Implementation of Intrusion Detection In Cognitive Radio Networks

Avinash Dilendra
Dept.of information technology
IIITM-K, Trivandrum, India
avinash.dilendra@gmail.com

Viza Shesha Shayna Reddy
Dept. of Information Security
IIITM- k, Trivandrum, India
sheshashayanareddy.viza@gmail.com

Mahesh Kumar Porwal
Prof. ECE Deptt
SITE, Nathdwara ,India
porwal5@yahoo.com

Abstract—*Cognitive radio networks (CRN) are intended for utilizing radio spectrum effectively. The network formed by cognitive radio devices achieves dynamic spectrum access by sensing the environment and adapting to the frequencies. But due to its enormous applications in wireless networks demands good security methods to be incorporated in CRN .To overcome these security issues an IDS (Intrusion Detection System) is proposed. The detection of PUE(Primary User Emulation) attack/Jamming is verified by applying the proposed IDS.*

Keywords—*Cognitive Radio Network, Intrusion Detection System, Security*

I. INTRODUCTION

Cognitive radio networks uses Dynamic Spectrum Access, the majority of the attributed spectrum bands(licensed frequency bands)are not used in certain periods of time or in certain geographic areas, causing he called “white space ”while the permitted frequency bands are always congested.

It differs from conventional radio devices in that a cognitive radio can equip users with cognitive capability and reconfigure ability. Cognitive capability refers to the ability to sense and gather information from the surrounding environment, such as information about transmission frequency, bandwidth, power, modulation, etc. With this capability, secondary users (Cognitive Radio devices) can identify the best available spectrum. Reconfigure ability refers to the ability to rapidly adapt the operational parameters according to the sensed information in order to achieve the optimal performance. By exploiting the spectrum in an opportunistic fashion, cognitive radio enables secondary users to sense which portion of the spectrum are available, select the best available channel, coordinate spectrum access with other users, and vacate the channel when a primary user reclaims the spectrum usage right.

It consists of multiple Primary Users (PUs) where a single primary user is a special case. Primary user is defined as a spectrum owner that may trade a spectrum to other Secondary Users (SUs)

Spectrum usage scenario for a secondary user in a cognitive radio network is as follows

- Periodically search for spectrum “white spaces”(i.e. ,fallow bands)to transmit/receive data
- When a primary user is detected in its spectrum band
- Immediately vacate that band and switch to a vacant one
- Vertical spectrum sharing
- When another secondary user is detected in its Spectrum band
- When there are no better spectrum opportunities, it may choose to share the band with the detected secondary user
- Horizontal spectrum sharing CR MAC protocol guarantees fair resource allocation among secondary users

There are several proposals made for tackling security solutions in cognitive radio networks based on different mechanisms like Trust management ,in this paper the network security technique called IDS is tried to implement in CN.

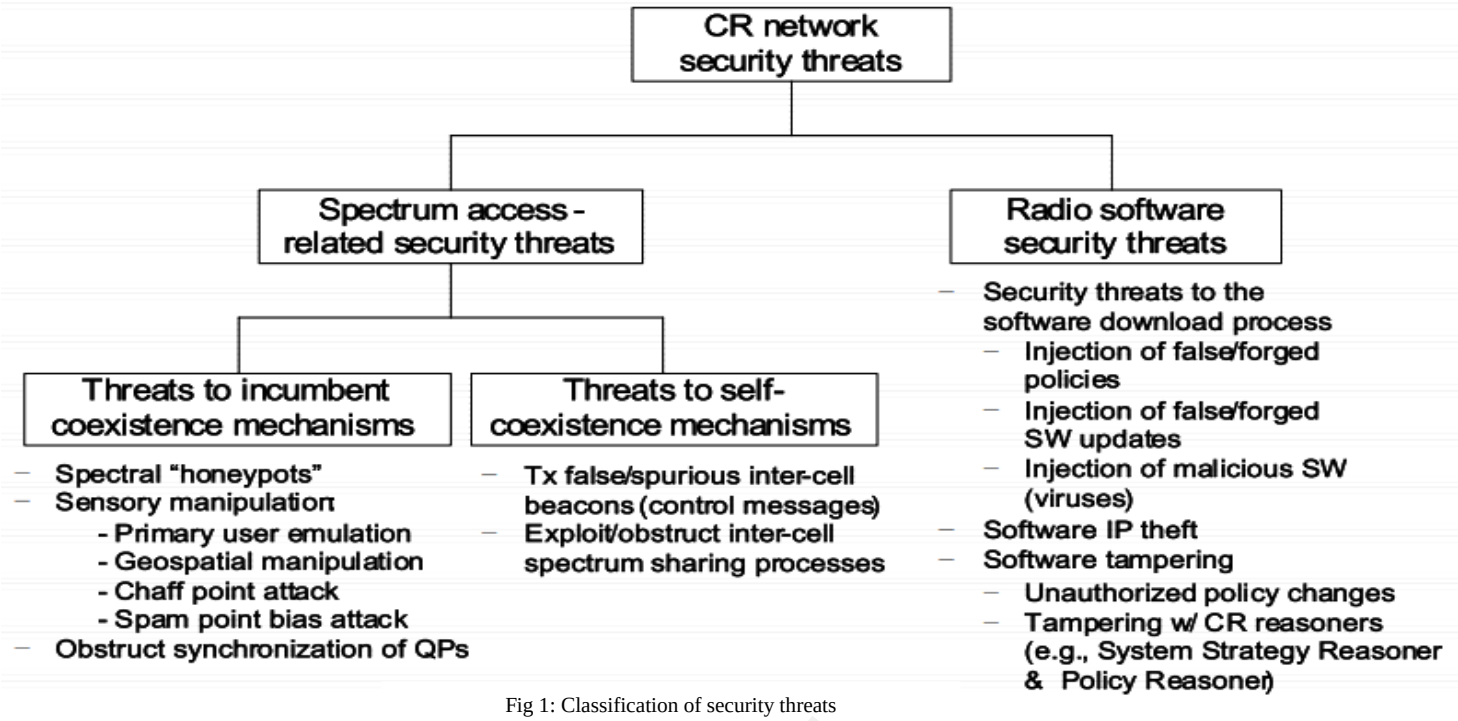

Fig 1: Classification of security threats

II. SECURITY THREATS:

Different types of security threats had been mentioned by several researchers. Some of the common security threats for cognitive radio network are stated here.

A. PUE attack:

In this attack, an adversary secondary user aims at preventing legitimate secondary users from using the white spaces in the spectrum. For example, the adversary may exploit the "quiet periods" of the CRN during which no secondary user should transmit in order to facilitate spectrum sensing. If the adversary transmits during the quiet period, then the other legitimate users will back off by considering that a primary user (i.e. the adversary in this case) is accessing the spectrum. There are a number of other techniques by which the adversary may pretend to be a primary user and trick the legitimate secondary users.

B. Objective function attack:

Cognitive radio is an intelligent radio, which is capable of sensing the spectral environment, learning from previous history, and making smart decisions for adjusting its transmission parameters depending on the current environmental conditions. These parameters are computed by the cognitive engine by solving objective functions

Assume a simple objective function to find the radio parameters, which balance the data rate and Security. Consider the impact when a knowledgeable malicious attacker performs a jamming attack every time a legitimate secondary user attempts to transmit data with high security. This makes the legitimate secondary user's cognitive engine to experience that the network conditions are unfavorable for secure transmission. As a consequence, the legitimate user drops his security level and transmits data with low/no security. Thus, the malicious attacker forces the victim radio to use a low security level, which can be eavesdropped or hacked.

C. Jamming attack:

Like other wireless communication systems, a 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.

In order to detect the above mentioned attacks, there have been many scattered proposals, which have been surveyed in [3, 4]. However, IDS-based attack detection strategy has not yet been studied extensively. In fact, it is important to have a common IDS with a general detection policy to fit (i.e. thwart) most, if not all, the

threats. In the next section, we present our proposed IDS to deal with this issue

D. Attacks to Cooperative Sensing

Cooperative sensing in CRNs [5, 6] allows taking a decision about the presence of a primary user in a given channel, based on the reports provided by a set of CRs. Each secondary user senses the spectrum individually and shares its results with the rest of the nodes in order to improve detection probability. As
a consequence, malicious and selfish behaviors can arise, such as a malicious node which deliberately report false measurements leading to false positives or negatives or a selfish node, which do not cooperate in order to save energy, for instance. Often these attacks are aimed at improving the chances of a successful PUE attack.

1) OF Attacks

Objective Function (OF) attacks [7] are targeted to disrupt the learning algorithm of CR devices. Within a CRN, incumbents control several radio parameters in order to enhance the network performance.

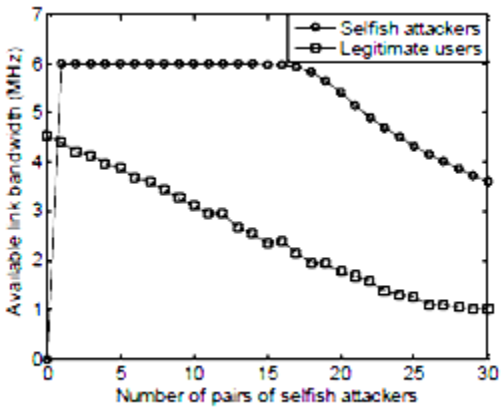

Fig2: Selfish PUE attack

The parameters choice is often done by means of an artificial intelligence algorithm that makes slight modifications of several input factors to find their optimal values that maximize an objective or goal function. An attacker can alter the performance of the learning algorithm to its own profit by intentionally degrading (e.g. by jamming) the channel when some input factors are greater than a certain threshold. As a naive example, the attacker can jam the channel whenever the security of the protocol is set and hence the learning algorithm will conclude that it is better to work without any security.

The threat will affect a CRN actually made of cognitive radios and thus complete IDS for CRN should take it into account.

a) Lion Attack

The Lion attack is a cross-layer attack targeted to disrupt TCP connections by performing a PUE attack in order to force the CRN network to switch from one band to another (frequency handoff). The interruption of Towards a Cooperative IDS for CRNs Communications at specific instants can considerably degrade TCP throughput, or, if the attacker can predict or know the new transmissions parameters to be used by the sender after the handoff, actually turn into a permanent Denial of Service (DoS).

The most famous attack in cognitive radio networks is PUE attack.
Some defense mechanisms for PUE attack are mentioned below

III. IMPACT OF PUE ATTACKS ON CR NETWORKS

The presence of PUE attacks causes a number of troubles problems for CR networks. The list of potential consequences of PUE attacks is:

A. Bandwidth waste

The ultimate objective of deploying CR networks is to address the spectrum under-utilization that is caused by the current fixed spectrum usage policy. By dynamically accessing the spectrum “holes”, the SUs are able to retrieve these otherwise wasted spectrum resources. However, PUE attackers may steal the spectrum “holes” from the SUs, leading to spectrum bandwidth waste again.

B. QoS degradation

The appearance of a PUE attack may severely degrade the Quality-of-Service (QoS) of the CR network by destroying the continuity of secondary services. For instance, a malicious attacker could disturb
the ongoing services and force the SUs to constantly change their operating spectrum bands. Frequent spectrum hand off will induce unsatisfying delay and jitter for the secondary services.

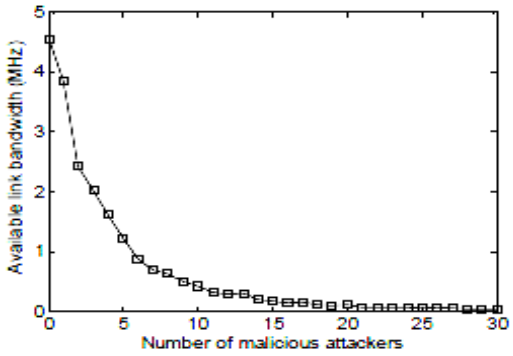

Fig3: Malicious PUE attack

C. Connection unreliability

If a real time secondary service is attacked by a PUE attacker and finds no available channel
when performing spectrum handoff, the service has to be dropped. This real time service is then terminated due to the PUE attack. In principle, the secondary services in CR networks inherently have no guarantee that they will have stable radio resource because of the nature of dynamic spectrum access. The existence of PUE attacks significantly increases the connection unreliability of CR
networks.

D. Denial of Service

Consider PUE attacks with high attacking frequency; then the attackers may occupy many of the spectrum opportunities. The SUs will have insufficient Band width for their transmissions, and hence, some of the SU services will be interrupted. In the worst case, the CR network may even find no channels to set up a common control channel for delivering the control messages

IV. DETECTION APPROACHES FOR PUE ATTACKS

In the literature, some detection approaches against PUE attacks have been presented. The existing detection approaches can be classified into energy detection, Received Signal Strength (RSS) based detection, feature detection, location verification and cooperative detection.

A. Energy Detection:

Energy detection is a simple but widely used approach for spectrum sensing in CR networks. It is also one of the basic approaches for the detection of PUE attacks. By measuring the power level of the received signal
at the SU receiver and comparing it with that from the true PUs, the CR network could judge whether the signal comes from an attacker or not. However, a pure energy detector is not robust enough to tackle an advanced PUE attack.

B. RSS-based Detection

Received Signal Strength (RSS) based detection approach is discussed in [8], where the authors analyze the PUE attack in the CR network without using any location information. Thus, this detection approach does not need dedicated sensor networks. The PUE attackers are assumed to be distributed randomly around the SUs. The authors present an analysis using Fentons approximation and Walds sequential probability ratio test (WSPRT) to detect PUE attacks.

C. Feature detection:

The approach proposed in [9] uses energy detection to identify the existing users in the frequency band. The approach then employs a cyclostationary calculation to represent the features of the user signals, which are then fed into an artificial neural network for classification. As opposed to current techniques for detecting PUE attacks in CR networks, this approach does not require additional hardware or time synchronization algorithms in the wireless network.

D. Location Verification**:**

Two location verification schemes are proposed in [10]. They are called Distance Ratio Test (DRT) and Distance Difference Test (DDT), respectively. In both schemes, dedicated cognitive nodes (SUs or a cognitive BS) with enhanced functionality are involved for location verification. DRT uses a Received Signal Strength (RSS) based method, where two dedicated cognitive nodes measure the RSS of the signal source and calculate the ratio of these two RSS to check whether it coincides with their distances to the true PU (e.g., a TV broadcast tower). Using DDT, the arrival time of the transmitted signal from the source is measured by the two dedicated cognitive nodes. The product of the time difference and the light speed is then compared to the distance difference from the true PU to the two dedicated nodes in order to identify the source.

V. PROPOSED METHOD

The basic idea and some of the modules of an intrusion detection are taken from [11], different types of attacks are explained in the model, but the major threats Jamming/PUE attack is checked for detection by our method.

Jamming attacks interfere with the CRN operation channel forcing the network to switch to another channel with better conditions. If the attack is repeated whenever the CRN switches, the throughput can be degraded or even starved at all. PUE attacks have the same purpose of jamming ones but differ in that they emulate primary transmissions instead of just producing noise. In 802.22,
PUE attacks can be classified depending on the type of the primary signal into TV signal-based and wireless microphone-based attacks based on jamming or wireless microphone-based PUE are detected with an anomaly detection IDS module: jamming/PUE appearing whenever the CRN switches from one channel to another. As a result this module should be able to identify and attacker “following” the CRN. This can be achieved by estimation of the attacker’s current and future position (with a given mobility pattern) and/or its Radio Frequency Fingerprint

(RFF). TV signal-based PUE attacks can be more easily overcome since legitimate

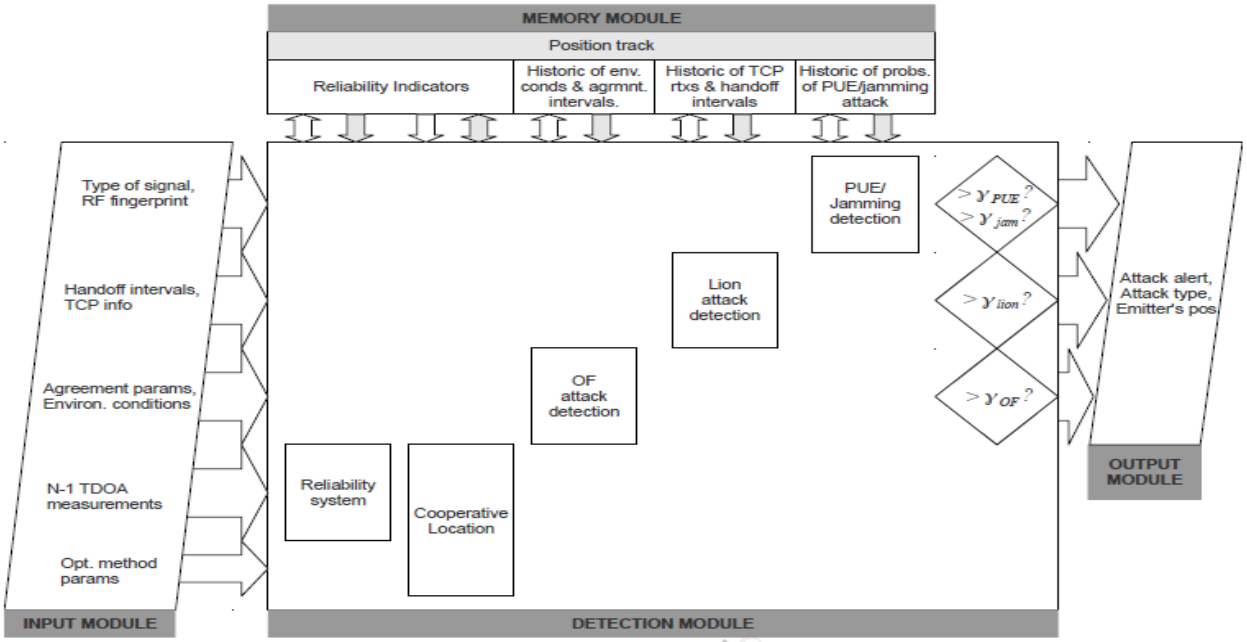

Fig 4: IDS Architecture

TV primary emitters' positions are assumed to be fixed and known. As a result just comparing the estimated position given by the cooperative location module with the database of TV emitters will clearly identify whether it is a PUE attack or not.

Different modules functionality is explained below.

A. Input module

Pure jamming, primary signal (e.g. TV or wireless microphone signals). Jamming would be any signal that is not a primary emission, e.g. TV or wireless microphone transmissions. Mechanisms for detecting primary signals have been widely studied and many proposals. RFF of the primary emitter.

B. Memory module

The estimated position of the primary emitter made by the cooperativelocation method and its associated error. Previously computed probability of jamming /PUE attack for the current emitter (stored by it current position estimation or its RFF). Memory module is Updated probability of jamming/PUE attack for the current emitter.

Output module:

If the probability of being under a jamming attack is above a certain threshold , the module outputs an alert of jamming attack by the current emitter. If the probability of being under a PUE attack exceeds a certain threshold PUE, the module outputs an alert of PUE attack by the current emitter, If any of the previous is true, the module outputs the estimated position of the emitter and its associated error. For simulation of PUE attack using the proposed IDS we made one of the nodes in CRN as a cluster node for storing the information.

VI. RESULTS AND SIMULATION:

The Experiment for the above mentioned method is carried out 12 and 8 number of nodes in the cognitive radio network for different number of malicious attacker nodes 2,5,8 denoted by L1,L2,L3 respectively. The results with graph for PUE attack detection probility and PUE attack false probability are shown. We used CRCN, where CRCN is Cognitive Radio Cognitive Networks(*CRCN*) Simulator based on *ns2* Simulator.

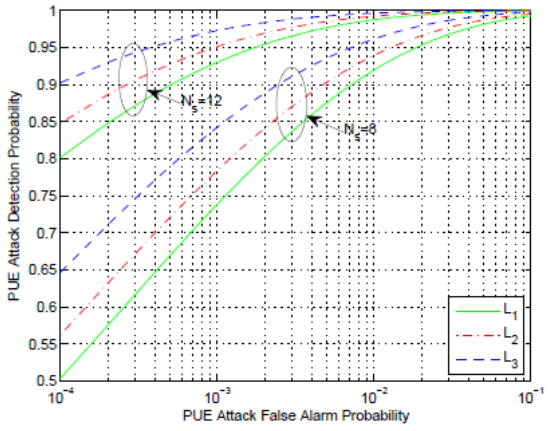

Fig5: Attack detection Vs False alarm probability

The graph says for example Ns(Number of nodes)= 12 and Pf(Probability of false alarm) = 0.1%, the PUE attack detection probabilities are 0.93, 0.95 and0.97, when the PUE attacks are performed for level1 of malicious nodes.

REFERENCE

[1] S. Haykin, "Cognitive radio: Brain-empowered wireless communications,"IEEE J. Sel. Areas Commun., vol. 23, no. 2, pp. 201–220, Feb.2005.

[2] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," Comput. Network., vol. 50, pp. 2127–2159, May 2006.

[3] O. Leon, J. Hernandez-Serrano, and M. Soriano, "Securing Cognitive Radio Networks,"Int'l. J. Commun. Systems, vol. 23, no. 5, May 2010, pp. 633–52.

[4] W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," J. Internet Technology (JIT), vol. 12, no. 2, Mar. 2011, pp. 181–98.

[5]. Song, C., Zhang, Q.: Achieving cooperative spectrum sensing in wireless cognitive radio networks. SIGMOBILE Mob. Computer. Commun. Rev. 13(2) (2009) 14–25

[6]. Mishra, S., Sahai, A., Brodersen, R.: Cooperative sensing among cognitive radios. In: Proceedings of IEEE International Conference on Communications, ICC'06. Volume 4. (June 2006) 1658 –1663

[7] Chen, R., Park, J.M.: Ensuring trustworthy spectrum sensing in cognitive radio networks. In: 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR). (September 2006) 110–119

[8] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in Proc. IEEE International Conference on Communications (ICC), 2009.

[9] D. Pu, Y. Shi, A. V. Ilyashenko, and A. M. Wyglinski. "Detecting primary user emulation attack in cognitive radio networks," in Proc. IEEE Global Telecommunications Conference, Dec. 2011.

[10] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in Proc. IEEE Workshop Networking Technologies for Software Defined Radio Networks, Sept**.** 2006.

[11] Olga Le´on1, Rodrigo Rom´an2, and Juan Hern´andez-Serrano1 "Towards a Cooperative Intrusion Detection System for Cognitive Radio Networks"