Multiselfish Attacks Detection Based on Credit Risk Information in Cognitive Radio Ad-hoc Networks

G.Gowrishankar[1], S.Balgani[2], R.Aruna[3]

PG Scholor[1], Assistant Professor[2], Assistant Professor[3]

Department of Information Technology, Kongunadu College of Engineering and Technology

ABSTRACT: *Cognitive radio network is an opportunistic communication technology supports unlicensed user to make use of the large amount of available number of bandwidth. CRN can identify more available communication of spectrum efficiently. CRN can maintain new wireless users in existing active spectrum. CRN user uses the free spectrum which is not being used by the unlicensed user without causing any interfering to the necessary communication. The main objective of the CRN is used to resolve the spectrum Scarcity by transfer the spectrum to the unlicensed user dynamically. CRN are dangerous to the selfish attacks, because of spectrum allocation in cognitive radio networks capability. SU spread fake information to the other close to SUs sequentially to occupy all vacant channels. Selfish Nodes are highly decreasing the performance of CRN. In this article we have predictable the Multiselfish attacks by using credit risk information. Hence we proposed a method to identify Multiselfish attacks by using credit risk information Algorithm.*

Keywords - *Primary user (PU), Secondary user (SU), Mobile ad-hoc network (MANET), cognitive radio networks (CRN), selfish node, Detection Rate (DR), Credit Risk Information (CRI).*

I. INTRODUCTION

Mobile ad-hoc network (MANET) is a communications less network; hence they make out a number of attacks are possible in MANET. Selfish attacks are also one of them. In cognitive Radio technology, primary users are called as licensed user and the secondary users are called as unlicensed users. The vacant frequency band by the primary user called as spectrum holes or white space. The original task of cognitive radio networks are used to discover the licensed users. While the licensed users are placed close by the range to identify the vacant spectrum. Hence, this process is called spectrum sensing.

Cognitive Radio Network (CRN) is a communication technology to make use of the most unoccupied licensed bandwidth for the unlicensed users. It has been recognized that, the licensed spectrum is not make use of to its full level at all the time. The user faced the as well much spectrum demands and to make use of the unoccupied spectrum. The major point of cognitive radio is to recognize the vacant licensed spectrum for secondary usage without interfering with the primary user. Then the approved primary user (PU) is not using the spectrum bands they consider as offered. Next the not in use number of channels will be hand over to the unlicensed user by the dynamic signal access behaviors [12].Whenever the primary user (PU) is present from the cognitive radio network, the secondary users (SU) without delay release the licensed bands because the Primary User (PU) has limited privilege to use of them [2&3].

A CRN node free-for-all to sense offered channels [4-7]. But some SUs are selfish, and try to occupy all part of the unused channels. Usually selfish CRN attacks are carried out by sending the fake signals or fake channels information. If a SU identifies 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 forged PU signals, a selfish SU prohibits other conflicting SUs from right to use the channels. In this case sending a fake PU signals a selfish SU prohibits other conflicting SUs from accessing the channels. An additional classification of selfish attack is carried out when SUs shares the sensed nearby channels.

Usually each SU from period to period notifies its neighbouring SUs of current available channels by spreading channel allocation information such as the number of unoccupied channels and channels in usage. In this case, a selfish SU transmits fake channel share information to other neighbouring SUs in order to occupy all part of the nearby channels. For example, even though a unlicensed SU uses only two out of five channels. Thus, these selfish attacks shrinkage the performance of a CR network significantly.

Because of the dynamic structures of CR

networks, it is not possible to use the selfish attack detect the techniques used in the old-style wireless communications for the CR networks. In the existing COOPON (Cooperating neighbouring cognitive radio networks nodes) tools, if there is more than individual selfish secondary user this mechanism is not suitable to detect the selfish nodes. COOPON uses the self-ruling deduction skill of an ad-hoc network, based on the swap over channel allocation information. In this article, we focus on the selfish attacks of unlicensed users towards numerous channel right to use in the CR Networks. For single selfish multiple node detection, each SU will frequently transmit the present multiple channel allocation information to all of its neighbouring SUs [12]. In our proposed method, for the multiple selfish node detection Credit Risk information is planned for the each node in the cognitive radio network.

II. RELATED WORK

Suitable to the originality of the performance of CR Network, Selfish attack finding technology for a normal wireless network cannot be used for the noticing selfish attacks in Cognitive Radio Networks (CRN). For CR Networks selfish attacks, first notorious a danger to the spectrum sensing, called PUEA (Primary User Emulation Attacks). In this attack, a selfish attacker transmits signals that monitor the worth of PU signals. The duplicate signals make valid SUs misjudge that the PU is active, and so the fake signals hamper SU right to use to the empty spectrum band. They find the faked PUs signals by the official verification.

The official verification resolve the effective source signal by the signal energy neck and neck combined with the beginning place of the position. In 2011, Yan practical the game-theoretic approach, Nash equilibrium, to avoid the selfish attacks [12]. Selfish attacks are generated by a selfish SU to increase the access possibility by reduces the back off window size in a CSMA-based CR Network. In 2012, a cross-layer altruistic differentiated service protocol (ADSP) was suggested for the keen cognitive radio networks to consider the quality of service provisioning in CR Network with selfish node simultaneity [15]. Their purpose is to give minor disruption, problematic throughput, and better-quality supply ratios for a cognitive radio network. Position is given to every SU constructed on well-known selfish actions data. A better-quality position given to littler selfish nodes will additional to shrink the chance of a unsuccessful release Direction-finding is discuss with the position of a SU. Our process to recognized attack type and proposed exposure technique, COOPON is various from the previous ones in the communication site and environments. COOPON is proposing for CR Networks with numerous channels and is proposed for the case that the channel give information is communicating for the transmission.

III. CRN ARCHITECTURE

This section gives an in deepness justification of the CR Network architecture. Along with the architecture, CR Networks can be categorized as central or distributed network systems. Additionally, CRN can be categorized into two types. They are licensed band operation and unlicensed band operation. CR Network can be measured as Network Access, CR Ad-Hoc access, and Primary network access. The base stations connect straightly with every user and achieve the medium access and the unlicensed user from the network. As shown in the above fig.1, the CR user connects with every user in an ad-hoc network. Data is transfers straightforwardly between the secondary users which fall in the network indoors communication range else data is shared over multiple hops. In Licensed band operation, this band is devoted for the primary user which is part of the network. This band can be used by the Spectrum Band

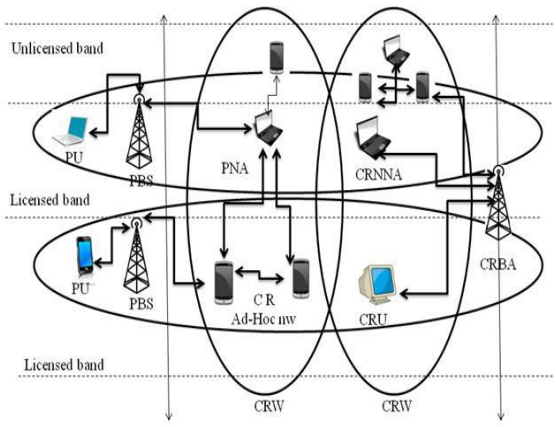

Fig.1. CRN Architecture

secondary user if not occupy by the primary user. Primary Network access is used in CR Networks in the cognitive radio user can right to use the primary base-station through the licensed

band, if the primary network certifications. Unlike other access types, cognitive radio users should support the medium access technology of the CR user can also access the primary base station through the licensed band, if CR Network users should maintenance the medium access technology of primary network.CR Networks user must empty the licensed band if the primary user returns then and move to another empty spectrum band. Unlicensed band operation: The secondary users have the similar correct to make use of the unlicensed band. There is no requiring to empty spectrum for the primary users. CR Networks architecture is shown above fig.1. The cognitive radio user can split the information with their base station from the qualified.

Spectrum band as well as the unlicensed spectrum band. Most important network access: CRN user can be interconnects with the most important base station from the licensed spectrum band with an MAC Protocol.

IV. Selfish Attacks

Selfish attack is types of attacks and then some after the other to occupy cognitive radio spectrum. There are different selfish attacks types.

Type one of the attacks is calculated to prohibit a legitimate secondary User SU (LSU) from the vacant spectrum bands by sending the fake primary User signals PU. The selfish secondary user (SSU) will follow the characteristics of the PU signals. A legitimate SU who eavesdrop the fake signals and makes to takings a result that the PU is active and then the legitimate secondary SU will give up sensing empty channels from the spectrum. This type of attack is normally accomplished when manufacture and restricted transmission between one selfish SU and another selfish SU not allowing for of the number of channels. There should be at least two selfish nodes attacks. Type second attacks area selfish SU monitor the characteristics of signals of PUs but they are carried out in the accessing of a dynamic multiple channels.

In a systematic dynamic signal access process, the SUs will from period to period sense the current in usage band to recognize if the PU is active or not, and if it is, the SUs will without interruption switch to make use of other nearby channels. In these types of attacks, a hamper can well limit legitimate SUs from categorize and using empty spectrum channels. Another type of attack is called channel pre-occupation selfish attacks [12]. This type of attacks can occur in the communication situation that is used to spread the recent empty channel information to neighboring nodes for communication. In the earlier existing methods there will be measured a communication situation the distribution is carried out throughout a common control channel (CCC) which is a channel committed only to substitution management information. A selfish SU will broadcast fake free channel list to its neighboring SUs even though a selfish SUs only make use of three channels, it will send a list of all the five occupied channels. The fake information on channel allocation of every node in the network. Thus, legitimate SUs are banned from using the two available channels. Finding of existing selfish technology is possible to be unsure and less reliable, because they are based on predictable status or predictable characteristics of stochastic signals.

V. Existing System

throughout the common Control Channel. The existing COOPON technique, first it verifies all the nodes in the networks are validated or not. If not, it verifies the nodes one by one using COOPON method. From the below fig 2 shows the selfish attacks detection algorithm and have The existing technique is an autonomous approach but due to using deterministic channel allocation information as well as the support of supportive neighboring nodes. The effectiveness is measured by a detection rate as follows:

$$DR = \frac{No.of\ det\ ected\ selfish\ sec\ ondary\ user}{No.\ of\ actual\ selfish\ sec\ ondary\ user}$$

One SU has a highest of eight data channel and one Common Control Channel. The data rate of channel is 11Mb/s. One SU can have two to five one-hop nearest SUs. The experimentation was performing below various selfish SU compactness in CRN. The article [12] proposed a resourceful selfish cognitive radio attack detection technique, called **COOPON,** (Cooperative neighboring cognitive radio nodes). In conventional spectrum management, for the most part of the spectrum is allocated to the licensed users for restricted use. From the cognitive Radio Technology is carried out in the following steps:

- First, it investigates the available spectrum

bands by a spectrum sensing technology for unlicensed secondary users (SUs).

- Second one is used to assign spectrum dynamically to the unlicensed users.

When the licensed primary user (PU) is not using the spectrum bands in the network, they are considered accessible. Secondary user emulates the characteristics of the primary user by sending the fake signals. Thus, all of the one-hop neighboring SUs will make a conclusion that the target SU is a selfish attacker. All the one-hop neighboring SUs sum of the currently used channels send by themselves and other neighboring nodes. We will describe the number of channels used by each node in the network. Verify if the target SU is a selfish attacker. Here, the spreading is carried out

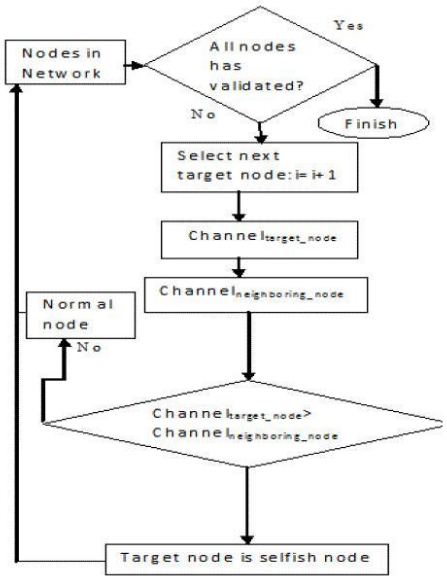

Fig.2. Selfish Attack Detection Algorithm

Explaination about the mechanisms flow chart of COOPON [12]. As reveal that the flow chart, all the currently used channels in the target node and the neighboring nodes are sum of in steps: The channel target node and the channel neighboring node, based on the channel allotment information. $Channel_{targetnode}$ is the calculation of the number of presently used channels to each neighboring nodes statement by the target node and the $channel_{neighboringnode}$ is the calculation of number of nodes at present used channels to the target node statement by each nearest nodes. Then the channel target node will be match up to the channel neighboring node. The target node, N-Node1, N-Node2, N-Node3 and N-Node4 will check any selfish attack of the target node. Using the COOPON detection technique clearly it will describe the number of channels used by each node in the network.

It is pointed that the T-Node 2 reports that have an two channels at this time in use, while N-Node 3 statement that there are two channels at this time in use, while N-Node 3 information that there are three channels currently in use, which creates a disparency N-Node 4 also receives forged channel allotment information from the target node.

On the other hand, all other swap over information pairs, T-Node/N-Node 1 and T-Node/N-Node 2, are accurate. Thus, all of the one-hop neighboring SUs will construct a decision that the target SU is a selfish attacker. According to the above fig.2 shown that the channel target node is 7 and the Channel neighboring node are 5. Because 7 > 5, the target secondary node is notorious as a selfish attacker. The COOPON mechanism is effective than the earlier detection methods, because the channel allotment information is more deterministic than the stochastic signal characteristics.

VI. Proposed System

The proposed technique is simple to calculate. The Proposed algorithm is the credit risk information algorithm. The credit risk information technique will identify the attacks of selfish SUs in the CRN by calculating the credit risk information value. In money matters, credit risk information the value is calculated risk of loss due to defaulter defaulting of loan. A bank checkup the credit risk of an applicant earlier to approving the loan which is relevant to our research of credit risk information value technology is carried out in the following steps. First it calculates the credit risk information value earlier than sending any packet, then route the packets, another time recalculates the credit risk information value. The credit risk information value is steady values, which specify the energy devoted for the packet communication.

CREDIT RISK INFORMATION=No. of packets* Total energy-Remaining Energy

Where, Total energy is the primary energy of the node and Remaining energy is the energy later than data routing. In the proposed technique, Multiselfish node attacks are identifying using the above simple formula. Credit risk

information value is the amount of packets multiplied by the energy used by the node in the CR network. In this method, topology is making first and then credit risk information is calculated for all the nodes in the network. Credit risk information is a stable value. Data routing is done after calculating the credit risk information for all the nodes. Then recalculate the credit risk information. The credit risk information is the energy for each node packet broadcast is intrinsic as ten, as the energy necessary for every normal transmission is close to the value ten. If the credit risk information is greater than ten credit risk information value, then it detect that node as attacker node and then redirect the packet. Once more calculate the credit risk information value. If the value is a lesser amount of than ten credit risk information value, then another time data routing is done.

By using the above formula, we are able to get the energy obsessive for each node's packet transmission. After the topology modernization, the credit risk information value is once more calculated for every node, then it checks whether the calculated Value is between 4 and 10 credit risk information value (or) not until it verify all the in the networks. If the value is in between 4 and 10, and the Performance is more proficient. Because, for regular broadcast, between 4 and 10, and the performance is more proficient. Because, for regular broadcast, the value won't be a smaller amount than four by using this simple calculate process, the attacker node in the CRN can be identify and also the network performance can be better.

This method is also the time overwhelming method, since the formula for calculating credit risk information is easy. Credit risk information value finding mechanism is point that near in a small circle to every node in the network. The credit risk information value for the ordinary broadcast ranges from 4 and 10. This method is also the time overwhelming method, since the formula for calculating credit risk information value is easy. Credit risk information value finding mechanism and to find the Credit risk information value is point that near in a small circle to every node in the network.

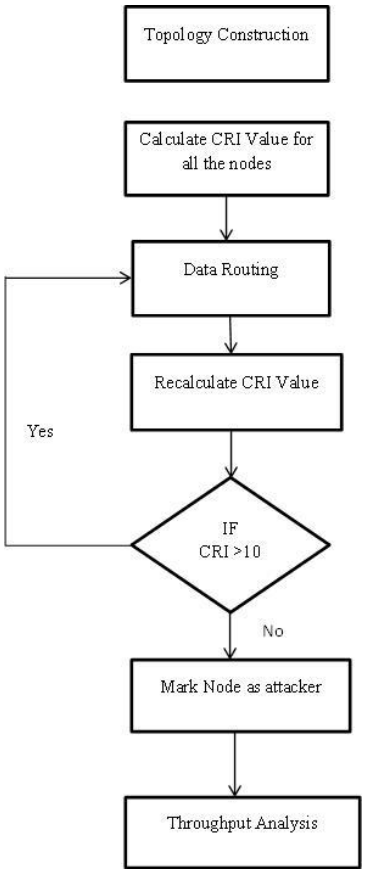

Fig.3. Credit Risk Information Algorithm

The credit risk information value for the ordinary broadcast ranges from 4 and 10. By setting this as threshold value and then calculating the credit risk information will be more effective. Later than calculating the credit risk information, data direction-finding is done once more if the credit risks information less than 10.

The CRI Detection mechanism information for Node 1 is 8, Node 2 is 10 and Node3 is 7. The credit risk information value for Node 4 is 13, which is bigger than 10. This means that Node 4 is a hinder Node. Thus, more than one selfish node in the CRN can be identifying by using the credit risk information.

To discover the selfish node in the cognitive Radio ad-hoc network, the process for handling error is as follows:

- After the node creation, credit risk information value is calculating for every node in the network.
- Match up to the credit risk information value create with all the other nodes. Then the big credit risk information is place as head.

- Transmit the head id to all other nodes. By observe all the nodes, it finds selfish nodes.

VII. PERFORMANCE ANALYSIS

Graph is a fundamental part of shows a result. The graph shows the range of result comparison with packets, throughput, energy capable, unsafe node detection investigation and packet deliverance ratio with respect to the imitation time. In particular, selfish nodes are determined to be selfish only when all additional nodes in the group have the same opinion with the nodes Selfishness. We first measure up to the large selfishness manner with that of COOPON to demonstrate the efficiency of our detection method.

We wait for that the overall selfishness alarm will be decreased in query processing by detecting selfish nodes efficiently with credit risk information value, ever since a lot of selfish nodes will be removed from the replica allotment stage and a lot of dependable nodes will serve up data requests from commencing nodes. It is wanted to observe truly selfish nodes to calculate the efficiency of the detection method. A data client cannot inform estimated nodes selfishness from network disconnection, i.e., no respond from the estimated node. The outline of the simulation network of the routing performance of credit risk information value match up to COOPON method is shown below Figure4.

The simulation output of the performance level of Intrusion Detection System (IDS) between credit risk information and the existing method is shown below fig.5. In the figure6, y-axis represents the number of nodes and the x-axis represents the selfish node detection. The performance level increases with our proposed detection mechanism.

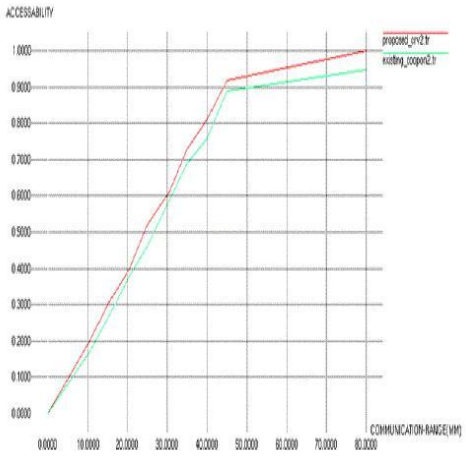

Fig.4. Routing performance on average accessibility

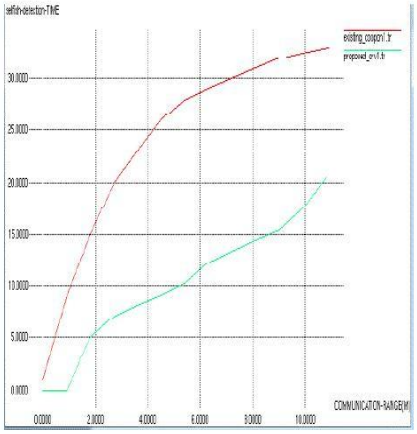

Fig.5. Performance level of Intrusion Detection System

Finally, we examine the effect of communication range. The simulation layout of the performance level of selfish node detection time and the communication range is shown above. The selfish node detection time of credit risk information value is less when compared with that of the COOPON method.

VIII. CONCLUSION

The existing methodology can expect only one selfish node deceits on the occupied CRN. Because, the COOPON uses the deterministic channel segment in sequence. In this article, to order the Multiselfish node attacks using the credit risk information value. The proposed credit risk information algorithms observe more than one selfish secondary user in the CR Networks using the credit risk information value.

Our approach is computing for the cognitive radio ad-hoc networks. The credit risk information algorithms make use of ad-hoc network advantage such as energy required for the packet broadcast at all node in the network worth of a better detection. The proposed dependable and simple work out procedure can be well built-in for real-world use in the future.

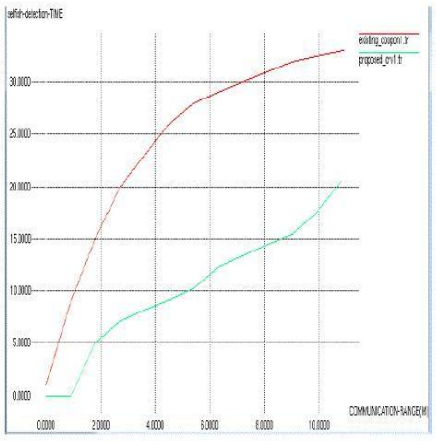

Fig.6. Performance level on selfish node detection time

REFERENCES

[1] K.Balakrishnan, J.Deng, and P.K.Varshney,"TWOACK: Preventing selfishness in Mobile Ad Hoc Networks," proc.IEEE Wireless Comm. And Networking, pp.2137-2142, 2005.

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

[3] R .Chen, J.-M. Park and J. H. Reed (Jan. 2008), "Defense against Primary User Emulation Attacks in Cognitive
Radio Networks", IEEE JSAC, vol. 26, no. 1, pp. 25–36. KSII Trans. Internet and Information Systems, vol. 6, no. 10, pp. 2455–72.

[4] Z. Dai, J. Liu, and K. Long (Oct. 2012), "Cooperative Relaying with Interference Cancellation for Secondary Spectrum Access".

[5] Z. Gao et al., (2012),"Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks", IEEE Wireless Commun., vol. 19, no. 6, pp. 106–12.

[6] C.-H. Chin, J. G. Kim, and D. Lee (Mar. 2011), "Stability of Slotted Aloha with Selfish Users under Delay Constraint", KSII Trans. Internet and Info. Systems, vol. 5, no. 3, pp. 542–59.

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

[8] T.Hara, "Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility", Proc.IEEE INFOCOM, pp.1568-1576, 2001.

[9] Jae-Ho Choi, Kyu-Sun Shim, Sangkeun Lee, and Kun-Lung Wu (2012),"Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network", IEEE Transactions on mobile computing,vol.11 no.2.

[10] "A Survey of Techniques Used Detect Selfish Nodes in MANET", Karthik.M, Jyothish K John, International Journal for scientific Research & Development /Vol.1, Issue 4,2013.

[11] S.Li et al., (2012),"Location Privacy Preserving Dynamic Spectrum Auction in Cognitive Radio Network", IEEE INFOCOM" 12, pp. 729–37.

[12] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter (May 2013), "Selfish Attacks and Detection in Cognitive Radio Networks", Korea University.vol 27, Issue: 3, IEEE Network.

[13] M. Yan et al. (May.2011),"Intrusion Detection System (Ids) for Combating attacks against Cognitive Radio Networks", IEEE/ACIS 10th Int"l. Conf. Computer and Information Science (ICIS), pp.58–61

[14] Nasser N, Chen Y. (2007), "Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network", in Proceeding IEEE (ICC"07), pp 1154-9.

[15] X. Tan and H. Zhang (Sept. 2012), "A CORDIC-Jacobi Based Spectrum Sensing Algorithm for Cognitive Radio", KSII Trans. Internet and Info. Systems, vol. 6, no. 9, pp. 1998–2016.

Author Profile

G.Gowrishankar currently is doing a PG degree, Computer Science and Engineering (With Specialization in Networks) in Kongunadu College of Engineering and Technology. Tamilnadu, India. I received Bachelor Engineering Degree in Sona College of Technology in 2011, Salem.

S.Balgani, working an Assistant Professor, in Kongunadu College of Engineering and Technology, India in the year of 2013.She completed the Master Degree in VSB Engineering College, Karur, Bachelor Degree in Vidhya Vikas College of Engineering and Technology, Thiruchengode.

R,Aruna working an Assistant Professor, in Kongunadu College of Engineering and Technology, India in the year of 2013. She completed the Master Degree in CMS College of Engineering, Namakkal, Bachelor Degree in SNS College of Technology, Coimbatore.