International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks using Markov Chain and Game Theory

Suchita S. Potdar[1], Dr. Mallikarjun

M. Math [1]Department of Compute Science & Engineering, KLS, Gogte Institute of Technology, Belgaum. Affiliated to Visvesvaraya Technological University Belgaum, Karnataka- India

Abstract: ***Cognitive radio is an opportunistic communication technology designed to help unlicensed users to 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 work 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 deals with serious security problem like fake signal attack, Channel pre-occupation attack. These security problems they significantly degrade the performance of a cognitive radio network. In this proposal we identify the types of selfish attacks in cognitive radio ad-hoc networks and propose an easy and efficient selfish cognitive radio attack detection technique using Markov chain model and Game Theory. This technique is simple and reliable and can be well fitted for practical work in future work.***

Keywords: Cognitive Radio, Markov Chain, Game Theory

1. Introduction

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] [2] [3]. CR nodes compete to sense available channels [4] [5]. 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.

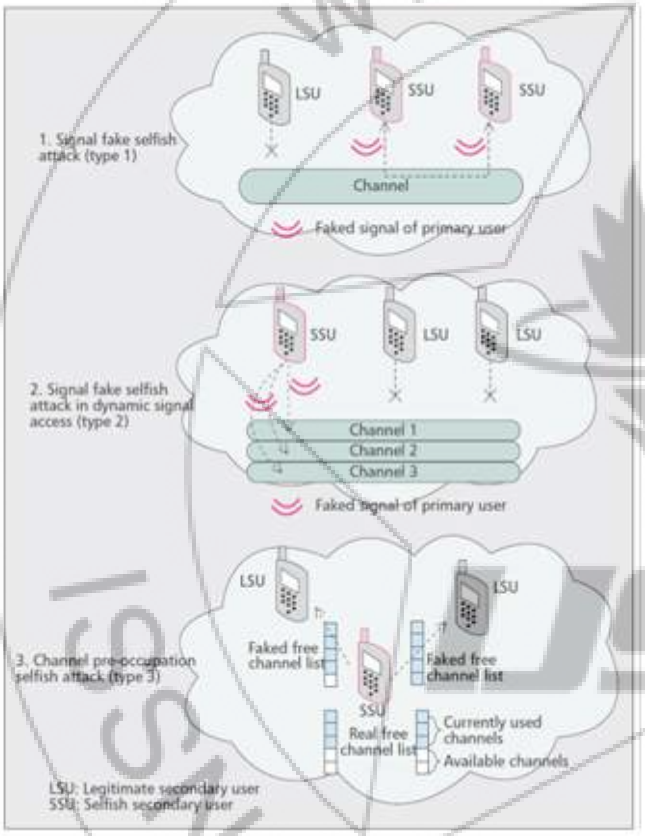
The rest of the paper is organized as follows. Section II covers various issues in spectrum sensing and detection. Section III briefly presents problem formulation. Section IV explains working process of the system. Section V presents detection mechanism. Section VI presents analysis results. Finally, Section VII draws the conclusion.

2. 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 [6]. 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 [7]. Selfish Attacks are made by a selfish SU that increases the access probability by reducing the back off 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 [8]. 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. The proposed detection technique identifies selfish attack and proposed detection technique is different from the previous ones in the communication environments and conditions. The proposed technique is designed for CR ad-hoc networks with multiple channels and is designed for the case that channel allocation information is broadcast for transmission.



3. Types of Selfish Attacks

3.1 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 [9]. 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.

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 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 the two available channels.

Figure 1: 3 different attack types.

4. Problem Formulation

Cognitive Radio (CR) is an opportunistic communication technology designed to help unlicensed users utilize the maximum available licensed bandwidth. 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. The proposed solution is to apply Markov chain and game theory to detect Channel pre-occupation selfish attack (Type 3 attack) in cognitive radio network. The problem is subdivided into following sub-problems

- Better utilization of available spectrum in Cognitive Radio (CR) network.
- Searching for the available spectrum band and assigning the available spectrum for unlicensed secondary users.
- Detecting the selfish node in the CR network.

5. Working Process of the System

The proposed system uses Markov Chain model and Game theory to detect the selfish attacks. Games can be classified into different types from other aspects, for example, cooperative and non-cooperative game, simultaneous and sequential game, perfect information and imperfect information game, and so on. Each type has its own

characteristics, and matches with some problems encountered in communication systems. Game theory has been widely applied to modeling and analysis in communication systems, including the spectrum allocation issues in cognitive radio networks. Architecture of proposed system is shown in figure 2.

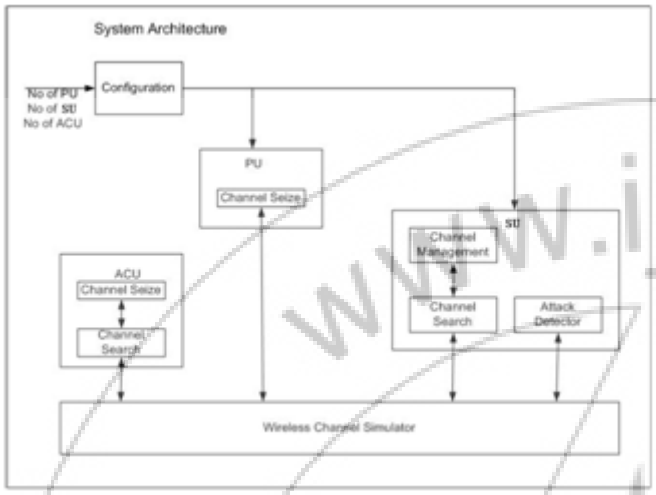


Figure 2: System Architecture

The working of each module is as follows.

Configuration: It takes the three inputs i.e number of nodes, range for displaying the nodes and number of channels to be acquired for the users. Number of nodes intern randomly divided as primary and secondary nodes. Range defines the area of the window over which the nodes to be displayed.

Primary User (PU): It seizes the channel for primary users whenever required and it has exclusive privilege to acquire the channel. After the completion of work it releases the channel and the channels will be available for the secondary users.

Secondary User (SU): This module search for free channels. If any channels are free then those channels will be occupied for the secondary users. This module also manages the channels. Free channels will be occupied by the secondary user in FIFO manner.

Attack detector: It implements the proposed markov chain and game theory to identify selfish secondary user.
Acquire Channels to User (ACU): It search for free channel and seize the channels.

6. Detection Mechanism

The proposed system uses two methods markov chain and game theory for channel occupation and selfish attack detection respectively. The markov chain algorithm is described below.

6.1 Markov Chain algorithm

Input: Network with N number of nodes M max number of channels S sequence of secondary for which the channels are negotiated and SU area in which the detection technique must be applied

Output: Selfish secondary user
1:for i=0; i<S; i++ ; do
2: Find the neighboring nodes of all the nodes for which the probability matrix to be formed using distance formula. Equation shows the distance formula.

$$\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad \text{.....(1)}$$

Where x1, y1 are the x and y position of the particular node.
3: Generate the sequence S which contains occupied nodes and Set the initial probability for each node.
4: end for
5: for k=0; k< S; k++; do
6: for each node in the sequence S
7: select the target node and get the probability of being target node as selfish node
8: Generate probability matrix for each target node
9: end for
10: select the node with maximum probability and declare that node as selfish node.

The algorithm takes the negotiated secondary users and the area over which the algorithm must be applied as the input. It maintains the probability matrix for each node by collecting the data from neighboring nodes. Then finally the node with maximum probability is declared as selfish node.

6.2 Game Theory

Usually a game consists of a set of players, a set of actions, and a set of payoffs. The players seek to maximize their payoffs by taking actions (also known as strategies) depending on the available information at the time of the action decision. The combination of best strategies for each player is known as equilibrium. When each player cannot benefit anymore by changing his/her strategy while keeping the other players' strategies unchanged, then we say that the solution of the game represents a Nash equilibrium. The payoff for each player can be represented as the actual or expected utility a player receives by playing the current strategy. In general, two kinds of games are used:

1)Cooperative games, which imply the joint considerations of the other players. Usually cooperative games explore the formation of coalitions between various players using a characteristic function to describe the maximum expected total income of the coalition. The core represents the solution concept of a cooperative game, and is usually used in order to obtain the stability region. It gives the set of all feasible outcomes that cannot be improved by the coalition individuals when acting independently.
2)Non-cooperative games in which each player selects his/her strategy individually.
3)Game theory deals with any problem in which each player's strategy depends on what the other players do. The reputation concept of game theory is used in project.

6.3 Reputation

Consider a game in which a player i has two types, say A and B. Imagine that if the other players believe that i is of type A, then i's equilibrium payoff will be much higher than his equilibrium payoff when the other players believe that he is of type B. If there's a long future in the game and i is patient, then he will act as if he is of type A even when his type is B,

in order to convince the other players that he is of type A. In other words, he will try to form a reputation for being of type A. This will change the equilibrium behavior dramatically when the other players assign positive probability to each type.

Steps of the strategy are as follows

1. Set some threshold value by using the following formula threshold = (totchannel * 80) / 100……..(2)
2. Set the fixed reputation value for each node.
3. After channel occupation check whether any node value is exceeding threshold value.
4. If any node value is exceeding threshold value then decrease the reputation score.
   score= score-(rand (4) +2)……(3)
5. Else increase the reputation score.
   score =score + rand (4) +2……(4)
6. The node with minimum score is the selfish node.

7. Analysis Results

In order to investigate how the Secondary user's density influences detection accuracy and time the experiment is carried out with different number of nodes and different number of secondary users. The results are shown in following graphs. Analysis of the work is done by considering two parameters. The parameters are accuracy and the time. The following graph shows the comparison between markov chain and game theory.

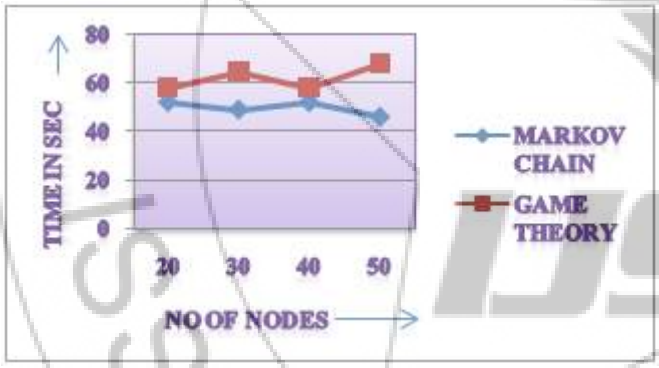


Figure 3: Time in Sec Vs No of nodes

If we consider the time as parameter, then the graph shows that markov chain is the better model than the game theory as it takes 47 seconds to detect the selfish node. Markov model takes less time to detect the selfish user. The graph is shown in the figure 3 and 4. The analysis is carried out based on number of nodes and number of Secondary users.

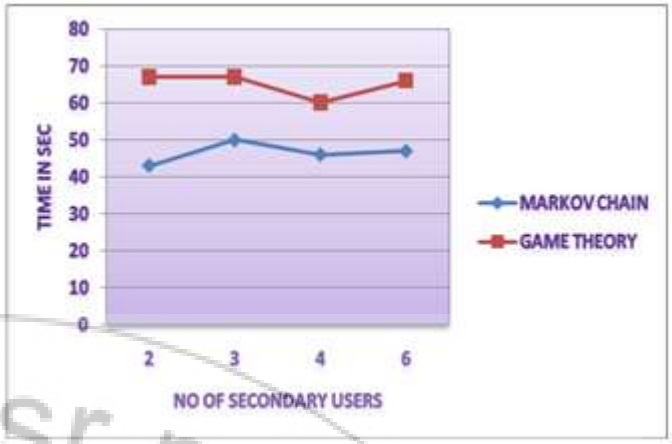


Figure 4: Time in sec Vs No of Secondary users

If we consider the accuracy as parameter, then the graph shows that Game theory is the better model than the markov chain. Game theory gives the more accurate results than Markov chain model. The graph is shown in the figure 5 and 6. The analysis is carried out based on number of nodes and number of Secondary users.

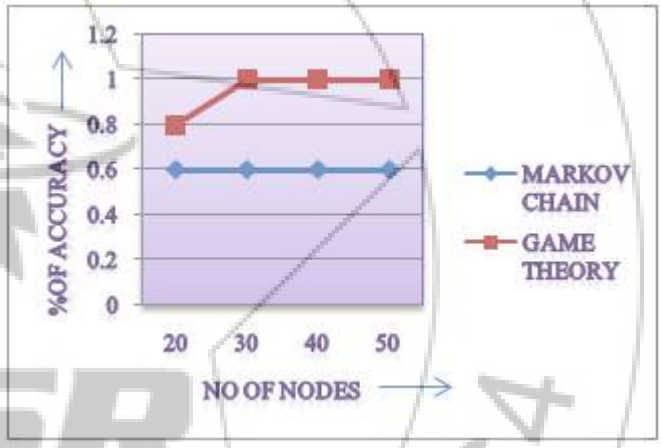


Figure 5: Percentage of accuracy Vs No of nodes

If accuracy is the comparison parameter then game theory is the better solution. If we compare the both the models then game theory is more accurate as it results in the accuracy rate of 90%.

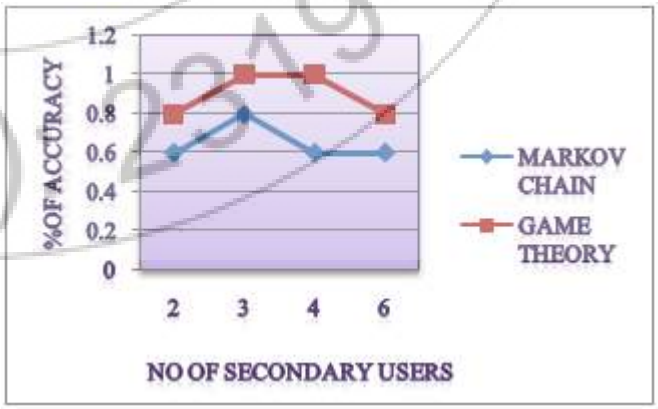


Figure 6: Percentage of accuracy Vs No of Secondary nodes

8. Conclusion

As part of the proposed work "Markov Model and Game Theory "identifies channel pre-occupation Selfish attack in Cognitive Radio ad-hoc network. The work could be designed for cognitive radio ad-hoc networks that use the advantages of ad-hoc network such as autonomous and cooperative characteristics for better detection reliabilities. The Selfish secondary user in a neighboring node can be easily detected using Markov Chain model and Game theory.

In order to investigate how the Secondary user's density influences detection accuracy, the experiment was carried using time and accuracy as the parameters. The result shows that number of secondary users has a trivial effect on accuracy rate. The comparison is carried out between markov chain and game theory. The performance of Game theory is best if the accuracy is the comparison parameter as it results in the accuracy rate of 90%. If the time is the comparison parameter then markov chain is the best solution as it takes 22% of time less than game theory.

9. Future Scope

The future scope of the proposed system can be extended to detect the multiple selfish secondary users in cognitive radio ad-hoc network for channel pre-occupation attack.

References

[1] X. Tan and H. Zhang, "A CORDIC-Jacobi Based Spectrum Sensing Algorithm for Cognitive Radio," in KSIITrans. Internet and Info. Systems, Sept 2012, pp. vol. 6, no. 9,no 9.
[2] J. Liu, and K. Long Z. Dai, "Cooperative Relaying with Interference Cancellation for Secondary Spectrum Access," in KSII Trans. Internet and Information Systems, Oct 2012, pp. vol. 6, no. 10,2455–72.
[3] W.-Y. Lee and I. F. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," in IEEE Trans. Wireless Communication, Oct 2008, pp. vol. 7, pp. 3845-3857.
[4] Longzhe Han, Dohoon Kim, and Hoh Peter Minho Jo, "Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks," in IEEE Network, May/June 2013, pp. 46-50.
[5] P, Mitran, and V. Tarokh N. Devroye, "Achievable Rates in Cognitive Radio Channels," in IEEE Trans. Inform. Theory, May 2006, pp. vol. 52, pp. 1813-1827.
[6] J.-M. Park, and J. H. Reed R. Chen, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," in IEEE JSAC, Jan 2008, pp. vol. 26,pp. 25–36.
[7] M. Yan et al, "Game-Theoretic Approach Against Selfish Attacks in Cognitive Radio Networks," in IEEE/ACIS 10th Int'l. Conf. Computer and Information Science (ICIS), May 2011, pp. pp. 58–61.
[8] H. Hu et al, "Optimal Strategies for Cooperative Spectrum Sensing in Multiple Cross-over Cognitive Radio Networks," in KSII Trans. Internet and Info. Systems, Dec 2012, pp. vol. 6, no. 12,3061–80.
[9] S.Manikandan A.Bency1, "Selfish attacks detection in cognitive radio network using CRV technique," in International Journal of Innovative Research in Science , April 2014 , pp. 11918-11923 vol 3.
[10] Christopher Carl Heckman, "Markov Chains and Game Theory," Arizona State University, 2006.
[11] Y. Tevfik and A. H¨useyin, "A survey of spectrum sensing algorithms for cognitive radio applications," in IEEE Communications Surveys & Tutorials, 2009, pp. vol.11, pp. 116-130.
[12] Carlos Cordeiro Chittabrata Ghosh, "Markov Chain Existence and Hidden Markov," in IEEE Conference, 2009, pp. 1-6.
[13] J. G. Kim, and D. Lee C.-H. Chin, "Stability of Slotted Aloha with Selfish Users under Delay Constraint," in KSII Trans. Internet and Info. Systems, March 2011, pp. vol. 5, no. 3,542–59.
[14] Douglas Sicker, Gary Minden, Dipankar Raychaudhuri Peter Steenkiste, "Future Directions in Cognitive Radio Network Research," NSF Workshop June 2009.
[15] Z. Gao et al, "Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks," in IEEE Wireless Communication, 2012, pp. vol. 19, no. 6,106–12.
[16] S. Li et al, "Location Privacy Preservation in Collaborative Spectrum Sensing," in IEEE INFOCOM, 2012, pp. 729–37.
[17] Alexander Wong, Pin-han Ho Xiao Yu Wang, "Dynamic Markov-Chain Monte Carlo Channel Negotiation for Cognitive Radio," in IEEE INFOCOM 2010, canada, 2010.