# Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks

**Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In, Korea University**

**Abstract**

Cognitive radio is an opportunistic communication technology designed to help unlicensed users utilize the maximum available licensed bandwidth. Cognitive radio has recently attracted a lot of research interest. However, little research has been done regarding security in cognitive radio, while much more research has been done on spectrum sensing and allocation problems. A selfish cognitive radio node can occupy all or part of the resources of multiple channels, prohibiting other cognitive radio nodes from accessing these resources. Selfish cognitive radio attacks are a serious security problem because they significantly degrade the performance of a cognitive radio network. In this article we identify a new selfish attack type in cognitive radio ad-hoc networks and propose an easy and efficient selfish cognitive radio attack detection technique, called COOPON, with multichannel resources by cooperative neighboring cognitive radio nodes.

Cognitive radio (CR) is an opportunistic communication technology designed to utilize the maximum available licensed bandwidth for unlicensed users. As wireless communication devices have been tremendously widespread, we have faced excessive spectrum demands and the need to better utilize the available spectrum. In traditional spectrum management, most of the spectrum is allocated to licensed users for exclusive use. CR technology is carried out in two steps. First, it searches for available spectrum bands by a spectrum-sensing technology for unlicensed secondary users (SUs). When the licensed primary user (PU) is not using the spectrum bands, they are considered available. Second, available channels will be allocated to unlicensed SUs by dynamic signal access behavior. Whenever the PU is present in the CR network, the SU will immediately release the licensed bands because the PU has an exclusive privilege to use them [1–3].

CR nodes compete to sense available channels [4–6]. 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. Our proposed technique is an intuitive approach and simple to compute, but reliable due to using deterministic channel allocation information as well as the support of cooperative neighboring nodes. We have proven the reliability of COOPON by simulation.

The rest of this article is organized as follows. We will discuss several existing selfish attack detection methods in the related work section. Three different selfish attack types are introduced in the types of selfish attacks section. Our proposed attack and detection technique is presented in the attack and detection mechanism section. We prove the reliability and efficiency of our proposed work, COOPON, in the simulation sections. In the last section, we conclude the article and mention future work.


0890-8044/13/$25.00 © 2013 IEEE

## Related Work

Due to the characteristics of the dynamic behavior of CR, selfish attack detection technology for a conventional wireless communication network cannot be used for detecting selfish attacks in CR networks. For CR selfish attacks, Chen *et al*. first identified a threat to spectrum sensing, called PU emulation attack, in 2008 [7]. In this attack, a selfish attacker transmits signals that emulate the characteristics of PU signals. The emulated signals make legitimate SUs misunderstand that a PU is active, and so the faked signals obstruct SU access to the available spectrum band. Then the selfish SU will pre-occupy the available bands. They detect the faked PU's signals by transmitter verification. Transmitter verification determines the legitimate source signal by signal energy level combined with the source signal location. In 2011, Yan *et al*. applied the game-theoretic approach, Nash equilibrium, to prevent selfish attacks [8]. Selfish attacks are made by a selfish SU that increases the access probability by reducing the backoff window size in a CSMA-based CR network. This selfish attack is a sort of denial-of-service. In 2012, a cross-layer altruistic differentiated service protocol (ADSP) was proposed for dynamic cognitive radio networks to consider the quality of service provisioning in CRNs with selfish node coexistence [9]. Their objective is to give lower delay, higher throughput, and better delivery ratios for a cognitive radio network. Reputation is assigned to each SU based on historical selfish behavior data. A better reputation assigned to less selfish nodes will further reduce the chance of a failed delivery. Routing is negotiated with the reputation of a SU. Our identified attack type and proposed detection technique, COOPON, is different from the previous ones in the communication environments and conditions. COOPON is designed for CR ad-hoc networks with multiple channels and is designed for the case that channel allocation information is broadcast for transmission.

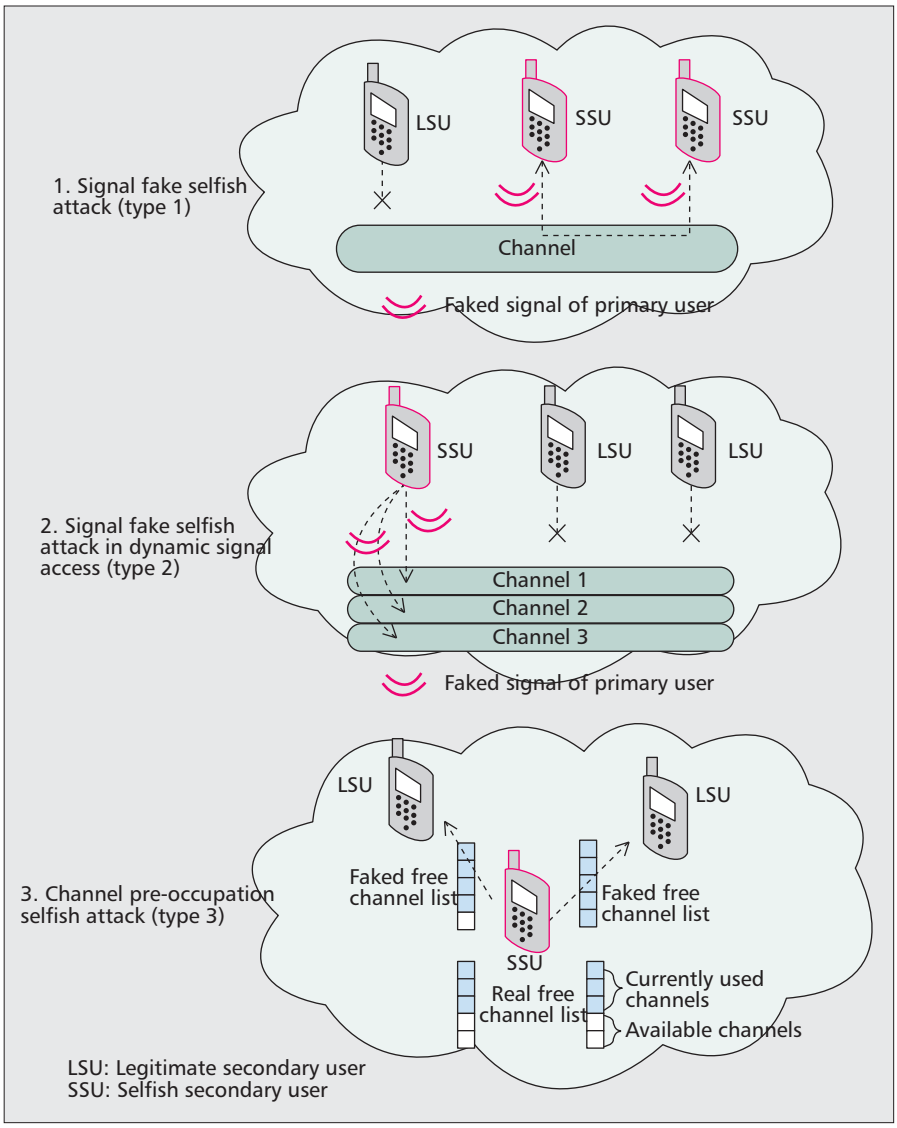


**Figure 1.** *3 different attack types.*

## Types of Selfish Attacks

### Attack Type 1

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. 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.

### 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.

### 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. 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

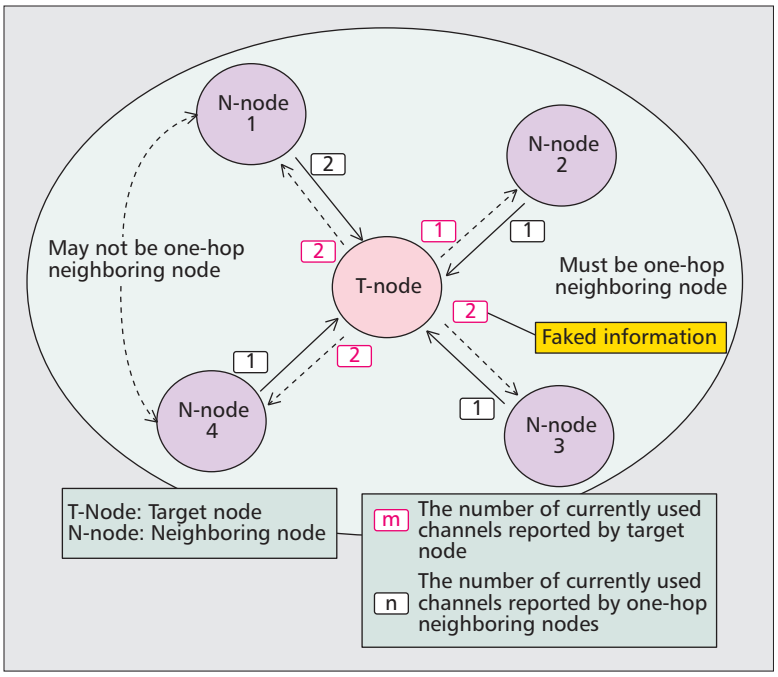


**Figure 2.** *Selfish attack detection mechanism.*

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.

## Attack and Detection Mechanism

### Attack Mechanism

In a cognitive radio network, the common control channel (CCC) is used to broadcast 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. 1. The list contains all of other neighboring users' channel allocation information. Type 3 in Fig. 1 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. 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. 1, 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.

### 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 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 Fig. 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 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, 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 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, 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 COOPON selfish attack detection method is very reliable since it is based on deterministic information. 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. Simulation to prove this claim was done, and we show the results in the next section.

*Detection Algorithm* — Figure 3 shows the proposed selfish attack detection algorithm flow chart of COOPON. As we mentioned above, all currently used channels in the target node and neighboring nodes are summed up in two steps $\text{Channel}_{\text{target\_node}}$ and $\text{Channel}_{\text{neigboring\_node}}$. Then $\text{Channel}_{\text{target\_node}}$ will be compared to $\text{Channel}_{\text{neigboring\_node}}$. According to the example in Fig. 2, $\text{Channel}_{\text{target\_node}}$ is 7 (2+1+2+2) and $\text{Channel}_{\text{neigboring\_node}}$ 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 COOPON will check the next neighboring node after it selects one of the unchecked neighboring secondary nodes as a target node.

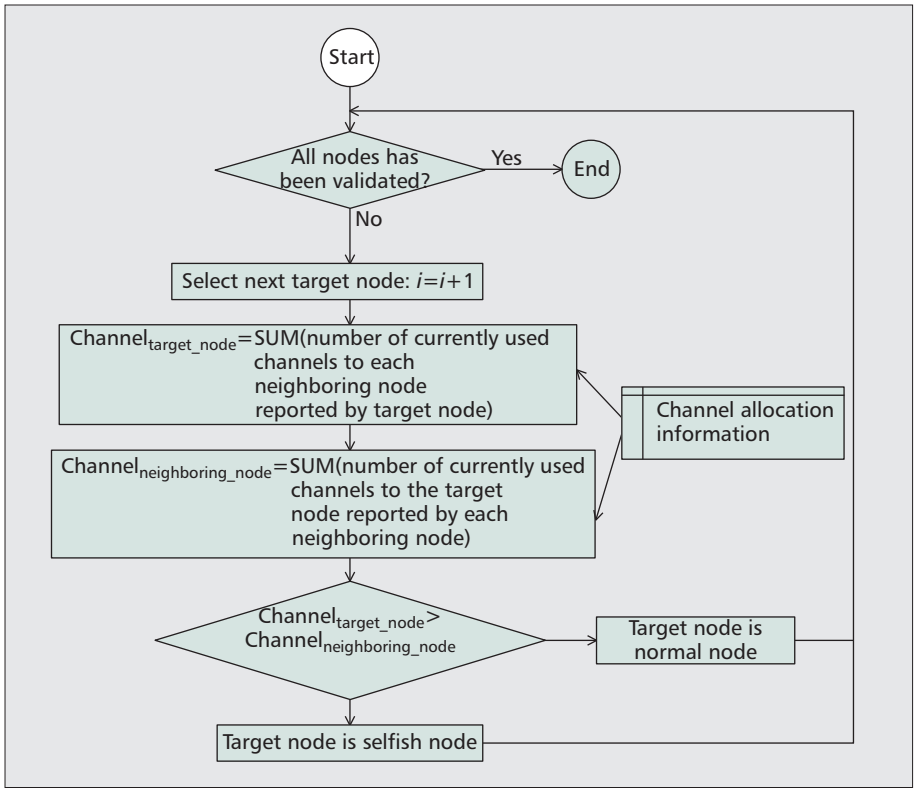


**Figure 3.** *Selfish attack detection algorithm.*

This detection procedure will continue until the last SU in a CR network is validated.

## Simulation Environment

We conducted the simulation using ns-2 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:

$$\text{Detection Rate} = \frac{\text{number of detected selfish secondary users}}{\text{number of actual selfish secondary users}}$$

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. 4. From Fig. 4, 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

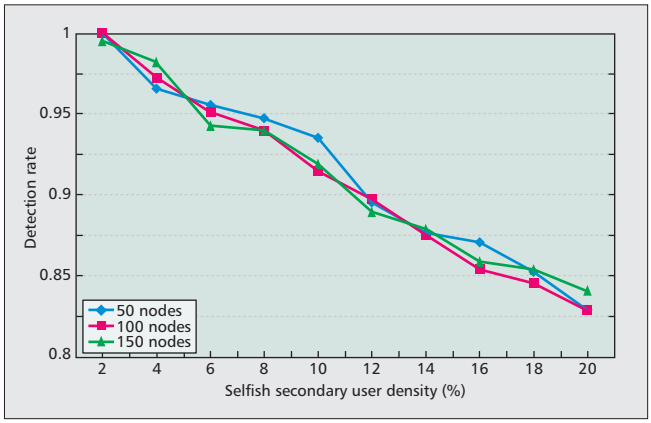


**Figure 4.** *Selfish SU detection rate vs. selfish SU density.*

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. 4 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

| Parameter | Setting |
|---|---|
| Antenna type | OmniAntenna |
| Propagation model | TwoRayGround |
| Network size | 3000m × 3000m |
| Routing protocol | Ad Hoc On-demand Multipath Distance Vector Routing |
| MAC protocol | IEEE 802.11b with extension to support CR networks |
| Data channel | 8 |
| Common control channel | 1 |
| Channel data rate | 11 M bits/s |
| Number of SUs | 50, 100, 150 |
| Number of selfish SUs | 2%, 4%, 6%, 8%, 10%, 12%, 14%, 16%, 18%, 20% |

Table 1. *Simulation environment.*

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. 5. 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.

## Conclusion

We identify a new selfish attack type, named Type 3 in this article, and propose 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 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 neighbor, which gives less detection accuracy.

For further research results, please contact the corresponding author, Prof. Hoh P In, at hoh_in@korea.ac.kr.

## Acknowledgement

This article was supported in part by a National Research Foundation of Korea grant funded by the Korea government (MEST) (No. 2011-0009454), and by Seoul R&BD Program (WR080951), and by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012M3C4A7033345).

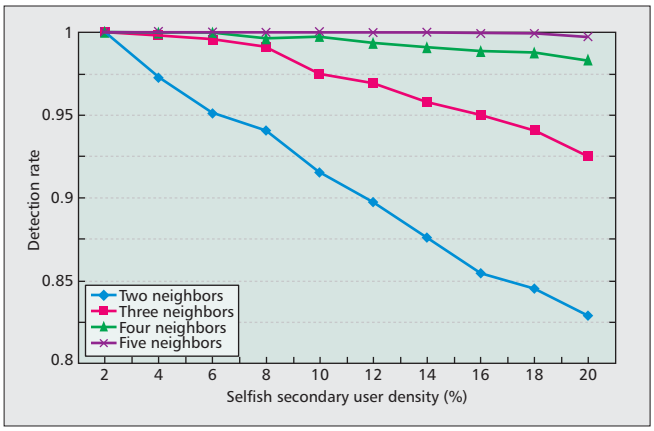


Figure 5. *Detection rate vs. number of neighboring nodes.*

## References

[1] X. Tan and H. Zhang, "A CORDIC-Jacobi Based Spectrum Sensing Algorithm for Cognitive Radio," *KSII Trans. Internet and Info. Systems*, vol. 6, no. 9, Sept. 2012, pp. 1998–2016.
[2] C.-H. Chin, J. G. Kim, and D. Lee, "Stability of Slotted Aloha with Selfish Users under Delay Constraint," *KSII Trans. Internet and Info. Systems*, vol. 5, no. 3, Mar. 2011, pp. 542–59.
[3] S. Li *et al.*, "Location Privacy Preservation in Collaborative Spectrum Sensing," *IEEE INFOCOM'12*, 2012, pp. 729–37.
[4] Z. Gao *et al.*, "Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks," *IEEE Wireless Commun.*, vol. 19, no. 6, 2012, pp. 106–12.
[5] Z. Dai, J. Liu, and K. Long, "Cooperative Relaying with Interference Cancellation for Secondary Spectrum Access," *KSII Trans. Internet and Information Systems*, vol. 6, no. 10, Oct. 2012, pp. 2455–72.
[6] H. Hu *et al.*, "Optimal Strategies for Cooperative Spectrum Sensing in Multiple Cross-over Cognitive Radio Networks," *KSII Trans. Internet and Info. Systems*, vol. 6, no. 12, Dec. 2012, pp. 3061–80.
[7] 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.
[8] 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.
[9] K. Cheng Howa, M. Maa, and Y. Qin, "An Altruistic Differentiated Service Protocol in Dynamic Cognitive Radio Networks Against Selfish Behaviors," *Computer Networks*, vol. 56, no. 7, 2012, pp. 2068–79.

## Biographies

MINHO JO received his Ph.D. in Dept. of Industrial and Systems Engineering, Lehigh Univ., USA in 1994. He is a BK professor of College of Information and Communication at Korea University, Seoul. He is the Founder and Editor-in-Chief of KSII Transactions on Internet and Information Systems. He is an editor of IEEE Network. He has published many refereed academic publications in very high quality journals and magazines. Areas of his current interest include cognitive radio, network algorithms, optimization and probability in networks, network security, wireless communications and mobile computing.

LONGZHE HAN received the M.S. degree in computer software from Myongji University, in 2006. He is a Ph.D. candidate in College of Information and Communication at Korea University, Seoul. His research interests are cognitive radio networks, information centric networks, network security, multimedia communications, wireless networks and embedded software engineering.

DOHOON KIM received the B.S. in mathematics and double degree in computer science & engineering at Korea University, Seoul, in 2005. He received Ph.D. degrees in College of Information and Communication from Korea Univ. in 2012. He is a senior researcher in the IT Management & Support Office from Agency for Defense Development. His current research interests are network security, risk management, cognitive radio networks, software engineering, situation awareness, future internet and forecast engineering.

HOH PETER (hoh_in@korea.ac.kr) IN received his Ph.D. in Computer Science from University of Southern California (USC). He is a professor in College of Information and Communication at Korea University, Seoul. His primary research interests are cognitive radio networks, embedded software engineering, social media platform and service, and software security management. He earned the most influential paper award for 10 years in ICRE 2006. He published over 100 research papers.