

Research Paper on Detection of Multiple Selfish Attack Nodes Using RSA in Cognitive Radio

Khyati Patel¹, Aslam Durvesh²

¹Research Scholar, Electronics & Communication Department, Parul Institute of Engineering & Technology, Gujarat, India

²Assistant Professor, Electronics & Communication Department, Parul Institute of Engineering & Technology, Gujarat, India

ABSTRACT

Cognitive radio (CR) is an opportunistic communication technology designed to utilize the maximum available licensed bandwidth for unlicensed users. Security in cognitive radio network becomes a challenging issue, since more chances are given to attackers by cognitive radio technology compared to general wireless network. A selfish SU broadcasts faked channel allocation information to other neighbouring SUs. It is very important to detect the selfish node and prevent the selfish attack in CR ad-hoc network. Selfish cognitive radio attacks are a serious security problem because they significantly degrade the performance of a cognitive radio network. There is a new selfish attack detection technique, called COOPON (called Cooperative neighbouring cognitive radio Nodes), which is used with multichannel resources by cooperative neighbouring cognitive radio nodes. RSA (Rivest-Shamir-Adleman) algorithm is used for securing sensitive data and for secure data transmission. Using RSA algorithm try to improve the different performance parameters of CR. RSA gives reliable encryption standard compare to other encryption standard.

Keyword: -Cognitive Radio, Mobile Ad-Hoc Network, Selfish Nodes, Primary Users, Secondary Users, Cooperative neighbouring cognitive radio Nodes, Cryptography, RSA Algorithm

1. INTRODUCTION

Cognitive radio (CR) is an opportunistic communication technology designed to utilize the maximum available licensed bandwidth for unlicensed users. Recent developments of wireless communication lead to the problem of growing spectrum shortage. Cognitive radio, as a novel technology, tends to solve this problem by dynamically utilizing the spectrum. In traditional spectrum management, most of the spectrum is allocated to licensed users for exclusive use. 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 channel information. If a SU recognizes the presence of a PU by sensing the signals of the PU, the SU won't use the licensed channels. By sending faked PU signals, a selfish SU prohibits other competing SUs from accessing the channels. Another type of selfish attack is carried out when SUs share the sensed available channels.

2. TYPES OF SELFISH ATTACK

2.1 Attack Type 1- Signal Fake Selfish Attack

Attack Type 1 is a signal fake selfish attack which is designed to prohibit a legitimate SU (LSU) from sensing available spectrum bands by sending faked PU signals. There must be at least two selfish nodes because this attack is usually performed when building an exclusive transmission between one selfish SU and another selfish SU regardless of the number of channels.

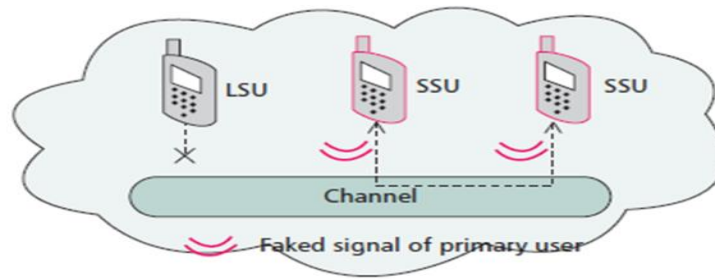


Fig -1: Signal fake selfish attack^[1]

2.2 Attack Type 2- Signal Fake Selfish Attack in Dynamic Signal Access

Attack Type 2 is a signal fake selfish attack in dynamic signal access. It is based on Dynamic multiple channel access. 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.

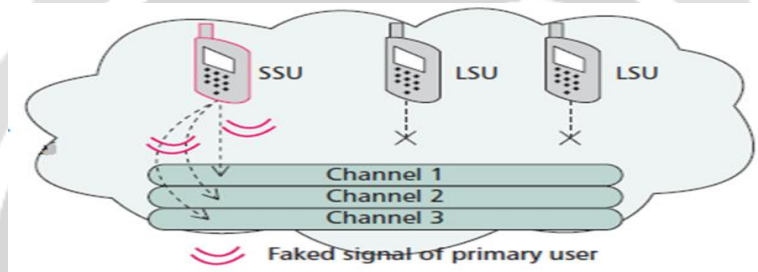


Fig -2: Signal fake selfish attack in dynamic signal access^[1]

2.3 Attack Type 3-Channel Pre-occupation Selfish Attack

Attack Type 3 is a channel pre-occupation selfish attack. A common control channel (CCC) which is used for exchanging management information. A selfish SU will broadcast fake free or available channel lists to its neighbouring SUs.

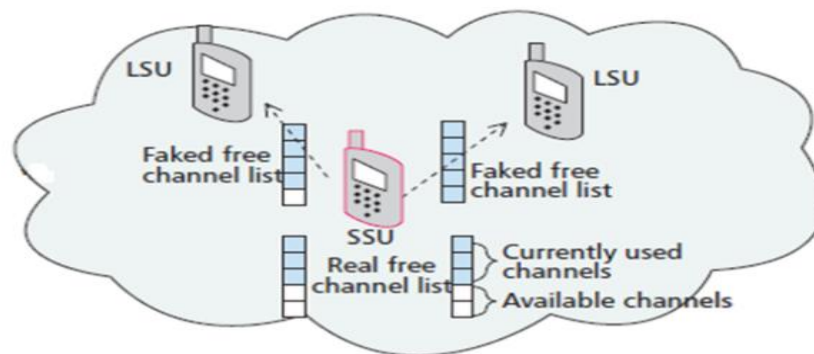


Fig -3: Channel pre-occupation selfish attack^[1]

3. ATTACK AND DETECTION MECHANISM

In a cognitive radio network, the common control channel (CCC) is used to broadcast and exchange managing information. In Type 3 of Fig. 3, the selfish SU sends a current fully pre-occupied channel list to the right hand side

LSU even though it is only occupying three channels. 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.

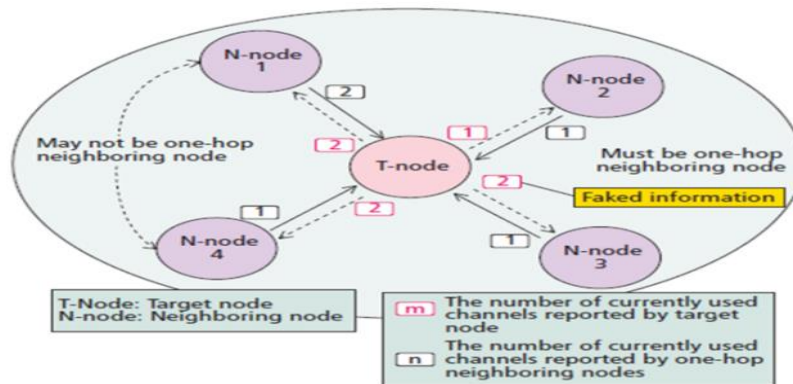


Fig -4: Selfish attack detection mechanism^[1]

COOPON may be less reliable for detection, because two neighbouring nodes can possibly exchange fake channel allocation information. But if there are more legitimate neighbouring nodes in a neighbour, a better detection accuracy rate can be expected, because more accurate information can be gathered from more legitimate SUs.

4. DETECTION ALGORITHM

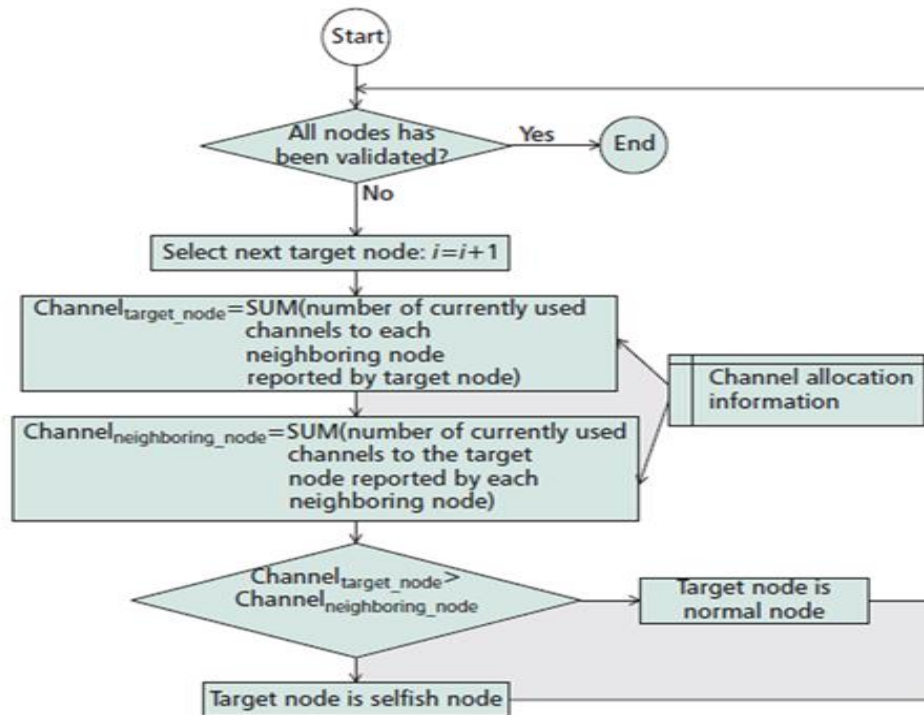


Fig -5: COOPON detection algorithm^[1]

Then $Channel_{target_node}$ will be compared to $Channel_{neighbouring_node}$. According to the example in Fig. 4, $Channel_{target_node}$ is 7 (2+1+2+2) and $Channel_{neighbouring_node}$ is 5 (2+1+1+1). Because $7 > 5$, the target

secondary node is identified as a selfish attacker. Then COOPON will check the next neighbouring node after it selects one of the unchecked neighbouring secondary nodes as a target node.

5. SIMULATION RESULTS

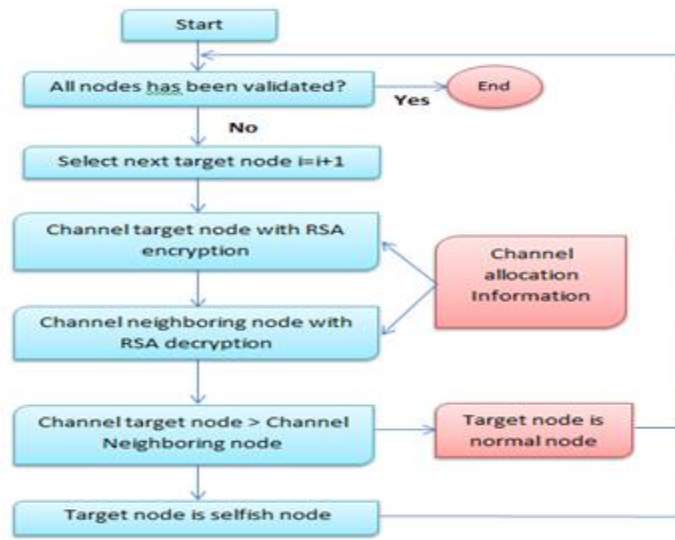


Fig -6: Proposed COOPON algorithm with RSA

In proposed work cooperative neighbouring cognitive radio nodes (COOPON) detection mechanism is used with RSA algorithm. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. In order to investigate how much selfish SU density influences detection accuracy, the experiment was carried out with 50, 100, and 150 SUs, respectively. From Fig. 7, the number of SUs has a trivial effect on COOPON’s detection rate. However, the detection rate is very sensitive to selfish SU density. When the density of selfish SUs in the CR network increases, the detection accuracy decreases rapidly. The experimental results in Fig. 8 give an insight into how the number of nodes in a neighbour will influence selfish detection accuracy. Intuitively, if we have more neighbouring nodes in a neighbour, detection accuracy may be less negatively affected.

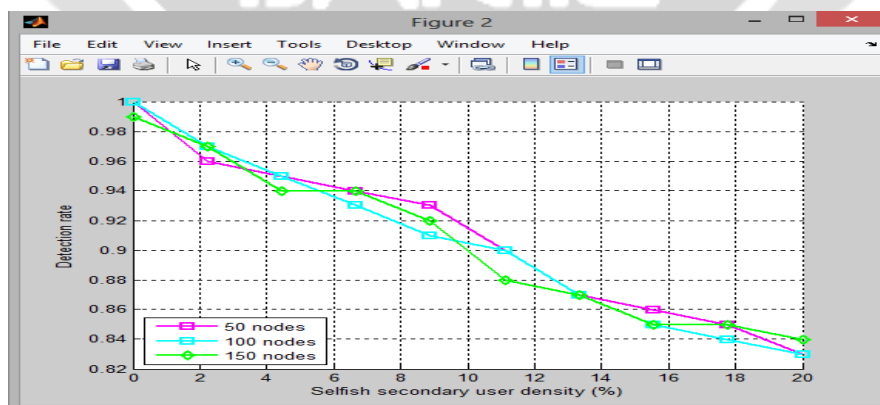


Fig -7: Detection rate vs. selfish SU density

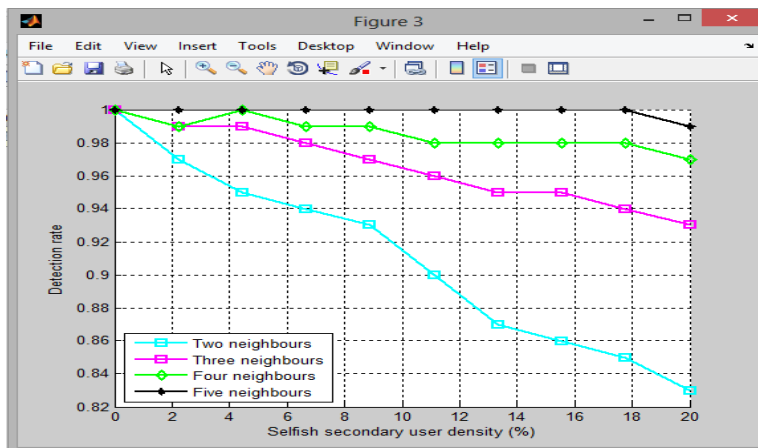


Fig -8: Detection rate vs. neighbouring nodes

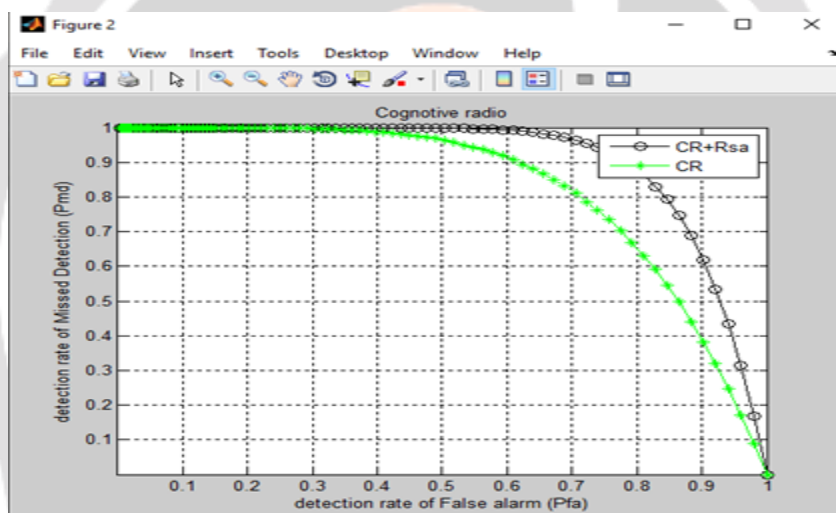


Fig -9: false alarm rate of CR and CR-RSA

As shown in figure 9 false alarm rate is increases the detection rate is decreases. So that the detection rate of combination of CR-RSA is less negatively affected.

6. CONCLUSIONS

A selfish cognitive radio node can occupy all or part of the resources of multiple channels, prohibiting other cognitive radio nodes from accessing the resources. Selfish cognitive radio attacks are a serious security problem because they significantly degrade the performance of a cognitive radio network. By using the deterministic channel allocation information, COOPON gives very highly reliable selfish attack detection results by simple computing. It can be used to find out more than one selfish SU in a neighbour, which gives less detection accuracy. RSA (Rivest-Shamir-Adleman) algorithm can be used for better security, authentication, authorization and integrity of data. Using RSA (Rivest-Shamir-Adleman) algorithm try to improve the different performance parameters of CR.

7. ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my Professor Aslam Durvesh, Parul Institute of Engineering & Technology, Vadodara, India, under whose supervision this research has undertaken. I would also like to thank all

other faculty members of Electronics and Communication Engineering department of Parul Institute of Engineering & Technology who directly or indirectly kept the enthusiasm and momentum required to keep the work towards an effective research alive in us and guided in their own capacities in all possible

7. REFERENCES

- [1] Minh Jo, Longzhe Han, Dohoon Kim, and Hoh Peter, "Selfish attacks and detection in cognitive radio Ad-Hoc networks", IEEE Network, May/June 2013.
- [2] G.A. Safdar, S. Albermany, Nauman Aslam, A. Mansour, G. Epiphaniou, "Prevention against threats to self co-existence-A Novel Authentication Protocol for Cognitive Radio Networks", IEEE Wireless and Mobile Networking Conference (WMNC), 2014.
- [3] Gaofei Sun, Youyun Xu, Xinxin Feng, Xinbing Wang, Yu Cheng, "Efficient Spectrum Utilization with Selfish Secondary Users in Cognitive Radio Networks", IEEE Global Communications Conference (GLOBECOM), 2012.
- [4] P.V. Niranchana, K. Anish Pon Yamni, "Credit risk value based detection of multiple selfish node attacks in cognitive radio networks", IJRET, Volume: 03 Special Issue: 07, May-2014.
- [5] Suchita S. Potdar, Dr. Mallikarjun, "Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks using Markov Chain and Game Theory", International Journal of Science and Research (IJSR), Volume 3, Issue 8, August 2014.
- [6] Xueying Zhang, Cheng Li, "The Security in Cognitive Radio Networks: A Survey", IEEE Network, May/June 2013.
- [7] Andrea Pellegrini, Valeria Bertacco and Todd Austin, "Fault Based Attack of RSA Authentication", IEEE, Design, Automation & Test in Europe Conference & Exhibition, 2010.
- [8] Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks", IEEE communications surveys & Tutorials, vol.15, no.1, First Quarter 2013.
- [9] Z. Gao et al., "Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks," IEEE Wireless Communication, vol.19, no.6, 2012, pp. 106–12.
- [10] M. Yan et al., "Game-Theoretic Approach Against Selfish Attacks in Cognitive Radio Networks," IEEE/ACIS 10th International Conf. Computer and Information Science (ICIS), May 2011, pp. 58–61.
- [11] Suhas Damodaran, Mrs. Savitha, "Tracking of Selfish Attacks in Cognitive Radio Ad-Hoc Networks Using COOPON", International Journal For Technological Research In Engineering, Volume 1, Issue 10, June-2014.
- [12] Wang Weifang, "Denial of Service Attacks in Cognitive Radio Networks", 2nd Conference on Environmental Science and Information Application Technology, IEEE, 2010.
- [13] G. Gowri Shankar, S. Balgani, R. Aruna, "Multi selfish Attacks Detection Based on Credit Risk Information in Cognitive Radio Ad-hoc Networks", SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume 2, issue 4, March 2015.