Improvement of Spectrum Utilisation in Cognitive Radio Networks by Detection of Selfish Attacks

Adnaan Ahmad
ME, Department of Electronics & Telecommunication
G.H. Raisoni College of Engineering & Management
Savitribai Phule Pune University

Vijay Joshi
Department of Electronics & Telecommunication
G.H. Raisoni College of Engineering & Management
Savitribai Phule Pune University

ABSTRACT
The traditional spectrum management techniques allow most of the spectrum to be used by licensed users exclusively. Spectrum sharing mechanism in Cognitive Radio Networks allows spectrum access to secondary user in addition to the primary licensed user. The Secondary Users, in order to compete for the spectrum, turn malicious and try to occupy all or a part of the available channel leading to Selfish Attacks. It results in a degradation of spectrum utilisation efficiency considerably. This paper presents a detection mechanism to counter the effect of selfish attack thereby aiming to improve the efficiency of spectrum utilization.

General Terms
Selfish Attack Detection, Details about the number of fake channels acquired, Co-operative Detection.

Keywords
Cognitive Radio Networks, Spectrum Utilisation, Selfish Attacks, Spectrum Sharing, Spectrum Sensing

1. INTRODUCTION
The increase in wireless communication device has led to excessive spectrum demands and hence a need for better utilisation of the available spectrum. The traditional spectrum management technique allows most of the spectrum to be used by licensed users exclusively. This leads to dynamic underutilization of the spectrum temporarily as well as spatially. It results in creation of vacant spaces in the spectrum which are termed as spectrum holes or white spaces.

There are two aspects of spectrum management. Firstly, the technical aspect which is concerned with the physical world affecting the utilisation of spectral resources. The second is the policy aspect which deals with the economic and political factors of the spectral market. With the introduction of spectrum sharing concept, these aspects got converged into a single paradigm. But still the utilisation of spectrum has not improved satisfactorily.

In spectrum sharing, a spectrum sensing mechanism is used to search for vacant spaces which can be allocated to secondary users. This implies that the spectrum can now be used by a secondary user by a secondary user in addition to the primary licensed user. When the primary user is not using allocated band it is considered available and secondary user can gain an access to it dynamically. Whenever the primary user is present in the network and demand for a service, secondary user will immediately release the license band because the primary user has an exclusive privilege to use them.

The secondary users have to compete to sense the available channel. In this flow of sensing, some secondary users try to occupy all or a part of available channel. Such users are termed as selfish and this phenomenon of illegal acquirement of spectral resources is termed as Selfish Attack.

Usually selfish attacks carried out by sending signals bearing fake information about the channel and hence degrade the performance of entire spectrum sensing mechanism. This paper presents a detection mechanism to counter the effect of Selfish attack thereby aiming to improve the efficiency of Spectrum Utilisation.

2. LITERATURE REVIEW
The study for these attacks began in 2008 when R. Chen, J. Park and J. Lee [2] identified a threat to spectrum sensing, which they called the primary user emulation (PUE) attack. In this attack, an adversary's Cognitive Radio transmitted signals whose characteristics emulated those of incumbent signals. To counter this threat, they proposed a transmitter verification scheme, called LocDef (localization based defense), which verified whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics. To estimate the location of the signal transmitter, LocDef employed a non-interactive localization scheme.

C. Chin, J. Kim and D. Lee [2] in 2011 proposed a repeated Bayesian slotted Aloha game model to analyze the selfish behavior of impatient users. They proved the existence of Nash equilibrium mathematically and empirically. The proposed model enabled any type of transmission probability sequence to achieve Nash equilibrium without degrading its optimal throughput.

In the same year M. Yan et al [3] formulated the secure access for Cognitive radio networks into a static game called Backoff Window Control Game (BWCG) and a repeated game with punishment mechanism based on the CSMA protocol. They proved the existence of a Nash Equilibrium in the BWCG game and designed a punishment mechanism to motivate selfish users not to perform selfish attacks in the repeated game thereby improving the network performance.

In the paper [4], the authors proposed a cross layer Altruistic Differentiated Service Protocol (ADSP) in the year 2012, for the dynamic CRNs to address the QoS provisioning issue in CRNs with selfish nodes coexistence. Simulation results demonstrate that the ASDP can achieve much better performance in terms of lower delay, higher throughput and better delivery ratio for the traffic originating from collaborative routing protocols in the presence of Selfish Nodes.

Finally, in the year 2015, authors developed an entirely new detection mechanism for counter attacking selfish secondary users [5]. They identified a new selfish attack type in cognitive radio ad-hoc networks and proposed an easy and efficient selfish cognitive radio attack detection technique, called COOPON, with multichannel resources by cooperative neighbouring cognitive radio nodes.

3. SELFISH ATTACKS

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. If a SU recognizes the presence of a PU by sensing the signals of the PU, the SU won't use the licensed channels. In this case, 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. Usually each SU periodically informs its neighboring 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 neighboring SUs in order to occupy all or a part of the available channels. For example, even though a selfish SU uses only two out of five channels, it will broadcast that all five channels are in use and then pre-occupy the three extra channels. Thus, these selfish attacks degrade the performance of a CR network significantly.

There has been some research on selfish attack detection in conventional wire- less communications. On the other hand, little research on the CR selfish attack problem has been done so far. Because of the dynamic characteristics of CR networks, it is impossible to use the selfish attack detection techniques used in traditional wireless communications for CR networks.

Selfish attacks are different depending on what and how they attack in order to pre-occupy CR spectrum resources. There are three different selfish attack types shown in Fig. 1.

3.1 Attack Type 1

Type 1 is the signal fake selfish attack. A Type 1 attack is designed to prohibit a legitimate SU (LSU) from sensing available spectrum bands by sending faked PU signals. The selfish SU (SSU) will emulate the characteristics of PU signals. A legitimate SU who overhears the faked signals makes a decision that the PU is now active and so the legitimate SU will give up sensing available channels. This attack is usually performed when building an exclusive transmission between one selfish SU and another selfish SU regardless of the number of channels. There must be at least two selfish nodes for this type of attack.

3.2 Attack Type 2

Type 2 attacks are also a selfish SU emulating the characteristics of signals of a PU, but they are carried out in dynamic multiple channel access. In a normal dynamic signal access process, 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. In this attack type, illustrated in Fig. 1, by launching a continuous fake signal attack on multiple bands in a round-robin fashion, an attacker can effectively limit legitimate SUs from identifying and using available spectrum channels.

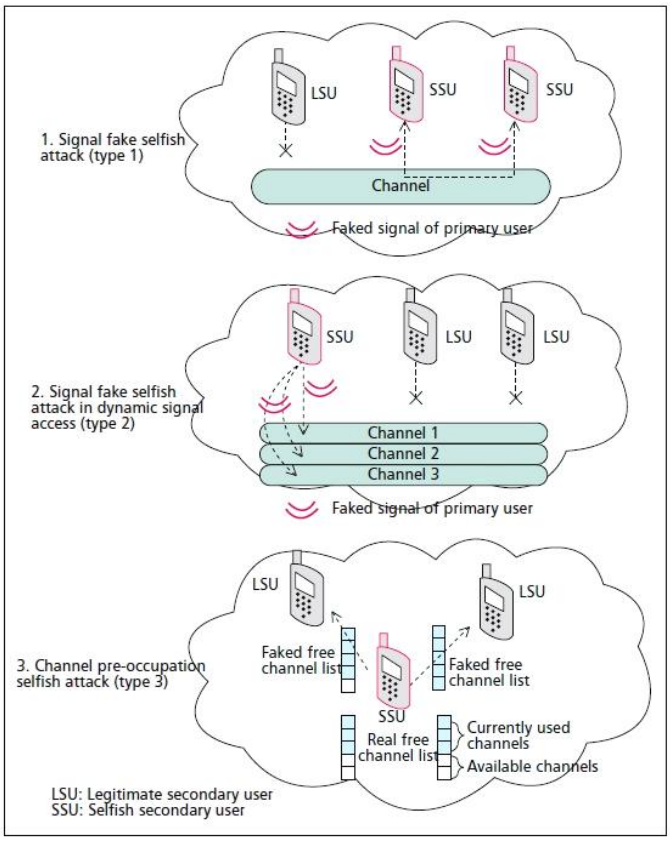

Figure 1 Types of Selfish Attacks

3.3 Attack Type 3

In Type 3, called a channel pre-occupation selfish attack, attacks can occur in the communication environment that is used to broadcast the current available channel information to neighbouring nodes for transmission. We consider a communication environment that broadcasting is carried out through a common control channel (CCC) which is a channel dedicated only to exchanging management information. A selfish SU will broadcast fake free (or available) channel lists to its neighbouring SUs, as illustrated in Fig. 1. Even though a selfish SU only uses three channels, it will send a list of all five occupied channels. Thus, a legitimate SU is prohibited from using the two available channels.

4. DETECTION MECHANISM

We consider a cognitive radio ad-hoc network. Ad-hoc networks have distributed and autonomous management characteristics. Our proposed detection mechanism in is designed for an ad-hoc communication network. We make use of the autonomous decision capability of an ad-hoc communication network based on exchanged channel allocation information among neighboring SUs.

In Figure 2, 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 cur- rent channel allocation information list via broad-casting 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. All 1-hop neighboring SUs sum the numbers of currently used channels sent by themselves and other neighboring nodes. 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.

Detection of existing selfish technologies is likely to be uncertain and less reliable, because they are based on estimated reputation or estimated characteristics of stochastic signals. On the other hand, our proposed selfish attack detection method is very reliable since it is based on deterministic information. However, it has a drawback. When there is more than one neighboring selfish node, this method may be less reliable for detection, because two neighboring nodes can possibly exchange fake channel allocation information. But if there are more legitimate neighboring nodes in a neighbor, a better detection accuracy rate can be expected, because more accurate information can be gathered from more legitimate SUs.

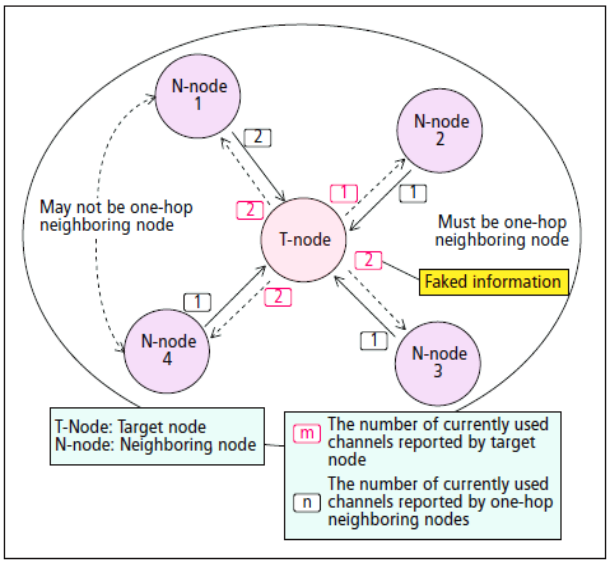

Figure 2 Selfish Attack Detection Mechanism

Figure 3 shows the proposed selfish attack detection algorithm flow chart. As we mentioned above, all currently used channels in the target node and neighboring nodes are summed up in two steps Ctarget and Cneighbouring. Then Ctarget will be compared to Cneighbouring.

According to the example in Fig. 2, Ctarget is 7 (2+1+2+2) and Cneighbouring is 5 (2+1+1+1). Because 7 > 5, the target secondary node is identified as a selfish attacker. In other words, the checked target node inflates its currently used channels number. Then detection algorithm will check the next neighboring node after it selects one of the unchecked neighboring secondary nodes as a target node. This detection procedure continues until the last SU in a CR network is validated.

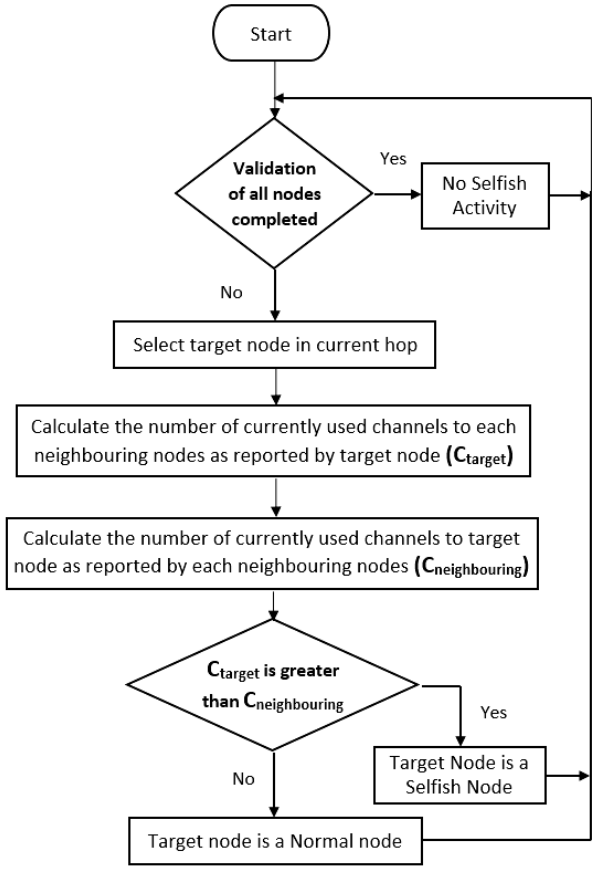

Figure 3 Selfish Attack Detection Flow Chart

5. RESULTS

The entire simulation is done for a comparative analysis. Firstly a spectrum sharing scenario is simulated wherein the Primary and Secondary users are allocated a random amount of channels. The number of channels allocated to either Primary or Secondary user is a dynamic value and it is designed to change over with time.

Secondly, the detection for Selfish Attack is simulated. The channel information is used to detect a conflict between the number stated by the target node and the one stated by the neighbouring node.

Figure 4 depicts the simulation output for a 128 channel spectrum with 115 channels allocated to Primary Users and 13 channels allocated to Secondary Users at that instance of time.

The detection mechanism shows that there are two selfish nodes. Their selfish activity results in the transmission of a fake channel information. As a result, 4 channels are wasted. Node two requires 3 channels but sends a fake information that it requires 5 channels. Similarly, Node five pretends as if it requires 4 channels whereas its actual requirement is of 2 channels only. It affects the performance of spectrum sensing and ultimately spectrum utilisation.

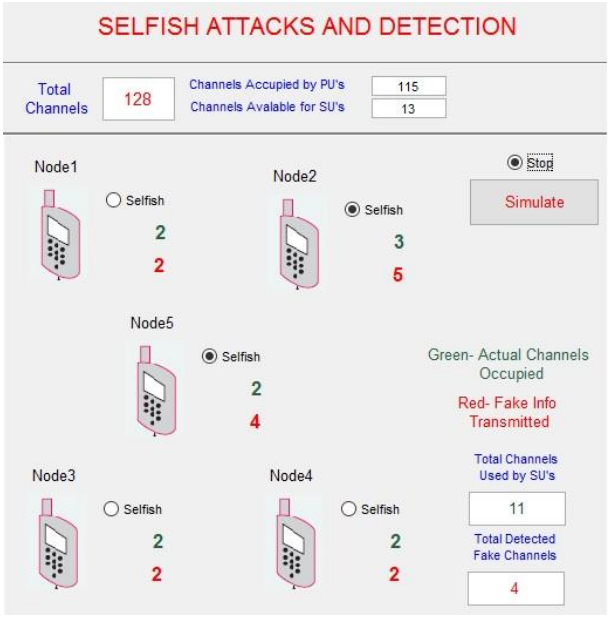

Figure 4 Simulation with Selfish Activity

Figure 5 simulates the output for a case where no selfish activity is prevalent in the system. The 128 channel spectrum is divided into 96 channels for Primary Users and 32 channels for Secondary Users.

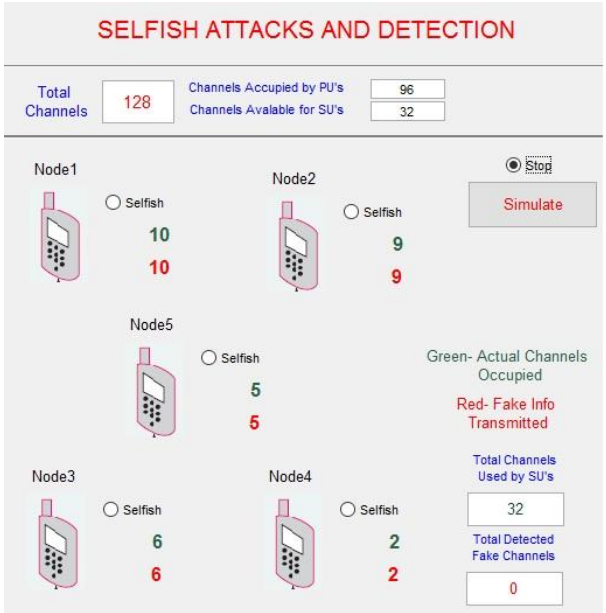

Figure 5 Simulation with no Selfish Activity

Figure 6 compares the results of performance of the system among three cases: no selfish activity, 20% selfish nodes and 40% selfish nodes. The probability of detection versus SU request graph shows that selfish activity degrades the performance of system considerably.

The simulation is carried out by plotting three graphs, one each for no selfish activity, one selfish node out of five nodes and two selfish nodes out of five respectively. The graph corresponding to no selfish activity outperformed the other two graphs by a huge margin as visible in the comparative analysis in figure 6.

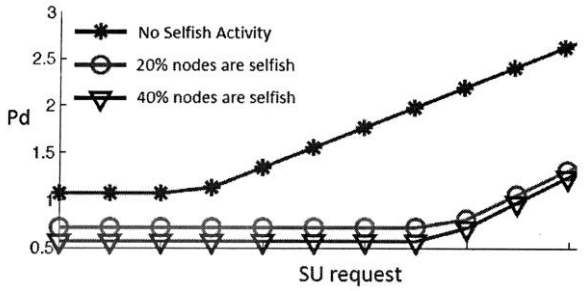

Figure 6 Probability of Detection versus SU Request graph

6. CONCLUSION

We proposed a detection approach for Selfish attacks in Cognitive Radio networks. Since we used the deterministic channel allocation information, the detection mechanism gave very highly reliable selfish attack detection results by simple computing. The proposed reliable and simple computing technique can be well fitted for practical use in the future. Our approach is designed for cognitive radio ad-hoc networks. We make use of ad-hoc network advantages such as autonomous and cooperative characteristics for better detection reliabilities.

For future work, we plan to apply Markov chain model and game theory to do theoretical analysis of more than one selfish SU in a neighbour, which is the major drawback of the proposed algorithm. We aim to improve this aspect of the algorithm to achieve higher levels of detection accuracy and ultimately much more improved spectrum utilisation.

7. REFERENCES

[1] 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.

[2] C. H. Chin, J. G. Kim, and D. Lee, "Stability of Slotted Aloha with Self- ish Users under Delay Constraint," KSII Trans. Internet and Info. Sys- tems, vol. 5, no. 3, Mar. 2011, pp. 542–549.

[3] 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, pp. 58–61.

[4] K. Cheng Howa, M. Maa, and Y. Qin, "An Altruistic Differentiated Ser- vice Protocol in Dynamic Cognitive Radio Networks Against Selfish Behaviors," Computer Networks, vol. 56, no. 7, 2012, pp. 2068–79.

[5] Jo, Minho, et al. "Selfish attacks and detection in cognitive radio ad-hoc networks." Network, IEEE 27.3 (2015): 46-50.