© 2017 IJSRST | Volume 3 | Issue 3 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Performance Evolution of CR-AD HOC Network by Updated Joint Cooperative Spectrum Sensing Technique

Komal Shinde, Prof.Jyoti S.Hatte Patil
E &TC **D**epartment, M. S. Bidave Engineering College, Latur, Maharashtra, India

ABSTRACT

Cognitive radio (CR) is an intelligent radio, which has been targeted to exploit the utmost available spectrum holes for unlicensed users by sensing the environment. 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. The proposed work provides selfish cognitive radio attack detection technique, called UJCSST, which will detect the attacks of selfish Secondary Users by the cooperation of other legitimate neighboring SUs. The UJCSST algorithm makes use of the autonomous decision capability of an ad-hoc communication network based on exchanged channel allocation information among neighboring SUs. This technique is simple and reliable and can be well fitted for practical work in future work. .

Keywords: Cognitive radio, UJCSST, Primary Users(PU),Selfish secondary user(SSU),Secondary Users (SUs)

I. INTRODUCTION

A. CRN (Cognitive Radio Network)

The major growth in wireless environment leads to the extreme usage of the spectrum. The static spectrum allocation for licensed users make the utilization of spectrum resources inefficient and the unlicensed bands i.e., ISM bands, are congested due to competing of many wireless applications. To enhance the efficiency of the spectrum, Mitola formulated "Cognitive Radio" in which the unlicensed user can use the spectrum holes of the licensed bands when they are idle without causing interference with primary user or licensed users. Federal Communication Commission (FCC) approved this CRN to defeat the spectrum shortage problems in both licensed and unlicensed bands. CR (Cognitive Radio) is an opportunistic radio that is well known in the wireless communication network.

A CR definition states as, "CR is defined as a radio that can vary its transmitter parameters by means of perception within the environment". In cognitive radio, the two uniqueness are major like "Cognitive capability and reconfigurability". Thus, Cognitive radio is an intelligent radio that modifies its internal capabilities or parameters in response to its environment changes and identifies the white spaces for unlicensed user's result in reliable Communication.

Dynamic Spectrum Access (DSA) method is integrated with cognitive radio in order to discover the spectrum holes and solve the troubles in spectrum inefficiency. Thus, the SU (Secondary User) switches to the new spectrum band when PU (Primary User) signals are detected and avoids interference with PU transmission.
cognitive radio network functions as mentioned below,

- Spectrum sensing: recognize the available resources and share it without causing interferences with others.
- Spectrum management: It grabs the finest available resources to accommodate the customer requirements.
- Spectrum sharing: It provides the spectrum scheduling approach for the existing user in the network.
- Spectrum mobility: It manages the communication necessities for transition.

The Cognitive Radio Network architecture (CRN) is

classified into infrastructure based CR as shown in Fig.1. And Cognitive Radio Ad-Hoc Network (CRAHN) is shown in Fig.2

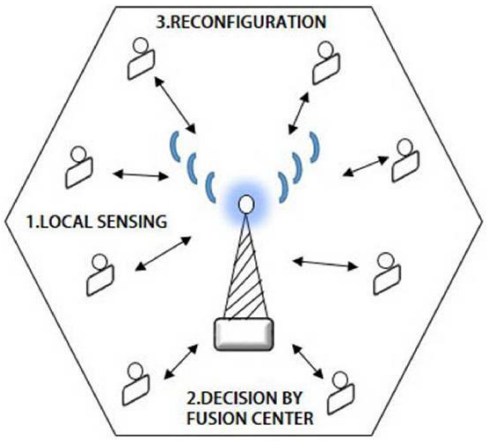

Figure 1. Infrastructure Based Cognitive Radio

The infrastructure based CR has a base station in which the interfering is avoided and also resource allocations are monitored and controlled.

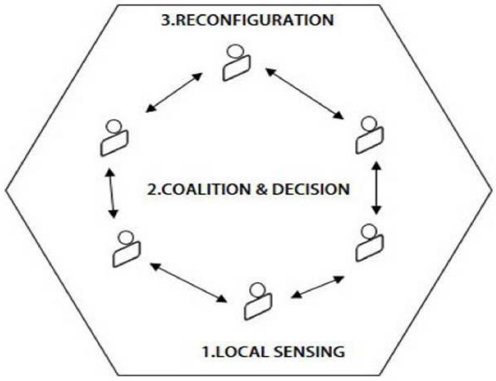

Figure 2. CR-AdHoc Network

The CR-Ad Hoc Network lacks in the infrastructure, and every CR node communicates with multi-hop, reconfigures itself and responses to its local observations. In order to avoid obstruction, the information is distributed to the neighbour nodes via cooperative technique. This process would mitigate the insufficiency of spectrum usage and results in high efficiency and utilization. In CRAHN, the spectrum management researches are done broadly in the area of spectrum sensing, routing protocols, and spectrum allocation. There is a major lack of interest level towards the security side, which can emerge as a potential issue later. Some SUs in the network will respond in a selfish manner, which leads to selfish attacks in the network. It results in the holding of resources by avoiding other LSU (Legitimate Secondary User) from accessing the spectrum resources. SSU (Selfish Secondary User) must be recognized and detected in order to get better the spectrum usage and performance in the network. The selfish attacks may be PU (primary user) emulation attack or a Preoccupation attack. The SSU will transmit PU signals i.e. Fake PU signals to other SU. Thus, LSU overhear to this signal and detects PU which is in action and switches to another channel. The selfish attacks are done either by PU emulation attack or Preoccupation attack.

II. TYPES OF SELFISH ATTACKS

Selfish attacks are different depending upon what and how they attack in order to pre-occupy CR spectrum resources. There are three different types of selfish attacks

A. Signal Fake Selfish Attack (Type 1)
B. Signal Fake Selfish Attack in Dynamic Signal Access (Type 2)
C. Channel Pre-Occupation Selfish Attack (Type 3)

These are the types of attacks depending upon the attack mechanism. These Attacks are responsible for the performance degradation of Cognitive Radio Ad Hoc network. In order to upgrade the performance of the network, the detection and avoidance of selfish attack is very essential. In this paper we proposed an algorithm for improving the trustworthiness amongst nodes in Cognitive Radio Networks.

A. Signal Fake Selfish Attack (Type 1)-

This attack is planned to prohibit a legal SU (LSU) from sensing vacant spectrum bands by transmitting faked PU signals, as shown in fig.3. The selfish SU (SSU) will emulate the characteristics of PU signals. A legal SU who listens the faked signals makes a conclusion that the PU is now active and so the legal SU will give up sensing available channels.

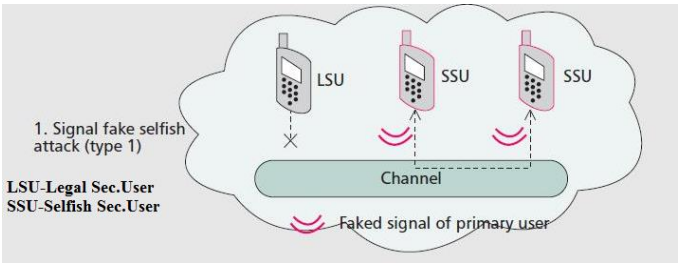

Figure 3. Signal Fake selfish attack(type1)

B. Signal Fake Selfish Attack in Dynamic Signal Access(Type 2)-

Type 2 attack is shown in fig.4.These 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 procedure, the SUs will periodically sense the present 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, 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.

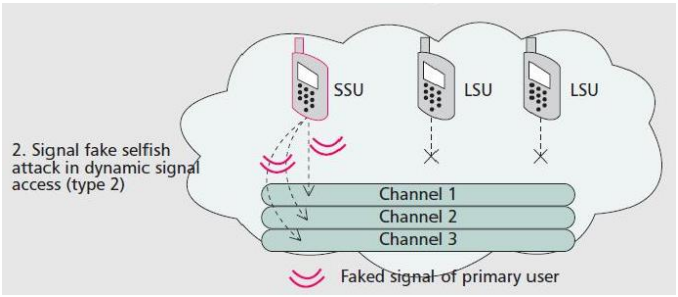

Figure 4. Signal Fake selfish attack in dynamic signal access (type2)

C. Channel Pre-Occupation Selfish Attack

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 neighbouring 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 neighbouring SUs.

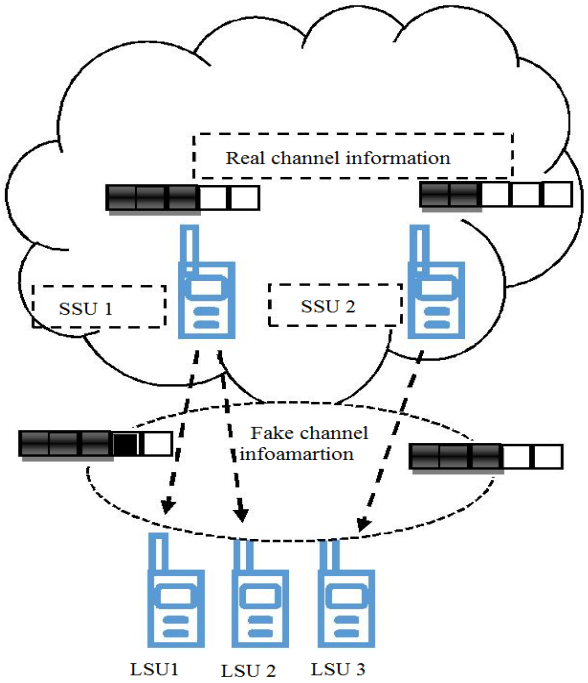

Figure 5. Channel Pre-occupation selfish attack

The pre-occupation problem is depicted in Fig.5. The fake information is exchanged between the neighbouring users and prevents them from accessing the resources. Consider that SSU 1 has 3 channels as allocated and remaining 2 channels which are free, is sensed by the available resources, so that the other LSU will request them. This SSU 1 response with fake channel information by sending 4 channels as is in usage and prohibits other users from accessing it. Likewise, SSU 2 behaves like SSU 1 to other users. If many selfish users send the fake information, pre-occupation problem arises; this will obviously degrade the performance in the network. In order to prevent this, coalitional approach called updated joint cooperative spectrum sensing technique is used.

III. PROPOSED SYSTEM DESIGN

The cognitive radio network aims to make the use of the available spectrum in the communication network. Normally SU uses CCC (common control channel) knowledge and begins to broadcast their channel information to its one hop users. The selfish users can send fake data to their neighbours in order to pre occupy more resources for their own use. Thus, the legal users are prohibited from accessing the channels thereby resulting in inflexibility during resource sharing.

The Updated Joint Cooperative Spectrum Sensing Technique is mentioned in Fig.6, overcomes this problem by seeking the cooperation of all the one hop users in order to identify whether the selected node is selfish or not. UJCSS Technique has advantages like reliability, high performance but lacks in certain conditions. This approach cooperates with each user such as PU and SU who involve in the game or work. Meantime the PU has the uppermost priority in accessing the channel than SU. In such a approach, when that PU demands resources, the SU should return back the resources and jump to other vacant resource. The PU incorporates by dropping their resources and subscribers in a pool. The pool maintains the resource allocation process and the stability of the system is maintained by the core concept.

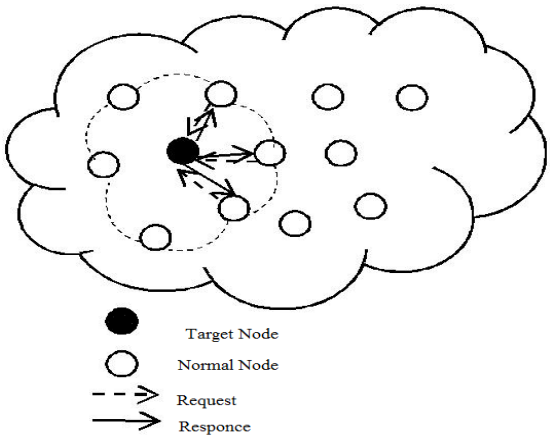

Figure 6. UJCSS Technique

We consider a cognitive radio ad-hoc network. Ad-hoc networks have distributed and autonomous management characteristics. Our proposed detection mechanism 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 neighbouring SUs. All 1-hop neighbouring SUs sum the numbers of presently used cannels sent by themselves and other neighbouring nodes. In addition, simultaneously all of the neighbouring nodes sum the numbers of currently used cannels sent by the target node.

Individual neighbouring nodes will compare the summed numbers sent by all neighbouring nodes to the summed numbers sent by the target node to check if the target SU is a selfish attacker. Thus, all neighbouring nodes will know if the target SU is a selfish attacker or not. This detection mechanism is carried out through the cooperative behaviour of neighbouring nodes. Once a neighbouring SU is chosen as a target node and the detection action for it is completed, another neighbouring SU will be selected as a target node for the next detection action.

Detection Algorithm- The system design depicts about the detailed process flow of the proposed methodology which is mentioned in Fig.7. This makes the system with good performance and flexibility in resource sharing.

A. Node Distribution Phase-

The node distribution phase is further classified into three sub modules,

- Node creation
- Node configuration
- Node deployment

B. Register Phase-

All nodes get registered as they get entered in to the Ad hoc network.

C. Update Routing Table-

Whenever a new node arrives in the radio cell, apply register phase. The routing table at each node is built in incremental steps. Like reactive routing protocol, the source initiates route discovery only on-demand. It uses the route request (RREQ) and route reply (RREP) packet of reactive routing protocol. Routing table in our propose protocol is built during the route discovery phase and is not exchanged along the nodes.

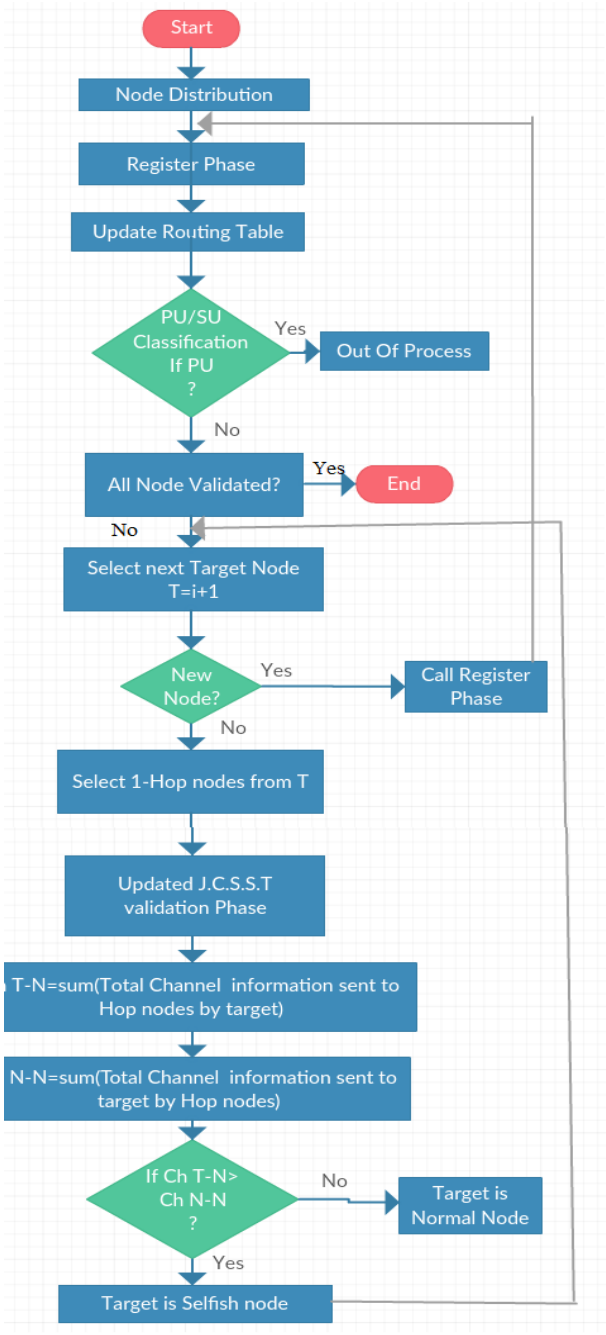

Figure 7. Flow chart of proposed Design

D. PU/SU Classification-

The CRs work to detect the activity of a primary user on a given spectrum band, Each working CR receives the primary signal with signal to noise ratio (SNR). Each of the cooperative CRs is supposed to employ an energy detector and measures the received power on the channel during the sensing period. In energy detection, each CR collects energy samples, where the signal observed *y(t)* by each CR is as in Equation 1.

$$y(t)=\begin{cases} x(t)+n(t) & if\ channel\ is\ busy, H1 \\ n(t) & if\ channel\ is\ free, H0 \end{cases} \quad (1)$$

Where, n(t) is additive white Gaussian noise with variance σ_n^2 .x(t) is the received primary user signal which is assumed to be Circularly Symmetric Complex Gaussian (CSCG) distributed with variance σ_x^2. In most of the PU authentication mechanisms designed, a PU is recognized using Energy detection. In Energy detection, a threshold is fixed and a node whose energy is found to be more than threshold is identified as PU. If PU is detected then it will be sent out of the process, because the selfish nodes are only the secondary nodes on which the further technique is to be applied.

E. *Validation Phase*

After the classification of PU and SU it will check all nodes are validated or not. If all nodes are validated then the process will end, if not then it will select the next target SU node, i.e. T=i+1. If the selected next target node is new then it will call register phase. In Ad Hoc network the nodes get entered in to the network at any time or they leave the network at any instant of time. So, if the selected target node is new means just entered in to the system then it will get registered. After registration it will passed to further process. One Hop neighbouring nodes from the target node will be selected for the verification process.

F. UJCSS Technique

Each CR node is provided with transceiver so that CR node can't transmit and sense at the same time. It needs periodic spectrum sensing. The frame of duration (T) is divided into three slots

a) Sensing slot
b) Reporting slot
c) Transmission slot

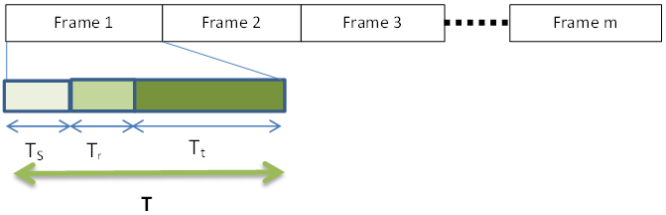

Figure 8. Frame structure for cooperative spectrum sensing in CR.

As a consequence:

$$T = T_S + T_r + T_t \quad (2)$$

If we consider τ as the time required by each CR node to report the sensed result to the Fusion Centre, then the total reporting time for all sensing CR nodes is $T_r = N*\tau$. The duration of the sensing can be expressed as a function of number of CRs:

$$T_S(N) = T - T_t - N * \tau \quad (3)$$

$T_s(N)$ is the time duration of sensing for N number of nodes.

Energy Consumption

The consumed energy in cooperative spectrum sensing by all CR nodes is related to the sum of three components:

Energy consumed in local sensing (Es)-

$$E_s(N) = N * T_s(N) * \rho_s \quad (4)$$

Energy consumed during result reporting (Er)-

$$E_r(N) = N * \tau * \rho_r \quad (5)$$

Energy consumed in Data transmission (E_t)-

$$E_t(N) = T_t(N) * \rho_t \quad (6)$$

$$E_T(N) = (T - T_s(N) - N * \tau) * \rho_t \quad (7)$$

Where ρ_s , ρ_r and ρ_t are the consumed powers per CR for local sensing, reporting, and data transmission, respectively. Total Energy required is equal to the sum of $E_s(N)$, $E_r(N)$ and $E_t(N)$.

In order to identify the selfish node in the network we are using the joint cooperative spectrum sensing technique. In this technique we are using the channel allocation information of target node and one hop neighbouring nodes. The channel allocation information at each node of one hop is shared with one hop neighbouring nodes. And the information sent by neighbouring nodes to target is summed up and compared with the summation of channel allocation information sent by target node to one hop neighbouring nodes. If the summation of channel allocation information by target is greater than the neighbouring nodes then target is detected as selfish.

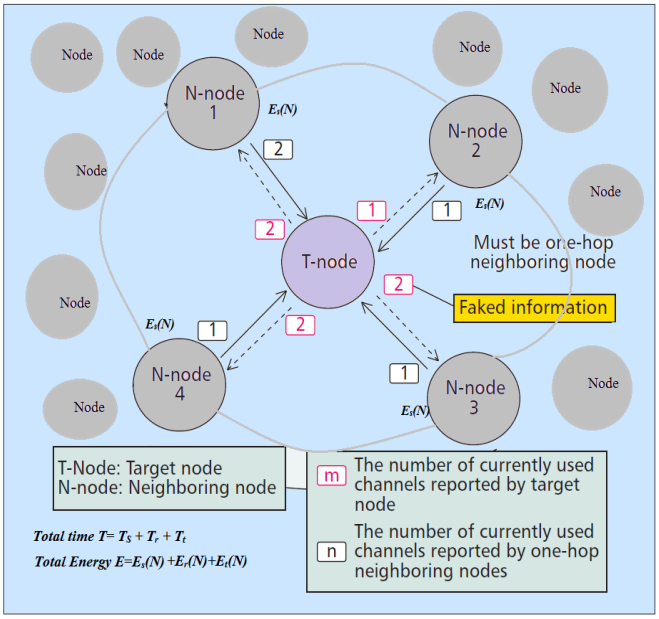

Figure 8. Selfish attack detection mechanism

As we mentioned above, all currently used channels in the target node and neighbouring nodes are summed up in two steps

Channeltarget_node and Channelneighboring_node. Then Channeltarget_node will be compared to Channelneighboring_node.According to the example in Fig.8, Channeltarget_node is 7 (2+1+2+2) and Channelneigboring_node is 5 (2+1+1+1). Because 7 > 5, the target secondary node is identified as a selfish attacker.

As we are using the joint cooperative spectrum sensing technique, the amount of energy required is saved due to the continuous sharing of information between the nodes. When the node is found a selfish node then the node is blocked so that other nodes will get protected from it and the sensing energy will be saved.

Then UJCSST will check the next neighbouring node after it selects one of the unchecked neighbouring secondary nodes as a target node.

IV SIMULATION RESULT AND ANALYSIS

We conducted the simulation using MATLAB to verify the efficiency. The efficiency is measured by a detection rate, which is the proportion of the number of selfish SUs detected to the total number of misbehaving nodes in a CR network: One SU has a maximum of eight data channels and one common control channel(CCC). The channel data rate is 11 Mb/s. In simulation, one SU can have two to five one-hop neighbouring 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 examine how much selfish SU density influences detection accuracy, the experiment was carried out with 50,100, and 150 SUs, respectively, as shown in Fig. 9. From Fig. 10, 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 neighbour 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 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 neighbour .The experimental results in Fig. 10 give an insight into how the number of nodes in a neighbour will influence selfish detection accuracy. Intuitively, if we have more neighbouring nodes in a neighbour, 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 neighbouring nodes to five neighbouring nodes. For the first CR network all of neighbours have only two neighbouring nodes; for the second CR network all of neighbours have only three neighbouring nodes; for the third CR network all of neighbours have only four neighbouring nodes; and for the fourth CR network all of the neighbours have only five neighbouring nodes. The experiment to answer this question was made and the results are shown in Fig. 10. One hundred secondary users were used in this experiment. Five neighbouring SUs in a CR ad-hoc network achieve very high accuracy regardless of selfish SU density. Four neighbouring SUs also provide very high accuracy and are trivially influenced by the density of selfish SUs. However, we notice that two SUs in a neighbour are negatively affected by the density of selfish SUs. Thus, more than three SUs in a neighbour of a CR ad-hoc network are recommended in order to avoid selfish CR attacks.

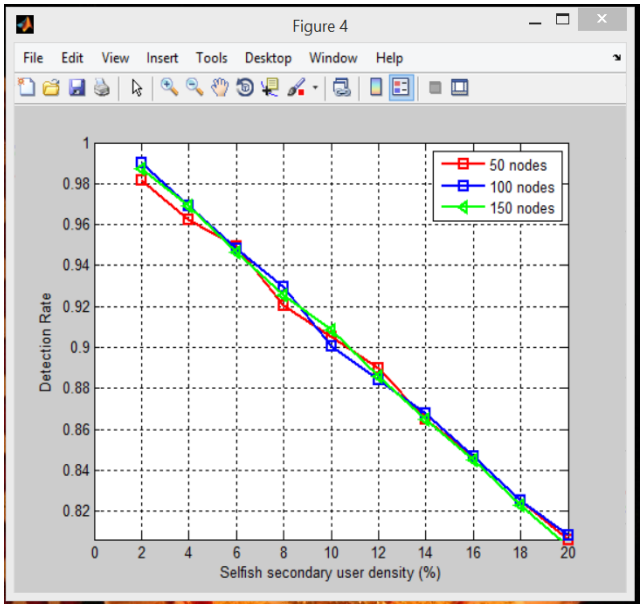

Figure 9. Selfish SU detection rate vs. selfish SU density.

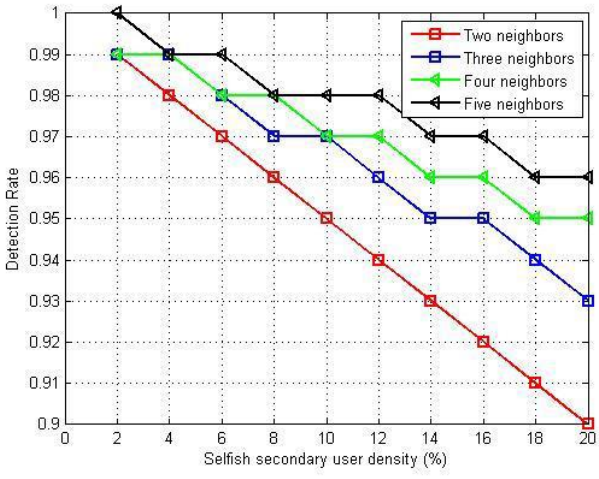

Figure 10. Detection rate vs. number of neighboring nodes

Five neighbouring SUs in a CR ad-hoc network achieve very high accuracy regardless of selfish SU density. Four neighbouring SUs also provide very high accuracy and are trivially influenced by the density of selfish SUs. However, we notice that two SUs in a neighbour are negatively affected by the density of selfish SUs.

Thus, more than three SUs in a neighbour of a CR ad-hoc network are recommended in order to avoid selfish CR attacks.

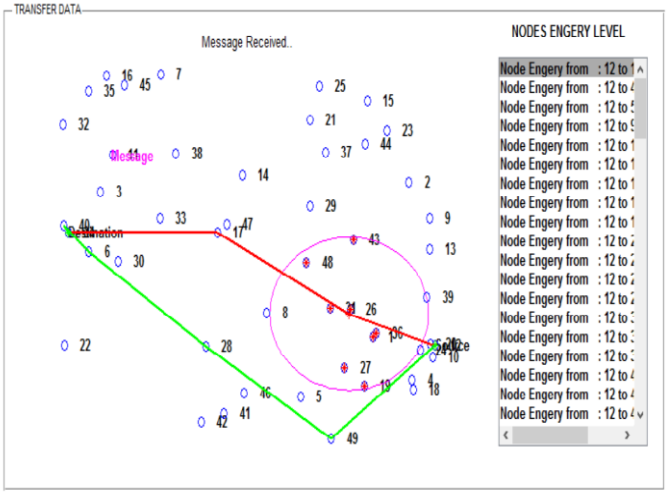

Figure 11. UJCSST Results.

The simulation output considering 100 nodes is shown in fig.11. The energy level from different nodes is considered. For successful transmission and reception of message the path without selfish nodes is selected.

V. CONCLUSION

In the proposed approach, selfish attacks by the multiple channels are avoided by introducing UJCSS Technique. The core idea is the flexible cooperative users which results in keeping the resource pool non-empty and periodically updated. Meanwhile the users are allocated on a timely basis so that the interferences are avoided in the system. This proposed methodology will give a high degree accuracy of detection and moreover will improve the resource allocation in the multiple channels. The perceived limitation in this approach is basically, as the number of users increase in coalition formation, it may lead to overcrowding for accessing the resources and may result in delay in accessing the resources. This may result in the allocation time to be high. The future scope of the proposed methodology is to mainly reduce these perceived limits in the upcoming research papers.

VI. REFERENCES

[1] Suchita S. Potdar1, Dr. Mallikarjun, “Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks using Markov Chain and Game Theory”. International Journal of Science and Research (IJSR), Volume 3 Issue 8, August 2014, ISSN (Online): 2319-7064.

[2] T.Jenefa , Mr. E. Sivanantham “COOPON FOR SELFISH ATTACK DETECTION IN Cr Ad-Hoc Networks”, International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014, ISSN 2250-3153

[3] Pavan H M, Mrs. K Vijaya, “Detection and Prevention of a Channel occupation selfish attack by SU in Cognitive Radio Networks”. International Journal on Recent and Innovation Trends in Computing and Communication Volume: 2 Issue 5, ISSN: 2321-8169.

[4] Dr. Anubhuti Khare1, Manish Saxena2 ,Roshan Singh Thakur3 , Khyati Chourasia*(4), “Attacks & Preventions of Cognitive Radio Network-A Survey” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013, ISSN: 2278 – 1323

[5] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In, “Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks” ARTICLE IEEE NETWORK MAY 2013.

[6] G.V.S.Gohila, A.Velayudham and R.Kanthavel “Selfish Attack avoidance in Cognitive Radio Ad-Hoc Networks using Coalition Game theory” International Conference on Innovations in Information Embedded and Communication Systems (ICIIECS’14), March 13-14, 2014, pp.571-575

[7] 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.

[8] J. Mitola III, Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio, Ph.D. thesis, KTH Royal Institute of Technology, 2000.

[9] 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

[10] 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.

[11]] Z.M.Fadlullah, H.Nishiyama, N.Kato, M.M. Fouda “An Intrusion Detection System (IDS) for Combating Attacks against Cognitive Radio Networks” Network IEEE, Vol.27,Issue.3, 2013, pp.51-56.