Detection of Jamming Attack in Cognitive Radio Networks

[1]C Manogna, [2]K Bhaskar Naik

[1]M.Tech-CNIS, Department of CSE, Sree Vidhyanikethan Engineering College, Rangampet, Tirupati
[2]M.Tech, Assistant Professor, Department of CSE, Sree Vidhyanikethan Engineering College, Rangampet, Tirupati
Email: [1]chundurimanogna@gmail.com, [2]bhaskar.cse501@gmail.com

Abstract— Cognitive Radio is becoming a hot research topic in wireless communication field now, which can be used to alleviate the spectrum shortage problem and improve the spectrum utilization. While Cognitive Radio Networks (CRNs) present a promising solution to solve the scarcity of the radio spectrum, they are still susceptible to jamming attacks. The CRN is based on IEEE Wireless Regional Area Network (WRAN). The attacker may be external users or secondary users. But cognitive network is sensitive to security threats. A secondary user in the CRN to quickly detect the attack, by simple yet effective detection method is presented.. To overcome jamming attack issues proposed detection method can be used, to find the abnormal behavior of the system. It can adopt the anomaly detection approach and use non-parametric cumulative sum (cusum) as a change point detection algorithm to discover the jamming attack in the system.

Index Terms— Jamming Attack, Cognitive Radio Network, Intrusion Detection System.

I. INTRODUCTION

Recently, the explosive growth of wireless services and

applications led to a shortage of radio spectrum. Since the Federal Communication Commission (FCC) approved unlicensed users to access the unused portion of the reserved spectrum (e.g., television channels) for wireless broadband services, various researchers have devoted a lot of effort in designing cognitive radio networks (CRNs) to exploit this feature. CRNs are intelligent networks, which allow unlicensed users to use software radio for making the best use of the available/unused spectrum. While doing so, the unlicensed "cognitive" users should be transparent. In other words, they may not interfere with the primary users (i.e., the users for whom the system was originally designed) in order to share the radio spectrum resource in CRNs such as those based on IEEE 802.22 wireless regional area network (WRAN) technology [1]. This radio spectrum sharing policy among the licensed and unlicensed users, however, opens up the possibility of various security threats. Indeed, a number of attacks have been studied in recent literature that target CRNs. Although some solutions have been presented to detect these attacks, to the best of our knowledge to date, a full-fledged intrusion detection system (IDS) has not yet been designed for combating the attacks against CRNs. The research work presented in [2] pioneered in addressing the need of IDS for CRNs as a second line of intrusion/attack detection in addition to the conventional cryptographic primitives for facilitating authentication and confidentiality. Even though the work in [2] defined some of the essential modules for designing an IDS for CRNs, it did not focus on specifying any lightweight detection algorithm. Having understood the lack of research work on the IDS based defense for CRNs, we are motivated to design an effective IDS for deployment in the cognitive unlicensed users. The proposed IDS uses cusum based anomaly detection, which is lightweight and is able to discover previously unknown attacks with significantly low detection latency.

II. EXISTING CRN ARCHITECTURE

Considered CRN system model based on IEEE 802.22 WRAN is depicted in Fig. 1. For simplicity, the figure includes only one television broadcasting tower whereas multiple broadcasting towers may also be present. The television companies have license to broadcast their programs through the reserved band of the 54 to 806 MHz. So, the television companies (along with their subscribers) formulate the "primary users" of the system. On the other hand, the IEEE 802.22 WRAN specification allows a number of "cells", each of which is managed by a base station (BS). The WRAN cells form our considered CRN. The service coverage radius of each of the WRAN cells featuring collocated CRNs varies from 33 to 100km. Each CRN can support a number of "secondary users", who may access the unused spaces of the spectrum, which is usually reserved for the television companies, i.e., the primary users. These unused spaces of the spectrum might occur due to different scenarios, e.g., when the television broadcast is offline/idle. The unused portions of the spectrum are referred to as "white spaces". Each secondary

user is equipped with software radio to sense whether the primary users are currently occupying a channel or not. If the channel is occupied, the secondary user has the ability to intelligently adapt his radio to another channel in order to sense the white spaces of that channel. The intelligent adaptation with the external environment is possible as the cognitive engine is able to continuously learn by utilizing online and offline learning policies.

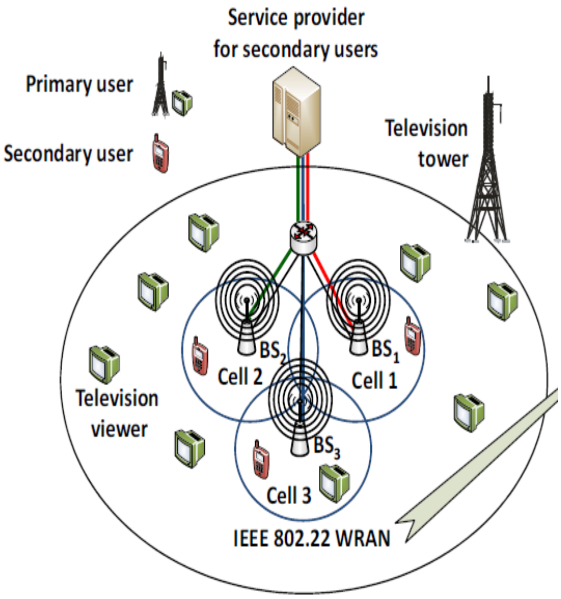

Figure 1 CRN Architecture

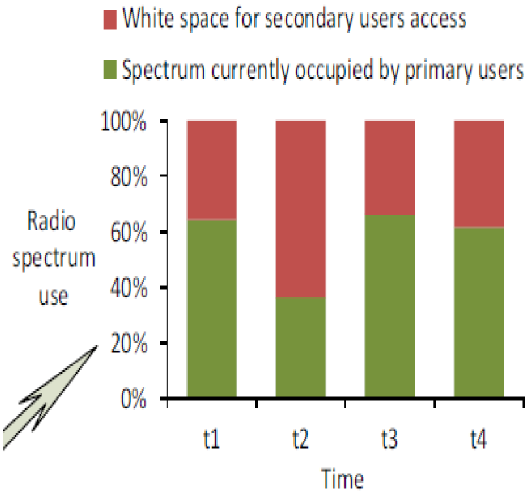

Figure 2 Radio Spectrum use in CRN

The plot in Fig. 1 demonstrates an example of how the secondary users share the spectrum with the primary ones over time. It is worth noting that the plot shows a simple illustration for ease of understanding, and the white spaces are not necessarily contiguous.

III. JAMMING ATTACK AGAINST CRN

Built upon a shared wireless medium, wireless networks are susceptible to jamming attacks. These types of attacks can easily be accomplished by an adversary by either bypassing MAC layer protocol or by emitting RF signals. Typically, jamming can be referred as intentional interference attacks on wireless networks. It is an attempt of making the users not possible to use network resources. Jamming attacks are severe Denial-of-service attacks against wireless medium. In this work, considering the role of wireless adversary, which targets the packets of high importance by emitting radio frequency signals and do not follow underlying network architecture. Typically, jamming attacks have been considered under external threat model, in which jammer is not part of network. However, adversaries with internal knowledge of protocol and network specification can introduce jamming attacks that are difficult to detect and prevent.

Jamming attack: Like other wireless communication systems, jamming attack is one of the most difficult threats in CRNs. A jamming attacker may transmit continuous packets to force a legitimate secondary user to never sense an idle channel. This leads to a DoS type attack whereby the legitimate user is unable to access any white space.

IV. PROPOSED DETECTION SYSTEM

The conventional detection methods usually follow either mis-use or anomaly based attack detection methods. The mis-use based detection method uses signatures of already known attacks. However, the mis-use based approach cannot discover new types of attacks effectively. On the other hand, as its name implies, the anomaly based detection methodology relies on finding the “anomaly”, which represents an abnormal mode of operation in the system. By designing an appropriate anomaly based intrusion/attack detection system, it may be possible to detect new (i.e., not known beforehand) attacks, which generate some abnormal change in the targeted CRN. This is the reason why it is better to use the anomaly based intrusion detection technique in the IDS for identifying attacks in CRNs. It is worth mentioning that some of our earlier works employed a variety of statistical detection techniques for different types of wireless networks. However, many of the existing statistical detection techniques may not be adequate for designing an IDS for CRN as it presents a unique challenge. Specifically in CRN, a centralized IDS may not be able to detect a jamming attack and notify the secondary users quick enough, and therefore, it is important to facilitate lightweight yet effective IDSs in the secondary users themselves. Toward this end, in the following, we present our anomaly based IDS, which utilizes time-series cumulative sum (cusum) hypothesis testing [7]. The reason behind choosing cusum for our proposed detection engine is due to its low complexity and overhead. As a consequence, the IDS can be lightweight and deployed in the individual secondary users. Note that such IDS deployment does not conflict with the regulation of the FCC that prohibits changing primary user systems [4]. As mentioned earlier, each secondary user is assumed to have an IDS. The IDS operates in two steps, namely learning or profiling phase and detection phase. In the remainder of this section, we describe these two phases in detail.

A. Learning phase

To effectively detect anomalies due to various types of attacks, the IDS needs to be designed in such a fashion that it may learn the normal behavior of protocol operation, traffic flow, primary user access time, packet delivery ratio (PDR), signal strength (SS), and so forth. The IDS may learn these information by constructing a statistical profile during normal CRN conditions or with acceptable (i.e., low) level of suspicious activities. To make it clear to the readers, an example of a physical layer attack, i.e., the jamming attack, is considered for our study. In order to identify the jamming attack, let us consider a simple observation made by a secondary user involving its PDR and SS. The PDR of a user indicates the ratio of the number of packets received by the user to that of the packets sent to him. Note that while this is an example case of the IDS learning phase (which arises from a specific jamming attack against the CRN), our IDS is not limited to learning this feature only. In fact, if the IDS is appropriately designed by taking into consideration the CRN system specifications, wireless protocol behavior, and so forth, it can learn various modes of operation of the CRN. The acquired information can facilitate the detection phase of the IDS to discover unknown intrusions or attacks against the targeted CRN.

B. Detection phase

The proposed IDS detection phase relies on finding the point of change in the CRN operation as quickly as possible under an attack. First, let us present a physical layer jamming attack a follows. When a malicious user jams a secondary user's connection, the following observations can be made. While the SS measured at that secondary user remains high, his PDR usually drops. This happens because the secondary user never receives some/all of the packets sent to him. Our point of interest is how to detect the change point in the PDR behavior of a secondary user (targeted by a jamming attacker).

In other words, how can the IDS find when the PDR of the Secondary user is dropping significantly enough to reflect the impact of a jamming attack? In the following, our proposed IDS with cusum based anomaly detection is presented to deal with this issue.

Assume that the IDS operates over equal time-rounds, Δn (Where n = 1, 2, 3, ...). Let the mean of Fn during the profiling period (i.e., no or low jamming attack scenario) be represented by m. The idea is that the IDS continues to monitor a significant change in the value of m that can be considered as the influence of the jamming attack. m remains close to one until an anomaly occurs (which is later shown in Fig. 3). However, an assumption of the nonparametric cusum algorithm suggests that the mean value of the random sequence should be negative during the normal conditions and becomes positive upon a change. Therefore, a new sequence Gn = β− Fn is obtained where β is the average of the minimum/negative peak values of Fn during the profiling period (as shown in Fig. 4). During a jamming attack, the increase in the mean of Gn can be lower bounded by h = (2β). Then, the cusum sequence Yn is expressed as follows.

Yn = (Yn−1 + Gn)+; Y0 = 0 ----->(1)

where x+ = x if x > 0; otherwise, x+ = 0.

A large value of Yn strongly implies an anomaly (i.e., the effect of jamming attack in this case). The detection threshold, θ is computed as follows.

θ= (m − β)tdes ------->(2)

where tdes denotes the desired detection time, which should set to a small value for quickly detecting an anomaly. At the detection phase, the IDS computes Yn over time. Yn remains close to zero as long as normal conditions prevail in the CRN. Upon a jamming attack, Yn starts to increase. When Yn exceeds θ and as long as the SS measured at the secondary user is high, the IDS generates an alert of a possible attack (i.e., jamming). This is illustrated in Fig. 5.

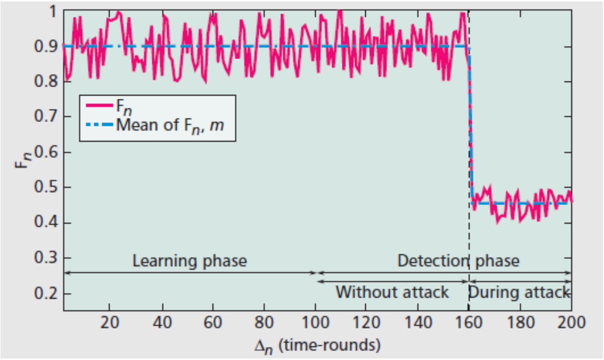

Figure 3: Computing Fn and Mean of Fn

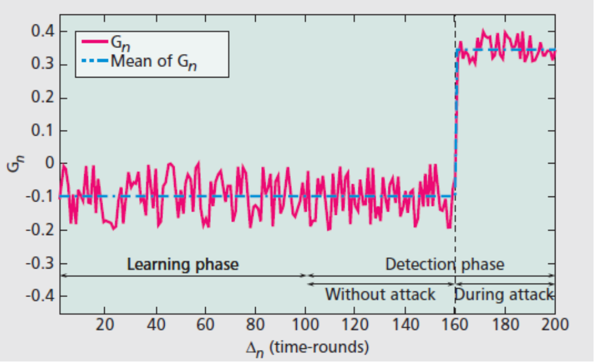

Figure 4: Computing Gn and Mean of Gn

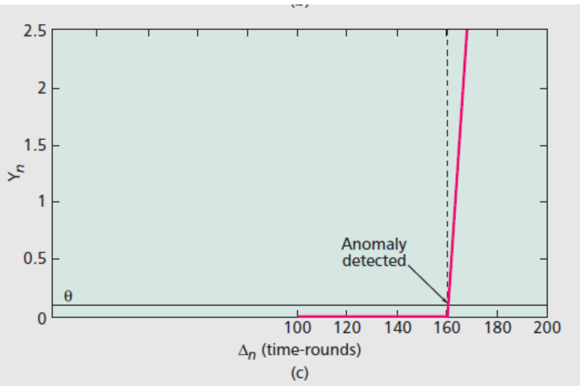

Figure 5: Computing cusum sequence, Yn

V. CONCLUSIONS

Jamming attack is one of the most dangerous attacks in CRNs. In this paper, proposed a simple yet effective detection method, which can be easily implemented in the secondary users' cognitive radio software. The proposed method uses non-parametric cusum algorithm, which offers anomaly detection. By learning the normal mode of operations and system parameters of a CRN, the proposed IDS is able to detect suspicious (i.e., anomalous or abnormal) behavior arising from a jamming attack. In future, this work will perform further investigations on how to enhance the detection sensitivity of the IDS.

REFERENCES

[1] C. Cordeiro, K. Challapali, and D. Birru, "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios," Journal of Communications, vol. 1, no. 1, pp. 38-47, Apr. 2006.

[2] O. Leon, R. Roman, and J. H. Serrano, "Towards a Cooperative Intrusion Detection System for Cognitive Radio Networks", in Proc. Workshop on Wireless Cooperative Network Security (WCNS'11), Valencia, Spain, May 2011.

[3] O. Leon, J. Hernandez-Serrano, and M. Soriano, "Securing cognitive radio networks", in International Journal of Communication Systems, vol. 23, no. 5, pp. 633-652, May 2010.

[4] W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," Journal of Internet Technology (JIT), vol. 12, no. 2, pp.181-198, Mar. 2011.

[5] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, Vol. 5, No. 3, pp. 338-346, Nov. 2007.

[6] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications, vol. 14, no. 5, 85-91, Oct. 2007.

[7] Z. M. Fadlullah, T. Taleb, A. Vasilakos, M. Guizani, and N. Kato, "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis," IEEE/ACM Transactions on Networking, vol. 18, no. 4, pp. 1234-1247, Aug. 2010.

[8] K. Ju and K. Chung, "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks," International Journal of Security and Its Applications, vol. 6, no. 2, pp. 149-154, Apr. 2012.

◈◈◈