Detection of Multiple Selfish Attack Nodes in Cognitive Radio : a Review

Khyati Patel[1], Aslam Durvesh[2]

[1]Research Scholar, Electronics & Communication Department, Parul Institute of Engineering & Technology, Gujarat, India
[2]Assistant 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 . These weaknesses are introduced by the nature of cognitive radio, and they may cause serious impact to the network quality of service. A selfish cognitive radio node can occupy all or part of the resources of multiple channels. 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.

In general, users are divided into two categories: Primary or incumbent users that hold a licence for a specific portion of the spectrum, and Cognitive or Secondary Users (SUs) that use parts of the spectrum in an opportunistic way, so as not to cause harmful interference to PUs. 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.

Each SU periodically informs its neighbouring SUs of current available channels by broadcasting channel allocation information such as the number of available channels and channels in use. In this case, a selfish SU broadcasts faked channel allocation information to other neighbouring SUs in order to occupy all or a part of the available channels. Each SU will broadcast the current multiple channel allocation information to all of its neighbouring 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 pre-occupy them. The COOPON will detect the attacks of selfish SUs by the cooperation of other legitimate neighbouring SUs.

All neighbouring SUs exchange the channel allocation information both received from and sent to the target SU, which will be investigated by all of its neighbouring SUs and here the target SU and its neighbouring SUs are 1-hop neighbours. Each individual SU will compare the total number of channels reported to be currently used by the target node to the total number of channels reported to be currently used by all of the neighbouring SUs. If there is any discrepancy between the two values, all of the legitimate SUs will recognize a selfish attacker.

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.

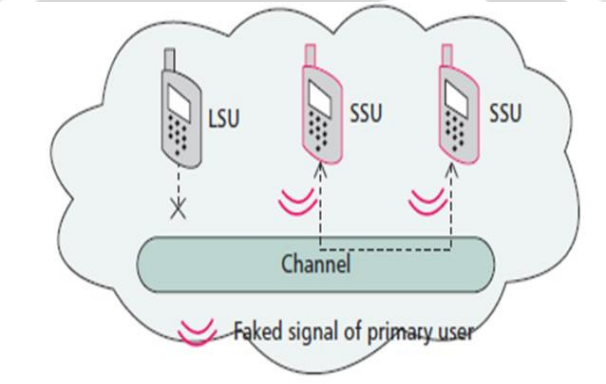

Fig -1: Signal fake selfish attack[1]

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.

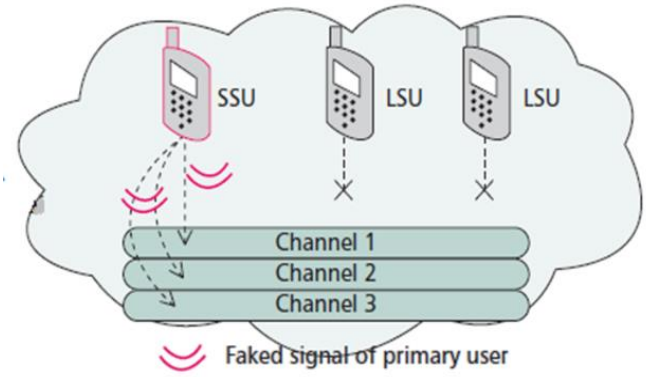

Fig -2: Signal fake selfish attack in dynamic signal access[1]

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.

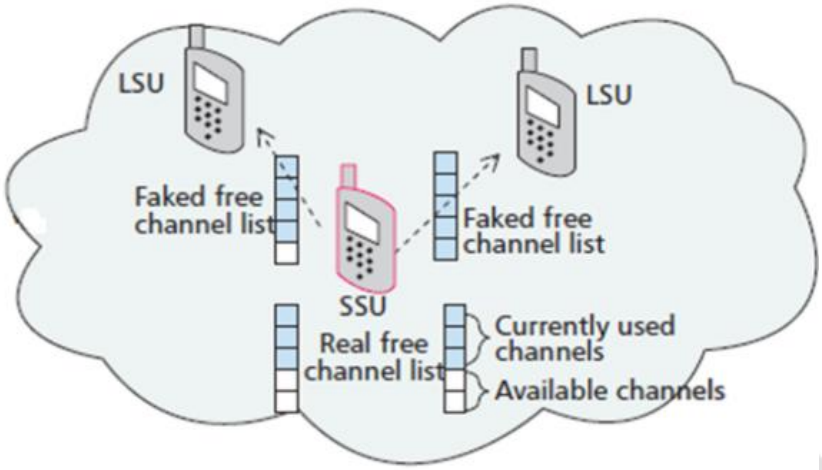

Fig -3: Channel pre-occupation selfish attack[1]

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.

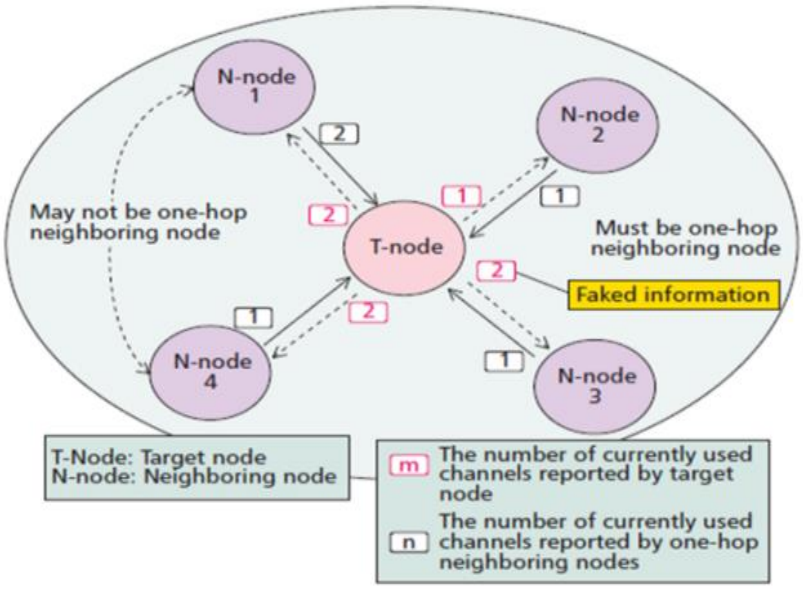

Fig -4: Selfish attack detection mechanism[1]

In Fig. 4, the target node, T-Node, is also a SU, but other 1-hop neighbouring 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 neighbouring users will exchange the current channel allocation information list via broadcasting on the dedicated channel. 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

All currently used channels in the target node and neighbouring nodes are summed up in two steps Channeltarget_node and Channelneigbouring_node. ThenChanneltarget_ node will be compared to Channelneigbouring_node.According to the example in Fig. 4, Channeltarget_node is 7 (2+1+2+2) and Channelneigbouring_node is 5 (2+1+1+1). Because 7 > 5, the target secondary node is identified as aselfish attacker.Then COOPONwill check the next neighbouring node after it selects one of the unchecked neighbouring secondary nodes as a target node.And the detection procedure will continue until the last SU in a CR network is validated.

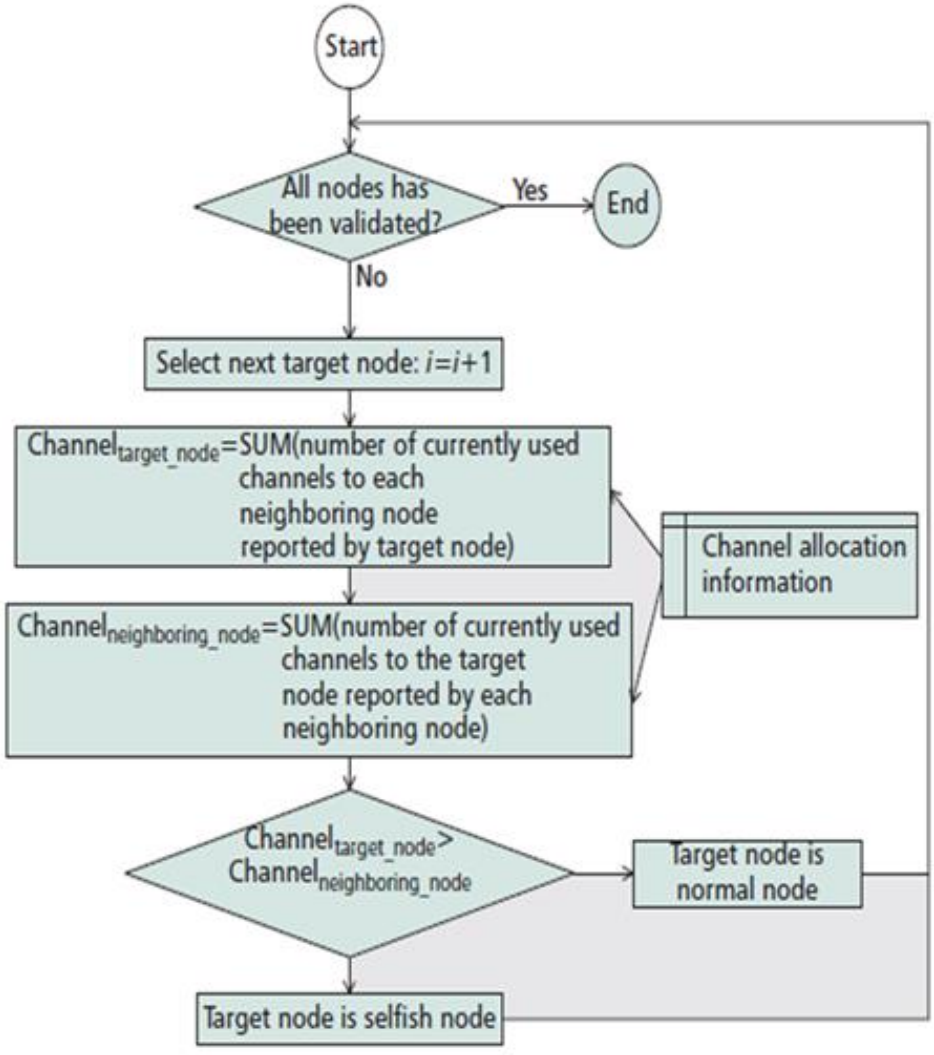

Fig -5: COOPON detection algorithm[1]

Table -1: Overview of Existing Techniques

Detection Techniques	Remarks
Cooperative neighbouring cognitive radio nodes(COOPON) detection technique	Detection Accuracy is around 97% Very highly reliable selfish attack detection method
Cognitive Authentication Protocol (CoG-AUTH) using RSA Algorithm	Authentication time is 5.5% better than PKMv2(Privacy Key Management) Transmission Successful Rate is 3% better than PKMv2
Credit Risk Value(CRV) detection technique	More efficient technique Selfish node detection time is less
Markov Chain and Game Theory Detection technique	Markov model takes 47 seconds to detect selfish user Game theory- accuracy rate is 90%
Cooperative neighbouring cognitive radio nodes(COOPON) detection technique	Detection Accuracy is around 97% Very highly reliable selfish attack detection method

5. 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.

6. 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] Minho 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, NaumanAslam, 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. AnishPonYamni, "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. Gaoet 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] SuhasDamodaran,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.Gowrishankar, S.Balgani, R.Aruna, "Multiselfish 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.