International Journal of Engineering & Technology, 7 (1.9) (2018) 229-233

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Spectrum-aware shared protection (SASP) algorithm for cognitive radio networks

Mr. S. Esakki Rajavel [1] *, Dr. T. Aruna [2], Mr. S. Allwin Devaraj [3]

[1] *Assistant Professor, Department of ECE, Francis Xavier Engineering College, Tirunelveli*
[2] *Assistant Professor, Department of ECE, Thiagarajar College of Engineering, Madurai*
[3] *Assistant Professor, Department of ECE, Francis Xavier Engineering College, Tirunelveli*

Abstract

Cognitive radio (CR) has become a key technology for addressing spectrum scarcity. In CR networks, spectrum access should not interfere the incumbent networks. Due to the requirement above, common control channel approaches, which are widely used in traditional multi-channel environments, may face serious CR long-time blocking problem and control channel saturation problem. Although channel-hopping-based approaches can avoid these two problems, existing works still have significant drawbacks including long time-to-rendezvous, unbalance channel loading, and low channel utilization. This paper tends to the issue of range mindful survivable methodologies with disappointment likelihood limitations under static activity in adaptable transfer speed optical systems. The joint disappointment likelihood amongst essential and reinforcement ways must be beneath the most extreme fair joint disappointment likelihood for each activity request. It creates whole number direct program (ILP) models for committed way security and shared-way assurance with a specific end goal to limit the aggregate number of recurrence spaces expended, and furthermore propose a range mindful devoted insurance (SADP) calculation and a range mindful shared security (SASP) calculation. This demonstrates the ILP show arrangements devour least number of recurrence spaces, however prompt higher normal joint disappointment likelihood contrasted with the SADP and SASP calculations. In addition, both the SADP and SASP calculations accomplish a superior execution as far as aggregate number of recurrence openings expended when contrasted with a customary devoted way insurance calculation and an ordinary shared-way assurance calculation, separately, however prompt higher normal joint disappointment likelihood.

Keywords: *Cognitive Radio; Spectrum-Aware Dedicated Protection (SADP); Frequency Slots and Shared-Path Protection Algorithm.*

1. Introduction

Inside the present range administrative structure, the majority of the recurrence groups are solely assigned to particular administrations, and infringement from unlicensed clients isn't permitted.The Federal Communications Commission (FCC) has indicated that the percentage of the assigned spectrum that is occupied only from 15 to 85 percent, varying widely in time and places. To address the critical problem of spectrum scarcity, the FCC has recently approved the use of unlicensed devices in licensed bands [1]. This new field of research foresees the development of cognitive radio networks (CRNs) to further improve the spectrum efficiency. nhancing the data transfer capacity effectiveness and diminishing the potential disappointment likelihood in adaptable transmission capacity optical systems are ending up progressively essential. Specifically, optical system survivability assumes a critical part in guaranteeing movement nature of administration. One approach for giving survivability is through insurance systems in which reinforcement assets are saved at the season of an association's foundation so as to ensure against failures [2].

Assurance systems can be delegated either devoted or shared insurance plans. Devoted assurance allots committed reinforcement assets to each activity request and is a viable system for giving quick recuperation disappointment movement. Shared insurance permits numerous working movement requests to share reinforcement assets as long as the essential ways don't bomb all the while. Shared insurance accomplishes preferable productivity of system assets over devoted protection [3].

When all is said in done, while security plans are successful in giving survivability against single-interface disappointment, they are less compelling in giving full survivability against numerous disappointments, especially if assets on both the working way and reinforcement way of an association flop at the same time. For this situation, another metric of intrigue is the joint disappointment likelihood of an association, which is the likelihood that both the working way and reinforcement way of an association come up short simultaneously [4]. This likelihood can be ascertained in view of the disappointment probabilities of individual fiber interfaces in the system and the courses taken by the essential and reinforcement ways. Every association may have a specific resilience to disappointment communicated as a most extreme decent joint disappointment likelihood (MJFP) limit, and this edge must be fulfilled while building up the essential and reinforcement paths.

Another essential issue in adaptable data transfer capacity optical systems is range proficiency. While provisioning assets for associations, it is frequently gainful to limit the measure of range assets devoured by the association. Limiting range utilization can lessen arrange costs and may enable the system to suit more movement. It address the issue of provisioning working and reinforcement assets for a static arrangement of association asks for in an adaptable data transfer capacity optical system with the objective of fulfilling the joint disappointment likelihood necessity of each demand while likewise endeavoring to limit range assets utilization. Specifically,

we center around assessing the exchange off between the joint disappointment likelihood accomplished and the measure of range assets devoured by the provisioning techniques.
Subjective Radio Sensor Networks furnishes remote sensor systems with the capacities of psychological radio and dynamic range administration. When all is said in done, a CRSN can be characterized as a circulated system of remote psychological radio sensor hubs, which sense an occasion flag and cooperatively impart their readings powerfully finished accessible range groups in a multi-bounce way eventually to fulfill the application-particular prerequisites. Range administration is the way toward managing the utilization of radio frequencies to advance proficient utilize and pick up a net social advantage. The term radio range commonly alludes to the full recurrence run from 3 kHz to 300 GHz that might be utilized for remote correspondence. Expanding interest for administrations, for example, cell phones and numerous others has required changes in the logic of range administration. Interest for remote broadband has taken off because of mechanical development, for example, 3G and 4G versatile administrations, and the quick extension of remote web administrations. Since the 1930s, range was alloted through authoritative permitting. Constrained by innovation, flag impedance was once considered as a noteworthy issue of range use[7].

2. Proposed system

2.1. Network survivability

Diverse insurance techniques may should be considered in adaptable data transmission optical systems all together both to ensure dependable nature of administration and to give distinctive administration levels. This paper thinks about both devoted way assurance and shared-way security in adaptable transfer speed optical systems, which are more unpredictable than in conventional WDM systems, since a solitary wavelength designation is changed to the task of a few adjacent recurrence openings in the recurrence area. Committed insurance and shared assurance have been generally contemplated in both WDM and adaptable data transfer capacity optical systems. For committed assurance, Search calculation and an ILP demonstrate were proposed to address a disconnected issue of steering and range assignment with devoted way insurance in flexible optical systems. Survivable hindrance mindful movement prepping and regenerator arrangement issue was tended to by considering the association level assurance under a devoted security conspire. Besides, an effective survivable adaptable optical WDM organize plan calculation was proposed in which gave a committed insurance plan to each activity request. To enhance benefit recuperation without trading off asset proficiency, a novel way match security technique was proposed to mutually join activity building and hazard minimization worries for multi-disappointment organize situations.
This technique apply an autonomous disappointment likelihood model to build up a joint disappointment likelihood demonstrate, in which it distinguish the connection between add up to number of recurrence spaces expended and the normal joint disappointment likelihood. Likewise, these plans address the issue of range mindful survivable systems with disappointment likelihood limitation under static movement in adaptable transfer speed optical systems.
This plan additionally propose a heuristic calculation called range mindful shared assurance (SASP) calculation with disappointment likelihood, to productively accomplish the objective of provisioning assets in sensible time for some, activity requests in an extensive scale organize. The SASP calculation appeared to accomplish a decent execution as far as the aggregate number of recurrence openings expended and the normal joint disappointment likelihood.
This plan characterize the adaptable data transmission optical system as a chart G(V, E, F), where V means the arrangement of hubs that are furnished with transfer speed variable optical cross-interfaces work, E is the arrangement of fiber connections, and F = {f1, f2, f3, . . . , fn} is the arrangement of accessible recurrence openings on each connection. |V|, |E|, and |F| speak to the quantity of hubs, the quantity of the connections, and the quantity of the recurrence openings, individually. A connection in E is meant as (l, k) for l, k V, which implies that the connection associates hub l to hub k. Each activity request comprises of a source hub, a goal hub, a transmission capacity necessity, and a satisfactory disappointment likelihood. In this manner, a movement request is signified as takes after:

TD(s, d, FS, MJFP) (1)

Where s and d are the source hub and goal hub, MJFP is the greatest bearable joint disappointment likelihood, and FS is the data transmission prerequisite in units of recurrence spaces. Watch groups are provisioned between various associations on a similar fiber interface keeping in mind the end goal to decrease obstruction between nearby associations, which are expected to have a width of GB recurrence spaces.
This characterize the issue as takes after: Given the system chart G(V, E, F), an arrangement of requests TD (s, d, FS, MJFP), the quantity of recurrence openings on each connection, the most extreme shared degree (MSD) of range on each connection, and the disappointment likelihood of each connection, the issue is to arrangement working and reinforcement assets for each request while fulfilling the MJFP for each activity request. For each TD(s, d, FS, MJFP), the monitor groups should be added to data transfer capacity prerequisite of the demand. In the meantime, the apportioned range assets need to fulfill both the range progression imperative and range sequence in the recurrence area on a connection.
The goal is to limit the range utilization for devoted way assurance and shared-way security in adaptable data transmission optical systems.
To accomplish this goal, this creates two ILP models and two heuristic calculations that address the issue while limiting the aggregate number of recurrence openings overwhelmed by devoted way security and shared-way insurance.

2.1.1. Joint failure probability of shared path protection

Keeping in mind the end goal to additionally enhance arrange asset usage, this strategy use the mutual reinforcement way as long as the joint disappointment likelihood fulfills the MJFP of the essential way and the common reinforcement way. In this work, we expect that disappointment occasions of various essential ways that offer a similar reinforcement assets are commonly autonomous occasions without connected connection disappointments. For this situation, if numerous essential ways that offer a similar reinforcement assets bomb all the while, at that point just a single of the essential ways can be reestablished. This strategy views that the working way as reestablished is chosen arbitrarily and consistently from the arrangement of all fizzled essential ways that offer a similar reinforcement asset. The reinforcement assets don't influence the disappointment likelihood of the essential way; consequently, we can acquire the disappointment likelihood of essential way x utilizing Equation (2).

$$F(x) = 1 - \prod_{(k,l)\in x} (1 - p_{k,l}) \quad (2)$$

In any case, because of asset sharing on the reinforcement way, just a single of the working associations that offer a similar reinforcement recurrence opening can be effectively changed to the common reinforcement way when more than one of these working associations flops at the same time. With a specific end goal to lessen the opposition for reinforcement assets, the quantity of associations that can have a similar reinforcement range assets is limited, consequently diminishing the movement misfortune after numerous connection disappointments happen. This technique characterize the term shared level of a recurrence opening, which signifies the quantity of working associations that are sharing the recurrence space, and characterize the parameter MSD of reinforcement range assets. This signifies the greatest number of associations that can have a similar reinforcement recurrence opening. The joint disappointment

likelihood between essential way x and reinforcement way y is gotten by the item F(x, y) = F(x) × F(y), since the disappointment of a working way and the disappointment of a reinforcement way are commonly free disappointment occasion. This strategy utilizes the detailing to figure the joint disappointment likelihood of shared-way assurance amongst x and y:

$$F(x,y) = \left[1 - \prod_{(k,l)\in x}\left(1-p_{k,l}\right)\right] \times \left[1 - \prod_{(m,n)\in y}\left(1-p_{m,n}\right)\frac{1}{MSD_{m,n}}\right] \quad (3)$$

Where pk,l , (k, l) ∈ x and pm,n, (m, n) ∈ y are the connection disappointment probabilities, and MSDm,n is the greatest shared degree on a connection (m, n) ∈y. Along these lines, the MJFP limitation of shared-way assurance is modified as takes after:

$$\left[1 - \prod_{(k,l)\in x}(1 - p_{k,l})\right] \times$$

$$\left[1 - \prod_{(m,n)\in y}(1-p_{m,n})\frac{1}{MSD_{m,n}}\right] \le F(s,d) \quad (4)$$

2.2. ILP model of shared-path protection

Keeping in mind the end goal to enhance the range usage, this technique can use shared-way assurance as long as the joint disappointment likelihood between every essential way and its common reinforcement way fulfills the MJFP necessity. Be that as it may, since the articulation in (4) for MJFP is non-straight, it can't be straightforwardly utilized as a part of an ILP show. Additionally, this strategy can't utilize an indistinguishable technique from the committed way assurance to detail a straight articulation by extending (4) with the second request term, since joint disappointment likelihood of shared security is as yet a non-direct condition by the estimate approach regardless of whether we keep the second high-arrange terms in Equation (4). With a specific end goal to take care of this issue, one conceivable approach is to figure K competitor way combines and their JFPs ahead of time by utilizing Equation (3) for each activity request from source hub s to goal hub d, where a way match incorporates one essential way and one reinforcement way. The ILP at that point chooses one of the K way matches for each activity request with the end goal that the aggregate number of recurrence openings is limited. To start with, let Rs,d be an arrangement of K applicant way combines for a movement request from source hub s to goal hub d, where $R^{s,d} = \{R_1^{s,d}, R_2^{s,d}, \ldots, R_k^{s,d}\}$. Both the pth primary path $R_p'^{s,d}$ and the pth backup path $R_p'^{s,d}$ are included in the pth path-pair $R_p^{s,d}$ for each traffic.

The joint disappointment probabilities JFPs,d of the K applicant way combines in Rs,d are figured ahead of time utilizing Equation (3), i.e., $JFP^{s,d} = \{JFP_1^{s,d}, JFP_2^{s,d}, \ldots, JFP_k^{s,d}\}$, where $JSP_p^{s,d}$ means the joint disappointment likelihood of the pth way match contender for an activity request from source hub s to goal hub d. For comfort, the documentation is compressed as takes after.

2.2.1. Input parameters

GB,θ, ns,d,D, |E|,|F|, pk,l , and F (s, d) these are characterized as in the ILP display for devoted way assurance MSDl the MSD on a connection l; K add up to number of way matches for each movement request from source hub s to goal hub d; Rs,d an arrangement of K hopeful way combines for an activity request from source hub s to goal hub d, $R^{s,d} = \{R_1^{s,d}, R_2^{s,d}, , R_k^{s,d}\}$. $JFP^{s,d}$ the joint disappointment probabilities of the K hopeful pathpairs for an activity request from source hub s to goal hub $JFP^{s,d} = \{JFP_1^{s,d}, JFP_2^{s,d}, . , JFP_k^{s,d}\}$

2.2.2. Variables

f the list of recurrence spaces,, f{1, 2, . . . , |F|}; l the record of a connection l in a system G, l{1, 2, . . . , |E|}; p: the list of a way combine that incorporates essential way and reinforcement way, wherep{1, 2, . . .,K} means the pth way match in the arrangement of way combines; φl add up to number of recurrence openings utilized by essential ways on connect l for all the activity requests; ϕl add up to number of recurrence spaces utilized by reinforcement ways on interface l for all the movement requests; $x_p^{s,d}$ parallel variable takes estimation of 1 if the pth way combine from the K applicant way matches is chosen as the essential way and reinforcement way of a movement request from source hub s to goal hub d;$u_{p,l}^{s,d,f}$ paired variable that takes estimation of 1 if interface l on the pth essential way $R_p'^{s,d}$ utilizes recurrence opening f for an activity request from source hub s to goal hub d and takes estimation of 0 generally; $v_{p,l}^{s,d,f}$ double factor that takes estimation of 1 if connect l on the pth reinforcement way $R_p'^{s,d}$ utilizes recurrence opening f for an activity request from source hub s to goal hub d and takes estimation of 0 generally; σ_l^f l paired variable that takes estimation of 1 if connect l utilizes recurrence space f as shared recurrence opening for some activity requests and takes estimation of 0. Generally the ILP show for shared-way assurance is numerically figured as takes after: Minimize the aggregate number of recurrence openings utilized:

$$\text{Minimize } \sum_{l\in|E|}(\varphi_l+\phi_l) \quad (5)$$

The aggregate number of the utilized recurrence spaces crossing the connection l along essential way is processed as takes after:

$$\varphi_l = \sum_{(s,d)\in D}\sum_{p\in k}\sum_{f\in|F|} u_{p,l}^{s,d,f} \ \forall l \quad (6)$$

The aggregate number of the utilized recurrence openings navigating the connection l along shared-reinforcement way is composed as takes after:

$$\phi_l = \sum_{f\in|F|}\sigma_l^f\phi l \quad (7)$$

2.3. Shared protection algorithm with failure probability

So as to additionally enhance range use, we build up a SASP calculation with disappointment likelihood. The calculation figures two connection disjoint ways that fulfill MJFP prerequisite for each activity request from source hub s to goal hub d. With a specific end goal to lessen the opposition for shared reinforcement resources,we force a MSD imperative on every recurrence opening. For each movement request, the K-SP calculation is run twice to discover K sets of ways from source hub s to goal hub d that consent to the adequate MJFP. The way with the base number of bounces is chosen as the essential way. For the reinforcement way, the effectiveness of reinforcement range asset sharing is essentially influenced by the range task. Subsequently how to pick a common reinforcement way and distribute range assets turns into a key undertaking in limiting the range utilization. Accordingly, we utilize an indistinguishable approach from to look and select an accessible range obstruct as the reinforcement range assets. The documentation is characterized as takes after: e file of range square,e ∈ {1, 2, . . . , |F| − FS}; k file of K hopeful reinforcement ways; FSk,e add up to number of free recurrence spaces for the eth range obstruct on the kth reinforcement way, if this range piece is accessible. Else, it is equivalent to 0; $N_{k,f}$ add up to number of the free recurrence openings for the fth recurrence space on kth reinforcement way, if the fth recurrence opening is accessible. Else, it is equivalent to 0.

Here, we look through the accessible range openings by choosing the base free range square utilization, which is the Equation as the mutual reinforcement range assets in reinforcement way

$$\text{Min}\{FS_{k,i} = \sum_{f\in(e,e+FS)} N_{k,f}\} \ \forall e,k \in K \quad (8)$$

In this manner, we should check all the range obstructs amo $FS_{1,1}$, $FS_{1,2}$, . . . , $FS_{K,|F|-FS}$, and after that select the jth range hinder on the ith hopeful reinforcement way with the base esteem, $FS_{i,j} \in \{FS_{1,1}, FS_{1,2}, \ldots, FS_{K,|F|-FS}\}$, as the reinforcement range assets.

Condition (8) can be utilized to choose the way with the base free range square utilization is utilized as the reinforcement way, and furthermore recognizes the range piece to be utilized for the mutual reinforcement range assets. From Equation (8), energizes the essential way and the reinforcement way to expend the base measure of range assets while designating the recurrence openings

3. Result and discussion

To verify our analytical model and validate the performance improvement of the proposed cognitive radio networks, we use simulation experiments based on NS-2 to evaluate the throughput performance

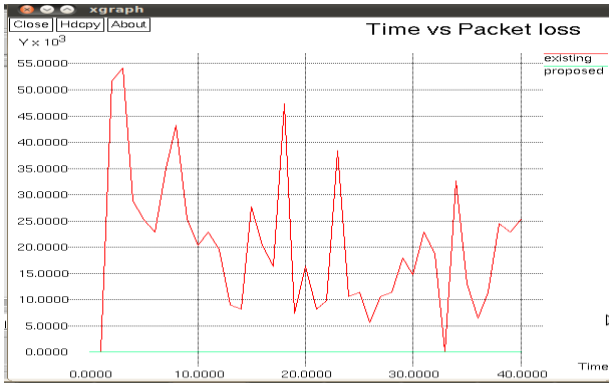

Fig. 3.1: Comparison Between Time and the Packet Loss.

Fig.3.1 shows the graph between time and packet loss.Using the shared path protection algorithm the data and control message are tranmitted without any packet loss and interference.But in the existing method while exchanging the control message information the interference and the packet loss occurs heavily.

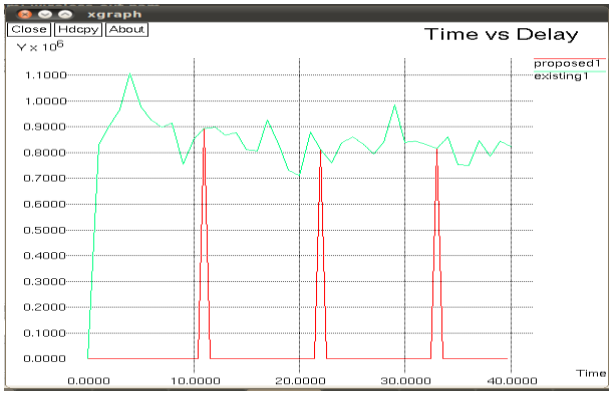

Fig. 3.2: Comparison Between Time and the Delay.

Fig 3.2 shows that the graph between the delay and time.In the existing channel hopping approaches bandwith utilization and the data is transmitted with longer delay period .In the proposed method using shared path protection algorithm the data and control exchange information is transmitted with less delay and the bandwith is utilized properly in a sequential manner.

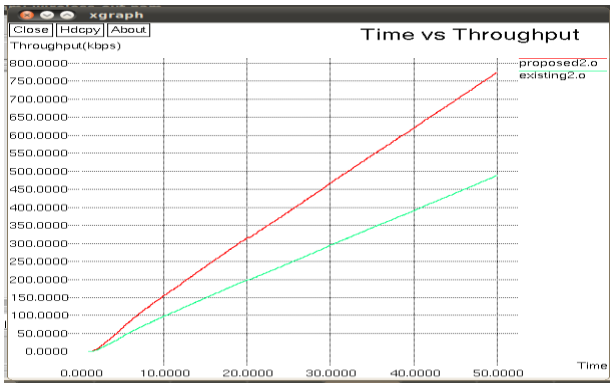

Fig. 3.3: Comparison Between Time and the Throughput.

Fig.3.3. shows the graph between time and throughput.Throughput is the rate at which the data is transmitted successfully without any loss.Using shared path protection algorithm throughput is achieved within a given time.

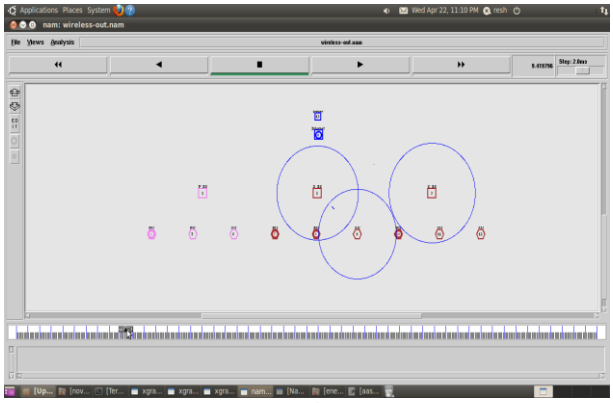

Fig. 3.4: Location of Secondary Users.

Fig.3.4 shows the location of secondary users .The node can be created with its node type, size and properties. Created node can be located in the network. Data is transmitted from the server to internet.Then the data from internet is transmitted to base station and the data from base station is transmitted to primary and secondary users.Data is transmitted without any packet loss and interference.

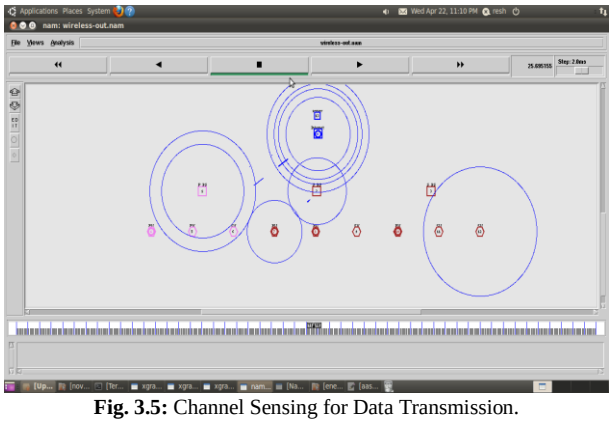

Fig. 3.5: Channel Sensing for Data Transmission.

Fig.3.5. Channel sensing for data transmission this each secondary users hops with the neighbouring nodes and senses the available channel to send the control message exchange information

4. Conclusion

This paper watched out for the issue of range careful survivable strategies with disillusionment probability goals under static movement in versatile transmission limit optical frameworks. In particular, joint dissatisfaction probabilities were analyzed for both the

conferred way protection and the common path affirmation under low association frustration probabilities. Our goal was to limit range asset utilization under static activity requests in both little and expansive systems while additionally fulfilling the MJFP prerequisite for each movement request. To productively manage the connection between add up to number of recurrence spaces devoured and normal joint disappointment likelihood, we created ILP models for devoted way security and shared-way insurance. In the meantime, both range mindful devoted way assurance and shared-way insurance calculations were proposed to deal with an extensive number of movement requests under the static situations in huge systems.
Contrasted and the SADP and SASP calculations in a little system, recreation comes about demonstrate that ILP models of committed way assurance and shared-way insurance limit the aggregate number of recurrence spaces devoured, yet in addition prompt higher normal joint disappointment likelihood. We approved that our proposed SADP and SASP calculations bit by bit approach the ideal ILP arrangements as K increments. Of course, in an extensive system, recreation comes about demonstrated that the SADP and SASP calculations accomplished better execution regarding both aggregate number of recurrence spaces devoured and normal number of bounces than CDPP and CSPP calculations, separately. Be that as it may, SADP and SASP result in bigger normal joint disappointment likelihood than the ordinary devoted way and shared-way assurance approaches.

References

[1] I.F. Akyildiz, W.-Y. Lee, M.C. Vuran, and S. Mohanty, “Next Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey,” Computer Networks J., vol. 50, no. 13, pp. 2127-2159, 2006. https://doi.org/10.1016/j.comnet.2006.05.001.

[2] P. Bahl, R. Chandra, and J. Dunagan, “SSCH: Slotted Seeded Channel Hopping for Capacity Improvement in IEEE 802.11 Ad Hoc Wireless Networks,” Proc. ACM MobiCom, pp. 216-230, 2004. https://doi.org/10.1145/1023720.1023742.

[3] K. Bian and J.-M Park, “Maximizing Rendezvous Diversity in Rendezvous Protocols for Decentralized Cognitive Radio Networks,” IEEE Trans. Mobile Computing, vol. 12, no. 7, pp. 1294-1307, July 2013. https://doi.org/10.1109/TMC.2012.103.

[4] H. Kim and K.G. Shin, “Efficient Discovery of Spectrum Opportunities with MAC-Layer Sensing in Cognitive Radio Networks,” IEEE Trans. Mobile Computing, vol. 7, no. 5, pp. 533-545, May 2008. https://doi.org/10.1109/TMC.2007.70751.

[5] Christo Ananth, Dr.S. Selvakani, K. Vasumathi, “An Efficient Privacy Preservation in Vehicular Communications Using EC-Based Chameleon Hashing”, Journal of Advanced Research in Dynamical and Control Systems, 15-Special Issue, December 2017,pp: 787-792..

[6] B.F. Lo, I.F. Akyildiz, and A.M. Al-Dhelaan, “Efficient Recovery Control Channel Design in Cognitive Radio Ad Hoc Networks,” IEEE Trans. Vehicular Technology, vol. 59, no. 9, pp. 4513-4526, Nov.2010. https://doi.org/10.1109/TVT.2010.2073725.

[7] H.A.B. Salameh, M.M. Krunz, and O. Younis, “MAC Protocol for Opportunistic Cognitive Radio Networks with Soft Guarantees,” IEEE Trans. Mobile Computing, vol. 8, no. 10, pp. 1339-1352, Oct.2009. https://doi.org/10.1109/TMC.2009.19.

[8] Y. Shi, Y.T. Hou, H. Zhou, and S.F. Midkiff, “Distributed Cross-Layer Optimization for Cognitive Radio Networks,” IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4058-4069, Oct. 2010. https://doi.org/10.1109/TVT.2010.2058875.

[9] J. Tang, R. Hincapie, G. Xue, W. Zhang, and R. Bustamante, “Fair Bandwidth Allocation in Wireless Mesh Networks with Cognitive Radios,” IEEE Trans. Vehicular Technology, vol. 59, no. 3, pp. 1487-1496, Mar. 2010 https://doi.org/10.1109/TVT.2009.2038478.

[10] N.C. Theis, R.W. Thomas, and L.A. DaSilva, “Rendezvous for Cognitive Radios,” IEEE Trans. Mobile Computing, vol. 10, no. 2, pp. 216-227, Feb. 2010. https://doi.org/10.1109/TMC.2010.60.