Enhancing Detection Rate by using Distributed Reaction Mechanisms in Cognitive radio ad-hoc networks

Sneha Thankachan
Computer Science and Engineering
Nehru Institute of Technology
Kaliapuram

M. Jebakumari
Computer Science and Engineering Department
Associate Professor
Nehru Institute of Technology, Kaliapuram

ABSTRACT

Cognitive radio (CR) is a promising technology in ad-hoc networks to solve the problems that result from the limited available spectrum and the inefficiency in the spectrum usage by utilizing the existing wireless spectrum advantageously. When the licensed primary user is not using the spectrum, the available channels are allocated for the unlicensed secondary users. An increasing numbers of security threats are being identified when the idea of cognitive radio becomes reality. One such threat is the possible presence of selfish secondary users who try to occupy all available channels. In this paper, an efficient selfish attack detection technique called Distributed Reaction Mechanism is introduced and implemented which results in enhanced detection rate.

Keywords

Cognitive radio, selfish attacks, detection rate

1. INTRODUCTION

The licensing of the wireless spectrum is currently undertaken on a long-term basis over vast geographical regions. In order to address the problem of spectrum paucity, the Federal Communications Commission (FCC) has recently approved the use of unlicensed devices in licensed bands [1].

This new area of research foresees the development of cognitive radio (CR) networks to further improve spectrum efficiency. Cognitive radio (CR) networks can change their transmitter parameters based on interaction with the environment in which they operate.

The basic idea of CR networks is that the unlicensed devices (also called cognitive radio users or secondary users) need to give up the band once the licensed device (or primary user) is detected [2]. CR nodes compete to sense available channels. [3].Providing security is a major issue that comes into picture in any network. In the case of CR networks, selfish attacks are a type of threat, in which the selfish secondary users (SSU) will occupy all or part of the channels and leave those channels underutilized. To detect this kind of misbehavior, COOPON (called Cooperative neighboring cognitive radio Nodes) technique is used [4]. It will detect the attacks of SSUs by the cooperation of other legitimate neighboring secondary users. However this technique is capable of detecting the presence of one selfish node in the network. If there is more than one selfish node, this method has less detection accuracy.

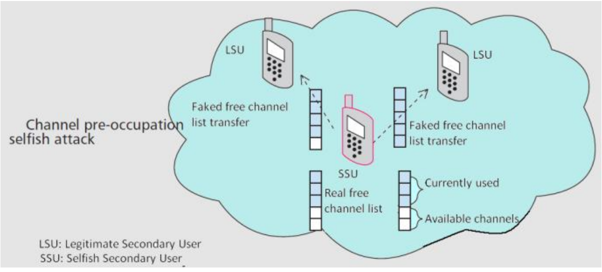

LSU
LSU
Channel pre-occupation selfish attack
Faked free channel list transfer
Faked free channel list transfer
SSU
Real free channel list
Currently used
Available channels
LSU: Legitimate Secondary User
SSU: Selfish Secondary User

Fig 1: Channel pre-occupation attack

The main goal of this work is to enhance the detection rate of SSUs even if there is more number of SSUs. This is achieved by introducing the selfish attack detection technique called Distributed Reaction Mechanism. It Includes two reaction mechanisms: non adaptive reaction scheme and adaptive reaction scheme, based entirely upon local information. The proposed reaction mechanisms strive to guarantee that the throughput of SSUs reduces below what it would have been if the user had not misbehaved.

2. RELATED WORKS

Selfish attack detection technology for a conventional wireless communication network cannot be used for detecting selfish attacks in CR networks because of the dynamic behaviour of CR.

Chen *et al*. first identified a threat to spectrum sensing, called PU emulation attack, in 2008[5]. In this attack, a selfish attacker transmits signals that imitate the characteristics of PU signals. These imitated 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 [6]. 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 [7]. 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 behaviour 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.

3. SYSTEM OVERVIEW AND CONTRIBUTION

3.1 Attack mechanism

Common control channel (CCC): A list of current channel allocation information is broadcast to all neighbouring SUs. 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 (see Figure 1). On the contrary, other legitimate SUs are prohibited from using available channel resources or are limited in using them.

3.2 Detection mechanism

3.2.1 COOPON Technique

Autonomous decision capability of an ad-hoc network based on exchanged channel allocation information among neighbouring SUs. All currently used channels in the target node and neighboring nodes are summed up in two steps: Channel_target_node and Channel_neighboring_node**.** If Channel_target_node > Channel_neighboring_node then the detected target node is a selfish node. This detection mechanism is carried out through the cooperative behavior of neighboring nodes (see Figure 2).

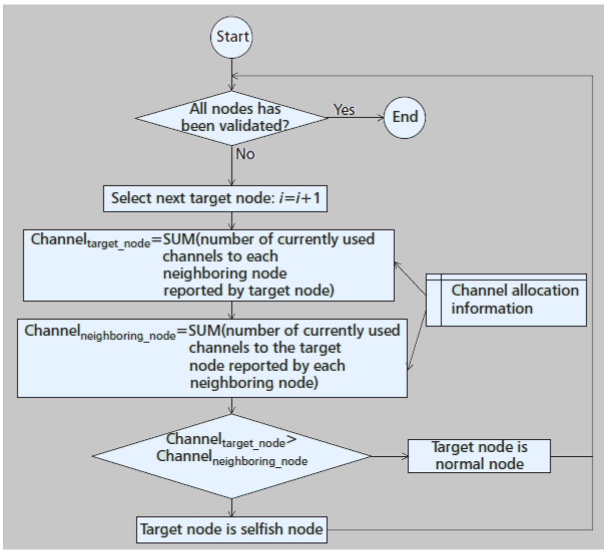

Start
All nodes has been validated?
Yes
End
No
Select next target node: i=i+1
Channel_target_node=SUM(number of currently used channels to each neighboring node reported by target node)
Channel allocation information
Channel_neighboring_node=SUM(number of currently used channels to the target node reported by each neighboring node)
Channel_target_node> Channel_neighboring_node
Target node is normal node
Target node is selfish node

Fig: 2 Algorithm for COOPON technique

3.2.2 Distributed Reaction Mechanism

An efficient selfish attack detection technique called Distributed Reaction Mechanism which results in enhanced detection rate is presented. It Includes two reaction mechanisms: non adaptive reaction scheme and adaptive reaction scheme, based entirely upon local information. The proposed reaction mechanisms strive to guarantee that the SSUs throughput reduces below what it would have been if the user had not misbehaved.

Non-Adaptive Reaction Mechanism: Consider N nodes where all nodes are genuine, i.e. they correctly follow Binary Exponential Backoff (BEB). Every time a node chooses a backoff value uniformly at random from [0….CW-1], it could choose CW-1 with probability, 1/ CW. Let node *A* chooses backoff values in this way every time. The access probability of node *A*, denoted is minimum since the node chooses the largest backoff value in the allowed interval every time. Using Markov Chain analysis, we characterize the steady state probability τ_{min}.

$$\tau_{min} \ / \ \tau = ½ + (1\text{-}2p)/ \ (2W_0 \, [(1\text{-}p)\text{-}p \ (2p)^m \ ])$$

Adaptive Reaction Mechanism: An adaptive and distributed reaction algorithm for the genuine nodes to react against mildly selfish misbehaviors is designed. Each genuine node measures its throughput degradation with respect to its saturation throughput share, T_0. The reaction aggressiveness is made proportional to the level of suspected selfishness, and in most cases, the reaction is not as strong so as to lower the overall network throughput tremendously. Considering the saturation throughput scenario with *N* nodes and using Bianchi’s analysis, the individual fair throughput of each node under saturation conditions equals, T_0 with the assumption that one of the nodes is misbehaving. This would lower the throughput observed (T_0^0) by the genuine nodes. Clearly, $T_0^0 < T_0$. A misbehavior is detected if the observed throughput T_0^0 reduces below DtnThr (detection throughput) * 100% i.e., $T_0^0<$ DtnThr (detection throughput) T_0.

Once a misbehavior has been detected using the above policy (and hence an aggressive misbehavior is assumed), following reaction mechanism is employed to penalize the misbehaving user(s). The entire *N* − 1 genuine nodes, upon detection of misbehavior, choose a constant contention window size = *W’* and do not vary the window size. Each node transmits in a slot with probability,

$$\tau' = 2 \ / \ (W'+1)$$

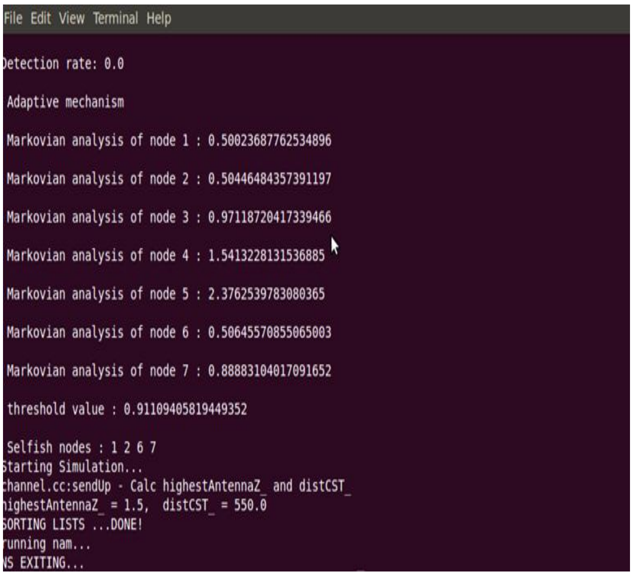
The probability that none of the *N* − 1 genuine nodes transmits in a time slot equals $(1\text{-}\tau')^{N\text{-}1}$. Let *B* denote the channel bandwidth. The maximum throughput available to the misbehaving user is given by B. $(1\text{-}\tau')^{N\text{-}1.}$ Now, *W’* is chosen such that,

$$\text{Max } W' \text{ such that B. } (1\text{-}\tau')^{N\text{-}1} < T_0$$

Thus the genuine nodes choose a constant contention window size small enough to guarantee that the throughput available to misbehaving user is less than T_0.

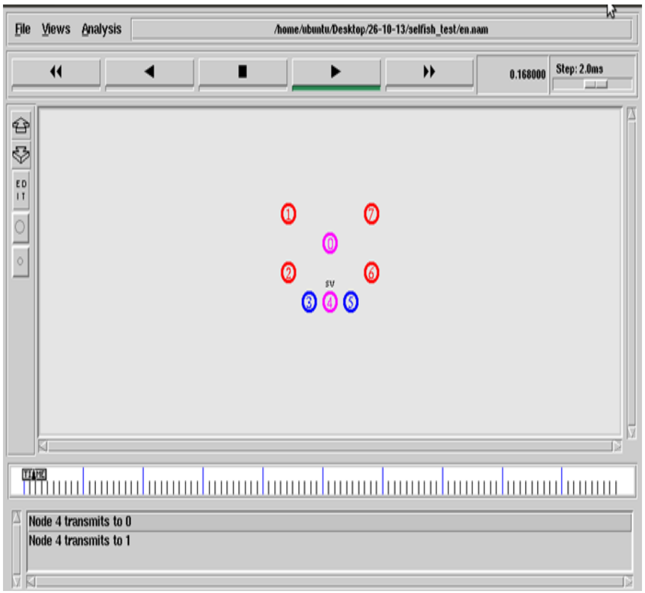
4. RESULTS

The distributed reaction mechanism is implemented in NS 2 simulator to detect the presence of selfish nodes in the ad-hoc networks. Detection of more than one selfish node is possible as observed in the screen shot of fig.3 and fig.4. Here the red-colored nodes, numbered 1, 2, 6 and 7 are the selfish nodes. Other nodes (purple and blue) are secondary users and primary users respectively.



```
Detection rate: 0.0

 Adaptive mechanism

 Markovian analysis of node 1 : 0.50023687762534896

 Markovian analysis of node 2 : 0.50446484357391197

 Markovian analysis of node 3 : 0.97118720417339466

 Markovian analysis of node 4 : 1.5413228131536885

 Markovian analysis of node 5 : 2.3762539783080365

 Markovian analysis of node 6 : 0.50645570855065003

 Markovian analysis of node 7 : 0.88883104017091652

 threshold value : 0.91109405819449352

 Selfish nodes : 1 2 6 7
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
running nam...
NS EXITING...
```

Fig 3: Result after Detecting Selfish Users using Distributed Reaction mechanism



```
Node 4 transmits to 0
Node 4 transmits to 1
```

Fig 4: Detecting Selfish users

5. CONCLUSION

In this paper, a new kind of selfish attack called channel pre-occupation attack is identified and an innovative detection approach called Distributive Reaction Mechanism is proposed and implemented. It overcomes the disadvantages of existing techniques like reduced detection rate in the presence of more than one selfish nodes and degradation in performance. This approach includes two reaction mechanisms called non-adaptive reaction mechanism and adaptive reaction mechanism. These are based entirely upon a node's observed throughput, and hence are easily implementable in practice.

6. REFERENCES

[1] Ian F. Akyildiz, Won- Yeol Lee, Kaushik R.ChowdhuryBroadband Wireless Networking Laboratory, School of Electrical and Computer Engineering, "Cognitive radio ad hoc networks".

[2] 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.

[3] 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.

[4] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In, Korea University, "Selfish attacks and Detection in Cognitive Radio Ad-hoc Networks".

[5] 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.

[6] M. Yan et al., "Game-Theoretic Approach against Selfish Attacks in Cognitive Radio Networks," IEEE/ACIS 10thInt'l.Conf.Computerand Information Science (ICIS), May 2011, pp. 58-61.

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

[8] 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.

[9] S. Li et al., "Location Privacy Preservation in Collaborative Spectrum Sensing," IEEE INFOCOM'12, 2012, pp. 729-37.

[10] Z. Dai, J. Liu, and K. Long, "Cooperative Relaying with Interference Cancellation for Secondary Spectrum Access," KSII Trans. Internet and Information Systems, vol6, no.10, Oct.2012,pp.2455-72.

[11] H. Hu et al., "Optimal Strategies for Cooperative Spectrum Sensing in Multiple Cross-over Cognitive Radio Networks,"KSIITrans.Internet and Info. Systems, vol. 6, no. 12, Dec. 2012, pp. 3061-80.