結合新排程媒介存取控制機制之 AODV 協定

周碩聰*
彭賓鈺**
姜子龍***

摘　要

在隨意式無線網路(Ad Hoc Network)中，各結點與相鄰的結點共用同一個無線通道，由於結點間互相競爭(Contention)使用同一無線資源，將因無線頻道壅塞而產生資料訊框(Data Frame) 的碰撞(Collision)，導致隨意式無線網路效能低落。有鑑於此，許多的文獻皆說明: 傳統的 IEEE 802.11 媒介存取控制採用競爭模式，無法減少資料訊框的碰撞、舒緩無線通道壅塞，使得隨意式無線網路的整體效能無法有效地提升。本論文將以網路層 AODV 協定及資料鏈結層 IEEE 802.11 協定作為研究標的，根據隨意式無線網路的主動式路由及多點跳躍特性，提出一種新的媒體層（Medium Access Control, MAC）排序演算法；將上層 AODV 路由協定之資料傳輸路徑總長及距離目的地節點剩餘跳躍數當作耦合參數，傳遞給下層 IEEE 802.11 協定，做為後續各結點競爭視窗(Contention Window)大小的計算依據。此一架構將改善上層 AODV 協定的網路傳輸效能，達到較高的資料封包傳輸率(Throughput)、較好的資料封包成功送達率（Packet Delivery Ratio）、較小且穩定的資料封包路由成本（Routing Load）及較低的鏈路失敗機率（Link-failure Probability）。最後，我們將經由電腦模擬來驗證本論文所提策略之正確性與優越性。

關鍵詞：競爭視窗、接收端壅塞、內部資料流競爭、鏈結失敗率、發送端訊框成本、
目的端訊框成本

---

*康寧大學 資訊管理科 助理教授(通訊作者)
**康寧大學 資訊管理科 講師
***康寧大學 資訊管理科 講師
電子郵件：frank@ukn.edu.tw

收稿日期：2017.11.15　　修改日期：2018.03.12　　接受日期：2018.03.22

A New Scheduling MAC Mechanism for AODV Protocol

So-Tsung Chou*
Bin-Yu Peng**
Tzyy-Long Jian***

Abstract

In a multi-hop ad hoc network, nodes contend for shared wireless channel with neighbors. The contention results in congestion and greatly degrades the performance of a network due to severe packet collisions. Several recent studies have shown that the performance of multi-hop ad hoc network is poor and the IEEE 802.11 scheme fails to achieve optimum scheduling for medium access contention. The present study demonstrtates a multi-hop packet scheduling framework to achieve high throughput, good packet delivery ratio, low routing load, and small link-failure probability in ad hoc environments. The routing information about the total hop count and the remaining hop count, required by a packet to reach its destination, is exploited by this scheme in the MAC layer to recalculate the contention window size of the nodes along routing path and to give priorities for the packets that are closer to their destination. Extensive simulations show that the proposed scheme is able to earn significant improvement over the conventional algorithm.

Key Words: contention window, receiver blocking, intra-flow contention, link failure probability, frame cost of source, frame cost of destination

---

*Assistant Professor, Department of Information Management, University of Kang Ning (correspondence author)
**Lecturer, Department of Information Management, University of Kang Ning.
***Lecturer, Department of Information Management, University of Kang Ning.

1. INTRODUCTION

With the advancement of wireless technology, we have witnessed an ever-increasing popularity of wireless networks in recent years. Wireless local area networks, or Wi-Fi hot spots, have been widely deployed in cities, college campus, airports, coffee bars, conference halls, hotels, and many other public places. Nevertheless, wireless local area network is limited to one-hop communication between clients and access points. It restricts wireless access to a small range. If communication devices are allowed to forward packets for others, a multi-hop ad hoc network can be formed, and the range of wireless access to Wi-Fi hot spots can be significantly extended. This kind of wireless multi-hop communication could be used in many applications such as environmental monitoring and health care.

In a multi-hop ad hoc network, nodes communicate with each other using wireless links of each node, and there is no stationary infrastructure such as access point or base station. Each node acts as a host as well as a router and forwards data packets for other nodes. A central challenge in the design of multi-hop ad hoc network is the development of dynamic routing protocol that can efficiently find routes between two communication nodes. Many protocols, such as dynamic destination sequenced distance vector (DSDV) (Perkins and Bhagwat, 1994), dynamic source routing (DSR) (Johnson and Maltz, 1996), ad hoc on demand distance vector (AODV) (Perkins and Royer, 1999), temporally ordered routing algorithm (TORA) (Park and Corson, 1997), and zone routing protocol (ZRP) (Pearlman and Haas, 1999) etc., have been proposed.

However, we focus on another issue in a multi-hop ad hoc network— data transmission efficiency. The wireless medium is a shared and scarce resource in ad hoc network. How to efficiently control the access of this shared medium becomes important and complicated. In a multi-hop ad hoc network, nodes have to cooperate to forward each other’s packets through the routing path. Because of the contention for the shared channel, the throughput of each single node is limited not only by the channel capacity itself but also by transmissions in the neighborhood. That is to say, the transmission at each hop has to contend for the channel with upstream and downstream nodes. This effect results in congestion at some nodes along the routing path and seriously limits the performance of a multi-hop ad hoc network. Li (2001), Xu (2001), and Basavaraju (2006) et al., found that the IEEE 802.11 mechanisms fail to achieve the optimum scheduling for multi-hop flows and greatly degrade the performance for the chain topology with heavy load. In fact, the end to end throughput of a multi-hop flow even degrades below 1/4 of the channel bandwidth. This result severely impacts the practicability and scalability of an ad hoc network.

In order to alleviate the congestion of the shared medium, several papers have developed the dynamic load balancing algorithms. Lee and Gerla (2001) presented a dynamic load-aware routing algorithm (DLAR) which used the traffic load of intermediate nodes as the route selection criterion. It periodically monitors the status of active data sessions and dynamically reconfigures the routes that are being congested. Lee and Campbell (2003) presented a hot spot mitigation protocol (HMP) where hot spots represent transient and highly congested regions. HMP balances resource consumption among neighboring nodes by suppressing new route requests and controlling TCP flow rate. These solutions focus only on the routing algorithms and do not consider the MAC layer contentions which result in different problems of channel access at the neighboring nodes.

Many protocols have been proposed to alleviate some problems for the MAC layer. Ye et al. (2003) presented two MAC layer enhancements, i.e., quick-exchange and fast-forward, to address self-contention in an ad hoc network. Although they could decrease some transmission negotiation procedures, e.g. the RTS/CTS exchanges, but not address the congestion problem due to the MAC layer contentions. Li & Knightly (2002) and Kanodia et al. (2001) proposed two schemes, the distributed priority scheduling and the multi-hop coordination, which assigned different priorities to back off the contention window for accessing the wireless channel. Their schemes satisfy the end to end QoS requirement better than the IEEE 802.11 scheme, but still do not solve the MAC congestion problem either.

In this paper, a new scheduling scheme based on the interaction between network layer and MAC layer is proposed. In our proposed scheme, two parameters, the total hop count and the remaining hop count to destination, are required at forwarding nodes. However, neither a source node nor a forwarding node has the information at MAC layer. The two parameters will be earned through the routing discovery at network layer; then the information will be transmitted to the MAC layer. These parameters now can be used to recalculate the IEEE 802.11 contention window of the nodes along routing path. The salient feature of our proposed scheme is to generalize the packet scheduling of chain topology to improve medium access contentions and to efficiently conduct each flow in ad hoc network. This new scheduling scheme suppresses packet collision in the MAC layer and results in better performances of data transmission in the network layer than conventional schemes.

The rest of this paper is organized as follows. In section 2 we briefly review the IEEE 802.11 MAC standard and the AODV routing protocol; section 3 introduces our proposed a new scheduling scheme. In section 4 we describe the simulation environment which is followed by the discussion of simulation results and analyses. Finally, we conclude this paper in section 5

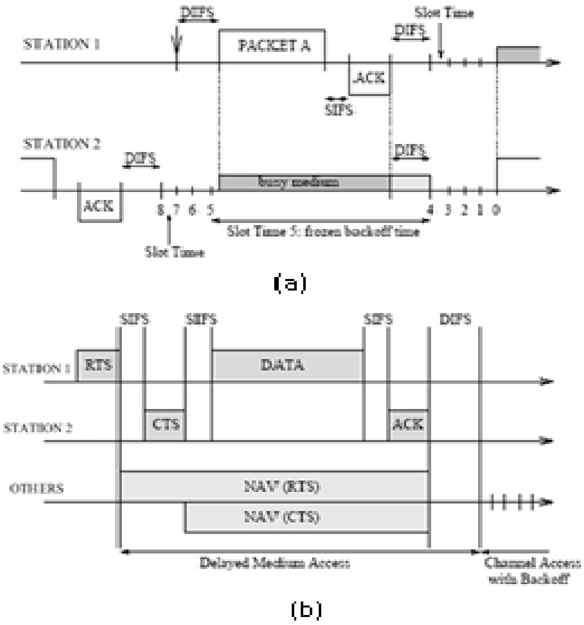
2. BACKGROUND AND PROTOCOL OVERVIEW

In this section, an overview of two related protocols is given. Our proposed scheme adopted the IEEE 802.11 distributed coordination function (DCF) as the medium access control protocol in the MAC layer and the AODV routing protocol to find a routing path in the network layer.

2.1 IEEE 802.11 DCF standard

This subsection briefly summarizes the distributed coordination function as standardized by the IEEE 802.11 Working Group (1999). A station with a new packet for transmission needs to monitor the channel activity first. If the channel is idle for a period of time equal to the distributed inter-frame space (DIFS), the station starts to transmit instantly. Otherwise, the channel is busy and the station persists to monitor the channel until it is measured idle for a DIFS. At this point, the station generates a random back off interval before transmitting in order to minimize the probability of multiple stations simultaneously starting transmission. Furthermore, to avoid channel capture a station must wait a random back off time between two consecutive-packet transmissions, even if the medium is sensed idle for a DIFS time period after the previous transmission. An ACK is transmitted by the destination to signal the source about the successful packet reception after a short inter-frame space (SIFS) at the end of the received packet.

The two-way handshaking technique for packet transmission described above is called basic access mechanism, shown in Figure 1(a). DCF also defines an optional four-way handshaking technique for packet transmission. This mechanism, also known as RTS/CTS, is shown in Figure 1(b). A station that has a packet queued for transmission follows the back off rules explained above, but instead of transmitting the data packet; it preliminarily transmits a special short frame called request to send (RTS). When the destination detects a RTS frame, it responds with a clear to send (CTS) frame after a SIFS time period. The source is only allowed to transmit the data packet if the CTS frame is correctly received within a duration called CTS_Timeout. The RTS frame and the CTS frame carry the information about the length of the packet to be transmitted. This information can be read by any listening station which is then able to update a network allocation vector (NAV), containing the information about the period of time in which the channel will remain busy. Therefore, when a station is hidden from either the transmitting or the receiving station, it can suitably delay further transmission by detecting just any one frame between the RTS and the CTS frames, and thus avoids packet collisions.



(a)

(b)

FIGURE 1

(a) Illustration of the basic access and back off mechanism for DCF.

(b) Illustration of the RTS/CTS and back off mechanism for DCF.

2.2 AODV routing protocol

Various routing algorithms for ad hoc networks have been proposed. One of the much interesting routing algorithms is the AODV protocol. AODV is an on demand dynamic routing protocol that uses routing tables with one entry per destination. When a source node needs a route to a destination, it initiates a route discovery process to locate the destination node. The source node floods a query packet, i.e. route request (RREQ), requesting a route to be set up to the destination. A reply packet, i.e. route reply (RREP), is sent back directly to the source node either by the destination itself or any other intermediate node that has a current route to the destination. On receiving a route request packet, intermediate nodes update their routing table for the reverse route to the source. Similarly, the forward route to the destination is updated on receiving a route reply packet. AODV uses sequence numbers to determine the timeliness of each packet and to prevent loops. Expire timers are used to keep the route entries fresh. Link failures are propagated by a route error (RERR) message, from the site of a link break, to the source node for that route. When the next hop link breaks, RERR packets are sent to a set of neighboring nodes that communicate over the broken link with their destinations. This recursive process erases all broken entries in the routing table of the nodes.

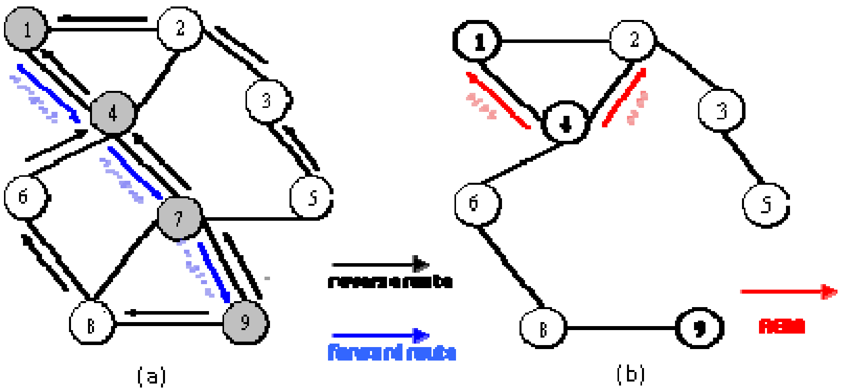


FIGURE 2
(a) A route is established between node 1 and node 9
(b) Scenario after the node 7 is switched off.

To describe the algorithm of AODV, an ad hoc network is shown in Figure 2(a) in which a process at node 1 wants to send data packets to node 9. Suppose that node 1 looks at its table and does not find an entry for node 9. It initiates discovery process for a route to node 9. In order to locate node 9, node 1 broadcasts a special RREQ packet. This packet reaches node 2 and node 4. Neither node 2 nor node 4 knows where node 9 is, so each of them creates a reverse route entry pointing back to node 1, and broadcasts the packet with hop count set to 1. The broadcast from node 2 reaches node 3 and node 4. Node 3 makes an entry for it in its reverse route table and rebroadcasts it. In contrast, node 4 rejects it as a duplicate. Similarly, node 4’s broadcast is rejected by node 2. However, node 4’s broadcast is accepted by node 6 and node 7. After node 5, 8, and node 9 receive the broadcast, the RREQ packet finally reaches the destination that knows where node 9 is.

In response to the incoming request, node 9 builds a RREP packet. This packet is unicasted to node 7 that the RREQ packet came from. It then follows the reverse path to node 4 and finally to node 1. The hop count is incremented at each node, so it knows how far from the destination (i.e., node 9) is. On the way back, the RREP packet is inspected at each intermediate node. It is added into the local routing table as a route to node 9. In this way, all the nodes on the reverse route learn the route to node 9, as a by-product of node 1’s route discovery. Nodes that received the original RREQ packet but were not on the reverse path (e.g., node 2, 3, 5, 6, and node 8) discard the reverse route table entry when the associated timer expires.

As an example of route maintenance, consider node 7 suddenly switches off. The changed topology is illustrated in Figure 2(b). When node 4 finds that node 7 is gone, it looks at its routing table and knows that node 7 was on routes to node 5, 7, and node 9. The union of the active neighbors for these destinations is the set {node 1, node 2}. In other words, node 1 and node 2 depended on node 7 for some of their routes, so they have to be informed that these routes no longer exist. Node 4 sends RERR packets to them (i.e., node 1 and 2) to update their own routing tables. Node 4 also purges the entries for node 5, 7, and, node 9 from its routing table.

In general, nodes reply to the first arriving RREQ; AODV favors the least congested route instead of the shortest route (Hu, Luo, and Shen, 2010). The AODV on-demand approach minimizes routing table information; however, it potentially leads to generate a large number of route requests (Bouhorma, Bentaouit, and Boudhir, 2009). AODV is also capable of broadcast, multicast, and multi-path routing. For more details, please refer to papers (Li, 2004; Sethi, 2009; Zhai, 2010; Li, 2010 et al.).

3. A NEW SCHEDULING MAC MECHANISM for AODV PROTOCOL

It has been shown in many articles that a multi-hop ad hoc network performs poorly with TCP as well as heavy UDP traffic (Tahiliani, 2010; Xiao, 2010; Walia, 2010; Liu, 2010; Zhang, 2010 et al.). Packets collide more severely in multi-hop ad hoc environment than in one-hop wireless infrastructure (Hirano, 2011; Zheng, 2011; Megha, 2011 et al.). In this section, we first investigate the inherent problems of the IEEE 802.11 MAC protocol in the shared channel environment of a multi-hop ad hoc network, and then illustrate our proposed design for the MAC and routing protocol.

3.1 Impact of the MAC layer contention on a traffic flow

The IEEE 802.11 MAC protocol has been successfully deployed in wireless local area networks and incorporated in many multi-hop ad hoc networks (Liu, 2010 and Megha, 2011 et al.). How to design an effective transmission scheme for ad hoc network based on the IEEE 802.11

standard is still open and challenging. However, there are still many problems that the IEEE 802.11 MAC protocol has not adequately addressed. The following subsections describe a few problems in a multi-hop ad hoc network while the IEEE 802.11 MAC protocol is deployed.

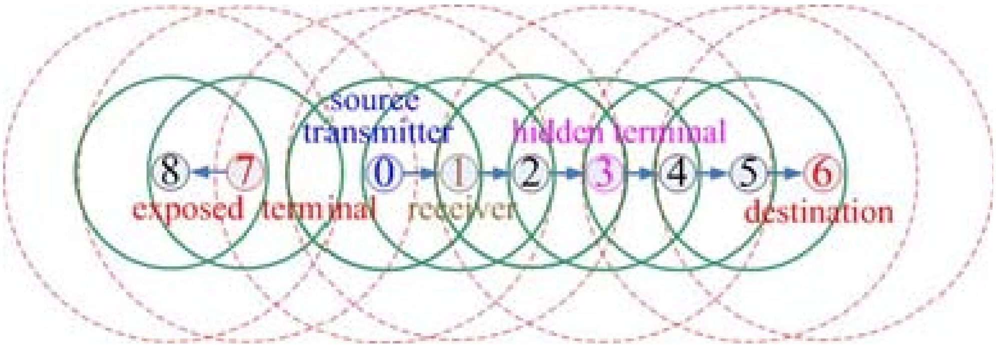


FIGURE 3
Illustration of the MAC interference among a chain topology

3.1.1 Hidden terminal problem

A hidden terminal is the one which is within the sensing range of the receiver, but out of the sensing range of the transmitter. The hidden terminal does not know that the transmitter is transmitting, and hence can initiate a transmission which results in a collision at the receiving node of the ongoing transmission. One example is shown in Figure 3, in which the small circles indicate the edges of the transmission range and the large circles represent the edges of the sensing range. Node 3 is a hidden terminal to node 0 when node 3 is transmitting to node 4, and it cannot sense node 0’s transmission but may still interfere with node 1’s reception if node 3 begins a transmission. The hidden terminal problem which introduces collision and packet loss in wireless network may lead to low throughput efficiency.

3.1.2 Exposed Terminal Problem

An exposed terminal is the one within the sensing range of the transmitter but out of the sensing range of the receiver. The exposed node senses the medium busy when the transmitter is transmitting, and does not transmit any packet, leading to bandwidth under-utilization. In Figure 3, node 7 is the exposed terminal to node 0 when node 0 is transmitting to node 1. Node 7 senses node 0’s transmission and keeps silent. Although node 7 can transmit to other node (e.g., node 8), which is outside of node 0’s sensing range without interfering with node 1’s reception. In fact, in the handshake procedures of IEEE 802.11, either RTS and CTS or DATA and ACK packets are bidirectional exchanged. Thus, the exposed node of one transmitter-receiver pair is also the hidden node of the same pair. That is to say, node 7 is also the hidden terminal to node 1 when node 1 replies CTS or ACK to node 0. So, in addition to the hidden terminal, the exposed terminal of the transmitter should not initiate any new transmission during the transmission cycle to avoid collision with the short packets (i.e., ACK or CTS). Thus, the carrier sensing strategy based on the IEEE 802.11 handshake will lead to a significant deficiency in spatial reuse.

3.1.3 Receiver blocking problem (channel capture)

The blocked receiver is the one that cannot respond to the intended RTS due to the other ongoing transmission in its sensing range. This may result in unnecessary retransmissions of RTS requests and discarding subsequent DATA packets. When the intended receiver is within the range of ongoing transmission, it cannot respond to the sender’s RTS according to the carrier sensing strategy in the IEEE 802.11 standard. The sender may attempt to retransmit several times if the back off times is smaller than the maximum number of retransmission allowed. Then, the contention window size becomes larger and larger when the RTS transmission fails, and the window size is doubled until the sender finally discards the packet. If the ongoing transmission finishes before the new sender reaches its maximum number of retransmission allowed, the old sender resets its contention window size and is much smaller in size than that of a new one. So the old sender has a high probability of continuing to transmit, and the new one continues doubling the contention window size and discards packets when the maximum number of transmission attempts is reached. This will result in serious unfairness and severe packet discarding among flows.

For example, as shown in Figure 3, when node 3 is transmitting packets to node 4, node 0 will not receive the intended CTS from node 1 if it sends RTS to node 1. Because node 1 cannot correctly receive node 0’s RTS due to collision from node 3’s transmission, node 0 keeps retransmitting and doubling the contention window size until it discards the packet. If node 3 has a burst of traffic, it will continuously occupy the channel, and will starve the flow from node 0 to node 1. Therefore, node 0 almost has no chance to successfully transmit a packet to node 1 when node 3 has packets destined to node 4.

3.1.4 Intra-flow contention problem

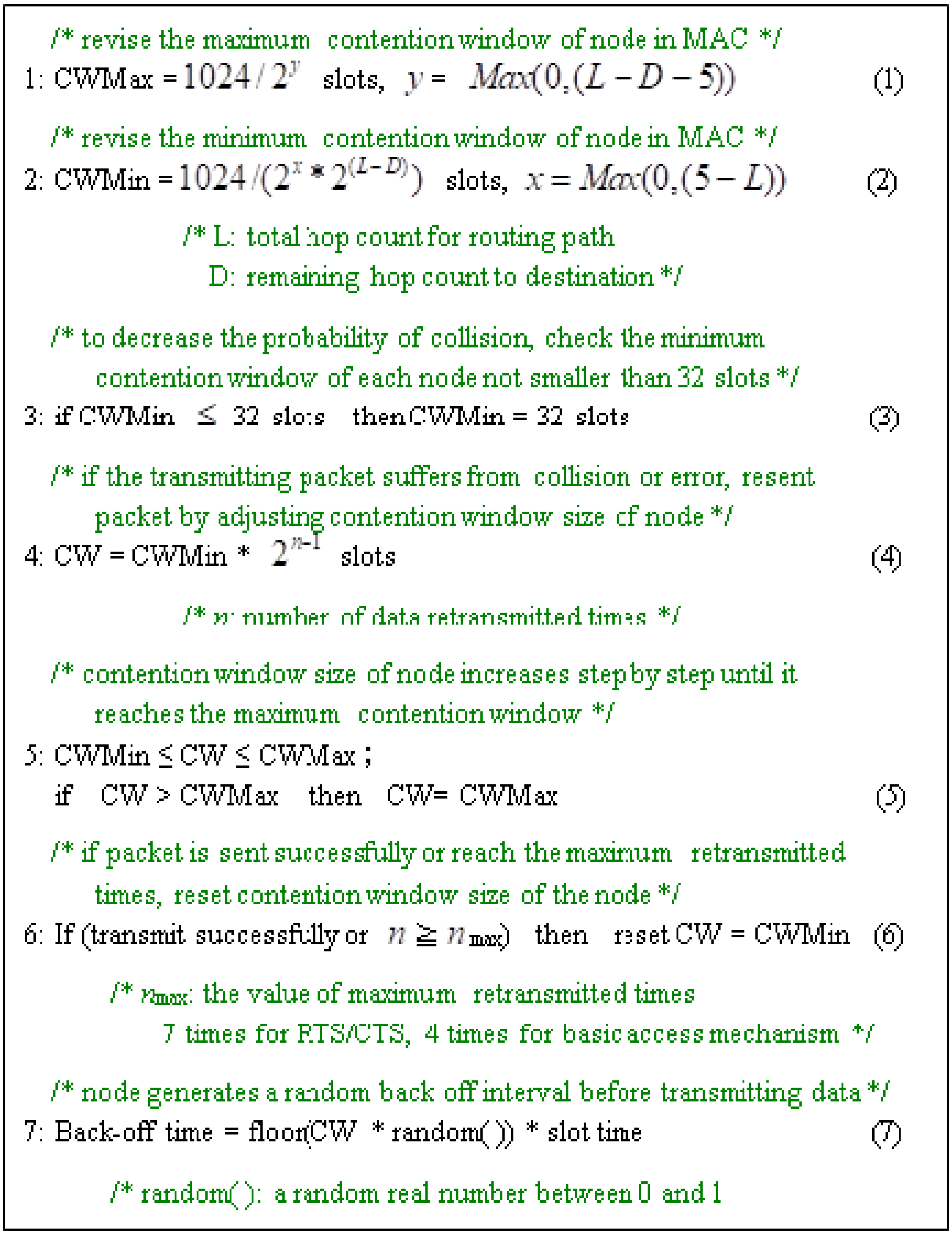
The intra-flow contention means the MAC layer contention, for the shared channel, among nodes that are in each other’s interference range along the routing path of the same flow. Nodes in a chain experience different amount of competitions, as shown in Figure 3. Node 0 is the source and node 6 is the destination. Assume for the moment that the radios of nodes can interfere with each other beyond the range, at which they can communicate successfully. Nodes 0 and node 1 cannot transmit at the same time because node 1 cannot receive and transmit simultaneously. Nodes 0 and node 2 cannot transmit at the same time because node 1 cannot correctly hear node 0 if node 2 is sending. Nodes 0 and node 3 cannot either. Thus the transmission of node 0 in a chain experiences interference from 3 subsequent nodes (i.e., node 1, 2, and 3); while transmission of node 1 is interfered with four other nodes (i.e., node 0, 2, 3, and 4), and transmission of node 2 is interfered with five other nodes (i.e., node 0, 1, 3, 4, and 5). This means that node 0, i.e. the source, could actually inject more packets into the chain than that the subsequent nodes can forward. These packets are eventually dropped at the two subsequent nodes (i.e., node 1 and 2). On the other hand, the redundant transmissions from node 0 grab the transmission opportunities of node 1 and node 2 because they cannot simultaneously transmit, and hence keep the end to end throughput far from the maximum value. This problem is called as intra-flow contention problem.

The source of the above problems comes mainly from the MAC layer. In fact, the IEEE 802.11 standard is only suitable for one-hop transmission in wireless infrastructure. These kinds of problems become more severe in multi-hop ad hoc environment; it results in throughput inefficiency, and seriously limits the performance of a network. Therefore, we argue that a good solution to the traffic flow and congestion control problems must consider both MAC characteristics and routing algorithm. An intuitive solution to the foregoing problems is to allow downstream nodes and congested ones to obtain higher probability of the channel access than that of upstream nodes to transmit packets smoothly. This motivates us to develop our scheme presented in the next subsection.

3.2 A new scheduling mechanism in MAC layer

We present a framework which addresses the intra-flow contention and receiver blocking problems by solving the medium contention and congestion. Our proposed scheme incorporates the IEEE 802.11 DCF mechanism into AODV routing protocol. All the routing algorithms (e.g., route discovering and path maintaining) are same as original AODV protocol in network layer. Nevertheless, we try to transmit routing information about the total hop count and the remaining hop count over MAC layer, which is used to recalculate the contention window size for each node along the routing path. This new scheduling strategy achieves optimum packet scheduling in the MAC layer and results in good transmission efficiency in the network layer. Our proposed algorithm is described as Figure 4.

The contention window (CW) is an important variable to determine the back-off time of each node. When the first packet is transmitted, a node sets its contention window size equal to the minimum value (i.e., CWMin). If the transmitting packet suffers from collision or error, the node will resend this packet by adjusting CW = CWMin * 2^{n-1}, n is the number of packet retransmitted times. The contention window increases its value step by step until it reaches the maximum contention window (CWMax). The value of the contention window size is set as following order 32, 64, 128, 256, 512, and 1024 slots according to the IEEE 802.11 standard.



```
/* revise the maximum contention window of node in MAC */
CWMax = $1024/2^{y}$ slots, $y = Max(0,(L-D-5))$                    (1)

/* revise the minimum contention window of node in MAC */
CWMin = $1024/(2^{x} * 2^{(L-D)})$ slots, $x = Max(0,(5-L))$        (2)

        /* L: total hop count for routing path
           D: remaining hop count to destination */

/* to decrease the probability of collision, check the minimum
   contention window of each node not smaller than 32 slots */
if CWMin ≤ 32 slots then CWMin = 32 slots                           (3)

/* if the transmitting packet suffers from collision or error, resent
   packet by adjusting contention window size of node */
CW = CWMin * $2^{n-1}$ slots                                        (4)

        /* n: number of data retransmitted times */

/* contention window size of node increases step by step until it
   reaches the maximum contention window */
CWMin ≤ CW ≤ CWMax ;
   if CW > CWMax then CW= CWMax                                     (5)

/* if packet is sent successfully or reach the maximum retransmitted
   times, reset contention window size of the node */
If (transmit successfully or $n \geqq n_{max}$) then reset CW = CWMin (6)

      /* $n_{max}$: the value of maximum retransmitted times
         7 times for RTS/CTS, 4 times for basic access mechanism */

/* node generates a random back off interval before transmitting data */
Back-off time = floor(CW * random( )) * slot time                   (7)

      /* random( ): a random real number between 0 and 1
```

FIGURE 4

Algorithm for a new scheduling mechanism in MAC layer

Our proposed scheme includes two mechanisms. One is to assign a higher priority of channel access to the downstream node than that to the upstream node. This could achieve optimum packet scheduling for the medium access and avoids the severe intra-flow contention in each flow. The other is to constraint the outgoing data rate of the source node. It could efficiently prevent the greedy source from injecting more packets than that the network could handle. To prevent a source node from injecting too many packets is to assign the lowest priority of channel access (e.g., set

CWMin = 1024) to the source node intentionally and give higher priority of channel access to the succeeding nodes. We revised the minimum contention window of each node along the routing path as function (2) shown in Figure 4. If the total hop count of the routing path is greater than five, the minimum contention window size of the first six nodes decreases in backward order; and sets as 1024, 512, 256, 128, 64, and 32 slots. In order to decrease the probability of data collisions on the succeeding nodes of the routing path, other nodes still keep the minimum contention window size equal to 32 slots. If the total hop count of the routing path is smaller than five, the minimum contention window size of the last node (i.e., destination) is set equal to 32 slots. The minimum contention window size of other nodes increases progressively forward in order, and sets as 64, 128, 256, and 512 slots. On the other hand, if the transmitting packet suffers from collision or error, the contention window size of node increases its value step by step until it reaches the maximum contention window. We revised the maximum contention window of each node along the routing path as function (1) shown in Figure 4. If the total hop count of the routing path is greater than five, the maximum contention window size of the first six nodes are all set to 1024 slots. The maximum contention window of other nodes decreases in backward order, and sets as 512, 256, 128, 64, and 32 slots. If the total hop count of the routing path is smaller than five, the maximum contention window size of all nodes is set to 1024 slots.

In short, the source node tends to hold succeeding packets until the preceding packets are transmitted out of their interference range (i.e., four hops away) (Hirano, Jain, and Raychaudhuri, 2011). The intermediate nodes try to efficiently conduct the traffic flow and only allow the upstream nodes to forward enough packets to make it possible for the downstream nodes to fully utilize the shared channel, but never introduce severe MAC collisions and network congestions.

4. SIMULATION AND ANALYSIS

The simulation was implemented under the network simulator NS2 2.29, which can simulate a layered network protocol stack and wireless channel. For more information about this software, please refer to.

4.1 Simple scenario— 7-node chain topology

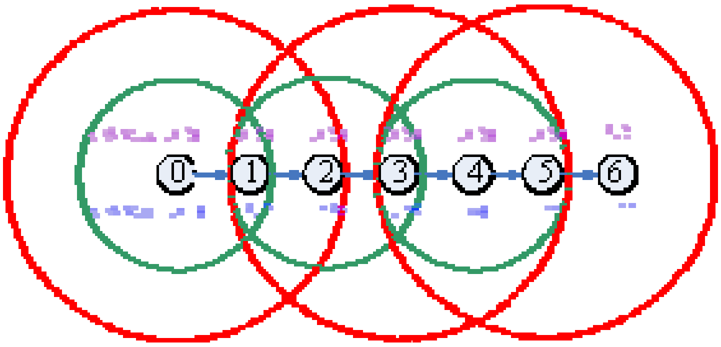


FIGURE 5

Illustration for setting the minimum and maximum contention windows among a 7-node chain

We first investigate how well our scheme works in the simple scenario. Our simulation scenario is conducted in a 7-node chain topology which is a general case of a static multi-hop ad hoc network, as shown in Figure 5. The distance between neighboring nodes is 200 meters, which allows a node to connect only to its neighboring nodes. The same distance between neighboring nodes ensures that all nodes act equally in the simulation. The simulation and analyses focus on a static multi-hop ad hoc network and do not address the routing failure problem which is caused by node mobility. IEEE 802.11 distributed coordination function (DCF) is used as the medium access control protocol. All nodes communicate with identical, half duplex, wireless radios that have a bandwidth of 1 Mbps, an effective transmission radius of 250 meters, and the interfering range of 500 meters. Each node has a queue called interface queue (IFQ) for packets waiting to be transmitted by the network interface, which holds up to 10 packets and is managed in a drop tail fashion. The two-ray ground reflection model is used for propagation. AODV routing protocol is adopted to find routing path in network layer.

In this simulation, we use constant bit rate (CBR) / UDP traffic to simplify the problems investigated in the MAC layer. Every CBR packet size is 1200 bytes, and the packet sending rate is varied in each run to change the offered traffic load (e.g., 0.01, 0.2, 0.3, and 0.5 Mbps) in the network. Every simulation takes time for 100 simulated seconds.

In subsections 4.1.1 to 4.1.4, we evaluate and compare the simulation results of our proposed scheme with the original AODV based on IEEE 802.11 DCF. In the following figures, Figure 6 to Figuer 10, our proposed scheme is considered relative to the conventional mechanisms of IEEE 802.11 standard both as basic access with priority and RTS/CTS with priority.

4.1.1 End to end throughput:

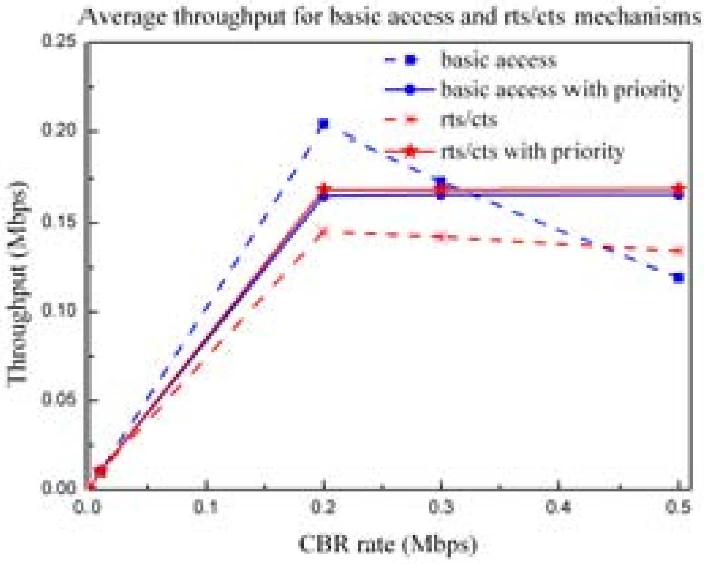


FIGURE 6

End to end throughput in the 7-node chain.

Figure 6 shows that the priority contention window scheme improves the end to end throughput of AODV for both basic access and RTS/CTS mechanisms under heavy traffic load (0.3~0.5Mbps CBR). The throughput of CBR packet with priority contention window scheme is much higher and more stable than that for RTS/CTS mechanism over all traffic loads. It means that the conventional basic access mechanism sends more CBR packets than our proposed scheme and many of them are lost.

4.1.2 Packet delivery ratio:

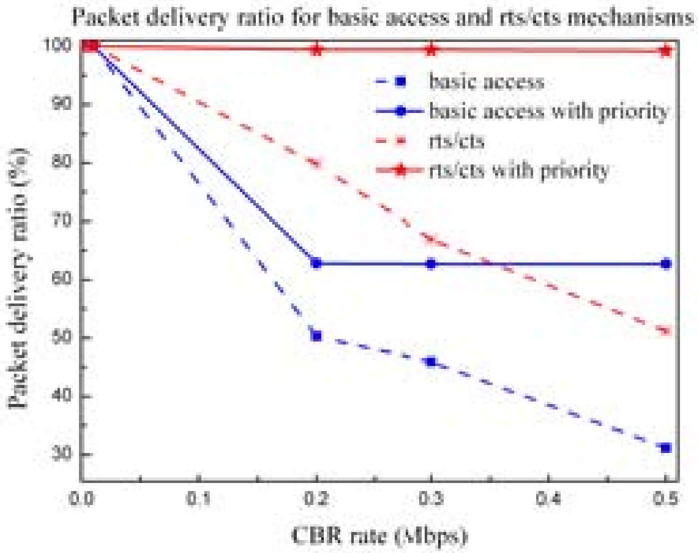


FIGURE 7

Packet delivery ratio in the 7-node chain.

Figure 7 shows that the priority contention window scheme has much higher packet delivery ratio than that of original AODV for both basic access and RTS/CTS mechanisms independent of traffic load. The packet delivery ratio of CBR data for our proposed scheme is much higher than that for the conventional basic access mechanism all the time. Moreover, it is almost reach one hundred percent without any collision of CBR packet during data transmission for RTS/CTS with priority contention window scheme. That is to say, both kinds of the priority contention window mechanisms suffer less collisions and losses than that of the conventional mechanisms of IEEE 802.11 all the time while transmit CBR packet.

4.1.3 Normalized control overhead

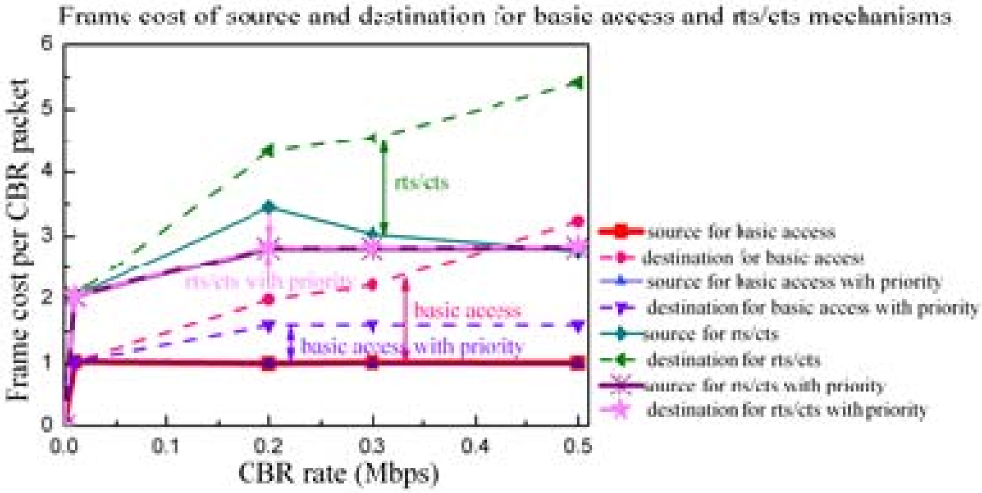


FIGURE 8

Normalized control overhead in the 7-node chain.

Figure 8 shows that the priority contention window scheme keeps normalized control overhead small and stable, and has much smaller difference of the frame cost between source and destination than that of the original AODV based on IEEE 802.11. This verifies that our proposed scheme avoids a lot of collisions in the MAC layer and reduces unsuccessful RTS/CTS negotiations and RREQ, RREP, RERR route control packets. The original AODV based on IEEE 802.11 has much higher normalized control overhead, which increases rapidly with the offered load for the multi-hop flow. This implies that the priority contention window scheme is a better choice than the conventional mechanism in a multi-hop ad hoc environment.

4.1.4 Probability of link failure

Figure 9(a), 9(b) shows that the number of route control packet, i.e. RREQ and RERR, for the priority contention window scheme is absolutely smaller than that of the original AODV based on IEEE 802.11. In Figure 9(a), the maximum number of RREQ sent by the source node is only 5 packets in both the priority contention window mechanisms, but 190 packets in original AODV based on RTS/CTS and 35 packets based on basic access mechanism. Relatively, Figure 9(b) shows the maximum number of RERR received by the source node is only 4 packets in our proposed schemes, but 163 packets in original AODV based on RTS/CTS and 16 packets based on basic access mechanism. In view of the above description, we declare that our proposed scheme is superior to original AODV.

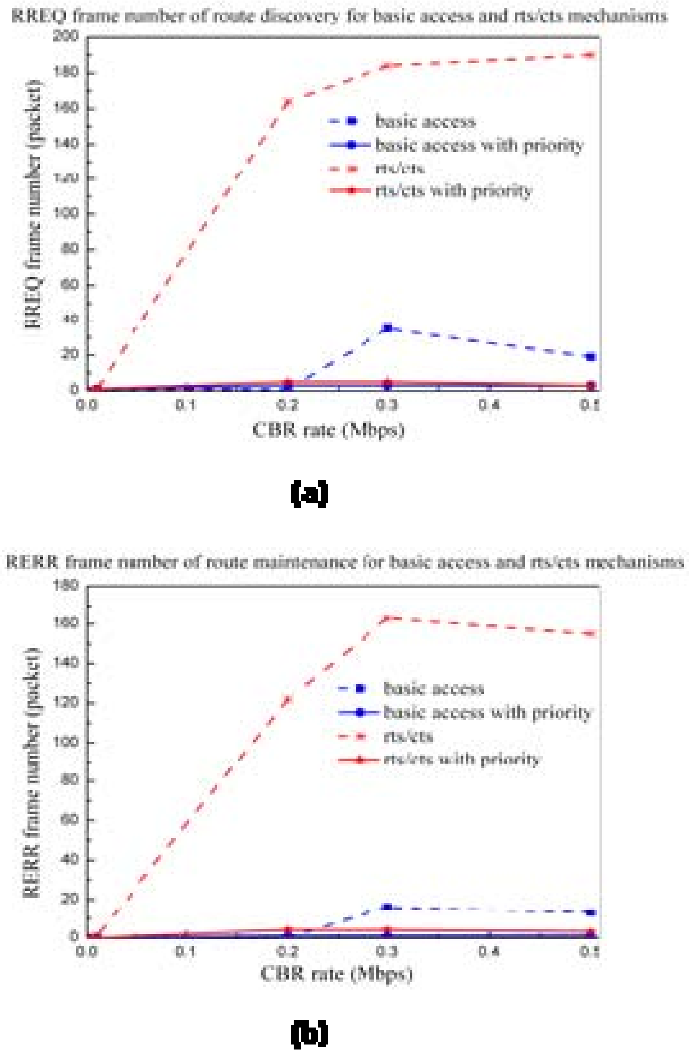


FIGURE 9

(a) Number of RREQ packet for route discovery in the 7-node chain.

(b) Number of RERR packet for route maintenance in the 7-node chain.

4.2 Enhanced scenario — random topology with mobility

In the simulation, 60 nodes are randomly located in a 1,500 * 1,500 m^2 area. All wireless channel and CBR/UDP parameters (e.g., bandwidth, effective and interfering range, CBR packet size, etc.) are same as the foregoing simulation. Nodes randomly move in the rectangular grid with a random speed (uniformly distributed between 0 – 5 m/s). The simulation begins with each node which moves toward its randomly chosen destination. Whenever a node arrives at the waypoint, it chooses another new waypoint and moves immediately toward it. Pause time is set to zero. The same process of node mobility is repeated until the end of simulation. There are 5 flows with the same CBR/UDP traffic load in the network. The source of each flow randomly selects one node as its destination and changes the offered traffic load (e.g., 0.05, 0.1 0.2, 0.3, 0.4, and 0.5 Mbps) in each run. Every simulation takes time for 300 simulated seconds.

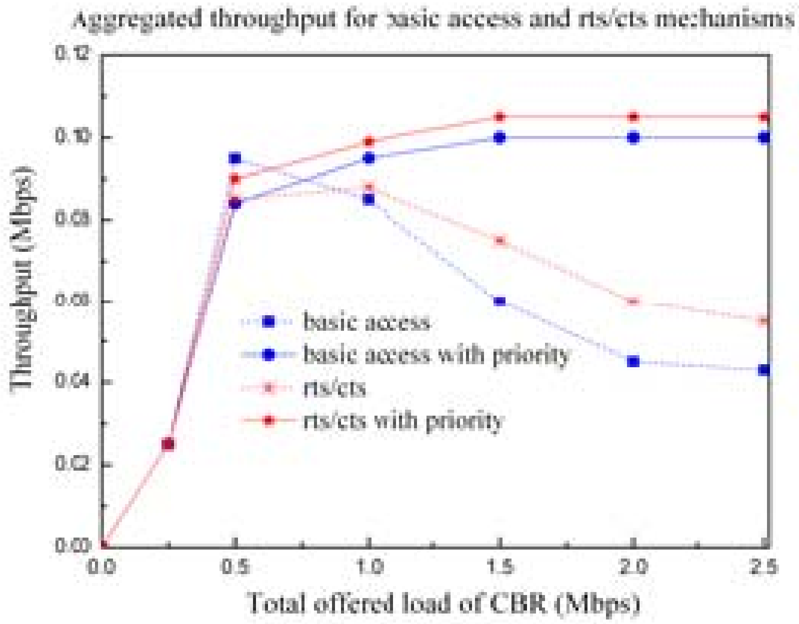


FIGURE 10

Aggregated end to end throughput in the 60-node random topology with mobility.

The purpose of considering the random topology with mobility is to illustrate that our proposed scheme works well in mobile scenario with the AODV protocol. We show only the aggregated end to end throughput for this scenario in Figure 10. It can be seen that the end to end throughput of our scheme is much better than original AODV based on 802.11. This is because our algorithm gives appropriate priorities to the packets that are closer to their destinations; efficiently conducts data flows; greatly reduces the resource wasted by those dropped packets at forwarding nodes, and thus more packets are able to reach their destinations successfully. Our proposed cross-layered approach increases the aggregated end to end throughput up to 30~50 percent in heavy load. We also notice that the node mobility significantly decreases the aggregated end to end throughput. This is because the route may be unavailable during data transmission due to routing failure caused by node mobility, even that each source node has a route to its destination at the start time.

5. CONCLUSION

In this paper, we state the problems about hidden terminal, receiver blocking, and intra-flow contention. They cause poor performances of the IEEE 802.11 DCF standard in a multi-hop ad hoc network. In order to alleviate these problems, we propose a framework of medium access scheduling algorithm based on the total hop count of routing path and the remaining hop count to the destination. The scheme assigns a higher probability of channel access to the downstream node than that of the upstream node, and limits the greedy source not injecting more packets than that of the succeeding nodes could handle; thus, greatly reduces excessive collisions and congestions at the MAC layer. Extensive simulations verify that comparing with the original AODV based on IEEE 802.11, our proposed scheme in most cases could achieve obviously better metrics of data transmission in the network layer, e.g., more stable and higher throughput, better packet delivery ratio, lower routing load, and smaller control packet number of RREQ and RERR which are relative to the probability of link failures. On the basis of the results, we could indicate a potential direction to improve the overall performances of a multi-hop ad hoc network.

References

Basavaraju, T. G., Sarkar, S. K., Puttamadappa, C. (2006). Impact of MAC Layer on the Performance of Routing Protocols in Mobile Ad hoc Networks. *International Journal of Information Technology, 3*(4), 237-244.

Bouhorma, M., Bentaouit, H., Boudhir, A. (2009). Performance Comparison of Ad-Hoc Routing Protocols AODV and DSR, Multimedia Computing and Systems, 2009. *ICMCS '09. International Conference*, 511-514

Hirano, Y., Jain, S., Raychaudhuri, D. (2011). Chain Effect of Route Recoveries and MAC Layer Collisions in Wireless Multi-hop Networks. *Wireless Communications and Networking Conference (WCNC)*, 452-457.

Hu, Y., Luo, T., Shen, J. (2010). An Improvement of the Route Discovery Process in AODV for Ad Hoc Network, Communications and Mobile Computing (CMC) . *2010 International Conference on Volume: 1,* 45-461.

IEEE 802.11 Working Group (1999). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. ANSI/IEEE Std. 802.11.

Johnson, D. B., Maltz, D. A. (1996). Dynamic Source Routing in Ad Hoc Wireless Networks, in Mobile Computing, T. Imielinski and H. Korth, Eds. Kluwer. *Academic Publishers,* 153-181.

Kanodia, V., Li, C., Sabharwal, A., Sadeghi, B., Knightly, E. (2001). *Distributed Multi-Hop Scheduling and Medium Access with Delay and Throughput Constraints,* in Proc. of ACM MobiCom 2001.

Lee, S. B., Campbell, A. T. (2003). *HMP: Hotspot Mitigation Protocol for Mobile Ad Hoc Networks*. in 11th IEEE/IFIP International Workshop on Quality of Service (IWQOS 2003).

Lee, S. J., Gerla, M. (2001). *Dynamic Load Aware Routing in Ad Hoc Networks*. in Proc of IEEE ICC 2001.

Li, B., Liu, Y., Chu, G. (2010). Improved AODV Routing Protocol for Vehicular Ad Hoc Networks, Advanced Computer Theory and Engineering (ICACTE) . *2010 3rd International Conference on Volume: 4*, 337-340.

Li, C., Knightly, E. (2002). Coordinated Multi-hop Scheduling: A Framework for End-to-End Services. *IEEE/ACM Transactions on Networking*, 776-789.

Li, J., Blake, C., Couto, D., Lee, H., Morris, R. (2001). *Capacity of Ad Hoc Wireless Network*, in Proceedings of ACM MobiCom.

Li, X., Cuthbert, L. (2004). Stable Node-Disjoint Multipath Routing with Low Overhead in Mobile Ad Hoc Networks. *Modeling, Analysis, and Simulation of Computer and Telecommunications Systems, (MASCOTS 2004)*, 184-191.

Liu, X., Tarek, S. (2010). Throughput Analysis of IEEE 802.11 Multihop Ad Hoc Wireless Networks underSaturation Condition. Computers and Communications (ISCC), *2010 IEEE Symposium*, 245-248.

Megha, M., Bechir, H. (2011). An Improved IEEE 802.11 MAC Protocol for Wireless Ad-Hoc Networks with Multi-Channel Access Capabilities. High Performance Computing and Simulation (HPCS), *2011 International Conference*, 162-168.

Park, V. D., Corson, M. S. (1997). A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks. *INFOCOM'97*, 1405-1413.

Pearlman, M. R., Haas, Z. J. (1999). Determining the Optimal Configuration for the Zone Routing Protocol. *IEEE JSAC*, 1395-1414.

Perkins, C. E., Bhagwat, P. (1994). Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers. *Proceedings of the SIGCOMM '94*, 234-244.

Perkins, C. E., Royer, E. M. (1999). Ad-Hoc On-Demand Distance Vector Routing. *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 90-100.

Sethi, S., Udgata, S. K. (2009). *IMAODV: A Reliable and Multicast AODV Protocol for MANET.* Wireless Communication and Sensor Networks (WCSN).

Tahiliani, M. P., Shet, K. C., Basavaraju, T. G. (2010). Performance Evaluation of TCP Variants over Routing Protocols in Multi-hop Wireless Networks. *Computer and Communication Technology (ICCCT)*, 387-392.

Walia, M., Challa, R. K. (2010). Performance Analysis of Cross-Layer MAC and Routing Protocols in MANETs. *Computer and Network Technology (ICCNT)*, 53-59.

Xiao, Y., Yin, X. (2010). Performance Modeling and Analysis of IEEE 802.11 MAC Protocol in Multihop Ad Hoc Networks. *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference*, 1-5.

Xu, S., Safadawi, T. (2001). Does the IEEE 802.11 MAC Protocol Work Well in Multi-hop Wireless Ad Hoc Networks? IEEE Comm. *Magazine, 39*, 130-137.

Ye, Z., Berger, D., Sinha, P., Krishnamurthy, S., Faloutsos, M., Tripathi, S. K. (2003). *Alleviating MAC Layer Self-Contention in Ad-Hoc Networks*. in Proc. Of ACM MOBICOM 2003 Poster.

Zhai, Z., Zhang, Y., Song, M., Chen, G. (2010). A Reliable and Adaptive AODV Protocol Based on Cognitive Routing for Ad Hoc Networks. *Advanced Communication Technology (ICACT), The 12th International Conference on Volume: 2* , 1307-1310.

Zhang, X. M., Zhu, W. B., Li, N. N., Sung, D. K. (2010). TCP Congestion Window Adaptation Through Contention Detection in Ad Hoc Networks. *Vehicular Technology, IEEE Transactions on Volume: 59*(9), 4578-4588.

Zheng, S. (2011). Performance Study of Cooperative Routing Metric for Multi-Hop Wireless Networks. *Vehicular Technology Conference (VTC Spring) IEEE 73rd*, 1-5.