International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 4, July 2014, PP 223-233
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Attacks and Detection in Cognitive Radio System

Mr. Nilesh Rajendra Chougule
Student, KIT's College of Engineering
Kolhapur
nilesh_chougule18@yahoo.com

Dr. Y. M. Patil
Professor, KIT's college of Engineering,
Kolhapur
ymp2002@rediffmail.com

Abstract: *Cognitive Radio (CR) is a promising technology that can alleviate the spectrum shortage problem by enabling unlicensed users equipped with CRs to coexist with incumbent users in licensed spectrum bands while causing no interference to incumbent communications. Spectrum sensing is one of the essential mechanisms of CRs and its operational aspects are being investigated actively. However, the security aspects of spectrum sensing have garnered little attention. In this paper, we identify a various threats to spectrum sensing and detection to it*

Keywords: *Cognitive Radio, Communication System Security, Primary User Emulation Attack, Localization, Spectrum Sensing, Wireless Sensor Network, Primary User, Secondary User, Sensing*

1. Introduction

Cognitive Radios (CRs) [1-2] are seen as the enabling technology for DSA. Unlike a conventional radio, a CR has the capability to sense and understand its environment and proactively change its mode of operation as needed. CRs are able to carry out *spectrum sensing* for the purpose of identifying fallow licensed spectrum—i.e., spectrum "white spaces". Once white spaces are identified, CRs opportunistically utilize these white spaces by operating in them without causing interference to primary users. The successful deployment of CR networks and the realization of their benefits will depend on the placement of essential security mechanisms in sufficiently robust form to resist misuse of the system. Ensuring the trustworthiness of the spectrum sensing process is a particularly important problem that needs to be addressed. The key to addressing this problem is being able to distinguish primary user signals from secondary user signals in a robust way. Recall that, in a CR network, secondary users are permitted to operate in licensed bands only on a non-interference basis to primary users. Because the primary users' usage of licensed spectrum bands may be sporadic, a CR must constantly monitor for the presence of primary user signals in the current operating band and candidate bands. If a secondary user (with a CR) detects the presence of primary user signals in the current band, it must immediately switch to one of the fallow candidate bands. On the other hand, if the secondary user detects the presence of an unlicensed user, it invokes a coexistence mechanism1 to share spectrum resources. In this paper we are focusing on various attacks made on cognitive radio system and the defense to those attacks.

The above scenarios highlight the importance of a CR's ability to distinguish between primary user signals and secondary user signals. Distinguishing the two signals is nontrivial, but it becomes especially difficult when the CRs are operating in hostile environments. In a hostile environment, an attacker may modify the air interface of a CR to mimics primary user signal's characteristics, thereby causing legitimate secondary users to erroneously identify the attacker as a primary user. We coin the term *primary user emulation (PUE) Attack* to refer to this attack. There is a realistic possibility of PUE attacks CRs are highly reconfigurable due to their software-based air interface. To thwart such attacks, a scheme that can reliably distinguish between legitimate primary signal transmitters and secondary signal transmitters masquerading as primary users is needed. In hostile environments, such a scheme should be integrated into the spectrum sensing mechanism to enhance the trustworthiness of the sensing result. The current research and standardization efforts suggest that one of the first applications of CR technology will be its use for DSA of fallow TV spectrum bands. In PUE attacks, the adversary only transmits in fallow bands. Hence, the aim of the attackers is not to cause interference to primary users, but to preempt spectrum resources that could have been used by legitimate secondary users. Depending on the motivation behind the attack, a PUE attack can be classified as either a selfish PUE attack or a malicious

1.1. PUE Attacks

Selfish PUE attacks: In this attack, an attacker's objective is to maximize its own spectrum usage. When selfish PUE attackers detect a fallow spectrum band, they prevent other secondary users from competing for that band by transmitting signals that emulate the signal characteristics of primary user signals. This attack is most likely to be carried out by two selfish secondary users whose intention is to establish a dedicated link.

Malicious PUE attacks: The objective of this attack is to obstruct the DSA process of legitimate secondary users— i.e., prevent legitimate secondary users from detecting and using fallow licensed spectrum bands, causing denial of service. Unlike a selfish attacker, a malicious attacker does not necessarily use fallow spectrum bands for its own communication purposes. It is quite possible for an attacker to simultaneously obstruct the DSA process in multiple bands by exploiting two DSA mechanisms implemented in every CR. The first mechanism requires a CR to wait for a certain amount of time before transmitting in the identified fallow band to make sure that the band is indeed unoccupied. Existing research shows that this time delay is non-negligible. The second mechanism requires a CR to periodically sense the current operating band to detect primary user signals and to immediately switch to another band when such signals are detected. By launching a PUE attack in multiple bands in a round-robin fashion, an attacker can effectively limit the legitimate secondary users from identifying and using fallow spectrum bands.

1.2. A Transmitter Verification Scheme for Spectrum Sensing

The primary user is assumed to be a network composed of TV signal transmitters (i.e., TV broadcast towers) and receivers. A TV tower's transmitter output power is typically hundreds of thousands of Watts, which corresponds to a transmission range from several miles to tens of miles. We assume that the secondary users, each equipped with a hand-held CR device, form a mobile ad hoc network. Each CR is assumed to have self-localization capability and have a maximum transmission output power that is within the range from a few hundred mill watts to a few watts—this typically corresponds to a transmission range of a few hundred meters. An attacker, equipped with a CR, is capable of changing its modulation mode, frequency, and transmission output power.

As Fig.1 shows Transmitter verification scheme for spectrum sensing that is appropriate for hostile environments. In the network model under consideration, the primary signal transmitters are TV broadcast towers placed at fixed locations. Hence, if a signal source's estimated location deviates from the known location of the TV towers and the signal characteristics resemble those of primary user signals, then it is likely that the signal source is launching a PUE attack. An attacker, however, can attempt to circumvent this location-based detection approach by transmitting in the vicinity of one of the TV towers. In this case, the signal's energy level in combination with the signal source's location is used to detect PUE attacks. It would be infeasible for an attacker to mimic both the primary user signal's transmission location and energy level since the transmission power of the attacker's CR is several orders of magnitude smaller than that of a typical TV tower. Once an instance of a PUE attack has been detected, the estimated signal location can be further used to pinpoint the attacker.

In above theory of proposed work it is shown that the probability of a successful PUE attack increases with the distance between the primary transmitter and secondary users and proposed localization-based defense strategies against the PUE attack, RSS-based localization was used to determine the location of the attacker by deploying an additional sensor network. The authors employed a no interactive localization scheme to locate the attacker.

2. DEFEATING PRIMARY USER EMULATION ATTACKS USING BELIEF PROPAGATION IN COGNITIVE RADIO NETWORKS

In previous method of detection as mentioned above some problems were located to overcome those disadvantages the approach of verification is mentioned below. Strategy against the PUE attack in CR networks using belief propagation, which avoids the deployment of additional sensor Networks and expensive hardware in the networks used in the existing literatures. In our proposed approach, each secondary user calculates the local function and the compatibility function, computes the messages, exchanges messages with the neighboring users, and calculates the beliefs until convergence. Then, the PUE attacker will be detected, and all the secondary users in the network will be notified in a broadcast way about the characteristics of the attacker's signal. Therefore, all SUs can avoid the PUE attacker's primary emulation signal in the future. Simulation results show that our proposed approach converges quickly, and is effective to detect the PUE attacker.

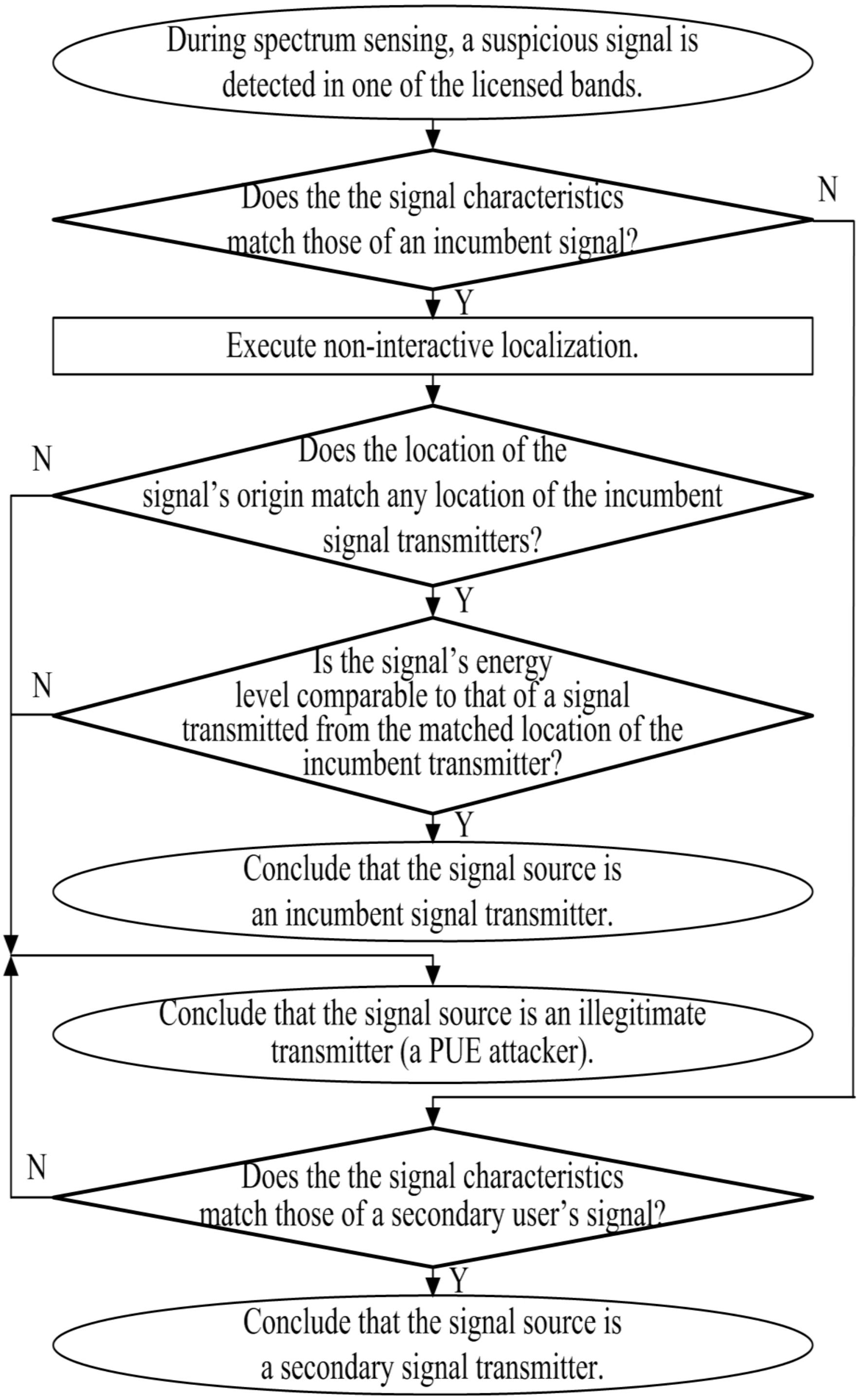

Fig1. *A flowchart of the transmitter verification scheme*

However, the CR wireless networks are susceptible to various attacks [4-6] .An attack called primary user emulation (PUE) has been emerged in CR wireless networks, in which the malicious nodes emulate the feature of primary user's signal characteristics and transmit in available secondary spectrum when PUs are inactive in CR networks. As a result, the naive secondary users may believe that the PUs are present and avoid using the actually available spectrum bands (or channels). In this case, the malicious nodes can occupy the whole licensed [7-9] spectrum by themselves, or just make the precious licensed channels wasted. Recently, a more dangerous PUE attack has been discovered, in which the attacker predicts which channel will be used by the secondary users and attacks on those particular channels. Simulation shows that the PUE attack is so serious that it can significantly increase the spectrum access failure probability .In this paper, we propose new received signal strength (RSS)-based defense strategy against the PUE attack in CR wireless networks. By comparing the distribution of the received signal power from the suspect and that from the primary user, each secondary user can have an approximate belief about the

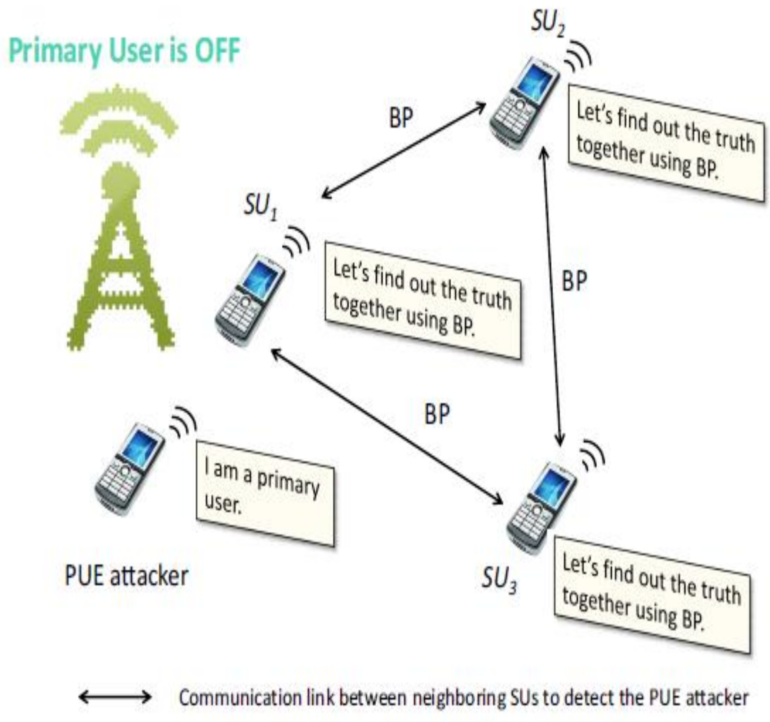

Fig2. *Illustration of belief propagation based detection against PUE attack in cognitive radio networks*

Probability that whether a suspect is a PUE attacker or not, since the secondary user has no knowledge about the transmission output power of the attacker, as well as the distance from the attacker to the secondary user. In addition, the channel shadowing fading between each secondary user and the attacker may vary significantly. To accurately identify the attacker, a defense strategy based on belief propagation (BP) is developed in this paper. As shown in Fig. 2, when the primary user is inactive, the PUE attacker will send primary user emulation signals to attack the cognitive radio network. When SUs receive this signal, they will perform local observations, and then use BP to exchange the information to detect whether the signal is from a PUE attacker to not. Each user will use the local functions to calculate the local estimation of the suspect, compute the compatibility functions to model the interactions between neighboring users, and update and exchange messages with the neighboring users in an iterative way using BP. After convergence, the PUE attacker can be detected according to the mean of all the final beliefs. If the mean of final belief values is lower than a threshold, the suspect can be detected as a PUE attacker. Otherwise, the suspect is seen as an honest secondary user. After that, all the secondary users in the network will be notified in a broadcast way about the PUE attacker's characteristics, and ignore the PUE attacker's primary emulation signal in the future. We also prove some properties of the proposed BP algorithm. Simulation results show that our proposed approach converges very fast, and is effective to detect the PUE attacker.

2.1. Advantages

No additional cost is required for new hardware. We do not need to purchase wireless sensors and deploy an additional sensor network, which is required in method discussed in I. Also in this framework, different from, we do not need to calculate the exact location of the PUE suspect. Instead, we only need to exchange the beliefs between the neighboring users, and the attacker is identified by the final belief value.

3. SELFISH ATTACK

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 wireless 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. In this article, we identify a new selfish attack type and introduce a selfish attack detection technique, COOPON (called Cooperative neighboring cognitive radio Nodes), for the attack type. We focus on

Selfish attacks of SUs toward multiple channel access in cognitive radio ad-hoc networks. We assume that an individual SU accommodates multiple channels. Each SU will regularly broadcast the current multiple channel allocation information to all of its neighboring 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 selfish SU will send a larger number of channels in current use than real in order to reserve available channels for later use. The COOPON will detect the attacks of selfish SUs by the cooperation of other legitimate neighboring SUs. All neighboring SUs exchange the channel allocation information both received from and sent to the target SU, which will be investigated by all of its neighboring SUs. The target SU and its neighboring SUs are 1-hop neighbors. Then, 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 neighboring SUs. If there is any discrepancy between the two figures, all of the legitimate SUs will recognize a selfish attacker.

3.1. Types of Selfish Attacks

3.1.1. Attack Type 1

Selfish attacks are different depending [10] on what and how they attack in order to pre-occupy CR spectrum resources. There are three different selfish attack types shown in Fig. 3. 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.

3.1.2. 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. 3 , 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.

3.1.3. 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 neighboring 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 neighboring SUs, as illustrated in Fig. 3 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. In this article, we identify the new selfish attack type 3 and propose the COOPON, which is designed for detecting Type 3 selfish attack.

3.2. Attack and Detection Mechanism

3.2.1. Attack Mechanism

In a cognitive radio network, the common control channel (CCC) is used to broadcast [10] and exchange managing information and parameters to manage the CR network among secondary ad-hoc users. The CCC is a channel dedicated only to exchanging managing information and parameters. A list of current channel allocation information is broadcast to all neighboring SUs as shown in Fig. 3. The list contains all of other neighboring users' channel allocation information. Type 3 in Fig. 3 shows that 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.

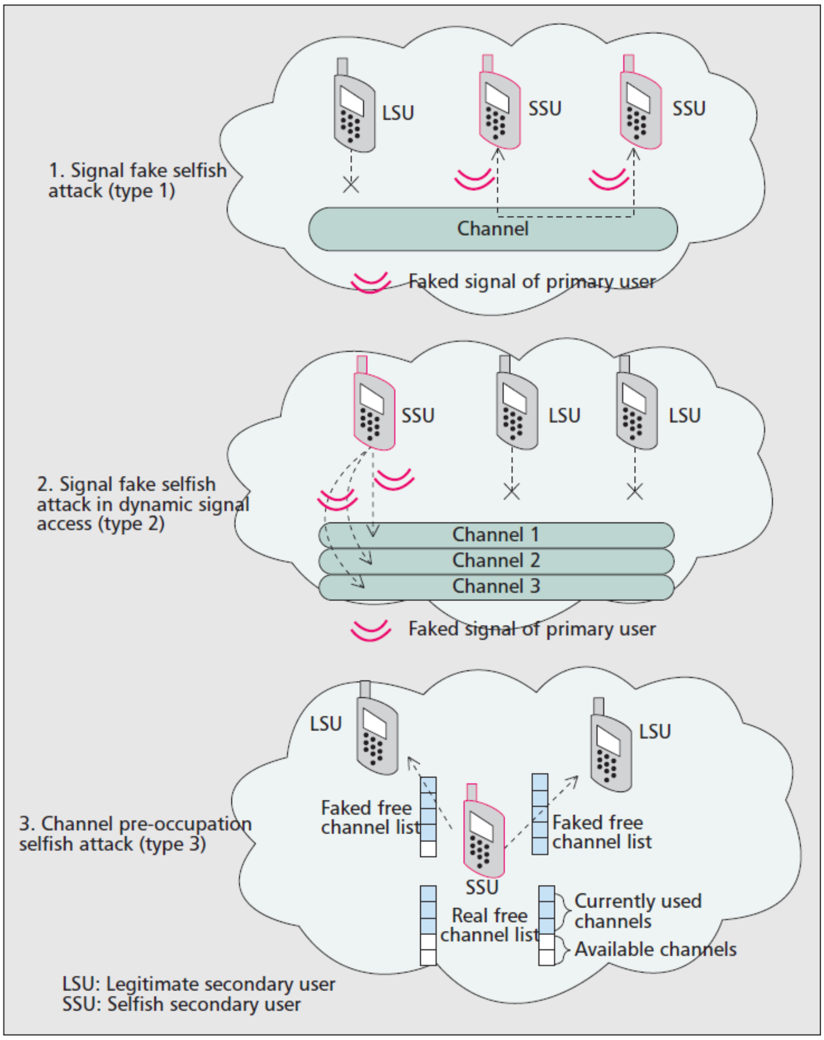

Fig3. *3 different attack types*

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. In Type 3 of Fig. 3, 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.

3.2.2. Detection Mechanism

Use of Channel Allocation Information — we consider a cognitive radio ad-hoc network. Ad-hoc networks have distributed and autonomous management characteristics. Our proposed detection mechanism in COOPON is designed for an adhoc 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 Fig. 4, 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, TNode/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 cannels 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, TNode. 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 COOPON selfish attack detection method is very reliable since it is based on deterministic information.

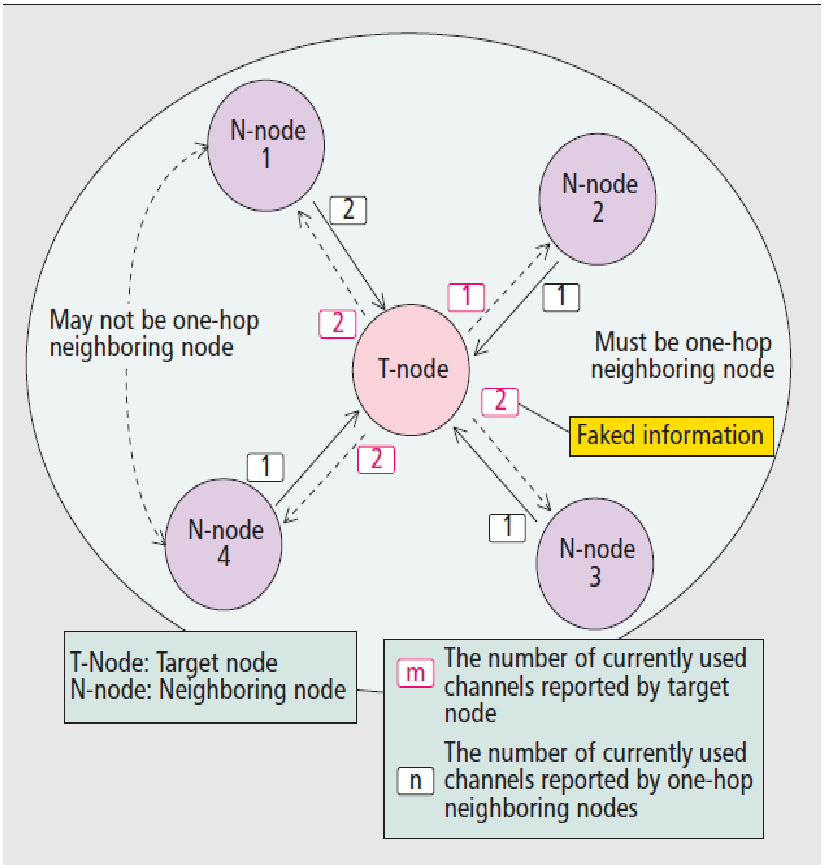

Fig4. *Selfish attack detection mechanism*

However, COOPON has a drawback. When there is more than one neighboring selfish node, COOPON 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.

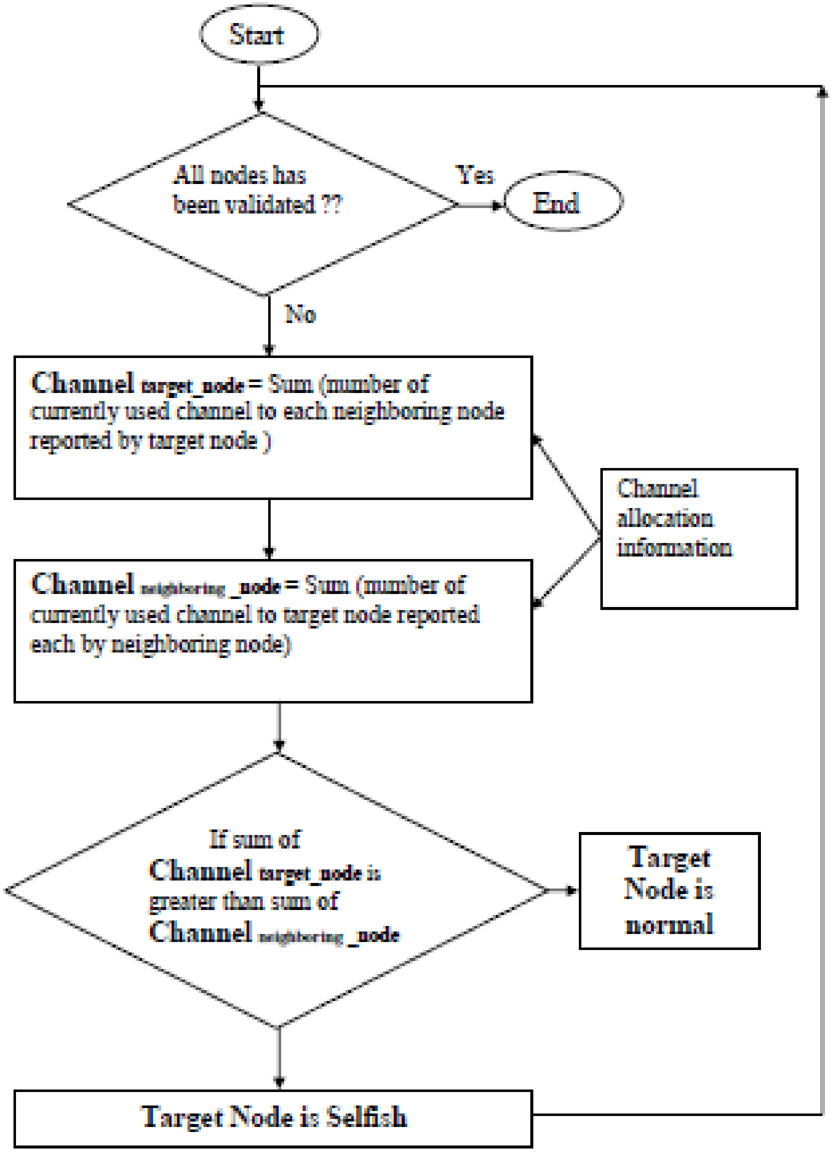

Fig5. *Algorithm for Detection Mechanism*

3.3. Simulation Environment

We conducted the simulation using MATLAB to verify the efficiency of COOPON. The efficiency is measured by a detection rate, which is the proportion of the number of selfish SUs detected by COOPON to the total number of actual selfish SUs in a CR network: One SU has a maximum of eight data channels and one common control channel. The channel data rate is 11 Mb/s. In simulation, one SU can have two to five one-hop neighboring SUs. The experiment was performed under various selfish SU densities in a CR network. The detailed simulation parameters are presented in Table 1.Simulation Results and Analysis. In order to investigate how much selfish SU density influences detection accuracy, the experiment was carried out with 50,100, and 150 SUs, respectively, as shown in Fig. 5. From Fig. 6, we can see that 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 reason why this problem occurs is that it is a higher possibility that more than one selfish SU exists in a neighbor with higher selfish node density, and in turn, they can exchange wrong channel allocation information. Obviously it is a higher possibility that a wrong decision can be made with more faked exchanged information. As mentioned before, because selfish nodes may broadcast faked channel allocation information, it will be more difficult to detect selfish attacks when both information exchanging nodes send fake channel allocation information. In other words, the capability of detecting attacks will decrease when more selfish nodes exist in a neighbor. However in reality the density of selfish SUs is not that high, at most 3–4 percent in a CR network. So the detection accuracy of our proposed selfish attack detection technology, COOPON, can still be more than 97 percent. The experimental results in Fig. 7 give an insight into how the number of nodes in a neighbor will influence selfish detection accuracy. Intuitively, if we have more neighboring nodes in a neighbor, detection accuracy may be less negatively affected, because we can have a possibility to receive more correct channel allocation information from more legitimate SUs. Thus, we did simulation with a cognitive radio network with two neighboring nodes to five neighboring nodes. For the first CR network all of neighbors have only two neighboring nodes; for the second CR network all of neighbors have only three neighboring nodes; for the third CR network all of neighbors have only four neighboring nodes; and for the fourth CR network all of the neighbors have only five neighboring nodes. The experiment to answer this question was made and the results are shown in Fig. 7. One hundred secondary users were used in this experiment. Five neighboring SUs in a CR ad-hoc network achieve very high accuracy regardless of selfish SU density. Four neighboring SUs also provide very high accuracy and are trivially influenced by the density of selfish SUs. However, we notice that two SUs in a neighbor are negatively affected by the density of selfish SUs. Thus, more than three SUs in a neighbor of a CR ad-hoc network are recommended in order to avoid selfish CR attacks

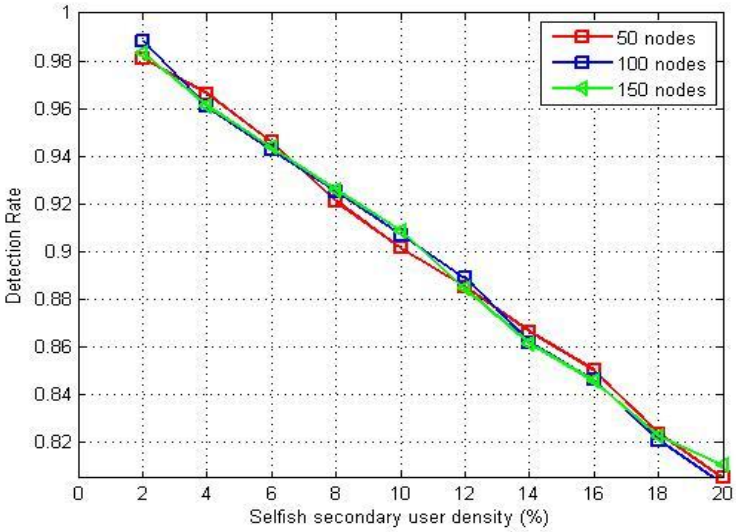

Fig6. *Selfish SU detection rate vs. selfish SU density*

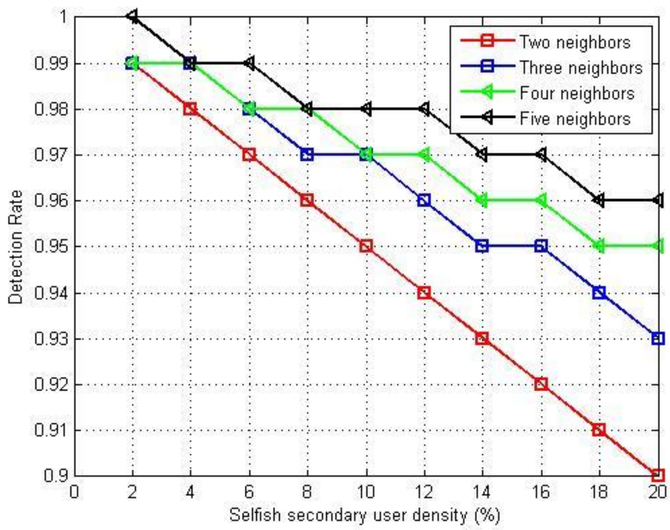

Fig7. *Detection rate vs. number of neighboring nodes*

3.4. Simulation Details

Here we have simulated for finding the selfish node in fig 8, here there is random allocation of the channel and the following steps are involved in the finding the selfish node

1. The number of channels detected unused is found out firstly ,as this value will be changing this is random allocation is done
2. The matrix is generated with FIVE neighbor where left hand side part indicating the source and top side the destination
3. Alternatively every node act as an secondary target node and share the information to neighbor and the neighbor also doing the same
4. The element in row R1 indicates the total information shared by target node to the neighbor and column C1 indicates the information shared by neighbor to the target node
5. For Ex. As shown in figure a matrix of five rows and five columns is been generated

Fig8. *Selfish Node detection*

In this the first element of first row and column is 0(zero) indicating that the node N1 is target and is sharing the information of channels available to its neighbor indicated in rows i.e N1 to N2 is 4 ,N1 to N3 is 1 and so on

6. The column element indicates the information share by neighbor N2, N3, N4, N5 to the target node in first column and second, third, fourth, fifth row respectively.
7. Now the summation of all elements in first row and all elements from first column is done and then they are compared and the decision is made based on it
8. If

   - Summation of all elements in row = Summation of elements in column then the target node is not the selfish node
   - Summation of all elements in row > Summation of elements in column then the target node is the selfish node

- Summation of all elements in row < Summation of elements in column then the target node is not the selfish node any of the neighboring node is the selfish one

9. The greater the difference between the summation of the particular node that node is the selfish node.

4. Conclusion

We identify a new selfish attack type, named Type 3 in this article, and made a detection approach for it, COOPON. Because we use the deterministic channel allocation information, COOPON gives very highly reliable selfish attack detection results by simple computing. The proposed reliable and simple computing technique can be well fitted for practical use. 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 can plan to apply Markov chain model and game theory to do theoretical analysis of more than one selfish SU in a neighbor, which gives less detection accuracy.

References

[1] 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.

[2] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," Proc. IEEE Infocom, Apr. 2006. I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt

[3] Ruiliang Chen, Jung-Min Park, and Jeffrey H. Reed " Defense against Primary User Emulation Attacks in Cognitive Radio Networks " IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 26, NO. 1, JANUARY 2008.

[4] J. Mitola III, Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio, Ph.D. thesis, KTH Royal Institute of Technology, 2000.

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

[6] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security: A Survey," IEEE Commun. Surveys Tuts., vol. 11, pp. 52-73, Jun. 2009.

[7] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof Collaborative Spectrum Sensing in Cognitive Radio Systems," in Proc. Conferenc on Information Sciences and Systems (CISS'09), Mar. 2009.

[8] K. Bian and J. M. Park, "Mac-layer Misbehaviors in Multi-hop Cognitive Radio Networks," in Proc. 2006 US - Korea Conference on Science,Technology, and Entrepreneurship (UKC2006), Aug. 2006.

[9] Zhou Yuan, Dusit Niyato, Husheng Li, Ju Bin Song, and Zhu Han " Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 30, NO. 10, NOVEMBER 2012

[10] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In, Korea University "Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks"