Anomalous Spectrum Usage Attack Detection in Cognitive Radio Wireless Networks

CaLynna Sorrells, Paul Potier, Lijun Qian
Department of Electrical and Computer Engineering
Prairie View A&M University, Texas A&M University System
Prairie View, TX 77446
Email: {csorrells, ppotier, liqian}@pvamu.edu

Xiangfang Li
Department of Electrical and Computer Engineering
Texas A&M University
College Station, TX 77843
Email: xiangfang@ece.tamu.edu

***Abstract*—In many mission-critical applications such as military operations or disaster relief efforts, wireless networks employing dynamic spectrum access enabled by cognitive radio technology gain popularity due to their high spectrum efficiency and interoperability. However, the use of cognitive radio further complicates the security problems in wireless networks and introduces additional challenges. For instance, an attacker may mimic the behavior of a licensed primary user and disrupt the communication strategy of opportunistic spectrum usage of cognitive radio nodes, known as Primary User Emulation Attacks. Another example is a smart jammer, who can scan the spectrum and jam channels selectively. A common characteristic of the attacks in both examples is that they cause anomalous spectrum usage and disrupt the dynamic spectrum access, thus we termed them Anomalous Spectrum Usage Attacks in the context of cognitive radio wireless networks. Anomalous Spectrum Usage Attacks are extremely difficult to detect. In order to address these challenges, we propose a cross-layer framework for security enhancement and attack mitigation. In addition to physical layer sensing, we also take advantage of statistical analysis of the routing information of multiple paths collected by the routing module at the network layer. Inference of congested areas due to spectrum shortage can be made by information fusion and the results from the inference module will be compared to prior knowledge of the primary users, and the suspicious spectrum shortage will be subject to selective auditing, where a manager such as a cluster head will poll more detailed data from the cognitive nodes locating near the suspicious area for further analysis. We use a spectrum-aware split multipath routing as a baseline routing for performance evaluation. The effectiveness of the proposed scheme is demonstrated by extensive simulations.**

I. Introduction

In many mission-critical applications such as military operations or disaster relief efforts, different organizations may collaborate on a mission and multiple wireless systems may coexist in a geographical area. Wireless networks employing dynamic spectrum access enabled by Cognitive Radio (CR) technology gain popularity due to their high spectrum efficiency and interoperability. Dynamic spectrum access allows an unlicensed Secondary User (SU) equipped with a CR coexist with a licensed Primary User (PU) without causing interference to that PU. Cognitive radio has the capability to sense a wide range of frequencies and to opportunistically use the unoccupied spectrum in a heterogeneous environment. The introduction of cognitive radio shifts the paradigm of spectrum management from command and control to dynamic spectrum access, thus improves the spectrum utilization dramatically. At the same time, a cognitive radio such as a JTRS radio [1] can reconfigure its waveform on the fly, and fulfills the requirement of interoperability.

Although the technology behind CR is cutting edge, it must be supplemented with essential security features to realize the benefits of the technology. Furthermore, the use of CR further complicates the security problems in wireless networks and introduces additional challenges [2]. For instance, an attacker may mimic the behavior of a primary user such as a licensed user and disrupt the communication strategy of opportunistic spectrum usage of CR nodes. This type of attacks is termed Primary User Emulation (PUE) attack [3], [4], and it can be considered as a special case of denial-of-service (DoS) attacks in a CR network [5]. Another type of attacks specific to CR is smart jamming, e.g., the jamming attack can push the CR network to select a specific frequency band for the common control channel, where another attacker can eavesdrop on the control messages [6].

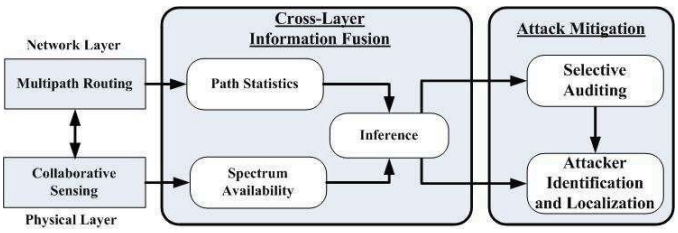

Fig. 1. Block diagram of the proposed cross-layer approach for detection of Anomalous Spectrum Usage Attacks.

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 and disrupt the dynamic spectrum access, thus we termed them "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 where an infrastructure may not exist or function, and typically wireless ad hoc networks are deployed, such as in emergency response. Thus we dedicate

978-1-4577-1376-7/11/$26.00 ©2011 IEEE

our effort on detecting Anomalous Spectrum Usage Attacks in CR ad hoc networks in this paper. Specifically, we propose a cross-layer framework for detecting ASUAs and locating the attackers. In addition to physical layer sensing, we also take advantage of statistical analysis of the routing information of multiple paths collected by the routing module at the network layer. Inference of congested areas due to spectrum shortage can be made by information fusion and the results from the inference module will be compared to the prior knowledge of the primary users. Then the suspicious spectrum shortage will be subject to selective auditing, where a manager such as a cluster head will poll more detailed data from the cognitive nodes locating near the suspicious area for further analysis. To illustrate our idea, a block diagram is shown in Fig. 1. We use a spectrum-aware split multipath routing as a baseline routing for performance evaluation. The effectiveness of the proposed scheme is demonstrated by simulations.

The rest of this paper is organized as follows. Related works and our contributions are highlighted in Section II. Network model and the details of the proposed scheme are given in Section III. Section IV is dedicated to simulation studies and our findings out of these experiments. Section V contains the concluding remarks.

II. Related Work

In this section, we briefly review some related works on detection of PUE and jamming attacks in CR networks[1], and highlight the rationale of our approach and our contributions in this paper.

A. PUE and jamming attacks detection in CR networks

Many recent studies focus on physical layer techniques to detect anomaly in spectrum usage, such as [7], [3], [4], [8], [9]. Unauthorized spectrum usage detection was investigated in [7] for a zone-based network where authorized users do not interfere with each other. Since only one or zero authorized user can present in each zone, the detection problem was formulated as distinguishing unknown signals based on the measurements of received signal powers. In [3], the authors propose a transmitter verification scheme in which the location of the Primary Signal Transmitter (PST) are known beforehand. If the suspicious signal is transmitting in area away from the PST, it is decided that it is a PUE attack. If the suspicious signal is transmitting in the vicinity of the PST, energy detection is used to validate the signal since it is assumed that a PUE attacker cannot emulate the energy of a PU signal. In [4], an energy detection technique is proposed in which a lower bound is defined for the probability of successful detection of PUE attack. A centralized spectrum decision protocol for mitigating PUE attacks is proposed in [9] that make use of the individual spectrum decision made by each SU. The authors in [10] proposed a method to add a watermark to PU signal that allow for a CR to authenticate the transmitted signal. Only physical layer information was used in these works, and either prior information about the PU or modifications to the PU signal is required. Moreover, they do not address the attack detection problem in a large CR ad hoc network.

Jamming in CR wireless networks has been also studied recently [11], [12], [8], just to name a few. In [11], a game theoretic approach is proposed to model the jamming and anti-jamming in multichannel cognitive radio systems. Nash equilibrium is obtained for one-stage game and stochastic control strategy is derived for multi-stage game. In [8], SUs follow a PN sequence code just like that in CDMA such that the smart jammer would not be able to compute which channel to jam in time, thus avoid jamming attacks. However, the above works are jamming mitigation techniques rather than jamming detection methods. The feasibility of launching and detecting jamming attacks in wireless networks is discussed in detail in [13]. The authors conclude that no single measurement is sufficient for reliably detecting a jammer. Furthermore, unlike traditional brutal-force jamming, smart jamming create a new phenomenon in CR networks, and the detection of jamming attacks in such networks is not well understood.

B. Our contributions

In this paper, we propose a cross-layer approach for detection of anomalous spectrum usage attack in CR ad hoc networks covering a large geographical area, where the SUs may need multihop connectivity to communicate with each other. Specifically, the information from the physical layer spectrum sensing and statistical analysis of multipath from the network layer will be combined to deduce the spectrum usage information, and detect possible anomalous spectrum usage attacks. This approach is based on the following observations:

- Using only information from physical layer spectrum sensing is usually not enough to detect anomaly in spectrum usage, especially in a large CR ad hoc network.
- The effect of location-dependent channel availability is significant in a CR ad hoc network which requires multihop communications. As a result, certain statistics of resulted paths from multipath routing can reveal potential "troubled" area in the network, which provide ground for further investigation of spectrum misuse as well as potential attacks.
- Collecting all the physical layer spectrum sensing results to a fusion center to perform collaborative spectrum sensing in a large CR ad hoc network requires a lot of overhead, both in terms of hardware (e.g., a spectrum sensing grid) and the bandwidth and delay incurred by reporting the results to the fusion center. At the same time, using multipath routing that is resilient to the dynamic behavior of the PUs is necessary [14], since the links among SUs may be highly unreliable due to the activities of the PUs. Hence, the proposed method using multipath routing will not incur much overhead if a multipath routing approach is needed for the robust operation of the CR ad hoc network.

[1]This review is by no means exhaustive and interested readers may refer to [2] and the references therein.

- The information provided by the physical layer spectrum sensing and from the proposed statistical analysis of the resulted paths from multipath routing can be used for cross-layer examination.

In this work, we tackle the problem of anomalous spectrum usage attack detection from the novel perspective of cross-layer examination. To the best of our knowledge, this is the first study to combine physical and network layer information for attack detection in CR networks. Note that cross-layer attack and defense was considered for CR networks in [15], where coordinated report-false-sensing data at the physical layer and small-back-off-window attack at the MAC layer is studied, and a trust-based cross-layer defense mechanism is proposed. PUE attacks and jamming attacks are not considered in [15], and network layer information is not used in [15].

III. Network Model and The Proposed Cross-Layer Examination Method

In this paper, we consider a CR ad hoc network covering a large area, where an infrastructure may not be available. In such a network, different "spectrum holes" may be available at different locations in the network due to diverse PUs' activities, and multihop connectivities may be needed for communications among SUs. It is assumed that collaborative spectrum sensing [16] is performed by the SUs periodically, and their sensing results are reported *truthfully*. Reporting False Sensing Data Attack (RFSD) is studied extensively in the literature and is well addressed by various mechanisms, such as the reputation-based or trust-based mechanism [17], [18], [19], the consensus-based scheme [20], outlier detection [21], and via incentive alleviation [22], hence we do not consider RFSD attack in this paper.

The locations of the SUs are assumed known through GPS or other localization methods. Two types of attackers may exist in the network, namely, PUE attackers and smart jammers. The attackers have similar energy resources and processing power as the SUs. The PUE attackers mimic the waveform of a PU, and occupy some or all of the spectrum. A smart jammer scans the spectrum constantly, and only transmits in those frequencies where communications of other legitimate users are detected. The transmission range of the attackers is typically smaller than that of the PUs. Furthermore, we assume low mobility of the attackers such that their locations are not changed much during one detection cycle.

An example scenario is shown in Fig. 2, where one PU, one PUE attacker, and one smart jammer present in the network. While the PUE attacker mimic the PU and occupies a set of channels, the smart jammer scans the channels and try to block any legitimate transmissions.

A. Outline of the proposed scheme

The proposed scheme for anomaly detection in spectrum usage consists of the following three steps:

1) Perform statistical analysis of the paths/nodes obtained from route discovery using spectrum-aware split multipath routing (details given in Section III-B). 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 suspicious areas/nodes with physical layer spectrum sensing results and any prior knowledge on PUs from empirical data.
3) Active checking by selective auditing: In order to confirm a PUE attack, perform active checking by selectively injecting controlled interference to the potential attacker. This is motivated by the fact that an attacker may mimic a PU in terms of signal waveforms, but since it lacks the full feature of the PU system, such as the closed-loop power control, it will not respond to the interfering signal the same way as the legitimate PU does.

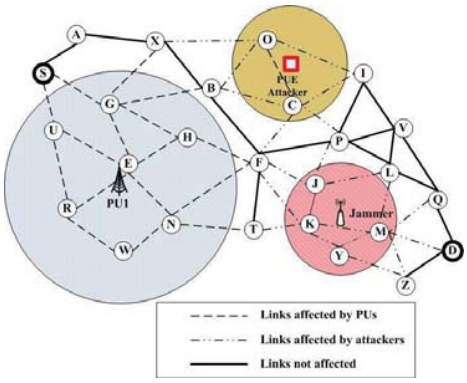

Fig. 2. An example of two types of attacks in a cognitive radio ad hoc network.

In step 1, exactly how many routes will be chosen is a design parameter in multipath routing protocols. It depends on multipath 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 path/node is indeed affected by attacks.

The main idea of step 1 is based on the observation that certain statistics of the discovered paths by the multipath routing protocol will change dramatically under the anomalous spectrum usage attacks. As an example using multipath routing from source node S to destination node D in Fig. 2, when no attacks occur, most nodes (SUs) are expected to be included in the resulted paths. Depending on how intense the PU uses the spectrum, the nodes affected by PU's activities will appear less in the resulted paths. Under anomalous spectrum usage attacks, the distribution of the nodes appear in the resulted paths would change dramatically, with nodes connected by solid links (e.g., B,F,P) appear frequently in the resulted paths, while the nodes under attack (e.g., J,K,M,Y) may not be included in any path if they are completely jammed. Hence, it is possible to examine such statistics to detect this type of attacks and pinpoint the attackers if enough routing information is available.

Step 2 is based on another important observation that the discrepancies between the paths obtained by multipath routing and the physical layer spectrum sensing reports may reveal

potential attacks. Again in the example shown in Fig. 2, the nodes under attack (J,K,M,Y) are not included in the obtained paths because the RREQ packets are interrupted by the smart jammer. However, the surrounding nodes (say, F,P,L,Z) report most of the spectrum is available in the neighborhood of (J,K,M,Y), since the spectrum sensing range is usually much larger than the transmission range. This discrepancy indicates that the area of nodes (J,K,M,Y) is probably under smart jamming attack.

B. Spectrum-Aware Split Multipath Routing (SA-SMR)

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 CR ad hoc networks. Routing protocols for CR 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 [23]. Since the objective here is *not* designing an optimal routing protocol, but to explore the effects of PUs' activities and spectrum sensing by the SUs on the resulted paths, we use a generic spectrum-aware multipath routing protocol by modifying Split Multi-path Routing [24] 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 [24], is an on-demand routing protocol that constructs maximally disjoint paths. SMR is based on DSR [25] 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 CR ad hoc networks where PUs' activities may constantly disrupt SUs' 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 channel in common to be used for the data traffic. However, to make the protocol generic and to avoid overhead for complicated distributed scheduling that 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 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 to fulfill the needs of cross-layer examination at the destination node.

In order to maintain the scalability of the proposed Spectrum-Aware Split Multipath Routing, each intermediate node will append the local spectrum sensing and traffic load information in the RREQ packet *only once*. Since the nodes along any path would not repeat the local information, the total overhead for reporting the spectrum sensing and traffic load information would be $\bar{\Phi} \times O(N)$, where $\bar{\Phi}$ denotes the average size of the field about spectrum sensing and traffic load per node in the RREQ packet, and N is the total number of SUs.

C. Statistical analysis of multipath

The following notations are used in the proposed statistical analysis scheme

- $\mathcal{P}$: the set of all obtained paths;
- $\mathcal{L}$: the set of all (distinctive) links in $\mathcal{P}$;
- $\mathcal{N}_{\mathcal{P}}$: the set of all nodes (SUs) in $\mathcal{P}$;
- $\mathcal{N}$: the set of all nodes (SUs) in the network;
- N_P: the total number of nodes in $\mathcal{P}$;
- N: the number of nodes in $\mathcal{N}$;
- n_i: the i^{th} node in $\mathcal{N}$;
- m_i: the number of times that n_i appears in $\mathcal{P}$;
- m: a random variable represents the number of times that a node appears in $\mathcal{P}$;
- f_i: the relative frequency that n_i appears in $\mathcal{P}$;
- $\underline{\theta}_i$: a lower-threshold value;
- $\mathcal{N}_{\mathcal{J}}$: the set of nodes whose f_i is below $\underline{\theta}_i$.

Since anomalous spectrum usage attacks are inherently DoS attacks, they block the surrounding neighbors from using any of the available channels, causing a local spectrum shortage, thus it is expected that all the nodes in that area will suffer from spectrum shortage and will not be able to assign a channel for the data traffic, or their RREQ packets are disrupted, and as a result, those nodes will not be included in the resulted paths. The relative frequency of each node appears in $\mathcal{P}$ from one route discovery

$$f_i = \frac{m_i}{N_P}, \ \ \forall n_i \tag{1}$$

where

$$N_P = \sum_i m_i. \tag{2}$$

After obtaining f_i for all the nodes, we are able to find the set of nodes whose f_i is below $\underline{\theta}_i$, $\mathcal{N}_{\mathcal{J}}$. By exploiting the properties of $\mathcal{N}_{\mathcal{J}}$, such as calculating "the center of gravity" based on their spatial correlations, it is possible to identify the area with extreme spectrum shortage, thus provides ground for step 2 and 3 in the proposed scheme.

An alternative statistics is the probability mass function (PMF) of random variable m/N_P, the relative frequency of nodes in $\mathcal{P}$. The samples (m_i/N_P) collected from the network under normal condition will form the training set. The distribution of m/N_P under normal condition may be obtained by approximation using the training set and act as a profile. Then the distribution of m/N_P obtained using real-time samples will be compared with the profile to help determine whether the network is under attack. This approach

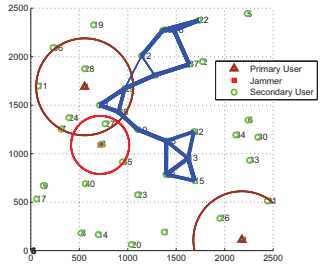

Fig. 3. An example routing result from node 22 to node 15.

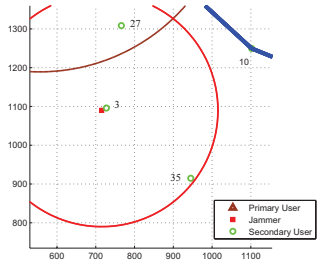

Fig. 4. A closer look at the suspected area.

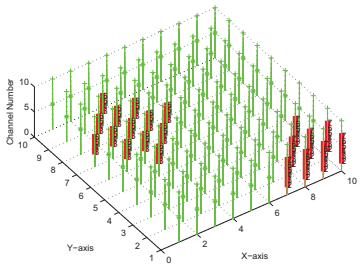

Fig. 5. Spectrum situation in the network.

will also provide a way to estimate the probability of low participating nodes using theoretical analysis since the PMF is available.

It worth pointing out that although anomalous spectrum usage attacks are used as examples throughout this paper, the statistical analysis method proposed here may be applied to other attacks as long as certain statistics of the obtained paths change significantly under the attack.

D. Selective auditing

When a suspicious area is deduced from the cross-layer information fusion, selective auditing is activated for the neighboring nodes surrounding the suspicious area to examine the situation closely. For instance, active checking 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 or a jammer would not have a corresponding receiver and thus would not respond to the interfering signal the same way as the legitimate PU does. Of course, there are also 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, such as in [26].

IV. Simulation Results and Analysis

In order to test the feasibility of the proposed method, we perform simulations using the proposed SA-SMR to check how different parameter settings would affect the resulted paths and detection accuracy. Our simulation results are obtained by considering a 2500m×2500m square area, with 5 PUs (but with variable number of PUs active in different scenarios) and 40 SUs randomly deployed. We assume that there are 10 licensed channels. An active PU transmits on randomly distributed (uniformly from 1 to 10) contiguous channels and interrupts a circular range with radius of 500m, within which the channels used by the PU are not available to the SUs.

A. Proof-of-concept experiment

In this case, there are 2 active PUs that occupy channels 3-6 and 2-7, respectively. A jammer also presents and blocks all the traffic in its range (300m). In one sample run for multipath routing from node 22 to node 15, 48 paths were found and displayed in Fig. 3. The thickness of the links represents how many times the link has been used in the obtained paths. It is observed that the nodes in the interference range of PU_1 still have some channels available, thus they participate in the routing process, while the nodes in the interference range of the jammer were blocked out. The corresponding spectrum availability from the collected spectrum sensing reports is plotted in Fig. 5. The 2500m×2500m square field is divided into 10×10 sub fields, with each sub field a 250m×250m square. Green denotes available channels while red denotes occupied channels. We can observe that occupancy is highly correlated in the spatial as well as the spectral domains. This indicates that neighboring nodes may provide information of spectrum situation in selective auditing phase without much error. Note that the spectrum sensing report shows only the spectrum occupancies of the 2 PUs, this contradicts the fact shown in Fig. 4 that nodes have all or partial spectrum available, node 3 and node 35, and node 27, are not included in the obtained paths. This contradiction reveals the potential suspect area of attack.

To be more specific, we compare the sample of probability mass function (PMF) of the relative frequency of nodes in $\mathcal{P}$, without and with attack in Fig.6. The further right side of the figure the data locates, the higher frequency the node appears in $\mathcal{P}$. It is observed that the percentage of both zero (the most left) and high (the most right) participating nodes increase with attacks. This is due to the fact that the nodes under attack would not be able to participate in the routing process, while those nodes in better locations need to carry more traffic.

B. Effect of number of PUs

In the rest of the simulation, we provide the results under different parameter settings of a typical run, with randomly

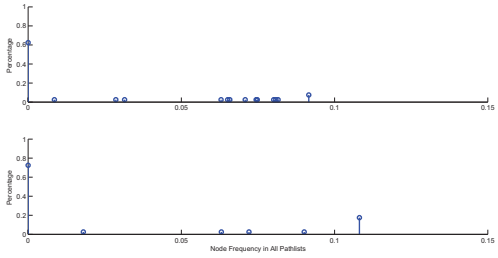

Fig. 6. Comparison of PMFs without and with attack.

chosen source and destination nodes that are at least 3 hops away from each other. It is observed that the average number of obtained paths are 140, 40 and zero with 1, 2 and 5 active PUs, respectively. Although the obtained paths changes significantly, it is interesting that the PMF of the relative frequency of nodes in $\mathcal{P}$ does not change. This is due to the fact that in our simulations, the PUs only occupy some of the channels and never consume all the channels. This also indicates that for PUE attacks, step 2 and 3 in the proposed cross-layer scheme are necessary.

Through this simulation study, we show that the resulted paths from the proposed SA-SMR change significantly under ASUAs. These results lay ground for further investigation of more advanced statistical measures from the resulted paths for the detection of potential attacks in cognitive radio ad hoc networks.

V. Conclusions and Future Work

In this paper, a cross-layer approach is proposed to detect Anomalous Spectrum Usage Attacks (ASUAs) in a cognitive radio ad hoc network. With the collected physical and network layer information, accurate spectrum awareness across the network can be achieved and discrepancy between the information from the two layers can be identified. This will provide intelligence for detecting and locating PUE attackers and smart jammers, and ensure the success of dynamic spectrum access, which leads to higher power and bandwidth efficiency that is indispensable in mission-critical applications. At the same time, better communication strategies can be designed using the cross-layer information, e.g., more reliable routing policies and more efficient congestion control protocols. 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 vehicle to carry critical information, both spectrum sensing information and traffic load information, to fulfill the needs for cross-layer examination. The scalability of the SA-SMR will be studied and higher mobility of the PUs will be considered in our future work.

VI. Acknowledgment

This research work is supported in part by NSF under CNS-1040207 and the US Army Research Office under Cooperative Agreement W911NF-10-1-0087.

References

[1] R. D. Hinman, "Application of cognitive radio technology to legacy military waveforms in a jtrs (joint tactical radio system) radio," in *Proc. of IEEE MILCOM 2006*.

[2] G. Baldini, T. Sturman, A. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys & Tutorials*, vol. PP, no. 99, pp. 1 –25, 2011.

[3] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE JSAC*, vol. 26, no. 1, pp. 25 –37, Jan. 2008.

[4] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *IEEE DySPAN 2008*.

[5] A. Sethi and T. Brown, "Hammer model threat assessment of cognitive radio denial of service attacks," in *IEEE DySPAN 2008*.

[6] J. Burbank, A. Hammons, and S. Jones, "A common lexicon and design issues surrounding cognitive radio networks operating in the presence of jamming," in *IEEE MILCOM 2008*.

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

[8] L. Ma and C.-C. Shen, "Security-enhanced virtual channel rendezvous algorithm for dynamic spectrum access wireless networks," in *IEEE DySPAN 2008*.

[9] Z. Jin, S. Anand, and K. Subbalakshmi, "Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks," in *IEEE GLOBECOM 2010*.

[10] N. Goergen, T. Clancy, and T. Newman, "Physical layer authentication watermarks through synthetic channel emulation," in *IEEE DySPAN 2010*.

[11] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics," *IEEE Trans. on Wireless Communications*, 2010.

[12] ——, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems;part ii: Unknown channel statistics," *IEEE Trans. on Wireless Communications*, 2010.

[13] 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.

[14] 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 *Proc. of CoRoNet'09* , pp. 55–60.

[15] W. Wang, Y. Sun, H. Li, and Z. Han, "Cross-layer attack and defense in cognitive radio networks," in *IEEE GLOBECOM 2010*.

[16] A. Ghasemi and E. S. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," *Journal of Communications*.

[17] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *IEEE INFOCOM 2008*.

[18] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 13, pp. 86–95, Sep 2009.

[19] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *IEEE CISS 2009*, pp. 130 –134.

[20] F. Yu, H. Tang, M. Huang, Z. Li, and P. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *IEEE MILCOM 2009*.

[21] H. Li and Z. Han, "Catching attacker for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," in *IEEE DySPAN 2010*.

[22] S. Sodagari, A. Attar, V. Leung, and S. Bil andn, "Denial of service attacks in cognitive radio networks through channel eviction triggering," in *IEEE GLOBECOM 2010*.

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

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

[25] 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.

[26] "Fcc tv contour map." [Online]. Available: http://transition.fcc.gov/ftp/Bureaus/MB/Databases/tv_service_contour_data/