Performance Degradation of IEEE 802.11 MANET due to Heavy Increase and Heavy Decrease in Contention Window

Vikram Jain
Asst. Professor and Head
Department of IT
Shri Ram Institute of
Technology, Jabalpur

Sakshi Suhane
Department of IT
Shri Ram Institute of
Technology, Jabalpur

ABSTRACT

The primary Medium Access Control (MAC) technique of IEEE 802.11 is called Distributed Coordination Function (DCF). This protocol adopts a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with a binary exponential backoff (BEB) algorithm to access the channel. The protocol performance mainly depends on backoff procedure which reduces the probability of collision.

With BEB, waiting time of a node gets doubled after every unsuccessful transmission. This introduces fast-growing retransmission delays for the backlog traffic. In a Mobile Ad hoc Network (MANET), it would be worthwhile to slow down the growth-rate of waiting time because the nodes communicating in a MANET might move out of collision range while waiting for retransmission. Moreover, DCF reduces the Contention Window to the initial value after each successful transmission which essentially assumes that each successful transmission is an indication that the system is under low traffic loading.

In this paper, we point out the inefficiencies in conventional DCF protocol by simulating the data transfer in a MANET with different number of nodes under different traffic conditions. It is shown that as the number of nodes in a MANET increases the performance of conventional DCF protocol in IEEE 802.11 decreases drastically. Finally we propose a layout for the new DCF protocol with modified backoff algorithm.

General Terms

Wireless Networks, Mobile Ad Hoc Networks

Keywords

DCF, MAC, CSMA/CA, BEB, MANET etc.

1. INTRODUCTION

In recent years, much interest has been involved in the design of wireless networks for local area communication. Study group 802.11 was formed under IEEE Project 802 to recommend an international standard for Wireless Local Area Networks (WLAN's). The final version of the standard was released in 1999, and provides detailed medium access control (MAC) and physical layer (PHY) specification for WLAN's [1].

WLANs can operate in two modes namely infrastructure based and infrastructure-less mode or ad-hoc mode. In infrastructure based mode, a central coordinator or an Access Point (AP) is needed for operation of network. The AP resolves issues related to channel access and transfer of information between stations. AP based networks are also called as a single-hop networks where the all the information from a source to destination is transferred via the AP. Stations cannot communicate with each other directly. In the other mode of operation, known as the Mobile Ad-hoc Network (MANET), nodes communicates directly with each other without any central coordinator. This requires that all nodes must act as packet forwards to relay packets between two stations that are outside the radio coverage of each other. This provides greater flexibility and robustness.

To transmit packets to a node outside its range, the network uses multi-hop store-and-forward routing. WLANs have great potential for both military and commercial applications. In a WLAN, nodes transmit packets in an unsynchronized fashion. The protocol employed in the medium access control (MAC) layer is responsible for coordinating access to the shared channel while minimizing conflicts. Hence it is important to design an efficient and effective MAC protocol.

In the 802.11 protocol, the fundamental mechanism to access the medium is called distributed coordination function (DCF). This is a random access scheme, based on the carrier sense multiple access with collision avoidance (CSMA/CA) protocol. Retransmission of collided packets is managed according to binary exponential backoff (BEB) rules. The standard also defines an optional point coordination function (PCF), which is a centralized MAC protocol able to support collision free and time bounded services [2].

2. OVERVIEW

2.1 802.11 Medium Access Control Layer

The MAC layer has to fulfill several tasks. It has to control medium access but it can also offer support for roaming, authentication, and power conservation. The basic services provided by the MAC layer are the mandatory asynchronous data service and an optional time bounded service. The following three basic access mechanisms have been defined for IEEE 802.11: the mandatory basic access method based on CSMA/CA, an optional method avoiding hidden terminal problem, and finally a contention-free polling method for time bounded services. The first two methods are also summarized as Distributed Coordination Function (DCF), the third method is called Point Coordination Function (PCF). The MAC mechanisms are also called as distributed foundation wireless medium access control (DFWMAC).

Following figure (figure 1) depicts the architecture of 802.11 MAC layer –
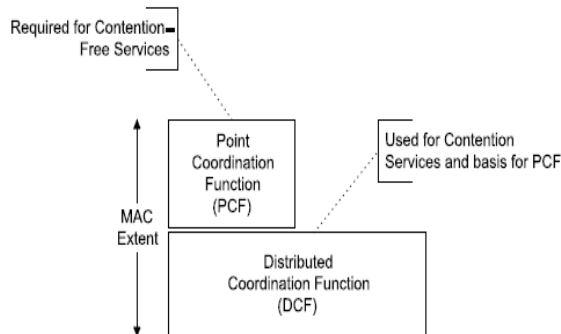

Figure 1: MAC architecture

2.2 Distributed Coordination Function

The fundamental access method of the IEEE 802.11 MAC is a DCF known as carrier sense multiple access with collision avoidance (CSMA/CA). The DCF must be implemented in all stations, for use within both ad-hoc and infrastructure network configurations. For a station to transmit, it shall sense the medium to determine if another station is transmitting. If the medium is not determined to be busy, the transmission may proceed. The CSMA/CA distributed algorithm mandates that a gap of a minimum specified duration exist between contiguous frame sequences. A transmitting station must ensure that the medium is idle for this required duration before attempting to transmit. If the medium is determined to be busy, the station shall defer until the end of the current transmission. After deferral, or prior to attempting to transmit again immediately after a successful transmission, the station shall select a random backoff interval and should decrement the backoff interval counter while the medium is idle.

2.3. Operation mode of Conventional DCF

In 802.11, the DCF is the fundamental access method used to support asynchronous data transfer on a best effort basis [1]. As specified in the standards, the DCF must be supported by all the stations in a basic service set (BSS). The DCF is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CD is not used because a station is unable to listen to the channel while transmitting. In 802.11 Carrier Sense is performed both at physical layer, which is also referred to as physical carrier sensing, and at the MAC layer, which is known as virtual carrier sensing. The PCF in the 802.11 is a polling-based protocol, which is designed to support collision free and real time services.

There are two techniques used for packet transmitting in DCF. The default one is a two-way handshaking mechanism, also known as basic access method. A positive MAC acknowledgement (ACK) is transmitted by the destination station to signal the successful packet transmission. The other optional one is a four-way handshaking mechanism, which uses request-to-send / clear-to-send (RTS/CTS) technique to reserve the channel before data transmission. Before transmitting a packet, a station operating in RTS/CTS mode "reserves" the channel by sending a special Request-To-Send short frame. The destination station acknowledges the receipt of an RTS frame by sending back a Clear-To-Send frame, after which normal packet transmission and ACK response occurs. Since collision may occur only on the RTS frame, and it is detected by the lack of CTS response, the RTS/CTS mechanism allows increasing the system performance by reducing the duration of a collision when long messages are transmitted.

A station with a new packet to transmit monitors the channel activity. If the channel is idle for a period of time equal to a distributed inter-frame space (DIFS), the station transmits. Otherwise, if the channel is sensed busy (either immediately or during the DIFS), the station persists to monitor the channel until it is measured idle for a DIFS. At this point, the station generates a random backoff interval before transmitting (this is the Collision Avoidance feature of the protocol), to minimize the probability of collision with packets being transmitted by other stations. In addition, to avoid channel capture, a station must wait a random backoff time between two consecutive new packet transmissions, even if the medium is sensed idle in the DIFS time.

For efficiency reasons, DCF employs a discrete-time backoff scale. The time immediately following an idle DIFS is slotted, and a station is allowed to transmit only at the beginning of each slot time. The slot time size is set equal to the time needed at any station to detect the transmission of a packet from any other station. As shown in Table I, it depends on the physical layer, and it accounts for the propagation delay, for the time needed to switch from the receiving to the transmitting state, and for the

time to signal to the MAC layer the state of the channel (busy detect time).

2.4 Backoff procedure

The backoff procedure shall be invoked for a STA to transfer a frame when finding the medium busy as indicated by either the physical or virtual carrier-sense mechanism (see Figure 2).

Figure 2: Backoff Procedure

The backoff procedure shall also be invoked when a transmitting STA infers a failed transmission. To begin the backoff procedure, the STA shall set its Backoff Timer to a random backoff time. All backoff slots occur following a DIFS period during which the medium is determined to be idle for the duration of the DIFS period, or following an EIFS period during which the medium is determined to be idle for the duration of the EIFS period following detection of a frame that was not received correctly. A STA performing the backoff procedure shall use the carrier-sense mechanism to determine whether there is activity during each backoff slot. If no medium activity is indicated for the duration of a particular backoff slot, then the backoff procedure shall decrement its backoff time by slot Time. If the medium is determined to be busy at any time during a backoff slot, then the backoff procedure is suspended; that is, the backoff timer shall not decrement for that slot. The medium shall be determined to be idle for the duration of a DIFS period or EIFS, before the backoff procedure is allowed to resume. Transmission shall commence whenever the Backoff Timer reaches zero. A backoff procedure shall be performed immediately after the end of every transmission. In the case of

successful acknowledged transmissions, this backoff procedure shall begin at the end of the received ACK frame. In the case of unsuccessful transmissions requiring acknowledgment, this backoff procedure shall begin at the end of the ACK timeout interval. If the transmission is successful, the CW value reverts
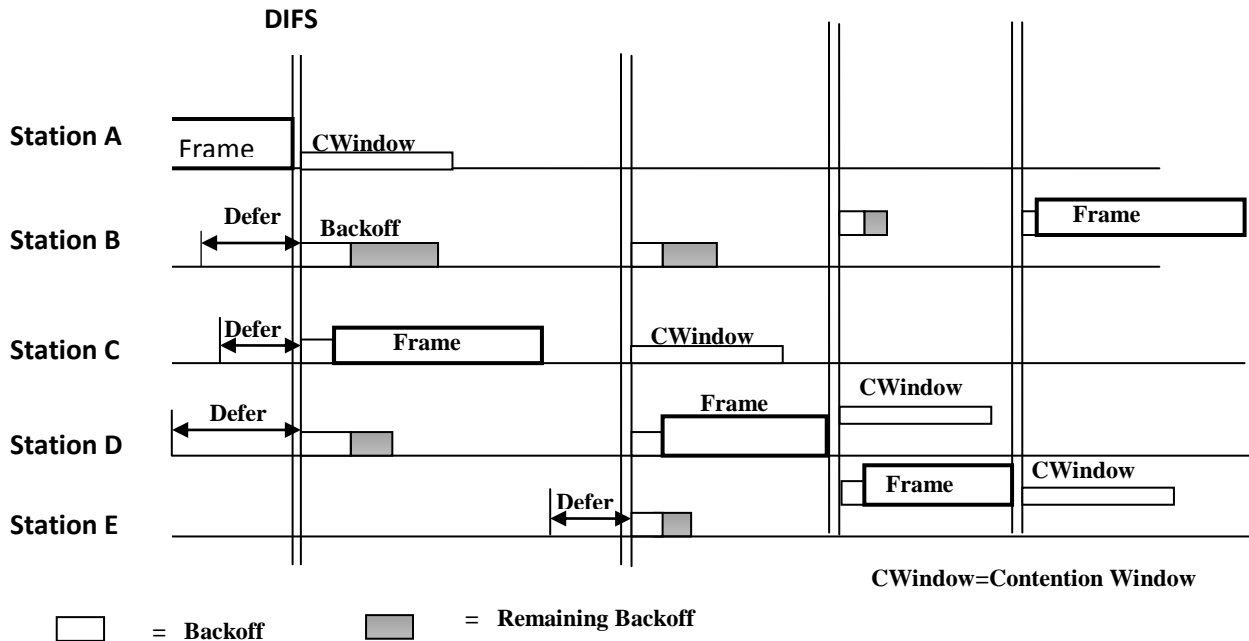
to CW_{min} before the random backoff interval is chosen, and the STA short retry count and/or STA long retry count are updated . This assures that transmitted frames from a STA are always separated by at least one backoff interval. The effect of this procedure is that when multiple STAs are deferring and go into random backoff, then the STA selecting the smallest backoff time using the random function will win the contention.

3. PROBLEMS WITH EXISTING BACKOFF ALGORITHM

From the above discussion we can see that DCF resolves collision through Contention Window and backoff time. As specified in the original standard, after each successful transmission, the backoff stage will resume to the initial stage 0,

and the contention window will be set to **CW_{min}** regardless of network conditions such as number of competing nodes. This method, referred to as 'heavy decrease' [3] tends to work well when the number of competing nodes is less. When the number of competing nodes increases, it will be shown to be ineffective, since the new collisions can potentially occur and cause significant performance degradation.

The operation of existing DCF protocol can be summarized from the following figure (Figure 3) –
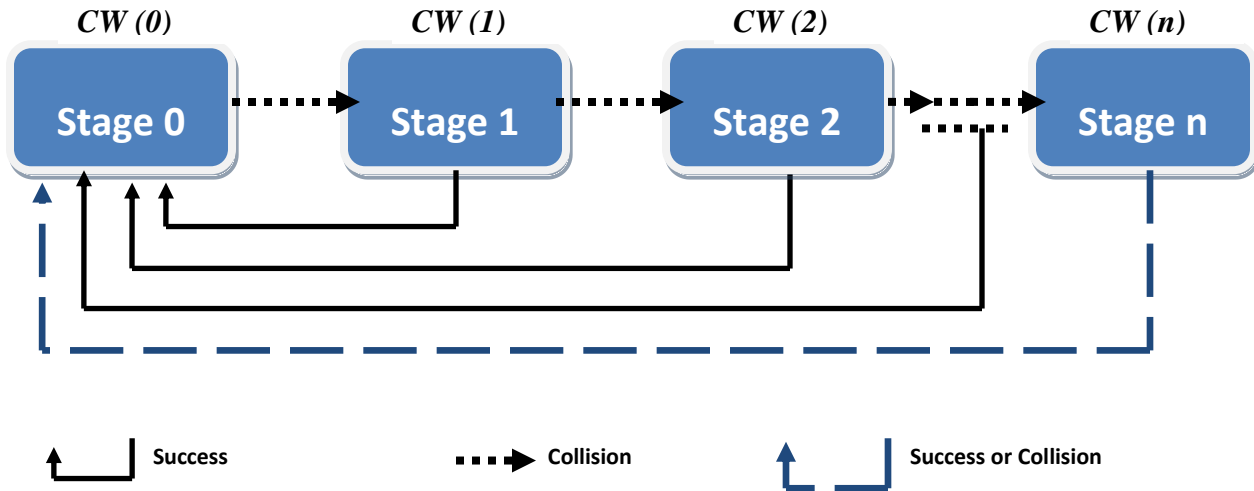

Figure 3: Operation of 802.11 DCF with BEB Algorithm

3.1 Heavy Decrease

For example, let us assume that the current backoff stage is 'i' with contention window CW (i) = 2^i * CW_{min}, and there is a successful transmission, the next backoff stage will be stage 0 with contention window CW(0) = 31 according to the specification. But if the number of competing nodes is large enough (>>31), the new collision will likely occur at the backoff stage 0. The main argument is that since the current backoff stage is 'i' some collision must have occurred recently at the previous stage. Now if the number of current competing nodes is larger than or close to CW(i), and if the backoff stage is set to 0, there is a high probability that new collisions will happen. So resetting the contention window after every successful transmission is an inefficient approach if the number of nodes is large.

Thus, the operation of the BEB algorithm can be summarized as follows:

CW = min [2*CW, CW_{max}], upon collision (1)

CW = CW_{min} , upon success (2)

The values of CW_{min} and CW_{max} reported in the final version of standard are summarized in the following Table –

Table 1. Slot Time, Minimum and Maximum Contention Window Values for three PHY specified by 802.11: Frequency Hopping Spread Spectrum(FHSS), Direct Spread Spectrum(DSSS) and InfraRed(IR)

PHY	Slot Time	CWmin	CWmax
FHSS	50 μsec	16	1024
DSSS	20 μsec	32	1024
IR	8 μsec	64	1024

3.2 Heavy Increase

We also observe that The BEB algorithm causes a fast build-up (i.e., growth-rate) of waiting times spreading the backlog traffic over a larger time frame. However, this fast build-up of waiting time with increasing number of occurrence of collisions might not be appropriate for a MANET, wherein the contending nodes might leave the geographical location of contention itself after a short while due to their mobility. In view of this, we conjecture that it may not be necessary to make a node wait for a duration that builds up exponentially with a binary base.

4. SIMULATION

Design and implementation of the proposed protocol has been carried out using Global Mobile Information System Simulator [6] (GloMoSim) which is a scalable simulation environment for large wireless and wired communication networks. GloMoSim uses a parallel discrete-event simulation capability provided by Parsec.

Our simulation considered a network of 50 mobile nodes placed randomly within a 1000 x 1000 m^2 area. Node movement is modeled using the random waypoint mobility model (RWMM), which is widely used in MANET simulations. In RWMM, nodes move at a speed uniformly distributed in [MIN SPEED, MAX SPEED].

Each node begins the simulation by moving towards a randomly chosen destination (waypoint). Whenever a node reaches a waypoint, it rests for a pause time. It then chooses a new waypoint and moves towards the same. This process is repeated until the end of simulation time. In our simulations, however, pause time is set at zero (i.e., nodes move continuously throughout the simulation period). This is done to study the impact of continuous node mobility (i.e., worst-case scenario) on the network performance. Constant bit rate (CBR) data sessions among randomly chosen source – destination pairs (SDPs) are used. For example, with 10 SDPs amongst 50 nodes, 10 source nodes and 10 destination nodes (i.e., 20 nodes in total) will be engaged in data transfer. However, during this data transfer process, all of the 50 nodes (including the above 20 nodes) will operate in the background for providing necessary support (i.e., routing/forwarding) to the ongoing communication process in the network.

4.1 Simulation Parameters
Simulation was carried out with 5, 11, 20, 25, 35, 45, 60, 70, 80, 90 and 95 computers transmitting data to each other as per the simulation parameters mentioned in Table 2.

Table 2 shows some of the important simulation parameters that were used during simulation. Every time a node transmits the data successfully, its contention window is set to default value of 32. With every unsuccessful transmission the contention window is doubled.

Table -2 Simulation Parameters

Parameter	Value
Mobility Model	Random Waypoint
Speed of Mobile Node	Uniformly distributed between [0,10] m/sec
Propagation Model	Two Ray
Transmission Range of each node	250 meters
Channel Frequency	2.4 GHz
Data Rate	2 Mbps
Network Protocol	IP
No. of SDPs	5, 11, 20, 25, 35, 45, 60, 70, 80, 90, 95
MAC Protocol	DCF with Binary Exponential Backoff
Routing Protocol	AODV, DSR

5. RESULTS OBTAINED
The conventional DCF protocol was tested for different numbers of Source Destination Pairs with AODV and DSR routing protocols. The routing protocols yielded no significant difference to the results obtained. A series of simulations were performed and the conventional DCF protocol was tested for parameters such as Throughput, Average End to End delay and Average Packet Loss Ratio. The following graphs were plotted from the obtained output –

5.1 Throughput Analysis –
Figure 4 reflects how the throughput varies with increase in number of nodes in conventional DCF protocol. As observed, the throughput drops sharply with increase in number of nodes. Hence, it can be said that the conventional DCF protocol is not suitable when the node density in a Wi-Fi network is high.
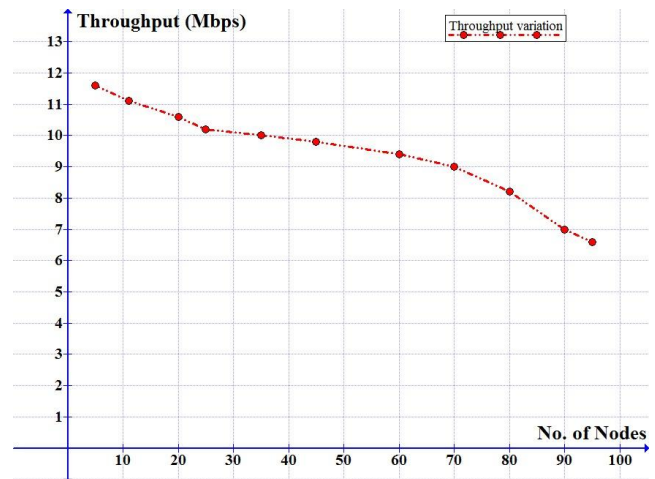

Figure 4: Throughput Vs Number of Nodes

5.2 Average End to End Delay –
Figure 5 reflects the variation in average end to end delay. As seen from the simulation results, the average end to end delay is within reasonable limits when the number of nodes in the network is small (less than 25). However, as the number of nodes in the network crosses 25, the delay increases significantly. Hence, the conventional DCF protocol is inefficient with high node density network when small end to end delay is desirable.
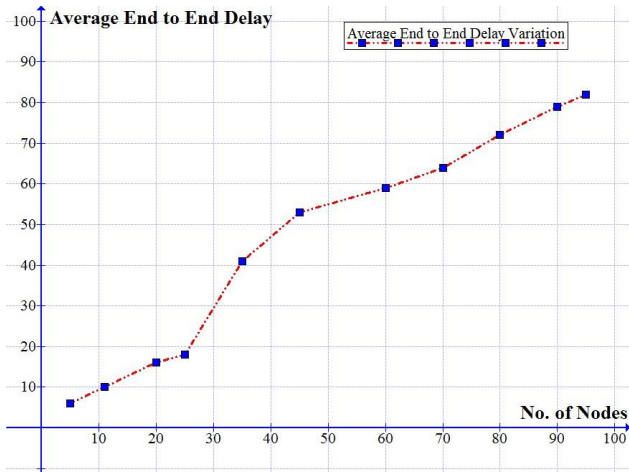
Figure 5: Average end to end delay Vs Number of Nodes

5.3 Packet Loss Ratio –

Packet loss ratio is defined as the ratio of total number of packets sent by the source computer to the total number of packets received by the destination. Figure 6 shows the average packet success rate variation with the number of nodes in the network.
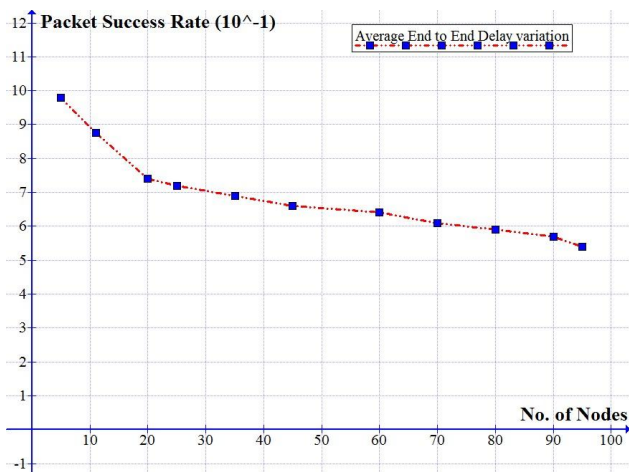

Figure 6: Packet Success Rate Vs No. of Nodes

As observed, the packet success rate drops sharply as the number of nodes increases in the network. As the number of nodes comes close to 90, the packet success rate approaches 0.5 which means that there is a 50% chance that the packet will be transmitted successfully.

6. CONCLUSION

In this paper, we simulated the conventional DCF protocol in a MANET under different number of competing nodes in the network. As discussed in the previous section, IEEE 802.11

DCF has several disadvantages in that its throughput decreases as the number of nodes in the network increases, average end to end delay is more, and there is a high packet loss ratio in high node density networks.

Hence, we suggest that the conventional DCF protocol be modified for the high node density network. The major inefficiencies in conventional DCF protocol are due to the heavy increase and heavy decrease in Contention Window upon unsuccessful/successful transmission of data frames from source to destination.

We propose the following modifications to the conventional DCF protocol to enhance the performance –

6.1 A gentle approach towards increasing and decreasing the Contention Window

Binary exponential backoff algorithm increases the waiting time of each node exponentially by 2 with every unsuccessful transmission. Also, after each successful transmission, the backoff stage will resume to initial stage 0, and the contention window will be set to minimum regardless of network conditions such as number of competing nodes. These methods, referred to as "heavy increase" and "heavy decrease" tends to work well when the number of competing nodes is small. However, as the number of nodes increase, it has been shown to be ineffective in our simulation results.

We propose a modification to BEB algorithm suitable for WLANs. In particular, the backoff time is increased exponentially but with a reduced base value 'b' (less than 2) after each unsuccessful transmission until a prescribed maximum value (CW_{max}) is reached. The modified backoff scheme upon unsuccessful transmission can then be expressed as –

CW = min [b*CW, CW_{max}], upon collision.

We also propose a gentle decrease of collision window. In certain hotspot areas, where the network is highly loaded, we can halve the contention window by a factor of 2 upon 'k' successful transmissions rather than resetting it to its initial value 'CW_{min}'.

The main challenge here lies in computing the optimal values of 'b' and 'k'. The intuition is that with many (or few) competing nodes, it requires large (or small) value of 'k'. So, if the number of current competing nodes can be obtained, we can intelligently adjust the parameter 'k'.

6.2 Obtaining the number of competing nodes

In a distributed environment, it is difficult to find the actual number of currently competing nodes. But, if we can have some kind of "**Admission Control**" or "**Node Registration**" method, in which a node registers itself in the network before it starts transmitting, we can have a rough estimate of total participating

nodes with which we can find the optimal value of 'k' as mentioned in previous method [4]. Also, we can regulate the value of Contention Window between an optimal minimum and maximum value instead of resetting it and doubling it upon every successful/unsuccessful transmission.

6.3 Providing a Quality of Service (QoS)

We can propose methods to provide service differentiation between high and low priority traffics with focus on fairness [4], [5]. The parameters that we can employ here for differentiation are Inter Frame Spacing (IFS) and CW increasing factor. These 2 important parameters are used to differentiate traffics in many researches. In a competition between 2 nodes which are sensing the medium with different IFS, the node having smaller IFS will win. Therefore, we allocate smaller IFS to high priority traffics. Hence, the chance of the node with smaller CW to send its packet is higher. We dedicate smaller IFS and CW increasing factor to high priority traffics.

Also, we can have different values of minimum and maximum CW for different traffic types. For example, we can have a contention window ranging from 16-124 for highest priority traffic, so that nodes involved in sending high priority data gets access of medium more frequently than normal priority nodes.

7. REFERENCES

[1]. IEEE 802.11 standard, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std. June 1999.

[2]. Haitao Wu, Yong Peng, Keping Long, Shiduan Cheng, "A simple model of IEEE 802.11 wireless LAN", International Conferences on Info-tech and Info-net, 2001. Proceedings. ICII 2001 - Beijing. 2001 Volume 2, 29 Oct.-1 Nov. 2001 Page(s):514 – 519

[3]. Manshaei M.H., Cantieni G.R., Barakat C., Turletti T, "Performance analysis of the IEEE 802.11 MAC and physical layer protocol", Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. 13-16 June 2005 Page(s):88 - 97

[4]. Yunli Chen, Qing-An Zeng, Dharma P. Agrawal, " Performance analysis and enhancement for IEEE 802.11 MAC protocol", ICT 2003. 10th International Conference on Telecommunications, 2003, Volume 1, 23 Feb.-1 March 2003 Page(s):860 – 867

[5]. Y.Kuo, C. Lu, E.H. Wu, and G. Chen, "An admission control strategy for Differentiated services in IEEE 802.11", IEEE GLOBECOM' 2003, Page(s): 707-712

[6]. Zeng, X., Bagrodia, R., Gerla, M., "GloMoSim: a library for parallel simulation of large – scale wireless networks", PADS 98, Twelfth workshop on Parallel and Distributed Simulation, May 1998 Page(s): 154 – 161