International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

A Survey: Detection Techniques on Selfish & Multi-Selfish Attacks in Cognitive Radio Networks

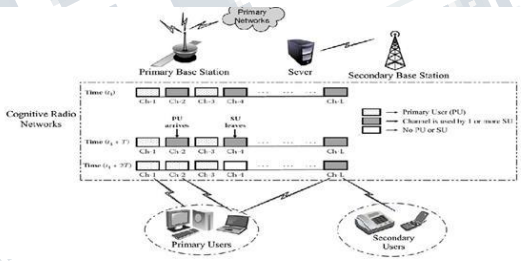
[1] Vanitha K.C [2] Dr. Bharathi S.H [3] Vidyasagar K.N
[1][2][3]Department of Electronics and Communication
REVA Institute of Technology And Management, Bangalore India
[1]4vanitha@gmail.com, [3]Vidyasagarkn@revainstitution.org

***Abstract*— Cognitive radio network is a rare communication technology which suggests the Unlicensed persons to use more amount of bandwidth existing in the spectrum which is not used by licensed persons. CRN identifies large number of available communication channels in spectrum very efficiently. The free spectrum of CRN is used by the users who are Unlicensed without harming the licensed users (PU) which are involved in communication. The main goal of CRN is to solve the problem of Spectrum Scarcity by making the unlicensed user to use the spectrum when it is free that means when the licensed user (PU) will not use the spectrum that time the unlicensed user can use it dynamically. Advantage of CR is to provide efficient data transmission without the breakup in the comminucation.CRN faces problems on selfish attacks which are carried out by the SU which sends fake information to the person near to SU as that to occupy all free channels available in spectrum. Selfish SU Nodes and Multi-selfish SU Nodes are degrading the performance by sending fake message to closer nodes of CRN. Here we suggested how to identify Selfish and Multi-selfish SU nodes by the two different algorithms based on survey.**

***Keywords*— Cognitive Radio Network (CRN), Secondary users (SU), Primary User (PU), Selfish Nodes, Multi-selfish nodes.**

I. INTRODUCTION

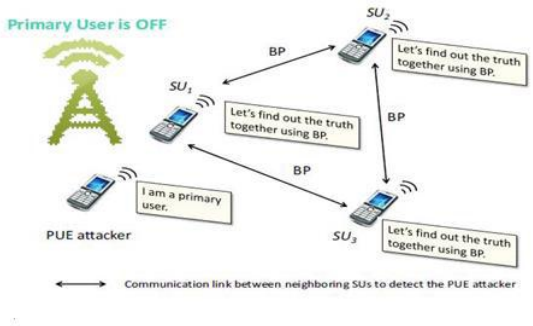
We know that nowadays Wireless technology is more prominent and running technology in modern world. So there is big demand for bandwidth. As we know if communication should happen then we need to allot one frequency band for particular user and which will happen only statically but not dynamically. Hence the scarcity of the same is increased, where the bandwidth which is free for some time should be used by other users and there existed a new technology of Cognitive radio. In CR when the primary user is free at that time the secondary user was able to occupy the free bandwidth. As soon as the primary Users come back the secondary users should leave that bandwidth. Once frequency band is allotted for a particular user then that will become licensed user and other user can't occupy this band. So all the frequencies are used by all users and there are no other empty frequencies to allot for new user. So CR came into picture to provide the hopes on helping the new users with the band allocated for the new users when the licensed users are free. This provides the transmission to happen in various speeds.



Hence the CR technology existed to help the others to use the vacant band when licensed user is busy in some other work or when it is idle. This solved the scarcity of bandwidth to some level by allotting the band to others. Also when the primary user is back the secondary user should leave the band for him without completing the transmission by secondary user so there will be loss of data. This kind of swapping of bandwidth between licensed and unlicensed happens only by allocating bands dynamically not statically.

Cognitive radio identifies the frequencies which are idle and allows the unlicensed user to occupy for transmission dynamically. Cognitive Radio (CR) which is system/model present in wireless communication. CR is present on Software defined radio as it is emerging techno providing a good platform for these kinds of flexible radio systems. CR technique is performed on two steps. First, it

will identify any available bands by sensing the spectrum for Secondary users.



When the licensed user (PU) is idle without using the spectrum, then they are considered available. Secondly, the free channels will be handover to unlicensed SUs. When the PU comes back into CRN, the SU should immediately handover the bands to PU as the PU has authority to use exclusively. Some CR nodes will be in completion to sense the available channel in CRN but few other SUs in CRN are selfish, and they want to occupy all channels available in whole spectrum. This kind of Selfish SUs will send a unwanted (Fake) signal or fake Channel message. If SU senses PU is present by identifying PU signals in CRN, the SU will not use the licensed band. For example in this case, even a selfish user i.e SU uses only one out of six channels, it will delivers to all nodes in CRN that all six channels are used by that particular secondary person with the intention of occupying the available channels which is four in this example. Thus, these kinds of selfish attackers will degrade the good performance of a CR network dynamically.

Some researchers have proposed different methods of spectrum sharing between both users which are licensed and unlicensed without harming or modifying the terminals, devices and networks in the system. Here they have proposed and analyzed with new method of accessing dynamic spectrum when the buffering mechanism is absent for the Secondary User. A Markov chain method [1] is approached here to analyze the sharing of spectrum with generalized bandwidth in both systems those are primary systems and secondary system. Performance for SU is developed w.r.t blocking of probability, forced termination probability, waiting time, interrupted probability and non-completion probability some numerical example is presented to show the contact of key systems like traffic on the performance. By comparing we come to know the results in indicating that buffers are able to significantly decrease the SU blocking prospect and non-completion prospect with minor bigger forced termination prospect.

In other research paper the authors have proposed on collaborative sensing [2] inside cognitive radio networks which can significantly advance the prospect of identifying the transmission of primary persons. In current the collaborative schemes of sensing, whole collaborative secondary persons are assumed as truthful. As this consequence, the system is defenseless on attacks on which dangerous secondary users provide false detection value. In this paper, the investigation happens on how to advance the security inside collaborative sensing. We develop a cruel user detection flowchart that calculates the level of suspicious secondary users depending on their previous reports. Afterwards, we estimate the trust values and also the consistency values which are used to remove the cruel user which influence on trusty primary user's finding results. Through this kind of simulations, we know even a single dangerous user can considerably disgrace the presentation of sensing of collaborative. The proposed method of trust value detector can effectively distinguish between the honest and cruel secondary users. The Rxr operating characteristic (ROC) lines for trusty user identification they have demonstrated the development in the safety of sensing of collaborative.

Rest of the paper is organized as section II with the information of requirements, applications, Challenges and various types of attacks.

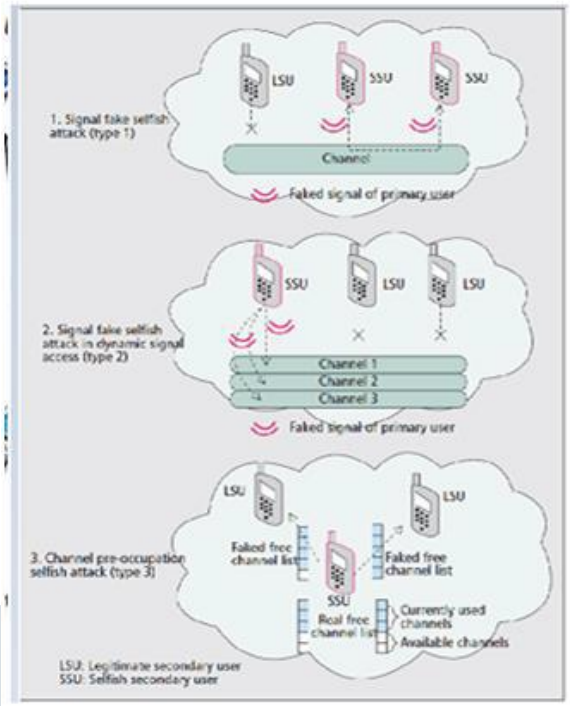
II. VARIOUS TYPES OF ATTACKS IN CRN

In the above section we analyzed what exactly cognitive radio is and also analyzed the architecture of CRN with the survey on attacks and security for CRN. Now we will start with the types of attacks with the requirements and applications of cognitive radios. CRs are used in smart radio with efficient flow of data and also the applications which are rising for addition to bright multiple or the cooperative-antenna arrays in which the applications to composite communication environments. Cognitive radios by comparing tell whether the terminals to sense whether the spectrum is free or it is used by someone. Also cognitive radio networks has more advantage on the Intelligent Antenna which is booming in recent trends CR provides open sharing, interference will be avoided by Spectrum sharing. Spectrum sensing will be costly in CR and also multi band RF technology, algorithm used is Spectrum management, Techniques applied on Cognitive radio software, approach is in orthogonal modulation schemes. We come across various methods of Attacks named selfish and Multi-selfish attacks. Types of Selfish Attacks depends [3] on how they attack and on what they attack so to occupy the spectrum which is available. We can see three kinds of selfish attacks they are

Type 1 Attack: The Secondary user send the fake signal for selfish attack. In Type 1 attack the secondary user will send a primary signal so to identify which channels are idle. The selfish Secondary user will perform as like primary user the characteristics and will enact in the same manner. A trusty SU who hears the faked signal will make sense that the owner of that channel is come back so he need to leave the channel immediately so the trusty Secondary user will leave the channel to the selfish secondary user. This attack will usually happen while building the transmission line between Selfish SU and another secondary selfish user without caring for number of users available. At least there must be two or more than two selfish nodes to perform this type of attack.

Type 2 Attack: These are also selfish SUs enacting with the characteristics of PU, but performed in dynamic multiple access of channels. In normal dynamic signal access process, the SUs frequently senses the current channel to know whether the PU is active or inactive, and if the PU is active then selfish SU will switch to another channel which is free for transmission. In this attack as mentioned in fig 3, by sending continuously fake information on to multiple bands of frequencies a selfish attacker can successfully stop the trusty SUs by using and sensing the available bands in spectrum.

Type 3 Attack*:* This is the technique which we have used for proposing our paper on selfish attacks. In this Type 3 attack, which is called preoccupying the channel, attacks happen when their will be communication broadcasted the current channels available to the neighboring nodes for transmission. We can consider an environment for broadcasting through Common Control channel which is only meant for exchanging information. A selfish Secondary User will broadcast fake list of channels to the neighboring nodes as given in Fig 3 even the selfish SU is not using so many channels but it is pre occupying the channels for using further, so as to leave the used channel when suddenly a Licensed user comes and asks for the channel for transmission. Example the Selfish SU will send 5 channels are in use though it is using only 3 channels for its communication so here it is occupying 2 channels extra under its Queue. Here in the article we are trying to identify the selfish type 3 attack and propose the algorithms of COOPON and also we will identify the multi selfish nodes and propose Credit risk method to solve the problem on this type of attacks.



III. CONCLUSION

The existing method provides the information on one selfish node attacker and multi selfish nodes attackers separately with the detection techniques of COOPON and credit risk algorithm. In our approach we are combining both selfish and multi selfish attackers with their detection techniques by providing the extra information of black list where, as soon as the node is identified as attacker we are pushing that node into black list so in future the node will be not given the access for requesting the channel. This prevents the usage of time in order to provide the access and later to identify the node as attacker and also to provide an efficient data transmission within the CRN.

REFERENCES

[1] S.Li et al., (2012),"Location Privacy Preserving Dynamic Spectrum Auction in Cognitive Radio Network", IEEE INFOCOM" 12, pp. 729–37

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

[3] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter (May 2013), "Selfish Attacks and Detection in Cognitive

Radio Networks", Korea University.vol 27, Issue: 3, IEEE Network.

[4] "A Survey of Techniques Used Detect Selfish Nodes in MANET", Karthik.M, Jyothish K John, International Journal for scientific Research & Development /Vol.1, Issue 4,2013.

[5] Jae-Ho Choi, Kyu-Sun Shim, Sangkeun Lee, and Kun-Lung Wu (2012),"Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network" , IEEE Transactions on mobile computing,vol.11 no.2.

[6] E. Hossain, D. Niyato, and Z. Han, Dynamic Spectrum Access in Cognitive Radio Networks, Cambridge University Press, 2009

[7] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, ―NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey,‖ Elsevier Computer Networks Journal, Vol. 50, Sept. 2006,pp.2127–2159.