Communication Performance of 802.11 WLANs

Shakil Akhtar
College of Information Technology
UAE University

Abstract
Results from simulation model of an 802.11 WLAN system that suffers in performance due to multiple stations interference are presented. The system communication performance is studied by changing the data packet fragmentation thresholds and the amount of traffic sent, received, and retransmission attempts with and without RTS/CTS mechanism. Two scenarios, with three and five interfering stations have been analyzed and steps to minimize the interference suggested. Specifically, the uses of fragmentation thresholds and RTS/CTS mechanism to control the interference are illustrated via the simulation. It is shown that for the modeled WLAN communications systems, the threshold value should not exceed 1024 bytes causing minimal interference with least number of retransmissions and a higher throughput.

1. Introduction
The popular Physical (PHY) layer and Medium Access Control (MAC) sublayer standard for Wireless LAN (WLAN) is provided by IEEE in form of a family of 802.11 protocols [1]. The MAC sublayer determines the efficiency in sharing the limited communication bandwidth of the wireless channel in WLANs.

The basic access method for 802.11 is the Distributed Coordination Function (DCF), which uses Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA). Since in CSMA/CA, the stations cannot detect the collision there is a possibility of unnecessary bandwidth wastage in case of collision due to completion of transmission by the involved stations. However, the “listen before talk” in CSMA/CA access method used in 802.11 guarantees equal duration of channel access to all devices irrespective of their needs. In other words, when a device with a low bit rate captures the channel, it penalizes other devices using a higher rate by degrading the speed of their connections. For example, when one wireless device connects to a WLAN at a lower bit rate than other devices for being too far from the access point, performance of other network devices degrades.

To combat this problem, a second carrier sense mechanism is available, which enables a station to reserve the medium for a specified period of time through the use of request to send / clear to send (RTS/CTS) frames. In the case described above, far station sends an RTS frame to the AP. The RTS will not be heard by the second station. The RTS frame contains a duration/ID field which specifies the period of time for which the medium is reserved for a subsequent transmission. Upon receipt of the RTS, the AP responds with a CTS frame, which also contains a duration/ID field specifying the period of time for which the medium is reserved. While the nearer station did not detect the RTS, it will detect the CTS and adjusts accordingly to avoid collision even though some nodes are hidden from other stations.

The hidden node and throughput degradation due to large packets lead to two main solutions. First mechanism allows an RTS Threshold (RT) value that determines when the RTS/CTS handshaking mechanism should be used. RTS is a signal sent from the transmitting station to the receiving station requesting permission to transmit. Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem”. Using this mechanism, if the packet size is smaller than the preset RT, the RTS/CTS mechanism will not be enabled. So, when the data size is bigger than RT, the optional RTS/CTS mechanism could be used to prevent a loss of channel bandwidth that could otherwise happen due to excessively large data units.

The second option that could be used effectively with or without RTS/CTS is the fragmentation. The Fragmentation Threshold
(FT) defines the number of bytes used for the fragmentation boundary for directed messages. The purpose of FT is to increase the transfer reliability thru cutting a MAC Service Data Unit (MSDU) into several MAC Protocol Data Units (MPDU) in smaller size. The RF transmission cannot allow transmission of very big frames due to the resulting undesirable heavy interference. Also if the frame size is too small, it will create the overhead during the transmission.

FT is used to limit the size of data packets thus reducing the bandwidth wastage. It is also used to combat the effects of poor channel quality. By reducing the size of the packets transmitted, there is a better probability of successful transmission, especially under poor channel conditions.

The hidden terminals cause performance degradation in WLANs, which can be controlled by using RTS/CTS mechanism as mentioned above. An optimal performance may be obtained by adjusting the RT while monitoring the impact on throughput. The 802.11 standard requires that a station must refrain from sending a data frame until the station completes a RTS/CTS handshake with an AP. Therefore it is important to have an optimal value for RT preventing the station for waiting unnecessarily under low traffic conditions.

The fragmentation option divides the data frames into smaller pieces sent separately to the destination. Each fragment consists of a MAC layer header, FCS (frame check sequence), and a fragment number indicating its position within the frame. With properly set values, fragmentation can reduce the amount of data that needs retransmission since the station only needs to retransmit the fragment containing the bit errors.

Effect on WLAN performance due to several factors, including the effect due to RT and FT has been shown in [2] and [3]. The results show that the performance degradation is severe for fragmentation thresholds above 1000 octets under high error rates (BER = 10^-3 or higher). In a similar work [4], authors suggest thru a model that carefully selecting protocol parameters can help improve the performance even under extreme conditions. Also, it has been shown previously that hidden terminals can have a very detrimental effect on the performance of the MAC protocol. For instance, it was noticed that the performance of protocol drops sharply when the number of hidden pairs exceeds 10 percent of the total number of station pairs [5]. In another work [6], authors present an analysis of the influence of the RT parameter on the wireless network, and give a guideline to dynamically adjust the RT value.

In [7], author suggests WLAN performance improvement via fragmentation. In [8], the method was tested via a simulation model, which shows the WLAN performance results with and without fragmentation. The developed model presents a typical WLAN scenario and shows an effective use of fragmentation threshold in 802.11 for performance enhancement. In this paper the previously presented results are expanded. Two scenarios with three and five interfering stations are considered and the two sets of results compared. The next section provides background information and some of the important WLAN performance issues addressed in this paper. The details of developed models are presented in section 3 followed by a discussion of results and conclusions.

2. WLAN Performance Issues

With higher bandwidths supported by the standards, WLANs are deployed for larger number of users involving applications of email, web browsing and database access. While protocols to support multimedia traffic is still evolving at the application layer, the transport protocol TCP on Internet exhibits reasonable performance. However, the performance improvements in TCP have been suggested for WLAN applications [9]. One of the greatest challenges faced for WLAN is the limitations of the physical layer as evidenced by theoretical models as well as actual measurements [10]. The current highest data rate supported by 802.11a is 54 Mbps for each of twelve (maximum) non-overlapping channels with freedom from most potential RF interference. However, the need for higher data rates and techniques to improve performance is crucial due to many reasons including the rise of multimedia and mpeg traffic in videoconferencing and mobile 3G and 4G applications.

The 802.11 standard consists of family of specifications with major definitions 802.11, 802.11a, 802.11b, 802.11e, and 802.11g. The original standard provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). The 802.11a is an extension to 802.11 providing up to 54 Mbps in the 5GHz band. 802.11a uses an Orthogonal Frequency Division Multiplexing
(OFDM) encoding scheme rather than FHSS or DSSS. The actual available data rates for 802.11a are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps where the support of transmitting and receiving at data rates of 6, 12, and 24 Mbps is mandatory.

The 802.11b (referred to as 802.11 High Rate or Wi-Fi) is also an extension to 802.11 that provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. The 802.11g offers wireless transmission over relatively short distances at 54 Mbps in the 2.4 GHz band. The 802.11g also uses the OFDM encoding scheme. The 802.11e is a relatively new addition to 802.11 family, which is based upon 802.11a and includes Quality of Service (QoS) issues for 802.11 as discussed in [11].

It is noted that WLAN performance suffers severely when operated in a typical office environment (around 200 ft diameter). The degradation in performance is observed due to excessive packet loss and error rates resulting in much lower throughput than expected (see [3] and [4]). Although most of the performance degradation is blamed on radio interference there may be some limitations due to physical and MAC layers of the protocol as well. In general, these factors are modulation techniques and standards, the used hardware, quality of radio signals, processing speed of the stations, environment effects such as path loss and echoes, radio interference, software design, and interfacing with high level protocols.

Some recent analytical models attempt to evaluate the performance of DCF and suggest improvement in the access scheme due to the limitations of the existing scheme. For instance, in [13], the performance of IEEE 802.11 DCF was analyzed considering the size of the initial contention window and its effect on saturation throughput and the energy consumption. In another work [14], the authors provide a new integrated metric to measure both the throughput and the energy consumption and compare the simulation performance results with the original 802.11 protocol. Limitations of DCF are addressed and a new protocol, Wireless Token Ring Protocol (WTRP), is presented and compared with IEEE 802.11 in DCF mode [15]. Since the DCF is based upon contention among stations and is not homogeneous due to the existence of hidden terminals and random behavior, QoS is not provided in the standard. However, WTRP is proposed by the authors as a MAC protocol and is designed to provide QoS in WLANs, in which stations take turn to transmit and are forced to suspend the transmission after having the medium for a specified amount of time.

3. Performance Models

Three station scenario

Consider a three node WLAN based upon 802.11 running at 1 Mbps. Two of the three nodes (nodes A and B), each transmit at an average rate of 80 Kbps with packets of average size 1000 bytes and average interarrival time of 0.1 sec (all following an exponential distribution). The third node acts only as a receiver and does not send any data (see Figure 1). We present the system performance model and study the effect on transmission as node A follows a trajectory as shown in Figure 2, first moving out from node 2’s listening area (thus becoming a hidden node) and then entering back. This study is based upon the simulation of Opnet provided wireless module [16].
It is important to note that in the provided model the simulated nodes generate the traffic at lower layers and the higher layers are replaced by a bursty source and a sink process within the node model. There is MAC interface provided whose operation is independent of the higher layers. Therefore, it may be necessary to develop additional process and node models to characterize the exact behavior of an application. However, since we do not study the effect of application traffic the provided node and process models are used.

The modeled WLAN systems exhibit a “hidden node” problem. Note that the radio coverage of nodes A and B coincide in the beginning of simulation. However, as node A follows a left trajectory and moves out of range from node B, the two nodes become hidden for one another during 350-650 seconds of simulation time. This results in a loss of received signal for both the nodes. In addition, their transmissions become very slow. The effect on transmission is shown in Figure 3 where the two nodes cannot sense each others transmission (received data drops to zero). This causes an increase in their sent traffic, which results in a sudden increase of delay and an excessive number of retransmission attempts. This adverse effect on traffic is noted since the amount of traffic sent is not controlled despite the collision avoidance mechanism is in operation.

We first study the effect of frame fragmentation under a hidden node scenario in the given WLAN. Using fragmentation for large sized packets improves the reliability of data exchange between the stations. We also notice in this study that fragmentation may control the retransmissions and in turn the hidden node problem up to some extent. However, since every data fragment requires an acknowledgement, the overall frame exchange per frame is higher than it would be without fragmentation. Fragmentation may also impact the total channel reservation time per data frame exchange.

The initial results as shown in [8] are obtained for two chosen extreme values of fragment thresholds for frames (2000 bytes and 100 bytes). Note that typical LAN protocols use packets several hundred bytes long (the longest Ethernet packet could be up to 1518 bytes long). There are several reasons why it is preferable to use smaller packets in a WLAN environment. First, due to the higher Bit Error Rate of a radio link, the probability of a packet getting corrupted...
increases with the bigger packets. Second, in case of packet corruption (either due to collision or noise), the smaller the packet, the less overhead it causes to retransmit it. Third, on a Frequency Hopping system, the medium is interrupted periodically for hopping, so the smaller the packet, the smaller is the chance that the transmission will be postponed after some time. The WLAN fragmentation/reassembly mechanism is done at the MAC Layer. Under this mechanism, the transmitting station is not allowed to transmit a new fragment until one of the following happens:

1. Node receives an ACK for the said fragment, or
2. Node decides that the fragment was retransmitted too many times and drops the whole frame.

The station sends the frame called MAC Service Data Unit (MSDU), which can be up to 2 Kbytes unless divided into fragments called MAC Protocol Data Units (MPDUs). The standard specifies a threshold to decide if a MSDU received from the higher layer needs fragmentation before transmission. The number of fragments to be transmitted is calculated based on the MSDU size and the fragmentation threshold. The destination station receives these fragments and stores them in the reassembly buffer until all fragments have been received.

The instantaneous traffic results of Figure 3 shows the reception inactivity by node A during the period it is hidden from node B. Similarly, it can be noticed that the received data by node A is zero during the period it is hidden from node B. The number of retransmission attempts due to unexpected collisions is excessive during the period when nodes are hidden from one another, which clearly illustrates the bottleneck under hidden node conditions (Figure 4). Lower retransmission attempts illustrate that using RTS/CTS mechanism controls the collisions, which is seen dropping to 25 from 65 without the use of RTS/CTS mechanism. Further simulations show that the retransmission attempts are between 70 and 80 without RTS/CTS (for 1000 or higher values of thresholds), and are between 20 and 25 for lower thresholds (about 100 bytes) with RTS/CTS. This obviously favors a smaller threshold value, probably around 256 octets since very low thresholds may cause other performance degradations as mentioned earlier.

**Five station scenario**

Next, consider a five node WLAN based upon 802.11 running at 1 Mbps. Four of the five nodes (A, B, C and D), each transmit at an average rate of 80 Kbps with packets of sizes between 1500 and 2300 bytes following a uniform distribution with an average interarrival time of 0.1 sec following an exponential distribution. The fifth node acts only as a receiver and does not send any data (see Figure 5). We present the system performance model and study the effect on transmission as nodes A, C, and D follow a trajectory as shown. Here A and C first move out from node B’s listening area (thus becoming a hidden node) and then entering back, whereas node D moves out of the listening area of node A and then moves back. Therefore nodes A-D become hidden from either the receiver or from node B for a certain period of time.

This study is based upon the simulation of Omnet provided wireless module [16] and a previous study conducted for three node network [8] as mentioned above.

![Figure 6: Retransmission attempts from node A with and without interference control](image-url)
The modeled WLAN system exhibits a “hidden node” problem. Note that the radio coverage of nodes A to D coincides in the beginning of simulation. However, as mobile nodes A and C follow a trajectory and moves out of range from node B, while node D moves out of range from the receiver simultaneously A-D become hidden during about 6-11 minutes of simulation time. This results in a loss of received signal for the involved nodes. In addition, their transmissions become very slow. The effect on transmission is noticed when nodes cannot sense each others transmission as received data drops to zero. This causes an increase in their retransmission traffic as shown in Figures 6 and 7. This also results in a sudden increase of delay. An adverse effect on traffic is noted since the amount of traffic sent is not controlled despite the collision avoidance mechanism is in operation.

We note that RTS mechanism and fragmentation reduces the packets dropped in the network, in general, under mobility and hidden node conditions. A careful selection of these threshold values can enhance the performance of wireless network. As we can see from Figure 6 that by selecting 1024 as FT and RT the least number of packets are dropped and similarly we note a drop in End-to-End delay as compared to scenario with 2000 as FT and RT. Now by choosing the threshold values below 256 bytes we may increase the load on the receiver (packets received/sec) which in turn increases the end to end delay and thus inversely affecting the performance of the network.

Also, the delay results suggest that FT and RT values of 1024 octets and below provide optimal values causing least End-to-End delays. Comparing the three results (retransmission attempts, dropped data and End-to-End delays) we conclude that FT and RT below 1024 bytes provide an optimal solution for the two simulated scenarios.

4. Conclusions

Simulation results of an 802.11 system with interference control are presented. Three set of results (retransmission attempts, dropped data and delay) are obtained that favors selection of 1024 octets or below for fragmentation threshold under RTS/CTS control mechanism for the selected simulation parameters.

5. Acknowledgements

This research work was supported in part by the Research Affairs at the UAE University under a contract no. 03-03-9-11/05.

6. References


