International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Secure Data Transmission by Detecting Different Attacks in CRN to improve the throughput

Anand Ashok Khatri, Yogesh Kumar Sharama, Satish Ramchandra Todmal

Abstract*: Cognitive Radio (CR) is a technology that promises to solve the data transmission problem by allowing secondary users to coexist with primary user without causing any interference to the communication. It means to improve the usage of the radio assets to improve the throughput. Despite the fact that the operational parts of CR are being investigated broadly, its security viewpoints have increased little consideration. In this work, present a CRN architecture , Different Protocol, with complete rundown of major known security dangers and assaults inside a Cognitive Radio Network (CRN). Our goal in this paper is to dissect the distinctive security issues of the primary ongoing advancements of Cognitive Radio Networks with proper resource allocation to improve the throughput.

Keywords* : Cognitive Radio, Cognitive Radio Network, Channel allocation, Protocol, security.

I. INTRODUCTION:

Cognitive Radio (CR) is a receptive, versatile radio system innovation which can progressively recognize the accessible nodes in a remote range and change transmission parameters empowering increasingly remote correspondence divert that are accessible in organize and improve the radio system activity [8]. By including to activity CN it improves its recurrence, ability and different parameters so can get more results, these parameters incorporate postponement, PDF ratio, throughput and Energy consumption.

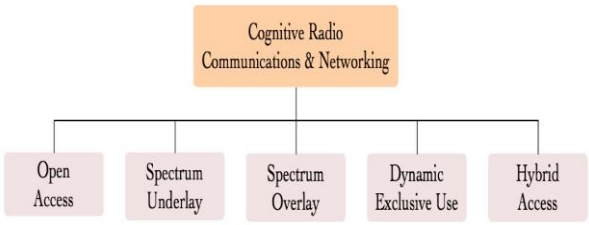

Figure 01: Types of C**ognitive** R**adio (CR) Network**

This can be function as an independent domain that can be access as indicated by his work to get all the more productively work from CR. The CR watched his very own in constant way with radio recurrence that can be gain from other. At that point this yield can be use by CR for other work so can get sheltered correspondence in WMN appears in figure. 02 and get most extreme throughput. Along these lines, would it be able to convey the necessary information with great quality the individuals who required constrained information with great quality in less time with most extreme yield.

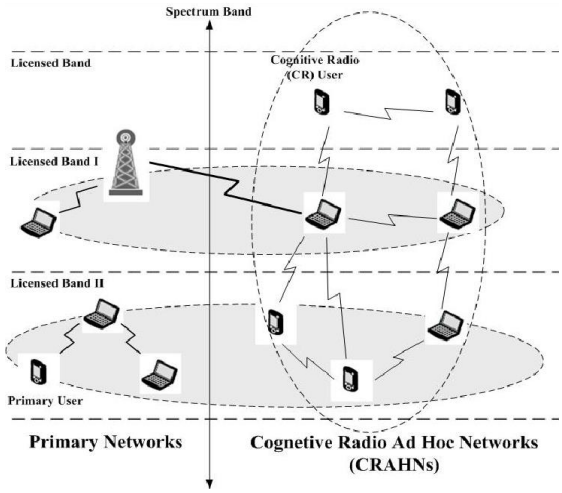

Figure 02: A Dynamic Cognitive Radio Network Architecture

cognitive radio network is a secondary network, in other words, just when the approved band of first-level client is inert, these groups can be utilized by subusers which are likewise called psychological modes for information correspondence [7]. So the channel determination calculation must be viewed as while steering convention is planned. So as to meet system execution prerequisites, each psychological nodes in cognitive radio system must have the option to switch between different accessible channels and select a suitable inert channel for correspondence.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Anand Ashok Khatri*, Research Scholar, HOD, Research coordinator, Shri. JJT University, Churella, Jhunjhunu (Rajasthan) Churella, Jhunjhunu (Rajasthan) Engineering and Research, Pune, Maharashtra
Yogesh Kumar Sharama, Research Scholar, HOD, Research coordinator, Shri. JJT University, Churella, Jhunjhunu (Rajasthan) Churella, Jhunjhunu (Rajasthan) Engineering and Research, Pune, Maharashtra
Satish Ramchandra Todmal, Research Scholar, HOD, Research coordinator, Shri. JJT University, Churella, Jhunjhunu (Rajasthan) Churella, Jhunjhunu (Rajasthan) Engineering and Research, Pune, Maharashtra

When intellectual client distinguishes that essential client is utilizing the channel, it should quickly and genuinely pull back. Along these lines, channel exchanging delay coming about because of channel regularly changing by psychological nodes must be considered, and, particularly in multihop arrange information transmission process, this issue is increasingly self-evident. We can clarify the issue in Figure 1: there are two ways, to be specific, A-B-C and D-B-E. The channel number chose by An and C is 1 and channel 2 is chosen by D and E.

So as to guarantee the two ways impart regularly, node B should switch between channel 1 and 2 every now and again, which brings about exchanging delay.

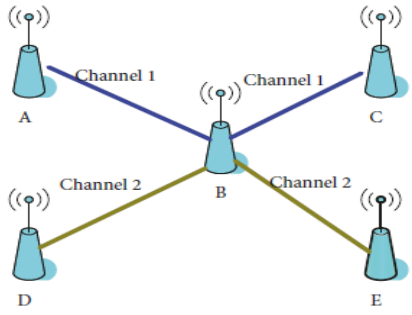

Figure 03: Channel Allocation in CN.

On other hand, the start to finish dependability is truly influenced by the exercises of essential client in multihop directing, so the soundness of each connection must be considered. For instance, there is a way S-a-b-D, and if the channel among an and b isn't accessible because of the movement of essential client, the connection will come up short, and right now whether the other connection is associated or not, the entire connection isn't accessible. We can't finish information transmission except if a course is remade. Anyway revamping courses will bring about extra deferral and more vitality squander. So for multihop steering, the soundness of course should be considered.

1.1 CRN engineering

The CRN engineering is a structure that points of interest the physical parts of the system, alongside the operational standards and methods.

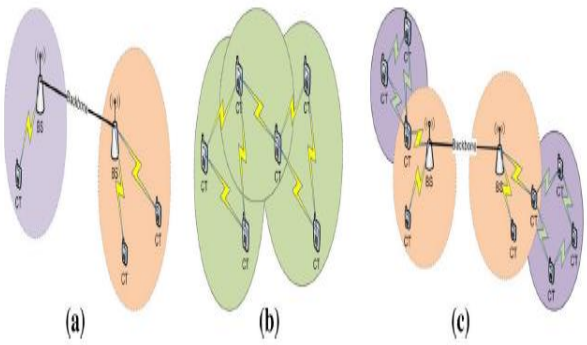

Figure 04: Different types of cognitive radio network architecture. a Infrastructure Architecture (single hop) b Ad-hoc Architecture c Mesh Architecture (with trunked backbone)

In a network-centric architecture, CRs can just speak with the Base Stations (BSs). Then again, in specially appointed design correspondence between two neighboring intellectual node can happen when these two node are tuned to an equivalent channel. Since in intellectual radio specially appointed system, every node has its own open channel set, two neighboring node need to have in any event one normal divert in their available channel sets to make correspondence. The CRN architectures can be classified as

- infrastructure-based CRN
- cognitive radio ad-hoc network
- Cognitive radio mesh network.

II. LITERATURE REVIEW:

In this section we are going to discuss different author review regarding the CRN,

Yogesh Kumar Sharma et al. (2019) - Sensor systems are very not quite the same as customary systems in various manners: sensor systems have serious vitality concerns, repetitive low-rate information, and many-to-one streams. Steering conventions produced for other Adhoc systems can't be applied legitimately in WSN in light of the vitality imperative of the sensor hubs. Information driven advancements are expected to perform in organize conglomeration of information to yield vitality proficient spread [8]. Sensor systems are utilized in numerous applications like condition checking, well being, modern control units, military applications and in the different figuring situations. Since sensor the whole sensor node are battery controlled device, vitality utilization of node during transmission or gathering of bundles influences the life-time of the whole system. In this paper, model information driven directing and contrast its presentation with customary end-with end steering plans [7].

Yunus Sarikaya et al. (2018) - A cognitive radio network with single antenna primary user (PU), multi-antenna secondary users (SUs) and destination and eavesdropper. SUs act as helper nodes transmitting noise to confound a passive eavesdropper while nulling the interference leakage at the destination. The jamming helper nodes are non-altruistic, and they gain access to the primary network by aiding in the confidential transmissions of the PU [8]. The delay-unlimited system, derive the achievable confidential rates given the control strategies for bandwidth and power allocation.

Yuanyi Wang et al. (2018) - Here proposed algorithm can allocate transmission power to each SU on each subcarrier with the objective of increasing the average throughput of secondary network over a finite time interval. Both the interference power constraint limited by primary user (PU) and minimum throughput constraint of each SU to improve the throughput of SUs while guaranteeing the communication quality of PU.

Xiaofeng Feng et al. (2017) - Consider a more complicated model with multiple PUs and try to investigate the cooperative jamming between multiple PUs and a single SU. When there is multiple PUs in CRN, more spectrum utilized for data transmission, SU will cooperate with multiple PUs at the same time. Considering that both PU and SU are coherent and selfish individuals, the interaction between PUs and SU is formulated as a multi-leaders and single-follower, wherein PU is the leader and SU is the follower.

Here also prove that when a specific condition is satisfied, the existence of SE can be guaranteed and a Gauss-Jacobi iterative algorithm is proposed to compute a SE.

Mahmoud Khasawneh, et al. (2017) - The proposed authentication scheme, in comparison to the existing approaches, decreases the number of cryptographic operations and the verification time needed to complete the authentication process.

The correctness of the proposed approach has been verified using the BAN logic and through the Scyther verification tool. Due to this authentication approach is safe against many attacks.

Huijin Cao, et al. (2016) - Cognitive radio network (CRN) that dynamically distributes packets from the secondary user (SU) to different available primary channels, readdress the spectrum decision issue for a CRN, where the SU supports delay sensitive (DS) and best effort (BE) services simultaneously and can access multiple channels which are shared by the two services. The SU makes channel selection decisions for both DS and BE packets at the beginning of each time slot, based on which the packets are sent to the most suitable channels upon their arrival. Here is the objective is to minimize the average packet transmission delay while maintaining the priority of the DS packets. A priority queueing model is introduced to consider the effect of different channel conditions, such as multiple interruptions due to PU transmissions and a general distribution of service time, on the delay performance of the prioritized SU's services.

Need of study:

- The growing number of wireless devices for in-house is causing a more intense use of the spectrum to satisfy the required quality-of-service such as throughput. That can't achieve by static network.
- In Static Cognitive Radio Network use a static route to send the packet from source to destination gives less throughput, issue in spectrum sensing, security issues and required more energy.
- To increase the security as well as reliable data transmission dynamic channel allocation is proposed in Cognitive Network.

III. CLASSIFICATION OF CHANNEL ASSIGNMENT TECHNIQUES OF CRN

The channel assignment techniques adopted by the state-of-the-art channel assignment algorithms in CRNs are game theory, linear programming (LP), nonlinear programming (NLP), heuristics, network-based graph, genetic algorithms, evolutionary algorithms and soft computing.

3.1 Game theory

Game theory (Byun et al., 2008; Hongshun and Xiao, 2010; Zhang and He, 2010; Wu et al., 2011; Li et al., 2010) can be defined as a mathematical framework which consists of models and techniques that can be used to analyse the iterative decisions behavior of individual units concerned about their own benefits. The objective of the game theory-based channel assignment algorithm is to find the Pareto-optimal solution for the channel assignment problem. Game theory has been widely used in cognitive SA algorithms because it is a powerful decision-making framework that can be used both for cooperative and non-cooperative decisions between SUs. Cooperative game is a game where all players are concerned about the overall benefits and they are not very worried about their own personal benefits.

3.2 Linear programming

LP (Irwin et al., 2013; Yu et al., 2010) is a technique for optimizing a linear objective function subject to linear equality and linear inequality constraints. The problem formulation in LP is easy and simple. Some current channel assignment algorithms in CRNs employ binary linear programming (BLP) and mixed integer linear programming (MILP) to formulate the problem. BLP solves problems when the variables are restricted to be either zero or one. The MILP solves problems when only some of the variables are constrained to be integers.

3.3 Nonlinear programming

NLP (Chen-li et al., 2009) will in general take care of the channel task advancement issue, which is characterized by requirements of balances and imbalances. The target capacity to be improved or a portion of the imperatives are nonlinear. Pareek and Lee (2011) use molecule swarm enhancement (PSO) to fathom the blended whole number nonlinear programming (MINLP) in an OFDMA-based two-way subjective transfer arrange that includes different source-goal sets and numerous transfers.

In Salah et al. (2015), the creators propose a cross-layer steering system for brought together multi-bounce CRNs in TV void areas. The issue is numerically demonstrated a blended whole number nonlinear program that requires a proper arrangement philosophy.

3.4 Heuristics

Heuristic strategies (Saleem et al., 2012; Kim et al., 2010; Alsarahn and Agarwal, 2009a, 2009b; Chen-li et al., 2009) are regularly used to accelerate the procedure of range task and to discover a decent arrangement rapidly in situations where a comprehensive inquiry is unrealistic. They don't require prohibitive suppositions of the improvement schedules and they license the utilization of models that are a greater amount of sort of certifiable issues. Heuristic methods can give a close ideal arrangement at sensible computational expense for algorithmically perplexing and tedious issues.

3.5 Network diagram based

Each system can be displayed as a chart, where the vertices compare to the cell phones or hubs and edges relate to the associations between cell phones. To fathom diagram based (Zhao et al., 2008; Xin et al., 2008; Zhao and Cao, 2012) range task issues, a few techniques are utilized. The most widely recognized one depends on developing the system strife diagram that catches the obstruction between neighbor SUs. Chart shading is generally utilized in intellectual SA calculations where the psychological system is mapped to a diagram, which is either unidirectional or bi directional as per the calculation's attributes. The vertices relate to the SUs that offer the range and the edges show the impedance between the SUs.

3.6 Evolutionary calculations

These are calculations that have some tendency towards recreating the advancement of individual structures by means of procedures of choice, recombination and change generation, in this way delivering better arrangements.

Distinctive transformative calculations, for example, subterranean insect settlement, molecule swarm enhancement, honey bee state, and so on are found in the diverse writing.

Modi and Murmu (2017) propose a subterranean insect settlement framework (ACS)- based range mindful handover calculation for numerous sets of SUs in CRN. ACS has been utilized to gain proficiency with the range conduct for tackling handover issue and for channel choice.

IV. CLASSIFICATION OF ROUTING PROTOCOLS:

Following are the three routing protocols generally use in Adhoc Network

i) Proactive Protocols
ii) Reactive Protocols
iii) Hybrid Protocols

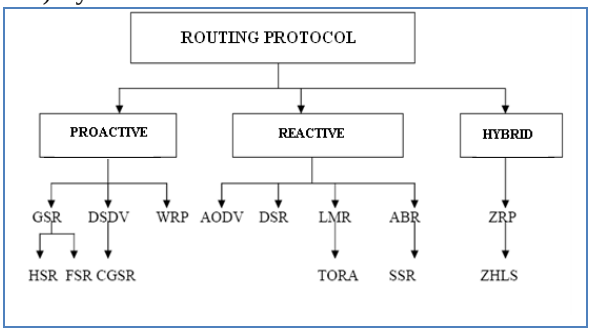

FIGURE 5 : CLASSIFICATION OF ROUTING PROTOCOL

REACTIVE PROTOCOLS:

These protocols are also known as Demand Driven Reactive Protocols [8, 9]. The reason why they are called as Reactive protocols is as because they never start the discovery of routes by themselves.

The reactive protocols used so far are DSR, AODV and TORA.

Usually Reactive protocols:

- Until demanded, don't find the route
- They use 'On Demand' flooding method to send the query to get the destination information
- They use bandwidth only while transmitting the data to destination node.

Proactive Protocols:

Proactive protocols [6] work differently if compared with the Reactive protocols. The protocols constantly check the updated topology. Every node in the network knows every other node of the network. Complete network is known to all the nodes of the network. The routing information is separately maintained in different tables. When network topology is changed, tables are updated. The nodes also share the network topology and change information with each other. Also get the information of route whenever required. The Proactive protocols are DSDV and OLSR.

HYBRID PROTOCOLS:

These protocols use the strengths of reactive as well as proactive protocols and combine these features to get more refined results. The network is partitioned into different zones and different protocols are used for two zones. The example of Hybrid Routing Protocol [6,17,18] is Zone Routing Protocol.

V.ATTACKS IN CRN

In the phase of design and analysis of secure distribution system, trust is an important feature. Trust and security in Cognitive Radio Networks are always interlinked. They are complementive and mutually inclusive to each other. To discuss the attacks on CRN, we classify them based on the layers in which the attack can occur. There are various attacks in different layers.

At the **Physical layer,** Primary User Emulation attack (PUE), Objective Function Attacks, Jamming, etc. are discussed.

Attacks at the **Link layer** include Spectrum Sensing Data Falsification (SSDF), Control Channel Saturation DOS Attack (CCSD), etc.

At the **Network layer,** Hello Flood Attack and Sinkhole Attack are discussed.

At the **Transport layer,** Lion attack is well known. Some of these attacks might work on different layers too, such as, jamming, which can be launched at physical or MAC layers.

5.1 Primary User Emulation Attack (PUEA): One of the major technical challenges associated with spectrum sensing is the problem of exactly distinguishing primary user signals from secondary user signals. In CR network, primary users possess the priority to access the channel. If a primary user be- gins to transmit across a frequency band occupied by a secondary user, it is required to leave that particular specific spectrum band immediately. Conversely [17], when there is no primary user activity present within a frequency range, all the secondary users possess equal rights to the unoccupied frequency channel. Based on these paradigms, there exists the potential for malicious secondary users to mimic the spectral characteristics of the primary users in order to gain priority access to the wireless channels occupied by other secondary users. Malicious PUE attack is similar to denial of service attack. It prevents the legitimate secondary users from detecting and using the free spectrum bands.

5.2 Jamming Attack: The objective of jamming attack in the communication network is to deny service by eating up high percentage of bandwidth. In jamming attack, the attacker (or the jammer) maliciously sends out packets continuously to obstruct the legitimate participants in a communication session from sending or receiving data; simultaneously it creates a denial of service situation. The jammer can also disrupt communication by blasting a radio transmission resulting in the corruption of packets received by legitimate users. A more dangerous attack that a jammer can perform is jamming the dedicated channel that is being used to exchange sensing information between CRs [5]. Thus, jamming is an attack that is known to both physical and MAC layers. Four types of jammers have been identified in [9] viz., Constant Jammer, Deception Jammer, Random Jammer and Reactive Jammer. Constant/Static jammer emits signal continuously on a particular channel.

Deception jammer is similar to constant jammer. But, in this case, the pulses are similar to the regular data packets from a legitimate user. Reactive jammer transmits jamming pulses only when it finds the channel to be busy, so as to cause collision to an on-going transmission. Random jammer alternates between jamming and sleeping mode [11].

5.3 Cross- layer Attack: A smart attacker can launch several attacks in different layers coordinately. This is referred to as the cross-layer attack [12].

This coordination of attack activities can reduce the attacker's probability of being detected, lowers the cost to conduct the attack and helps to achieve the attacker's goal which may not be possible in a single layer. To make this attack a success, all attackers should have a clearly defined goal. It can also reduce channel utilization both in PHY layer and MAC layer. Cross-layer attack can be defined as, a collection of attack activities that are conducted co-ordinately in multiple network layersin order to achieve specific attack goals.

5.4 Spectrum Sensing Data Falsification Attack (SSDF): This attack is the transmission of false spectrum sensing data by malicious secondary users. SSDF are referred to such attacks where an attacker may send false local spectrum sensing results to a data collector, causing the data collector to make a wrong spectrum sensing decision. This attack is also known as the Byzantine Attack. It takes place when an attacker sends false local spectrum sensing data to its neighbours or to the fusion center. In a centralized CRN, a fusion center collects all the sensed data and then uses them to take a decision on which frequency bands are occupied and which are free. Cheating and fooling the fusion center will either deny some legitimate users from using a free band or al- low users to use a band that is already occupied. Similar problems are found with distributed CRN at the time of spectrum sensing decision [17]. Thus, it is being considered that SSDF attack could be more harmful in a distributed CRN because the false information can propagate quickly with no means to control them. While in the centerlized CRNs, the fusion center can control and lessen the effect of false information by comparing the data received from all CRs.

5.5 Control Channel Saturation DoS Attack (CCSD): This attack leaves the CRN with near-zero throughputs. In a multihop CRN, CRs communicate with each other performing a channel negotiation process. MAC control frames are exchanged to reserve channel during the negotiation phase. The common control channel has limited capacity for supporting concurrent data channels. When many CRs communicate at the same time, the channel becomes a bottleneck. The attackers take advantage of this situation and generate forged MAC control frames for saturating the channel, thus decreasing the network performance.

5.6 Hello Flood Attack: In Hello-flood attack, the attacker sends broadcast message to all the nodes in a network with enough power to convince them it is their neighbour. For instance, an attacker sending a packet to a specific destination can encourage even far away nodes to use this route, convincing them he is their neighbour. As a result, the packet is lost and it will have no neighbour to forward its packet.

5.7 Lion Attack: Lion attack is defined as a jamming targeted to reduce the through- put of Transmission Control Protocol (TCP) by forcing frequency handoffs [16]. The lion attack, together with the PUE attack, can effectively reduce the throughput of TCP. The attacker can even perform a Denial of Service (DoS) by emulating a primary transmission at specific instant of time, if he knows some of the connection parameter.

VI. SECURING COGNITIVE RADIO NETWORKS

In this area, some broad countermeasures for attacks from each layer are talked about. For reducing sticking attacks in CRN, Spread Spectrum approach is being utilized. The accessible range band is separated into various non-covering channels. From among this channel, just a little part of the channel is utilized for transmission at once. The assailant can even stick a channel, however with unimportant sticking impact or the channel may not be utilized by the Cognitive Radio. Forward Error Correction (FEC) plans can be utilized to develop the lost information because of sticking attacks in CRN. Interruption Detection System (IDS) likewise fill in as important instrument for recognizing sticking attacks. For verifying against PUE attacks, the transmitting source should be distinguished, i.e., regardless of whether the transmitting source is an essential client or a vindictive client. For this, cryptographic validation component can be applied for recognizing the client. As the FCC guideline doesn't permit adjusting essential client framework, scientists picked to locate the careful area of an essential client. On the off chance that the transmitting source coordinates the area of the essential client, the source is viewed as essential client. Else, it is viewed as an aggressor. To decide the area of the transmitting source, two methodologies are considered, Distance Ratio Test (DRT) and Distance Difference Test (DDT), which depends on signal stage contrast. Target Function attacks adjusts the parameter of the remote media by sticking at a particular time and recurrence in regard to the parameters characterized in the arrangement. A basic answer for this assault is to characterize an edge an incentive for each updatable radio parameter. This will anticipate any correspondence when at least one parameters don't satisfy its predefined limit. Interruption Detection System (IDS) can likewise be utilized to moderate Objective Function attacks. For verifying against Spectrum Sensing Data Falsification (SSDF) attacks, an information combination method called Weighted Sequential Ratio Test (WSRT) is utilized [18]. WSRT has two stages: Reputation support and Sequential Probability Ratio Test (SPRT). In notoriety support step, each node has beginning notoriety esteem equivalent to zero. Upon each right neighborhood range report, the notoriety worth will be expanded by 1. Another methodology for recognizing the Byzantine attacks is by tallying the confuses between nearby choices and worldwide choices at the combination focus over a period window. CCSD assault can be constrained by adjusting a confided in engineering. Here, any suspicious CR host will be observed and assessed by its neighbors. A neighbor can play out a successive examination dependent on the perception information and draw an official choice.

The Sequential Probability Ratio Test (SPRT) can likewise be utilized. For shielding against Hello Flood attacks, symmetric key calculations are proposed.

A symmetric key is imparted to a confided in base station. The base station fills in as a Third Party, which encourages the foundation of session enters between the gatherings in the system. Sinkhole assault is hard to identify, as it abuses the steering convention plan and system design. Lion assault expects to diminish the throughput of TCP.

To moderate this attacks, the TCP convention must know about what's going on in the physical layer and change its conduct as indicated by the system condition, along these lines improving its exhibition. To verify the control information from listening stealthily during transmission, a gathering key administration (GKM) can be utilized to permit CRN individuals to scramble, decode and validate themselves. At that point, cross-layer IDS can be utilized to recognize the attacks. Another system for moderating lion assault is molecule swarm streamlining (PSO) [8]. Here, each cognitive radio goes about as a molecule which has thought regarding the best conduct in a specific circumstance.

VII. PROPOSED METHOD

Finding path & sending data by using the dynamically resources allocation method in available network are close application of wireless network. By using CR Network in our system we are able to achieve the close cooperation, better performance and lower complexity. In order to improve the efficiency of Dynamic resource allocation in system the Secure Data Transmission process should be considered jointly with the Dynamic resource allocation, main objective of doing this is to maximize the packet delivery patio and throughput by using limited resources and Spectrum. Research Plan of our work is as follows:

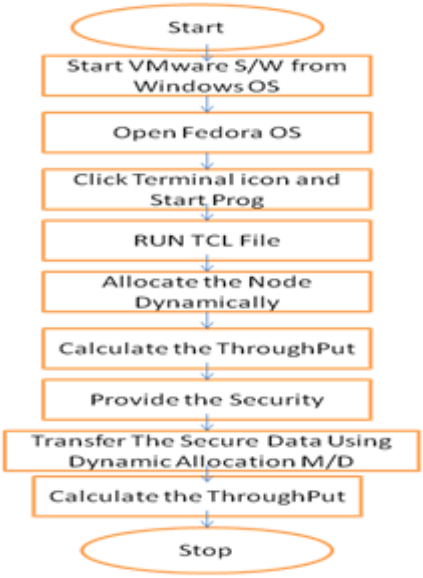

Figure 06: Flowchart of How Program work & Transfer Data Securely.

As algorithm works in iterative in nature for improvement in accuracy then if more number of anchors use in algorithm slow down the system,

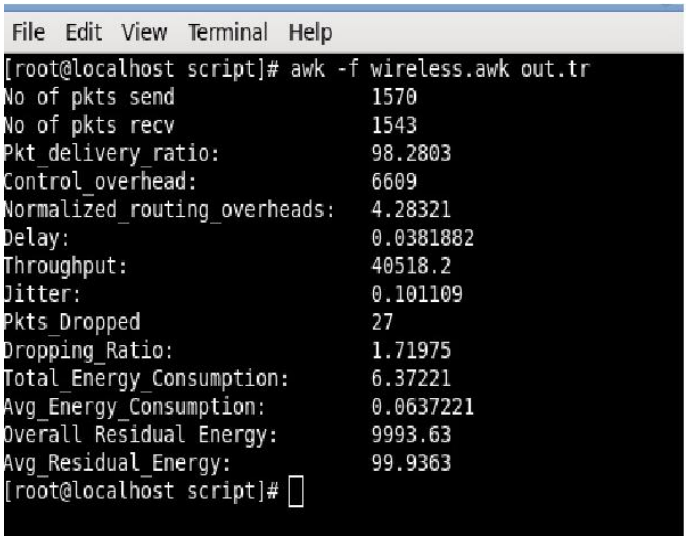

Figure 07: Simulation Output

VIII. CONCLUSION

In this paper, examine the CRN design, it working, Routing Protocol with CRNs security and basic dangers/assaults on various layers are broke down and tended to with their countermeasures. CRNs are based on existing innovations and the ways to deal with give successful security to these systems are insufficient. Because of the specific qualities of CRNs, new attacks arise and some of the previous ones increase in its complexity with loss of packets. In addition, as CRN innovation keeps on developing and turns out to be increasingly normal, further desire for security be required with proper resource allocation.

Similarly, new security proposals are needed to be effective against specific attacks, particularly in the physical layer to the upper layers. Likewise, there is still requirements for exhaustive component to prevent or counter act the attacks at all layers.

In order to address these challenges, each CRN users in the CR network must have the following features:

- Determine the available spectrum.
- Select the best available channel.
- Coordinate the free channel access with other users.
- Proper Allocation of Available Sources.
- Improve the security in CRN.

In particular, signal authentication and mechanisms to detect malicious insiders will overcome most of the specific attacks to CRN, but require future in-depth research with proper resource allocation to improve the throughput in network.

REFERENCES:

1. Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis, c(2012) “A Survey on Security Threats and Detection Techniques cin Cognitive Radio Networks”, IEEE Communications Surveys c& Tutorials, 15, 1, 1553-877X.
2. Ali Al-Talabani, Yansha Deng, A. Nallanathan and Huan X. Nguyen, (2015) “Enhancing Secrecy Rate in Cognitive Radio Networks via Multi-level Stackelberg Game”, 1089-7798.

3. Amr A. El-Sherif, and Amr Mohamed, (2014) "Joint Routing and Resource Allocation for Delay Minimization in Cognitive Radio Based Mesh Networks", IEEE Transactions on Wireless Communications, 13, 1, 1558-2248.
4. Anthony Busson, Bijan Jabbari, Alireza Babaei, and V´eronique V`eque, (2014) "Interference and Throughput in Spectrum Sensing Cognitive Radio Networks using Point Processes", Journal of Communications and Networks, 16, 1, 1976-5541.
5. Ayaz Ahmad, Sadiq Ahmad, Mubashir Husain Rehmani and Naveed Ul Hassan, (2015)" A Survey on Radio Resource Allocation in Cognitive Radio Sensor Networks", IEEE, 1553-877X.
6. C. Liang and F. R. Yu, (2015) "Wireless Network Virtualization: A Survey, Some Research Issues and Challenges" IEEE Communication Surveys & Tutorials,17, 1, 358-380, 1553-877X.
7. A B.Kathole "Exclusion of Blackhole attack to provide privacy security service in Adhoc wireless Network", International Journal Bioinfo publication, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012.
8. A B Kathole, N V Pardakhe, D S Kute, "A REVIEW PAPER ON COMPARISON AND ANALYSIS OF DIFFERENT ATTACK AND INTRUSION DETECTION SYSTEM" International Journal of Bioinfo, ISSN: 2249-7013 & E-ISSN: 2249-7021.
9. Atul B Kathole, Dr.Dinesh N.Chaudhari, " Fuel Analysis and Distance Predication using Machine learning", 2019 ,International Journal on Future Revolution in Computer Science & Communication Engineering, Volume: 5 Issue: 6.
10. Techniques for Efficient Spectrum Access in Cognitive Radio Networks", 1553-877X.
11. Himanshu Agrawal, "Spectrum Allocation in Cognitive Networks", JIIT-128 NOIDA, India.
12. Huijin Cao, Hongqiao Tian, Jun Cai, Attahiru S. Alfa, Shiwei Huang, (2016) "Dynamic Load-balancing Spectrum Decision for Heterogeneous Services Provisioning in Mutil-channel Cognitive Radio Networks", IEEE, 1536-1276.
13. Hurtado Borràs, J. Palà Solé, D. Camps Mur and S. Sallent Ribes, (2015) "SDN Wireless Backhauling for Small Cells" in IEEE ICC 2015 - Mobile and Wireless Networking Symposium, Electronic ISBN: 978-1-4673-6432-4.
14. Hyungsik Ju, and Rui Zhang, (2014) "Throughput Maximization in Wireless Powered Communication Networks", IEEE transactions on wireless communications, 1536-1276.
15. Jian Yang, and Hangsheng Zhao, (2015) "Enhanced Throughput of Cognitive Radio Networks by Imperfect Spectrum Prediction", IEEE Communications Letters,19, 10, 1089-7798.
16. Junni Zou, Qiong Wu, Hongkai Xiong, Chang Wen Chen, (2015) "Dynamic Spectrum Access and Power Allocation for Cooperative Cognitive Radio Networks", 2015 IEEE, 1053-587X.
17. A B Kathole, N V Pardakhe, D S Kute, "A REVIEW PAPER ON COMPARISON AND ANALYSIS OF DIFFERENT ATTACK AND INTRUSION DETECTION SYSTEM" International Journal of Bioinfo, ISSN: 2249-7013 & E-ISSN: 2249-7021.
18. Lei Xu IEEE Member, A. Nallanathan IEEE Fellow, Xiaofei Pan, Jian Yang IAPR Fellow, and Wenhe Liao, (2018) "Security-Aware Resource Allocation with Delay Constraint for NOMA-based Cognitive Radio Network", IEEE Transactions on Information Forensics and Security, 1556-6013.
19. LI Hongning, PEI Qingqi, MA Lichuan, (2014) "Channel Selection Information Hiding Scheme for Tracking User Attack in Cognitive Radio Networks", China Communications,1673-5447.
20. Li Jianwu1, Feng Zebing2, Feng Zhiyong2, Zhang Ping1, (2015) "A Survey of Security Issues in Cognitive Radio Networks", China Communications • March, 1673-5447.
21. Long Yang, Hai Jiang, Sergiy A. Vorobyov, Jian Chen and Hailin Zhang, (2015) "Secure Communications in Underlay Cognitive Radio Networks: User Scheduling and Performance Analysis", IEEE Communications Letters, IEEE, 1089-7798.
22. Mahmoud Khasawneh, Anjali Agarwal, (2017) "A Secure and Efficient Authentication Mechanism Applied to Cognitive Radio Networks", IEEE, 2169-3536.
23. Securing Cognitive Radio Networks against Primary User Emulation Attacks, Rong Yu, Yan Zhang, Yi Liu, Stein Gjessing, and Mohsen Guizani, December 2016.
24. Analysis of Attacks in Cognitive Radio Networks, M.Padmadas, Dr.N.Krishnan, V.Nellai Nayaki, Vol. 4, Issue 8, August 2015.
25. X. Chen, H-H. Chen, and W. Meng, "Cooperative Communications for Cognitive Radio Networks-from Theory to Applications," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1180-1192, Third quarter 2014.
26. M. Naeem, A. Anpalagan, M. Jaseemuddin, and D. C. Lee, "Resource Allocation Techniques in Cooperative Cognitive Radio Networks," IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 729-744, Second quarter 2014.
27. N V Pardakhe, A B Kathole ,"A REVIEW: MANET ROUTING PROTOCOLS AND DIFFERENT TYPES OF ATTACKS IN MANET" International Journal Bioinfo publication, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1.
28. S. K. Sharma, T. E. Bogale, S. Chatzinotas, B. Ottersten, L. B. Le and X. Wang, "Cognitive Radio Techniques Under Practical Imperfections: A Survey," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 1858-1884, Fourth quarter 2015.
29. 1& 1Tutorials, 1vol. 116, 1no. 12, 1pp. 1729-744, 1Second 1quarter 12014.
30. A. 1Ahmad, 1S. 1Ahmad, 1M. 1H. 1Rehmani, 1and 1N. 1Ul 1Hassan, 1"A 1Survey 1on 1Radio 1Resource 1Allocation 1in 1Cognitive 1Radio 1Sensor 1Networks," 1IEEE 1Communications 1Surveys 1& 1Tutorials, 1vol. 117, 1no. 12, 1pp. 1888-917, 1Second 1quarter 12015.
31. S. 1K. 1Sharma, 1T. 1E. 1Bogale, 1S. 1Chatzinotas, 1B. 1Ottersten, 1L. 1B. 1Le 1and 1X. 1Wang, 1"Cognitive 1Radio 1Techniques 1Under 1Practical 1Imperfections: 1A 1Survey," 1in 1IEEE 1Communications 1Surveys 1& 1Tutorials, 1vol. 117, 1no. 14, 1pp. 11858-1884, 1Fourth 1quarter 12015.

AUTHORS PROFILE

.

Anand A Khatri, Research Scholar, Dept of CSE, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India. He is the Life member of professional body of ISTE. His area of interests is in Cognitive Radio Network, Network Security, Wireless Networks, Network Security and Internet of things (IOT)

Dr. Yogesh Kumar Sharma, He is working as Head of Dept & Associate Professor in Computer Science at Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan, India. He is the dealing with R& D wing of JJT University and professional memberships of IAENG, IEEE. His area of interests is Wireless Networks,Cognitive Radio Network, Information Security & Cloud Computing

Dr. Satish Todmal, He is Dean Academics & Associate Professor in Computer Engineering, JSPM's Imperial College of Engineering and Research, Pune, Maharashtra India. . He is the Life member of professional body of ISTE, IACSIT. His area of interest is in Image Processing, Wireless Network, Network Security & Cognitive Area Network