DUCHA: A New Dual-Channel MAC Protocol for Multihop Ad Hoc Networks

Hongqiang Zhai, *Student Member, IEEE*, Jianfeng Wang, *Student Member, IEEE*, and Yuguang Fang, *Senior Member, IEEE*

***Abstract*— IEEE 802.11 MAC protocol has been the standard for Wireless LANs and is also implemented in many simulation software for mobile ad hoc networks. However, IEEE 802.11 MAC has been shown to be quite inefficient in the multihop mobile environments. Besides the well-known hidden terminal problem and the exposed terminal problem, there also exists the receiver blocking problem, which may result in link/routing failures and unfairness among multiple flows. Moreover, the contention and interference from the upstream and downstream nodes seriously decrease the packet delivery ratio of mulitihop flows. All these problems could lead to the "explosion" of control packets and poor throughput performance. In this paper, we first analyze these anomaly phenomena in multihop mobile ad hoc networks. Then, we present a novel effective random medium access control (MAC) protocol based on IEEE 802.11 MAC protocol. The new MAC protocol uses an out-of-band busy tone and two communication channels, one for control frames and the other for data frames, and can give a comprehensive solution to all the aforementioned problems. Extended simulations demonstrate that our protocol provides a much more stable link layer, greatly improves the spatial reuse, and works effectively in reducing the packet collisions. It improves the throughput by up to 20% for one-hop flows and by up to 5 times for multihop flows under heavy traffic comparing to the IEEE 802.11 MAC.**

***Index Terms*— Dual-channel, hidden terminal and exposed terminal problems, intra-flow contention, medium access control (MAC), multi-hop mobile ad hoc networks, receiver blocking problem.**

I. INTRODUCTION

CONTENTION-BASED medium access control (MAC) protocols have been widely deployed for wireless networks due to the low cost and easy implementation. Among them, IEEE 802.11 MAC protocol [1] has been the standard for wireless LANs and also been incorporated in many wireless simulation packages for mobile ad hoc networks. It adopts four-way handshake procedures, i.e., RTS/ CTS/ DATA/ ACK. Short packets, RTS and CTS, are used to avoid collisions between long data packets. The NAV (Network Allocation Vector) value carried by RTS/ CTS/ DATA/ ACK is used to avoid potential collisions (i.e., virtual carrier sensing) and hence mitigate the hidden terminal problem. The ACK is used as a confirmation of a successful transmission without an error.

However, the effectiveness of IEEE 802.11 MAC in multihop mobile ad hoc networks has been recognized as a serious problem. The packet collision over the air is much more severe in the multihop environments than that in the wireless LANs [1], [20], [22], [23]. The packet losses due to such a kind of MAC layer contentions will definitely affect the performance of the high layer networking schemes such as the TCP congestion control and routing maintenance because a node does not know whether an error is due to the collision or the unreachable address [3], [4], [12], [18], [19], [21], [23], [24].

The source of the above problems comes mainly from the MAC layer. The hidden terminals introduce collisions and the exposed terminals lead to low spatial reuse ratio. Besides these two notorious problems, the receiver blocking problem, i.e., the intended receiver does not respond to RTS or DATA due to the interference or virtual carrier sensing operational requirements from other ongoing transmissions, also deserves a serious attention. This problem becomes more severe in the multihop environments and results in packet dropping, starvation of some traffic flows or nodes, and possible network layer re-routing, which we will elaborate later in Section III. Furthermore, for multihop flows, the contentions or interferences from the upstream and downstream nodes and other flows could lead to poor packet delivery performance.

There are many schemes proposed in the current literature to reduce the severe collisions of DATA packets at MAC layer. BTMA [15] uses a busy tone to address the hidden terminal problem. The base station broadcasts a busy tone signal to keep the hidden terminals from accessing the channel when it senses a transmission. It relies on a centralized network infrastructure which is not applicable in mobile ad hoc networks. FAMA-NCS [5] uses the long dominating CTS packets to act as the receive busy tone to prevent any competing transmitters in the receiver range from transmitting. This requires any nodes hearing interference keep quiet for the period of one maximum data packet to guarantee no collisions with the ongoing data transmission, which is obviously not efficient especially when the RTS/CTS negotiation process fails or the DATA packet is very short.

Some multi-channel schemes based on random access have also been investigated in the last few years. One common approach to avoiding collisions between control packets and data packets is to use separate channels for different kinds

Manuscript received January 5, 2005; revised July 25, 2005; accepted January 29, 2006. The associate editor coordinating the review of this paper and approving it for publication was X. Shen. This work was supported in part by the U.S. Office of Naval Research under Young Investigator Award N000140210464 and by the National Science Foundation under Faculty Early Career Development Award ANI-0093241 and under grant DBI-0529012.

The authors are with the Department of Electrical & Computer Engineering, University of Florida, Gainesville, FL 32611-6130 USA (e-mail: (zhai@ecel.ufl.edu; jfwang@ufl.edu; fang@ece.ufl.edu).

Digital Object Identifier 10.1109/TWC.2006.04869

of packets. DCA [16] uses one control channel for RTS/CTS and one or more data channels for DATA/ACK. It presents one method to utilize multiple channels but does not solve the hidden terminal problems. Dual busy tone multiple access (DBTMA) schemes [6] [7] [17] handles the hidden terminal and exposed terminal problems. It uses the transmit busy tone to prevent the exposed terminals from becoming new receivers, the receive busy tone to prevent the hidden terminals from becoming new transmitters, and a separate data channel to avoid collisions between control packets and data packets. DBTMA, however, does not consider the ACK packets which, if used, may result in collisions with the DATA packets while the acknowledgment (ACK) is needed for the unreliable wireless links. PAMAS [13] uses a separate control channel to transmit both RTS/CTS packets and busy tone signals. It gives a solution to the hidden terminal problem and mainly focuses on power savings. MAC-SCC [9] uses two Network Allocation Vectors (NAVs) for the data channel and the control channel, respectively. The two NAVs make it possible for the control channel to schedule not only the current data transmission but also the next data transmission. Although it reduces the backoff time, it does not address the aforementioned problems.

To the best of our knowledge, there are no comprehensive study and good solutions to all the hidden terminal problem, the exposed terminal problem, the receiver blocking problem, and the intra-flow and inter-flow contention problems. All of them contribute to the poor performance of MAC protocol in the multihop wireless mobile ad hoc networks. Most of the current schemes aggravate the receiver blocking problem while alleviating the hidden terminal problem and do not fully address the problems of multihop flows in the mobile ad hoc networks.

In this paper, we utilize two channels (dual-channel) for control packets and DATA packets, separately. RTS and CTS are transmitted in a separate control channel to avoid the collisions with data packets. Negative CTS (NCTS) is used to solve the receiver blocking problem and is also transmitted in the control channel. An outband receiver-based busy tone [6] is used to solve the hidden terminal problem. We do not use ACK here because there is no collision to the ongoing DATA packet. To address the packet error due to the imperfect wireless channel, we introduce Negative Acknowledgment (NACK) signal, a continuing busy tone signal, when the receiver determines that the received DATA packet is corrupted and in error. The sender will not misinterpret this NACK signal because there are no other receivers in its sensing range and hence no interfering NACK signals, and it will assume that the transmission is successful if no NACK signal is sensed. Furthermore, our protocol has an inherent mechanism to solve the intra-flow contention and could achieve optimum packet scheduling for chain topology. It turns out that this protocol has solved almost all aforementioned problems and does not require synchronized transmission at the MAC layer as in [2] [14].

The rest of this paper is organized as follows. Section II presents the basic concepts of the physical model which are important to design the MAC protocol. Then, Section III elaborates the source of collisions in the IEEE 802.11 MAC protocol when applied in the multi-hop mobile ad hoc networks and the ideal protocol behavior we may desire. Section IV describes the new MAC protocol for multihop mobile ad hoc networks. Simulation results are given in Section V. Finally, we conclude the paper in section VI.

II. Background

A. Transmission Range and Sensing/Interference Range

In wireless networks, the signal to noise plus interference ratio (SINR) must be greater than some threshold β for the receiver to detect the received signal correctly.

$$SINR_i = \frac{P_i}{\sum\limits_{k \neq i} P_k + N} \geq \beta \tag{1}$$

The received power P_r:

$$P_r = P_o \left(\frac{d_o}{d}\right)^{\alpha}, \tag{2}$$

where d_o is the reference distance, P_o is the received power at the reference distance, and $\alpha \geq 2$ is the power-loss exponent. In the following discussions, we assume all nodes use the same transmission power.

In the transmission range, the receiver should be able to correctly demodulate (or decode) the signal when there is no interference, i.e., the received power P_r must be greater than a threshold RX_{Thresh}, which defines the maximum transmission distance, called the *transmission range*,

$$d_t = d_o \left(\frac{P_o}{RX_{Thresh}}\right)^{1/\alpha}. \tag{3}$$

If there is interference from another transmission at the receiver, the power of the interference signal P_i must be smaller than that of the intended signal P_r, i.e. $P_i * CP_{Thresh} < P_r$, where $CP_{Thresh} > 1$ is the capture threshold. So

$$d_i = d_r \left(\frac{P_r}{P_i}\right)^{1/\alpha} > d_r \times CP_{Thresh}^{1/\alpha} = \Delta_c \times d_r, \tag{4}$$

where d_i is the distance from the interference source to the receiver, and d_r is the distance from the sender to the receiver. The quantity $\Delta_c = CP_{Thresh}^{1/\alpha} > 1$ defines a zone where other transmissions will interfere the receiving activities.

When the receiver is at the maximum transmission distance d_t away from the sender, the minimum interference distance, d_{imin}, which allow correct demodulation at the receiver and the interference power P_{imin} are

$$d_{imin} = \Delta_c \times d_t, \qquad P_{imin} = P_t \left(\frac{d_t}{d_{imin}}\right)^{\alpha} = \frac{P_t}{CP_{Thresh}}. \tag{5}$$

So the sender should be able to sense the interference with power level P_{imin} before transmission, i.e., the interference from d_{imin} away, to avoid potential interference to other ongoing transmission. Considering the probability that there are more than one interfering transmissions in the neighborhood of the intended receiver, the sensing range d_s should be even greater than d_{imin}, i.e.,

$$d_s = \Delta_s \times d_t, \Delta_s > \Delta_c, \tag{6}$$

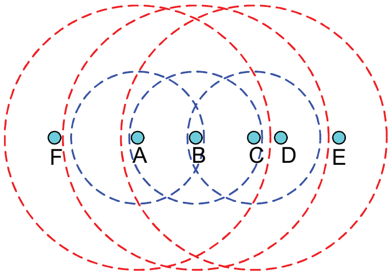


Fig. 1. A simple scenario to illustrate the problems.

which guarantees correct reception at the receiver if it senses the channel idle in spite of the possible interferences from multiple sources outside of the sensing range.

The sensing range is also called interference range in many literatures [8] since other transmissions in this range may introduce enough interference to corrupt the intended signal. The widely used network simulation tool ns2 implements the settings of WaveLAN card from Lucent company with default values $CP_{Thresh} = 10dB$, $d_t = 250m, \Delta_c \approx 1.78$, and $\Delta_s \approx 2.2$, respectively. Some recent literatures [11] [10] about power control schemes adopt $CP_{Thresh} = 6dB$, $\Delta_c \approx 1.41$, and $\Delta_s \approx 2.2$. Thus, it is reasonable to assume that the radius of the sensing/interference range is about twice of the transmission range for our evaluation study.

III. Problems and the Desired Protocol Behavior

In this section, we describe a few problems in multi-hop mobile ad hoc networks when the IEEE 802.11 MAC protocol is deployed.

A. Hidden and Exposed Terminal Problem

A hidden terminal is the one outside of the sensing range of the transmitter, but within that of the receiver. It does not know that the transmitter is transmitting, hence may transmit to some node, resulting in a collision at the receiving node. Fig. 1 illustrates a simple example, where the small circles indicate the edges of transmission range and the large circles indicate the edges of the sensing range. D is the hidden terminal of A. It cannot sense A's transmission but may still interfere with B's reception if D transmits.

An exposed terminal is the one outside of the sensing range of the receiver but within that of the transmitter. If an exposed node senses the medium busy, it will not transmit although its transmission may not affect the ongoing transmission, leading to bandwidth under-utilization. In Fig. 1, F is the exposed terminal of A. When A is transmitting to B, F senses A's transmission and keeps silent. However, F can transmit to other nodes outside of A's sensing range without interfering with B's reception.

In the four-way handshake procedures in IEEE 802.11 MAC, RTS/CTS and DATA/ACK are bidirectional packets exchanged. Therefore the exposed node of one of the transmitter-receiver pair is also the hidden node of the other. Besides the hidden terminal, the exposed terminal of the transmitter should not initiate any new transmission either during the ongoing transmission to avoid collisions with the short packets CTS or ACK. This implies that the carrier sensing scheme executed at the transmitter is to avoid the collision with the reception of the CTS or ACK at the transmitter, which result in significant decrease of the spatial reuse (and hence the network throughput).

B. Limitations of NAV Setup Procedure

IEEE 802.11 family protocols adopt NAV setup procedure to claim the reservation of the channel for a certain period to avoid collision from the hidden terminals. The NAV field carried by RTS/ CTS/ DATA/ ACK notifies the neighbors to keep silent during a certain period indicated by the NAV value.

NAV setup procedure cannot work properly when there are collisions. As shown in Fig. 1, A wants to send packets to B. They exchange RTS and CTS. If E is transmitting when B transmits CTS to A, B and E's transmission will collide at C, and C cannot set its NAV according to the corrupted CTS from B.

NAV setup procedure is redundant if a node is continuously sensing the carrier. For example, in Fig. 1, transmission ranges of both A and B are covered by the common area of their sensing ranges. Without collisions, C can set NAV correctly when receiving B's CTS. However, it can also sense A's transmission which prevents C from transmitting even when there is no NAV setup procedure. RTS's NAV is not necessary either because any node which can receive RTS correctly can also sense B's CTS and succeeding DATA and ACK, and will not initiate new transmission to interrupt the ongoing transmission.

NAV setup procedure does not solve the hidden terminal problems even if the neighbors of the receiver can correctly receive CTS and set their NAVs. In Fig. 1, D is the hidden terminal of A and out of transmission range of B. It cannot sense A's transmission and cannot correctly receive B's CTS either. Thus, when A is transmitting a long data packet to B, D may initiate a new transmission, which will result in a *collision* at B.

C. Receiver Blocking Problem

The blocked receiver is the one which cannot respond to the RTS intended for itself due to other ongoing transmissions in its sensing range. This may result in unnecessary RTS's retransmissions and the subsequent DATA packet discarding. When it is in the range of some ongoing transmission, the intended receiver cannot respond to the sender's RTS according to the carrier sensing strategy in IEEE 802.11 standard. Then the sender will retransmit the packet. The backoff window size is doubled each time when the RTS transmission fails and becomes larger and larger, until the sender finally discards the packet. When the ongoing transmission finishes, the packet in the queue of the old sender will have higher priority than the new one because it resets its backoff window size and has much smaller value than that of a new one. So the old sender has higher probability to continue to transmit and the new one continues doubling the backoff window size and discards packets when the maximum number of transmission attempts is reached. This will therefore result in serious unfairness

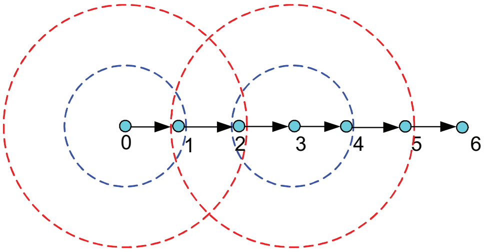


Fig. 2. Chain topology.

among flows and severe packet discarding, and worse yet, it may lead to path repair or network rerouting.

For example, in Fig. 1, when D is transmitting to E, A sends RTS to B, but will not receive the intended CTS from B. This is because B cannot correctly receive A's RTS due to collision from D's transmission. Thus, A keeps doubling contention window and retransmitting until it discards the packet. If D has a burst of traffic to E, it will continuously occupy the channel which will starve the flow from A to B.

The hidden terminal problem only makes the receiver blocking problem worse. In the above example, even if A has a chance to transmit a packet to B, its hidden terminal D could start transmission and collide with A's transmission at B because D cannot sense A's transmission. Therefore, A almost has no chance to successfully transmit a packet to B when D has packets destined to E.

D. Intra-Flow Contention

Intra-flow contention is the contention from the transmissions of packets at upstream and downstream nodes along the path of a same flow. The packet at each hop along the path may encounter collisions and be discarded. Thus, the packets which reach the last few nodes of the path is much fewer than those at the first few nodes. And the resource consumed by those discarded packets is wasted.

Another abnormality is that packets continuously accumulate at the first few hops of the path. The reason is that the transmission at the first few hops encounters less contention than that at subsequent nodes. One simple example, as shown in Fig. 2, is the chain topology with more than 5 hops where nodes are separated by a fixed length of a little less than the maximum transmission distance. The first node is interfered by three subsequent nodes. This number is four for the second node and 5 for the third node. This means the first node could inject more packets into the chain than the subsequent nodes could forward. Li et al. have discussed this phenomena in [8] and indicated that 802.11 MAC fails to achieve the optimum throughput for the chain topology.

E. Inter-flow Contention

Inter-flow contention happens when two or more flows pass through the same region. The transmission of packets in this region encounters the interference and collisions not only from the packets of its own flow but also from other flows. This region becomes the bottleneck and could make it more severe to accumulate packets at the first few hops of the flows than that in the scenario where there is only intra-flow contention.

F. Desired Protocol Behavior

The desired MAC protocol for mobile ad hoc networks should resolve the hidden/exposed terminal problem and the receiver blocking problem. It should guarantee that there is only one receiver in the range of a transmitter and only one transmitter in the range of a receiver. The exposed nodes can start to transmit in spite of the ongoing transmission. The hidden nodes cannot initiate new transmissions but may receive packets. Thus, to maximize the spatial reuse, it should allow multiple receivers in the range of any receiver to receive and multiple transmitters in the range of any transmitter to transmit. The transmitter should also know whether its intended receiver is blocked or is outside of its transmission range when it does not receive the returned CTS to avoid discarding packets and the undesirable behavior at the higher protocol layer, such as false alarms of route failures.

G. Limitation of IEEE 802.11 MAC Using a Single Channel

The collisions between RTS, CTS, DATA and ACK are the culprits preventing the MAC protocol from achieving the aforementioned desired behavior. The exposed terminal cannot initiate new transmissions which may prevent the current transmitter from correctly receiving the ACK. The hidden terminal which cannot correctly receive the CTS or sense the transmission may initiate a new transmission which collides with the current ongoing transmission. Furthermore, it should not become a receiver because its CTS/ACK may introduce collisions at the receiver of the current transmission. Its DATA packet reception may also be corrupted by the ACK packet from the current receiver. If the intended receiver of a new transmission is in the range of the ongoing transmission, it may not be able to correctly receive RTS and/or sense the busy medium, and hence will not return the CTS. Thus, the intended sender cannot distinguish whether it is blocked or out of the transmission range.

To summarize, many aforementioned problems cannot be solved if a single channel is used in the IEEE 802.11 MAC protocol.

IV. DUCHA: A New Dual-Channel MAC Protocol

In this section, we present the new dual-channel MAC protocol (DUCHA) for multi-hop mobile ad hoc networks.

A. Protocol Overview

To achieve the desired protocol behavior, we utilize dual-channel for DATA and control packets, separately. DATA is transmitted over the data channel. RTS and CTS are transmitted over the control channel. Negative CTS (NCTS) is used to solve the receiver blocking problem and is also transmitted on the control channel. An outband receiver based busy tone [15] [6] is used to solve the hidden terminal problem. ACK is unnecessary here because our protocol can guarantee that there is no collision to DATA packets. To deal with wireless channel errors, we introduce a NACK signal which is a continuing busy tone signal when the receiver determines that the received DATA packet is corrupted. The sender will not misinterpret this NACK signal since there are no other receivers in its

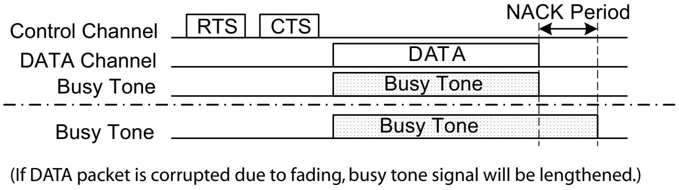


Fig. 3. Proposed protocol.

sensing range and hence no interfering NACK signals. It will conclude that the transmission is successful if no NACK signal is sensed.

Our protocol DUCHA adopts the same transmission power and capture threshold CP_{Thresh} in both control and DATA channels. And the transmission power level for correct receiving RX_{Thresh} is also the same for the two channels so that the two channels have the same transmission and sensing range. The basic message exchange sequence is shown in Fig. 3.

B. Basic Message Exchange

1) RTS: Before initiating a new transmission of an RTS, any node must sense the control channel idle at least for DIFS and sense no busy tone signal. If it senses the noisy (busy) control channel longer than or equal to the RTS period, it should defer long enough (at least for SIFS + CTS + 2 × max-propagation-delay) to avoid possible collision to the CTS's reception at some other sender. For example, in Fig. 1, when A finishes transmitting its RTS to B, F should wait at least long enough for A to finish receiving the possible CTS/NCTS from B.

2) CTS/NCTS : Any node correctly receiving the RTS should return CTS after SIFS spacing regardless the control channel status if the DATA channel is idle. If both control and DATA channels are busy, it ignores the RTS to avoid possible interference to the reception of CTS at other transmitter. If the control channel has been idle for at least one CTS packet long and the DATA channel is busy, it returns NCTS. The NCTS provides the estimate for the remaining DATA transmission time in its duration field according to the difference between the transmission time of maximum DATA packet and the length it has sensed a busy medium in the DATA channel.

3) DATA: A transmitter, after correctly receiving the CTS, should start DATA transmission if no busy tone signal is detected. If the transmitter receives an NCTS, it defers its transmission according to the duration field of NCTS. Otherwise, it assumes that there is a collision, will then double its backoff window and defer its transmission.

4) Busy Tone: The intended receiver begins to sense the data channel after it transmits CTS. If the receiver does not receive signal in the data channel in the due time (for the first few bits of the DATA packet), it will assume that the sender does not transmit DATA. Otherwise, it transmits the busy tone signal to prevent hidden terminals from possible transmissions.

5) NACK: The intended receiver has a timer to indicate when it should finish the reception of the DATA packet according to the duration field in the previously received RTS. If the timer expires and has not received the correct DATA packet, it assumes that the DATA transmission fails and sends NACK by continuing the busy tone signal for an appropriate period. If it correctly receives the DATA packet, it stops the busy tone signal and finishes the receiving procedure.

The sender assumes that its DATA transmission is successful if there is no NACK signal sensed during the NACK period. Otherwise, it assumes that its transmission fails because of wireless channel error and then starts the retransmission procedure.

In addition, during the NACK period and the DATA transmission period, any other nodes in the sensing range of the sender are not allowed to become the receiver of DATA packets, and any other nodes in the sensing range of the receiver are not allowed to become the sender of DATA packets. This is to avoid confusion between NACK signals and the normal busy tone signals.

In the above message exchange, our protocol transmits or receives packets in only one channel at any time. We only use receive busy tone signal, but not transmit busy tone signal. So it is necessary to sense the DATA channel before transmitting CTS/NCTS packets to avoid becoming a receiver in the sensing range of the transmitters of the ongoing DATA packet transmissions.

C. Solutions to the Aforementioned Problems

In the following discussions, we illustrate with examples how DUCHA solves those well-known problems.

1) Solution to the Hidden Terminal Problem: As shown in Fig. 1, B broadcasts a busy tone signal when it receives DATA packet from A. The hidden terminal of A, i.e., D, could hear B's busy tone signal and thus will not transmit in the DATA channel to avoid interference with B's reception. Thus, the busy tone signal from the DATA's receiver prevents any hidden terminals from interfering with the reception. Therefore, no DATA packets are dropped due to the hidden terminal problem.

2) Solution to the Exposed Terminal Problem: In Fig. 1, B is the exposed terminal of D when D is transmitting DATA packet to E. B could initiate RTS/CTS exchange with A though it can sense D's transmission in the DATA channel. After the RTS/CTS exchange is successful between B and A, B begins to transmit DATA packet to A. Since A is out of the sensing range of D and E is out of sensing range of B, both A and E could correctly receive the DATA packet destined to them. Thus, an exposed terminal could transmit DATA packets in DUCHA, which could greatly enhance the spatial reuse ratio.

3) Solution to the Receiver Blocking Problem: In Fig. 1, B is the blocked receiver in the IEEE 802.11 MAC when D is transmitting DATA packets to E. In our protocol DUCHA, B can correctly receive A's RTS in the control channel while D sends DATA packets in the DATA channel. Then B returns NCTS to A because it senses busy medium in the DATA channel. The duration field of NCTS contains the estimate for the remaining busy period in the DATA channel which takes to finish D's transmission. When A receives the NCTS, it defers its transmission and stop the unnecessary retransmissions. It retries the transmission after the period indicated in the duration field of NCTS. Once the RTS/CTS exchange is successful between A and B, A begins to transmit DATA packet to B. B will correctly receive the DATA packet because there is no hidden terminal problem for receiving DATA packets.

4) Improvement of Spatial Reuse: As discussed above, an exposed terminal could transmit DATA packets. Furthermore, in our protocol, a hidden terminal could receive DATA packets though it cannot transmit. In Fig. 1, D is the hidden terminal of A when A is transmitting DATA packet to B. After the RTS/CTS exchange between E and D is successful in the control channel, E could transmit DATA packets to D. Since D is out of A's sensing range and B is out of E's sensing range, both D and E could correctly receive the intended DATA packets. Thus DUCHA could greatly increase spatial reuse by allowing multiple transmitters or multiple receivers in the sensing range of each other to communicate. At the same time, there are no collisions for DATA packets as well as the NACK signals because there is only one transmitter in its intended receiver's sensing range and only one receiver in its intended transmitter's sensing range.

5) Inherent Mechanism to Solve the Intra-Flow Contention Problem: In our DUCHA protocol, the receiver of DATA packets have the highest priority to access the channel for next DATA transmission. When one node correctly receives a DATA packet, it could immediately start the backoff procedure for the new transmission while the upstream and downstream nodes in its sensing range are prevented from transmitting DATA packets during the NACK period. In fact, this could achieve optimum packet scheduling for chain topology and it is similar to any single flow scenario.

For example, in Fig. 2, node 1 has the highest priority to access the channel when it receives one packet from node 0 and hence immediately forwards the packet to node 2. For the same reason, node 2 immediately forwards the received packet to node 3. Then node 3 forwards the received packet to node 4. Because node 0 can sense transmissions from nodes 1 and 2, it will not interfere with these two nodes. Node 0 could not send packets to node 1 either when node 3 forwards packet to 4 because node 1 is in the interference range of node 3. When node 4 forwards packet to 5, node 0 could have a chance to send packet to node 1. In general, nodes which are 4 hops away from each other along the path could simultaneously send packets to their next hops. Thus the procedure could utilize 1/4 of the channel bandwidth, the maximum throughput which can be approached by the chain topology [8].

D. Remarks on the Proposed Protocol

There is no collision for DATA packets in the proposed protocol because there is only one DATA transmitter in the sensing range of any ongoing receiver in the DATA channel. The out-of-band busy tone signal prevents any hidden node from initiating a new DATA transmission in the DATA channel.

There is no collision for NACK signal, i.e., the continuing busy tone, either, because there is only one DATA receiver in the sensing range of any ongoing transmission in the DATA channel. After successful RTS/CTS exchange between the sender and its intended receiver, all other nodes in the sensing range of the sender can sense its transmission in the DATA channel and thus are restricted from becoming DATA receivers.

The control overhead could be reduced although we introduce a new NCTS packet and a new NACK signal. First, NCTS is transmitted only when the intended receiver does not receive DATA packet correctly. It saves a lot of unnecessary retransmitted RTS packets as discussed in Section IV-C.3. Second, NACK signal occurs only when the DATA packet is corrupted due to channel fading, and hence its transmission frequency is also much smaller than that of ACK packets in the 802.11 MAC protocol. Third, there is no collision in DATA packets and hence the transmissions of RTS and CTS for corrupted DATA packets are avoided.

V. Performance Evaluation

A. Simulation Environments

We now evaluate the performance of our DUCHA protocol and compare it with the IEEE 802.11 scheme. The simulation tool is one of the widely used network simulation tools – *ns2*. The propagation model is the two-ray ground model. The transmission range of each node is approximately 250m. The data rate for the IEEE 802.11 protocol is 1Mbps, and the data rates for the DUCHA protocol are 220Kbps and 780Kbps for the control and data channel, respectively. The length of the physical preamble is 192bits. The length of NACK signal is 150μs. The data packet size is 1000bytes. The capture threshold is 10dB.

In our simulation study, several important performance metrics are evaluated, which are described below:

- *Aggregate end-to-end throughput* – The sum of data packets delivered to the destinations.
- *Aggregate one-hop throughput* – The sum of all the packets delivered to the destinations multiplied by hop count. This metric measures the total resource efficiently utilized by the applications or the traffic. If all flows are one-hop flows, this is the same as the aggregate end-to-end throughput, referred to as the *aggregate throughput* in the figures.
- *Transmission efficiency of DATA packets* – The ratio of the aggregate one-hop throughput to the number of the transmitted DATA packets. This metric reflects the resource wasted by the collided DATA packets and the discarded DATA packets due to the overflow of queue at the intermediate nodes of the path.
- *Normalized control overhead* – The ratio of all kinds of control packets including RTS, CTS, NCTS and ACK to the aggregate one-hop throughput.

The *collided DATA packets* and the *discarded DATA packets* have also been evaluated in some cases. The collided DATA packets are those transmitted but corrupted by the hidden terminals. The discarded DATA packets are those discarded due to continuous failed retransmissions of RTS or DATA packets.

B. Simple Scenarios

To verify the correctness of our protocol, we first investigate one simple scenario shown in Fig. 4, where there are hidden terminals, exposed terminals and receiver blocking problems if IEEE 802.11 MAC protocol is used.

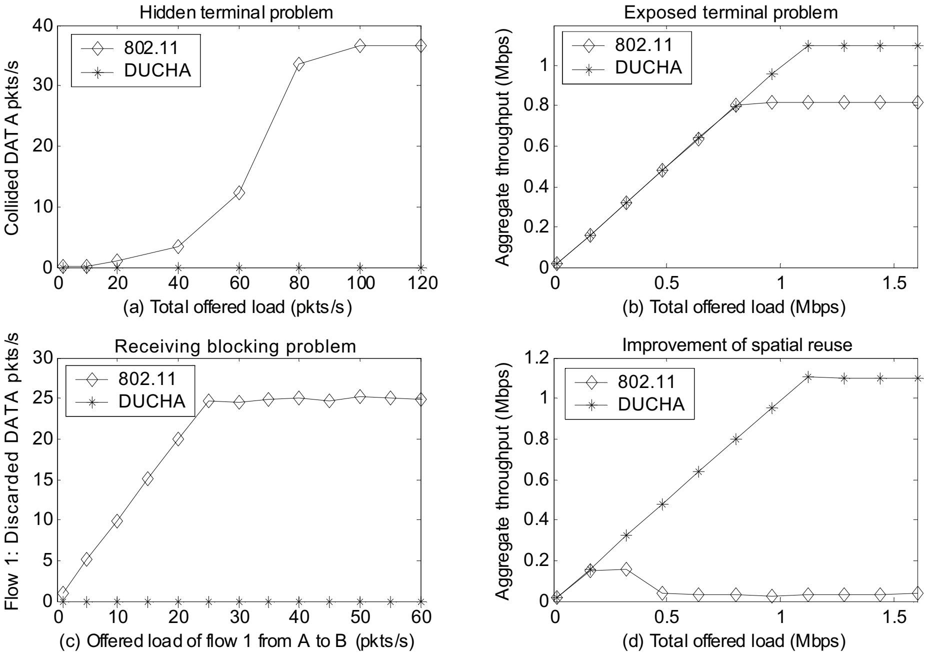


Fig. 5. Simulation results for the simple topology.

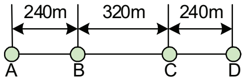


Fig. 4. One simple topology.

1) Hidden Terminals: There are two flows with the same CBR traffic: flow 1 is from A to B and flow 2 is from C to D. C is the hidden terminal of A. Fig. 5 (a) shows that the number of collided DATA packets increases with the offered load in IEEE 802.11 while our protocol has no collisions with the DATA packets. This in fact verifies that there is no hidden terminal problem for the transmission of DATA packets in our protocol. The reason is that B's busy tone signal prevents the hidden terminal C from transmitting and hence there is no collision at B and hence B can still receive A's DATA packets. However, in the IEEE 802.11 MAC protocol, C has no way to know that A is transmitting DATA packets to B and hence cause collisions at B if C begins transmissions.

2) Exposed Terminals: We now examine the exposed terminal problem. Assume that there are two flows with the same CBR traffic: one is from B to A and another is from C to D. B and C are the exposed terminals of each other. In IEEE 802.11 MAC, B and C cannot transmit DATA packets at the same time while they can in our DUCHA. So our protocol should have much higher aggregate throughput in this simple scenario under heavy offered load. The improvement is about 35% as shown in Fig. 5 (b).

3) Receiver Blocking Problem: The topology remains the same as in Section V-B.1 except C always has packets to transmit to D. Fig 5 (c) shows that there are lots of discarded DATA packets in IEEE 802.11 while there are none in DUCHA. This is because that in IEEE 802.11 the blocked receiver B of the sender A, could not correctly receive A's RTS and thus A continuously discards DATA packets after multiple transmission failures of RTS packets and A cannot successfully transmit any packets. While in our protocol DUCHA, the control packets are transmitted in a separate channel and the blocked receiver could return an NCTS packet to its intended sender during the period of neighboring DATA transmissions. Furthermore, in our protocol, A can obtain a part of the bandwidth to transmit DATA packets while in IEEE 802.11, A's DATA transmissions will be corrupted by its hidden terminal C even if the RTS-CTS exchange is successful between A and B.

4) Improvement of Spatial Reuse: Our DUCHA protocol could allow a hidden terminal to receive DATA packets as well as to allow an exposed terminal to transmit DATA packets to improve the spatial reuse. In the simulation, there are two flows with the same CBR traffic: flow 1 is from A to B and flow 2 is from D to C. Fig. 5 (d) shows that our protocol has up to 37 times higher aggregate throughput than IEEE 802.11 MAC. The latter suffers not only from the poor spatial reuse but also from the collisions among RTS, CTS, DATA and ACK packets since B and C are hidden terminals of A and D, respectively.

5) Intra-Flow Contention: Our protocol DUCHA could mitigate the intra-flow contention as discussed in section IV. Fig. 6 shows the aggregate throughput of a 9-node chain topology. DUCHA improves the throughput by about 33% compared with IEEE 802.11 MAC under heavy offered load. This is because DUCHA has a large spatial reuse ratio in the DATA channel and could achieve the optimum packet scheduling for the chain topology independent of the traffic load while IEEE 802.11 MAC suffers from collisions under heavy load.

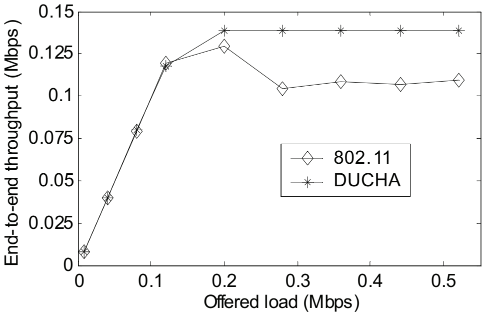


Fig. 6. End-to-End throughput for the 9-node chain topology.

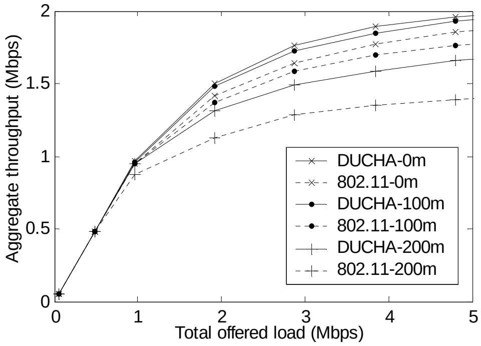


Fig. 7. Simulation results for random one-hop flows with different minimum one-hop distance.

C. Random Topology for One-hop Flows

In this simulation study, 60 nodes are randomly placed in a 1000m x 300m area. Each node has the same CBR traffic and randomly selects one neighbor as the destination, which is at least the minimum source-destination distance, i.e., 0, 100, 200 m, far apart. All results are averaged over 30 random simulations.

We observe from Fig. 7 that the aggregate throughput for all flows decreases when the minimum source-destination distance increases. The aggregate throughput of our protocol is higher than that of IEEE 802.11 MAC, degrades much slower in our protocol than in IEEE 802.11 MAC, and is improved by up to 20% when the minimum source-destination distance increases from 0m to 200m.

This is reasonable. For example, A and B are the source-destination pair. The larger the distance between A and B, the larger the hidden terminal area, in which nodes cannot sense A's transmission but can sense B's transmission. So in IEEE 802.11 MAC, the hidden terminal problem becomes more severe when the distance between A and B becomes larger. On the other hand, in IEEE 802.11 MAC, all the nodes in the sensing range of A or B should not transmit, i.e., both sensing ranges of A and B could not be reused by other transmissions. However, in our protocol DUCHA, the exposed terminal area, in which nodes can sense the sender's transmission but not the receiver's transmission, could be reused for new senders, and the hidden terminal area could be reused for new receivers. Thus the larger the source-destination distance is, the higher the system capacity our protocol DUCHA could achieve comparing with the IEEE 802.11 MAC.

In fact, most current routing algorithms maximize the distance between the upstream node and the downstream node when selecting a path to reduce the hop-count, the delay and the power consumption for delivering the packets from the source to the destination. Our protocol DUCHA also gives a good solution to the intra-flow contention problem and could achieve optimum packet scheduling for the chain topology.

D. Random Topology for Multihop Flows

In this simulation study, 60 nodes are randomly placed in a 1000m x 300m area. The source of each flow randomly selects one node as the destination, which is with at least certain minimum hops away, i.e., 3 or 5 hops. There are total 20 flows with the same CBR/UDP traffic in the network. We use pre-computed shortest path with no routing overhead. All results are averaged over 30 random simulations.

1) Aggregate End-to-End Throughput: We observe from Fig. 8 (a) that when the minimum hop-count for each flow increases, the aggregate end-to-end throughput of both protocols decreases. This is reasonable because packets of multihop flows have to pass more links and thus consume more resource for the same arriving traffic.

The throughput of IEEE 802.11 MAC reduces more dramatically than that of DUCHA when the minimum hop-count for each flow increases. The improvement of throughput comparing to the IEEE 802.11 MAC is up to 5 times, respectively, for the scenarios where the minimum of the hop-counts for all flows are 3 and 5.

2) Aggregate One-Hop Throughput: Our protocol DUCHA has much higher aggregate one-hop throughput than the IEEE 802.11 MAC as shown in Fig. 8 (b). This implies that DUCHA could effectively utilize much more resource of the wireless ad hoc networks than IEEE 802.11 MAC.

The resource efficiently utilized by the flows greatly decreases in IEEE 802.11 MAC when the hop count of each flow increases, while our protocol DUCHA maintains a relatively high resource utilization ratio for multihop flows with different hop counts. And our protocol even efficiently utilizes more resource when the hop count for each flow increases. This implies that IEEE 802.11 MAC is not appropriate for multihop ad hoc networks while our protocol DUCHA works well and is scalable for larger networks where the flows have larger hop counts.

3) Transmission Efficiency of DATA Packets: The transmission efficiency of DATA packets in our protocol is also much higher than that in the IEEE 802.11 MAC. And the longer the path is, the greater the improvement of the transmission efficiency is, which can be observed in Fig. 8 (c).

In addition, our protocol maintains relatively stable transmission efficiency of DATA packets for flows with different hop counts while the IEEE 802.11 MAC degrades significantly when the hop count for each flow increases. The reason is that our protocol DUCHA not only does not have collided DATA packets, but also has much less accumulated and discarded packets at the intermediate nodes along the paths. This means that our protocol could save significant resource and lower the power consumption to deliver the same amount of DATA packets.

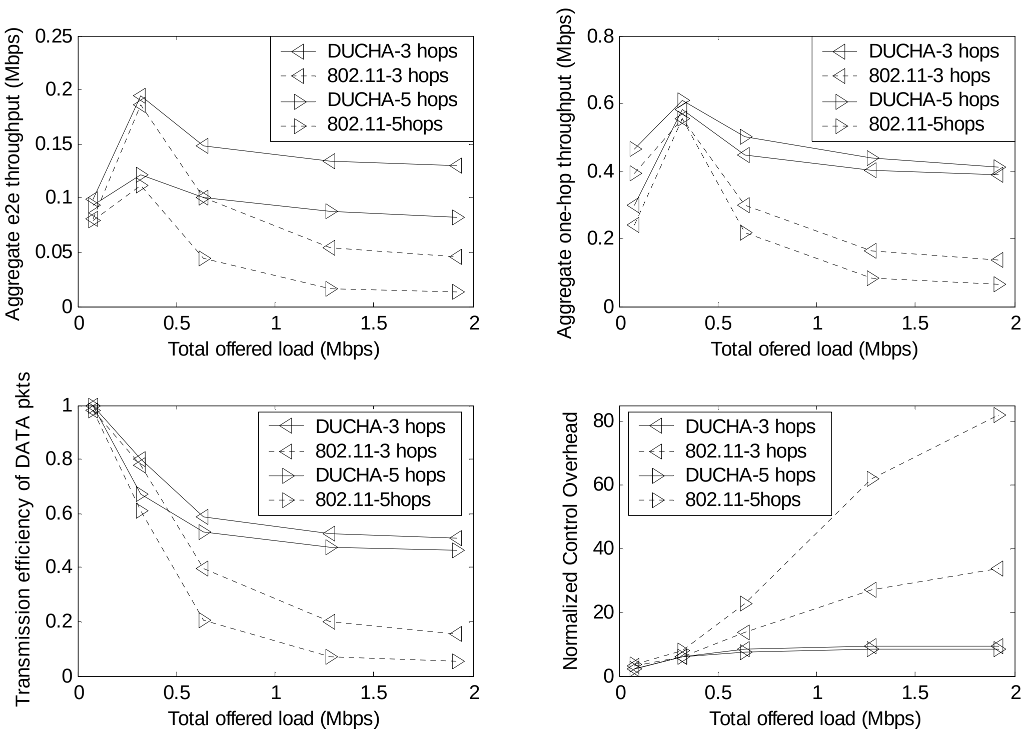


Fig. 8. Simulation results for multihop flows in random topology.

4) Normalized Control Overhead: From Fig. 8 (d), we observe that the normalized control overhead is also much lower in our protocol than that in the IEEE 802.11 MAC. It linearly increases with the offered load for the multihop flows in the IEEE 802.11 MAC while our protocol DUCHA maintains a small stable value. Moreover, similar to other performance metrics, the normalized control overhead maintains a relatively stable value for flows with different hop counts in our protocol DUCHA while in IEEE 802.11 MAC it becomes larger and larger when the hop count for each flow increases. This implies that our protocol has much higher efficiency in transmitting DATA packets. And IEEE 802.11 MAC does not work well for multihop flows especially under heavy load and will result in the "explosion" of control packets, leading to more control packets and lower throughput.

VI. Conclusions

This paper first identifies the sources of dramatic performance degradation of IEEE 802.11 MAC in multihop ad hoc networks and then presents a new MAC protocol DUCHA using dual channels, one is for control packets and the other is for DATA packets. Busy tone signal is used to solve the hidden terminal problem and also used to transmit the negative ACK (NACK) signal if necessary. Our protocol simultaneously solves the hidden terminal problem, the exposed terminal problem, the receiver blocking problem and also the intra-flow contention problem, and has much higher spatial reuse ratio than the IEEE 802.11 MAC. There are no collisions for DATA packets with much fewer control packets and lower discarded DATA packets. Our protocol uses the negative CTS (NCTS) to notify the sender that its intended receiver is blocked and cannot receive DATA packets while IEEE 802.11 MAC cannot distinguish it from unreachable destination. Thus, our protocol is more friendly to the routing layer with much fewer unnecessary rerouting requests by providing more accurate next-hop information.

Extensive simulations show that our protocol improves the throughput by up to 20% for one-hop flows and by several times for the multihop flows when it uses the same total bandwidth as that of the IEEE 802.11 MAC. In addition, our protocol is scalable for large networks, and maintains high resource utilization ratio and stable normalized control overhead while the IEEE 802.11 MAC does not work well for multihop flows under heavy traffic.

References

[1] "IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, ISO/IEC 8802-11: 1999(E)," Aug. 1999.

[2] L. Bao and J. J. Garcia-Luna-Aceves, "Distributed dynamic channel access scheduling for ad hoc networks," *J. Parallel and Distributed Computing*, vol. 63, no. 1, pp. 3-14, Jan. 2003.

[3] J. Broch, D. A. Maltz, D. B. Johnson, Y. Hu, and J. Jetcheva, "A performance comparison of multihop wireless ad hoc network routing protocols," in *Proc. ACM/IEEE MobiCom*, Oct. 1998, pp. 85-97.

[4] X. Chen, H. Zhai, J. Wang, and Y. Fang, "TCP Performance over mobile ad hoc networks," *Canadian J. Electrical and Computer Engineering (CJECE) (Special Issue on Advances in Wireless Communications and Networking)*, vol. 29, no. 1/2, pp. 129-134, Jan./Apr. 2004.

[5] C. L. Fullmer and J. J. Garcia-Luna-Aceves, "Solutions to hidden terminal problems in wireless networks," in *Proc. ACM SIGCOMM*, Sep. 1997, pp. 39-49.

[6] Z. J. Haas and J. Deng, "Dual busy tone multiple access (DBTMA)-A multiple access control for ad hoc networks," *IEEE Trans. Commun.*, vol. 50, pp. 975-985, June 2002.

[7] Z. J. Haas and J. Deng, "Dual busy tone multiple access (DBTMA): Performance results," *Proc. IEEE WCNC*, Sep. 1999, vol. 3, pp. 1328-1332.

[8] J. Li, C. Blake, D. S. J. De Couto, H. I. Lee, and R. Morris, "Capacity of ad hoc wireless network," in *Proc. ACM MobiCom*, July 2001, pp. 61-69.

[9] Y. Li, H. Wu, D. Perkins, N. Tzeng, and M. Bayoumi, "MAC-SCC: Medium access control with a separate control channel for multihop wireless networks," in *Proc. 23rd International Conf. Distributed Computing Systems Workshops*, May 2003, pp. 764-769.

[10] J. Monks, V. Bharghavan, and W. Hwu, "A power controlled multiple access protocol for wireless packet networks," in *Proc. IEEE INFOCOM*, Apr. 2001, vol. 1, pp. 219-228.

[11] A. Muqattash and M. Krunz, "Power controlled dual channel (PCDC) medium access protocol for wireless ad hoc networks," in *Proc. IEEE INFOCOM,* Mar. 2003, vol. 1, pp. 470-480.

[12] C. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Pers. Commun.*, pp. 16-28, Feb. 2001.

[13] S. Singh and C. S. Raghavendra, "PAMAS-Power aware multi-access protocol with signalling for ad hoc networks," *Computer Commun. Review*, July 1998, pp. 5-26.

[14] J. So and N. H. Vaidya, "Multi-channel MAC for ad hoc wireless networks: Handling multi-channel hidden terminals using a single transceiver," in *Proc. ACM MobiHoc*, May 2004, pp. 222-233.

[15] F. A. Tobagi and L. Kleinrock, "Packet switching in radio channels: Part II–The hidden terminal problem in carrier sense multiple-access and the busy-tone solution," *IEEE Trans. Commun.*, vol. 23, pp. 1417-1433, Dec. 1975.

[16] S.-L. Wu, C.-Y. Lin, Y.-C. Tseng, and J.-P. Sheu, "A new multi-channel MAC protocol with on-demand channel assignment for mobile ad hoc networks," in *Proc. Int'l Symp. on Parallel Architectures, Algorithms and Networks*, Dec. 2000, pp. 232-237.

[17] S. Wu, Y. Tseng, and J. Sheu, "Intelligent medium access for mobile ad hoc networks with busy tones and power control," *IEEE J. Select. Areas Commun.*, vol. 18, pp. 1647-1657, Sep. 2000.

[18] S. Xu and T. Safadawi, "Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?" *IEEE Commun. Mag.*, pp. 130-137, June 2001.

[19] H. Zhai, X. Chen, and Y. Fang, "Alleviating intra-flow and inter-flow contentions for reliable service in mobile ad hoc networks," in *Proc. IEEE MILCOM*, Nov. 2004, vol. 3, pp. 1640-1646.

[20] H. Zhai, X. Chen, and Y. Fang, "How well can the IEEE 802.11 wireless LAN support quality of service?" *IEEE Trans. Wireless Commun.*, vol. 4, no. 6, pp. 3084-3094, Nov. 2005.

[21] H. Zhai and Y. Fang, "Distributed flow control and medium access control in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 5, no. 11, Nov. 2006.

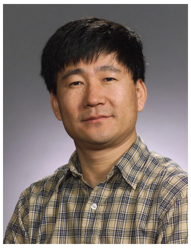
[22] H. Zhai, Y. Kwon, and Y. Fang, "Performance analysis of IEEE 802.11 MAC protocols in wireless LANs," *Wiley Wireless Communications and Mobile Computing*, vol. 4, pp. 917-931, Dec. 2004.

[23] H. Zhai, J. Wang, X. Chen, and Y. Fang, "Medium access control in mobile ad hoc networks: Challenges and solutions," *Wiley Wireless Communications and Mobile Computing*, vol. 6, no. 2, pp. 151-170, Mar. 2006.

[24] H. Zhai, J. Wang, and Y. Fang, "Distributed packet scheduling for multihop flows in ad hoc networks," in *Proc. IEEE WCNC*, Mar. 2004, vol. 2, pp. 1081-1086.

Hongqiang Zhai (S'03) received the B.E. and M.E. degrees in electrical engineering from Tsinghua University, Beijing, China, in July 1999 and January 2002 respectively. He worked as a research intern in Bell Labs Research China from June 2001 to December 2001, and in Microsoft Research Asia from January 2002 to July 2002. Currently he is pursuing the PhD degree in the Department of Electrical and Computer Engineering, University of Florida. His current research interests include medium access control, quality of service, cross-layer design and performance analysis of wireless networks. He is a student member of IEEE.

Jianfeng Wang (S'03) received the B.E. and M.E. degrees in electrical engineering from Huazhong University of Science and Technology, Wuhan, China, in 1999 and 2002 respectively. Now he is working toward the Ph.D. degree in the Department of Electrical and Computer Engineering, University of Florida. His current research interests include wireless MAC, wireless multimedia, IP QoS, seamless mobility, radio resource management, and system coexistence for 3G/4G cellular networks, WLANs, WPANs, mobile ad hoc networks, wireless mesh networks, and wireless sensor networks. He is a student member of the IEEE.



Yuguang Fang (S'92-M'94-S'96-M'97-SM'99) received a Ph.D. degree in Systems Engineering from Case Western Reserve University in January 1994 and a Ph.D degree in Electrical Engineering from Boston University in May 1997. He was an assistant professor in the Department of Electrical and Computer Engineering at New Jersey Institute of Technology from July 1998 to May 2000. He then joined the Department of Electrical and Computer Engineering at University of Florida in May 2000 as an assistant professor, got early promotion to Associate Professor with tenure in August 2003 and to Full Professor in August 2005, and is a University of Florida Research Foundation (UFRF) Professor from 2006 to 2009. He has published over 200 papers in refereed professional journals and conferences. He received the National Science Foundation Faculty Early Career Award in 2001 and the Office of Naval Research Young Investigator Award in 2002. He has served on the editorial board of several technical journals including *IEEE Transactions on Communications*, *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Mobile Computing* and *ACM Wireless Networks*.