IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007112|

Energy Efficient Spider Monkey Optimization Routing Protocol for Ingenious Data Transmission

M.S. Sharmila[1], Mr.J.Tamilselvan[2], M.Sc.,M.Phil, M.C.A.,M.E.,(Ph.D)

Research Scholar, Department of Computer Science(PG), K.S.Rangasamy College of Arts and Science (Autonomous)Tiruchengode, TamilNadu, India[1]

Assistant Professor, Department of Computer Science(UG), K.S.Rangasamy College of Arts and Science (Autonomous)Tiruchengode, TamilNadu, India[2]

ABSTRACT: Privacy-preserving routing protocols in distant associations regularly use additional phony traffic to discharge the source-target uniqueness of the granting pair. Typically, the development of fake traffic is done heuristically with no guarantees that the transmission charge, dormancy, etc, are worked on in every association topography. In this paper, we unmistakably check the insurance utility trade off issue for distant associations and expand a novel security protecting coordinating estimation called Optimal Privacy Enhancing Routing Algorithm (OPERA). Show uses a numerical unique packaging to propel the security of the coordinating show set an assistance (or cost) power. We consider overall adversary with both lossless and lossy clarification that use the Bayesian Maximum-A-Posteriori (MAP) deducing approach. We set up the Privacy-Utility "Compromise" Problem as an immediate program which can be capably settled. Our augmentation result display that OPERA decline the adversary's acknowledgment probability by up to half diverged from the sporadic Uniform and Greedy heuristics, and up to numerous occasions appeared differently in relation to an example plot. Moreover, OPERA similarly out plays out the ordinary information speculative typical all together strategy.

KEYWORDS: Cognitive radio networks, routing optimality-scalability tradeoff, Routing Protocol.

I. INTRODUCTION

Cognitive Radio Networks (CRNs) present a promising response for range lack in distant associations to adjust to the continually growing interest for higher information move limit in flexible trades. In CRNs, unlicensed Secondary Users (SUs) cunningly utilize void pieces of the reach without intruding with approved Primary Users (PUs). This ensures a tremendous course of action of anticipated applications, given the lack of the unlicensed far off range, including dispersed versatile applications for notoriety and astoundingly stuffed circumstances like the Internet of Things, prevalent grade an earlier variation of this paper displayed in the strategies of IEEE Global Communications Conference (GLOBECOM) 2015. Adaptable video, and disaster or emergency response settings. One outline of these applications is the new Spectrum Collaboration Challenge (SC2) proposed by DARPA in 2016 In this test, "competitors will reimaging another, more useful far off perspective wherein radio associations self-governingly collaborate to effectively choose how the reach should be used second to second". Disregarding this assurance, one of the key issues that influence the show of multi-bounce CRNs is coordinating. Stood out from standard uniquely designated associations, guiding in CRNs needs to deal with the exceptional challenges of dynamic reach openness (on account of the stochastic lead of fundamental and helper customers), resource heterogeneity (coming about in view of the availability of different channels and radios on a comparative center point), and synchronization between centers on different channels, among others. In this manner, we present the Optimal Privacy Enhancing Routing Algorithm (OPERA) which uses a quantifiable powerful framework to depict assorted association circumstances and select the best way scattering that tracks down some sort of concordance between the insurance and utility (e.g., to the extent transmission cost) of the guiding show given some security monetary arrangement (e.g., transmission cost necessity). Extra deceptive traffic may in like manner be used to loosen up the guiding method to fuse additional recipient (centers that got the phony traffic). The quantifiable powerful design approach widens our past work in where a heuristic probabilistic coordinating computation was proposed to update the security for the goal center point. In this work, we

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007112|

consider a to some degree more grounded adversary that uses the Bayesian MAP appraisal system and besides consider the circumstance where the foe has lossy insights. We detail the assurance of the best "security shielding ways for each source-target pair using a quantifiable unique design that results in a straight program" which is easily handled by various business solvers.

II. RELATED WORK

In traditional wired associations, the tradeoff issue among worldwide and neighborhood directing is thought broadly. For example, in the degree of the Internet, the possibility of Autonomous Systems (Intra and Inter AS coordinating) is used to achieve this tradeoff. Also, the tradeoff between course optimality and flexibility has been in like manner concentrated concerning distant associations. In any case, the onion coordinating technique is more normal in light of its lower latency which makes it sober minded. Fortunately, the close by obviousness assumption that is genuine in the colossal extension Internet. Strangely, the decently more unobtrusive distant associations are all the more unprotected against traffic examination from an overall adversary. Moreover, due to the distant transmission medium, it is useful for an adversary to inactively tune in on all transmissions from a far off center without being perceived.

III. METHODOLOGY

3.1 OPTIMAL DETECTION OF SOURCE-DESTINATION PAIR w: Expect that the veritable source-target pair is w and the foe sees y. A viable recognizable proof happens when the enemy's check of the source-target pair BW(y) matches w. Lossy Adversarial Observations we deal with Problem to get the best P perceive values for the proposed OPERA. Shows the P perceive values for OPERA and the gauge strategy in Section IV-C4 for a line network with the cancellation probabilities _ = 0:1 and _ = 0:5. Generally, P perceive lessens as additions since the undetected transmissions may have a spot with a greater course of action of possible source centers. Moreover, a greater n regard is relied upon to all the more promptly induced P recognize for greater characteristics. There exists an opposite association between the value of n and the unpredictability of the smoothing out issue in and higher n achieves a more precise measure of the authentic P perceive to the burden of extra computational costs. More execution defilement is educated about the grid network stood out from the line network as the amount of possible w pair's augmentations when less transmission is taken note. Unusually, the high level ways from the assessment method concur with the best methods of the principal system in our entertainment, the adversary's acknowledgment rate doesn't chip away at whether or not he uses while the structure uses the theory strategy.

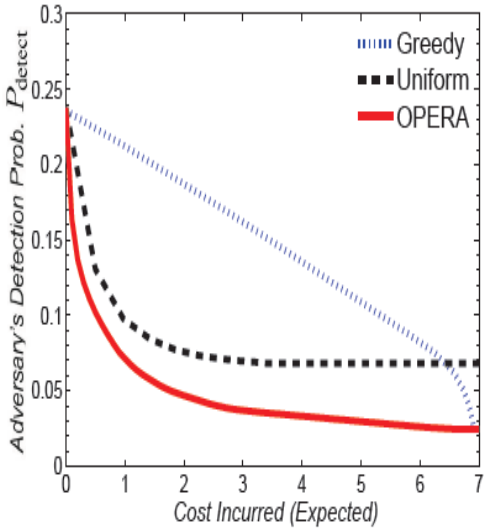

Figure 3.1: Optimal Detection of Source-Destination Pair

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007112|

3.2 LIMITATIONS OF CURRENT HEURISTIC ALGORITHMS:

It is evident that the security further developing plans don't come in vain and there exists a trade off between the assurance and transmission overheads caused. Though the above plans have dominatingly relied upon extra false traffic (or/and delays) to soothe traffic assessment attempts, there is no exhaustive estimation of the adversary's area probability, their ideal attacking method, and the overheads achieved by the arrangement. Hereafter, it is interesting to quantify the inadequacy of utility (or cost) brought about by the security defending arrangement and check it against the additional proportion of assurance gave. System Model In this fragment, we present our structure assumptions and a while later give a short blueprint of the proposed disclosure scheme. We consider the circumstance where a source center u requirements to send packages to a lone target center v in a static distant association. Structure Assumptions We consider an extraordinarily delegated scholarly radio association where PUs hold the choice to use the approved reach while SUs can get to simply the vacant portions of the reach become dynamic onion directing method The self-sufficient striking appointments with birth limit and downfall limit depending upon the traffic of the PUs. These limits can be evaluated using separated experiences, close by distinguishing information, or through certain contribution to full duplex exchanges. The homogeneous to the extent their limits and transmission ranges. We acknowledge that SUs and PUs channels follow the unit circle model. This is ordinary in various CRN circumstances, for instance, TV clear region based CRNs. We also don't make a specific speculation on the MAC or higher layer shows for the PUs' structure. We further expect that SUs are discovered reliably in the two-dimensional Cartesian space and each SU knows its own region and the space of its nearby neighbors. A center point can evaluate its region using any of the current limit systems, including GPS or convenient based structures. Furthermore, a sender can gain the region information of an authoritative target through out of band benefits that map center point areas to regions, or have it scattered through the association. Tolerating knowing simply the space of the goal is a typical and authentic assumption in various applications including military and sensor networks where specifying centers know the spaces of the sink centers. Despite the way that having the spaces of all centers of the association may incite better and more lively courses, we don't acknowledge having center points' regions except for the sink and the abutting centers; we acknowledge that spreading the center points' regions information to the whole association and keeping awake with the most recent requires a gigantic overhead, which ruins our system execution. Without loss of misrepresentation, exchanging directing control groups ought to be conceivable through a Common Control Channel (CCC). Additionally, our model doesn't expect a specific repeat band.

3.3PRIVACY-PRESERVING ROUTING In this part, we present the proposed security saving strategies for guaranteeing the region information of noticed articles and data sinks. We expect that all exchanges between sensor centers in the association are mixed so the substance of groups appear to be sporadic to the overall sneak. Source-Location Privacy Techniques In this part, we present two strategies to give region insurance to noticed things in sensor associations, incidental arrangement and source reenactment. An intermittent collection procedure achieves the best insurance yet should be applied to applications that accumulate data at a low rate and don't have demanding necessities on the data transport lethargy. The source proliferation procedure offers rational trade offs between insurance, correspondence overhead, and inactivity. Sink Simulation Similar to source reenactment, an instinctual answer for sink region security is dumbfound the foe by making virtual sinks. Therefore, we propose to make distinctive candidate follows toward the fake sinks in the association to disguise the traffic between certified articles and veritable sink Protocol depiction.

IV. PRIVACY PROTECTION

4.1 PRIVACY PROTECTION OBSERVATION: As the adversary has overall detectable quality, he is possibly prepared to see all center transmissions from the entire association. Nevertheless, we consider the going with two insight models for the foe.

4.2 LOSSY OBSERVATIONS:

Taking everything into account, the foe may have lossy observations because of the lossy thought about the distant channel or some powerless sides in his affiliation. In sink reenactment, counterfeit sinks will be imitated in the field. Every one of them will get traffic like the traffic got by a genuine sink. To accomplish this, we see no qualification among phony and authentic sinks when sensors send bundles. During affiliation, we place affirmed sinks and select areas where phony sinks are to be copied. A subset of the sensors will be utilized as phony sinks. It is in like way necessitated that each genuine sink have a phony sink imitated in its correspondence range. We will basically send messages to the phony sinks and have all phony sinks play out a one-ricochet broadcast of the message, guaranteeing

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007112|

full front of the genuine sink districts. Construction and danger models this paper contemplates a WSN with a solitary BS place point. BS goes most likely as the sink of the gathered sensor information, i.e., the BS is a convincing end-point of all the correspondence in the affiliation. Continuously end, the BS is an in situ client of the affiliation. We consider a homogenous affiliation where all sensor place focuses have comparative assets like beginning energy, interface cutoff and correspondence range. While a sensor has restricted presented energy supply and is simply prepared to do short take transmission, the BS isn't as obliged in its energy, correspondence and assessment limits. The BS in like way can move starting with one district then onto the accompanying inside the WSN area. For instance, the BS can be a PC mounted on a vehicle that can go inside the sending region. Strength of Privacy Protection to assess the strength of locale security insistence, we utilize two models: the guaranteed time of the recipient and the assault time of the enemy. The beneficiary's gotten time is surveyed as the measure of packs passed on before the authority is gotten. The foe's assault time is evaluated as the measure of moving strides (from one sensor locale to a neighbor) the foe needs to make before he appears at the beneficiary. We play out the entertainments on a sensor relationship of 900 focus focuses, among which 100 erratically picked ones are source focus focuses that intermittently make information packs for the finder. The source period is depicted as the time between two groups produced using a source community point. The concealed division from the adversary to the finder is 15 skips. The enemy has the properties depicted in Section III-B. In his assault strategy, the adversary stays in a lone situation to get bundles, and move to the going with locale dependent upon the method portrayed. In the event that no pack is gotten for scope of 100 source periods, the enemy backtracks to his past area. The enemy surveys 5 stages in his moving history. After his course of action of experiences record is depleted, he strolls discretionarily until getting a bundle. We put forward a course of events for our redirection, which is the most obvious opportunity for 500,000 gatherings to be passed on. The program closes if the adversary can't get the recipient in very far. That we generally speaking know from our 1-ricochet neighbors. Considering impedance, a middle point apparently won't recall of some 1-weave neighbors. Foe Model We consider an outer, dormant, worldwide and taught foe who sees a (possibly lossy) social event of transmissions y from a true transmission way x. Utilizing a Bayesian traffic appraisal methodology, the enemy intends to see the personality of the source-target pair w for every acumen y, i.e., he desires to perceive which focus is talking with which focus ward on his possibly inadequate experiences.

4.3 LOSSLESS OBSERVATIONS:

The lossless insights model is a remarkable case wherein the foe faultlessly sees a progression of transmissions y which concurs with the veritable transmission way x (i.e., y = Adversary's Capabilities: We acknowledge that the enemy is taught, in that it has all out data on the association outline G, prior probabilities p (w), discernment transport p (yjx), and way apportionment p (xjw). The genuine center point transmissions are lossless and simply the adversary's insights may be lossy. We acknowledge that the enemy is external, in that it doesn't move toward the individual centers in the association, and the substance of the correspondences, including the pack headers, are guaranteed by encryption and don't deliver any information on w. We similarly expect that the adversary is uninvolved, in that it doesn't control the association traffic by dropping or injecting packages, which can be successfully perceived. The adversary can recognize w from each saw y by indicating the entire plan of possible discernments for each source target pair. Connection with Greedy and Uniform Heuristics From this part onwards, we acknowledge a lossless discernments adversary. The nuances for the Greedy and Uniform this shows that growing the amount of recipient center points doesn't needed mean better security. Surely, the differentiation between the Greedy heuristic and OPERA can be enormous as shown in the figure. The Uniform heuristic doesn't join to the most outrageous Uniform heuristic will reliably pick each real briefest way that serve w (which spills information about the target) while the Greedy and OPERA methodologies will overall pick a singular way. Hereafter, this results in a higher Detect for the Uniform heuristic regardless, when the typical cost is zero. Assessment of Single-way and Multipath The improvement in Detect for the proposed OPERA emits an impression of being delicate in the line association and doesn't have any enormous effect in the framework association. Regardless, the improvement is more enormous in the twofold tree network as the insurance monetary arrangement gets slack. This is because the multipath approach can additionally foster security in circumstances where a leaf center is talking with another leaf center in a comparable sub tree. Exactly when the course is bound to simply a singular way, the goal can be adequately associated with a comparative sub tree as the way doesn't wander out to other sub trees. This genuinely limits the amount of recipients and cuts down assurance when the security spending plan is slack. Eventually, the single-way directing impediment can be used if the security monetary arrangement is tight.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007112|

V. INCREASING BASE-STATION ANONYMITY

This section at first loosens up notable haziness measures to suit the BS. Then we present the BAR approach for boosting the BS mystery. Finally, protecting the BS through relocation and the point by point RIA approach are analyzed. Assessing base-station mystery the adversary who can remotely hurt the BS would be excited about finding the locale in which BS lies rather than its exact region. From this time forward the BS can expect that adversary would show the course of action locale as a structure of comparable estimated cells. The adversary uses his stuff, for instance signal revelation radio wires, at the telephone level and appropriately a telephone is seen as a Surveillance Area. He will strongly endeavor to diminish the size of the anonymity set, which from the start joins all phones, by excepting low assurance choices. All things considered, the adversary would try to recognize the observation district in which the BS is most apparently present. An enemy perpetually tracks radio transmission using his sign area recieving wires and totals his knowledge using a proper lack of clarity examination model. Ensuing to assessing anonymity the enemy should have the alternative to exhort probabilistically how much the observation locale may contain the BS. At the point when he develops with high assurance that a perception district contains the target then he can strike. On the other hand, the BS tries to keep its work and region obscure by avoiding network wide transmission using its incredible radio transmissions that isolates the BS from the resource confined sensors. The BS moreover picks to keep away from sight by applying intuitive wellbeing endeavors, for instance, having a clandestineness genuine arrangement and arranging covertly spots, etc The major test that the BS would fight to deal with is covering it's anything but's a data sink. It is basic for the BS station to screen its own lack of definition. But on the off chance that the BS doesn't have its own special generous extent shortcoming it can't pursue any therapeutic movement. Neither would it have the option to affirm whether the therapeutic measures to be certain diminished its shortcoming. Therefore it is ultimately the obligation of the BS to evaluate its mystery. Regardless, anonymity should be assessed by foe's perspective to be trademark. Hence the BS makes a couple of doubts about the capacities of the enemy and the cell size he would use to discover the BS. Then the BS would imitate the direct of the foe and perform traffic examination on the association to measure its mystery. The going with explains how the three appraisals analyzed in Section 3 can be contacted suit the BS in WSN. Note that the activities are as per the adversary's point of view. Entropy The Entropy of a WSN tends to the transport of traffic across the association. We consider an overall adversary who can make a connection of the amount of packs conveyed from each cell.

VI. CONCLUSION

We have developed a certified amazing development to ideally manage the security saving controlling issue in far off affiliations given some utility limitations expecting an inconceivable generally adversary that utilizes the best most breaking point posteriori (MAP) assessment framework. We in addition showed through expansions that our framework is without a doubt better diverged from the Uniform and Greedy heuristics, a check plot, and the normal data minimizations create. For future work, it is fascinating to consider the affirmation utility compromise issue for versatile affiliations and to give stricter security goals to the passing on parties. We propose another plan for adaptable organizing exposure in CRNs where the measure of weaves to be found can be changed with the affiliation topography dependent upon a client depicted utility breaking point. We study the tradeoff between the course optimality and the organizing overhead as a portion of the measure of found weaves both deductively and through redirections. Results show the possible increases of the proposed plan and how it can change as per diverse client necessities. This work can be loosened up several different ways. In any case, we can apply our exposure plot over various classes of coordinating shows in CRNs. Another future course is to explore new and more unpredictable numerical methods for choosing the best k. The testing our methodology while having different channels and a channel affirmation plan would be a pleasant course for future examination. At last, we are significance to extend our show by unequivocally thinking about different limits regarding the optimality metric.

REFERENCES

1. J. Deng, R. Han, and S. Mishra, “Countermeasures against traffic analysis attacks in wireless sensor networks,” in Proc. Int. Conf. Security and Privacy for Emerging Areas in Commun. Networks, pp. 113–126, 2005.
2. M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards statistically strong source anonymity for sensor networks,” in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), Apr. 2008.
3. J. Y. Koh, J. Teo, D. Leong, and W.-C. Wong, “Reliable privacypreserving communications for wireless ad hoc networks,” in Proc. IEEE Int. Conf. Commun. (ICC), pp. 6271–6276, Jun. 2015.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

|DOI:10.15680/IJIRSET.2021.1007112|

4. P. Zhang, C. Lin, Y. Jiang, P. Lee, and J. Lui, "ANOC: Anonymous network-coding-based communication with efficient cooperation," IEEE J. Sel. Areas Commun., vol. 30, pp. 1738–1745, Oct. 2012.
5. H. Shen and L. Zhao, "ALERT: An anonymous location-based efficient routing protocol in MANETs," IEEE Trans. Mobile Comput., vol. 12, pp. 1079–1093, Jun. 2013.
6. M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," IEEE Commun. Surveys Tuts., vol. 15, pp. 1238–1280, Jan. 2013.
7. Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan, and W. Jia, "A new cell-counting-based attack against tor," IEEE/ACM Trans. Networking, vol. 20, pp. 1245–1261, Aug 2012.
8. D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, pp. 84–90, Feb. 1981.
9. Peter Steenkiste, Douglas Sicker, Gary Minden, and Dipankar Raychaudhuri. NFS Workshop on Future Directions in Cognitive Radio Network Research. Technical report, 2009.
10. Suman Banerjee, Dapeng Oliver Wu, Xiaojun Lin, and Xinyu Zhang. NFS Workshop on Future Directions in Wireless Networking. Technical report, 2013.
11. DARPA. Spectrum Collaboration Challenge. Https:/spectrumcollaborationchallenge.com/, 2016. [Online; accessed October-2017].
12. E Fadel, Muhammad Faheem, Vehbi C Gungor, Laila Nassef, N Akkari, Muhammad Ghulam Abbas Malik, Suleiman Almasri, and Ian F Akyildiz. Spectrum-aware bio-inspired routing in cognitive radio sensor networks for smart grid applications. Computer Communications, , 2017.
13. Moustafa Youssef, Mohammad Ibrahim, Mohamed Abdelatif, Lin Chen, and Athanasios V Vasilakos. Routing metrics of cognitive radio networks: A survey. Communications Surveys & Tutorials, IEEE, 92–109, 2014.
14. Shriram Kulkarni and Shriram Markande. Comparative study of routing protocols in cognitive radio networks. In Pervasive Computing (ICPC), 2015 IEEE, 2015.
15. Angela Sara Cacciapuoti, Marcello Caleffi, and Luigi Paura. Reactive Routing for Mobile Cognitive Radio Ad Hoc Networks. Ad Hoc Networks, , 2012.
16. Angela Sara Cacciapuoti, Cosimo Calcagno, Marcello Caleffi, and Luigi Paura. CAODV: Routing in mobile ad-hoc cognitive radio networks. Wireless Days (WD), 2010.
17. Peter Steenkiste, Douglas Sicker, Gary Minden, and Dipankar Raychaudhuri. NFS Workshop on Future Directions in Cognitive Radio Network Research. Technical report, 2009.
18. Suman Banerjee, Dapeng Oliver Wu, Xiaojun Lin, and Xinyu Zhang. NFS Workshop on Future Directions in Wireless Networking. Technical report, 2013.
19. DARPA. Spectrum Collaboration Challenge.https:spectrumcollaborationchallenge.com/, 2016. [Online; accessed 28-October-2017].
20. E Fadel, Muhammad Faheem, Vehbi C Gungor, Laila Nassef, N Akkari,Muhammad Ghulam Abbas Malik, Suleiman Almasri, and Ian F Akyildiz. Spectrum-aware bio-inspired routing in cognitive radio sensor networks for smart grid applications. Computer Communications,101:106–120, 2017.
21. Moustafa Youssef, Mohammad Ibrahim, Mohamed Abdelatif, Lin Chen, and Athanasios V Vasilakos. Routing metrics of cognitive radio networks: A survey. Communications Surveys & Tutorials, IEEE,16(1):92–109, 2014.
22. Shriram Kulkarni and Shriram Markande. Comparative study of routing protocols in cognitive radio networks. In Pervasive Computing (ICPC), 2015 International Conference on, pages 1–5. IEEE, 2015.
23. Angela Sara Cacciapuoti, Marcello Caleffi, and Luigi Paura. Reactive Routing for Mobile Cognitive Radio Ad Hoc Networks. Ad Hoc Networks, 10(5):803–815, 2012.
24. Angela Sara Cacciapuoti, Cosimo Calcagno, Marcello Caleffi, and Luigi Paura. CAODV: Routing in mobile ad-hoc cognitive radio networks. Wireless Days (WD), 2010.
25. Ashwin Sampath, Lei Yang, Lili Cao, Haitao Zheng, and Ben Y Zhao. High throughput spectrum-aware routing for cognitive radio networks. Proc. of IEEE Crowncom, 2008.
26. Bing Xia, M.H. Wahab, Yang Yang, Zhong Fan, and M. Sooriyabandara. Reinforcement learning based spectrum-aware routing in multi-hop cognitive radio networks. In Cognitive Radio Oriented Wireless Networks and Communications CROWNCOM '09. 4th International Conference on, june 2009.
27. Xiaoxia Huang, Dianjie Lu, Pan Li, and Yuguang Fang. Coolest Path: Spectrum Mobility Aware Routing Metrics in Cognitive Ad Hoc Networks. In Distributed Computing Systems (ICDCS), 2011 31st International Conference on, pages 182 –191, 2011.
28. Cornelia-Ionela Badoi, Victor Croitoru, and Ramjee Prasad. IPSAG:An IP Spectrum Aware Geographic Routing Algorithm Proposal for Multi-hop Cognitive Radio Networks. In Communications (COMM), 8th International Conference on, pages 491–496. IEEE, 2010.
29. Wooseong Kim, Mario Gerla, Soon Y Oh, Kevin Lee, and Andreas Kassler. CoRoute: A New Cognitive Anypath Vehicular Routing Protocol. Wireless Communications and Mobile Computing, 11(12):1588–1602, 2011.
30. Xing Tang, Yanan Chang, and Kunxiao Zhou. Geographical Oportunistic Routing in Dynamic Multi-hop Cognitive Radio Networks. In Com-puting, Communications and Applications Conference (ComComAp), pages 256–261. IEEE, 2012.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details