MULTIPLE NASH REPUTATION CROSS LAYER CLASSIFICATION FRAMEWORK FOR COGNITIVE NETWORKS

Ganesh Davanam1, T. Pavan Kumar2, M. Sunil Kumar3

1Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, AP, India.
2Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, AP, India.
3Professor, Department of Computer Science and Engineering, Sree VidyaniKetan Engineering College, Tirupati, AP, India.
1dgani05@gmail.com, 2pavankumar_ist@kluniversity.in, 3sunilmalchi@vidyanikethan.edu

https://doi.org/10.26782/jmcms.2020.08.00033

Abstract

Cognitive Radio Networks (CRNs) are new type of communication networks which solves the problems of spectrum utilization and channel assignments in an important manner. Cognitive users are two types i.e Primary and Secondary users. Secondary users use the unused spectrum which is not used by the primary user i.e unlicensed users uses the licensed bandwidth with their permission. Hence, Trust and Reputation management of secondary users has gained more attention. Mainly Reputation management models are required for CRNs to clearly identify whether the Secondary user is Malicious or trusted. If the secondary user is malicious he will attack the network at different layers and degrades the performance. In this paper, a method called Multiple Nash Reputation (MNR) method is proposed to secure the CRN at two different layers namely physical and network. First, trust is separately calculated for each CR user at two different layers, physical layer and network layer using trust parameters. After that the classification of malicious and normal user is made by applying the Multiple Nash Game Theory model. The performance of MNR method is evaluated based on Energy consumption and detection accuracy.

Keywords : Trust, Reputation, Cross Layer attack, Cognitive Radio Networks, Multiple Nash Equilibrium.

I. Introduction

The main advantages of mobile applications are mobility and flexibility compared to cabled systems. Decoupling of available spectrum achieves the coexistence of various radio systems which are operating in parallel with traditional cabled systems. Spectrum allocation is basically categorized as licensed and free-

Copyright reserved © J. Mech. Cont. & Math. Sci.
Ganesh Davanam et al
bands [I]. Spectrum allocation is basically of two types: static and Dynamic. In CRN’s Dynamic spectrum allocation is followed. Dynamic allocation permits unlicensed devices to make use of unused, unoccupied spectrum by other devices. Spectrum occupancy is of three types: completely free, partially free or fully occupied, is known as white, grey or black holes in spectrum usage. CRN’s solved the problem of available spectrum allocation between primary and secondary users without causing harmful interference [V]. Basically CRN system is aware of its environment, internal states and takes good decisions regarding spectrum allocation. It will take the decisions by first it will sense the environment, adjusting its radio parameters (i.e. frequency, transmit power etc.) and takes decisions using a cognition process. Different open architectures are available in the last decade on the fields of software defined radio’s and Cognitive radio networks [XI].

The important element in CRN architecture is Cognitive engine and this uses environmental, spectral and channel conditions as input and made changes in its behavior accordingly for predefined objectives. For re-configurability view, a cognitive radio looks naturally as a software-defined radio. In critical industrial applications all the devices will work in close proximity and hence they will interfere with each other. But in traditional radio systems have limited built in mechanisms which reduces the interference between devices which are working in parallel. In CRN’s awareness on the environment, reasoning and learning are the basic components in which it will solves the multi objective problems.

Mean Bid Cross Layer Trust Evaluation model is applied to measure the trustworthiness of secondary user [IV]. A Routing and Spectrum Allocation algorithm (ROSA) was designed in [VIII] with the objective of minimizing the communication overhead and also adjust the available resources in a dynamic manner. A mean field game approach was proposed in [XV] to detect Primary User Emulation attack based on energy detection and location verification. Besides, with the application of mean game model, strategic defense decisions were made in the presence of multiple attackers. To provide strategic interaction in cooperative, non-cooperative and complex environments we can use game theory models.

Game theory is a mathematical tool for decision makers to solve strategic interactions. The players in competitive or cooperative gaming may have complete, partial or no knowledge on others in the gaming environment. In all the games utility tells the players motivation and the utility function maps the type and strategies by all the players to real number [XVIII]. For a well defined equilibrium, the strategy of the every player will maximize the expected utility to get best response of every player. The results of the utility interactions can be used in a cognitive decision process for optimization. Hence, game theory can be applied in cognitive radio networks. Games are basically two types: cooperative and non-cooperative where in cooperative game player has an option of revising his strategy for best response [XVII] but in non cooperative there is no option of revising the strategy because player doesn’t have any option of coordination with others. Motivated by economics of game theory, a game model based on trust and an algorithm using distributed cooperative spectrum sensing oriented to detect malicious secondary users’ was presented in [XVI] to improve transaction success ratio and spectrum access performance [XIX] for CRN.
In this work, we mainly apply Multiple Nash Game Theory model for classification of malicious and normal users. Then evaluate our results by using the parameters energy consumption and detection accuracy.

The rest of the paper is organized as follows; Section II presents a game theory background for CRN’s, followed by Methodology followed in Section III. Multiple nash reputation cross layer framework and its algorithm are presented in Section IV. Section V shows the simulation results and section VI concludes the work.

II. Game Theory in Cognitive Networks

Wired networks have limited mechanisms for reduction of interference and coexistence, some of the industrial environment used networks is iWLAN, Bluetooth and Nano NET. When they are operating in close proximity leads to interference and signal loss so that there is a loss of data. Hence in industrial applications there is an increasing demand of new kind of wireless technologies which caused spectrum scarcity. Depending on time and location spectrum scarcity problem may vary hence we need some network which mainly solves spectrum scarcity problem by understanding the environment. Such type of network is Cognitive network which efficiently solves the problem by utilizing unused portions of primary user (PU’s) Cognitive radio network senses the environment, analyzes it and adapts to the RF environment dynamically using Self defined radio (SDR) re-configurability. In game theory moving nodes may have some uncertainty about what other players might do. Radio environment can characterize radio environment map (REM) as an integral part of database. REM can be maintained by network infrastructure and cognitive network nodes which are popularly used in industrial environment such as geographical features, spectral regulations, locations and activities of radios. The previous channel assignments can be helpful to find environmental change and update to the network. Hence game theory is highly applicable for cognitive radio networks.

III. Methodology

To improve the spectrum utilization in wireless communications CRN’s mainly classifies users into two types i.e Primary users ‘PU’s’ and Secondary users ‘SU’s’. Here Secondary users ‘SU’s’ are unlicensed and Primary users ‘PU’s’ are licensed, ‘SU’s’ uses the vacant and unutilized spectrum left by ‘PU’s’ which improves the spectrum utilization. As CRN’s are wireless in nature these are prone to errors and more number of attacks will happen on the networks. To make CRN more secure and more reliable, different methods have been presented in the literature section. In this work, Multiple Nash Reputation (MNR) method is proposed. The MNR method is designed with an objective of decreasing the time and energy consumption in identifying reliable nodes and specifies which Secondary user is authorized and unauthorized so that it automatically reduces the attacks on the CRN’s in a significant manner. Figure 1 shows the flow diagram of the proposed work.

As illustrated in the above figure, for each cognitive radio user or cognitive radio nodes, a third party node measures the trustworthiness of the secondary user while allocating underutilized spectrum or vacant spaces using mean bid function [IV]. Next, multiple nash equilibrium model is applied to the individual trust evaluated.
secondary nodes with which appropriate classification is made. Two types of nodes, third party and secondary user are used throughout this paper. The elaborate description of the proposed method is given below followed by the network model.

III. Network Model

Consider two types of users, namely, Primary User ‘PU’ and Secondary User ‘SU’. The primary users are also called as licensed users, own licensed spectrum, hence they can operate in particular frequency bands allocated to them. On the other hand, the secondary users are also called as unlicensed users, hence they do not own any licensed spectrum but are also called as cognitive radio users and these secondary users continuously sense the licensed spectrum with the permission of Primary users. With these two types of network entities, a network model for the MNR method is designed as given below in Figure 2.
From the above diagram, the spectrum is classified into both occupied space ‘OS’ and Free spaces ‘FS’, where Free space is denoted in white color and occupied space is denoted in yellow color. Next, the spectrum hole where the primary user has not used the spectrum is represented by ‘SH’, includes both the unused licensed frequency of primary users ‘PU’ and the unlicensed frequency of secondary users ‘SU’ respectively.

IV. Multiple Nash Game Theory model

Game theory [VII] involves a mathematical tool that represents the strategic decision making and interactions between multiple users. To arrive at the final decision, the third party gathers the spectrum detection from the secondary user based on the reputation value. In this work, Multiple Nash Game Theory model is used to classify between the malicious users and normal users. It is called as Multiple Nash because of the observation by environment parameters and the sensing outcome made by the secondary user node. The environment parameters analyzed are, the availability of spectrum ‘Spec_a’, quality of spectrum ‘Spec_q’ and level of interference ‘Int’. In this work, let us define a spectrum sensing game as represented below.

\[ G_{thres} = (n, S_i, POFi) \cup Spec_a, Spec_q, Int \] (1)

From the above equation (1), a relationship between the third party ‘i’ and the secondary user ‘SU_i’ in the spectrum detection phase is defined based on the environment parameters. With the players participating in our game being the third party and secondary user, ‘S_i’ is assumed as the strategies adopted by two players. The strategies for the secondary user ‘SU_i’ are ‘forward true sensing results’ and forward false sensing results’. The strategies for the third party ‘i’ are ‘examines’ and ‘does not examine’. Finally ‘POFi’ represents the payoff function utilized to determine the gain of the ‘SU’ and the ‘TP’ during the spectrum sensing phase. The payoff matrix for the ‘SU’ and the ‘TP’ is given by the table 1.

|                  | SU forward true sensing results | SU forward false sensing results |
|------------------|--------------------------------|---------------------------------|
| Third party examines | \(-CF(O_i,SO_i,R_i),CF(O_i,SO_i,R_i)\) | \(CF(O_i,SO_i,R_i),CF(O_i,SO_i,R_i)\) |
| Third party do not examine | \(GF(TP,R_i),GF(TP,R_i)\) | \(-GF(TP,R_i),GF(TP,R_i)\) |

When the third party chooses to examine the spectrum, the secondary user with a correct detection obtains a gain equal to ‘\(CF(O_i,SO_i,R_i)\)’. From the above table ‘\(CF(O_i,SO_i,R_i)\)’ refers to the checking function with the corresponding
outcomes of the third party represented as \( O_i \)’, sensing outcomes ‘\( SO_i \)’ and recommendations ‘\( R_i \)’ respectively. The malicious secondary user node is punished by reducing the reputation ‘\( R_i \)’. On the other hand, when the third party does not examine the spectrum, it gathers the sensing results and hence, the secondary node is not punished and hence it obtains a gain equal to ‘\( GF(TP, R_i) \)’. Next, for the normal node, the value of reputation for each secondary user is reduced for each dissimilarity and increased for each detection according to the formula given below.

\[
R_i = R_i + 1, \text{if } SO_i \in 1 \\
R_i = R_i - 1, \text{if } SO_i \in 0
\]  
(2)  
(3)

From the above equations (2) and (3) the recommendation values for each secondary node is incremented if the sensing outcome possesses a profit value (as in equation 2) and is decremented if the sensing outcome possesses a loss value (as in equation 3). Hence, based on the reputation value ‘\( R_i \)’, the nature of secondary user ‘\( SU_i \)’ is determined as given below.

\[
SU_i = \begin{cases} 
\text{if } R_i < R_{\text{thres}}, SU_i \text{ is mischievous} \\
\text{if } R_i > R_{\text{thres}}, SU_i \text{ is normal}
\end{cases}
\]  
(4)

Based on the above mathematical formulation, the pseudo code representation of Multiple Nash Equilibrium Spectrum Sensing is given below.

| **Input:** Cognitive Radio User = Primary User ‘\( PU \)’, Secondary User ‘\( SU \)’, third party node ‘\( i \)’ | **Output:** optimal classified results |
|---|---|
| Step 1: Initialize recommendation | |
| Step 2: Begin | |
| Step 3: For each cognitive radio user | |
| Step 4: Define spectrum sensing game using (1) | |
| Step 5: If \( SO_i \in 1 \) then increment ‘\( R_i \)’ as in (2) end if | |
| Step 6: If \( R_i < R_{\text{thres}} \) then ‘\( SU_i \)’ is mischievous end if | |
| Step 7: If \( SO_i \in 0 \) then decrement ‘\( R_i \)’ as in (3) end if | |
| Step 8: If \( R_i > R_{\text{thres}} \) then ‘\( SU_i \)’ is normal end if | |
| Step 9: Return (optimal classified results) | |
| Step 10: End for | |
| Step 11: End | |

**Algorithm 1:** Multiple Nash Equilibrium Spectrum Sensing
As given in the above Multiple Nash Equilibrium Spectrum Sensing algorithm, for each secondary user, with the aid of the third party, a spectrum sensing game theory is used to classify between the malicious and normal user.

V. Simulations

In this section, we compare the performance of Multiple Nash Reputation (MNR) method with Routing and Spectrum Allocation (ROSA) algorithm [VIII] and Mean Field Game approach [XV] through simulation experiments with different network scenes. The performance of MNR method is evaluated by means of dynamic simulations with the aid of Network Simulator NS-2. First, the simulation setup is described and followed by which the performance metrics are defined and finally, the simulation results are shown.

V.a. Simulation Setup

In our experiments, networks with a specified number of cognitive radio nodes that are distributed in a random manner within an area of 200×200. The number of cognitive radio nodes is varied as 50, 100, 150, 200, 250, 500. Initially the cognitive radio nodes are placed randomly in the specified area. The following table summarizes the simulation parameters used.

Table 2: Description of simulation elements

| No. | Parameters                          | Description         |
|-----|------------------------------------|---------------------|
| 1   | Cognitive radio nodes              | 500                 |
| 2   | Transmission range                 | 40m                 |
| 3   | Number of cycle simulation         | 10                  |
| 4   | Square region                      | 200m * 200m         |
| 5   | Available spectrum                 | 6                   |
| 6   | Traffic type                       | Constant bit rate flow |
| 7   | Simulation time                    | 1000sec             |
| 8   | Size of data packet                | 128bytes            |
| 9   | Data packet generation             | 1 packet/sec        |
| 10  | Node displacement                  | Random distribution |
| 11  | Initial energy                     | 100J                |
V.b. Performance Metrics

In this section, two different performance metrics used for analysis is presented. They are

- Energy consumption
- Detection accuracy

**Energy Consumption**: The cognitive radio node participating in the network, the energy form one of the most significant factors. Certain amount of energy is consumed for sensing task. The average energy is measured as given below.

$$ E = \frac{1}{Ns} \sum_{n=1}^{Ns} e[n] $$

(5)

From the above equation (5), the energy ‘$E$’ is measured based on the generated sampled energy vectors ‘$e[n]$’, where ($n = 1, 2, 3, ..., N_s$)’.

**Attack Detection Time**: Attack detection time refers to the time consumed in detecting the attack. While allocating the underutilized spectrum to the secondary user, some secondary user is malicious whereas some secondary user are said to be normal user. However, detection between malicious and normal user in the early stage reduces the performance degradation of the entire network. The detection time is measured as given below.

$$ D_{time} = \sum_{l=1}^{n} CRN_i \times Time[SU_l] $$

(6)

From the above equation (6), the detection time ‘$D_{time}$’ is measured based on the number of CRN nodes ‘$CRN_i$’ and the time taken for detecting attacks ‘$Time[SU_l]$’. It is represented in terms of milliseconds (ms).

**Attack detection accuracy**: Finally, the attack detection accuracy measures the amount of correct detection (i.e. normal secondary user as normal and malicious secondary user as malicious) made by the third party. The detection accuracy is measured as given below.

$$ D_{acc} = \sum_{i=1}^{n} \frac{SU_i[m/n]}{CRN_i} $$

(7)

From the above equation (7), the detection accuracy ‘$D_{acc}$’ is measured based on the number of CRN nodes considered for experimentation ‘$CRN_i$’ and the secondary user correctly detected as malicious or normal ‘$SU_i[m/n]$’.

**Simulation Results**

In this section, the simulation results for two different parameters are presented. Simulations are conducted using the simulation elements are provided in table 2. Comparative analysis is made with the aid of table and graph for three different methods, MBT-MNR, ROSA [VIII] and mean field game [XV] respectively.

**Scenario 1: Energy Consumption**

First, to start with the energy consumed during the process of sensing that forms the vital parameters for CRN attack defense is presented. As sensing is one of
the most preliminary and fundamental part of any type of network the first metric analyzed is energy consumption. Table 3 given below provides the energy consumption made using three different methods.

Table 3: Simulation results for energy consumption

| Number of CRN nodes | Energy consumption (kJ) |
|---------------------|-------------------------|
|                     | MBT MNR | ROSA | Mean field game |
| 50                  | 2.5     | 3.5  | 4.5            |
| 100                 | 4.5     | 6.5  | 9.5            |
| 150                 | 7       | 9    | 12             |
| 200                 | 7.5     | 11.5 | 14.5           |
| 250                 | 8       | 13.5 | 18             |
| 300                 | 8.5     | 15   | 21.5           |
| 350                 | 9       | 18.5 | 25.5           |
| 400                 | 12.5    | 21.5 | 30.5           |
| 450                 | 14      | 25.5 | 33.5           |
| 500                 | 16      | 30   | 35             |

Figure 3 given above shows the graphical representation of energy consumption using three different methods, MBT-MNR, ROSA [VIII] and mean field game [XV]. During allocation of underutilized spectrum to the unlicensed secondary user, the secondary user consumes a considerable amount of energy during spectrum sensing. The x axis in the figure represents the number of CRN nodes, including both primary

Copyright reserved © J. Mech. Cont.& Math. Sci.
Ganesh Davanam et al

363
user and secondary user. From the figure it is inferred that increasing the number of CRN nodes consecutively results in the increase of energy consumption. As because of the presence of both the primary and secondary users in the CRN, the energy consumed does not proportionately increases. When comparing with two different methods [VIII] and [XV], the energy consumption during spectrum sensing was found to be reduced using MBT-MNR. Mean Bid Cognitive Radio Node Trustworthiness algorithm has been applied in MBT-MNR where the trusted third party based on Mean Bid theory evaluates the trustworthiness of the secondary nodes. Hence, normal secondary nodes are left with larger number of underutilized spectrum and hence used by them in an optimal energy consumed manner. Therefore, the energy consumption using MBT-MNR is said to be reduced by 39% compared to [VIII] and 54% compared to [XV].

Scenario 2: Detection Accuracy

Finally, the comparative analysis of attack detection accuracy is presented in this section. Table 4 given below provides the detection accuracy made using three different methods.

| Number of CRN nodes | Detection accuracy (%) |
|---------------------|------------------------|
|                     | MBT-MNR | ROSA | Mean field game |
| 50                  | 92      | 88   | 84              |
| 100                 | 90.15   | 87.75| 82.15           |
| 150                 | 90.08   | 87   | 80              |
| 200                 | 90.05   | 86.85| 79.55           |
| 250                 | 90      | 86   | 79.25           |
| 300                 | 88.25   | 85.55| 79              |
| 350                 | 88.15   | 84.15| 78.15           |
| 400                 | 88.05   | 84.08| 78.03           |
| 450                 | 87.55   | 84.05| 77.16           |
| 500                 | 87      | 82   | 77.05           |

Table 4: Simulation results for detection accuracy
Figure 4 given above shows the attack detection accuracy measured for 500 CRN nodes considered for simulation at different time intervals. The detection accuracy from the figure is not linear in observation. This is due to the reason that all the secondary nodes that request for underutilized spectrum from the third party node are not malicious nodes and only certain nodes are said to be malicious. So, the trustworthiness of the secondary user or secondary node is first identified from two different aspects of cross layers, i.e., physical layer and the network layer. Accordingly, trust is measured. Followed by evaluating the trust, differentiation between malicious and normal secondary user is made by means of an artificial intelligence technique, i.e., Multiple Nash Game Theory. Here, two different aspects are considered during the classification. First, three different environment parameters are analyzed and followed by which the Nash equilibrium is applied to determine the payoff. In this manner, the attack detection accuracy using the MBT-MNR is said to be improved by 4% when compared to [VIII] and 12% when compared to [XV].

VI. Conclusion

Designing an effective protection mechanism for reducing cross layer attacks in CRN’s is very important issue that is discussed in this work. We propose a Mean Bid Trust and Multiple Nash Reputation (MBT-MNR) method to classify the type of users in the CRN. Multiple Nash Reputation game theory method works well in both physical and network layers Firstly, we model the interactions between the third party and the secondary user with a simultaneous non cooperative model with the objective of using the underutilized spectrums. Then we create a methodology combining two metrics namely Energy and accuracy to measure the trustworthiness of the node. Unlike several trust approaches, our trust-based mechanism takes into consideration the mean bid of neighbor nodes through which trustworthy node is evaluated. Finally, an artificial intelligence technique called, Multiple Nash Equilibrium function is defined to classify between the malicious and normal users making the cognitive radio network more secure and more reliable. Simulations were conducted and from the results it is observed that MBT-MNR method performs better than that of ROSA and mean field game in terms of energy consumption and detection accuracy.
References

I. Brochure, “Coexistence of wireless systems in automation technology,” in Proc. ZVEI - Central Association for Electrical and Electronic Industry, Germany, April 2018.

II. Deanna Hlavacek, J. Morris Chang, “A layered approach to cognitive radio network security: A survey”, Computer Networks, Elsevier, Oct 2014

III. Ernesto Cadena Muñoz, Enrique Rodriguez-Colina, Luis Fernando Pedraza, Ingrid Patricia Paez, “Detection of dynamic location primary user emulation on mobile cognitive radio networks using USRP”, EURASIP Journal on Wireless Communications and Networking, Springer Open, Feb 2020

IV. Ganesh Davanam, T. Pavan Kumar, M. Sunil Kumar, ”Mean Bid Trust Cross Layer Trust Evaluation Model for Cognitive Radio Networks”, International Journal of Advanced Science and Technology, Vol. 29, No. 5, (2020), pp. 11450-11461

V. G. Staple and K. Werbach, “The end of spectrum scarcity [spectrum allocation and utilization],” IEEE Spectrum, vol. 41, no. 3, March 2010.

VI. Jaydip Sen, “A Survey on Security and Privacy Protocols for Cognitive Wireless Sensor Networks”, Journal of Network and Information Security, Jun 2013

VII. Jihen Bennaceur Hanen Idoudi Leila Azouz Saidane, “Trust management in cognitive radio networks: A survey”, International Journal of Network Management, Wiley, Aug 2017

VIII. Jithin Jagannath, Sean Furman, Tommaso Melodia, Andrew Drozd, “Design and Experimental Evaluation of a Cross-Layer Deadline-Based Joint Routing and Spectrum Allocation Algorithm”, IEEE Transactions on Mobile Computing, Vol. 18, No. 8, Aug 2019

IX. Linyuan Zhang, Guoru Ding, Qihui Wu, Yulong Zou, Zhu Han, Jinlong Wang, “Byzantine Attack and Defense in Cognitive Radio Networks: A Survey”, Elsevier, Jun 2015

X. Mee Hong Ling, Kok-Lim Alvin Yau, Geong Sen Poh, “Trust and reputation management in cognitive radio networks: a survey”, Security and Communication Networks, Wiley, Nov 2013

XI. Mitola, “Cognitive Radio Architecture Evolution,” in Proc. of the IEEE, vol. 97, no. 4, April 2009.

XII. Mounia Bouabdellah, Naima Kaabouch, Faiissal El Bouanani, Hussain Ben-Azza, “Network layer attacks and countermeasures in cognitive radio networks: A survey”, Journal of Information Security and Applications, Elsevier, Jul 2018
XIII. Nadine Abbas, Youssef Nasser, Karim El Ahmad, “Recent advances on artificial intelligence and learning techniques in cognitive radio networks”, EURASIP Journal on Wireless Communications and Networking, Springer, Jul 2015

XIV. Quanyan Zhu, Stefan Rass, “Game Theory Meets Network Security”, ACM, Oct 2019

XV. Saim Bin Abdul Khaliq, Muhammad Faisal Amjad, Haider Abbas, Narmeen Shafqat, Hammad Afzal, “Defence against PUE attacks in ad hoc cognitive radio networks: a mean field game approach”, Telecommunication Systems, Springer, May 2018 (3)

XVI. Wang Zhendong, Wang Huiqiang, Zhu Qiang, “A Trust Game Model and Algorithm for Cooperative Spectrum Sensing in Cognitive Radio Networks”, International Journal of Future Generation Communication and Networking Vol. 8, No. 3 (2015).(7)

XVII. W. Saad, et al., “Coalitional game theory for communication networks,” in IEEE Signal Processing Magazine, vol. 26, no. 5, Sept 2017.(8)

XVIII. Y. Zhao, S. Mao, J. O. Neel, and J. H. Reed, “Performance evaluation of cognitive radios: metrics, utility functions, and methodology,” in Proc. Of the IEEE, vol. 97, no. 4, April 2009.(6)

XIX. Z. Han et al., Game Theory in Wireless and Communication Networks: Theory, Models, and Applications, Cambridge Press, Cambridge, 2012.(9)

XX. Z. Jin, S. Anand, K. P. Subbalakshmi, “Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks”, IEEE Transactions on Communication, Vol. 60, Issue 9, Sep 2012

Copyright reserved © J. Mech. Cont.& Math. Sci.
Ganesh Davanam et al