International Journal of Computer Network and Security (IJCNS)
Vol 6. No.1 – Jan-March 2014 Pp. 59-65
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0975-8283

DETECTION OF MULTIPLE SELFISH SECONDARY USERS IN COGNITIVE RADIO NETWORK USING CRV

Ajantha.M, Mr. Suresh Kumar. P,
Arunai Engineering College, Thiruvannamalai,
ajanthamuthu@gmail.com, suresh8680@gmail.com

ABSTRACT

Cognitive Radio (CR) is a network technology that can automatically sense the underutilized spectrum resources. A Selfish Secondary User (SSU) can occupy all or part of the resources of multiple channels, prohibiting other cognitive radio users from accessing these resources. These selfish attacks degrade the performance of a CR network significantly. In the previous method, many algorithms are used to detect the selfish node, for that they had assumed only one neighboring selfish user in the network. The sensing accuracy is less reliable. In the proposed Credit Risk Value (CRV) method, more than one selfish Secondary User in a network can be detected. It eliminates the selfish attack and increases the sensing accuracy and security in the cognitive radio network. It also reduces the detection delay.

Index Terms - Cognitive Radio, Primary User (PU), Secondary Selfish User, Legitimate Secondary User. Credit Risk Value.

1. INTRODUCTION

The recent development in wireless communication has led to the problem of growing spectrum scarcity. As there are large numbers of wireless communication devices, we are now facing problems in the utilization of spectrum resources. Due to increasing spectrum demand for new wireless applications the available radio frequency spectrum has become scarcer. A significant amount of allocated radio frequency spectrum is used sporadically, causing underutilization of spectrum. Cognitive radio technology provides a promising solution for the spectrum scarcity issues in wireless networks. By using this technology the scarcity of bandwidth can be avoided. It allows the efficient use of the finite usable radio frequency spectrum.

In cognitive radio terminology, Licensed users i.e. Primary users are defined as users who have right to use the spectrum band whereas unlicensed users/Secondary users are defined as users who can use the spectrum which is temporarily not used by licensed users. Also it does not cause interference to the licensed users. The security concerns of cognitive radio have received more attentions as the inherent properties of CR networks would pose new challenges to wireless communications. In CR network, an attack can be defined as an activity that can cause interference to the primary users or licensed users.

Cognitive radio technology arises due to the inefficient utilization of radio frequency spectrum (3 KHz to 300GHz) i.e. for example, cellular frequencies are widely used and frequencies for military and emergency communication are used insufficiently.

It helps the unlicensed users to utilize the maximum available licensed bandwidth without affecting the operation of primary users. While satisfying the given PU requirement this CR improves the secondary performance of the underlay models under the stringent power constraints.

In CR cycle, a cognitive radio scans the radio frequency spectrum, gathers information, and then identifies the vacant channels. Initially the properties of the vacant channels are evaluated using spectrum sensing. . Then, the appropriate spectrum band is chosen according to the spectrum characteristics and user requirements.

After determining the operating frequency band the communication can be carried out. The four main functions of cognitive radio are as follows: Spectrum sensing, Spectrum sharing, Spectrum decision, Spectrum mobility.

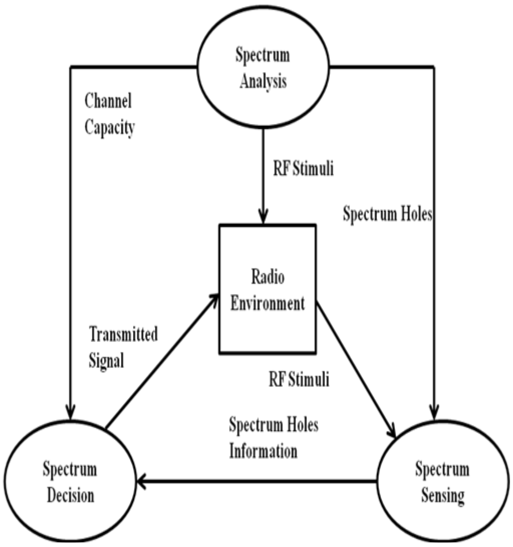

Figure.1. Cognitive Radio Cycle

The fundamental task of CR network is to detect the licensed users, if they are present then identifies the available spectrum. This process is called spectrum sensing. Several spectrum sensing techniques have been proposed so far which can be categorized into three general groups, energy detection, coherent detection and cyclostationary feature detection.

The energy detection technique is known to be optimal when the only information available about the primary received signal is the noise power density and the received primary signal samples are independent and identically distributed. In the case of Coherent detection, an Eigen value-based algorithm which exploits the ratio of the maximum and minimum Eigen values of the sample covariance matrix can be used. If some other features of the primary signal such as the modulation scheme, pilot information, synchronization symbols, etc. are available at the cognitive radio receiver.

Feature detector may be exploited in order to have more robust sensing. However, due to its low computational (and hence implementation) complexities and its fast detection ability, energy detection is widely deployed as the underlying detection scheme. However, all of these strategies have been previously restricted to sensing narrowband channels. The framework referred here for spectrum sensing is Multiband Sensing Time Adaptive Joint Detection(MSJD).Wide band Gaussian channel is divided into number of non overlapping narrowband sub channels and find the detector parameters individually and then the detector parameters and sensing time are jointly optimized. For accessing the spectrum in adaptive manner, SUs must constantly monitor the local spectrum and sense spectrum reliability to detect spectrum holes so as to avoid harmful interference to the PUs.

2. SECURITY ISSUES IN COGNITIVE RADIO NETWORK

A. Security Attack Types

Due to the nature of CRN, security became a problem at every step (Spectrum Sensing, Location Identification, Spectrum sharing, etc.) of its functionality. The security problems will occur in different ways.

- ➢ False detection (sensing) and misdetection of primary signal may happen due to denial of service or malicious user pretends as the primary signal.
- ➢ Malicious user can control the environment.
- ➢ Available spectrum used by the cognitive users can be prevented by an (primary signal sensing mechanism).
- ➢ The unauthorized data could be accessed or modify/inject the false data by an attacker (integrity of data is required).

Cross-layer attacks are possible in CRN. There is a need to be given individual attention for such attacks. Jamming on routing information happens due to lack of common control channels. Traffic analysis attack on data privacy and location privacy will be avoided by authentication and controlling the access rights of cognitive user. The other attacks include false feedback of information from one group of cognitive users to mislead the different group of cognitive users. This consequence ends to mislead the detection of primary signal.

Network Endo-Parasite (NEP) attack avoids the selection of the right channel by the other cognitive users. The NEP attack is played by a different group of cognitive users. The objective function attack controls a large number of radio parameters. According to Clancy and Georgen secure communication with low or high power has provided the weights. The channel gain depends upon the weight rate. The dishonest users will mislead the other users to gain access. Further, they mislead the honest user to misdetection of the primary signal with the introduction of extra noise.

The common control problem involves the exchange of security keys between the nodes. The authentication among the nodes provides confidentiality and integrity of the transactions. This method provides the security and the hidden terminal problem still remain. The jamming problem, hidden terminal problem, exchange of keys between the nodes and malicious user acts can be eliminated by using the cloud application. The security to cloud still remains an open problem.

Providing Security is the biggest task in Cognitive Radio Network, Security solutions should be effective by providing best security and consuming less resources like energy, computational power and memory. After the nodes get compromised it performs various attacks as follows:

- Bad Mouthing attack: It propagates negative information about Good nodes.
- Good Mouthing attack: It propagates positive information about Bad nodes.
- Sniffing attack: It overhears the Valuable data from by other nodes
- Dos Attack: It prevents any part of WSN from Functioning.
- Black Hole attack: Drop the packets and attract the traffic to be routed as Shortest Route.
- Intelligent Behavior attack: According to this attack the nodes may provide good or bad services according to the threshold of trust rating.
- Sybil Attack: Replica the information and Clone Several Nodes.
- Sink Hole Attack: It attracts nearby Traffic through Comprised node.
- White washing attack: Using this, the nodes which have their trust value less than the threshold value will try to re-enter into the system.

To provide secure network the need of trust management in encountered. Trust is a security mechanism that can be used to detect the unexpected behavior of nodes in the network. There is various trust techniques used to detect the nodes and eliminate the selfish nodes.

Primary user emulation attack is one of the common security threats in CRN. Chen et al proposed a transmitter verification scheme called LocDef (localization based defense) that verifies the received signal based on location and characteristics. They concluded that the signal disruptive process will be eliminated by incorporating the LocDef process into spectrum sensing processes. They showed through simulations that LocDef scheme is an effective program and can be employed in a hostile environment

Depending on the motivation of the attack, PUE attacks can be classified into two types:

Disruptive attacks: The driving force behind this class of attacks is simply to disrupt transmissions of protocol compliant SUs rather than any need for additional radio resources for the MA itself. Hence, this attack is similar to the jamming attacks.

Selfish attacks: In contrast to the disruptive attacks, the attack intent in this case is to actually occupy the spectrum band when the SUs vacate it. In that sense, this attack is associated with a positive benefit.

The motivations vary depending upon the attacker. The selfish nature of a cognitive user projects he/she as the primary user to use the spectrum with higher priority. They modify the spectrum sensing parameters for selfish advantage. The selfish user can prevent other users from using the spectrum by jamming or with DOS. The DOS can be created using various authorized and unauthorized waveforms with a low-cost consumer device. The selfish users can be controlled through access permissions and authentication. Further, by using channel sensing algorithms we can control the cognitive users from interference.

B. Security Challenges in CRN

Primary user authentication: An attacker may transmit its signal with high power or mimic specific features of a primary user's signal in CRN's (e.g., use the same pilot or synchronization word) to bypass the PU detection methods. Consequently, secondary users may incorrectly identify the attacker's signal as a PU's signal and will not use the relevant channels. Such attacks are called primary user emulation (PUE) attacks.

Secondary user authentication: When an FC (or a secondary user) collects sensing reports from other users; it should authenticate the identities of the secondary users. Otherwise, a potential attacker may forge the identity of a secondary user to send false sensing reports.

Sensing report authentication: Although the secondary users' identities can be authenticated during the sensing report aggregation process, it is possible that some secondary users are malicious and report unauthentic sensing results as an internal attack. This attack is called a spectrum sensing data falsification (SSDF) attack. Hence, the sensing reports of each secondary user should be authenticated as well.

C. Existing Proposals for Securing Cognitive Radio Networks

In this section, we summarize the existing works related to the security problems in CRNs. All of these works mainly focus on the PUE, SSDF, and incentive problems, and none of them notice the privacy problems in CRNs.

Thwarting a PUE attack: The PUE attack is introduced for the first time in an article, where a location distinction approach is suggested to distinguish an attacker's signal from a PU's signal and therefore mitigate a PUE attack. This approach uses received signal strength (RSS) to estimate the source location of a signal, and decides whether the signal is from the PU based on prior knowledge of the PU's location.

A link signature is adopted to authenticate the PU's signal. A helper node is proposed to inform a secondary user about the link signature of the PU at its location. After that, when the attacker launches PUE attack, the secondary user is able to detect it by comparing the link signature between the PU and the received signal. Thwarting an SSDF attack: An abnormal misbehavior detection scheme is proposed. This scheme is based on the assumption that the spectrum usage pattern of the PU is known. A secondary user whose sensing reports conflict with this pattern is regarded as malicious. When the ON-OFF ratio of the spectrum usage pattern approximates to 1 the effectiveness of this scheme decreases.

A machine-learning-based scheme is proposed, which does not rely on any specific signal propagation model. In this scheme, a trusted initial set of signal propagation data in a region is taken as input to build a support vector machine (SVM) classifier. This is then used to detect integrity violations. The proposed user-centric misbehavior detection scheme (UMDS) is based on the fact that a secondary user tends to trust its own sensing reports rather than others'. A user chooses its own sensing reports over multiple target channels as the trust base and evaluates other users' trust levels. It regards users with fairly different sensing reports as malicious. The advantage of UMDS is that it also performs well in attacker-dominant situations.

Stimulating selfish behaviors in collaborative sensing: Selfish users in collaborative sensing may not be willing to contribute to cooperation, because scanning the spectrum and broadcasting the sensing results will cost them extra time and energy. There are quite a few previous proposals addressing selfish behaviors in CRNs. For a free rider, not to share sensing result is proved to be the dominating strategy in non-incentive CRNs. Besides, some classic incentive strategies (Tit-for-Tat, 2-player Trigger, etc.) are demonstrated to be improper for enhancing collaborative spectrum sensing, since punishing a specific node without affecting others will be a challenging problem.

In order to thwart selfishness, an N player horizontal infinite game is adopted to analyze several incentive strategies, such as Grim Trigger and some improved strategies under random errors are proposed to achieve better system performance. An evolutionary game is adopted to study how to collaborate for a secondary user when there are selfish users. Evolution dynamics is used to analyze whether the secondary user should choose to be a free ride at the risk of no contributor in the network, at some cost. Learning algorithms are also proposed to enable the secondary user to have an evolutionary stable strategy based on their own payoff observations.

3. SYSTEM ANALYSIS AND DESIGN

Selfish attacks are different depending on what and how they attack in order to preoccupy CR spectrum resources. There are three different selfish attack types.

A. Attack Type 1

Type 1 attack is designed to prohibit a Legitimate SU (LSU) from sensing available spectrum bands by sending faked PU signals. The selfish SU (SSU) will emulate the characteristics of PU signals. A legitimate SU who overhears the faked signals makes a decision that the PU is now active and so the legitimate SU will give up sensing available channels. This attack is usually performed when building an exclusive transmission between one selfish SU and another selfish SU regardless of the number of channels. There must be at least two selfish nodes for this type of attack.

B. Attack Type 2

Type 2 attacks are also a selfish SU emulating the characteristics of signals of a PU, but they are carried out in dynamic multiple channel access. In a normal dynamic signal access process, the SUs will periodically sense the current operating band to know if the PU is active or not, and if it is, the SUs will immediately switch to use other available channels. In this attack type, by launching a continuous fake signal attack on multiple bands in a round-robin fashion, an attacker can effectively limit legitimate SUs from identifying and using available spectrum channels.

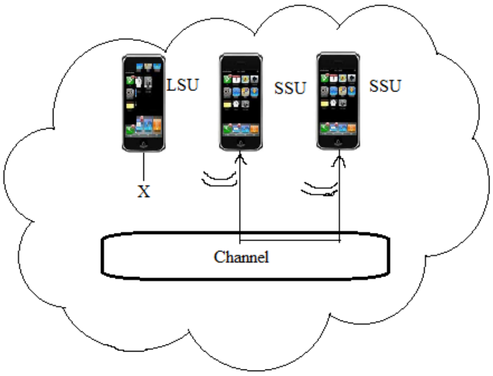

Figure 2. Signal Fake Selfish Attack

C. Attack Type 3

In Type 3, called a channel preoccupation selfish attack, attacks can occur in the communication environment that is used to broadcast the current available channel information to neighboring nodes for transmission. We consider a communication environment that broadcasting is carried out through a Common Control Channel (CCC) which is a channel dedicated only to exchanging management information. A selfish SU will broadcast fake free (or available) channel lists to its neighboring SUs, as illustrated in Figure 4 Even though a selfish SU only uses three channels, it will send a list that it needs all five occupied channels. Thus, a legitimate SU is prohibited from using the two available channels. Detection of existing selfish technologies is likely to be uncertain and less reliable, because they are based on estimated reputation or estimated characteristics of stochastic signals.

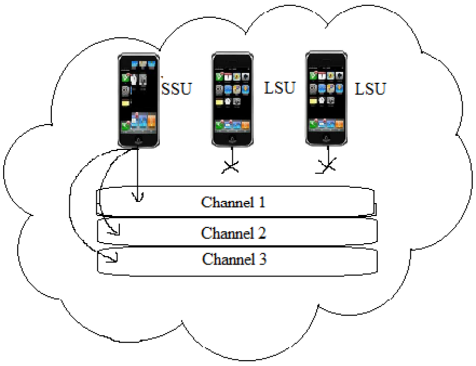

Figure 3. Signal Fake Selfish Attack in Dynamic Signal Access

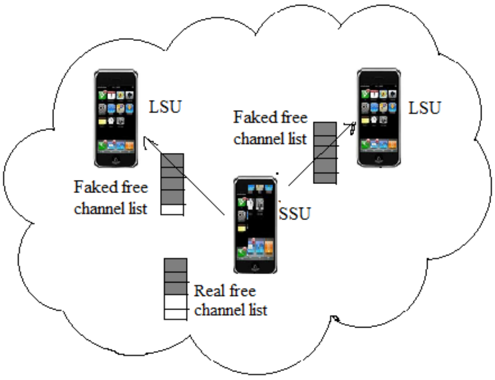

Figure 4. Channel preoccupation Selfish Attack

In this paper, all the attacks are assumed to be in the same network and these attacks are detected and eliminated from the network. In all the papers, which we have discussed earlier, they have assumed that their network consists of only one selfish user. But in practical there may be multiple selfish users in the network. So in this paper multiple selfish users are detected from the network and are eliminated.

Credit Risk Value is the value given to each and every node based on the initial energy of the particular node. When this value is above 10, it is considered as the selfish node and if it is below 10 then it was considered as a non selfish node. The selfish node indicates that the node provides false information about the number of packets needed and number of channels used. By eliminating these nodes we can improve the security in the network and also we can reduce the detection delay in the network.

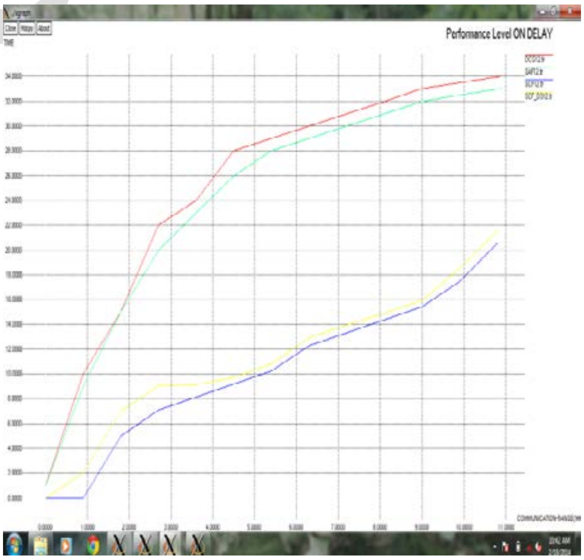

Figure 5.   Performance Level on Delay

4. SIMULATION RESULTS

In order to improve the throughput and the detection accuracy, experiments are carried out by considering many selfish secondary users and the performance are analyzed by means of the result. One hundred secondary users were used in this experiment. Five neighboring SUs in a CR network achieve very high accuracy regardless of selfish SU concentration. Four neighboring SUs also provide very high accuracy and are trivially influenced by the density of selfish SUs. Though, we notice that two SUs in a neighbor are negatively affected by the density of selfish SUs. As a result, more than three SUs in a neighbor of a CR network are recommended in order to avoid selfish CR attacks.

In figure 5, the number of bits transmitted at a particular time and the delay in detecting each and every selfish user is shown by means of the performance analysis graph. The figure 6 shows the detection rate of selfish secondary user when the density of secondary user increases. As the number of secondary user density increases then the detection accuracy also increases. The routing performance of each and every secondary user is analyzed and is provided in the graph.

5. CONCLUSION

The proposed work identifies all the selfish users in cognitive radio networks. Reliable and simple computing technique can be well fitted for practical use in the future. Our approach is designed for cognitive radio networks, which makes use of network advantages such as autonomous and cooperative characteristics for better detection reliabilities. Credit Risk Value is proposed to do analysis of more than one selfish SU in a neighbor, which gives more detection accuracy and less detection accuracy.

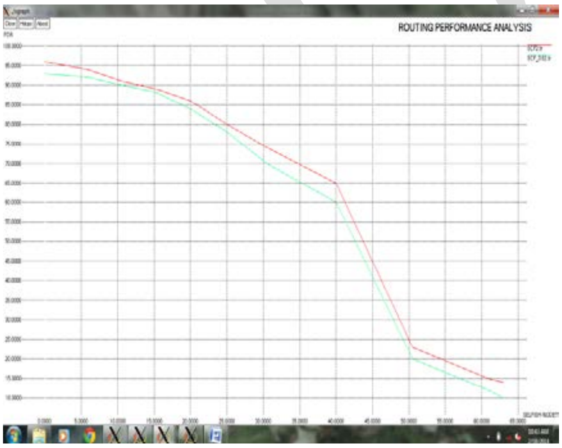

Figure 6. Routing Performance Analysis

ACKNOWLEDGMENT

First of all I express my helpful thanks to GOD ALMIGHTY for his presence and abundant grace in giving knowledge, wisdom and strength to take up this project and complete it on time. I take this opportunity to express thanks to my parents, for their sincere support and efforts they took to complete this work completely. I convey my thanks deep sense of gratitude to our Head Of the Department and my internal guide Mr.P.SURESHKUMAR., M.E., Department of Electronics And Communication Engineering (PG Studies), for his timely suggestion, valuable advises and encouragement during this phase and for guidance and support in completing my project.

REFERENCES

[1] Hang Hu, Youyun Xu, Zhiwen Liu, Ning Li and Hang Zhang," Optimal Strategies for Cooperative Spectrum Sensing in Multiple Cross-over Cognitive Radio Networks", KSII Transactions on Internet and Information Systems Vol. 6, No. 12, Dec 2012.

[2] Haythem A. Bany Salameh, Marwan Krunz,, Ossama Younis, IEEE," Cooperative Adaptive Spectrum Sharing in Cognitive Radio Networks", IEEE/ACM Transactions On Networking, Vol. 18, No. 4, August 2010.

[3] Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu, Fellow, IEEE," Handling Selfishness in Replica Allocation Over a Mobile Ad Hoc Network", IEEE Transactions On Mobile Computing, Vol. 11, No. 2, February 2012.

[4] Muheet Ahmed Butt and Majid Zaman," Cognitive Radio Network: Security Enhancements", Journal of Global Research in Computer Science, Volume 4, No. 2, February 2013.

[5] R. Chen, J.M. Park, and J. H. Reed.(Jan. 2008), "Defense against Primary User Emulation Attacks in Cognitive Radio Networks", IEEE JSAC, vol. 26, no. 1, pp. 25–36.

[6]S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen .(2012), "Location privacy preservation in collaborative spectrum sensing", Proc. of INFOCOM'12.

[7] X. Tan and H. Zhang. (Sept. 2012), “A CORDIC-Jacobi Based Spectrum Sensing Algorithm for Cognitive Radio”, KSII Trans. Internet and Info. Systems, vol. 6, no. 9, pp. 1998–2016.

[8] Zhaoyu Gao, Haojin Zhu, Shuai Li, And Suguo Du, Shanghai Jiao Tong University Xu Li, Inria Lille,” Security And Privacy Of Collaborative Spectrum Sensing In Cognitive Radio Networks”, IEEE Wireless Communications, December 2012.

[9] Z. Dai, J. Liu, and K. Long. (Oct. 2012), “Cooperative Relaying with Interference Cancellation for Secondary Spectrum Access”, KSII Trans. Internet and Information Systems, vol. 6, no. 10, pp. 2455–72.

[10] Z. Gao Et Al. (2012), “Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks”, IEEE Wireless Commn. vol. 19, no. 6, pp. 106–12.

[11] Z. Jin, S. Anand, K.P. Subbalakshmi.(2009),” Detecting Primary User Emulation Attacks In Dynamic Spectrum Access Networks”, IEEE INFOCOM’12, pp. 729–37.