A novel routing protocol for cognitive radio networks with cooperation process

Sunwoo Kim[1], Dohoo Pyeon[1], Ingook Jang[1] and Hyunsoo Yoon[1]
[1] Department of Computer Science, Korea Advanced Institute of Science and Technology
Daejeon, Korea
[E-mail: swkim, dhpyeon, ikjang, hyoon@nslab.kaist.ac.kr]
*Corresponding author: Ingook Jang

Received June 2, 2014; revised October 10, 2014; accepted October 22, 2014; published November 30, 2014

Abstract

Cognitive radio networks (CRNs) are composed of mobile users who can use multiple spectrum bands for communication. CRNs allow unlicensed users (called *cognitive users*) to efficiently utilize unused licensed spectrums without interfering with communications of licensed users (called *primary users*). The main goals of CRNs are to mitigate spectrum saturation and to improve spectrum utilization. This paper introduces state-of- the-art routing protocols for CRNs and addresses some limitations of these protocols. To resolve the limitations, we suggest a new research direction for routing protocols in CRNs. We implement our protocol to compare with the existing routing protocols for multi-hop CRNs. Our protocol shows good performance compared to the existing routing protocols in terms of network performance and PU protection.

Keywords: Cognitive radio networks, routing protocol, cooperation

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government (MEST) (No. 2014R1A2A2A01006957) and the IT R&D program of MKE/KEIT [10041244, SmartTV 2.0 Software Platform].

http://dx.doi.org/10.3837/tiis.2014.11.011

1. Introduction

Most of the existing wireless networks operate based on a fixed spectrum assignment policy. To obtain a right (license) for use of a spectrum, a company or an organization should participate in spectrum auction. The possession of the right allows the entity to transmit signals over a *licensed spectrum*. On the other hand, an *unlicensed spectrum* is not regulated by the government. In recent years, the unlicensed spectrums have been saturated due to an increasing demand for wireless devices and applications such as wireless sensor networks (WSNs), wireless local area networks (WLANs), and wireless ad-hoc networks (WAHNs). However, most of the licensed spectrums are still under-utilized despite the increasing demand [1].

Since the existing wireless networks suffer from the spectrum inefficiency problem, *dynamic spectrum access* (*DSA*) has been proposed [2]. DSA enables unlicensed users to use multiple spectrums including licensed spectrums when licensed users do not use the licensed spectrums. Therefore, DSA significantly improves the spectrum utilization.

Cognitive radio networks (*CRN*s) are telecommunication networks designed to improve the spectrum utilization, which are composed of multiple mobile users who have DSA devices. CRNs generally consist of two different networks [3]. The first one is a *primary network* that utilizes the licensed spectrums. Users of the primary network (called *primary users* (*PU*s)) have a high priority to use the licensed spectrums. The second one is a cognitive radio network which consists of unlicensed users called *cognitive user*s (*CU*s) or *secondary user*s (*SU*s). CUs have possibility to interfere with PU communications when CUs use the licensed spectrums. Therefore, CUs must carefully access the licensed spectrums in order to avoid interfering with PU communications.

CRNs are classified as centralized CRNs and decentralized CRNs [3], as shown in **Fig. 1**. **Fig. 1 (a)** shows centralized CRNs which have a central entity. The role of the central entity is similar to that of an access point (AP) in WLANs and a base-station in cellular networks. Each CU collects data related to the PU communication and transmits the data to the central entity. The central entity informs CUs of the best spectrums after processing the received data. Each CU reconfigures its device to use the best spectrums according to the information from the central entity. In centralized CRNs, protecting the PU communication is easily achieved by the central entity. However, the communication overhead of the central entity significantly increases as the number of CUs in a network increases.

Unlike centralized CRNs, decentralized CRNs have no central entity. Each CU should select a spectrum that it operates on without the aid of a central entity. It is hard for CUs to protect PUs due to lack of information of the PU communication. Therefore, cooperation between CUs must be needed in decentralized CRNs [3]. Each CU collects and processes the data by itself, as shown in **Fig. 1 (b)**. Then, CUs exchange their information with each other. Each CU decides the best spectrum and reconfigures its device by using the information from other CUs.

Since the existing works are mainly based on centralized CRNs, most of the research focuses on issues for managing spectrums and reducing a complexity in a central entity. These research works for centralized CRNs are not appropriate for decentralized CRNs because centralized CRNs are based on single-hop transmissions between the CU and the central entity. Therefore, it is necessary to research higher-level issues for multi-hop transmissions in

decentralized CRNs. In this paper, we introduce and summarize some existing routing protocols for CRNs. We also suggest a new research direction for routing protocols for multi-hop CRNs.

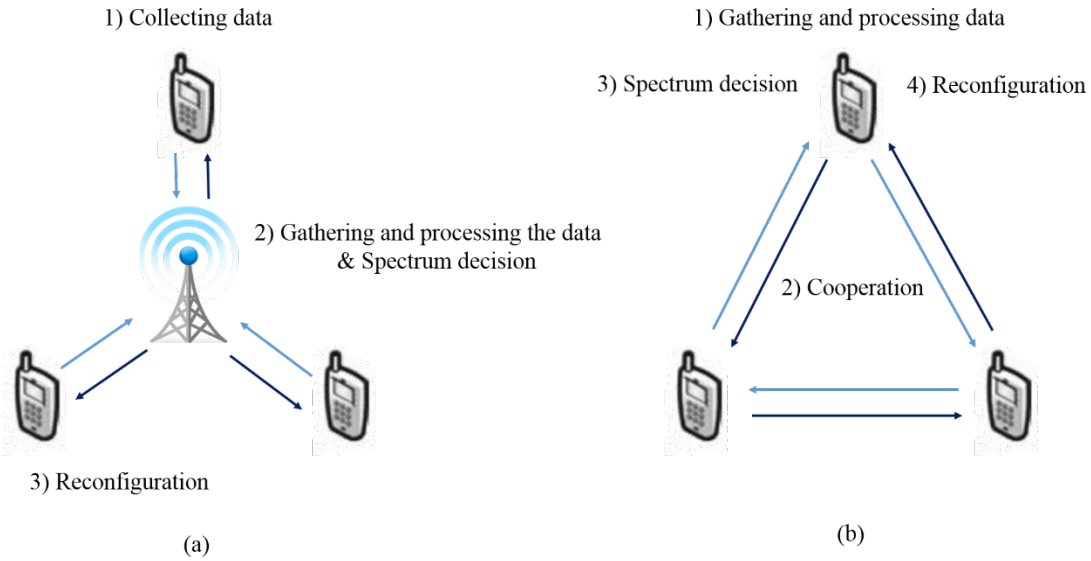


Fig. 1. (a) Centralized CRNs and (b) decentralized CRNs

The rest of this paper is organized as follows. Section 2 presents routing issues in CRNs. We introduce some existing routing protocols in Section 3 and suggest a new research direction for routing protocols for multi-hop CRNs in Section 4. We compare our protocol with the existing routing protocols by simulation in Section 5. Finally, conclusions and future works are given in Section 6.

2. Design issues of a routing protocol in cognitive radio networks

A routing protocol for decentralized CRNs must be designed to deal with three issues: (i) deciding the best path, (ii) exchanging a control packet, and (iii) route maintenance [16].

The first issue is how to decide the best routing path between two CUs. In the existing wireless networks, routing protocols consider network performance metrics such as hop count, throughput, and end-to-end delay. However, it is necessary to guarantee the quality of service (QoS) of primary users who have a priority to access the licensed spectrums in CRNs. Routing protocols should consider the interference and the collision caused by cognitive technique [15].

The second one is how to exchange control packets between CUs. Decentralized CRNs do not have a central entity, so CUs must exchange control packets with each other to avoid interfering with PU communications. A common control channel approach can be used for exchange of control packets. CUs simply exchange their control packets through the common control channel. However, it is not suitable to be used in CRNs due to performance degradation in unlicensed spectrums and PU interference in licensed spectrums [7]. Thus, a routing protocol for CRNs must consider exchange of control packets in an environment where CUs' operating channels dynamically change.

The third issue is route maintenance. Unlike routing protocols for the existing wireless networks, a routing protocol for CRNs should consider not only mobility of the CUs but also sudden appearance of PUs. When a CU detects the PU communication during a transmission, it pauses its transmission and tells the appearance of the PU to other CUs. Then, the CU finds an alternative route to continue the halted transmission.

3. Related work

Decentralized wireless networks generally adopt reactive (on-demand) routing protocols instead of proactive routing protocols. Proactive routing protocols should maintain a table which contains next-hop information of all nodes, so they are not appropriate to mobile networks where topologies frequently change. On the other hand, reactive routing protocols find a route only when a sender and a receiver want to communicate. Thus, overhead of maintaining the table is not required. Most of routing protocols in decentralized CRNs stand on the ad-hoc on-demand distance vector routing protocol (AODV) which is one of the most famous reactive routing protocols.

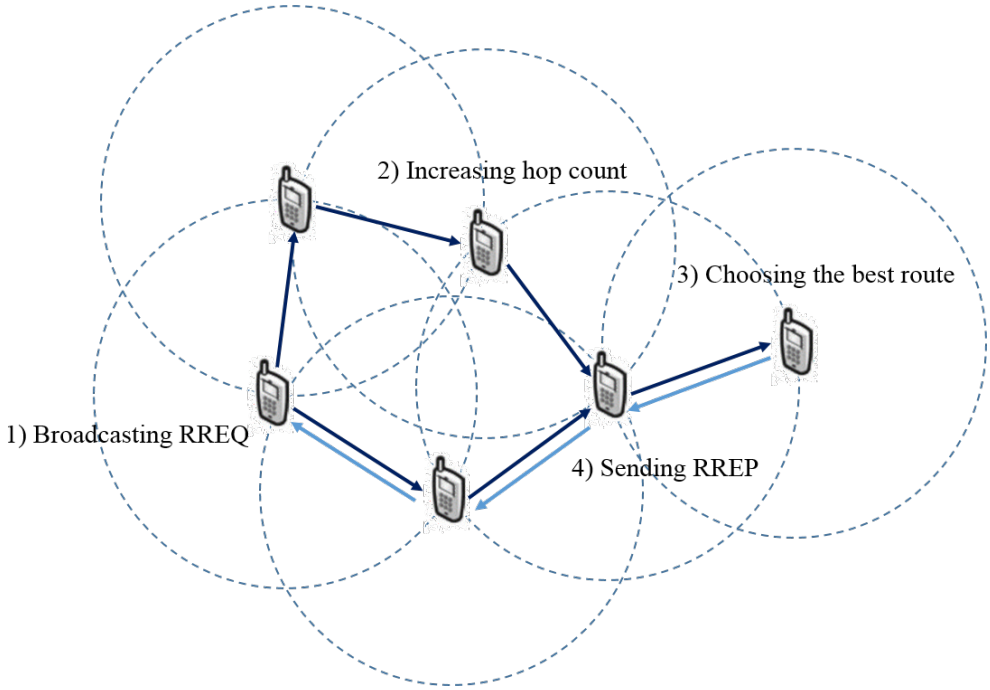


Fig. 2. Path formation procedure of AODV

3.1 AODV: ad-hoc on-demand distance vector routing [8]

AODV is a fundamental routing protocol in wireless ad-hoc networks. AODV uses hop count as a metric to find the best route to a destination node. **Fig. 2** illustrates the procedure of AODV. A source node broadcasts a route request (RREQ) packet. After receiving the RREQ packet, each intermediate node increases a hop count value in the RREQ packet and rebroadcasts it. A destination node receives multiple RREQ packets and chooses a route which has a minimum hop count value. The destination node sends a route reply (RREP) packet to the source node through nodes along the selected route.

3.2 CAODV: routing in mobile ad-hoc cognitive radio networks [9]

CAODV is a modified version of AODV for CRNs. A node transmits a RREQ packet through all licensed channels where the PU communication is not detected. However, this mechanism can cause hidden primary user problem [3] [13]. **Fig. 3** shows the hidden primary user problem of CAODV. In CRNs, a node generally uses an energy detection method to detect the PU communication. A node CU_y in the PU transmission range can detect the PU transmitter, but a node CU_x cannot detect the PU transmitter. If CU_x chooses a spectrum used by PU transmitter and transmits the data through the spectrum, CU_x has a possibility to interfere with PU receivers inside the PU transmission range. Hence, transmitting a RREQ packet through licensed spectrums may interfere with the PU communication.

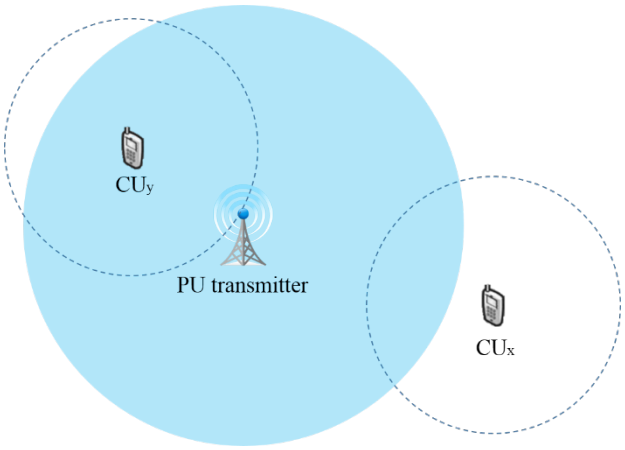


Fig. 3. Hidden primary user problem

3.3 SEARCH: a routing protocol for mobile cognitive radio ad-hoc networks [10]

The main idea of SEARCH is to find multiple routes which have a minimum hop count value. SEARCH uses a greedy algorithm by using location information. SEARCH also takes a PU transmission range into account. However, SEARCH does not consider stochastic activity of PUs. In addition, it operates only when every node knows other nodes' location.

3.4 CRP: a routing protocol for cognitive radio ad hoc networks [11]

CRP suggests two different routing approaches for CRNs based on their service difference. The first one focuses on network performance such as hop count, end-to-end delay, and throughput. The second one focuses on PU protection. CRP suggests novel metrics to decide the best route, considering stochastic PU activity.

CRP is composed of two stages. In the first stage, each node chooses the best spectrum by using some metrics such as effective time available for transmission, propagation distance, and overlapped area of transmission range between PU and CU. The performance-centric routing approach uses the propagation distance and the available transmission time to reduce hop count and end-to-end delay. The PU-protection-centric routing approach uses the overlapped area to minimize PU interference. CUs choose the best spectrum by using these metrics depending on service demand (network performance or PU protection).

The second stage is to select next hop. Based on the metrics, a source node broadcasts a

RREQ packet after delay time. If a chosen spectrum has bad metric values, the delay time increases. A destination node knows that the earliest arriving RREQ packet passes through the best route. The destination node sends a RREP packet to the source node through nodes along the best route.

CRP shows great performance in terms of throughput in the performance-centric protocol and PU protection in the PU-protection-centric protocol, respectively. However, CRP assumes that every node knows the location of PU transmitters and the sensing schedule of CUs. This assumption is quite unrealistic.

3.5 LAUNCH: a location-aided routing protocol for cognitive radio networks [12]

Authors of [12] propose a location-aided routing protocol that considers stochastic PU activity and provides a stable route. The core of LAUNCH is a channel locking method for route stability. The procedure of route setup is as follows.

LAUNCH assumes that every node knows the location of a destination node. Each node considers propagation time, channel switching time, and spectrum availability to decide the best spectrum. A source node broadcasts a RREQ packet through a channel in the best spectrum. Only intermediate nodes closer to the destination node send a RREP packet to the source node. The source node chooses the best next hop among intermediate nodes, and then sends a route configure (RCONF) packet to the best next hop node. The node receiving the RCONF packet locks the channel and sends a route acknowledge (RACK) packet to the source node. This procedure is repeated until the RREQ packet reaches the destination node.

The authors say that LAUNCH is a modified version of SEARCH. However, LAUNCH assumes that every node can obtain the location information of a destination node by using global positioning system (GPS). This assumption is hard to be implemented in the real world if service providers do not provide external database centers.

3.6 Reactive routing for mobile cognitive radio ad-hoc networks [13]

Authors of [13] suggest two modified versions of CAODV. The first one is inter-route diversity CAODV (ERI-CAODV) which finds several routes where each route uses only one channel. The second one is intra-route diversity CAODV (ARI-CAODV) which finds one route with multiple channels. ERI-CAODV shows better performance in terms of route formation than ARI-CAODV, but ARI-CAODV can recover a broken route faster than ERI-CAODV by simply switching a channel. However, both ARI-CAODV and ERI-CAODV only depend on local information gathered by nodes, so it is hard to protect the PU communication. Furthermore, the hidden primary user problem shown in **Fig. 3** still exists [3].

3.7 Summary

Table 1. Summary of existing routing protocols

Protocols	Strength	Weakness
CAODV	•Simple extension of AODV for cognitive radio networks	•Weak PU protection
SEARCH	•Greedily finding a route to a destination	•Not considering stochastic PU activity

LAUNCH	•Finding stable a route to a destination •Minimizing switching time	•Requiring GPS and external DB centers
CRP	•Providing the tradeoff between network performance and PU protection •Dealing with wide issues for cognitive radio networks	•Using a common control channel •Global state information of PU transmitter location and CU schedule
ERI-CAODV ARI-CAODV	•No common control channel •Using local information	•Weak PU protection •Hidden primary user problem

Table 1 shows the summary of the existing routing protocols for CRNs. SEARCH, CRP, and LAUNCH use global location information of other nodes and PU transmitters for PU protection, so these protocols are hard to be implemented in the real world. On the other hand, other reactive routing protocols for CRNs such as CAODV, ERI-CAODV, and ARI-CAODV use only local information. However, it is hard to protect the PU communication because nodes only use the local information.

To resolve the aforementioned limitations such as use of global scope information and the hidden primary user problem, we suggest a novel routing protocol including a *cooperation process* to protect PU efficiently.

4. Proposed protocol

4.1 Procedure of route formation

In our proposed protocol, a cooperation process is composed of two stages: (i) *information request stage* and (ii) *route setup stage*. In the information request stage, each node collects information of spectrum availability from one-hop neighbor nodes. We assume that each node in CRNs knows on/off-time of channels through spectrum sensing [14]. The on-time means the period when a channel is used by PU, and the off-time means the period when the channel is idle. The channel availability is calculated as follows:

$$p_i = \frac{\frac{1}{\beta_i}}{\frac{1}{\alpha_i}+\frac{1}{\beta_i}} = \frac{\alpha_i}{\alpha_i+\beta_i} \tag{1}$$

where p_i is the channel availability of the ith channel, and $\frac{1}{\alpha_i}$ and $\frac{1}{\beta_i}$ are average periods of on/off-time, respectively. A spectrum is composed of multiple channels, as shown in **Fig. 4**. The spectrum availability is calculated as follows:

$$P_k = \prod_n p_i \tag{2}$$

where P_k is the spectrum availability of kth spectrum and n is the number of channels comprising the kth spectrum. The spectrum availability represents the condition of spectrums.

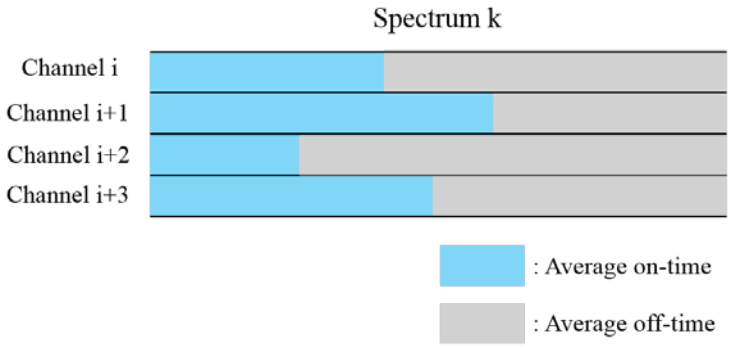


Fig. 4. Concept of the spectrum availability

Each node obtains the spectrum availability by using periodic spectrum sensing and maintains a table which contains the average frequency of spectrum usage. It helps to mitigate interference and reduce the number of collisions in PU transmissions caused by a cognitive technique.

After collecting the spectrum availability, each node exchanges this information with one-hop neighbor nodes by using a dedicated common control channel (CCC). The procedure of spectrum information exchange is shown in **Fig. 5**. A source node broadcasts an information request (IREQ) packet to its neighbor nodes. After receiving this IREQ packet, each neighbor node puts its spectrum availability into an information reply (IREP) packet. The source node gathers the spectrum information from multiple IREP packets and makes a table which contains the average of the spectrum availability.

Spectrum information table

Spectrum	Spectrum availability
A	P_A
B	P_B
C	P_C
D	P_D

1) Broadcasting an IREQ packet 2) Receiving IREP packets 3) Updating a table

Fig. 5. Procedure of IREQ/IREP exchange in the information request stage

The second stage is the route setup stage. The procedure of the second stage is similar to that of AODV, but our protocol considers a variety of spectrums to protect PU communications. **Fig. 6** shows the flow chart of the route setup stage. A source node or an intermediate node examines its spectrum information table before sending a RREQ packet. If the table is up-to-date, the node sends a RREQ packet through the best spectrum that has the largest value of the spectrum availability in its spectrum information table. Otherwise, the node updates its spectrum information table before sending a RREQ packet. Every node receiving the RREQ packet repeats the same procedure until the RREQ packet arrives at a destination. Our protocol exploits arrival time of RREQ and hop count as routing metrics. The destination node

considers those two metrics to determine the best route from the source node to itself. The destination node sends a route reply (RREP) packet to the source node through nodes along the selected route.

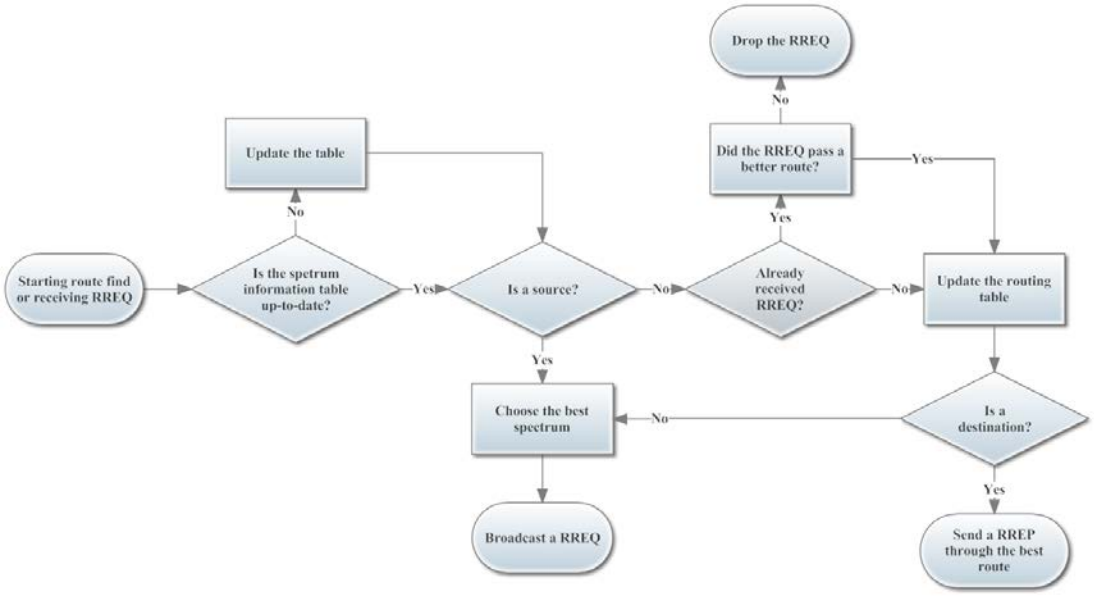
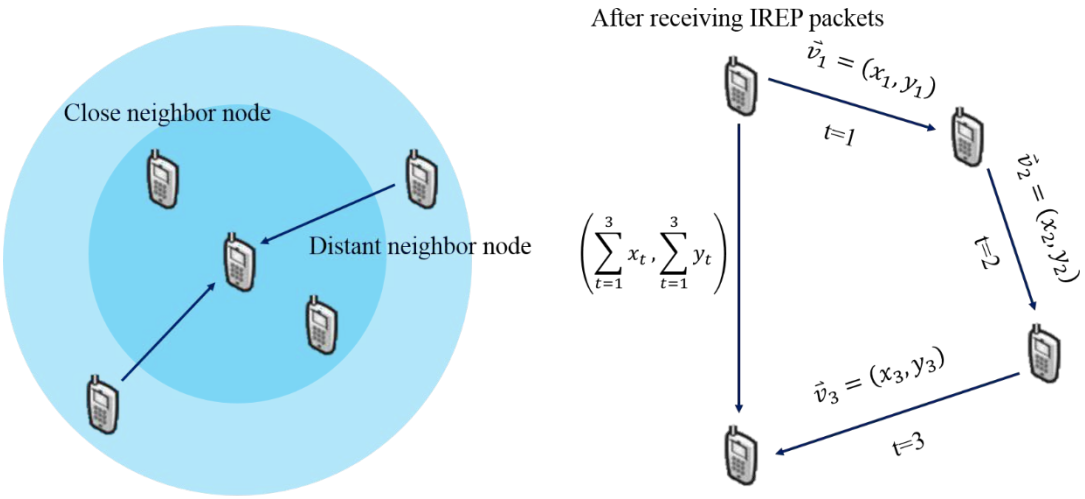


Fig. 6. Flow chart of the route setup stage

4.2 Policies to reduce control packet overhead

IREQ/IREP exchange may cause huge overhead in dense networks, so our protocol provides two policies in order to reduce the overhead.



(a) (b)

Fig. 7. Two policies to reduce overhead: (a) location based policy and (b) distance based policy

The first policy is to reduce overhead by using location information of nodes, as shown in **Fig. 7 (a)**. The spectrum information from distant neighbor nodes may involve a large area of the spectrum availability. However, the spectrum availability of close neighbor nodes is

similar to that of a source node which sends IREQ packets. Hence, IREP packets from close neighbor nodes have a high probability to contain the redundant spectrum availability. To reduce unnecessary IREP packet transmissions, our protocol proposes a new reply mechanism that allows neighbor nodes to send IREP packets adaptively. Neighbor nodes receiving an IREQ packet from a source node calculate the distance from the source node by using a simple path loss propagation model:

$$D_{x,y} = \left[\left(\frac{c}{4\pi f_k}^2\right)\frac{P_{tx}^{CU}-P_{rx}^{CU}}{P_{rth}^{CU}}\right]^{\frac{1}{\beta}} \quad (3)$$

where $D_{x,y}$ is the distance between a sender x and a receiver y, $\frac{1}{\beta}$ is an attenuation constant, c is the speed of the light, f_k is the frequency of a chosen channel, P_{tx}^{CU} is the maximum transmission power at x, P_{rx}^{CU} is the received signal strength at y, and P_{rth}^{CU} is the power threshold of the receiver. If a distance between a sender and a receiver is longer than a *distance threshold*, the receiver regards itself as a distant neighbor node. The distant neighbor node puts the distance into an IREP packet and immediately sends the IREP packet to the source node. If the distance is shorter than the distance threshold, the receiver determines itself as a close neighbor node. The close neighbor node waits for a fixed amount of time (T_{wait}) to overhear IREP packets from the distant neighbor nodes. If the close neighbor node overhears one or more IREP packets from the distant neighbor nodes, it does not send an IREP packet. Otherwise, the close neighbor node transmits an IREP packet. The distance threshold value can be adjusted by a network operator and we will shows the performance results by changing this threshold value in Section 5.

The second policy is to reduce overhead by using the distance between nodes, as shown in **Fig. 7. (b)**. Frequent broadcasting of IREQ packets causes a huge amount of control packet transmissions, so we suggest an IREQ broadcasting policy based on the distance between nodes. In our protocol, each node makes a table which traces its movement by using an accelerometer and an indicator. When a node updates its spectrum availability table after receiving IREP packets, it calculates a velocity vector based on its current location every second. While the node moves around, it continuously accumulates vectors and calculates a *norm* (distance). When the norm is bigger than a *norm threshold*, it sends an IREQ packet to its neighbor nodes to update the table. Otherwise, the node does not broadcast an IREQ packet and uses the existing spectrum availability table.

Our protocol exploits additional two control packets (IREQ and IREP) to make up for the weak points of the existing routing protocols. Although PU protection becomes better by using IREQ and IREP, other network performance can be degraded due to increase in the number of control packets. Since there is a trade-off between PU protection and network performance, transmitting control packets should be efficiently conducted without loss of PU protection. Our aforementioned two policies to reduce control packet overhead helps to improve network performance with guarantee of PU protection.

5. Performance evaluation

5.1 Simulation environment

We implement our protocol in the *ns-2* simulator with a multi-channel multi-radio extension. The simulation parameters are shown in **Table 2**.

Table 2. Simulation parameters in ns-2

Parameter	Value range	Nominal value
Number of spectrums	5	5
Number of PUs	100	100
Number of CUs	100, 150, 200, 250, 300	200
CU transmission range (m)	125	125
PU transmission range (m)	165	165
Effective Bandwidth (Mbps)	10	10
Packet size (KB)	1	1
Area size (square meter)	1000	1000
Node speed (m/s)	0 to 2	Randomly
MAC	802.11	802.11
Channel switching time (μs)	200	200
Distance threshold (m)	25, 50, 75, 100, 125	75
Norm threshold (m)	25, 50, 75, 100, 125	75
T_{wait}	0.1	0.1
On time	0, 0.2, 0.4, 0.6, 0.8, 1.0	0.5
Off time	0, 0.2, 0.4, 0.6, 0.8, 1.0	0.5

We adopt the simulation parameters used in [11] and use a network topology shown in **Fig. 8**. The area of a region is 1000 square meters, and the region is divided into 9 square cells. In the center of each cell, there is a PU transmitter which has a transmission range of 165m. 100 PU receivers and 200 CUs are randomly distributed in the region and each CU has a transmission range of 125m. PUs and CUs use the IEEE 802.11b transmission standards and the Two-Ray Ground propagation model. PU receivers are fixed in the topology and CUs keep moving with speed between 0 and 2 m/s. There are 5 different spectrum bands and each band has a 10Mbps channel. We generate random traffic models with CBR data packets which are 1000 bytes long. We use UDP connections to transmit the data packet.

We compare our protocol with the PU-protection-centric CRP (represented as CRP-II) and ERI-CAODV. The performance results focus on the (i) network performance, (ii) PU receiver protection, and (iii) impact of policies to reduce control packet overhead.

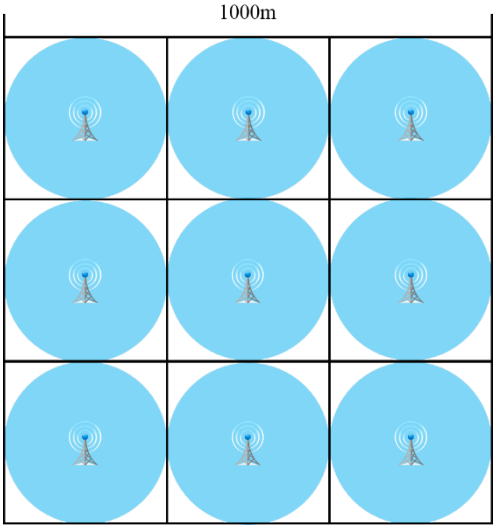


Fig. 8. A topology for simulation

5.2 Network performance

In this section, we evaluate the network performance of three routing protocols with varying the distance between the source and destination node. **Fig. 9 (a)** shows the packet delivery ratio of three protocols. This graph shows the route stability and quality of chosen spectrums. CRP-II shows the best performance by using the global scope information of the PU transmitter location and schedules CUs. Since, however, ERI-CAODV does not use any additional information, it shows relatively low performance with respect to CRP-II. Our protocol collects the spectrum availability from neighbor nodes to make up for lack of the spectrum information, so our protocol shows better performance than ERI-CAODV. The results of our protocol are close to that of CRP-II. **Fig. 9 (b)** shows the results of the average hop count. CRP-II chooses a next hop node which has the minimum overlapped area. Therefore, the average hop count increases significantly as the distance between source nodes and destination nodes increases. The result of ERI-CAODV and our protocol shows better performance than CRP-II from 100m to 200m of distances between source and destination nodes. Our protocol and ERI-CAODV increase hop count because of PU interference and collision as the distance increases. Since, however, each node in our protocol maintains its spectrum information table, our protocol shows better performance than ERI-CAODV in long distances (i.e. 300m) between source and destination nodes.

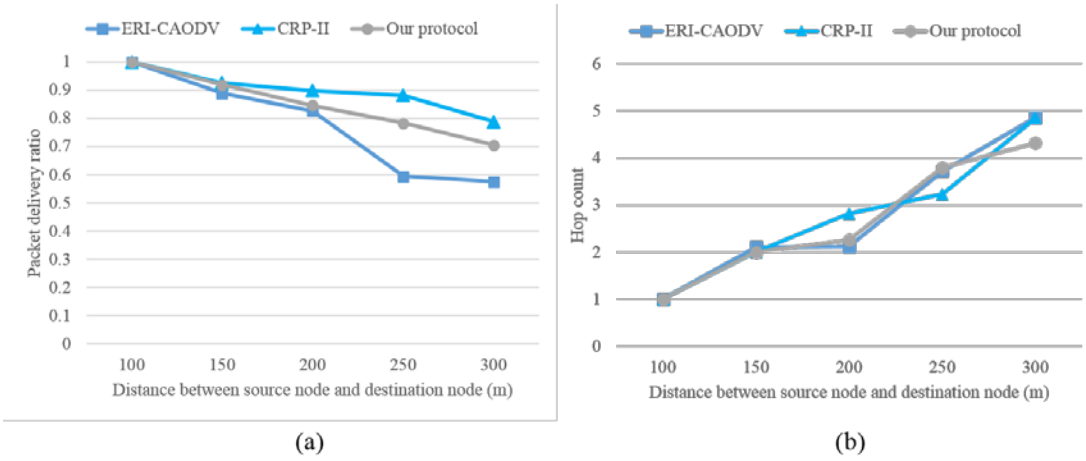


Fig. 9. (a) Packet delivery ratio and (b) average hop count

5.3 PU protection

To evaluate PU protection, we measure the collision risk ratio which is the value of ratio between the total number of transmissions and the total number of collisions caused by CUs at PU receivers. In this experiment, we vary the probability of spectrum bands being under PU activity in a cell. **Fig. 10** shows the results of the collision risk ratio. CRP-II shows the best performance in PU protection because CRP-II assumes that every node knows the spectrum availability and the location of PU transmitters. The result of our protocol shows better performance than that of ERI-CAODV and is very close to that of CRP-II. This experiment shows that the cooperation process improves PU protection and reduces the hidden primary user problem [3] [13].

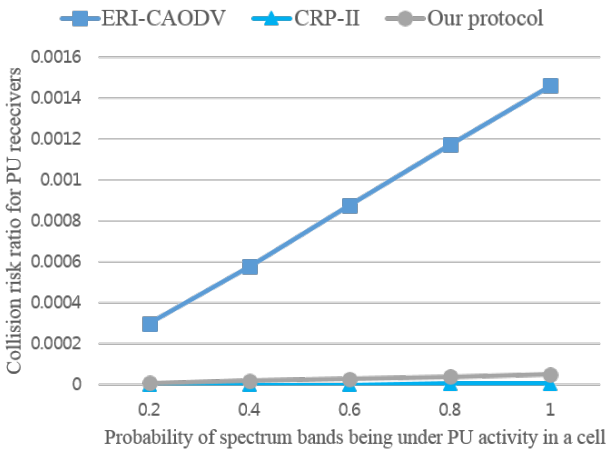


Fig. 10. Collision risk ratio for PU receivers

5.4 Control (IREQ and IREP) packet overhead

In this section, we measure the control packets overhead (IREQ/IREP and RREQ/RREP) in various distances between source and destination nodes. **Fig. 11** shows the control packet overhead of our protocol with two reduction policies discussed in Section 4.2. The x-axis represents the distance between source and destination and the y-axis represents the number of generated control packet per second. The results of three protocols increase as the distance between source and destination nodes becomes longer because a huge number of RREQ and RREP packets are generated in long distance communications. Since our protocol exploits additional control packets (IREQ and IREP), our protocol shows worse performance than ERI-CAODV and CRP-II in short distance communications. However, IREQ and IREP control packets helps to reduce the number of RREQ and RREP packets in long distance communications. Therefore, our protocol outperforms ERI-CAODV and CRP-II in long distance communications.

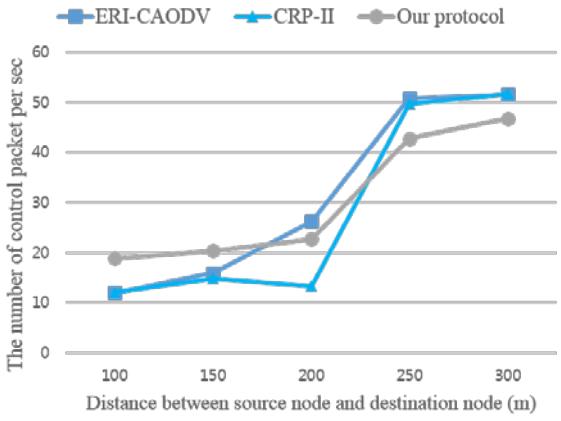


Fig. 10. The number of control packet per sec

5.5 Control packet reduction policies

In this section, we measure the control packet overhead and the collision risk ratio for PU protection to show reasonability of our policies. **Fig. 11** shows the control packet overhead and the collision risk ratio for PU protection according to the location based policy mentioned in Section 4.2. We vary the distance threshold from 25m to 125m. As the threshold increases, the number of IREQ and IREP packets decreases, as shown in **Fig. 11(a)**. When nodes use short distance thresholds (e.g. 25m and 50m), spectrum information received from close neighbor nodes is similar to that which a source node already had. So the collision risk ratio is relatively high due to hidden primary user problem, as shown in **Fig. 11(b)**. When nodes use long distance thresholds (e.g. 100m and 125m), less or no spectrum information from distant neighbor nodes is delivered to a source node. In this case, the collision risk ratio is relatively high because a source node does not have enough spectrum information. Our protocol shows the best performance of PU protection when we set the distance threshold to 75m.

Fig. 12 shows the control packet overhead and the collision risk ratio for PU protection according to the distance based policy. In this simulation, we set the average node speed value to 1.0 m/s. As the norm threshold decreases, the number of IREQ and IREP packets significantly increases due to frequent broadcast of them, as shown in **Fig. 12 (a)**. However, the collision risk ratio decreases as a node broadcasts IREQ packets more frequently, as shown in **Fig. 12 (b)**. Our protocol shows the best performance with the norm threshold value of 75m. This simulation result shows the trade-off between frequency of IREQ broadcast and PU protection.

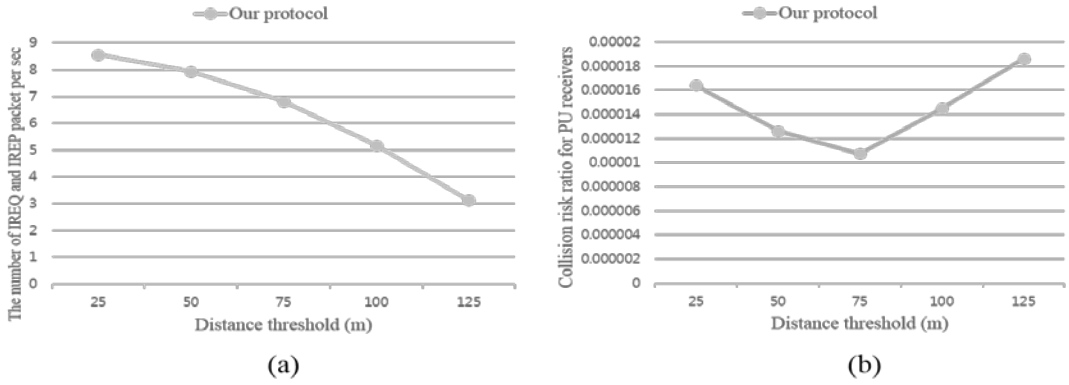


Fig. 11. Location based policy:
(a) The number of IREP and IREQ packet per sec and (b) Collision risk ratio for PU protection

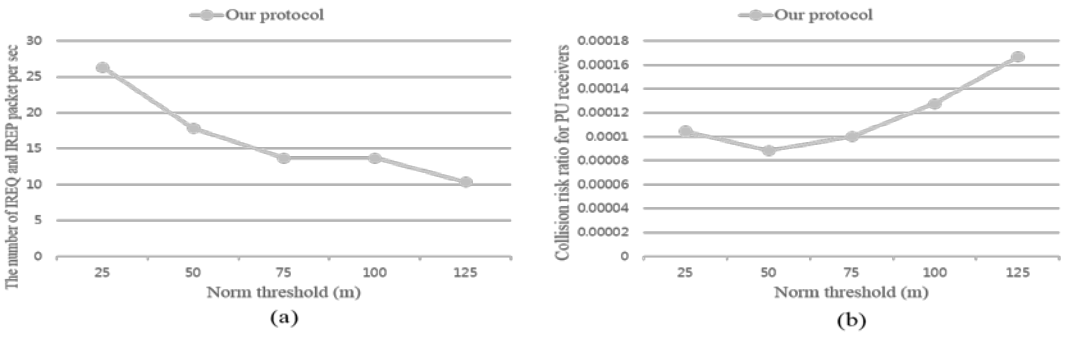


Fig. 12. Distance based policy:
(a) The number of IREP and IREQ packet per sec and (b) Collision risk ratio for PU protection

6. Conclusion

In this paper, we have introduced some state-of-the-art multi-hop routing protocols for CRNs. We have summarized the existing routing protocols and analyzed the limitations of them. To resolve the limitations, we have suggested a novel routing protocol for CRNs. Our protocol tries to protect PU communication and to improve network performance by simply exchanging additional control packets (IREP and IREQ). Our protocol shows better performances than the existing routing protocols. However, our protocol uses a common control channel to exchange control packets. The use of a common control channel makes performance of our protocol to be degraded in sparse networks because CUs cannot gather enough spectrum information from neighbor nodes. To resolve the weaknesses of our protocol, we plan to thoroughly study and elaborate our protocol further as a future work.

References

[1] F.C. Commission, "Spectrum policy task force," *Technical report*, Nov 2002
[2] J. Mitola, "Cognitive radio, An Integrated Agent Architecture for Software Defined Radio," *PhD Dissertation Thesis*, KTH, Sweden, May, 2000.
[3] I.F. Akyildiz, W.-Y Lee, M.C. Vuran, S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks Journal (Elsevier) 50*, vol. 50, pp. 2127-2159, Sep. 2006. Article (CrossRef Link).
[4] Z. Zhang, K. Long, "Self-organization paradigms and optimization approaches for cognitive radio technologies: a survey," *IEEE Wireless Communications*, vol. 20, pp. 36-42, April, 2013. Article (CrossRef Link).
[5] I.F Akyildiz, W.-Y Lee, K.R. Chowdhury, "CRAHNs: cognitive radio ad hoc networks," *Ad Hoc Networks (Elsevier) 7*, vol. 7, pp. 810-836, July, 2009. Article (CrossRef Link).
[6] S. Sengupta, K.P. Subbalakshmi, "Open research issues in multi-hop cognitive radio networks," *IEEE Communications Magazine*, vol. 51, pp. 168-176, April, 2013. Article (CrossRef Link).
[7] Brandon F. Lo, "A survey of common control channel design in cognitive radio networks," *Physical Communication 4 (Elsevier)*, vol. 4, pp. 26-39, Mar. 2011. Article (CrossRef Link).
[8] C.E. Perkins, E.M. Royer, "Ad-hoc on-demand distance vector routing," *IEEE Mobile Computing Systems and Applications*, pp. 90-100, Feb. 1999. Article (CrossRef Link).
[9] A.S. Cacciapuoti, C. Calcagno, M. Caleffi and L.Paura, "CAODV: Routing in Mobile Ad-hoc Cognitive Radio Networks," *IEEE Wireless Days (WD), 2010 IFIP Venice*, pp. 1-5, Oct. 2010. Article (CrossRef Link).
[10] K.R. Chowdhury, M.D. Felice, "Search: A routing protocol for mobile cognitive radio ad-hoc networks," *Computer Communications 32 (Elsevier)*, vol. 32, pp. 1983-1997, Dec. 2009. Article (CrossRef Link).
[11] K.R. Chowdhury, I. F. Akyildiz, "CRP: A routing protocol for cognitive radio ad hoc networks," *IEEE Journal on Selected Areas In Communications*, vol. 29, no. 4, pp. 794-804, April, 2011. Article (CrossRef Link).
[12] K. Habak, M. Abdelatif, H. Hagrass, K. Rizc, M. Youssef, "A location-aided routing protocol for cognitive radio networks," *IEEE Computing, Networking and Communication*, pp. 729-733, January, 2013. Article (CrossRef Link).
[13] A. S. Cacciapuoti, M. Caleffi and L. Paura, "Reactive routing for mobile cognitive radio ad hoc networks," *Ad hoc Networks (Elsevier)*, vol. 10, pp. 803-815, July, 2012.Article (CrossRef Link).
[14] I. F. Akyildiz, W.Y-.Lee, M. C. Vuran and S. Mohanty, "A Survey on Spectrum Management in Cognitive Radio Networks," *IEEE Communications Magazine*, vol. 46, pp. 40-48, April, 2008. Article (CrossRef Link).
[15] Lisheng Fan, Xianfu Lei, Trung Q. Duong, R. Q. Hu, and M. Elkashlan, "Multiuser Cognitive Relay Networks: Joint Impact of Direct and Relay Communications," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 5043-5055, Sep. 2014. Article (CrossRef Link).

[16] Matteo Cesana, F. Cuomo, and E. Ekici, "Routing in cognitive radio networks: Challenges and solutions," *Elsevier Ad Hoc Networks 9*, vol. 9, no. 3, pp. 228-248, May, 2011.
Article (CrossRef Link).

Sunwoo Kim received his B.S degree in Computer Engineering from Hanyang University, Seoul, Korea, in 2013. He is working towards the M.S degree at Department of Computer Science, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea. His research interest includes cognitive radio networks such as spectrum sensing, spectrum sharing, and routing.

Dohoo Pyeon received his B.S degree in the College of Information and Communications at Hanyang University, Seoul, South Korea, in 2011, and his M.S degree in Computer Science at Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2013. He is currently on Doctoral Degree Program in Computer Science at KAIST. His research interests include the communication protocols, such as medium access control, routing, and broadcast protocols, for energy efficiency in wireless sensor networks and for efficient spectrum utilization in cognitive radio networks.

Ingook Jang received the B.S. degree in computer science and engineering from the Chung-Ang University, Seoul, Korea, in 2008. He is currently working toward Ph.D. degree through the Integrated Master's and Doctoral Degree Program in computer science from Korea Advanced Institute of Science and Technology, Daejeon, Korea. His current research interests include the design and analysis of energy efficient communication protocols, especially broadcast, medium access control, scheduling of packet transmissions, with applications in wireless sensor networks, wireless ad hoc networks, and broadband access networks.

Hyunsoo Yoon received the B.S. degree in electronics engineering from Seoul National University, Seoul, Korea, in 1979, the M.S. degree in computer science from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 1981, and the Ph.D. degree in computer and information science from The Ohio State University, Columbus, in 1988. He is currently a Professor of with the Department of Computer Science, KAIST.
During 1978 - 1980, he was with the Tongyang Broadcasting Company, Korea, then Samsung Electronics Company, Seoul, Korea, during 1980 - 1984. From 1988 to 1989, he was a Member of the Technical Staff with AT&T Bell Labs, Indial Hill, IL. Since 1989, he has been a Professor with the Department of Computer Science, Korea Advanced Institute of Science and Technology. His research interests include mobile ad hoc networks, wireless networks, and network security.