ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization Vol. 3, Special Issue 3, April 2014

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

# A Secure Transmission of Cognitive Radio Networks through Markov Chain Model

Mrs. R. Dayana, J.S. Arjun

Assistant Professor, Dept of ECE, SRM University, Kattankulathur, Tamilnadu, India

II – M.Tech(Communication Systems), SRM University, Kattankulathur, Tamilnadu, India

**Abstract: -** To help unlicensed users utilize the maximum available licensed bandwidth an opportunistic communication technology cognitive radio is designed. A little research has been done regarding security in cognitive radio. Selfish attacks are a serious security problem because they significantly degrade the performance of a cognitive radio network. In this paper, we identified the selfish attacks using COOPON (Cooperative of Neighboring) and also we rectified the selfish attacks using Markov chain model and increased the Cognitive radio network system performance

**Index Terms**—Cognitive Radio Network, Selfish Attack, COOPON, Markov Chain Model.

## I. INTRODUCTION

A cognitive radio is an intelligent radio that can be programmed and configured dynamically. Its' transceiver is designed to use the best wireless channels. Such a radio automatically detects available channels in wireless spectrum Depending on transmission and reception parameters; there are two main types of cognitive radio

- Full Cognitive Radio: - In which every possible parameter observable by wireless node (or network) is considered.
- Spectrum –sensing cognitive Radio:- In which only the radio-frequency spectrum is considered.

  ***Licensed-Band Cognitive Radio***, capable of using bands assigned to licensed users (except for unlicensed bands, such as the U-NII band or the ISM band. The IEEE 802.22working group is developing a standard for wireless

***Unlicensed-Band Cognitive Radio***, which can only utilize unlicensed parts of the radio frequency (RF) spectrum. One such system is described in the IEEE 802.15Task Group 2 specifications, which focus on the coexistence of IEEE 802.11 and Bluetooth.

As wireless communication devices have been tremendously widespread, we have faced excessive spectrum demands and the need to better utilize the available spectrum. In traditional spectrum management, most of the spectrum is allocated to licensed users for exclusive use. CR technology is carried out in two steps. First, it searches for available spectrum bands by a spectrum-sensing technology for unlicensed secondary users (SUs). When the licensed primary user (PU) is not using the spectrum bands, they are considered available. Second, available channels will be allocated to unlicensed SUs by dynamic signal access behavior. Whenever the PU is present in the CR network, the SU will immediately release the licensed bands because the PU has an exclusive privilege to use them CR nodes compete to sense available channels. But some SUs are selfish, and try to occupy all or part of available channels. Usually selfish CR attacks are carried out by sending fake signals or fake channel information.

## II. SYSTEM DESCRIPTION

### A. Existing System

Introducing a selfish attack detection technique, COOPON (called Cooperative of Neighboring), for the attack type. We focus on selfish attacks of SUs toward single channel access in cognitive radio networks. COOPON is designed for CR networks with single channels and is designed for the case, that, the channel allocation information is broadcasted for transmission of Primary users. We make use of the decision capability of a communication network based on exchanged channel allocation information among neighboring SUs.

### B. *Proposed System*

To identify the selfish attack and the rectification of node, we introduce the detection technique of, Markov chain Model. Proposed technique is an intuitive approach and simple to compute, but reliable due to deterministic channel allocation information as well as the support of cooperative neighboring nodes. We focus on, multiple channels and is designed for the case of channel allocation. Node information is broadcast for transmission. We make use of the multiple decision capability of communication network based on exchanging the channel information among the neighboring nodes.

### C. *Attacks and Detection Mechanism*

#### *1) Attack Mechanism*

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 users. The CCC is a channel dedicated only for exchanging and managing, information and parameters. A list of current channel allocation information is broadcast to all neighboring SUs. The list contains all other neighboring users' channel allocation information. A selfish secondary user (SSU) broadcasts separate channel allocation information lists through individual CCC to the left-hand side legal selfish user (LSU) and the right-hand side LSU, respectively. 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

When the attackers try to pre-occupy available channels, they will broadcast an inflated larger number of currently used spectrum channels than they actually are. On the other hand, other legitimate SUs are prohibited from using available channel resources or are limited in using them. The selfish SU, or SSU, sends a current fully pre-occupied channel list to the right hand side LSU even though it is only occupying three channels. In this case, the right-hand side legitimate SU will be completely prohibited from accessing available channels. Also, the SSU could broadcast a partially pre-occupied channel list even though it actually only uses fewer channels. For instance, the SSU is currently using only three channels, but, broadcasting to the left hand side LSU that it is using four channels. In this case, legitimate SUs can still access one available channel out of five maximum, but are prohibited from using one channel that is actually still available

#### *2) Detection Mechanism*

Use of Channel Allocation Information. We consider a cognitive radio network, Networks have distributed and autonomous management characteristics. Our proposed detection mechanism in Markov chain is designed for a communication network. We make use of the autonomous decision capability of a communication network based on exchanged multiple channel allocation information among neighboring SUs. The target node, T-Node, is also a SU, but other 1-hop neighboring SUs, N-Node 1, N-Node 2, N-Node 3, and N-Node 4, will scan any selfish attack of the target node. The target SU and all of its 1-hop neighboring users will exchange the current channel allocation information list via broadcasting on the dedicated channel. We notice that T-Node 2 reports that there are two channels currently in use, while N-Node 3 reports that there are three currently in use, which creates a discrepancy. N-Node 4 also receives faked channel allocation information from the target node. On the other hand, all other exchanged information pairs, T-Node/ N-Node 1 and T-Node/N-Node 2, are correct. Thus, all of the 1-hop neighboring SUs will make a decision that the target SU is a selfish attacker.

### D. *Detection Algorithm*

Fig.1, shows the Selfish attack detection algorithm flow chart using Markov chain model. As mentioned above all currently used channels in the target node and neighboring nodes are summed up into 2steps $channel_{target\_nc}$ and $channel_{neighboring\_nc}$ then $channel_{target\_nc}$ will be compared to $channel_{neighboring\_nc}$

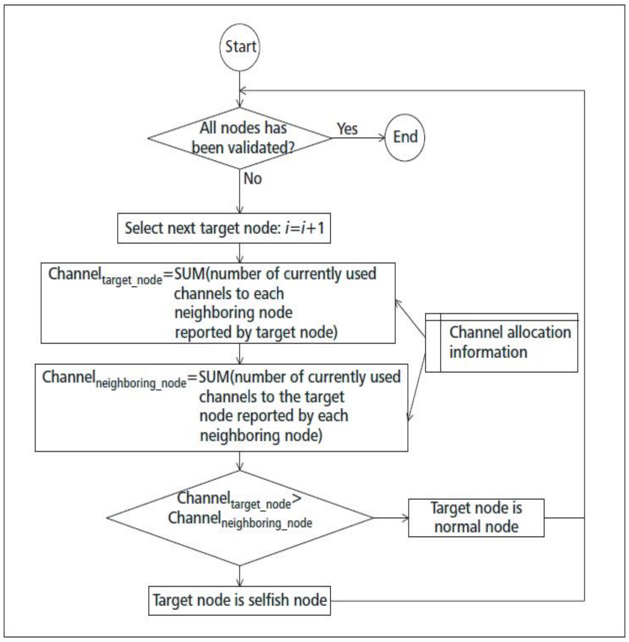

Start
All nodes has been validated?
Yes
End
No
Select next target node: i=i+1
Channel$_{target\_node}$=SUM(number of currently used channels to each neighboring node reported by target node)
Channel allocation information
Channel$_{neighboring\_node}$=SUM(number of currently used channels to the target node reported by each neighboring node)
Channel$_{target\_node}$> Channel$_{neighboring\_node}$
Target node is normal node
Target node is selfish node

Fig 1: Detection Algorithm

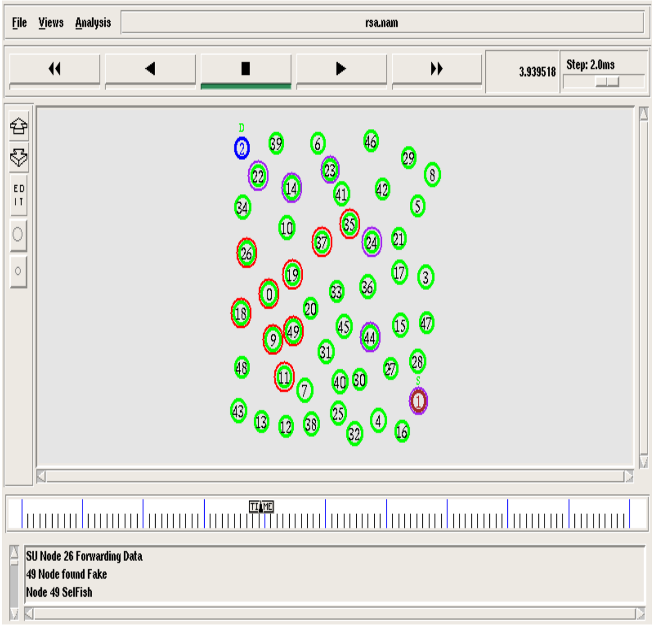
According to example $channel_{target\_nc}$ is 10(4+4+2) and $channel_{neighboring\_nc}$ is 5(3+1+1). Because 10 ≠5, the target secondary node is identified as a selfish attacker. Table 1 shows the simulation parameters for the analysis.

Table 1: Simulation Environment

| Parameter | Setting |
|---|---|
| Antenna type | Omni directional Antenna |
| Routing protocol | AODV(Ad-Hoc On-demand Multipath Distance Vector Routing |
| Data channel | 8 |
| Common Control Channel | 1 |
| Channel data | 11 M bits/s |
| Number of SUs | 50 |
| Number of Selfish SUs | 2, 4, 6,8,10 |

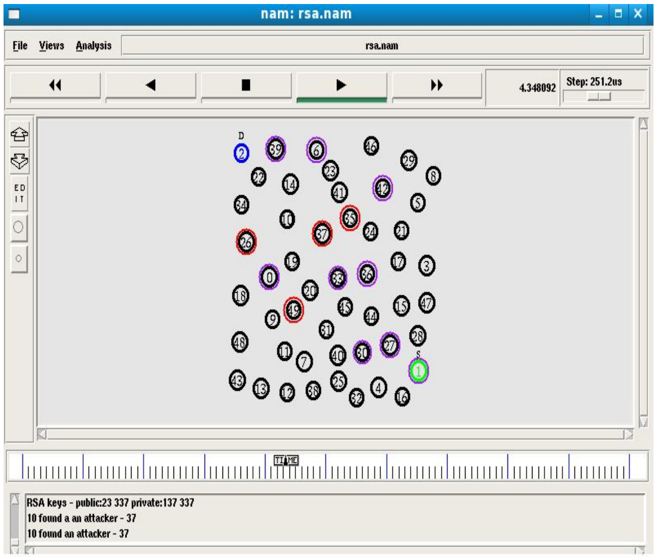
## III. Simulation Results and Analysis

COOPON identifies the attacks and drops the misbehaving SU's nodes and use the transmission path with using active nodes and COOPON has single channel transmission path Markov chain model. Fig.2 shows the output of the COOPON with 50 SUs nodes.



SU Node 26 Forwarding Data
49 Node found Fake
Node 49 SelFish

Fig. 2: Output of the COOPON with 50 SUs Nodes



RSA keys - public:23 337 private:137 337
10 found a an attacker - 37
10 found an attacker - 37

Fig. 3: Output of Markov chain model with 50 SUs Nodes

Fig. 3 shows the Markov chain model output which identifies the attacks of Selfish SU's nodes and rectifies the selfish SU's nodes and uses the nodes in the transmission path and Markov chain model has multiple channel transmission paths.

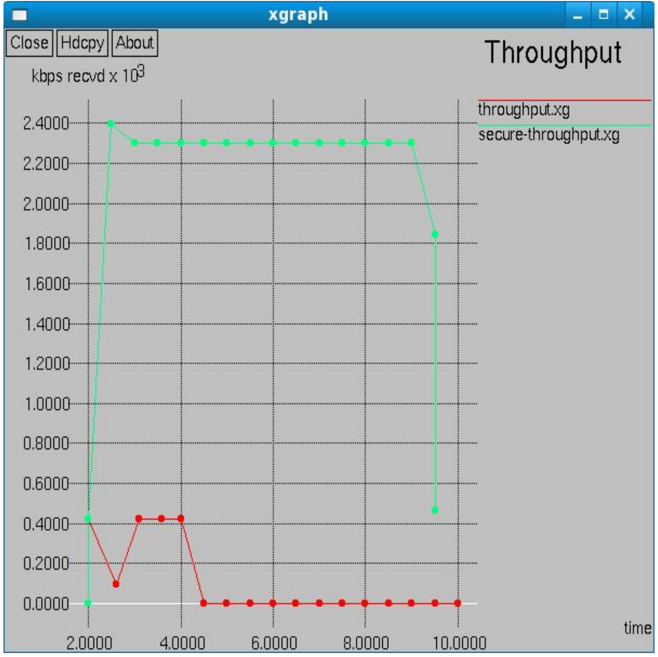


Fig.4:Difference between COOPON & Markov Chain Model

In the above graph, we shown, the difference between the COOPON technique and Markov chain model technique. X-axis is time and Y-axis is bit rate (kbps) recevied per packets. The red trace indicates the COOPON technique. The Green trace indicates the Markov chain technique. Where, the throughput is very high using the markov chain model

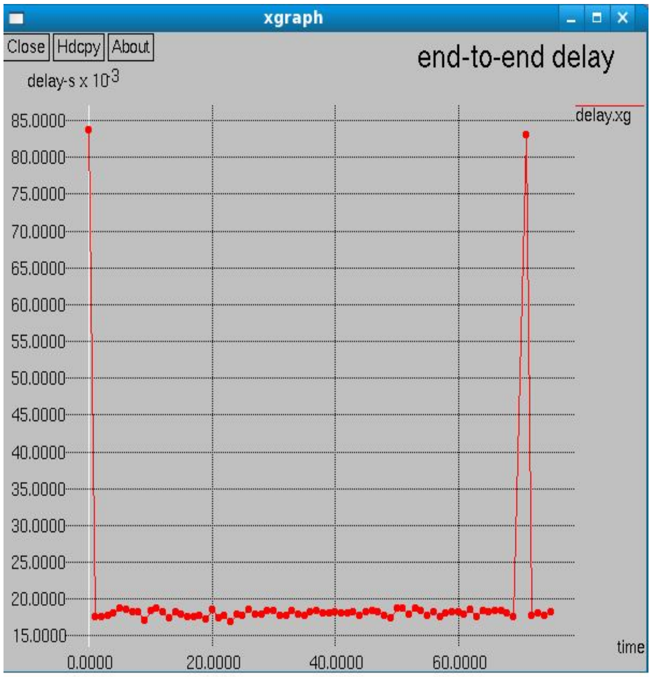


Fig. 5: Delay of CR Network using Markov chain Model

Fig. 5 shows the delay of the Cognitive radio Network using Markov chain model and from the graph we can infer, that, the delay of the network reduces with respect to me.

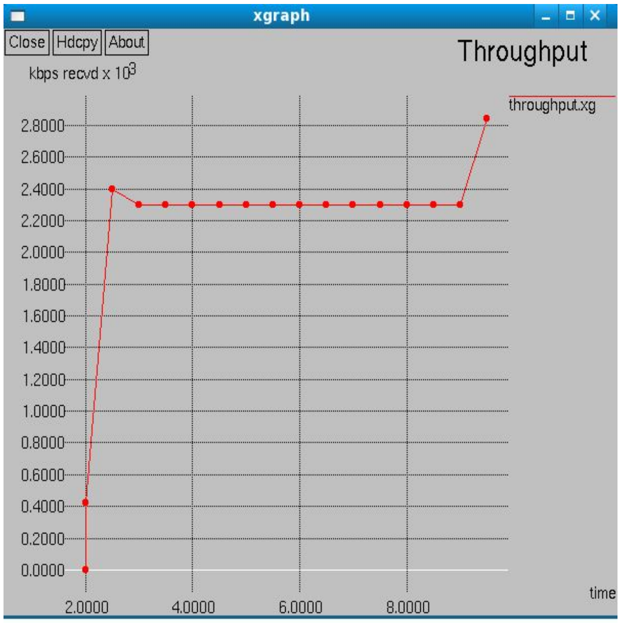


Fig. 6: Over all throughput of CR Network using Markov Chain Model

Fig. 6 shows the throughput of the Cognitive Radio Network with Markov Chain Model and we found that the overall throughput increased Compare to COOPON and it increases the performance of the system.

## IV. Conclusion

Hence, we detect the selfish attack at the SU's and this attacks node were reduced .The transmission path can be constructed through this reduced nodes. Thus Markov chain model provides secure communication to cognitive radio networks.

## References

[1] —X. Tan and H. Zhang, "A CORDIC-Jacobi Based Spectrum Sensing Algorithm for Cognitive Radio," *KSII Trans. Internet and Info. Systems*, vol. 6, no. 9, Sept. 2012, pp. 1998–2016.

[2] C.-H. Chin, J. G. Kim, and D. Lee, "Stability of Slotted Aloha with Selfish Users under Delay Constraint," *KSII Trans. Internet and Info. Systems*, vol. 5, no. 3, Mar. 2011, pp. 542–59.

[3] S. Li *et al.*, "Location Privacy Preservation in Collaborative Spectrum Sensing," *IEEE INFOCOM'12*, 2012, pp. 729–37.

[4] Z. Gao *et al.*, "Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks," *IEEE Wireless Commun.*, vol. 19, no. 6, 2012, pp. 106–12.

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

[6] H. Hu *et al.*, "Optimal Strategies for Cooperative Spectrum Sensing in Multiple Cross-over Cognitive Radio Networks," *KSII Trans. Internet and Info. Systems*, vol. 6, no. 12, Dec. 2012, pp. 3061–80.

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

[8] M. Yan *et al.*, "Game-Theoretic Approach Against Selfish Attacks in Cognitive Radio Networks," *IEEE/ACIS 10th Int'l. Conf. Computer and Information Science (ICIS)*, May 2011

[9] J. Ma , G. Y. Li and Î'. Î—. Juang "Signal processing in cognitive radio", *Proc. IEEE*, vol. 97, 2009

[10] Q. Zhao , L. Tong and A. Swami "Decentralized cognitive MAC for dynamic spectrum access", *Proc. IEEE DySPAN*, 2005

[11] C.-K. Yu , K.-C. Chen and S.-M. Cheng "Cognitive radio network tomography", *IEEE Trans. Veh. Technol.*, vol. 59, 2010

[12] F. Digham , M.-S. Alouini and M. K. Simon "On the energy detection of unknown signals over fading channels", *IEEE Trans. Commun.*, vol. 55, 2007

[13] W. Hastings "Monte Carlo sampling methods using Markov chains and their applications", *Biometrika*, vol. 57, no. 1, 1970

[14] Simon Haykin, "Cognitive Radio: Brain-Empowered Wire-less Communications", IEEE journal on Selected Areas in Communications.vol. 23, no. 2, February 2005,pp. 201-220.

[15] "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications", Communications Surveys & Tutorials, IEEE 2009 BY TevfikYucek and Huseyin Arslan.