This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

A Concurrent Transmission MAC Protocol for Enhancing Throughout and Avoiding Spectrum Sensing in Cognitive Radio

Li-Chun Wang*, Chung-Wei Wang*, Yin-Chih Lu*, and Chuan-Ming Liu+
* National Chiao Tung University, Taiwan
+ National Taipei University of Technology (NTUT), Taiwan
*Email : lichun@cc.nctu.edu.tw

***Abstract*— For the cognitive radio (CR) network, a fundamental issue is how to identify the spectrum opportunities. First, each CR node determines whether there exists transmission opportunities on unlicensed bands. If not, this node will find other opportunity on licensed bands. Thus, increasing the opportunities of concurrent transmissions in unlicensed bands can reduce the overhead of wide-band sensing.**

In this paper, based on the carrier sensing multiple access protocol, we propose a novel concurrent transmissions MAC (CT-MAC) protocol to identify the possibility of establishing the second link in the presence of the first link in the unlicensed band. In addition to reducing the overhead of wide-band sensing, the proposed CT-MAC scheme can enhance overall throughput and is backward compatible with the IEEE 802.11 standard.

I. Introduction

In the cognitive radio (CR) network, each CR node can operate in both unlicensed and licensed bands. The functionalities of medium access control (MAC) protocol required for CR devices vary according to whether the spectrum is licensed or unlicensed. If a CR node operates in the licensed band, it must avoid degrading the performance of the primary link. On the other hand, all nodes have the same right to access the unlicensed spectrum. Hence, a suitable contention resolution algorithm is necessary to achieve the objective of *intelligent spectrum sharing*.

An important issue for CR MAC is to identify the spectrum opportunities. Usually, each CR node first determines whether there exists transmission opportunities on unlicensed bands. If so, this node will concurrently transmit together with the first link. If not, this node will dynamically find other opportunity on licensed bands by wide-band sensing. Thus, increasing the concurrent transmission opportunities on unlicensed bands can reduce the overhead of wide-band sensing.

In the literature, recent research on MAC protocols for the multihop ad-hoc network on unlicensed band,

This work was supported by the National Science Council, Taiwan and the MOE ATU Program under the contracts NSC-94-2213-E-009-060 and 95W803C, respectively.

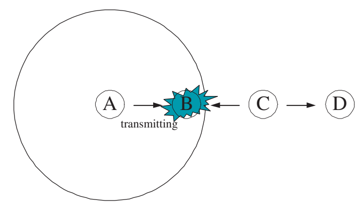

Fig. 1. The hidden node problem due to physical carrier sensing, where C is hidden from A and, in fact, C cannot transmit any data.

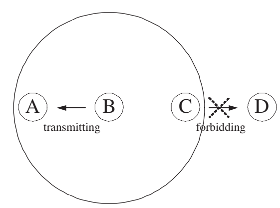

Fig. 2. The exposed node problem due to physical carrier sensing, where the data from nodes B to A and from nodes C to D can be concurrently transmitted, but the channel sensing results will refrain the transmission from node C.

the carrier sense multiple access (CSMA)-based MAC protocol is the most popular one. However, the CSMA-based MAC protocol induces the hidden node and exposed node problems as shown in Figs. 1 and 2, respectively. The *hidden node problem* occurs because node C out of the interference range of the transmitter can potentially cause frame collisions. On the other hand, node C within the range of the transmitter is prohibited from accessing the medium unnecessarily, which is called the *exposed node problem*. The exposed node problem yield spectrum inefficiency issue because it decreases the concurrent transmission opportunities. Moreover, although the concept of virtual carrier sensing is proposed in IEEE 802.11 MAC to solve the hidden node issue, the exposed node problem is remained open. Therefore, the focus of this paper is mainly on solving the exposed node problem .

In this paper, we propose a novel *concurrent transmissions MAC* (CT-MAC) scheme for a wireless ad hoc network based on the CSMA MAC protocol. Although the existing concurrent transmission MAC protocols can solve the exposed node problem, these protocols also induce other problems, such as the virtual-carrier exposed node

1525-3511/07/$25.00 ©2007 IEEE

problem [1], [2], the scalability issue for packet size [3], or the compatibility issue with IEEE 802.11 MAC protocol [4], [5]. Our proposed CT-MAC scheme can overcome the exposed node problem without the aforementioned problems.

To achieve this goal, we suggest that each CR device had better discover the neighboring nodes that support concurrent transmissions. With this information, it is easy for a node to decide whether the nodes in the existing link can help establish a concurrent transmission link. On the one hand, if the transmitter and receiver in the existing link are able to support concurrent transmissions, they can be designed to defer the transmission of the DATA frame. By utilizing this extra duration, a CT node can invite another CT node to establish the concurrent transmission link, thereby solving the virtual-carrier exposed node problem. On the other hand, when the nodes in the existing link are unable to support concurrent transmissions, a CT node will not try to establish the second link so that the interference due to incompatibility of the CT node and the regular node in the IEEE 802.11 WLAN will not occur. To discover the neighboring CT nodes, we design a simple CT-neighbor discovery scheme based on the principles of dynamic source routing protocol.

With this CT-neighbor discovering procedure, a novel concurrent transmissions MAC protocol is designed by taking advantage of the knowledge of the address fields in control frames, in addition to the physical and virtual carrier sensing techniques. If its two-hop neighbor is a transmitter, a CT node can be a receiver of the second link so that it can invite another CT node to be a transmitter. By contrast, if its two-hop neighbor is a receiver, a CT node can initiate the second link to another CT node. More importantly, observing the address fields in control frame can help a CT node confirm whether both the transmitter and receiver of the first link are CT nodes. Without confirming that its one- and two-hop neighbors are both CT nodes and knowing its roles of being a transmitter or a receiver, a CT node may cause interference to the legacy IEEE 802.11 WLAN.

The rest of this paper is organized as follows. In Section II, we introduce some problems induced from the CSMA MAC protocol and review some solutions of these problems. Section III presents the proposed CT-MAC protocol. Then, some simulation results are given in Section III-E. Finally, we give our concluding remarks in Section IV.

II. Background and Related Work

In following discussion, we consider the network topology as shown in Fig. 3 where each node can only communicate with its neighbors. First, we review some problems induced from the existing MAC protocols. Then, we survey some solutions of these problems in the recent literatures. However, these solutions cannot solve all problems perfectly.

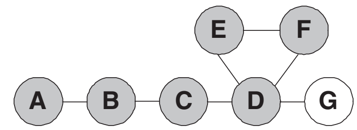

Fig. 3. An example of network topology. The gray nodes A, B, C, D, E, and F are CT-nodes, and the white node G is legacy-node.

A. Physical Carrier Sensing and Virtual Carrier Sensing

CSMA MAC protocol will face the well-known problems of hidden node and exposed node in wireless ad hoc networks. According to the CSMA MAC protocol, each node senses the channel before transmitting data. We refer to such sensing as *physical carrier sensing*. Therefore, we call these two problems the *physical-carrier hidden node problem* and the *physical-carrier exposed node problem*, respectively.

Because physical carrier sensing may be unreliable in the wireless channel, the MACA protocol introduced the concept of *virtual carrier sensing* [6]. The basic principles of virtual carrier sensing are briefly introduced in the following. When a node intends to transmit data to another node, it first broadcast a Request-To-Send (RTS) frame. After receiving the RTS frame, the target receiver replies a Clear-To-Send (CTS) frame. After the CTS frame is received by the transmitter, it can send out the data. It the data successfully reach the destination, the receiver will respond an acknowledgement (ACK) frame. This RTS-CTS-DATA-ACK four-way handshaking procedures can achieve the goal of carrier sensing without involving physical carrier sensing. Therefore, it is called *virtual carrier sensing*. Network Allocation Vector (NAV) embedded in the CTS frame is the key ingredient of the virtual carrier sensing technique. Except for the target user that sent out the RTS frame, all the other nodes receiving the CTS frame will defer their transmissions until the period defined in NAV is expired. In this case, these nodes keep quiet just like that they sense a busy channel.

By means of sending the RTS and CTS frames and adopting NAV to indicate the reserved channel usage time, MACA can resolve the hidden node problem. Referring to Fig. 1, after node B replies the CTS frame back to node A, node C will also be notified that the channel will be used for the transmission from node A to node B. Consequently, node C will wait for the end of the reserved period specified in the NAV value of the CTS frame and the hidden node problem due to physical carrier sensing is avoided.

The exposed node issue resulted from physical carrier sensing (shown in Fig. 2) cannot be completely resolved by the pure MACA protocol. The RTS/CTS handshaking mechanism in the pure MACA protocol does not consider the collision between a CTS frame and a data frame. In the next subsection, we will discuss the RTS/CTS-induced hidden and exposed node issues, where we will explain why the RTS/CTS mechanism of pure MACA protocol cannot solve the exposed node problem due to physical carrier sensing.

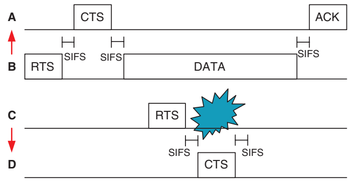

Fig. 4. The hidden node problem for CTS with VCS: the data links B to A and C to D can actually coexist.

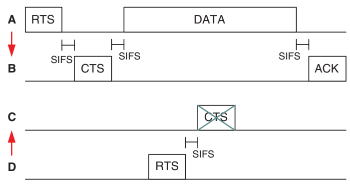

Fig. 5. The exposed node problem for CTS with VCS: the data links A to B and D to C can actually coexist.

B. RTS/CTS-induced Hidden Node and Exposed Node Issues

Although the RTS/CTS handshaking mechanism can solve the hidden node issue due to physical carrier sensing, it also induces another type of hidden and exposed node issues due to virtual carrier sensing.

The RTS/CTS-induced hidden node issue is illustrated in Fig. 4. In the figure, it is assumed that after the successful RTS/CTS handshaking procedure, node B is transmitting data to node A, while node C tries to connect to node D. Based on the MACA protocol, a node is allowed to send an RTS frame as long as it does not hear the CTS frame from other nodes. In this case, when node D replies a CTS frame to node C, collision occurs because the transmission of node B's DATA frame can also reach node C. This issue happens because node D is hidden to node B, which is quite similar to the hidden node issue due to physical carrier sensing except that the collision occurs between a CTS frame and a data frame, instead of pure data frames' collision. We call such a problem the *hidden node problem due to virtual carrier sensing*. Because of this problem, the exposed node issue due to physical carrier sensing is still left open. Recall that the transmissions of $B \rightarrow A$ and $C \rightarrow D$ are supposed to be able to coexist in the considered scenario, but the MAC protocols discussed so far, including physical and virtual carrier sensing, cannot achieve the goal of concurrent transmissions.

Now we discuss the exposed node issue induced by the RTS/CTS handshaking mechanism. As illustrated in Fig. 5, suppose that the link of $A \rightarrow B$ has been established based on the MACA protocol, as long as a node hear a CTS from other node, it will not be allowed to transmit any data in order to prevent the hidden node issue shown in Fig. 1. As a result, node C cannot reply a CTS frame to node D. Hence, the concurrent transmission opportunity of links $A \rightarrow B$ and $D \rightarrow C$ becomes wasted. In this case, node C is exposed to node B. We call this situation the *exposed node problem due to virtual carrier sensing*.

C. Existing Concurrent Transmission MAC Protocols

In this subsection, we discuss the concurrent transmission MAC protocols that can solve the exposed node issue in wireless ad hoc networks. Now we give an overview on the concurrent transmission MAC protocols with physical and virtual carrier sensing available.

1) Medium Access via Collision Avoidance with Enhanced Parallelism (MACA-P) [4]: To address the exposed node issue, an enhanced version of the MACA protocol, called the MACA-P protocol, was proposed in [4]. The key idea of this protocol is to introduce an extra gap between the RTS/CTS frames and the subsequent DATA frames in addition to the *short inter-frame space* (SIFS) of the IEEE 802.11 MAC protocol. This extra gap allows all the neighboring nodes to exchange the RTS/CTS frames for the purpose of concurrent transmission. After successfully exchanging the RTS/CTS frames by the end of this extra gap, the links with concurrent transmission opportunity, such as the links $B \rightarrow A$ and $C \rightarrow D$ in Fig. 4, can start transmitting their DATA frames. For concurrent transmissions, extra information bits are added in the RTS and CTS frames to indicate the start time of the DATA frame and the ACK frame. Hence, the two concurrent transmission links can synchronize their starting time. Similarly, the virtual-carrier exposed node issue can be solved by the MACA-P MAC scheme.

The improvement of concurrent transmission opportunity from the MACP-P MAC protocol come at the price of memory cost and incompatibility. The wireless ad hoc network adopting the MACA-P MAC protocol requires a larger memory size for storing the scheduled transmission time of all the neighboring nodes. More importantly, the MACA-P MAC protocol is not compatible with the IEEE 802.11 MAC protocol.

2) Parallel-MAC (P-MAC) [1]: [1] proposed a parallel-MAC (P-MAC) protocol to increase the concurrent transmission opportunity of a short packet together with a long packet. The basic idea of the P-MAC protocol is to apply the RTS/CTS/DATA/ACK four-way handshaking procedure and the DATA/ACK two-way handshaking procedure for long packets and for short packets, respectively. Based on this MAC protocol, if overhearing an RTS frame under the condition that no CTS frame is received, a node can establish another link to send a small-sized packet based on the DATA/ACK two-way handshaking procedure. With the NAV value in the overheard RTS frame of other nodes, the sender of the second link can schedule the transmission of the DATA frame to be synchronized with that of the first link. Similarly, the transmission time of the ACK frames in both the first link and the second link can be synchronized. The P-MAC protocol can achieve the objective of concurrent transmissions by simply not using RTS/CTS in the sending small-sized packets. Because approximately 50% of packets have a size smaller than 100 bytes in the Internet, the P-MAC protocol is quite suitable for delivering the traffic in the Internet.

To summarize, the P-MAC protocol can solve the virtual-carrier hidden node problem of Fig. 4 and thus the physical-carrier exposed node problem of Fig. 2. This MAC protocol can also overcome the physical-carrier hidden node problem of Fig. 1 because the RTS/CTS handshaking mechanism is employed. Nevertheless, the virtual-carrier exposed node problem of Fig. 5 still cannot be alleviated by adopting the P-MAC protocol.

3) Enhanced-MAC (E-MAC) [3]: By exploiting the fragmentation mechanism of the IEEE 802.11 MAC scheme, the enhanced-MAC (E-MAC) scheme was proposed to increase the concurrent transmission opportunity [3]. According to the IEEE 802.11 MAC scheme, a long packet can be partitioned into many small fragments, each of which is followed an ACK. The basic idea of the E-MAC scheme is to synchronize its transmission with the segments of the existing long packet. Then, the virtual-carrier hidden and exposed node problems can be solved.

However, this solution has some disadvantages. First, E-MAC must fragment the packets from the upper layers, which in only suitable for a larger-sized packet network. However, as mentioned previously, about 50% packets are smaller than 100 bytes in the Internet. Second, because the size of the last segment is a variable, it is necessary to monitor the NAV of the last segment from its previous segment. However, it is difficult for the second link to overhearing the DATA segment of the other nodes and transmit its own data simultaneously except that there are multiple radio interfaces. Third, referring to Fig. 5, if the synchronization duration between the RTS and parallel-CTS frame between nodes D and C is longer than the SIFS duration, node D in the second link may enter the backoff procedure after a timeout duration. Thus, the RTS frame is sent again by node D.

III. The Proposed CT-MAC Protocol

The proposed CT-MAC protocol aims to solve the hidden and exposed node problems with physical and virtual carrier sensing subject to the constraint of being compatible with the IEEE 802.11 MAC protocol. The basic idea in the proposed CT-MAC protocol is described as follows. First, each node identifies whether or not a concurrently transmitted link can be established based on the observations from (1) physical carrier sensing; (2) virtual carrier sensing; and (3) the Destination Address (DA)/Source Address (SA) fields in the overheard RTS or CTS. With the DA/SA fields in the RTS frame (or the DA field of the CTS frame), a node can determine if the current existing link are able to support concurrent transmissions by comparing the address with the results obtained from the CT-neighbor discovery procedure. Furthermore, with these observations, each CT node can identify its transmission directions (i.e., whether it can “transmit” or “receive”) in the concurrent transmission link.

In the following, we develop a CT-MAC protocol based on these observations. Figure 3 shows an example network topology, where nodes A, B, C, D, E, and F are capable of supporting the CT-MAC protocol (called the CT nodes), but node G is a legacy node employing the conventional IEEE 802.11 MAC protocol.

A. CT-Neighbors Discovery Procedure

One of key features in the proposed CT-MAC protocol is that each nodes can know which neighbors can support concurrent transmissions. The proposed CT-neighbors discover procedure is detailed in the following. In the beginning, each CT node broadcasts a Concurrent Transmission Request (CT-REQ) frame to its neighbors within two hops. As soon as a CT node receives the CT-REQ frame, it is required to respond a Concurrent Transmission Reply (CT-REP) frame. This handshaking mechanism is similar to the route setup procedure of the dynamical source routing protocol. From the received CT-REP frames, the transmitter that sent the CT-REQ frame previously can know which neighboring CT nodes can help establish concurrent transmission links. All the other CT nodes perform the same neighbors discovery procedure.

Now we take the network topology of Fig. 3 as an example to illustrate the CT-neighbors discovery procedure. First, node C broadcasts the CT-REQ frame to nodes B and D. Then, nodes B and D immediately forward CT-REQ to nodes A and E, F, and G, respectively. Suppose that node F does not allow concurrent transmissions at this moment and node G is a legacy node who does not understand the CT-REQ frame. Thus, nodes F and G will not reply CT-REP for this CT-REQ frame. In the meanwhile, nodes E and A reply a CT-REP(E) frame to node D and a CT-REP(A) to node B, respectively, where CT-REP(E) and CT-REP(A) represent that nodes E and A are willing to help establish concurrent transmission links. Next, nodes B and D respectively reply a CT-REP(A,B) frame and a CT-REP(E,D) frame to node C. Hence, node C finds that nodes A, B, D and E are neighboring CT nodes within two hops and then records these nodes in its CT-neighbors list.

B. Solution to the Exposed Node Problem with Virtual Carrier Sensing

Consider the exposed node problem with virtual carrier sensing as shown in Figure 5, where link $A \rightarrow B$ is already established. From the RTS/CTS handshaking procedure, node C only overhears the CTS frame from node B but no RTS frame. If node C further finds that the channel is idle from physical carrier sensing, node C can conclude that itself is an exposed node with virtual carrier sensing, of which transmissions are prohibited due to hearing the CTS frame.

The proposed CT-MAC protocol can solve the exposed node problem with virtual carrier sensing as illustrated in Fig. 6. Specifically, in this case the proposed CT-MAC protocol can help the exposed node successfully function as a receiver for the second link. In the figure, during the setup process of link $A \rightarrow B$, node A sends an RTS frame, and then B responds the CTS frame. Since node C looks up the DA field of the overheard CTS frame, it can know

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

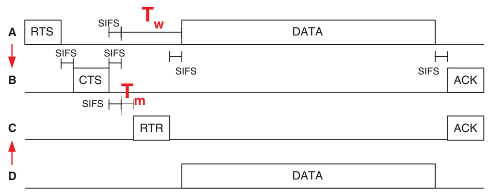

Fig. 6. A solution to the exposed node problem with virtual carrier sensing.

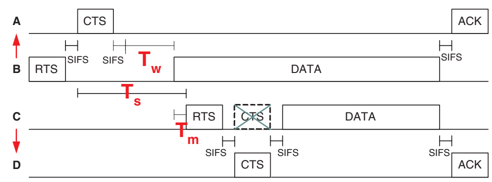

Fig. 7. A solution to the hidden node problem with virtual carrier sensing.

who is the transmitter of the first link. By checking the CT-neighbors list, node C can decide whether both the transmitter and receiver of the first link are CT-nodes. Moreover, being aware that it has a CT neighbor within two hops, node A will not immediately transmit DATA to B, but will wait for a duration of T_w. This waiting duration is equal to the sum of SIFS (T_{SIFS}), the monitoring time (T_m) and the transmission time (T_{RTR}) of the Ready-to-Receive (RTR) frame. Note that the monitoring time is the duration for identifying the channel state. Because only overhearing the CTS frame from node B but no RTS in an idle channel after the duration T_m, node C knows that itself is an exposed node. Hence, it sends an RTR frame to node D during T_{RTR} in order to request the data from D. This RTR frame should record the allowing data length in order to synchronize ACKs between the first and second links. Notice that the NAV value (T_{nav}) in RTS of A is equal to $3T_{SIFS} + T_{CTS} + T_w + T_{DATA} + T_{ACK}$ where $T_\diamond$ means the transmission time of the $\diamond$ type frame.

C. Solution to the Hidden Node Problem with Virtual Carrier Sensing

Now let us discuss how the proposed CT-MAC protocol can solve the the hidden node problem with virtual carrier sensing. Figure 4 shows an example with this problem. In the figure, link $B \rightarrow A$ is already established. Thus, from the RTS/CTS handshaking procedure, node C only overhears the RTS frame from node B but no CTS frame. Hence, node C can have an opportunity to transmit data without interfering the first link.

However, how can the collision issue between the CTS frame from node D and the DATA frame form node B be overcome? As illustrated in Fig. 7, if node C has not received any RTS or CTS frames from node D, it is very likely that node D is idle and can receive data. It is implied that the confirmation of CTS frame from node D may not be necessary for establishing the second link. After sending the RTS frame, node C further waits for $2T_{SIFS} + T_{CTS}$ duration and then immediately sends the DATA frame to node D. Unlike [1] that applies the two-way handshaking (DATA/ACK) mechanism to establish the second link, our proposed CT-MAC protocol still suggests adopting RTS/CTS/DATA/ACK four way handshaking with some modification. The advantage of letting node D send the CTS frame is to avoid the physical-carrier hidden node problem around its neighbor.

The next important issue is to determine the transmission duration for the second link. Assume that nodes A and B are CT nodes and they will defer their DATA transmission if they learn their neighbors are also CT nodes. In the case, the DATA transmission duration ($T_{C\rightarrow D}$) of the second link can be obtained as

$$T_{C\rightarrow D} = T_{nav} - T_w - T_m - T_{RTS} - 2T_{CTS} - T_{ACK} - 5T_{SIFS} \;, \quad (1)$$

where T_{nav} is the transmission duration of the first link obtained from the NAV field of the RTS frame overheard from node B, and T_w and T_m are defined in Section III-B. If the transmission time required for sending a packet in the second link is longer or shorter than $T_{C\rightarrow D}$, one can fragment the original packet or pad some dummy bits.

The last critical issue for concurrent transmission is to ensure that the first link is already established successfully. If the first link is established, it will be unnecessary to initiate the concurrent transmission procedure. Hence, based on our proposed CT-MAC protocol, it is suggested to perform physical carrier sensing even if the channel is already classified to be busy based on virtual carrier sensing. Referring to Fig. 7, after receiving an RTS frame, node C starts a timer to wait for a duration of T_s ($= T_{SIFS} + T_{CTS} + T_w + T_m$) and then execute physical carrier sensing. If the channel is busy, node C understands that its transmission to node D should be operated in the concurrent transmission mode (i.e, ignoring the CTS frame); otherwise, it needs to receive an CTS frame before transmitting. For the concurrent transmission case, the NAV value in the RTS frame of node C is set as the remaining NAV value of the first link, i.e., $T_{nav} - T_{SIFS} - T_s - T_{RTS}$. For the non-concurrent transmission case, the establishment of the first link may fail because node A does not reply CTS.

D. Discussion

Here we refine our proposed CT-MAC protocol to handle a special case. In our proposed CT-MAC protocol, as described in Section III-C, if a node only overhears the RTS frame but no CTS frame when the channel is busy, it can be a transmitter in the second link. However, this rule may not be always true. For example, consider the network topology shown in Fig. 3. Since the first link $E \rightarrow F$ is already established, node D can overhear the RTS frame sent from node E to node F. Assume that nodes C and F simultaneously send RTS and CTS to nodes D and E, respectively. In this case, collision occurs at node D. Thus, node D fails to receive any frames. From the standpoint of node D, it receives RTS but no CTS and senses a busy channel due to the transmission of link $E \rightarrow F$. Therefore, node D may mistakenly believe that

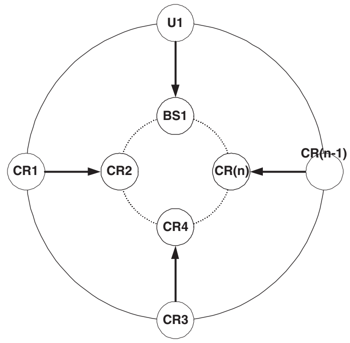

Fig. 8. A double-ring topology for simulation.

it can be the transmitter of the second link according to our proposed CT-MAC protocol described in Section III-C. However, the links $E \rightarrow F$ and $D \rightarrow C$ cannot transmit concurrently because node D's transmission will interfere node F's reception.

To resolve this issue, we refine the concurrent transmission rule as follows. If the DA field in the overheard RTS frame indicates that the receiver of the first link is its one-hop neighbor, a node is forbidden to be a transmitter in the second link. For example, by observing the DA field in the RTS frame of node E, node D knows that the receiver (F) of the first link is also its neighbor. According to the above refined concurrent transmission rule, node D will not transmit data in order not to interfere the existing link. Similarly, we can also observe the SA filed in the RTS frame and the DA field in the CTS frame to identify whether the neighboring node is a potential transmitter/receiver.

E. Numerical Results

We perform simulations based on ns-2 in the double ring topology as shown in Fig. 8. Each inner node can communicate with its neighbors. However, each outer node can only communicate with its corresponding inner node. Furthermore, each outer node sends data to its corresponding inner node. The considered traffic type is constant bit rate. Figure 9 compares the maximal network throughput of the legacy IEEE 802.11 MAC and the proposed CT-MAC protocols. As shown in the figure, the legacy IEEE 802.11 MAC does not allow more than two transmissions simultaneously. Thus, the maximal throughput is constant for various numbers of nodes. By contrast, the proposed CT-MAC protocol allows multiple concurrent transmissions. As shown in the figure, the maximal throughput increases as the total number of nodes increases. For example, when both the numbers of inner and outer nodes are equal to four, the maximum throughput of the proposed CT-MAC protocol is 370% higher than that of the IEEE 802.11 MAC protocol.

IV. Conclusion

In this paper, we proposed a novel MAC to identify the concurrent transmission opportunities for the cognitive wireless networks. The key features of the proposed CT-MAC protocol include: (1) an integrated observation that utilizes physical and virtual carrier sensing as well as observes the address fields in the control frames; and (2) two-hop CT-neighbors discovery procedure with a better topology awareness capability. With these features, the proposed CT-MAC protocol can enhance the overall throughput of a cognitive ad hoc network and avoid the time- and energy-consuming wide-band sensing. Other advantages can be summarized as follows:

- overcome the hidden and exposed node issues with physical and virtual carrier sensing;
- backward compatible with the IEEE 802.11 MAC protocol;
- suitable to concurrently transmit various sizes of packets with higher flexibility.

There are some interesting open issues. So far the proposed concurrent transmission MAC protocol has not taken into account of the effect of location awareness. In the future, we aim to incorporate the impact of location awareness into the concurrent transmission MAC protocol design is also an interesting research direction [7].

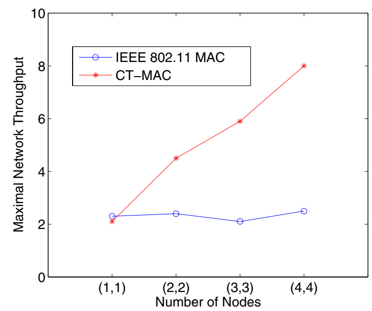

Fig. 9. Comparison of the maximal network throughput between the propose CT-MAC protocol and the legacy IEEE 802.11 MAC protocol for various numbers of nodes, where (k, k) means the both numbers of inner and outer nodes are k.

References

[1] D. Shukla, L. Chandran-Wadia, and S. Iyer, “Mitigating the Exposed Node Problem in IEEE 802.11 Ad Hoc Networks,” *The 12th International Conference on Computer Communications and Networks*, pp. 157–162, October 2003.

[2] D. Kim and E. Shim, “P-MAC: Parallel Transmissions in IEEE 802.11 Based Ad Hoc Networks with Interference Ranges,” *International Conference on Information Networking (ICOIN)*, vol. 3391, pp. 735–744, January-February 2005.

[3] A. Velayutham and H. Wang, “Solution to the Exposed Node Problem of 802.11 in Wireless Ad-Hoc Networks.” [Online]. Available: http://www.cs.iastate.edu/~vel/research/E-MAC.pdf

[4] A. Acharya, A. Misra, and S. Bansal, “Design and Analysis of a Cooperative Medium Access Scheme for Wireless Mesh Networks,” *First International Conference on Broadband Networks*, pp. 621–631, 2004.

[5] N. Santhapuri, J. Wang, Z. Zhong, and S. Nelakuditi, “Piggybacked-Ack-aided Concurrent Transmissions in Wireless Networks,” *In Poster Session of ICNP'05*, November 2005. [Online]. Available: http://arena.cse.sc.edu/papers/pact.icnp05.pdf

[6] P. Karn, “MACA - A New Channel Access Method for Packet Radio,” *ARRL/CRRL Amateur Radio 9th computer Networking Conference*, pp. 134–140, 1990.

[7] L.-C. Wang and A. Chen, “On the Coexistence of Infrastructure-Based and Ad Hoc Connections for a Cognitive Radio System,” *First International Conference on Cognitive Radio Oriented Wireless Network and Communications (CROWNCOM)*, June 2006.