Journal of Theoretical and Applied Information Technology
20th June 2015. Vol.76. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RACARP: A ROBUSTNESS AWARE ROUTING PROTOCOL FOR COGNITIVE RADIO AD HOC NETWORKS

[1]ZAMREE CHE-ARON, [2]AISHA HASSAN ABDALLA, [3]KHAIZURAN ABDULLAH, [4]WAN HASLINA HASSAN, [5]MD. ARAFATUR RAHMAN

[1]PhD student, Department of Electrical and Computer Engineering, IIUM, Malaysia

[2]Professor, Department of Electrical and Computer Engineering, IIUM, Malaysia

[3]Assistant Professor, Department of Electrical and Computer Engineering, IIUM, Malaysia

[4]Associate Professor, Malaysia-Japan International Institute of Technology (MJIIT), UTM, Malaysia

[5]Research Fellow, Dept. of Biomedical Electronics and Telecommunications Engineering, UNINA, Italy

E-mail: [1]one_zamree@hotmail.com, [2]aisha@iium.edu.my, [3]khaizuran@iium.edu.my,
[4]wanhaslina@ic.utm.my, [5]arafatur.rahman@unina.it

ABSTRACT

Cognitive Radio (CR) is a new paradigm which offers a viable solution to deal with the spectrum shortage problem and enhances the spectrum utilization in wireless communication systems. In Cognitive Radio Ad Hoc Networks (CRAHNs), data routing is one of the most challenging tasks due to varying link-quality, frequent topology changes and intermittent connectivity caused by the activities of Primary Users (PUs). This paper proposes a robustness aware routing protocol for CRAHNs, referred to the Robustness Aware Cognitive Ad-hoc Routing Protocol (RACARP), with an aim to provide robust transmission path and offer fast route recovery in presence of PU activities during data delivery. The Expected Path Delay (EPD) routing metric used in the protocol for path decision is also introduced. The protocol avoids creating a transmission path that uses PU's channel in PU regions in order to counteract the impact of PU activity. Moreover, for the purpose of fast route recovery, the multi-path multi-channel routes are given by utilizing the joint path and spectrum diversity in routing. The performance evaluations are conducted through simulations using NS-2 simulator. The simulation results obviously demonstrate that the RACARP protocol can significantly achieve better performance in terms of average throughput, packet loss, average end-to-end delay, and average jitter as compared to the recently proposed D2CARP protocol in identical scenarios.

Keywords: *Cognitive Radio Ad Hoc Network, Robustness Aware Routing, Expected Path Delay, PU Impact Avoidance, Joint Path and Spectrum Diversity*

1. INTRODUCTION

The recent experiment results conducted by the Federal Communications Commission (FCC) [8] have proved that the static spectrum allocation policy, which allows each wireless service to access fixed frequency bands, poses the spectrum inefficiency problem. Furthermore, due to the rapidly increased demand for wireless services, the radio spectrum is one of the most heavily used and costly natural resources, thus leading to the problem of spectrum scarcity.

Cognitive Radio (CR) technology [9] has been proposed as a promising solution to improve the spectrum utilization, reduce the congestion in the unlicensed bands and alleviate the shortage of spectrum resources. In Cognitive Radio Networks (CRNs) [2], Secondary Users (SUs) (or CR users) are allowed to opportunistically access the temporally unused licensed bands without harmful interference to licensed users (or Primary Users (PUs)).

Cognitive Radio Ad Hoc Network (CRAHN) [1] is a class of CRN which applies the CR paradigm to ad hoc scenarios. In the networks, SUs exploit the available Spectrum Opportunities (SOPs) (a set of spectrum bands currently unoccupied by PUs) for creating multi-hop communications in a peer-to-peer manner, i.e. without a central controller. Unlike the traditional wireless ad hoc networks, CRAHNs can take advantage of dynamic use of spectrum bands to achieve higher network capacity.

With unique characteristics of CRAHNs, the traditional ad hoc routing protocols (e.g. AODV [11], DSR [10], OLSR [7], DSDV [12] etc.) are not suitable to apply in the networks and new several challenges [5] must be taken into account. The main challenge is to deal with the dynamic spectrum availability. In CRAHNs, the SOPs are time and location varying due to dynamic PU activities. Consequently, the collaboration between spectrum decision and path selection is needed. Another challenge is how to determine the optimal path for data transmission, which provides high network performance. Therefore, the effective routing metrics able to accurately account for the quality of different paths are required. Moreover, in CRAHNs, a link failure frequently occurs caused by not only the node mobility but also the appearance of PU activity. The data transmission of SUs may be interrupted immediately after a PU activity is detected in order not to cause harmful interference to the PU. As a result, the efficient path recovery mechanism is also necessary in order to rapidly recover the failed paths. Therefore, the CR ad hoc routing protocols must satisfy the requirements of both CRNs and ad hoc networks.

In this paper, we propose a robustness aware routing protocol for CRAHNs, namely the Robustness Aware Cognitive Ad-hoc Routing Protocol (RACARP), which is an extension of AODV protocol [11]. In RACARP, the new routing metric called the Expected Path Delay (EPD) metric, which takes account of the effect of packet loss and link delay, is proposed and implemented. Furthermore, the protocol establishes a transmission path that avoids using the PU's channel in the PU regions in order to counteract the impact of PU activity which can simply cause communication interruptions. The proposed path-selection mechanism favors a transmission path with small delay, low packet loss and less service interruption caused by PU activity. In addition, the protocol exploits the joint path and spectrum diversity in routing to provide multi-path multi channel routes so that the source node is able to dynamically switch to different paths and channels in presence of PU activity during data transmission for fast route recovery. The simulation results obviously show that the RACARP protocol outperforms the Dual Diversity Cognitive Ad-hoc Routing Protocol (D2CARP) [13] in terms of average throughput, packet loss, average end-to-end delay, and average jitter.

The remainder of this paper is organized as follows. In Section 2, we discuss about the related work. The overview of the RACARP protocol and the description of control packets formats are provided in Section 3 and Section 4 respectively. Section 5 describes the robust routing techniques in the protocol. Then, in Section 6, the protocol operations are explained in detail. The simulation environment and parameters are presented in Section 7. Subsequently, we exhibit the simulation results and evaluate the protocol performance in Section 8. The protocol performance is compared with that of the D2CARP protocol. Finally, the conclusion is provided in Section 9.

2. RELATED WORK

Although recent literatures in the area of routing in CRAHNs have been studied, research in cognitive ad hoc routing is still in its infancy and various issues [15] are still largely unexplored. In [17], a tree-based routing protocol, named the STOD-RP, has been proposed for CRAHNs. A spectrum tree is created in each spectrum band in order to help in the path selection and spectrum decision. Nonetheless, the protocol is based on assumption that all nodes are stationary or move very slowly. Furthermore, if the data transmission of SUs is interrupted by a PU activity on a particular channel, all SUs in the network must vacate that channel, even though they are not in the PU's transmission range. In [6], Chowdhury and Felice has proposed the SpEctrum Aware Routing protocol for Cognitive ad-Hoc networks (SEARCH) based on geographic routing paradigm (i.e. each SU can determine the location of other nodes). The protocol jointly performs channel and path selection to elude areas of PU activity during path establishment. However, the route recovery approach, in case of path failures occurring during data delivery, is not taken into account in this protocol. Moreover, the protocol may create long detours to avoid PU regions for data transmission, which can produce high packet delay. In [3], Beltagy et al. has proposed a multipath routing protocol with a purpose to improve the reliability of transmission paths in CRAHNs. The "Route Closeness" metric has been introduced to create transmission routes based on non-closeness to each other. The main goal of this routing design is to provide less vulnerability to the impact of PU activity as an active mobile PU is unable to interrupt all the selected paths in the same time if they are not close to each other. However, the issue of spectrum diversity is not considered, which is a main characteristic of CRAHNs, and the protocol is unsuitable to be applied in the highly dynamic mobile CRAHNs. The article in [4] has introduced the Cognitive Ad-hoc On-demand Distance Vector (CAODV) routing protocol, which applies individually path and spectrum diversity, with an aim to support dynamic CRAHNs. Nevertheless, the network performance can be significantly degraded due to the impact of PU activity and node mobility because the protocol has not jointly considered path and spectrum diversity in routing process. In [13], the Dual Diversity Cognitive Ad-hoc Routing Protocol (D2CARP) has been proposed by sharing some common functionalities with the CAODV. The protocol exploits the joint path and spectrum diversity in routing to reduce the impact of performance degradation experienced by SUs due to PU activities. Nonetheless, both CAODV and D2CARP use the number of hops as the routing metric in order to select the transmission path with minimum hop count. Although the main advantage of this metric is its simplicity, the quality of wireless links and the interference in the network are not taken into account, resulting in the establishment of non-optimal transmission paths which can significantly cause poor protocol performance. Moreover, since the avoidance of PU's channel in PU regions is not considered during path establishment process, hence, the transmission paths can be easily interrupted by PUs, especially when crossing PU regions.

3. OVERVIEW OF RACARP PROTOCOL

The RACARP protocol is an on-demand routing protocol, which triggers the route discovery process only when a data transfer is required by a source node, and also shares some common functionalities with D2CARP protocol [13]. Furthermore, the protocol exploits the joint path and spectrum diversity in routing to provide multi-channel multiple paths based on the EPD routing metric and also avoids creating the transmission paths that uses the PU's channel in the PU regions during route formation process with an aim to improve the network performance, provide fast route recovery in presence of PU activity, and make the transmission paths less vulnerable to the impact of PUs. A path with lowest EPD value is selected for data transmission. The sequence number, which indicates the freshness of route information, is utilized to circumvent the problem of routing loops. The RACARP's main control messages include RREQ (Route REQuest), RREP (Route REPly), RERR (Route ERRor), ETX (Expected Transmission Count) probe, RTT (Round-Trip Time) probe and RTT acknowledgement packet.

By applying RACARP protocol, each node in the network is unnecessary to know the complete path from source to destination for data transmission, but instead, only utilizes the local routing information (e.g. next-hop node and forward channel) stored in its routing table. A routing table consists of a list of routing entries containing the following information:

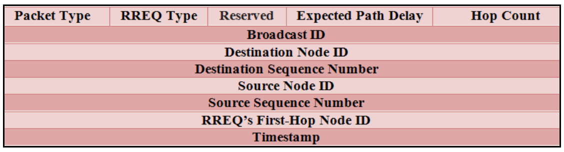
- ID of destination node.
- Destination sequence number.
- Channel interface through which a data packet will be forwarded.
- ID of next-hop node for data forwarding.
- First-hop node ID (the ID of the first-hop node receiving a RREQ packet directly from a source node or receiving a RREP packet directly from a destination node).
- Hop count (the number of hops required to reach a destination node).
- EPD (Expected Path Delay) value of a path from itself to a destination node.
- Route state flag, which marks a route as active (UP) or inactive (DOWN).
- PU impact flag, which indicates whether or not a route is unavailable due to a PU activity (i.e. 0 (interface enabled) or 1 (interface disabled)).
- Last hop count (the hop count before route invalidation).
- Last EPD value (the EPD value before route invalidation).
- Lifetime (the expiration time of the route).

4. CONTROL PACKET FORMATS

This section presents the structure of control packets used in the RACARP protocol. The format and semantics of the control packets will be explained in detail. The control packets can be classified into six types: (1) RREQ packet, (2) RREP packet, (3) RERR packet, (4) RTT probe packet, (5) RTT acknowledgement packet, and (6) ETX probe packet.

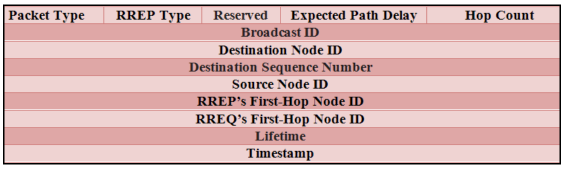
4.1 RREQ Packet

There are two types of RREQ packet used in the RACARP protocol: (1) Normal Route REQuest (N-RREQ) packet which is broadcasted by a source node requiring a transmission path to a destination node; and (2) Route REQuest Enable (RREQ-E) packet which is broadcasted by a node to enable a routing entry that has been disabled due to PU activity. The format of RREQ packet is shown in Figure 1.



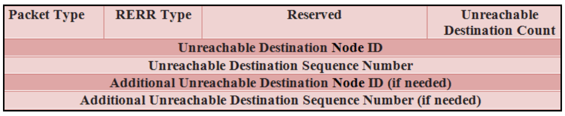
Packet Type	RREQ Type	Reserved	Expected Path Delay	Hop Count
Broadcast ID				
Destination Node ID				
Destination Sequence Number				
Source Node ID				
Source Sequence Number				
RREQ's First-Hop Node ID				
Timestamp				

Figure 1: RREQ Packet Format



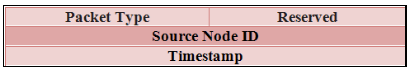
Packet Type	RREP Type	Reserved	Expected Path Delay	Hop Count
Broadcast ID				
Destination Node ID				
Destination Sequence Number				
Source Node ID				
RREP's First-Hop Node ID				
RREQ's First-Hop Node ID				
Lifetime				
Timestamp				

Figure 2: RREP Packet Format



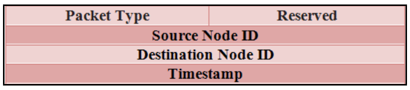
Packet Type	RERR Type	Reserved	Unreachable Destination Count
Unreachable Destination Node ID			
Unreachable Destination Sequence Number			
Additional Unreachable Destination Node ID (if needed)			
Additional Unreachable Destination Sequence Number (if needed)			

Figure 3: RERR Packet Format



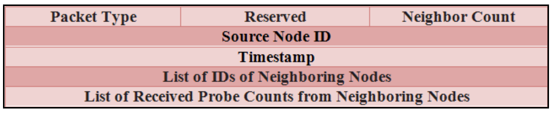
Packet Type	Reserved
Source Node ID	
Timestamp	

Figure 4: RTT Probe Packet Format



Packet Type	Reserved
Source Node ID	
Destination Node ID	
Timestamp	

Figure 5: RTT Acknowledgement Packet Format



Packet Type	Reserved	Neighbor Count
Source Node ID		
Timestamp		
List of IDs of Neighboring Nodes		
List of Received Probe Counts from Neighboring Nodes		

Figure 6: ETX Probe Packet Format

4.2 RREP Packet

The RACARP protocol utilizes two types of RREP packet: (1) Normal Route REPly (N-RREP) packet which is generated and sent back to the source of the received N-RREQ packet; and (2) Route REPly Enable (RREP-E) packet which is generated and transmitted back to a node which originates the received RREQ-E packet. The format of RREP packet is illustrated in Figure 2.

4.3 RERR Packet

In the RACARP protocol, there are two types of RERR packet including: (1) Normal Route ERRor (N-RERR) packet which is broadcasted to notify other nodes of the unavailability of transmission link; and (2) Route ERRor Disable (RERR-D) packet which is sent to inform the affected nodes to disable a route because a PU activity is detected. The format of RERR packet is shown in Figure 3.

4.4 RTT Probe Packet

In the RACARP protocol, an RTT probe packet is periodically broadcasted by a node to its neighbors over all channels in order for calculating the updated RTT value of a link. The format of RTT probe packet is presented in Figure 4.

4.5 RTT Acknowledgement Packet

When a node receives an RTT probe packet, an RTT acknowledgement packet is generated and sent back to the source of the RTT probe packet. The format of RTT acknowledgement packet is exhibited in Figure 5.

4.6 ETX Probe Packet

To measure the updated ETX value of a link, an ETX probe packet is periodically broadcasted by a node to its neighbors through all channels. The format of ETX probe packet is shown in Figure 6.

5. ROBUST ROUTING TECHNIQUES

In this section, we shall describe how the mechanism of path establishment is optimized with an aim to provide robust communications in CRAHNs. The RACARP selects a transmission path based on the EPD metric and prevents SUs in the PU regions from using the PU's channel to create a transmission link in order to offer low vulnerability to the impact of PU activities. Moreover, the joint path and spectrum diversity technique is also applied in routing process to provide multi-path multi-channel routes. We begin by explaining the EPD routing metric in detail and compare it with the hop count metric which is used in the existing D2CARP protocol for path selection. Next, the mechanism of PU channel avoidance in PU regions during path establishment process is described and, subsequently, the advantage of utilizing the joint path and spectrum diversity in routing is presented.

5.1 Path Decision Based on EPD Routing Metric

The EPD routing metric used in the RACARP protocol takes account of the link delay and the effect of packet loss on wireless links during route setup stage. The EPD(p) represents the expected time it takes a probe packet to travel along a path p from a node to another node which can be defined as:

$$\boxed{\text{EPD}(p) = \sum_{\text{Link } l \,\in\, p} \text{ELD}(l)} \tag{1}$$

where p is a path which are composed of the set of links. The ELD(l) that denotes the Expected Link Delay of the link l can be calculated as:

$$\text{ELD}(l) = \text{ETX}(l) * \left(\frac{\text{RTT}(l)}{2}\right) \tag{2}$$

where ETX(l) is the Expected Transmission Count of the link l, representing the expected number of retransmissions required to successfully transmit an ETX probe packet over the link l. The ETX(l) can be measured as:

$$\text{ETX}(l) = \frac{1}{[1-P_f(l)][1-P_r(l)]} = \frac{1}{[d_f(l) * d_r(l)]} \tag{3}$$

where $P_f(l)$ and $P_r(l)$ are the probability of packet loss in the forward and reverse direction of the link l respectively. The $d_f(l)$ (forward delivery ratio) denotes the probability that an ETX probe packet is successfully transmitted to the neighbor over the link l during the window period (i.e. *ETX_PROBE_WINDOW*). The $d_r(l)$ (reverse delivery ratio) represents the probability that an ETX probe packet sent from the neighbor is successfully received through the link l during the window period (i.e. *ETX_PROBE_WINDOW*). The $d_f(l)$ and $d_r(l)$ can be calculated as:

$$d_f(l) = \frac{n_f(l)}{\text{ETX\_PROBE\_WINDOW}} \tag{4}$$

$$d_r(l) = \frac{n_r(l)}{\text{ETX\_PROBE\_WINDOW}} \tag{5}$$

where $n_f(l)$ is the number of ETX probe packets successfully sent to the neighbor through the link l. While $n_r(l)$ represents the number of ETX probe packets successfully received from the neighbor via the link l.

Figure 7 depicts the measurement of ETX value in the RACARP protocol. From the figure, during the ETX_PROBE_WINDOW period from t_1 to t_2, the number of ETX probe packets that node A successfully transmits to node B over channel 1 is equal to 3 (i.e. $n_f = 3$). While the number of ETX probe packets that node A successfully receives from node B over channel 1 is equal to 3 (i.e. $n_r = 3$). Therefore, at time t_2, node A measures the ETX value between node A and node B over channel 1 as 2.777 (i.e. ETX(t_2) = 1/(d_f * d_r) = 1 / [(n_f / *ETX_PROBE_WINDOW*)*(n_r/*ETX_PROBE_WINDOW*)] = 1 / [(3/5) * (3/5)] = 2.777). However, during the ETX_PROBE_WINDOW period from t_2 to t_3, the number of ETX probe packets that node A successfully sends to node B over channel 1 is equal to 4 (i.e. $n_f = 4$). While the number of ETX probe packets that node A successfully receives from node B over channel 1 is equal to 4 (i.e. $n_r = 4$). Consequently, at time t_3, node A measures the ETX value between node A and node B over channel 1 as 1.562 (i.e. ETX(t_3) = 1 / (d_f* d_r) = 1 / [(n_f / *ETX_PROBE_WINDOW*) * (n_r / *ETX_PROBE_WINDOW*)] = 1 / [(4/5) * (4/5)] = 1.562).

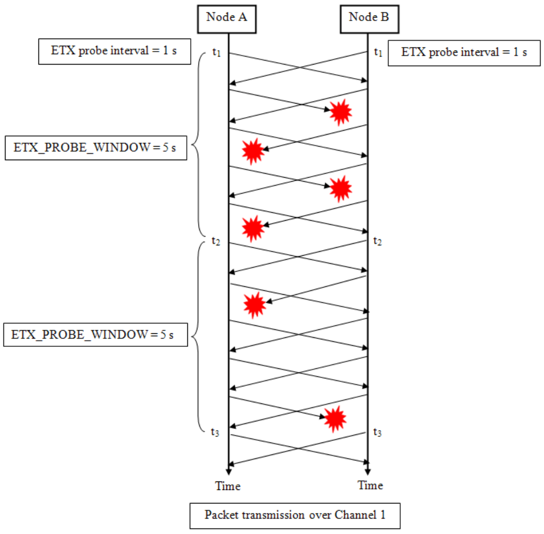


Figure 7: ETX Measurement

In Equation (2), the RTT(l) is the interval between the sending of an RTT probe packet and the receipt of the corresponding RTT acknowledgement packet over the link l. Figure 8 shows the measurement of RTT value in the RACARP protocol. From the figure, at time T_a, T_b and T_c, node A measures the RTT value between node A and node B over channel 1 as RTT 1, RTT 2 and RTT 3 second respectively (where (RTT 2 = T_b-t_2) > (RTT 3 = T_c-t_3) > (RTT 1 = T_a-t_1)).

To measure the updated ETX and RTT value of a link, each SU periodically broadcasts an ETX and RTT probe packet to the neighbors according to the ETX probe interval and RTT probe interval respectively.

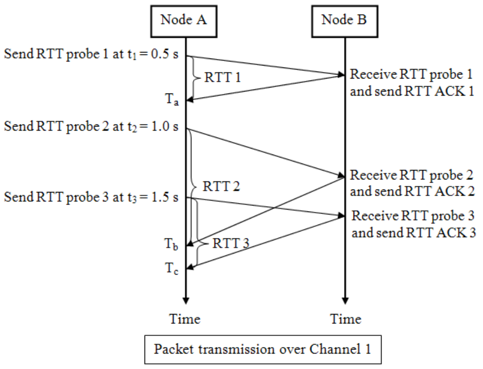


Figure 8: RTT Measurement

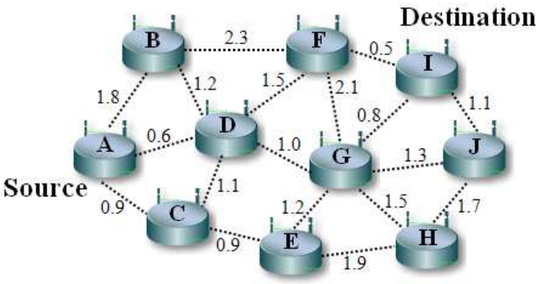
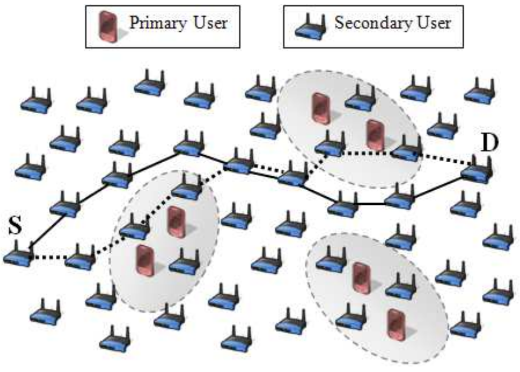


Figure 9: Path Decision Based on EPD Routing Metric

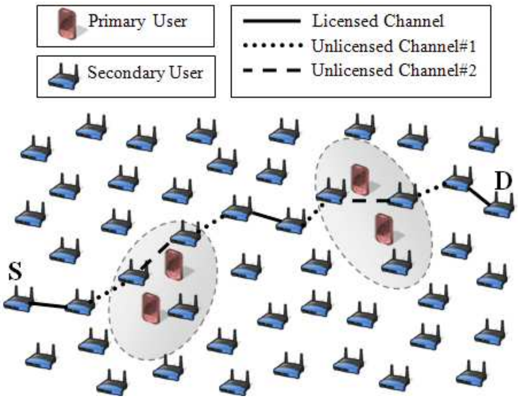
In CRAHNs, a SU selects an appropriate available channel among various channels for communication with each other based on a routing metric. Basically, the quality of each channel varies over time and location. However, the minimum hop count metric (used in the existing D2CARP protocol) is unable to reflect the accurate quality of transmission link, i.e. packet loss probability, link delay, etc. This especially occurs in a heterogeneous channel environment in which each channel has different characteristics. In the simple network shown in Figure 9, Node A (source node) requires a transmission path towards Node I (destination node). It is under the assumption that only one channel is available for communications and the ELD value of each link is exhibited. If the hop count is used as a routing metric in the network, the selected transmission path with minimum hop count can be one of these, i.e. A-B-F-I, A-D-F-I, or A-D-G-I. These transmission paths are composed of equal number of hops but their path qualities are different. On the other hand, the path A-D-G-I with lowest EPD value is chosen for data transmission if the EPD metric is used for path decision as in RACARP protocol. Therefore, the RACARP protocol always selects a transmission path with highest quality in terms of link delay and packet loss probability.

5.2 PU Channel Avoidance in PU Regions

The RACARP protocol always avoids establishing a transmission path that uses the PU's channel in the PU regions in order to alleviate the impact of PU activities, which can result in frequent communication interruptions. To accomplish this goal, every specific time interval, each SU checks to determine whether it is currently in a PU's transmission range or not. In case a SU is aware that it exists in a PU region, the PU's channel will be stored in its list of blocked channels; otherwise, it removes the PU's channel from the blocked channel list. In RACARP, a SU inside a PU region always declines to create a transmission path that uses the PU's channel. Therefore, the data packets are not delivered through the PU's channel when crossing the PU region.



(a) If Only One Licensed Channel is Available



(b) If both Licensed and Unlicensed Channels are Available

Figure 10: Path Establishment Based on PU Channel Avoidance in PU Regions

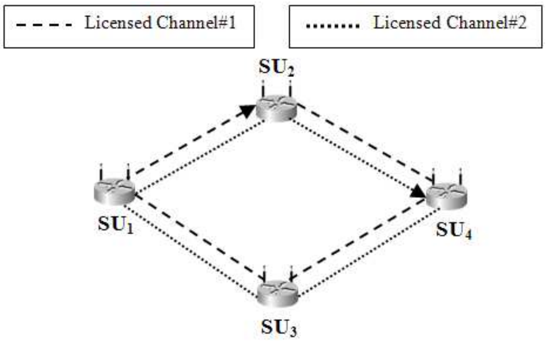
As exhibited in Figure 10(a), when only one licensed channel is available in the network, if the PU channel avoidance in PU regions is not taken into account (as in the existing D2CARP protocol), the transmission path may be created across PU regions (as depicted as the square-dot line from source (S) to destination (D)), which is extremely vulnerable to the impact of PU activities, especially in highly active PU regions. On the contrary, by avoiding using PU's channel in PU regions, the RACARP protocol establishes the transmission path as represented as the solid line from S to D in order to reduce service interruptions caused by PU activities.

In case both licensed and unlicensed channels are available in the network, to create a transmission path by avoiding PU territories may produce a large end-to-end delay due to the establishment of long detour. In such a case, the RACARP protocol may establish a transmission path which crosses the PU regions. However, the PU's channel is not used to deliver the data packets when crossing the PU regions (as shown in Figure 10(b)).

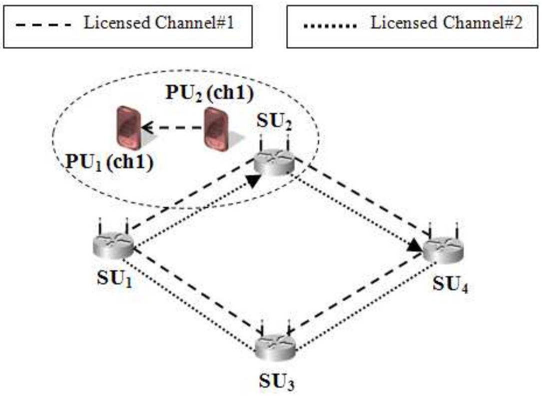
5.3 Exploitation of Joint Path and Spectrum Diversity

The RACARP protocol utilizes the joint path and spectrum diversity in routing process in order to provide multi-path and multi-channel routes. As a result, the source node is able to immediately switch among different paths and different channels in appearance of path failure during data transmission in order for fast route recovery. Therefore, the performance degradation caused by the activity of PUs can be alleviated.

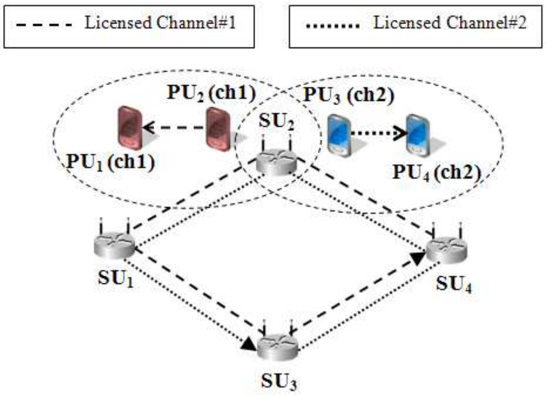
Figure 11(a), Figure 11(b) and Figure 11(c) depict the advantage of exploiting the joint path and spectrum diversity in the RACARP protocol. In the network as shown in Figure 11(a), after the route discovery process is successfully completed, SU_1 (source node) begins transmitting data packets along the optimal path with minimum EPD value (i.e. $SU_1 \xrightarrow{ch1} SU_2 \xrightarrow{ch2} SU_4$) towards SU_4 (destination node). During data delivery, in case SU_2 is moved into the PU_1-PU_2 region and the PU activity on channel#1 is detected (see Figure 11(b)), it notifies its neighbors (i.e. SU_1 and SU_4) of the PU activity detection and then SU_1 immediately uses another available channel (i.e. channel#2) to transmit data packets without changing path direction. Consequently, the new transmission path is $SU_1 \xrightarrow{ch2} SU_2 \xrightarrow{ch2} SU_4$. Afterwards, if SU_2 detects another PU activity over channel#2 (see Figure 11(c)), it must instantaneously disable the channel#2 for data transmission and notify its neighbors of the PU activity detection. Subsequently, since SU_2 is unable to operate over both channel#1 and channel#2, SU_1 immediately switches to another available path (i.e. $SU_1 \xrightarrow{ch2} SU_3 \xrightarrow{ch1} SU_4$) for data delivery without needing to trigger a new route discovery process.



(a) No PU Activity is Detected



(b) PU Activity over Channel#1 is Detected



(c) PU Activities over Channel#1 and Channel#2 are Detected

Figure 11: Advantage of Exploiting the Joint Path and Spectrum Diversity

6. PROTOCOL OPERATIONS

The key operations of the RACARP protocol include the route discovery, route maintenance and route recovery mechanism which are described below in further detail. Moreover, in our network model, we assume that each SU is equipped with multiple wireless interfaces. Each interface can only operate over one of non-overlapping channels.

6.1 Route Discovery

When a source node needs to transmit a data packet towards another node for which the routing information is unknown, it broadcasts an N-RREQ packet for the destination node to its neighbors through all its available channels (i.e. not used by a PU). An intermediate node which receives the first N-RREQ packet creates a routing table entry for a route towards the source node, called a reverse route, and records the channel, through which the packet has been transmitted, in its routing table. Afterwards, it re-broadcasts the packet via all its vacant channels (i.e. free from a PU). If an extra N-RREQ packet with the same sequence number received from the same node but on different channel, it creates another routing table entry of reverse route for that channel without rebroadcasting the packet. In such a way, the multi-channel reverse routes are established. The record of reverse route will be updated only if it receives an additional N-RREQ packet with a higher sequence number or the same sequence number but lower EPD value. The stale N-RREQ packet received by a node will be discarded to avoid the problem of routing loops.

The N-RREQ packet is re-broadcasted until it reaches the destination node or, alternatively, arrives at an intermediate node that has a record of a valid route towards the destination. In both cases, an N-RREP packet is generated and sent back to the previous node via the same channel that the N-RREQ packet has been received. Also, a further N-RREQ packet received from the same node but on different channels will not be ignored. However, if the destination node receives an extra N-RREQ packet from a different node and all the following conditions are satisfied: (1) RREQ’s First-Hop Node ID in the N-RREQ packet is different from First-Hop Node ID of reverse route entries in its routing table; (2) the ID of the node from which the N-RREQ packet has been received is different from Next-Hop Node’s ID of reverse route entries in its routing table; and (3) EPD value in the N-RREQ packet is less than or equal to the minimum EPD value of previously established reverse route entries in its routing table, it will create another routing table entry of reverse route for the channel through which the N-RREQ packet has been sent. As a result, the multi-path reverse routes are created.

In the route reply phase, an intermediate node which receives the first N-RREP packet creates a routing table entry for a route towards the destination node, referred to as a forward route, and records the channel, through which the N-RREP packet has been transmitted, in its routing table. Subsequently, it forwards the copies of the N-RREP packet back towards the source node through all its active reverse routes over available channels (i.e. not occupied by a PU). If an intermediate node receives an extra N-RREP packet from the same sender but on different channel, it creates another routing table entry of forward route for that channel and then re-forwards the N-RREP packet towards the source node only through its reverse route over the same channel. In this fashion, the multi-channel forward routes are built. Only in case a node receives a fresher or better N-RREP packet, which has a greater sequence number or the same sequence number with smaller EPD value, the forward route entry will be updated.

When an N-RREP packet arrives at the source node, a path from source to destination is created and the node can begin sending data packets. To have multi-channel forward routes, the source node will not discard the additional N-RREP packets received from the same sender but on different channels. Moreover, the multi-path forward routes can be also established in case it receives an extra N-RREP packet from a different sender under the following conditions: (1) RREP's First-Hop Node ID in the N-RREP packet is different from First-Hop Node ID of forward route entries in its routing table; (2) the ID of the node from which the N-RREP packet has been received is different from Next-Hop Node’s ID of forward route entries in its routing table; and (3) EPD value in the N-RREP packet is less than or equal to the minimum EPD value of previously established forward route entries in its routing table.

In addition, to avoid creating a transmission path using PU’s channel in PU regions with an aim to alleviate the impact of PU activities, a node inside a PU region always discards an N-RREQ and N-RREP packet received through the PU’s channel which is stored in its blocked channel list.

6.2 Route Maintenance and Recovery

As data packets flow from source to destination, each node over the transmission path updates the lifetime (i.e. expiration time) of its forward and reverse routes in order to maintain the link connectivity. However, if a route's lifetime is expired, the routing entry for that route will be invalid.

In the RACARP protocol, each SU sets a timer for every specific time to sense a PU activity. During data transmission, if a SU detects a PU activity, it is unable to transmit a data packet through the channel which overlaps the PU's transmission frequency, thus resulting in a link failure. For that case, the node responds to the failure by immediately selecting another available channel or path for data delivery without needing to trigger a new route discovery process. Afterwards, it broadcasts a Route ERRor Disable (RERR-D) packet to its all neighbors in order to notify them about the detection of PU activity. After the neighbor receives the RERR-D packet, it disables the routing table entry that meets the following conditions: (1) the ID of the RERR-D sender is the same as *Destination Node's ID* or *Next-Hop Node's ID* (for other destinations) in the routing table entry; and (2) *Channel Interface* in the routing table entry is the same as the PU's transmission channel. However, the previously disabled routing entries can be enabled again after the PU activity is stopped or finished. In such a case, a Route REQuest Enable (RREQ-E) packet will be broadcasted to notify all its neighbors to enable the routing entries that have been disabled due to the PU activity. Subsequently, the neighbor receiving the RREQ-E packet will generate a Route REPly Enable (RREP-E) packet and send back to the RREQ-E originator.

In addition, a link failure, which is detected by link-layer feedback, can result from not only PU activity but also node mobility, node fault, link degradation, etc. During data delivery, if a node detects a link breakage and no alternative available channel or path is found, after marking the broken route in its routing table as invalid, it generates an N-RERR packet and broadcasts it to all its neighbors. As the N-RERR packet propagates towards the source node, a node that receives the N-RERR packet invalidates all affected routing table entries. When the N-RERR packet arrives at the source node, a new route discovery process will be triggered.

7. SIMULATION CONFIGURATION

The performance evaluations were conducted using the NS-2 simulator [16] with an extension to support the CR environments. Table 1 summarizes the simulation parameters used for this study. In our simulations, we place 100 SUs and 10 PUs over a 1000m x 1000m terrain. The PU activities are modeled according to the ON/OFF process [6] with exponential distribution with parameter λ of 75, referred to as PU activity parameter. The ON state denotes the period where the channel is occupied by PU and the OFF state represents the period where the channel is available for SUs' communications. The transmission range of SU and PU is set to 150 m. The traffic load is modeled as CBR (Constant Bit Rate) data packets with size of 512 bytes at the packet interval of 50 ms over UDP connections. The duration of simulation run is 150 seconds. We specify the two-ray ground reflection model as the radio propagation type and the IEEE 802.11 is used for MAC protocol. Additionally, to calculate the updated ELD value of each link, an ETX and RTT probe packet are periodically broadcasted to the neighbors every 1 and 0.5 second respectively. The *ETX_PROBE_WINDOW* period is set to 10 seconds.

Table 1: Simulation Parameters

Parameter Name	Value
Simulation Area	1000 x 1000 m^2
Simulation Time	150 seconds
Number of SUs	100
Number of PUs	10
PU Activity Parameter (λ)	75
Number of Channels	4
Traffic Type	CBR
Data Packet Size	512 bytes
Data Packet Interval	Every 50 ms
MAC Layer	IEEE 802.11
Transport Layer	UDP
SU Transmission Range	150 m
PU Transmission Range	150 m
Radio Propagation	Two-Ray Ground Reflection
PU Activity Checking Interval	Every 5 seconds
Checking Interval for PU Channel Avoidance	Every 5 seconds
RTT Probe Interval	Every 0.5 second
ETX Probe Interval	Every 1 second
ETX Probe Window	10 seconds

8. SIMULATION RESULTS AND PERFORMANCE EVALUATION

The protocol performance is evaluated through simulations (with varying the number of data traffic connections) based on the performance metrics including average throughput, percentage of packet loss, average end-to-end delay, and average jitter. The NS2 Visual Trace Analyzer [14] is used to analyze the simulation results. To validate the performance improvement of RACARP protocol, we compared the simulation results with that of D2CARP protocol [13] under identical scenarios.

In Figure 12, we show the results of average throughput versus the different number of data traffic connections. The average throughput is defined as the ratio of the total amount of data successfully received by the destination to the time it takes from the data start time to the data stop time. From the figure, when the number of data traffic connections increases, the throughput results of both protocols also rise. However, RACARP protocol outperforms in all cases compared to D2CARP protocol. The RACARP takes account of the impact of packet losses and link delay for path selection as well as circumventing creating a path that uses PU's channel in PU regions for data delivery in order to alleviate the performance degradation caused by PU activities. Therefore, its transmission path is more robust than the one established by the D2CARP, thus leading to higher throughput results. In the network with 14 data traffic connections, the RACARP achieves a throughput enhancement of about 15.19% over the D2CARP protocol.

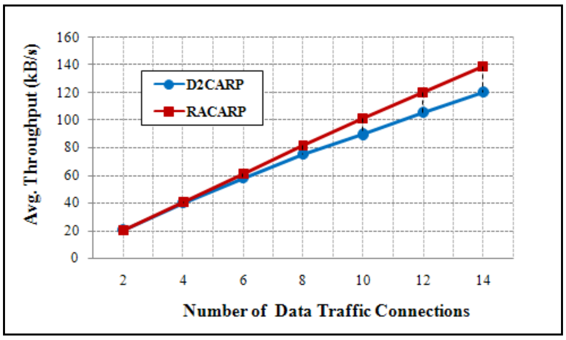


Figure 12: Simulation Results of Average Throughput

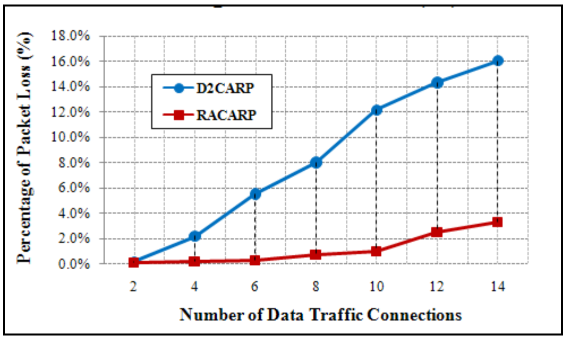


Figure 13: Simulation Results of Percentage of Packet Loss

Figure 13 exhibits the percentage of packet loss against the increased number of data traffic connections. For D2CARP protocol, it is obvious that the results of packet loss grow dramatically when increasing the number of data traffic connections. In contrast, the percentage of packet loss for RACARP protocol increases slowly in the same situations. In the RACARP, data packets are always transmitted through more robust path with less vulnerability to the impact of PU activity when compared to the D2CARP. Also, in presence of PU activity during data delivery, a SU operating over the channel which overlaps with the PUs' transmission frequency is able to immediately switch to another available channel or path for data transmission without severe service interruption. Therefore, the RACARP provides significantly lower number of dropped data packets than the D2CARP. In the network with 14 data traffic connections, the RACARP achieves a packet loss enhancement of about 79.15% over the D2CARP protocol.

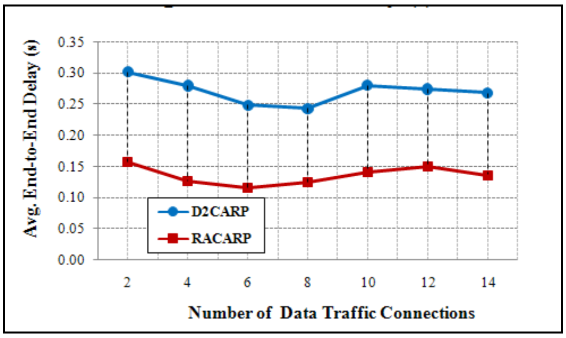


Figure 14: Simulation Results of Average End-To-End Delay

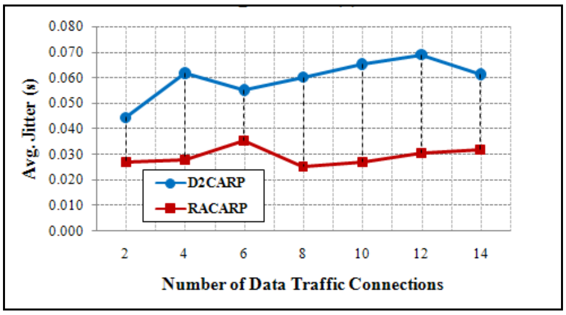


Figure 15: Simulation Results of Average Jitter

The results of average end-to-end delay versus the number of data traffic connections are presented in Figure 14. The average end-to-end delay is defined as the average time taken by data packets to be delivered across a network from source to destination. From the figure, it is observed that RACARP protocol enhances the average end-to-end delay more than D2CARP protocol. As expected, the RACARP utilizes the EPD routing metric. The EPD routing metric considers the link delay and the effect of packet loss for path decision, i.e. a path with lowest EPD value is chosen for data transmission. Therefore, a transmission path with highest quality in terms of link delay and packet loss probability is always selected. On the contrary, the minimum hop count which is used as a routing metric in the D2CARP is unable to reflect the accurate quality of transmission path, especially in terms of latency, hence causing higher end-to-end delay results. In the network with 14 data traffic connections, the RACARP achieves an end-to-end delay enhancement of about 48.94% over the D2CARP protocol.

Figure 15 displays the simulation results of both protocols in terms of the average jitter by varying the number of data traffic connections. The average jitter is defined as the average of the variation in time between data packets arriving at the destination. Although the figure shows the fluctuation in the results of average jitter as the number of data traffic connections increases, RACARP protocol provides better performance than D2CARP protocol. The reason is that the RACARP takes account of PU's channel avoidance in PU regions and utilizes the joint path and spectrum diversity in the route discovery process. As a result, the data packets are not delivered through PU's channel when crossing PU regions to mitigate the impact of PU activity. Furthermore, by utilizing the multi-path multi channel routes, the protocol keeps the data transmission process still running continually even in presence of path failure. On the other hand, as compared to the RACARP, a transmission path created by the D2CARP is more vulnerable to the impact of PU activities, thus resulting in more frequent communication interruptions which produce higher average jitter results. In the network with 14 data traffic connections, the RACARP achieves a jitter enhancement of about 48.42% over the D2CARP protocol.

9. CONCLUSION

CR technology has emerged as a promising solution to deal with the spectrum shortage problem and improve the efficiency of spectrum usage. Due to the unique characteristics of CRAHNs, the novel routing protocols designed and developed to match the dynamic nature of such networks are required.

In this paper, we have proposed the RACARP protocol which is a robustness aware routing protocol for CRAHNs. Also, the EPD routing metric used for path decision in the RACARP has been introduced. The metric takes account of the link delay and the effect of packet loss on wireless links. In addition, the protocol circumvents creating a path that uses PU's channel in PU regions for data transmission in order to alleviate the impact of PU activities that can cause frequent communication interruptions. Moreover, the protocol exploits the joint path and spectrum diversity in routing process to provide multi-path multi-channel routes with an aim to offer fast route recovery in appearance of path failures caused by PU activities during data delivery. Furthermore, we have evaluated the protocol performance through simulations using NS-2 simulator. The performance comparison between the RACARP and D2CARP protocol has been presented. The simulation results have confirmed that the RACARP outperforms the D2CARP by achieving higher average throughput, reducing the number of dropped data packets, providing lower average end-to-end delay, and decreasing the average jitter in identical conditions. However, as compared to D2CARP protocol, the RACARP protocol may produce more routing overhead and additional complexities to the networks. In terms of future work, the integration of the RACARP protocol and the testbed implementation with cognitive radio devices will be conducted in order to validate the findings and refine the system.

10. ACKNOWLEDGMENT

This research project is based upon work supported by the Research Management Center (RMC) at the International Islamic University Malaysia (IIUM). The authors would like to thank all members of the research group for their support.

REFRENCES:

[1] I.F. Akyildiz, W.-Y. Lee, and K.R. Chowdhury, "CRAHNs: Cognitive Radio Ad Hoc Networks", *Ad Hoc Networks*, Vol. 7, No. 5, 2009, pp. 810-836.

[2] 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*, Vol. 50, No. 13, 2006, pp. 2127–2159.

[3] I. Beltagy, M. Youssef, and M. El-Derini, "A New Routing Metric and Protocol for Multipath Routing in Cognitive Networks", *Proceedings of the IEEE Wireless Communications and Networking Conference*

(WCNC), Quintana Roo, Mexico, March 28-31, 2011, pp. 974-979.

[4] A.S. Cacciapuoti, C. Calcagno, M. Caleffi, and L. Paura, "CAODV: Routing in Mobile Ad-Hoc Cognitive Radio Networks", *Proceedings of the 3rd IFIP Wireless Days Conference (WD)*, Venice, Italy, October 20-22, 2010, pp. 1-5.

[5] M. Cesana, F. Cuomo, and E. Ekici, "Routing in Cognitive Radio Networks: Challenges and Solutions", *Ad Hoc Networks*, Vol. 9, No. 3, 2011, pp. 228-248.

[6] K.R. Chowdhury and M.D. Felice, "SEARCH: A Routing Protocol for Mobile Cognitive Radio Ad-Hoc Networks", *Computer Communications*, Vol. 32, No. 18, 2009, pp. 1983-1997.

[7] T.H. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", *RFC 3626*, Internet Engineering Task Force (IETF), 2003.

[8] FCC's Spectrum Policy Task Force, "Report of the Spectrum Efficiency Working Group", *Technical Report*, Federal Communications Commission (FCC), 2002.

[9] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications", *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 2, 2005, pp. 201-220.

[10] D.B. Johnson, Y.-C. Hu, and D.A. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", *RFC 4728*, Internet Engineering Task Force (IETF), 2007.

[11] C.E. Perkins, E.M. Belding-Royer, and S.R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing", *RFC 3561*, Internet Engineering Task Force (IETF), 2003.

[12] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", *ACM SIGCOMM Computer Communication Review*, Vol. 24, No. 4, 1994, pp. 234-244.

[13] M.A. Rahman, M. Caleffi, and L. Paura, "Joint Path and Spectrum Diversity in Cognitive Radio Ad-Hoc Networks", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2012, No. 1, 2012, pp. 1-9.

[14] F. Rocha, "NS2 Visual Trace Analyzer", 2012. *Available at: http://nsvisualtraceanalyzer.wordpress.com*.

[15] S. Sengupta and K.P. Subbalakshmi, "Open Research Issues in Multi-Hop Cognitive Radio Networks", *IEEE Communications Magazine*, Vol. 51, No. 4, 2013, pp. 168–176.

[16] The VINT Project, "The Network Simulator - NS-2", 1995. *Available at: http://www.isi.edu/nsnam/ns/index.html*.

[17] G.-M. Zhu, I.F. Akyildiz, and G.-S. Kuo, "STOD-RP: A Spectrum-Tree Based On-Demand Routing Protocol for Multi-Hop Cognitive Radio Networks", *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, New Orleans, LA, USA, Nov. 30 - Dec. 4, 2008, pp. 1-5.