Comparative Study between Exponential Back off and Dynamic Waiting Strategies for Medium Access in Wireless Ad Hoc Networks

by

Rahul Shah
200711016

A thesis submitted in the partial fulfillment of the requirements for the degree of
Master of Technology
in
Information and Communication Technology

Dhirubhai Ambani Institute of
Information and Communication Technology, Gandhinagar

May 2009

Declaration

This is to certify that

i) The thesis comprises my original work towards the degree of Master of Technology in Information and Communication Technology at DA-IICT and has not been submitted elsewhere for a degree.

ii) Due acknowledgment has been made in the text to all other material used.

Rahul Shah

Certificate

This is to certify that the thesis work entitled *"Comparative Study between Exponential Backoff and Dynamic Waiting Strategies for Medium Access in Wireless Ad Hoc Networks"* has been carried out by *Rahul Shah* (200711016) for the degree of Master of Technology in Information and Communication Technology at this Institute under my supervision.

Dr. Sanjay Srivastava

Contents

List of Figures

Abstract

IEEE 802.11 DCF (IEEE 802.11 Distributed Coordination Function) is widely used MAC protocol for wireless channel access. Although it is developed for single hop networks where all nodes are in the same radio range, it can be directly used for wireless multihop ad hoc networks. But performance of IEEE 802.11 DCF in wireless ad hoc networks suffers as it has been developed considering single hop networks only. Many amendments has been proposed to enhance its performance in multihop ad hoc networks. One such scheme is DWMAC (Dynamic Waiting Medium Access Control). In this work, performance of IEEE 802.11 DCF and DWMAC are compared for different network scenarios and traffic patterns. It has been observed that the performance of DWMAC can be further improved if we alter the restricted mode operation of the nodes. We have proposed a new modified protocol DWMAC-Modified and have shown by simulations that DWMAC-Modified offers significant improvements.

Acknowledgments

I am deeply indebted to my thesis supervisor Prof. Sanjay Srivastava for his constant guidance, creative criticism and incessant motivation given to me throughout the year. His advice and suggestions always encouraged me to work.

I am very much thankful to Prof. V. Sunitha for her suggestions and encouraging presence in MAGNeT meetings.

I would like to thank all my friends and MAGNeT members, Sunil, Manish, Brijesh, Pankesh, Kavan, Harshil, Mahesh for their delightful company and helpful nature. The time we spent in LAB is unforgettable.

No words are enough to show gratitude to all my family members for their love, warmth and support without which it would not have been possible to complete this work.

Finally, I would like to thank all who directly or indirectly involved in this work.

Chapter 1

Introduction

An ad hoc network is a dynamically formed spontaneous network that consists solely of mobile stations without base stations. Battlefield, disaster areas where centralized infrastructure is not possible, ad hoc networks are very useful. Ad hoc networks are also useful when network is not needed for a long time for example in business meetings, conferences etc. As wireless devices (like laptops, palmtops, cellphones) get cheaper and the amount of mobility and flexibility they provide, wireless ad hoc networks seem to be emerging communication method in networking.

One challenge in wireless ad hoc networks is to handle with the collision resulting from two or more nodes transmitting packets at the same time over the same transmission medium or channel. This problem is also called channel allocation or multiple access problem. MAC (Medium Access Control) protocols have been developed to assist each node to decide when and how to access the channel keeping in mind channel utilization and fairness. Classification of MAC protocols can be done by many ways depending on number of channels they use (single-channel and multi-channel), type of hardware they need (directional antennas,GSM etc), type of access algorithm (distributed or centralized), contention based or contention free access mechanism, sender initiated or receiver initiated transmission etc.

In wireless ad hoc networks, there is no infrastructure so no centralized control, number of nodes in network is not fix making scheduling the nodes difficult, all nodes are not in same radio range making synchronization between nodes difficult. Considering these characteristics of wireless multihop ad hoc networks, asynchronous, distributed, contention based protocol is well suited for such network. 802.11 DCF by IEEE is one such protocol which originally developed for wireless LAN only. But as it distributed and asynchronous, it can be used in wireless multihop ad hoc networks.

1.1 Thesis Outline

Rest of the thesis is organized in following chapters.

Chapter 2 describes IEEE 802.11 DCF protocol.

Chapter 3 discusses problems with IEEE 802.11 DCF when used in multihop ad hoc networks.

Chapter 4 is literature survey consists mainly of performance analysis of IEEE 802.11 in single hop and multihop networks and proposed amendments to it.

Chapter 5 describes DWMAC protocol, issues with it and proposed modification to it.

Chapter 6 shows the results of all the simulations we performed for different network scenarios and traffic patterns for IEEE 802.11 DCF and DWMAC protocols.

Chapter 7 summarizes thesis by conclusion and future work.

Chapter 2

IEEE 802.11 DCF Description

This chapter describes the working mechanism of IEEE 802.11 DCF. Complete specification of it is given in IEEE 802.11 standard specification. [1].

IEEE 802.11 DCF is an asynchronous random access scheme based on the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) protocol. CSMA protocol is used to control the access of broadcast medium between number of stations. Here, if any node has a packet to send it first senses the channel and if channel is free then it can transmit otherwise it has to wait for medium being free. In wireless medium it is possible that transmitter senses the channel free but still collision is possible at the receiver when all the nodes are not in the same radio range and some activity is going on receiver side. To avoid such collisions, transmitter and receiver exchange short frames conforming channel is free at both side before data transmission. This is called collision avoidance phase. Following is the detailed description of IEEE 802.11 DCF scheme.

A station with a new packet to transmit monitors the channel activity. If the channel is idle for DIFS (Distributed Inter Frame Spacing)time, the station transmits. Otherwise, if the channel is busy (either immediately or during the DIFS), it persists to monitor the channel until it is idle for DIFS time. After this, station chooses random back-off to minimize the probability of collision between ready stations. This random back-off value is chosen from 0 to W where W is contention window size. This value is decremented after every fix time interval called slot. If channel becomes busy during back-off decrement, the station freezes its back-off counter and reactivates it when channel becomes free. When back-off counter reaches zero, station transmits. After the successful reception of data, receiving station sends ACK frame to the sender after SIFS (Short Inter Frame Spacing) time interval. After successful transmission, if station has next packet ready in transmission queue, it performs another DIFS deference and random back-off even medium

is free for DIFS time interval to avoid capture of the channel by only one node. Following figure describes the access mechanism for IEEE 802.11 DCF for a node.

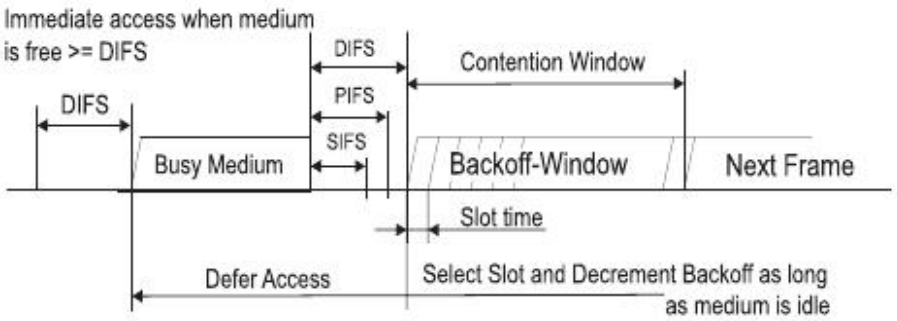


Figure 2.1: Channel Access for a Node

[From [1], page-77.]

To handle the collisions between the stations 802.11 DCF adopts an exponential back off scheme. After every collision (collision is identified when sender does not get ACK frame) the value of W is doubled up to the maximum value $CW_{max} = 2^m \times CW_{min}$. After the successful transmission station resets the W to CW_{min}. Following figure illustrates more clearly channel access between 5 nodes.

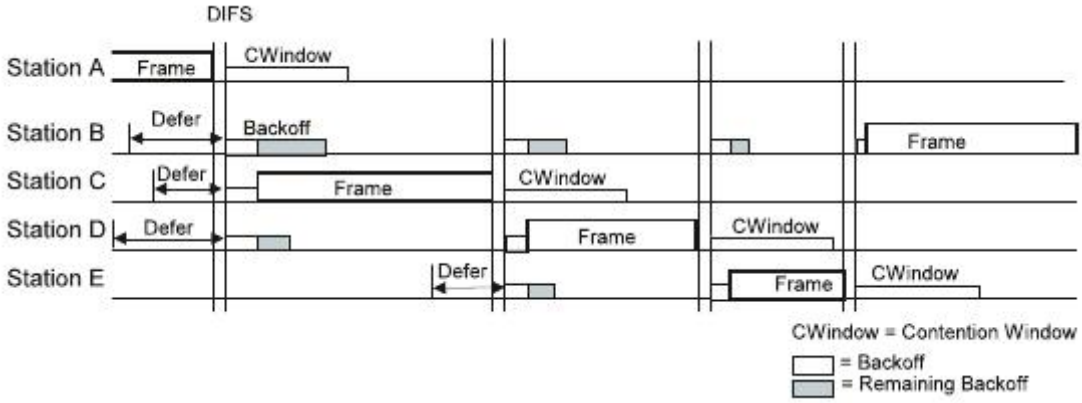


Figure 2.2: 5 Nodes Accessing the Channel

[From [1], page-78.]

Above procedure is called basic access mechanism in which DATA-ACK frames are sent. 802.11 DCF also provides four way handshaking which includes RTS-CTS-DATA-ACK frames. Four way

handshaking is shown in following figure.

Here, a station that wants to transmit a packet waits for DIFS time, follows back-off rules and

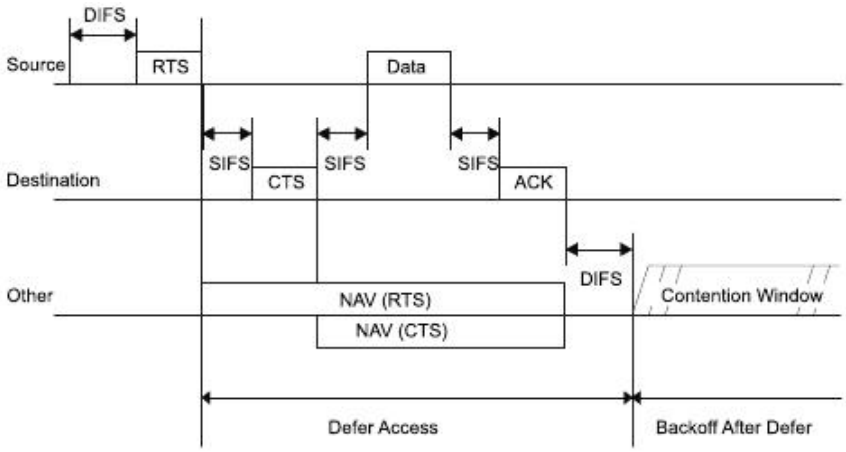


Figure 2.3: Channel Access with RTS-CTS
[From [1], page-79.]

then, sends a short control frame called RTS (Request To Send). When receiving station gets RTS frame destined to itself, responds with CTS (Clear To Send) frame. If both these frames are received correctly then actual DATA-ACK frames are sent. RTS-CTS frames carry the information of the length of the packets to be transmitted, so all the stations hearing these frames come to know how long they should wait to avoid the collision. Each node maintains a variable called NAV (Network Allocation Vector) and sets it according to time interval specified in RTS and CTS frame. Value of NAV is decremented at every slot. This is very useful mechanism to avoid collision when all nodes are not in the same radio range. Even when all nodes are in the same radio range use of short RTS-CTS control frames before actual data transmission saves the time wasted in collision increasing throughput.

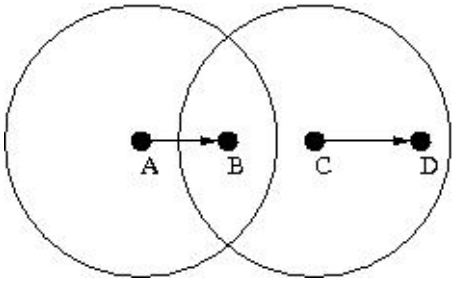
Chapter 3

Problems with 802.11 in Ad Hoc Multihop Networks

802.11, which is developed for wireless LAN only, faces some problems when used in ad hoc networks. This chapter describes some major problems.

- **Ineffectiveness of Physical Carrier Sensing and Need for RTS/CTS**
  In single hop networks all nodes are within the range of each other. So ongoing transmission between any two nodes can be physically sensed by any node which prevents node to start transmission when one transmission is going on. Collision between two stations is possible only when two stations choose the same back off value and start transmission in the same slot.

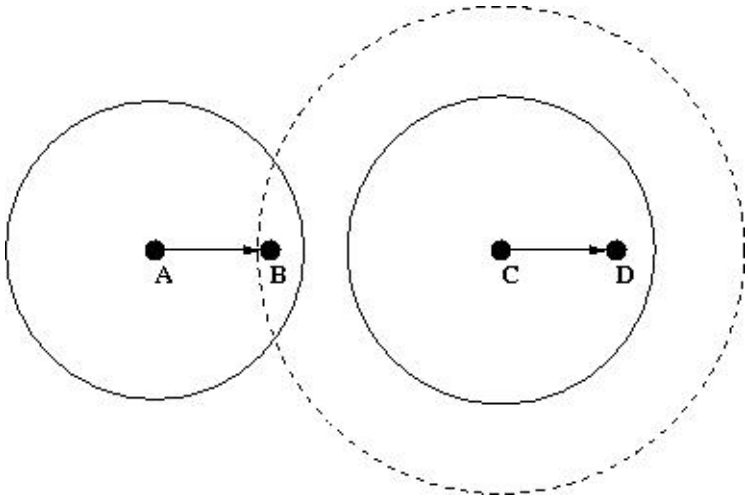
  In ad hoc networks all nodes are not in same radio range. So a station, which is outside the range of the sender of ongoing transmission, may start the transmission resulting in collision with ongoing transmission. Entire transmission period is vulnerable to collision in ad hoc networks. This type of collision degrades the performance of 802.11 in multi hop environment. RTS/CTS frames help to avoid this type of collision at some extent. As shown



in figure, when node A is transmitting data to node B, C can transmit data to D which causes collision at B.

- **Interference Range is Larger than Transmission Range**

  A station may not able to decode the radio signal of transmission as it is outside the transmission range of the sender but still it may be interfered by that signal if it is receiving some data. In other words interference range is larger than transmission range. For this reason, a station may not able to receive RTS and CTS frames of the ongoing transmission and may start transmission which interfere with ongoing transmission. This problem can not be solved until RTS and CTS frames are send with more power than data frames. As shown in figure,



  node C is outside the transmission range of node B, so it can not receive CTS frame and so unaware of transmission from A to B. Also C is outside the carries sensing range of A. So C starts to transmit to D and its signals interfere with A to B transmission causing collision at B.

- **Exposed Terminal Problem**

  RTS-CTS-DATA-ACK sequence of frames in 802.11 needs all the nodes listening not only CTS frames but also RTS frames to remain silent during the whole transmission period. This unnecessarily prevents some nodes (called exposed terminals) to transmit degrading total network throughput. As shown in the figure, while B is transmitting to A, C can

  transmit to D, if it is outside the interfering range of A. But in 802.11 protocol this is not

possible because all the nodes listening RTS frames are prevented to transmit. Here, C is called exposed terminal for A.

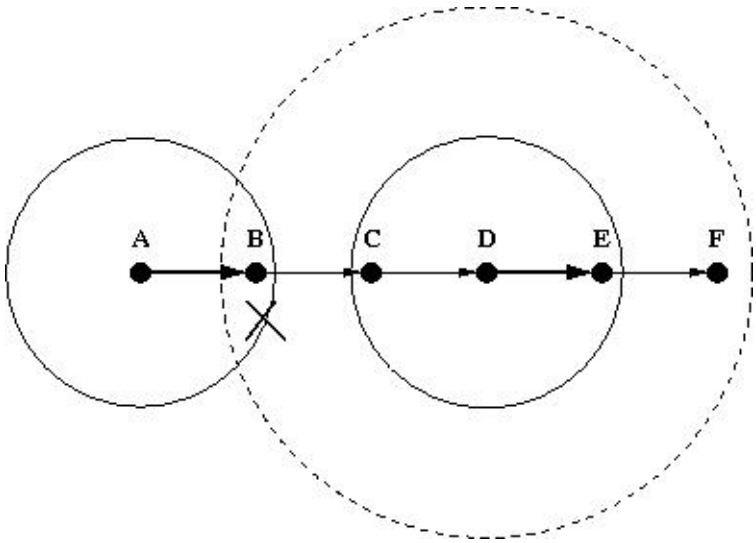
- **Fairness**

  In multi hop networks due to lack of synchronization and inability to sense the transmission physically, some nodes always collide with other transmissions and keep doubling their contention window. Such nodes suffer severe unfair channel allocation. For example, as shown

  in figure, let flow F2 starts before flow F1. When node A sends RTS to B, B can not reply with CTS as it falls in carrier sensing range of node C. So node A continues doubling its contention window. Only time A can successfully transmit is when its backoff counter reaches zero at the same time when C had finished its transmission and not started next transmission. Chance of this to happen is rare.

- **Intra-flow Contention**

  In multi hop networks a node may be working as a forwarding node. Here all the nodes of the same flow unnecessarily contend for the channel without co-operation. This is called intra-flow contention which causes throughput of the flow to degrade. If nodes of the same flows give chance to downstream relay nodes to transmit throughput can be increased. As

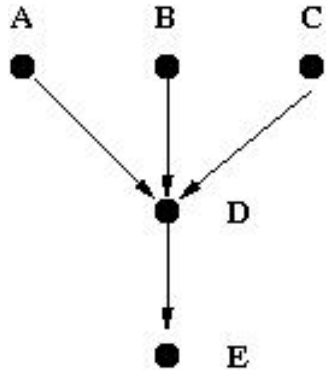


  shown in figure, due to intraflow contention,

- If node A starts transmission when D is transmitting causes collision at B
- Such collision may result in very large contention window at A forcing A to remain silent even channel is free when D finishes its transmission.
- If node is saturated it may pump more data than downstream relay nodes can forward resulting in packet drop at downstream relay nodes.

- **Inter-flow Congestion**

  Due to critical position of some nodes, many nodes can use them as forwarding nodes for their end-to-end flows. These nodes experience higher congestion level than others nodes but at MAC layer 802.11 protocol does not give them more chances of channel access than other. If these nodes are given higher priority than end-to-end throughput can be increased. As shown in figure, node D does forwarding job for 3 flows so it should get 3 times higher



  channel access than node A,B,C. 802.11 can not provide this priority to node D.

Chapter 4

Literature Survey

IEEE 802.11 DCF protocol is extensively studied by many researchers for throughput and fairness measures by simulation or mathematical modeling. In this chapter, some of the important studies are discussed. Also some proposed protocols which can be easily developed by changing 802.11 DCF are described.

4.1 802.11 DCF in Single Hop Networks

In [3], Bianchi has derived accurate analytical model to compute the 802.11 DCF throughput, in the assumption of finite number of terminals and ideal channel condition. According to the paper, as the number of stations increases, throughput decreases in saturated traffic condition but maximum throughput is always achievable if minimum contention window size is adjusted according to number of stations. But unfortunately minimum contention window size is fix in IEEE 802.11 standard. Also RTS/CTS access mechanism is shown less dependent on system parameters and that it performs better than basic access mechanism in most of the scenarios.

4.2 802.11 DCF in Multihop Ad Hoc Networks

In [5], authors have used Markov Chain Analysis method, originally devised by Tobagi and Kleinrock in [4], for throughput analysis of 802.11 DCF in general multihop ad hoc networks. In [8], authors have made correction to bianchi's model of 802.11 DCF to model freezing of back-off counter in 802.11, added extra state for analysis of unsaturated traffic condition and extended it in three dimensional Markov chain to analyze 802.11 performance in multihop networks. In [6], authors have extended bianchi's model for throughput analysis of 802.11 in multihop networks

considering collision probability by hidden nodes.

In [9], Li et.al. have examined interaction of the 802.11 MAC and ad hoc forwarding and the effect this on capacity of ad hoc networks for several simple configurations and traffic patterns. While 802.11 discovers reasonably good schedules, they nonetheless observed capacities markedly less than optimal for very simple chain and lattice networks with very simple traffic patterns. They have shown in chain topology, throughput is 1/7 of the channel capacity which actually should be 1/4 of the channel capacity. The reason is, in chain topology middle nodes experience more interference than starting nodes, so starting nodes inject more packets than forwarding nodes can forward. Packets are eventually dropped at middle and channel capacity which has been used to forward these packets is wasted decreasing the resultant throughput. The second reason is due to collision happening because of interference range is larger than transmission range, some nodes keep doubling their contention window size resulting dramatically increased window size and remain silent even when channel is idle. Authors have also shown one hop capacity of the ad hoc network scales with network size.

In [10], Xu and Saadawi have studied interaction of the 802.11 MAC and TCP with simulation. They have shown that larger carrier sensing range and interfering range prevents nodes to reply CTS causing route failure advertisement by MAC layer which is actually due to congestion. So route discovery is started and until new route is found TCP throughput degrades to zero. Also they have shown 802.11 back-off always favors successfully transmitted nodes causes some TCP connection to completely shut up.

In [7], Ng and Liew have also noted that as we increase the load in multihop chain throughput increases but after some point throughput starts to decrease instead of remaining constant at channel capacity. Reason is as middle nodes experiencing more interference they can not forward data at same speed as pumped in by source and starts to drop packets. The channel capacity which has been used to forward the packets till the dropping point is actually wasted. Authors have suggested controlling offered load at sources increase throughput and analytically derived optimal load at which throughput becomes maximum.

4.3 802.11 DCF and Fairness Issues

In [11], Bharghvan has pioneered fairness analysis for MACA protocol in multihop environments and first found out some specific scenarios in which such protocols show severe unfair behavior causing some flows to completely shut down.

4.4 Proposed Amendments in 802.11 DCF

In [16], authors have argued that 802.11 DCF exponential backoff fails to estimate traffic intensity and node density resulting large number of collisions in heavy traffic and have proposed traffic adaptive back off mechanism to reduce the collisions by estimating surrounding traffic by help of NAV(Network Allocation Vector). In [17], authors have investigated effect of false blocking (unnecessary blocking of nodes in ad hoc networks by RTS frame when CTS is not replied by receiver) and heavy offered load at source nodes on throughput of ad hoc networks and have proposed layer-2 pacing scheme on top of 802.11 DCF for MAC coordination between nodes of persistent flows. The main idea is to minimize contention between saturated nodes by transmission rate control by the sender. In [12], authors have proposed OPET protocol for multihop ad hoc networks which gives higher priority to current receiver for transmission reducing intraflow contention, does hop by hop backward pressure scheduling reducing interflow congestion, keeps some space in interface queue for other flows and does round robin scheduling for increasing fairness between flows. In [15], authors have proposed DWMAC protocol by changing 802.11 DCF in which every node waits for each active neighbor after its successful transmission reducing interflow and intraflow contention. In [13], authors have proposed VWMAC for multihop networks in which every node estimates how long it should wait after successful packet transmission so that its previously transmitted packet has been forwarded outside its interfering range. In [14], authors have proposed quick exchange for data transmission between sender and receiver and fast forward to give priority to downstream relay nodes to reduce intraflow contention.

In [18], authors have proposed distributed algorithm to calculate waiting time from collecting information about the active sub-flows in neighborhood of the node to eliminate unfair behavior of the 802.11 DCF between different flows. In [11], Bharghavan has proposed MACAW protocol with some more control frames and exchanging contention window size with neighbors to eliminate unfair behavior of MACA. In [19], authors have found out three main causes of unfair behavior of 802.11 and proposed method (EHATDMA) to solve each one of the causes and performed simulation for number of different scenarios for different protocols and analyzed their behavior in terms of fairness. In [20], authors have proposed MadMac protocol on top of 802.11 DCF in which node waits extra amount of time to give chance to active neighbors by listening to channel activity and collision.

Chapter 5

DWMAC and its Modification

In [15], authors have suggested a novel DWMAC (Dynamic Waiting MAC) protocol to solve MAC layer contention between neighboring nodes in wireless ad hoc networks. In this protocol, every node after a successful transmission waits for some pre-calculated time and gives chance of transmission to its neighbors. Following is the description of the protocol.

5.1 Description of DWMAC

This protocol is built on IEEE 802.11 protocol. Here, each node can work in one of the two states. Normal state and Restricted state. Figure 5.1 shows state diagram for a node in DWMAC protocol where T denotes transmission by the node, R denotes node is in restricted state and B is contention or normal state. In normal state, a node can transmit, receive or keep idle exactly as in 802.11. But in restricted state, node looses the right of transmission though it can receive data from other nodes. Dynamic Waiting Duration (DWD), the time for which a node remains in restricted mode is a key parameter for the protocol performance because by putting itself in restricted state for DWD time and giving chance to others, every node effectively tries to keep contention level very low although the number of contending nodes is large. How DWD is calculated is described later. In DWMAC, when a node has packet to send it checks its state. If it is in the restricted state then it has to wait until DWD finishes and it comes into normal state. In normal state, node's behavior is exactly same as in 802.11 protocol. In normal state, when a node has packet to send, it senses the channel and transmits directly if channel is free for DIFS time and waits if physical carrier sensing or virtual carrier sensing indicates channel is busy. When channel becomes

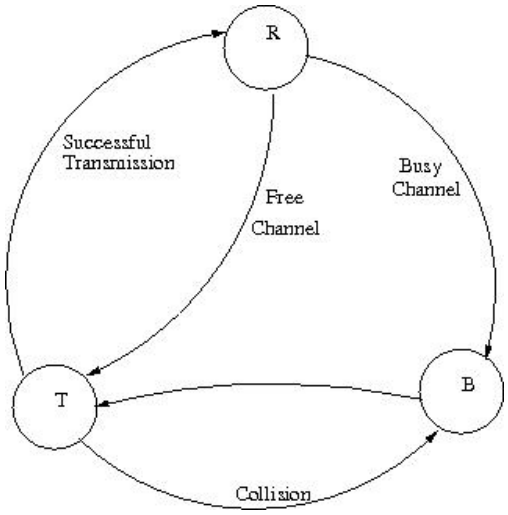


Figure 5.1: State Diagram for a Node in DWMAC

free it chooses the random back-off from 0 to CW. Where CW is the size of Contention Window. In, DWMAC the size of contention window is fix as opposed to 802.11, in which size of contention window is doubled after every collision and becomes minimum after successful transmission. In DWMAC as each node waits for its neighbors to transmit contention level is supposed to be low and node should not increase its contention window exponentially to cope with contention level. Following is figure for channel access of node in DWMAC.

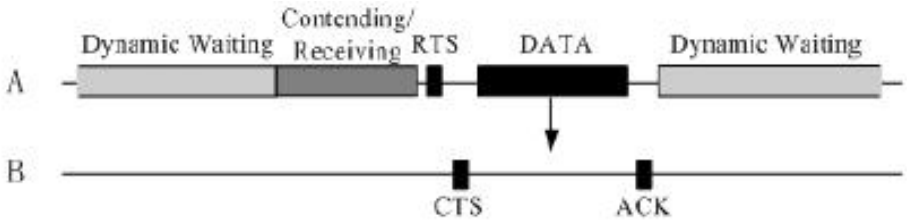


Figure 5.2: Channel Access in DWMAC
[From [15].]

5.1.1 Calculation of DWD

As described before, the length of DWD is key factor to reduce the contention between neighboring nodes. It should be equal to the time in which active neighbors can transmit their data so each

neighbor can transmit data between two successful transmission of a node. If it is larger than needed, nodes wait even channel is free and if it is smaller than needed, possibility of collision increases.

Here, each node maintains a new data structure called CNL_i which records node i's knowledge about potential transmission in the vicinity after its previous successful transmission. CNL_i contains the following information:
$\{U_{address}, T^{(u)}_{duration}\}$
Here, $U_{address}$ is the address of the node u and $T^{(u)}_{duration}$ is the duration that the node u claims to occupy the channel. This information is gathered from the RTS frame. CNL_i is updated only in restricted mode. After the restricted mode, node gets total duration by adding up the duration fields of all the entries in CNL_i.

$$T^{(i)}_{CNL} = \sum_{u \in CNL_i} T^{(i)}_{duration} \tag{5.1}$$

Through 5.1, we have got the sum duration of the transmission in the transmission range of node i. Next we need to estimate the total duration of all the transmissions in the interference range of the node i. If R_i is the interference range and R_t is the transmission range and $\beta = R_i/R_t$ then let the total time a node should wait for all the nodes whose transmission may interfere with the node is:

$$T^{(i)}_{total} = T^{(i)}_{CNL} * \beta^2 \tag{5.2}$$

In ad hoc networks many flow can pass through one node. In this situation a node which forwards data of many flow should wait shorter than others. For this each node maintains a variable N_{RTS} which is incremented every time when RTS packet is destined to itself until DWD finishes. Final DWD can be calculated as follows:

$$T^{(i)}_{DWD} = cp * T^{(i)}_{total}/N_{RTS} \tag{5.3}$$

Here, cp is the correction parameter which is included because we have not considered CTS frame.

5.2 Some Issues with DWMAC

There are some points in DWMAC which is not specified in paper properly.

1. What will be the value of DWD when node transmit very first time is not specified in[15]. If it is zero than node will not go in restricted state at all and will not able to update CNL_i.

2. According to paper[15], CNL_i is updated only in restricted state. This may create problems. Because if node has estimated active neighbors is let x than it will wait accordingly so all x neighbors can transmit. Let some more neighbors become active. Clearly in this waiting duration it can hear only maximum x transmission so it can never accommodate more neighbors than x. It is serious problem because eventually it increases the contention level in the system which is not desirable.

5.3 Modification in DWMAC

To solve this we suggest that CNL_i should be updated in both restricted mode and when node is backing off. So effectively counting will be done between two successive successful transmission of a node. In this way a node will always be able to truly estimate all its active neighbors.

From 5.2 and 5.3,

$$T_{DWD}^{(i)} = T_{CNL}^{(i)} * \beta^2 * cp/N_{RTS} \tag{5.4}$$

Term $\beta^2 * cp$ can be replaced by CP making equation 5.4 to

$$T_{DWD}^{(i)} = T_{CNL}^{(i)} * CP/N_{RTS} \tag{5.5}$$

Simulations are performed with different values of CP for multihop scenarios. CP is correction parameter and it should be varied to for calculating optimal waiting time.

Chapter 6

Performance Comparison

To evaluate the performance of DWMAC protocol and compare it with 802.11 protocol we have conducted number of simulations in NS-2.32 [2] simulator for different scenarios and different traffic patterns. As we are interested only in MAC protocol performance, in all simulations ad hoc routing algorithm is disabled. Instead each node gets predefined path from source to destination and uses it throughout the simulation. Single hop simulations are performed for 802.11, DWMAC (in which active neighbors are counted only in restricted state) and DWMAC-Modified (in which active neighbors are counted both in restricted and normal state). Multihop simulations are performed only for 802.11 and DWMAC-Modified as DWMAC-Modified proves itself better than DWMAC.

6.1 Performance Comparison in Single Hop Network

Simulation is performed for different number of nodes all are in same radio range. Nodes are randomly placed in the area of $200 \times 200m^2$. All the nodes are static. Transmission range is 250 meter and carrier sensing range is 550 meter. TwoRayGround propagation model is used. No noise model is used. Channel bandwidth is set to 1 Mbps. CBR (Constant Bit Rate) traffic model is used. Packet size is 512 bytes which is same for all the nodes. Each point in graph is an average of 5 runs with different seeds and each run is 101 seconds long. Every node starts CBR flow at 1 seconds which lasts till 101 seconds. Every CBR flow has distinct source and destination nodes means each node in simulation is either source or destination of one and only one CBR flow. CBR source node has always packet ready to send so all the source nodes are always contending for the channel. For 802.11 minimum contention window is varied from 4 to 1024 whereas for DWMAC minimum contention window is varied from 4 to 128. Following figures show the simulation results for 802.11, DWMAC and DWMAC-Modified in single hop networks. 6.1 shows the graph for throughput vs.

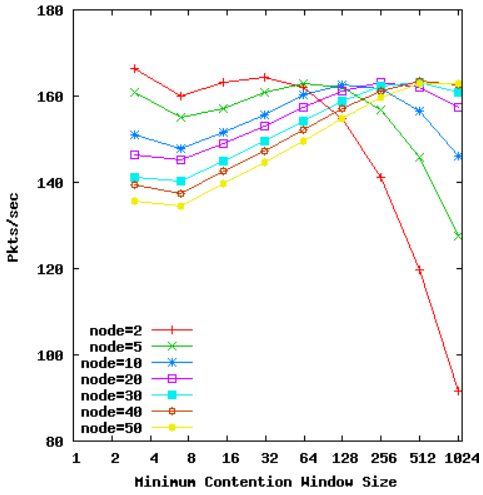


Figure 6.1: 802.11

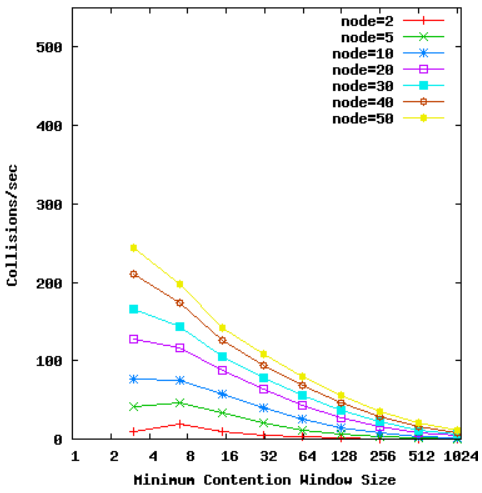


Figure 6.2: 802.11

minimum contention window size. We can see that as we increase the minimum contention window size throughput increases and after some points throughput starts to decrease with increase in minimum contention window size. For small number of nodes if minimum contention window size is large than probability of channel being idle is high and so throughput decrease whereas for large number of nodes if minimum contention window size is small then probability of collision becomes high causing throughput to decrease. This behavior of 802.11 can be seen from the 6.1. Also we can see that optimal throughput for 802.11 depends on minimum contention window size and number of active nodes in the network. We have to vary minimum contention window according to the number of active nodes in the network to get the optimal performance with 802.11. Although IEEE has kept minimum contention window size fix for 802.11 DCF protocol. So we can say that 802.11 performance varies largely with different number of active nodes in the network. Figure 3 shows graph for collisions/sec vs. minimum contention window size. We can see that number of collisions decrease with the minimum contention window size.

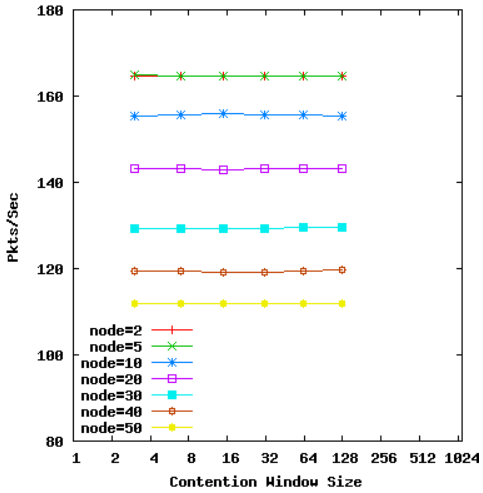


Figure 6.3: DWMAC

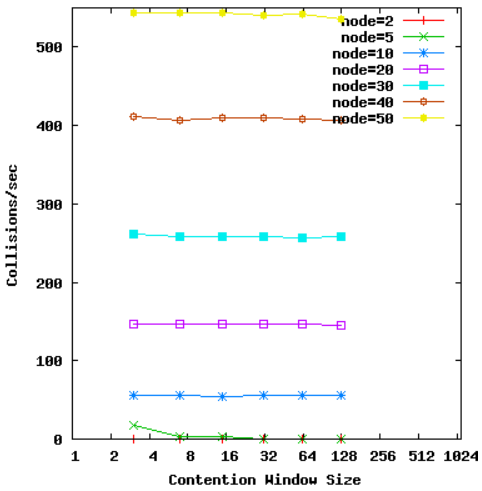


Figure 6.4: DWMAC

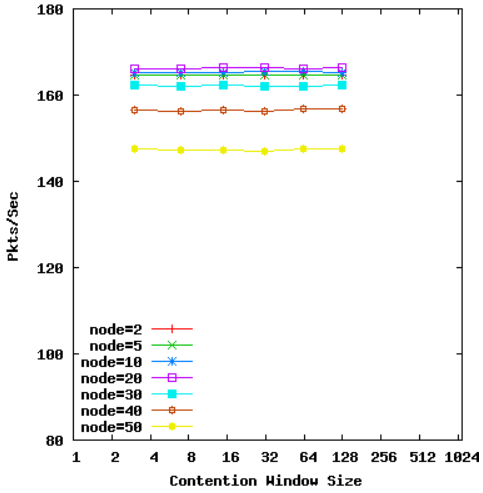


Figure 6.5: DWMAC-Modified

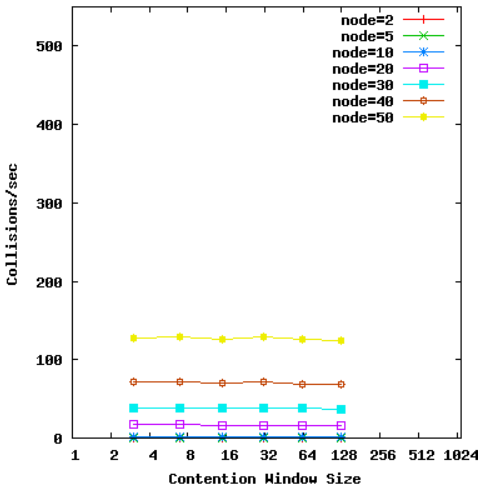


Figure 6.6: DWMAC-Modified

Above figures show simulation results for DWMAC and DWMAC-Modified. Figures 6.3 and 6.5 show throughput vs. contention window size for DWMAC and DWMAC-Modified respectively and figures 6.4 and 6.6 show collisions/sec vs. contention window size for DWMAC and DWMAC-Modified respectively. From figures 6.3 and 6.5 we can see that for DWMAC and DWMAC-Modified throughput is independent of contention window size as opposed to 802.11. Also we can see that in DWMAC throughput decreases as number of nodes increases whereas in DWMAC-Modified throughput does not decrease so much with increase in number of nodes. As in DWMAC-Modified number of active nodes are counted in both restricted and normal states it has correct estimation of active nodes in the network. So number of collisions/sec in DWMAC-Modified is very less than DWMAC and so throughput for DWMAC-Modified is high and stable even with large

number of nodes. Also we can see that when number of nodes is less than 30, DWMAC-Modified throughput is same as 802.11 optimal throughput. However when number of nodes is greater than 30, DWMAC-Modified also fails to prevents all the collisions and throughput is less than 802.11 optimal throughput for large number of nodes.

6.2 Performance Comparison in Multihop Networks

Simulation is performed for different scenarios. We have selected scenarios such that they capture the situation in which MAC protocol may perform bad due to some characteristics of ad hoc networks. Following are the topologies we have selected.

1. **Chain Topology** It shows the effect of intra-flow contention and collisions due to hidden nodes.

2. **Crossing Chains** It shows the effect of bottleneck developing at the crossing node in which network throughput is limited by one node.

3. **Parallel Chains** It shows the effect of not only intra-flow contention but also inter-flow contention.

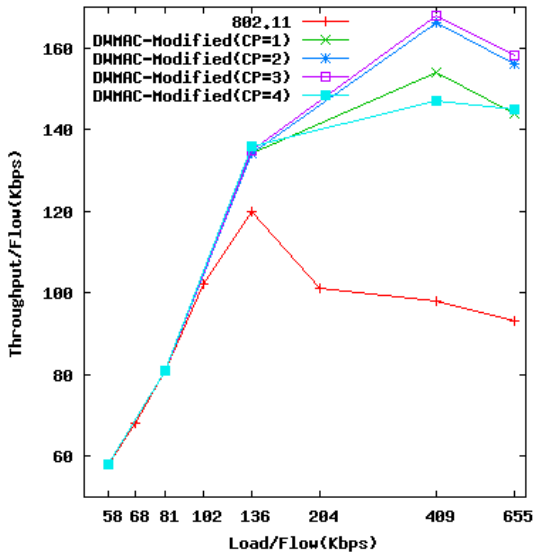
4. **Mesh Topology** Fifty single hop flows in the mesh topology which clearly shows effect of hidden nodes, exposed nodes and false blocking of the channel by RTS frames.

Transmission range is 250 meters and carrier sensing range is 550 meters. Channel bandwidth is 1 Mbps. TwoRayGround propagation model is used. No noise model is used. Ad hoc routing protocol is disabled instead each node has predefined static path which is used as a route so no routing overhead and only data packets are transmitted. CBR traffic with 512 data packet size is used. All the CBR connections have same data packet size. Each point in graph is average of 5 runs and each run is performed with different seed for 100 seconds. CW_{min} for 802.11 is set at 32 and for DWMAC is set to 7. For DWMAC protocol each line in graph is for different CP (Correction Parameter) value which multiplies the waiting time for a node.

1. **Topology 1**

As shown in figure, a source node is transmitting CBR packets to destination 9 hop away.

(a) 10 Nodes in Chain.



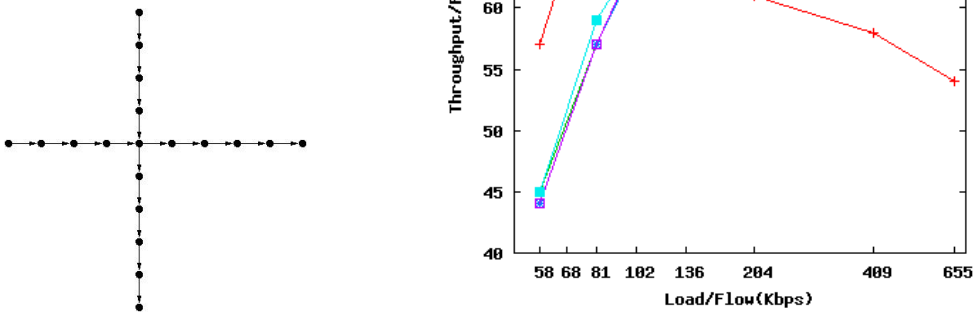
(b) Throughput/Flow(Kbps) vs. Load/Flow(Kbps)

Figure 6.7: Topology 1

Distance between two nodes is 200 meter. We can see from the figure that at low load throughput for both protocols, 802.11 and DWMAC-Modified, are same. For high load throughput for DWMAC-Modified is much higher than 802.11. The reason behind this is in 802.11, as we increase load CBR source pumps more and more packets in chain than can be forwarded by middle nodes. Middle nodes can not forward data packets at the same speed as starting nodes because they share channels with more nodes than starting nodes. So packets are gathered at middle nodes and finally dropped due to queue overflow or end of simulation. In DWMAC-Modified protocol more priority is given to the nodes which has more number of active nodes in its neighborhood whose destination is itself. Source node has no active neighbors whose destination is itself. So it will get less priority for channel access than forwarding nodes and hence it will pump less packets than 802.11 in chain. In other words all these packets sent by source reach to the destination which increases throughput in DWMAC-Modified even in high load. Also for both the protocols after some points throughput starts to decrease but in DWMAC-Modified protocol this point comes at very high load than 802.11.

2. **Topology 2**

As shown in figure 2 chains are passing from one node. Distance between each node is



(a) 2 Crossing Chains

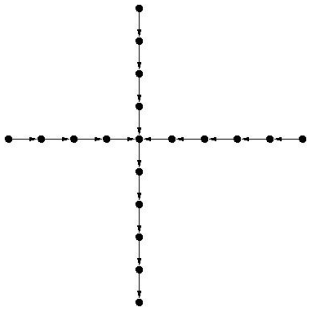
(b) Throughput/Flow(Kbps) vs. Load/Flow(Kbps)

Figure 6.8: Topology 2

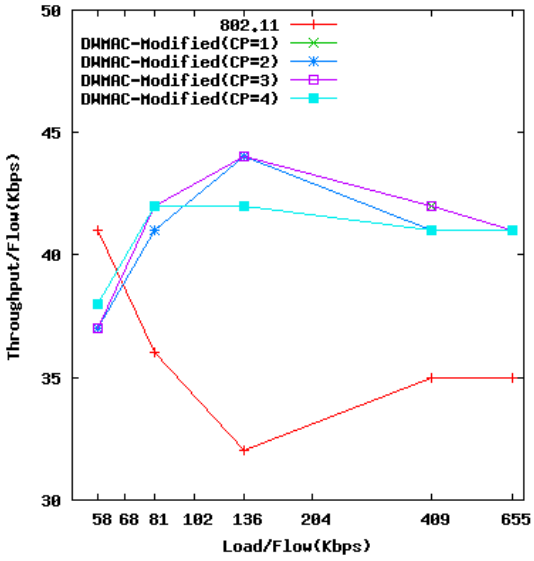
200 meter. As shown in figure, throughput/flow is less than that of in case of single chain topology. Here as two flows are passing from a single node, network capacity is limited by a single node and throughput/flow approximately half of chain topology. At high load DWMAC outperforms 802.11 but at light load 802.11 performs better than DWMAC-Modified. Reason is when collision happens, 802.11 doubles its contention window. So packet is not dropped due to ShortRetryLimit (=7). Whereas in DWMAC-Modified contention window is fix so it continues to send RTS even CTS is not replied resulting packet drop due to ShortRetryLimit. Also as we increase load, in 802.11 throughput starts to decrease whereas in DWMAC-Modified it starts to decrease at much more load than 802.11.

3. **Topology 3**

As shown from the figure, throughput/flow is approximately one third of the chain topology



(a) 2 Crossing Chains



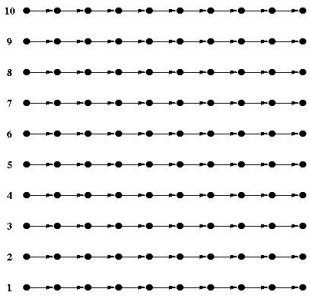
(b) Throughput/Flow(Kbps) vs. Load/Flow(Kbps)

Figure 6.9: Topology 3

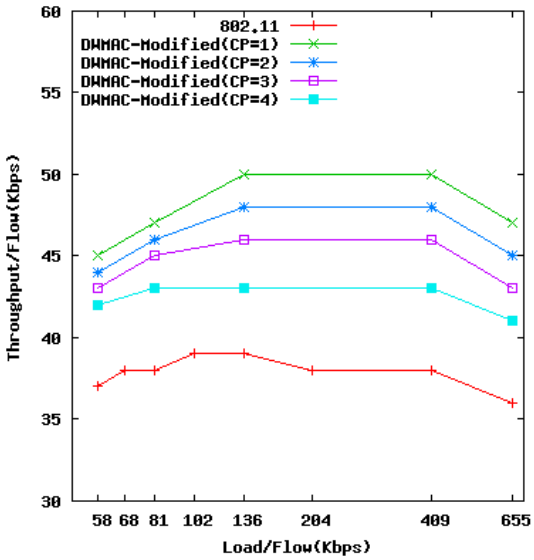
as three chains are passing from one node. Same as in previous two cases DWMAC-Modified outperforms 802.11 at higher load. Here, the strange behavior of 802.11 can be explained as below. There are 3 flows in networks. So at some load bottleneck node get congested and packets are dropped at bottleneck node so channel capacity has been used to forward these packets is wasted. Whereas at higher load packets are dropped at starting nodes so channel capacity is not wasted.

4. **Topology 4**

Here, the better performance of DWMAC-Modified than 802.11 can clearly be seen. As



(a) 10 parallel Chains



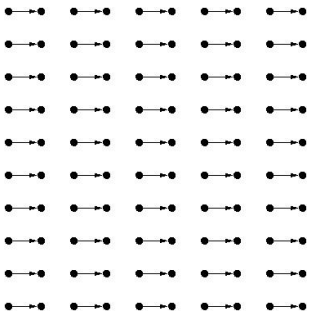
(b) Throughput/Flow(Kbps) vs. Load/Flow(Kbps)

Figure 6.10: Topology 4

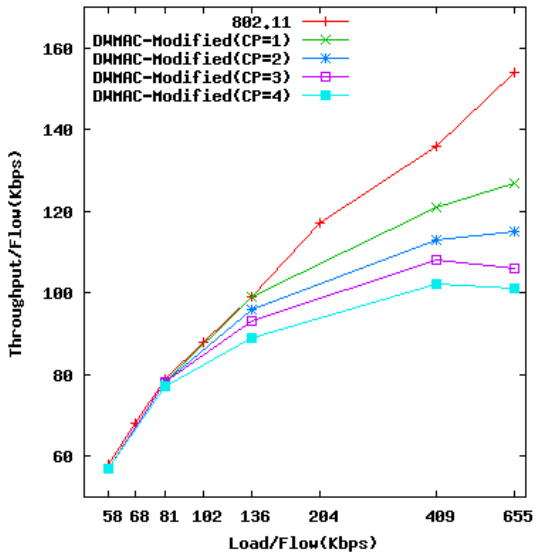
there are 10 parallel chains, total networks throughput for DWMAC-Modified is very much higher than 802.11. Even for low load at least some chains have packets to send which causes DWMAC-Modified to perform better than 802.11.

5. **Topology 5**

As shown from the figure for low load 802.11 and DWMAC-Modified have same throughput



(a) 50 Single hop Flows



(b) Throughput/Flow(Kbps) vs. Load/Flow(Kbps)

Figure 6.11: Topology 5

but at higher load 802.11 has more throughput than DWMAC-Modified. Reason is as in multihop networks most of the collisions are due to hidden nodes and 802.11 adjusts its contention window after collision, many continuous collisions and hence packet drop due to ShortRetryLimit can be reduced. Whereas in DWMAC-Modified packets are dropped due to its fix contention window size. In DWMAC-Modified, CP with high values causes channel to be idle reducing throughput as shown from the figure. So 802.11 performs better than DWMAC-Modified in such scenarios where there are many hidden nodes and flows are not multihop.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

As per simulation results DWMAC-Modified protocol's performance in single hop networks, is independent of minimum contention window size as opposed to IEEE 802.11 DCF. But for large number of nodes performance of DWMAC-Modified somewhat degrades whereas in IEEE 802.11 DCF best performance can always be achieved by varying minimum contention window size. Also in DWMAC-Modified protocol if we count active neighbors in both restricted mode and contention mode then protocol becomes able to estimate active neighbors correctly and performance remains good and stable for large range of active nodes as shown in graphs.

For multihop networks, DWMAC-Modified can not perform better than IEEE 802.11 DCF in all scenarios as in multihop networks most of the collisions happen due to hidden terminals whose transmissions can not be listened and so DWMAC-Modified is not able to accommodate them as active neighbors. Due to its fix contention window DWMAC-Modified protocol can not prevent such continuous collisions as opposed to IEEE 802.11 DCF, which causes performance degradation. Estimation of active neighbors in interference range also can not help in all scenarios and depends on nodes distribution.

Particularly in chain topology DWMAC-Modified protocol outperforms IEEE 802.11 DCF because of high priority given to the forwarding nodes eliminates packet drop at middle nodes.

7.2 Future Work

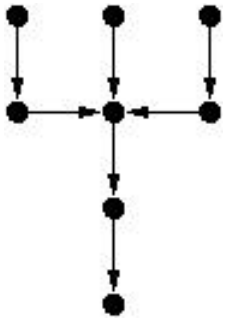
Contention window is fix in DWMAC-Modified which can be made variable (keeping dynamic waiting also) as in IEEE 802.11 DCF or by another way to avoid continuous collisions in multihop networks which might increase DWMAC-Modified performance in multihop networks also.

As DWMAC-Modified protocol waits for its neighbors to transmit, its behavior is fairer than IEEE 802.11 DCF. For future work, DWMAC-Modified can be compared with IEEE 802.11 DCF for fairness with different network scenarios and traffic patterns.

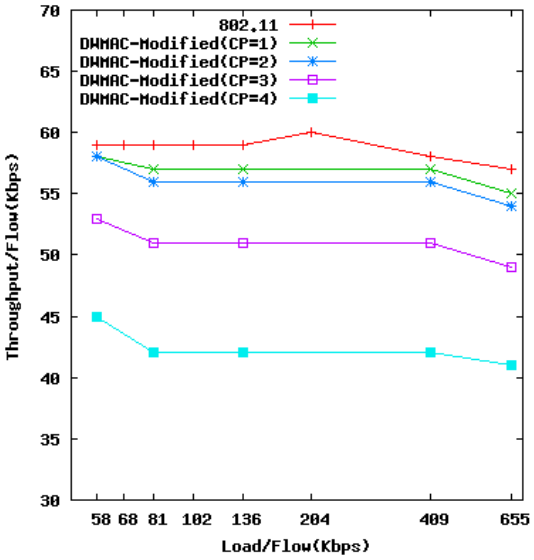
Appendix A

Topology with 3 4-hops flows

The results of the following topology do not match with other topologies and are not as expected. We will be interested to analyze these results in future. Here, 802.11 is able to pass



(a) 3-4 hop flows



(b) Throughput/Flow(Kbps) vs. Load/Flow(Kbps)

Figure A.1: 3 4-hops crossing flows

more packets than DWMAC-Modified. Somehow 802.11 manages to give priority to bottleneck node. DWMAC-Modified's performance is poorer than 802.11 which is not expected. Larger value of CP in DWMAC-Modified causes the nodes to wait extra amount of time and degrades the performance.

Bibliography

[1] IEEE Standard for Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications, Nov. 1997. P802.11

[2] Network Simulator 2 (NS2), http://www.isi.edu/nsnam/ns

[3] Bianchi, G., "Performance analysis of the IEEE 802.11 distributed coordination function," Selected Areas in Communications, IEEE Journal on , vol.18, no.3, pp.535-547, Mar 2000

[4] Tobagi, F.; Kleinrock, L., "Packet Switching in Radio Channels: Part IV–Stability Considerations and Dynamic Control in Carrier Sense Multiple Access," Communications, IEEE Transactions on , vol.25, no.10, pp. 1103-1119, Oct 1977

[5] Chen, Y., Zeng, Q., and Agrawal, D. P. 2008. Analytical modeling of MAC protocol in ad hoc networks: Research Articles. Wirel. Commun. Mob. Comput. 8, 1 (Jan. 2008), 45-59. DOI= http://dx.doi.org/10.1002/wcm.v8:1

[6] J. He, D. Kaleshi, A. Munro, Y. Wang, A. Doufexi, J. Mcgeehan, and Z. Fan, "Performance investigation of ieee 802.11 mac in multihop wireless networks," in MSWiM '05: Proceedings of the 8th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems. New York, NY, USA: ACM Press, 2005, pp. 242-249

[7] Ping Chung Ng; Soung Chang Liew, "Offered load control in IEEE 802.11 multi-hop ad-hoc networks," Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on , vol., no., pp. 80-89, 25-27 Oct. 2004

[8] Barowski, Y.; Biaz, S.; Agrawal, P., "Towards the performance analysis of IEEE 802.11 in multi-hop ad-hoc networks," Wireless Communications and Networking Conference, 2005 IEEE , vol.1, no., pp. 100-106 Vol. 1, 13-17 March 2005

[9] Li, J., Blake, C., De Couto, D. S., Lee, H. I., and Morris, R. 2001. Capacity of Ad Hoc wireless networks. In Proceedings of the 7th Annual international Conference on Mobile Com-

puting and Networking (Rome, Italy). MobiCom '01. ACM, New York, NY, 61-69. DOI= http://doi.acm.org/10.1145/381677.381684

[10] Xu, S.; Saadawi, T., "Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?," Communications Magazine, IEEE , vol.39, no.6, pp.130-137, Jun 2001

[11] Bharghavan, V., Demers, A., Shenker, S., and Zhang, L. 1994. MACAW: a media access protocol for wireless LAN's. In Proceedings of the Conference on Communications Architectures, Protocols and Applications (London, United Kingdom, August 31 - September 02, 1994). SIGCOMM '94. ACM, New York, NY, 212-225. DOI= http://doi.acm.org/10.1145/190314.190334

[12] Hongqiang Zhai; Jianfeng Wang; Yuguang Fang, "Distributed packet scheduling for multihop flows in ad hoc networks," Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE , vol.2, no., pp. 1081-1086 Vol.2, 21-25 March 2004

[13] Wanrong Yu, Jiannong Cao, Xingming Zhou, VWMAC: An efficient MAC Protocol for Resolving Intra-flow Contention in Wireless Ad Hoc Networks, 1st International Conference on Grid and Pervasive Computing, May 3-5, 2006, Taiwan

[14] Zhenqiang Ye, Dan Berger, Prasun Sinha, Srikanth V. Krishnamurthy, Michalis Faloutsos, Satish K. Tripathi, "On Alleviating MAC Layer Self-Contention in Ad-hoc Networks" Poster,MobiCom 2003

[15] Wanrong Yu; Xiaodong Wang; Xingming Zhou, "Alleviating MAC Layer Contentions through Dynamic Waiting in Wireless Ad Hoc Networks," Computer and Information Technology, 2006. CIT '06. The Sixth IEEE International Conference on , vol., no., pp.93-93, Sept. 2006

[16] Jun Wang; Min Song, "An Efficient Traffic Adaptive Backoff Protocol for Wireless MAC Layer," Wireless Algorithms, Systems and Applications, 2007. WASA 2007. International Conference on , vol., no., pp.169-173, 1-3 Aug. 2007

[17] Fengji Ye; Hua Yang; Sikdar, B., "Enhancing MAC Coordination to Boost Spatial Reuse in IEEE 802.11 Ad Hoc Networks," Communications, 2006. ICC '06. IEEE International Conference on , vol.8, no., pp.3814-3819, June 2006

[18] Deekshitulu, M.V.S.; Nandi, S.; Chowdhury, A.R., "Improving MAC Layer Fairness in Multi-Hop 802.11 Networks," Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on , vol., no., pp.1-8, 7-12 Jan. 2007

[19] J. He and H. K. Pung, "Fairness of medium access control protocols for multi-hop ad hoc wireless networks," Comput. Networks, vol. 48, no. 6, pp. 867-890, August 2005. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2004.11.020

[20] Razafindralambo, T. and Gurin-Lassous, I. 2008. Increasing fairness and efficiency using the MadMac protocol in ad hoc networks. Ad Hoc Netw. 6, 3 (May. 2008), 408-423. DOI= http://dx.doi.org/10.1016/j.adhoc.2007.03.003

[21] Hung-Yun Hsieh; Sivakumar, R., "IEEE 802.11 over multi-hop wireless networks: problems and new perspectives," Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. 2002 IEEE 56th , vol.2, no., pp. 748-752 vol.2, 2002