793–808, Dec. 2007.

[21] J. Chiang and Y.-C. Hu, "Cross-layer jamming detection and mitigation in wireless broadcast networks," *Networking, IEEE/ACM Transactions on*, vol. 19, no. 1, pp. 286 –298, feb. 2011.

[22] G. Thamilarasu, S. Mishra, and R. Sridhar, "A cross-layer approach to detect jamming attacks in wireless ad hoc networks," in *Military Communications Conference, 2006. MILCOM 2006. IEEE*, oct. 2006, pp. 1 –7.

[23] J. Joseph, A. Das, B.-C. Seet, and B.-S. Lee, "Crads: Integrated cross layer approach for detecting routing attacks in manets," in *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, 31 2008-april 3 2008, pp. 1525 –1530.

[24] S. Djahel, F. Nait-Abdesselam, and A. Khokhar, "A cross layer framework to mitigate a joint mac and routing attack in multihop wireless networks," in *Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on*, oct. 2009, pp. 730 –737.

[25] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys and Tutorials*, vol. PP, no. 99, pp. 1 –18, 2012.

Lijun Qian received the B.E. degree from Tsinghua University, Beijing, China, and the M.S. degree from Technion-Israel Institute of Technology,Haifa, Israel, and the Ph.D. degree from Rutgers - The State University of New Jersey. He is currently an Associate Professor in the Department of Electrical and Computer Engineering, Prairie View A&M University (PVAMU), a member of the Texas A&M University System. Before joining PVAMU, he was a MTS at the Mathematical Science Research Center of Bell Labs in Murray Hill, NJ. He is a Visiting Professor at the Helsinki University of Technology (now Aalto University), Finland. His major research interests include wireless networks, network security, and systems biology. His research is supported by NSF and ARO.

Xiangfang Li received the B.S. and M.E. degrees from Beihang University, Beijing, China, and the M.S. and Ph.D. degrees from Rutgers University, NJ, both in electrical and computer engineering. She is an Associate Research Scientist in Genomic Signal Processing Laboratory, Department of Electrical and Computer Engineering, Texas A&M University, College Station. Her major research interests include dynamical systems and signal processing, systems and computational biology, and information security.

Shuangqing Wei got his B.E and M.E in Electrical Engineering from Tsinghua University in 1995 and 1998, respectively. He started his academic career at Louisiana State University after obtaining his Ph.D. from the University of Massachusetts, Amherst in 2003. He is currently an Associate Professor at the Department of ECE at Louisiana State University. His research interests include information theory, statistical inference, game theory, and their applications in the areas of wireless security and cognitive radio networks. He is an Associate Editor for IEEE Transactions on Vehicular Technology, and an Editor for IEEE Transactions on Wireless Communications. His research has been funded by the NSF, AFRL and DOE, and the Board of Regents of Louisiana.