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 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003079

Enhanced Optimal Primary User-Aware Innovation Routing For Cognitive Radio Networks

S. Nandhini[1]., Dr.N.Elamathi.,[2]

Research Scholar, Department of Computer Science, Trinity College for Women (Arts and Science), Namakkal, Tamilnadu, India[1]

Assistant Professor, Department of Computer Science, Trinity College for Women (Arts and Science), Namakkal, Tamilnadu, India[2]

ABSTRACT : Privacy-preserving routing protocols in wireless networks commonly use additional artificial traffic to secrete the source-destination uniqueness of the communicating pair. Usually, the addition of artificial traffic is done heuristically with no guarantees that the transmission charge, latency, etc., are optimized in every network topology. In this paper, we obviously check the privacy-utility trade-off problem for wireless networks and extend a novel privacy-preserving routing algorithm called **Optimal Privacy Enhancing Routing Algorithm (OPERA). OPERA** uses a numerical decision-making frame to optimize the privacy of the routing protocol set a service (or cost) power. We consider global adversary with both lossless and lossy clarification that use the **Bayesian Maximum-A-Posteriori (MAP**) inference approach. We prepare the Privacy-Utility "Trade-Off" Problem as a linear program which can be capably solved. Our reproduction outcome demonstrate that **OPERA** reduce the adversary's detection probability by up to 50% compared to the random Uniform and Greedy heuristics, and up to five times compared to a baseline scheme. In addition, **OPERA** also out performs the conventional information-theoretic common in order approach.

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

I. INTRODUCTION

Cognitive Radio Networks **(CRNs)** present a promising solution for spectrum scarcity in wireless networks to cope with the ever-increasing demand for higher bandwidth in mobile communications. In **CRNs**, unlicensed Secondary Users **(SUs)** opportunistically utilize vacant portions of the spectrum without interfering with licensed Primary Users **(PUs)**. This promises a large set of potential applications, given the scarcity of the unlicensed wireless spectrum, including distributed mobile applications for high-demand and highly crowded scenarios such as the Internet of Things, high-quality an earlier version of this paper appeared in the proceedings of IEEE Global Communications Conference (GLOBECOM) 2015. Mobile video, and disaster or emergency response settings. One example of these applications is the recent Spectrum Collaboration Challenge **(SC2)** proposed by DARPA in 2016 In this challenge, "competitors will reimaging a new, more efficient wireless paradigm in which radio networks autonomously collaborate to dynamically determine how the spectrum should be used moment to moment". Despite this promise, one of the main problems that impact the performance of multi-hop **CRNs** is routing. Compared to traditional ad hoc networks, routing in **CRNs** has to deal with the unique challenges of dynamic spectrum availability (due to the stochastic behavior of primary and secondary users), resource heterogeneity (resulting from the availability of different channels and radios on the same node), and synchronization between nodes on different channels, among others. Hence, we present the **Optimal Privacy Enhancing Routing Algorithm (OPERA)** which uses a statistical decision-making framework to characterize different network scenarios and select the optimal path distribution that strikes a balance between the privacy and utility (e.g., in terms of transmission cost) of the routing protocol given some privacy budget (e.g., transmission cost constraint). Additional dummy traffic may also be used to extend the routing path to include additional receiver nodes (nodes that received the dummy traffic). The statistical decision-making framework approach extends our earlier work in where a heuristic probabilistic routing algorithm was proposed to enhance the privacy for the destination node. In this work, we consider a relatively stronger adversary that uses the Bayesian **MAP** estimation strategy and also consider the case where the adversary has lossy observations. We formulate the selection of the optimal "privacy-preserving paths for each source-destination pair using a statistical decision-making framework that results in a linear program" which is easily solved by many commercial solvers.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003079

II. RELATED WORK

In traditional wired networks, the tradeoff problem between global and local routing is studied extensively. For example, in the scope of the Internet, the concept of Autonomous Systems (Intra and Inter AS routing) is used to achieve this tradeoff. Similarly, the tradeoff between route optimality and scalability has been also studied in the context of **wireless networks**. However, the onion routing technique is more prevalent due to its lower latency which makes it practical. Fortunately, the local observability assumption is valid in the large-scale Internet. In contrast, the relatively smaller wireless networks are more vulnerable to traffic analysis from a global adversary. In addition, due to the wireless broadcast medium, it is possible for an adversary to passively eavesdrop on all transmissions from a wireless node without being detected.

III. METHODOLOGIE

3.1 OPTIMAL DETECTION OF SOURCE-DESTINATION PAIR w: Suppose that the true source-destination pair is w and the adversary observes **y. A** successful detection occurs when the adversary's estimate of the source-destination pair **BW(y)** matches **w**. **Lossy Adversarial Observations** we solve Problem to obtain the optimal P detect values for the proposed **OPERA**. Shows the P detect values for **OPERA** and the approximation method in Section IV-C4 for a line network with the erasure probabilities _ = 0:1 and _ = 0:5. Generally, P detect decreases as increases since the unobserved transmissions may belong to a larger set of possible source nodes. Also, a larger **n** value is needed to better approximate P detect for larger values. There exists an inverse relationship between the value of **n** and the complexity of the optimization problem in and higher **n** results in a more accurate estimate of the true P detect at the expense of additional computational costs. More performance degradation is experienced in the grid network compared to the line network as the number of possible w pair's increases when less transmission is observed. Interestingly, the optimized paths from the approximation method coincide with the optimal paths of the original method in our simulation, the adversary's detection rate does not improve even if he uses while the system uses the approximation method.

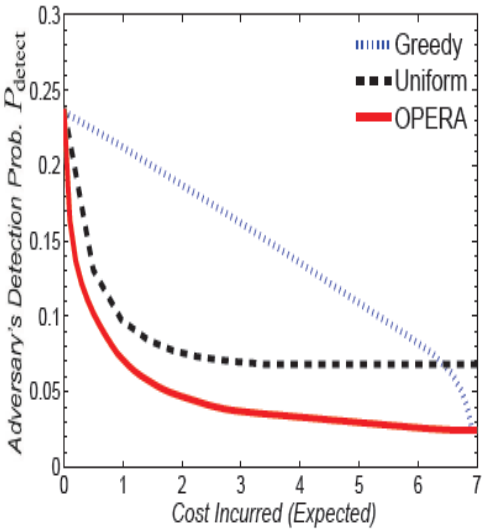

Figure 3.1: Optimal Detection of Source-Destination Pair

3.2 LIMITATIONS OF CURRENT HEURISTIC ALGORITHMS:

It is evident that the privacy-enhancing schemes do not come for free and there exists a trade-off between the privacy and transmission overheads incurred. Although the above schemes have mainly relied on additional dummy traffic (or/and delays) to mitigate traffic analysis attempts, there is no rigorous quantification of the adversary's detection probability, their optimal attacking strategy, and the overheads incurred by the scheme. Hence, it would be interesting to quantify the loss of utility (or cost) incurred by the privacy-preserving scheme and weigh it against the additional amount of privacy provided. System Model In this section, we present our system assumptions and then provide a brief overview of the proposed discovery scheme. We consider the scenario where a source node u wants to send packets to a single destination node v in a static wireless network. System Assumptions We consider an ad hoc

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003079

cognitive radio network where **PUs** hold the right to use the licensed spectrum while **SUs** can access only the unoccupied portions of the spectrum become active onion routing technique The independent exponential distributions with birth parameter and death parameter depending on the traffic of the **PUs**. These parameters can be estimated using offline statistics, local sensing information, or through implicit feedback in full duplex communications. The homogeneous in terms of their parameters and transmission ranges. We assume that **SUs** and **PUs** channels follow the unit disc model. This is common in many **CRN** scenarios such as TV white space-based **CRNs**. We also do not make any specific assumption on the **MAC** or higher layer protocols for the PUs' system. We further assume that **SUs** are located uniformly in the two-dimensional Cartesian space and each **SU** knows its own location and the location of its direct neighbors. A node can estimate its location using any of the current localization systems, including **GPS** or mobile-based systems. Moreover, a sender can obtain the location information of the ultimate destination via out of band services that map node addresses to locations, or have it disseminated through the network. Assuming knowing only the location of the destination is a typical and valid assumption in many applications including military and sensor networks where reporting nodes know the locations of the sink nodes. Although having the locations of all nodes of the network may lead to better and more robust routes, we do not assume having nodes' locations except for the sink and the neighboring nodes; we believe that disseminating the nodes' locations information to the whole network and keeping it up-to-date requires a huge overhead, which degrades our system performance. Without loss of generality, exchanging routing control packets can be done through a **Common Control Channel (CCC)**. Moreover, our model does not assume any specific frequency band.

3.3PRIVACY-PRESERVING ROUTING In this section, we present the proposed privacy-preserving techniques for protecting the location information of monitored objects and data sinks. We assume that all communications between sensor nodes in the network are encrypted so that the contents of packets appear random to the global eavesdropper. Source-Location Privacy Techniques In this section, we present two techniques to provide location privacy to monitored objects in sensor networks, periodic collection and source simulation. The periodic collection method achieves the optimal privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication overhead, and latency. Sink Simulation Similar to source simulation, an intuitive solution for sink location privacy would be to confuse the adversary by creating virtual sinks. For this purpose, we propose to create multiple candidate traces toward the fake sinks in the network to hide the traffic between real objects and real sink Protocol description.

IV. PRIVACY PROTECTION

4.1 PRIVACY PROTECTION OBSERVATION: As the adversary has global observability, he is potentially able to observe all node transmissions from the entire network. However, we consider the following two observation models for the adversary.

4.2 LOSSY OBSERVATIONS: In practice, the adversary may have lossy observations due to the lossy nature of the wireless channel or some blind spots in his network. In sink simulation, fake sinks will be simulated in the field. Each of them will receive traffic similar to the traffic received by a real sink. To achieve this, we make no distinction between fake and real sinks when sensors send packets. During deployment, we place real sinks and select locations where fake sinks are to be simulated. A subset of the sensors will be used as fake sinks. It is also required that each real sink have a fake sink simulated in its communication range. We will only send messages to the fake sinks and have all fake sinks perform a one-hop broadcast of the message, ensuring full concealment of the real sink locations. System and threat models this paper considers a **WSN** with a single **BS** node. **BS** acts as the sink of the collected sensor data, i.e., the **BS** is the ultimate end-point of all the communication in the network. In other words, the **BS** is an in situ user of the network. We consider a homogenous network in which all sensor nodes have similar resources such as initial energy, link capacity and communication range. While a sensor has limited onboard energy supply and is only capable of short haul transmission, the **BS** is not as constrained in its energy, communication and computation capabilities. The **BS** also is able to move from one location to another within the **WSN** area. For example, the **BS** can be a laptop mounted on a vehicle that can travel within the deployment area. Strength of Privacy Protection to evaluate the strength of location-privacy protection, we use two criteria: the safe time of the receiver and the attack time of the adversary. The receiver's safe time is measured as the number of packets delivered before the receiver is captured. The adversary's attack time is measured as the number of moving steps (from one sensor location to a neighbor) the adversary has to make before he reaches the receiver. We perform the simulations on a sensor network of 900 nodes, among which 100 randomly-selected ones are source nodes that periodically generate data packets for the receiver. The

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003079

source period is defined as the time between two packets generated from a source node. The initial distance from the adversary to the receiver is 15 hops. The adversary has the characteristics described in Section III-B. In his attack strategy, the adversary stays in one position to overhear packets, and move to the next location based on the policy described. If no packet is overheard for duration of 100 source periods, the adversary backtracks to his previous location. The adversary remembers 5 steps in his moving history. After his history record is exhausted, he walks randomly until catching a packet. We set a time limit for our simulation, which is the time for 500,000 packets to be delivered. The program terminates if the adversary cannot capture the receiver in the time limit. That we all know from our 1-hop neighbors. Thanks to interference, a node might not remember of some 1-hop neighbors. Adversary Model We consider an external, passive, global and informed adversary who observes a (possibly lossy) sequence of transmissions y from an actual transmission path **x**. Using a Bayesian traffic analysis technique, the adversary aims to detect the identity of the source-destination pair w for each observation y, i.e., he aims to identify which node is talking to which node based on his possibly imperfect observations.

4.3 LOSSLESS OBSERVATIONS: The lossless observations model is a special case in which the adversary perfectly observes a sequence of transmissions y which coincides with the actual transmission path **x (i.e., y** = Adversary's Capabilities: We assume that the adversary is informed, in that it has complete knowledge of the network graph **G**, prior probabilities **p (w),** observation distribution **p (yjx)**, and path distribution p **(xjw).** The actual node transmissions are lossless and only the adversary's observations may be lossy. We assume that the adversary is external, in that it does not have access to the individual nodes in the network, and the contents of the communications, including the packet headers, are protected by encryption and do not leak any information on **w.** We also assume that the adversary is passive, in that it does not manipulate the network traffic by dropping or injecting packets, which can be easily detected. The adversary can identify w from each observed y by enumerating the entire set of possible observations for each source destination pair. Comparison with Greedy and Uniform Heuristics From this section onwards, we assume a lossless observations adversary. The details for the Greedy and Uniform this indicates that increasing the number of receiver nodes does not necessary translate to better privacy. In fact, the difference between the Greedy heuristic and **OPERA** can be quite significant as shown in the figure. The Uniform heuristic does not converge to the maximum Uniform heuristic will uniformly pick each valid shortest path that serve **w** (which leaks information about the destination) while the Greedy and **OPERA** methods tend to choose a single path. Hence, this results in a higher Detect for the Uniform heuristic even when the expected cost is zero. Comparison of Single-path and Multipath The improvement in Detect for the proposed **OPERA** appears to be mild in the line network and does not have any significant effect in the grid network. However, the improvement is more significant in the binary tree network as the privacy budget becomes slack. This is because the multipath approach can improve privacy in scenarios where a leaf node is communicating with another leaf node in the same sub tree. When the route is restricted to only a single path, the destination can be easily linked to the same sub tree as the path does not travel to other sub trees. This severely limits the number of receivers and lowers privacy when the privacy budget is slack. In practice, the single-path routing constraint can be used if the privacy budget is tight.

V. INCREASING BASE-STATION ANONYMITY

This section first extends popular anonymity measures to suit the **BS.** Then we present the **BAR** approach for boosting the **BS** anonymity. Finally, safeguarding the **BS** through relocation and the detailed **RIA** approach are discussed. Measuring base-station anonymity the adversary who has the capacity to remotely damage the **BS** would be interested in finding the region in which **BS** lies rather than its exact location. Hence the **BS** can assume that adversary would model the deployment area as a grid of equal-sized cells. The adversary employs his equipment, e.g. signal detection antennas, at the cell level and thus a cell is considered a Surveillance Area. He will aggressively try to reduce the size of the anonymity set, which initially includes all cells, by excluding low confidence choices. In other words, the adversary would strive to identify the surveillance area in which the **BS** is most probably present. An adversary continuously tracks radio transmission using his signal detection antennas and accumulates his knowledge using a suitable anonymity assessment model. After measuring anonymity the adversary should be able to tell probabilistically the degree to which the surveillance area may contain the **BS**. Once he establishes with high confidence that a surveillance area contains the target then he can strike. On the other hand, the **BS** strives to keep its role and location anonymous by avoiding network wide broadcast using its high powered radio transmissions that differentiates the **BS** from the resource-limited sensors. The **BS** also opts to stay out of sight by applying intuitive security measures such as having a stealth physical design and positioning in hidden spots, etc. The main challenge that the **BS** would struggle to tackle is concealing its role as a data sink. It is extremely important for the **BS** station to keep a track of its own anonymity. Unless the **BS** does not have a concrete measure of its own vulnerability it cannot pursue any corrective

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003079

action. Neither can it verify whether the corrective measures indeed reduced its vulnerability. Thus it is ultimately the responsibility of the **BS** to measure its anonymity. However, anonymity has to be measured from adversary's perspective in order to be indicative. Hence the **BS** makes some assumptions about the capabilities of the adversary and the cell size he would use to track down the **BS**. Then the BS would simulate the behavior of the adversary and perform traffic analysis on the network to measure its anonymity. The following explains how the three measures discussed in Section 3 can be extended to suit the **BS** in **WSN**. Note that the measures are from the adversary's point of view. Entropy The Entropy of a **WSN** represents the distribution of traffic across the network. We consider a global adversary who can make a comparison of the number of packets transmitted from each cell.

VI. CONCLUSION

We have developed a statistical decision-making framework to optimally solve the privacy-preserving routing problem in wireless networks given some utility constraints assuming a powerful global adversary that uses the optimal maximum- posteriori **(MAP)** estimation strategy. We also showed via simulations that our approach is significantly better than the Uniform and Greedy heuristics, a baseline scheme, and the mutual information minimization scheme. For future work, it would be interesting to study the privacy-utility trade-off problem for mobile networks and to provide stricter privacy constraints for the communicating parties. We propose a new scheme for adaptive routing discovery in **CRNs** where the number of hops to be discovered can be adapted with the network topology based on a user-defined utility function. We study the tradeoff between the route optimality and the routing overhead as a function of the number of discovered hops both analytically and through simulations. Results show the advantages of the proposed scheme and how it can adapt to different user requirements. This work can be expanded in several directions. First, we can apply our discovery scheme over different classes of routing protocols in **CRNs**. Another future direction is to investigate new and more complex mathematical approaches for deriving the optimal **k**. The experimenting our approach while having multiple channels and a channel selection scheme would be a good direction for future research. Finally, we are planning to extend our protocol by explicitly considering other functions for 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.
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.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003079

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:
7.512

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