



COOPON for Selfish Attack Detection in Cr Ad-Hoc Networks

¹T.Jenefa, ²Mr.E.Sivanantham

Dhanalakshmi Srinivasan College of Engineering and Technology, Mamallapuram, Chennai.

Abstract- Cognitive radio is an opportunistic communication technology designed to help unlicensed users utilize the maximum available licensed bandwidth. Selfish cognitive radio attacks are a serious security problem because they significantly degrade the performance of a cognitive radio network. The proposed work provides selfish cognitive radio attack detection technique, called COOPON, which will detect the attacks of selfish Secondary Users by the cooperation of other legitimate neighboring SUs. The COOPON algorithm make use of the autonomous decision capability of an ad-hoc communication network based on exchanged channel allocation information among neighboring SUs.

Index Terms- cognitive radio, secondary user

I. INTRODUCTION

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. 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. Selfish attacks are different depending on what and how they attack in order to pre-occupy CR spectrum resources. The various selfish attacks present in networks has been illustrated in fig1.1

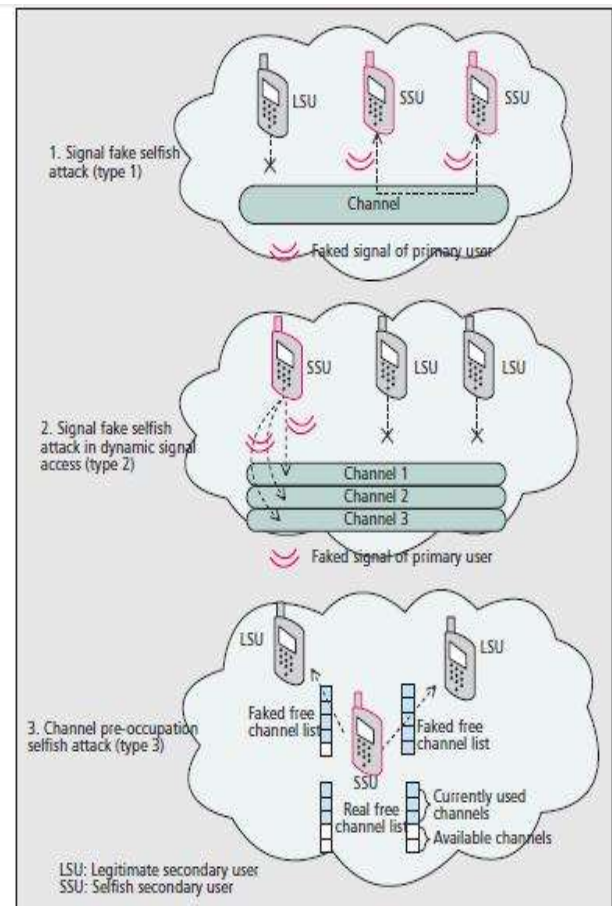




Fig 1.1 Types Of Attacks

1.1 Types of Selfish Attacks

1.1.1 Attack Type

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 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.

1.1.3 Attack Type 3

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. Even though a selfish SU only uses three channels, it will send a list of all five occupied. Thus, a legitimate SU is prohibited from using the two available channels.

1.2 Attack and Detection Mechanism

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.

Fig 1.2 Selfish attack detection mechanism.

In Fig 1.2, 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.

Our proposed COOPON selfish attack detection method is very reliable since it is based on deterministic information. We focus on selfish attacks of SUs toward multiple channel access in cognitive radio ad-hoc networks.

II. LITERATURE REVIEW

2.1 Multi-hop Cognitive Mesh Networks

Manuj Sharma, Anirudha Sahoo, and K. D. Nayak proposed a Channel Selection under Interference Temperature Model in Multi-hop Cognitive Mesh Networks. Here a cognitive radio-based wireless mesh network is considered.

Each mesh node senses the channels of a target primary system to identify the spectrum opportunities, and uses them for its own data transmission. Interference temperature model is used to define the occupancy and availability of a channel. A cooperative algorithm based on interference temperature model is proposed for computation of available channels by mesh nodes. Cases for mesh nodes with fixed transmission power and adaptive transmission power are considered separately. Link and end-to-end routing metrics are proposed to select



appropriate channels from the computed set of available channels.

2.2 Adaptive Spectrum Sharing

Haythem A. Bany Salameh, Marwan Krunz, and Ossama Younis introduced a Cooperative Adaptive Spectrum Sharing in Cognitive Radio Networks. The cognitive radio (CR) paradigm calls for open spectrum access according to a predetermined etiquette.

Under this paradigm, CR nodes access the spectrum opportunistically by continuously monitoring the operating channels. A key challenge in this domain is how the nodes in a CR network (CRN) cooperate to access the medium in order to maximize the CRN throughput. Typical multichannel MAC protocols assume that frequency channels are adjacent and that there are no constraints on the transmission





multichannel CSMA-based protocols, DDMAC reduces the blocking rate of CR requests by up to 30%, which consequently improves the network throughput.

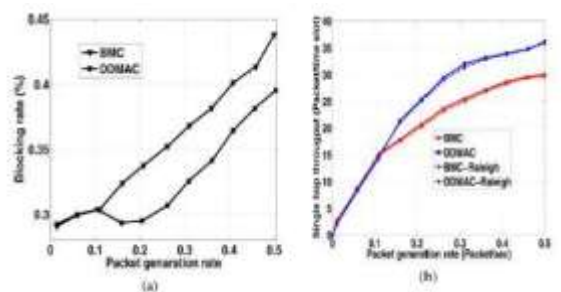


Fig 2.1 Performance of a CRN.

2.3 Distributed Relay-Assignment

Ahmed K. Sadek, Zhu Han, Senior Member and K.J. Ray Liu, Fellow introduced a method called Distributed Relay Assignment Protocols for Coverage Expansion in Cooperative Wireless Networks.

One important application of cooperative communications is to extend coverage area in wireless networks without increasing infrastructure. However, a crucial challenge in implementing cooperation protocols is how to select relay-source pairs. So addressing this problem based on the knowledge of the users' spatial distribution which determines the channel statistics.

Considering two scenarios at the destination node, when the receiver uses MRC and when no-MRC is used. First we characterizing optimal relay location to minimize the outage probability. Then propose and analyze the performance of two schemes: a distributed nearest neighbor relay assignment in which users can act as relays, and an infrastructure-based relay-assignment protocol in which fixed relay nodes are

deployed in the network to help the users forward their data. The outage probabilities of these two schemes are derived. Also deriving universal lower bounds on the performance of relay-assignment protocols to serve as a benchmark for our proposed protocols. Numerical results reveal significant gains when applying the proposed simple distributed algorithms over direct transmission in terms of coverage area, transmit power, and spectral efficiency. At 1 percent outage probability, more than 200 percent increase in coverage area can be achieved, 7 dBW savings in the transmitted power, and the system can operate at 2 b/s/Hz higher spectral efficiency.

Fig 2.2 Illustrating the difference between the direct and cooperative transmission schemes, and the coverage extension prospected by cooperative transmission.

2.4 Intrusion Detection System

Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, Tohoku University Mostafa M. Fouda, Tohoku University and Benha University proposed a method called Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks.

Cognitive radio networks (CRNs) present a promising solution to solve the scarcity of the radio spectrum, they are still susceptible to security threats. Until now, only a few researchers considered the use of intrusion detection systems (IDSs) to combat these threats against CRNs.

In this article CRN based on IEEE wireless regional area network (WRAN) and describe some of the security threats against It are considered. For the secondary users in the CRN to quickly detect whether they are being attacked, a simple yet effective IDS is then presented. Our proposal uses non-parametric cumulative sum (cusum) as the change point detection algorithm to discover the abnormal behavior due to attacks. The proposed IDS adopts an anomaly



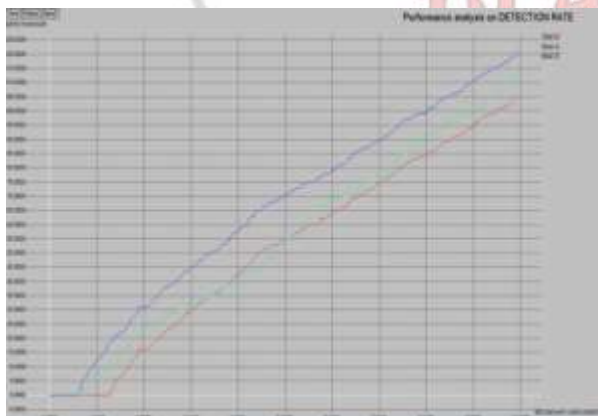
proposed IDS is able to detect suspicious (i.e. anomalous abnormal) behavior arising from an attack.

III. RESULT AND TABULATION

In order to investigate how much selfish su density influences detection accuracy, the experiment was carried out with 4 secondary user. Fig 3.1 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.

Nodes

Fig 3.1 Detection Rate In Nodes





The experimental results in Fig 3.1 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.

IV. CONCLUSION

By using the deterministic channel allocation information, COOPON which 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. A new approach is designed for cognitive radio ad-hoc networks. This make use of ad-hoc network advantages such as autonomous and cooperative characteristics for better detection reliabilities. For future work cryptographic model and game theory to do theoretical analysis of more than one selfish SU in a neighbor, which gives less detection accuracy.

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]. 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.

[6]. 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.