International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Enhanced Pue Detection and Selfish Secondary User Detection Method in Cognitive Radio Networks

Zakiyya M A

Assistant Professor on Contract, KBMGCT Chokli

Abstract:
In cognitive radio networks (CRNs), cognitive radio (CR) nodes adaptively access the spectrum aiming to maximize the utilization of the scarce resource. A new security threat known as the Primary User Emulation attack raises a great challenge to CRNs. In the proposed method an innovative technique is introduced which is called as Enhanced PUE detection method and selfish secondary user detection method. In the Enhanced PUE detection, PUE detection approach can be extended to address the scenario with multiple classes of PUs that have different SAP features. The Selfish Secondary User detection method, attacks are detected by the cooperation of other legitimate neighboring Secondary Users.

Keywords: Cognitive Radio Network (CRN), Primary User Emulation (PUE) attack, primary user (PU), secondary user (SU), Signal Activity Pattern Acquisition and Reconstruction System (SPARS), Signal Activity Pattern (SAP)

INTRODUCTION

Cognitive Radio Network (CRN) is an innovative approach to wireless engineering in which radios are designed with an unparalleled level of intelligence and alertness. This advanced technology enables radio devices to use spectrum (i.e., radio frequencies) in entirely different and stylish ways. Cognitive radios have the ability to monitor, analyze, and detect the conditions of their operating atmosphere, and dynamically alter their own characteristics to best match those conditions. In a cognitive radio network (CRN), secondary users (SUs), i.e., unlicensed users, are envisioned to be able to sense and analyze their environment, learn from the environment variations, and access the licensed bands to achieve highly reliable communications without interference. Specifically, the main functions of CR technology in CRNs include: (1) spectrum sensing, i.e., to determine the available spectrum and detect the presence of PUs; (2) spectrum management, i.e., to select the best available channel spectrum sensing to meet users' communication requirements; (3) spectrum sharing, i.e., to coordinate access to this channel with other users; and (4) spectrum mobility, i.e., to vacate the channel when a PU is detected.

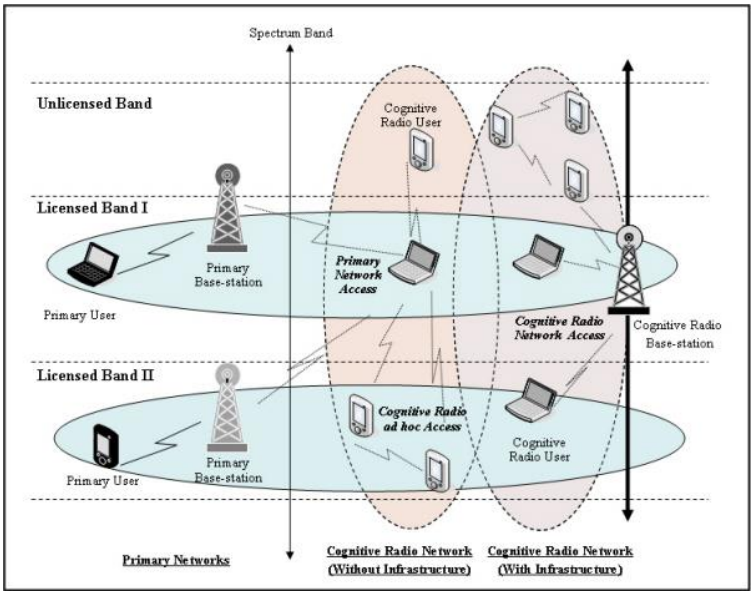

Fig 1: Architecture diagram of Cognitive Radio Network

Primary User Emulation Attacks on CRNs: Security threats related to the cognitive capability include attacks launched by adversaries that mimic primary transmitters (i.e., primary emulation). When a primary user (PU) is detected in a given band, all SUs avoid accessing that band. In primary emulation (PE) attack, malicious secondary users (SU) tries to gain priority over other SUs by transmitting signals that emulate the characteristics of a PU. An adversary may have two different motives for launching PE attacks: selfish and malicious. Selfish motivation is to gain an unfair advantage in accessing spectrum in the spectrum sharing paradigm of dynamic spectrum access (DSA). Because SUs will avoid accessing a band if an incumbent signal is sensed in the band. An attacker can avert and dominate a band if it manages to fool others into believing that it is a PU. The malicious motivation is to suppress legitimate SUs from accessing spectrum, thereby causing Dos. Both types of PE attacks can drastically decrease the available bandwidth opportunities that each legitimate SU can detect.

RELATED WORK

The existing system discussed in [3] proposed a novel PUE Detection system termed Signal Activity Pattern Acquisition and Reconstruction System (SPARS), which collects the signal activity pattern (SAP) of a transmitter as a series of ON and /or OFF period of a transmitter along the time. Existing method solves the primary user emulation attack but the problem is this method only consider one class of PUs that have similar SAP features, i.e., with similar distributions for the ON or OFF periods. The multiple classes of primary users are not considered.

Furthermore, the selfish users act as secondary users and occupy the more number of channels. The defense against the Primary User Emulation Attack is studied in [6] using the scenario of unknown channel statistics. The technique adopted in [6] is a passive defense policy and modeled the dogfight in spectrum as a zero –sum game. Author designed a good defending strategy for the honest Secondary Users using the theories of game and learning. A DECLOAK, is presented to identify the PUE attacks in [9] which utilizes a nonparametric Bayesian approach for detecting PUE attacks. The authors in [10-12] proposed different methods to detect the Primary User Emulation attacks using different techniques.

EXISTING METHODOLOGY

In the existing system, in order to detect primary user emulation attacks, a novel PUE detection system, termed Signal activity Pattern Acquisition and Reconstruction System (SPARS) is presented. In the ensuing discussion, if not otherwise noted, an attacker refers to a PUE attacker, a signal refers to a PU signal, and a transmitter refers to a PU signal transmitter, which may be a PU or an attacker. A Signal Activity Pattern of a transmitter is defined as a series of ON and or OFF periods of the transmitter along the time. An ON period refers to the duration of a busy period of PUs. It acquires the SAP of a transmitter through spectrum sensing, and compares it with SAPs of PUs through a SAP reconstruction model. If the observed SAP is not 'like' the SAPs of PUs, which is measured by the reconstruction error, then the transmitter is an attacker.

The major drawback of the existing system is that which does not consider multiple classes of PUs, and also selfish secondary users attack detection. It concentrates on only a single class of PUs that have similar SAP features, i.e., with similar distributions for the ON/OFF periods.

PROPOSED METHODOLOGY

In the proposed system, an innovative technique is introduced which is called Enhanced PUE detection method and selfish secondary user detection method. In the Enhanced PUE detection, PUE detection approach can be extended to address the scenario with multiple classes of PUs that have different SAP features. Also, the secondary users also sometimes misbehave in the network. So, selfish secondary user detection method is also considered.

The contributions are:

For detecting multiple classes of primary user attackers, the SPARS is extended for the PUE detection in which different classes of PUs have different signal activity patterns. Specifically, SPARS is extended to classify an observed SAP to see if it belongs to a certain class of PUs. If yes, then this SAP is from a PU. Otherwise, it is from an attacker. To achieve this objective we have to examine the structure of the weights in the reconstruction of a SAP, in addition to the reconstruction error.

For the selfish secondary user detection, this method will detect the attacks of selfish SUs by the cooperation of other legitimate neighboring SUs. All neighboring SUs exchange the channel allocation information both received from and sent to the target SU, which will be investigated by all of its neighboring SUs. The selfish attacks of SUs are focused toward multiple channel access in cognitive radio ad-hoc networks. Assume that an individual SU accommodates multiple channels. Each SU will regularly broadcast the current multiple channel allocation information to all of its neighboring SUs, including the number of channels in current use and the number of available channels, respectively. The selfish SU will broadcast fake information on available channels in order to preoccupy them. The selfish SU will send a larger number of channels in current use than real in order to reserve available channels for later use.

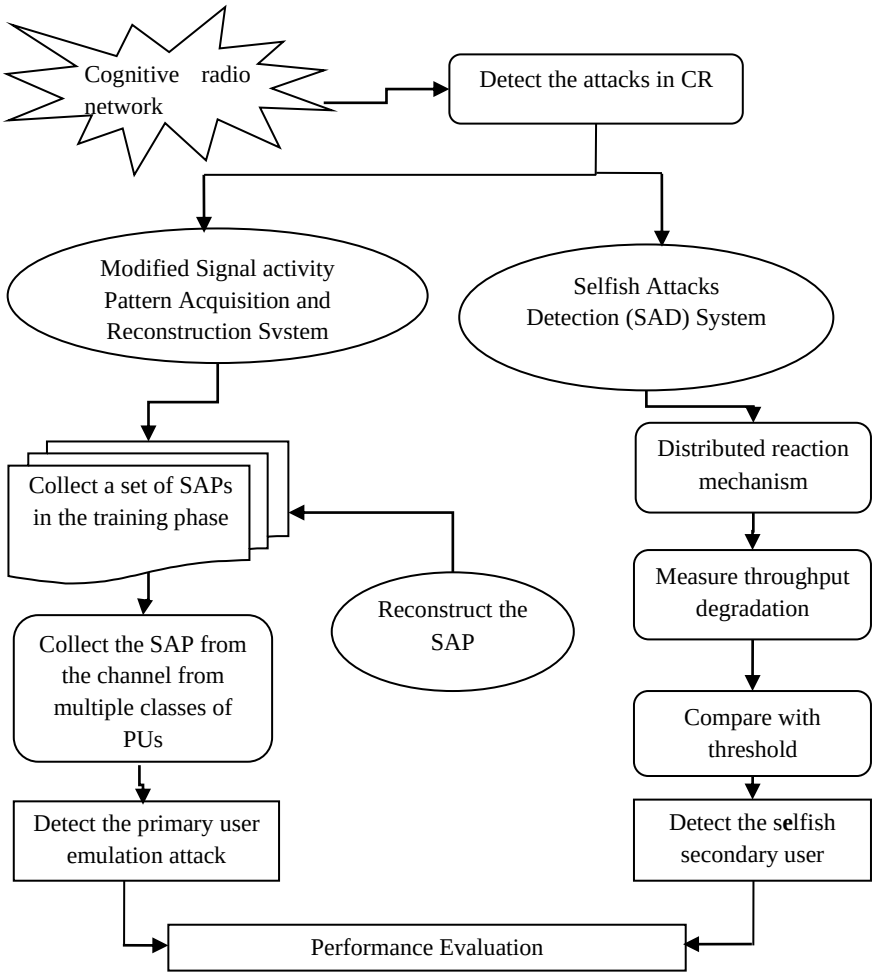

Fig 2: Architecture View of the proposed system

A. Enhanced PUE detection Method (Modified SPARS)

In the Enhanced PUE detection method, the multiple classes of primary users are detected. The existing SPARS method is extended to detect the multiple and different classes of the primary users. Particularly, SPARS is extended to classify an observed SAP to see if it belongs to a certain class of PUs. If yes, then this SAP is from a PU. Otherwise, it is from an attacker. To achieve this objective, we have to examine the structure of the weights in the reconstruction of a SAP, in addition to the reconstruction error.

Algorithm 4: Modified SPARS

1. If CRN is in the initial setup phase then
2. Passively carry out spectrum sensing to collect m SAPs for multiple classes $X_{i1},..X_{im}$ on candidate channels, which are used in the training data set X.
3. Apply Algorithm 1 in [3] on X with parameters λ, c and n obtain the bases $B^* = [B_1^*,..B_n^*]$ and SSEs $\eta_1,..\eta_m$
4. End if
5. Loop
6. For a SAP for multiple classes Y collected from a candidate channel, solve problem (20) in [3] to get W.

7. Assign weight value for every classes of SAP
8. Compute SSE ζ by (21) in [3]
9. Compute $\hat{\mu}$ and $\hat{\sigma}$ by (22) in [3] using η_i from Algorithm 1
10. Compute θ by (25) in [3]
11. Compute $\hat{\gamma}$ by (23) in [3]
12. If $\zeta > \hat{\gamma}$ then
13. SAP Y is from an attacker. ALARM=YES
14. Else
15. SAP Y is from a PU. Alarm=NO
16. End if
17. End loop

B. Selfish Secondary User Detection Method

In a cognitive radio network, the common control channel (CCC) is used to broadcast and exchange managing information and parameters to manage the CR network among secondary ad-hoc users. The CCC is a channel dedicated only to exchanging managing information and parameters. A list of current channel allocation information is broadcast to all neighboring SUs. In reality, a list is broadcast once, and it contains the channel allocation information on all of the neighboring nodes. The SU will use the list information distributed through CCC to access channels for transmission. A selfish secondary node will use CCC for selfish attacks by sending fake current channel allocation information to its neighboring SUs. In addition, simultaneously all of the neighboring nodes sum the numbers of currently used cannels sent by the target node, T Node. Individual neighboring nodes will compare the summed numbers sent by all neighboring nodes to the summed numbers sent by the target node to check if the target SU is a selfish attacker. Thus, all neighboring nodes will know if the target SU is a selfish attacker or not. This detection mechanism is carried out through the cooperative behavior of neighboring nodes. Once a neighboring SU is chosen as a target node and the detection action for it is completed, another neighboring SU will be selected as a target node for the next detection action.

Distributed Reaction Mechanism: In this mechanism, consider with N nodes where all nodes are genuine, i.e. they correctly follow BEB. A lower bound on the channel access probability of a node is derived (and thus its throughput). Every time a node chooses a back off value uniformly at random from [0….CW-1], it could choose CW-1 with probability $\frac{1}{CW}$. Let node *A* chooses back off values in this way every time. The access probability of node *A*, denoted τ_A is minimum since the node chooses the largest backoff value in the allowed interval every time. Using Markov Chain analysis, characterize the steady state probability τ_{min}.

$$\frac{\tau_{min}}{\tau} = \frac{1}{2} + \frac{(1-2p)}{2W_0[(1-p)-p(2p)^m]} \quad (1)$$

An adaptive and distributed reaction algorithm is designed for the genuine nodes to react against mildly selfish misbehaviors. Each genuine node measures its throughput degradation with respect to its saturation throughput share T_0 given. The reaction aggressiveness is made proportional to the level of suspected selfishness, and in most cases, the reaction is not as strong so as to lower the overall network throughput tremendously. Let us consider the saturation throughput scenario with N nodes. Using Bianchi's analysis let the individual fair throughput of each node under saturation conditions equal

T_0 . Let us consider that one of the nodes is misbehaving. This would lower the throughput observed by the genuine nodes. Clearly, $T_0^o < T_0$.

Algorithm 5: Selfish Attack Detection Algorithm

Input: Number of nodes

Output: Selfish secondary user detection

1. Initialize N number of nodes $N = n_1, n_2, \ldots n_i$ i=1 to N
2. While $i \leq N$
3. If $Th_i < Threshold\_Th$
4. Employ contention window CW to successfully transmit RealPktThr packets
5. Else
6. Employ Standard BEB to sucesssfully transmit BebPktThr packets
7. End if
8. Recompute Th_i during the above time interval
9. End while

RESULTS AND DISCUSSION

In this section the performance of the existing and the proposed system is compared. In the existing system, Signal activity Pattern Acquisition and Reconstruction System (SPARS) is used in the existing system. In the proposed system, Selfish Attacks Detection (SAD) method is used to identify the selfish secondary users and enhanced SPARS system is used to identify the multiple classes of Pus attack in the cognitive radio network. The performance is evaluated in terms of false alarm probability, true positive rate and miss-detection probability.

Description of Output Parameter

False alarm Probability

False alarm probability is defined as the probability of detecting the selfish nodes falsely.

True positive rate

It is the proportion of positive cases that were correctly identified.

Miss detection probability

Misdetection probability is defined as the probability of not detecting misbehaviors.

Graph Comparisons

False alarm probability

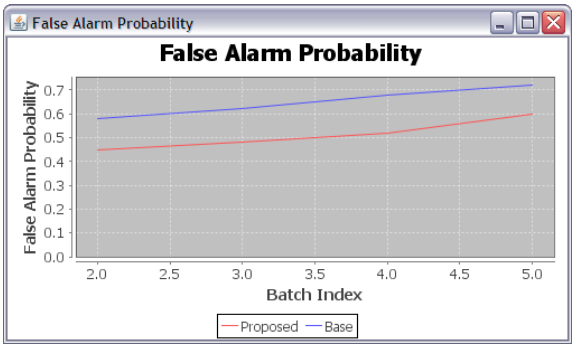

Fig 3: False alarm probability

In the X-axis the batch index is taken. In the Y-axis false alarm probability is taken. In the existing system, Signal activity Pattern Acquisition and Reconstruction System (SPARS) is used in the existing system. In the proposed system, Selfish Attacks Detection (SAD) method is used to identify the selfish secondary users in the cognitive radio network. When Compared to the existing system, there is less false alarm probability in the proposed system.

True Positive rate

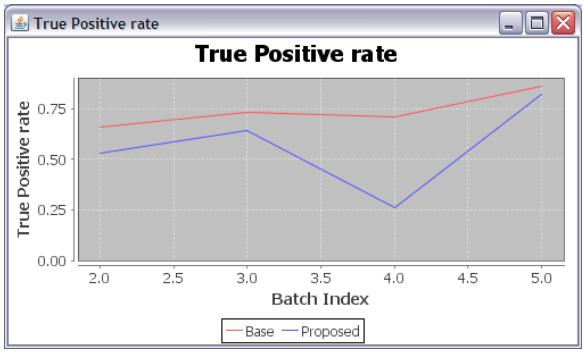

Fig 4: True Positive rate

In the X-axis the batch index is taken. In the Y-axis true positive rate is taken. In the existing system, Signal activity Pattern Acquisition and Reconstruction System (SPARS) is used but in the proposed system, Selfish Attacks Detection (SAD) method is used to identify the selfish secondary users in the cognitive radio network. When Compared to the existing system, there is high true positive rate in the proposed system.

Miss detection Probability

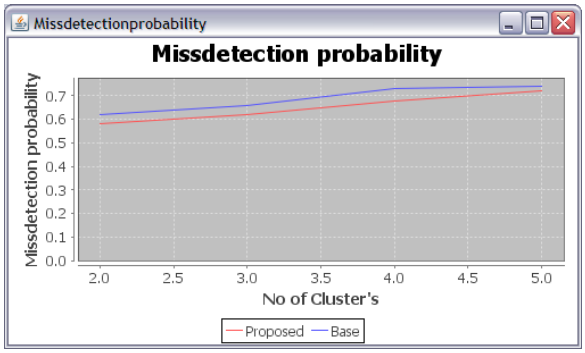

Fig 5: Miss detection Probability

In the X-axis the batch index is taken. In the Y-axis true misdetection probability is taken. In the existing system, Signal activity Pattern Acquisition and Reconstruction System (SPARS) is used in the existing system. In the proposed system, Selfish Attacks Detection (SAD) method is used to identify the selfish secondary users in the cognitive radio network. When Compared to the existing system, there is less misdetection probability in the proposed system.

CONCLUSION

The drawback of the existing system is that it does not detect the selfish secondary user attack and multiple classes of primary user attack. In the proposed system, Selfish Attacks Detection (SAD) is used to identify the selfish secondary users in the cognitive radio network. This method will detect the attacks

of selfish SUs by the cooperation of other legitimate neighboring SUs. Furthermore, the distributed reaction mechanism is used to detect more than one selfish node. In this method the two reaction mechanisms are proposed based entirely upon local information, to prevent selfish misbehaviors in cognitive radio adhoc networks. Additionally, the multiple classes of primary users are detected in which the weight is allocated for each application. Based on the weights, the multiple classes of primary users are detected. The numerical results show that the proposed method achieves better performance than the existing system.

REFERENCES

1. B. A. Olshausen and D.J. Fieldt (1997), "Sparse coding with an Over complete basis set: A strategy employed by v1?" Vision Res., vol. 37, no.23, pp. 3311– 3325.
2. B. Zhao, L. Fei-Fei, and E. Xing (2011), "Online detection of unusual events in videos via dynamic sparse coding," in Proc. IEEE Conf. CVPR, Providence, RI, USA, pp. 3313–3320.
3. ChunShengXin, and Min Song (2014), "Detection of PUE Attacks in Cognitive Radio Networks Based on Signal Activity Pattern", IEEE Transactions On Mobile Computing, VOL.13, No. 5.
4. D. L. Donoho (2006), "For most large underdetermined systems of equations, the minimal l1-norm near-solution approximates the sparsest near-solution," Wiley Commun. Pure Appl. Math., vol. 59, no. 7, pp. 907–934.
5. H. Lee, A. Battle, R. Raina, and A. Y. Ng(2006), "Efficient sparse coding algorithms," in Proc. NIPS.
6. H. Li and Z. Han (2011), "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part II: Unknown channel statistics," IEEE Trans. Wireless Commun., vol. 10, no. 1, pp. 274–283.
7. J. Wright, A. Yang, A. Ganesh, S. Sastry, and Y. Ma (2009), "Robust face recognition via sparse representation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 31, no. 2, pp. 210–227.
8. M. G. Natrella, Experimental Statistics, NBS Handbook 91. Washington, DC, USA: U.S. Department of Commerce, 1963.
9. N. Nguyen, R. Zheng, and Z. Han (2012), "On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification," IEEE Trans. Signal Process., vol. 60, no. 3,pp. 1432–1445.
10. R. Rubinstein, M. Zibulevsky, and M. Elad (2010), "Double sparsity: Learning sparse dictionaries for sparse signal approximation," IEEE Trans. Signal Process. vol. 58, no. 3, pp. 1553–1564.
11. S. Chen, K. Zeng and P. Mohapatra (2011), "Hearing is believing: Detecting mobile primary user emulation attack in white space," in Proc. IEEE INFOCOM.
12. Y. Tan, K. Hong, S. Sengupta, and K. Subbalakshmi (2011), "Using Sybil identities for primary user emulation and byzantine attacks in dsa networks," in Proc. IEEE GLOBECOM, Houston, TX, USA.
13. R. Chen, J.-M. Park, and J. Reed (2008), "Defense against primary user emulation attacks in Cognitive radio networks", IEEE J.Sel.Areas Commun., vol.26, no. 1, pp.25-37.
14. J. Yang, K. Yu, and T. Huang (2010), "Efficient highly over-complete sparse coding using a mixture model," in Proc. 11th ECCV, Heraklion, Greece, pp. 113–126.
15. O. Vinyals and L. Deng (2012), "Are sparse representations rich enough for acoustic modeling?" in Proc.13th Annu. Conf. International Speech Communication Association, Portland, OR, USA.

16. K. Krishnamoorthy and T. Mathew (2009), Statistical Tolerance Regions: Theory, Applications, and Computation. Hoboken, NJ, USA: Wiley.
17. A. Madanayake, C. Wijenayake, N. Tran, S. Hum, L. Bruton, and T. Cooklev (2012), "Directional spectrum sensing using tunable multi-d space-time discrete filters," in Proc. IEEE Workshop CORAL, SanFrancisco, CA, USA.
18. Z. Yuan, D. Niyato, H. Li, and Z. Han (2011), "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in Proc. IEEE WCNC, Cancun, Mexico.