

Enhancing MAC Performance with a Novel Reverse Direction Protocol for High-Capacity Wireless LANs

Mustafa Özdemir
mozdemir@ece.neu.edu
RWIN-Lab ECE Dept.
Northeastern University
Boston, MA 02115

Daqing Du
dgu@merl.com
Mitsubishi Electric
Research Laboratories
Cambridge, MA 02139

A. Bruce McDonald
mcdonald@ece.neu.edu
RWIN-Lab ECE Dept.
Northeastern University
Boston, MA 02115

Jinyun Zhang
jzhang@merl.com
Mitsubishi Electric
Research Laboratories
Cambridge, MA 02139

Abstract—IEEE 802.11 Wireless Local Area Networks (WLANs) legacy standards can provide up to 54Mbps, and the next generation WLAN will offer a physical-layer speed at least an-order-of-magnitude higher than the existing standards. However, when the current medium access control (MAC) is applied directly to the higher-data-rate WLAN, it leads to high protocol overhead and significant throughput degradation because of its design for lower data rates. Designing efficient MAC schemes becomes critical and crucial. In this paper, we propose a novel reverse direction (RD) protocol to transfer data in both directions, to overcome the fundamental overhead and to improve performance. The aim is to render the MAC efficient and robust not only for current IEEE 802.11a/b/g standards, but also for the next generation WLAN with higher speed and higher throughput, i.e., IEEE 802.11n. Simulations with OPNET are performed and the comprehensive simulation results show that the novel RD protocol provides more efficient, effective and robust performance results.

I. Introduction

The recent proliferation in the deployment of WLANs has been unprecedented. Facilitated largely through widespread broadband Internet access and a robust consumer electronics market, demand for innovative WLAN systems has outpaced industry and standards bodies' ability to support key applications. Presently, 802.11a/b/g Wireless Local Area Networks (WLANs) legacy standards provide adequate performance for today's networking applications where the convenience of a wireless connection can provide the user value. As next-generation wireless applications emerge, higher WLAN data throughput will be required. Key considerations in architecture of the next generation WLANs are costs and robust performance. In addition to different Physical (PHY) technology and wider bandwidth channels, new Medium Access Control (MAC) features maximizing throughput efficiency will be required to reliably satisfy the higher throughput demands of next-generation applications.

IEEE 802.11 MAC utilizes mandatory contention-based channel access function called Distributed Coordination Function (DCF), and an optional centrally controlled channel access function called Point Coordination Function (PCF) [1]. The DCF exploits CSMA/CA with binary exponential backoff. To support the MAC-level QoS, the IEEE 802.11 WG is currently finalizing the standardization of IEEE 802.11e [5]. The upcoming IEEE 802.11e standard provides QoS features

and multimedia support to the current 802.11a/b/g WLAN standards, while supporting full backward compatibility with these standards. To provide better QoS, especially for multimedia applications, improving the WLAN performance is very crucial.

There are two major methods to improve the performance of high capacity WLAN: One is to increase the raw bit rate at the physical (PHY) layer and the other one is to increase the efficiency of the WLAN and reducing the overhead, usually at MAC layer. For instance, the maximal physical layer rates have been increased from 2 Mbps for IEEE 802.11 to first 11 Mbps for 802.11b and then 54 Mbps for 802.11a/g [1], [2], [3], [4]. The main challenge for this high-performance MAC design is how to minimize the protocol overhead. The current 802.11 DCF [1] uses control messages of RTS, CTS, and ACK, contention backoff and various inter-frame spacing parameters, in order for the CSMA/CA-based MAC to function properly. However, these parameters incur high protocol overhead. When the physical-layer rate further increases, the high overhead becomes even more significant since the data-carrying time shrinks as the overhead time remains fixed. It is proved that a theoretical throughput limit exists due to overhead of MAC and PHY [7]. Hence, increasing transmission rate cannot help a lot. As well as pursuing higher data rates, reducing overhead is very essential and necessary for high capacity WLAN. Therefore, the MAC solutions needs to handle the issue of reducing the overhead. The state-of-art MAC solutions are not designed for the high-capacity physical layer. They do not address issues of minimized overhead and maximized MAC throughput simultaneously. For this purpose, the IEEE 802.11n High Throughput Study Group was established emphasizing higher throughput for higher data rates over 100Mbps WLANs in September 2003. IEEE 802.11n will provide both PHY and MAC enhancements with a scope of defining an amendment to IEEE 802.11 standards such a way that it is supporting a maximum throughput of at least 100Mbps, as measured at the MAC data service access point.

In this paper we propose a novel Reverse Direction (RD) protocol, a highly efficient MAC solution for high-capacity WLANs. Hence, the goal of this paper is the same as IEEE 802.11n in terms of focusing on MAC enhancements instead of PHY enhancements. RD protocol primarily targets reduc-

ing overhead at the MAC layer by transferring data in both directions without initiating a new transfer. RD protocol uses two main ideas, aggregation of multiple MAC frames into a single physical frame and transmission of bidirectional frame aggregations. Since acquiring channel access is expensive, in particular in a highly loaded WLAN due to frame collisions, in addition to transmission of aggregates of multiple MAC frames, allowing reverse direction aggregation from the peer MAC entity inside the same channel access is highly desirable and efficient. This way, the turnaround times between MAC entities is minimized while ensuring contention protection within Basic Service Set (BSS).

Extensive simulations show that RD protocol can deliver more efficient data. It also support more robust and effective multimedia applications, compared with the 802.11 MAC without RD protocol solutions.

The rest of the paper is organized as follows. Section II gives an brief overview of IEEE 802.11/11e. Section III illustrates the limitations of current IEEE MAC. Section IV describes the design of RD protocol. Section V evaluates RD protocol via extensive simulations, and section VI compares it with the related work. Section VII concludes the paper.

II. An Overview of IEEE 802.11/11e

We focus on WLANs operating in the contention-based channel access. Contention-based channel access is referred as distributed coordination function (DCF) in IEEE 802.11 and enhanced distributed channel access (EDCA) in IEEE 802.11e. We briefly describe both of them in the following.

A. DCF in IEEE 802.11

DCF works as a "listen-before-talk" scheme based on CSMA/CA where stations listen to the medium to determine when it is free. If a station that has packets to send senses the medium is busy, it will defer its transmission and initiate a backoff counter. The backoff counter is a uniformly distributed random number between 0 and contention window (CW). Once the station detects that the medium has been free for a duration of DCF Interframe Space (DIFS), it starts a backoff procedure, i.e., decrementing its backoff counter as long as the channel is idle. If the backoff counter has reduced to zero and the medium is still free, the station begins to transmit. If the medium becomes busy in the middle of the decrement, the station freezes for a period of time, and resumes the countdown after deferring for a period of time, which is indicated by the so-called network allocation vector (NAV) stored in the winning station's packet header.

It is possible that two or more stations begin to transmit at the same time. In such a case, a collision occurs. Collisions are inferred by no acknowledgement (ACK) from the receiver. After a collision occurs, all the involved stations double their CWs (up to a maximum value, CW_{max}) and compete to gain control of the medium next time. If a station succeeds in channel access (inferred by the reception of ACK), the station resets its contention window CW to CW_{min} .

We can see that DCF does not provide QoS supports since all stations operate with the same channel access parameters and have the same medium access priority. There is no mechanism to differentiate different stations and different traffic.

B. EDC in IEEE 802.11e

In EDCA, the QoS support is realized through introducing multiple access categories (ACs) in each QoS station (QSTA). EDCA defines four ACs, and different ACs have different priorities, servicing different types of traffic. ACs are background, best effort, video or voice kinds of traffic [5]. Each AC is an enhanced variant of DCF that contends for transmission opportunity (TXOP) using AC specified channel access parameters from EDCA parameter set, which includes

- Minimal CW value for a given AC ($CW_{min}[AC]$): CW_{min} can be different for different ACs. Assigning smaller values of CW_{min} to high priority classes can ensure that high priority classes obtain more TXOPs than low priority ones.
- Maximal CW value for a given AC ($CW_{mac}[AC]$): Similar to CW_{min} , CW_{max} is also on a per AC basis.
- Arbitration Interframe Space (AIFS[AC]): Each AC starts its backoff procedure after the channel is idle for a period of AIFS[AC] instead of DIFS. The AIFS[AC] for a given AC should be equal to a short interframe space (SIFS) plus multiple time slots, i.e. $AIFS[AC] = aSIFSTime + AIFSN[AC] * aSlotTime$. Considering $DIFS = aSIFSTime + 2 * aSlotTime$ in legacy 802.11, $AIFSN[AC]$ is typically set to not less than 2 such that the shortest waiting time is DIFS.
- $TXOP_{limit}[AC]$: TXOPs obtained via EDCA are referred as EDCA-TXOPs. During an EDCA-TXOP, a station may be allowed to transmit multiple data frames from the same AC with a SIFS gap between an ACK and the subsequent data frame transmission. $TXOP_{limit}[AC]$ gives the limit for such a consecutive transmission.
- "Virtual Collision": If the backoff counters of two or more co-located ACs in one station elapses at the same time, a scheduler inside the station treats the event as a virtual collision. The TXOP is given to the AC with the highest priority among the "colliding" ACs, and the other colliding ACs defer and try again later as if the collision occurred in the real medium.

III. Limitations of Current IEEE 802.11/11e MAC

We focus on WLANs operation at the ad hoc mode. In the ad hoc mode the key factor that determines efficiency of WLAN is the asynchronous data service, as specified by [1] for the basic 802.11 MAC and showed on Figure 1. In this service, the local MAC sends a MAC service data unit (MSDU) to a peer MAC entity on a best-effort connectionless basis. This local and peer MAC entities are called initiator and responder, respectively. The responder uses immediate positive acknowledgment (ACK), which is sent within the short interframe space (SIFS) interval of the receipt of the MSDU. If no ACK is received, responder schedules a retransmission. As shown in Figure 1, only one data packet is delivered during each channel access. However, the channel access is expensive, in particular in a highly loaded WLAN due to frame collisions. Hence, the data service of the basic MAC is not effective in employing the acquired channel.

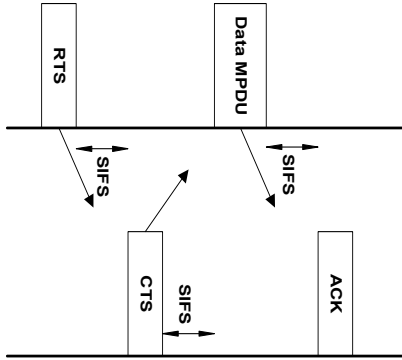


Fig. 1. Asynchronous data service for basic MAC

The IEEE 802.11e standard [5] improves the MAC efficiency by transmitting multiple data frames separated by a SIFS period in a transfer opportunity (TXOP) with only one channel access and in a single direction from initiator to responder. Here initiator and responder can be either station (STA) or access point (AC). The TXOP is an interval of time when a particular station has the right to initiate transmissions onto the wireless medium and is defined by a starting time and a maximum duration. One Block Acknowledgement (BA) for multiple packets is employed. Note however that in one TXOP, the delivered multiple packets are still separated by SIFS interval and the data packets can only flow in one direction. In the RD protocol we further improve the MAC efficiency by eliminating the SIFS period that separates different packets and allow data packets flow in both directions in one TXOP.

IV. Reverse Direction Protocol Design

We hereby propose a new simple reverse direction data exchange scheme in which the bottleneck overhead is reduced sufficiently and the data packets flow is allowed in both direction. RD protocol exploits the existing control frames, Request to Send (RTS) and Clear to Send (CTS), which provide enough capability in order to exchange reverse direction data.

A proposed reverse direction protocol would simply grant any remaining TXOP to the peer upon reception of peer's request if the requested duration is less than the remaining TXOP. Grant is only given when a BA response is expected. Reverse data is always piggybacked with BA. Here the simple heuristic is that initiator grants remaining TXOP when there is no more data to send. Responder only returns data for same AC for the purpose of not violating the existing rules. Responder can request grant inside the Network Allocation Vector (NAV) duration, always less than the TXOP duration. In other words, usage is limited to NAV protection. Moreover, initiator always keeps track of the channel ownership during the transmission. Responder never owns it. This provides simplicity in the implementation by not involving responder into the time scheduler. The responder is allowed to transmit

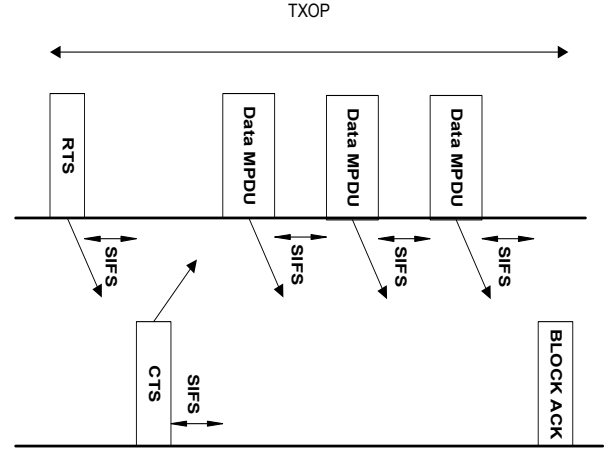


Fig. 2. Improved asynchronous data service in 802.11e

only one PHY protocol data unit (PPDU) so that the return of TXOP to initiator is simplified. In the error case initiator fails to decode the signal field in the responder's transmission and reverts to Clear Channel Assessment (CCA) mechanism in the Physical Layer for avoiding collisions with other transmissions [2]. The initiator always gets the channel back SIFS after the end of energy detection and the TXOP protected with RTS/CTS is then usable by the initiator.

In the light of above discussion, the reverse direction protocol has shaped in the following: Initiator sends RTS which includes NAV duration of TXOP. Upon receipt of RTS, the responder checks if it has any packet to send to initiator. If it has, it determines the duration needed for the reverse direction data transmission. Under the normal conditions CTS from responder must be the duration in RTS minus the sum of CTS and SIFS duration. Here for the reverse direction, responder also subtracts the value of reverse data duration from the received duration in RTS and sends CTS with modified duration to initiator. Initiator checks the duration in CTS if the difference between the duration in RTS and CTS is equal to CTS plus SIFS duration. If it is not equal to, then initiator knows that responder has packet to transmit. If this duration is less than the remaining TXOP, initiator grants use to responder by piggybacking data MPDU or BA Request (BAR) MPDU. This is shown in Fig. 3.

NAV duration in CTS from responder does not reflect the real NAV duration stated in the legacy standard. First of all, it is corrected with the upcoming frames. Secondly, the STAs already received RTS from initiator will not consider this NAV duration from responder because it is smaller than the previous one [1]. This is true only for Basic Service Sets (BSSs). It is better to have smaller unprotected area for overlapping BSSs (OBSSs) in case the frames following CTS is erroneous.

Because of the duration change in CTS, the TXOP is not protected anymore from hidden nodes, located at OBSSs. This problem is eliminated by the following. As seen from Fig. 3, the duration in CTS is always bigger than the critical time. In other words, responder will transmit BA or RD data, which

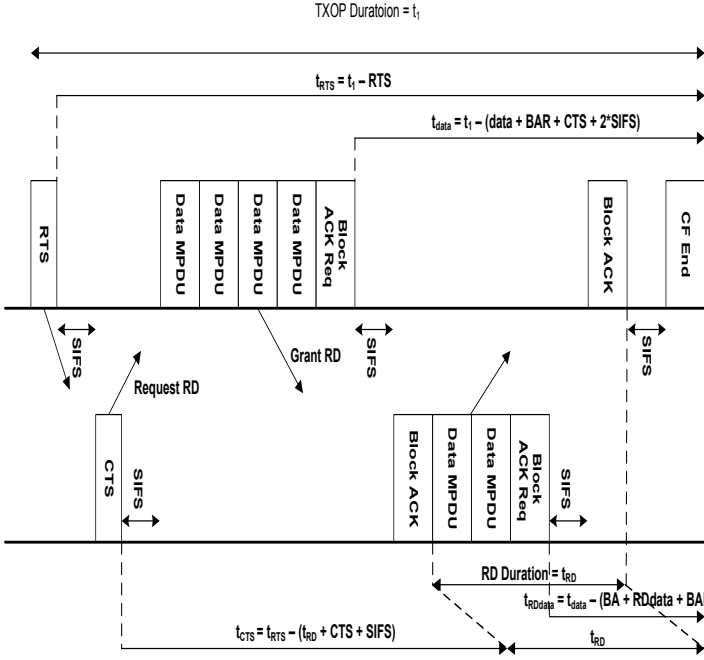


Fig. 3. Asynchronous data service in RD protocol

has updated the duration field, before the unprotected area starts. Hence, the hidden nodes will set up their NAV upon receipt of BA or RD data. If the requested duration is not less than remaining TXOP, then initiator rejects it anyway. However, there is still possibility of unprotected area if next BA or data are not received correctly by hidden nodes. We take out this possibility by reducing the unprotected area in the following mechanism. Responder requests RD duration which is scaled down by "n". Both responder and initiator know what "n" is so initiator can easily calculate exact duration request by multiplying the difference by "n". This apparently reduces unprotected area in case BA or data are not received by hidden nodes. Scaling down the request for RD duration to a value, less than DIFS time, guarantees the protection from hidden nodes.

The Reverse Direction (RD) data duration in CTS is decided upon receipt of RTS from initiator that includes only about the address of initiator but not which AC the TXOP belongs to. Therefore, responder picks one frame for each AC of this initiator from the corresponding queues and calculates the corresponding transmission times and finally adjusts the duration field in CTS according to the maximum among the calculated transmission times. If granted, responder sends the frame matching the present AC to initiator.

If acceptance would be 1-way handshake instead of our 2-way handshake, the responder has to do both preparing BA and figuring out the frames addressed to the initiator in SIFS. From the practical point of view responder can not meet the SIFS budget to do both. Yet, initiator does not know how much the responder will acquire the channel in 1-way handshake so initiator loses track of TXOP. The best

solution to eliminate the SIFS budget problem is to let initiator advertise AC to responder before requesting RD, leading to 3-way handshake. Initiator should advertise AC in addition to duration to responder in RTS. There are 7 unused bits in Frame Control field in RTS so 2 bits of them are used to advertise which AC initiator is acquiring for. In case initiator does not advertise AC in RTS, it is meant that no remaining TXOP is available for responder. Now, responder does not need the SIFS budget.

A. Achieving Adaptability in RD Protocol

When the responder receives RTS, it does not know how much of TXOP the initiator will utilize for the transmission of multiple data burst and BA. If multiple data transmission by initiator is too big, there is less time left for reverse direction. For example, when the traffic is heavy in the system, the stations will transmit more packets in the TXOP time since more packets arrive at MAC until the channel is acquired later than usual. Comparably, less packets will be transferred per TXOP in the light traffic conditions. The question to be answered is how the responder knows the remaining time to exchange the data in the reverse direction.

Each station measures the remaining time for each asynchronous data service per each AC and destination and estimates appropriate number of reverse direction data size dynamically for the next RD data transmission. For this purpose, the following moving average integration technique is adopted to take history measurements into consideration. Note that at the first measurement, the history value is equal to the corresponding measurement.

$$RD(i) = \min\{\lfloor \alpha \times RD(i-1) + (1-\alpha) \times RD_{measured} \rfloor, 64\} \quad (1)$$

where α is a smoothing/aging factor and $RD(i)$ is the number of RD data packets for the i th asynchronous data service and is determined by responder regardless of rejection or acceptance of the request. It can be at most 64 because of the bitmap design in BA control frame. We have only one parameter α that needs to be defined. The predefined value θ used in the simulations is 0.5.

More complex schemes can be designed easily. However, this scheme given here is good enough for our adaptable RD protocol according to simulation results in section V-C.

B. IEEE 802.11 Compatibility

This section presents the changes in IEEE 802.11 frame format for using RD Protocol. All changes are backward compatible with IEEE 802.11. That is, introducing RD-enhanced stations do not affect legacy stations in any way. In particular, all packet format modifications and algorithmic modifications are made in a manner transparent to the legacy stations. Thus, RD-enhanced stations will co-exist with legacy stations. Further, this allows us to "incrementally" deploy RD protocol in an enterprise using WLANs.

How to piggyback for granting use can be done through signaling one bit in data or BAR MPDU. One bit in QoS control field in data MPDU can be used for this purpose. Bit 7 is reserved in IEEE 802.11e standard so it is available or we can create a new QoS data subtype called QoS Data + Request-Accepted (RAD). In the frame control field, if b3b2 is set to

802.11e Parameters	Values
Channel Transmission Rate	54Mbits/sec
TXOP size	0.002 sec.
Data Flow AC	Voice
CW_{min}/CW_{max}	7/31
AIFS[VOICE]	2
retry limit	11

TABLE I
IEEE 802.11E SYSTEM PARAMETER VALUES

10, it is QoS data and 1101 value of b7b6b5b4 is reserved and we can use 1101 for RAD. If we want to use BAR MPDU for granting to responder, the first 12 bits in the BAR control field have been reserved in IEEE 802.11e standard so one of these bits can be used for signaling purposes. Also, there are 7 bits, not used in the frame control field in BAR so at least one of them is accommodated for this signaling purpose [5]. For example "Order" bit can be used for this purpose.

V. Simulation Model and Performance Analysis

This section presents results from discrete event simulation modeling that achieves the following goals: (1) a new adaptable scheme improving RD protocol in terms of adaptability to the dynamic traffic-load conditions; (2) performance analysis of RD protocol in the QoS-enabled station configuration using one QoS traffic class for bidirectional VoIP traffic with and without a TCP traffic as a background traffic. The performance analysis focuses on throughput and packet-loss metrics while varying the number of VoIP stations in the presence and absence of TCP traffic. The experiments include comparison of RD protocol turned on and off on the station given everything else is same.

A. Simulation Parameters

The discrete-event simulation engine OPNET provided the tools to build an effective model of RD protocol for performance analysis. All simulation results reflect statistically significant analysis based on a 95% confidence level and relative precision of 0.05. The important system parameter values are given in table-I. The others can be found in the IEEE 802.11 MAC layer implementation in [5]. System parameters were chosen to reflect typical installations of IEEE 802.11g. 10 simulation runs are performed to show performance benefit of RD protocol for the support of VoIP traffic.

The traffic parameters were selected to model the behavior of the G.711 codec using 10ms packetization intervals for VoIP. All traffic sessions assumed a wired AP, hence, traffic was not generated between wireless nodes. The simulation scenarios include one AP and a ring of VoIP and TCP stations around it. The radius of the ring is 10 meters. Based on the G.711 specification the raw packet lengths for voice were fixed at 92 bytes. However, Table II indicates the overhead required by the underlying protocol layers: RTP, UTP, IP and MAC; the aggregate frame lengths came to 190 bytes (significant protocol overhead). Each VoIP session was held for 2 minutes, consisting of bidirectional traffic from the wireless client. The background load was kept fixed at 10Mbps of TCP traffic. TCP Data traffic was generated by AP towards 10 stations which downloads local files from AP sending fixed 1424 byte frames at a mean interarrival rate of 10 ms. The aggregate data load

VoIP Traffic Parameters	Values
Packet Interarrival time	10ms
Voice packet length	92 bytes
RTP layer overhead	12 bytes
UDP layer overhead	8 bytes
IP layer overhead	20 bytes
MAC layer overhead	34 bytes
PHY layer overhead	24 bytes

TABLE II
VOICE TRAFFIC PARAMETERS

was set at 10 Mbps for fixed number of VoIP stations. The number of voice stations was varied from 10 to 40.

B. Performance Metrics

The two most important metrics reflecting the delivered QoS for VoIP are packet-loss and end-to-end delay. Packet loss may result from any of the following: (1) buffer overrun, (2) excessive MAC-layer collisions or (3) channel interference. Delay may be incurred in numerous ways; here we consider queuing delay at the source station and MAC delay incurred by the frame in service at the source station. Studies have shown that for acceptable voice quality VoIP can tolerate 200 ms delays with as much as 5% packet loss. In simulation scenarios the tolerable MAC delay between stations and AP is 30 ms. If a VoIP frame arrives at a peer MAC from other MAC more than 30 ms, it is included in a new metric, total packet-loss. In other words, the new metric, total packet-loss, reflects all measures for the performance analysis of a QoS application. Note that packet loss is represented as a percentage according to the following equation:

$$PL = 100 \cdot \left(1 - \frac{Pkts_{rcvd}}{Pkts_{sent}}\right) \quad (2)$$

where the fraction shows the ratio of received packets to the total number of packets generated by the source. The total packet loss is also represented as a percentage as follows:

$$TotalPL = 100 \cdot \left(1 - \frac{Pkts_{rcvd}}{Pkts_{sent}} + \frac{Pkts_{too-late}}{Pkts_{sent}}\right) \quad (3)$$

where the second fraction is for the ration of too-late (more than 30 ms) packets to the total number of packets sent by the source.

C. Simulation Results

We conduct extensive simulations to study different parameters such as throughput, packet loss and total packet loss considering MAC delay, and effects of traffic load on performance metrics with and without the RD protocol. There are two different data flows in the simulations. The down flow is from AP to the stations, whereas the up flow is vice versa. The number of down flow from AP is the number of stations in the system and same for the number of up flow.

Figure-4 shows average packet-loss and too-late packets metrics in percentage per VoIP flow for down and up flows versus the number of VoIP clients in the system. As seen from the figure, the QoS performance metrics for up and down flows has been greatly improved when adaptive RD protocol is turned on the station except for the too-late packets metric for up flows. Note the asymmetric difference between up and down flows for both metrics when adaptive RD protocol is not used. With RD protocol this asymmetry greatly reduces, especially,

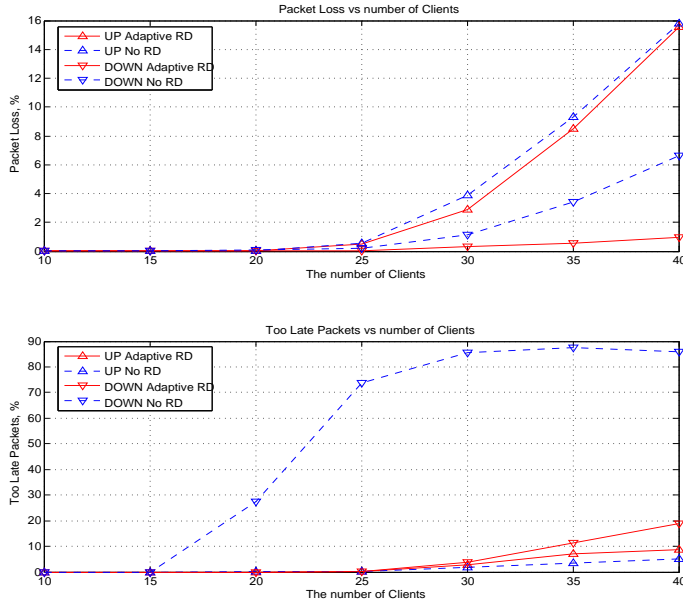


Fig. 4. Average QoS performance metrics of up and down VoIP flows in percentage versus the number of VoIP client stations (a) for packet-loss (b) for too-late packets

for too-late packets. Since bidirectional flows are required in VoIP applications, RD protocol significantly enhance the VoIP performance.

Figure-5 depicts the mean total packet loss in percentage which is determined by taking average for both up and down VoIP flows and the total throughput in Mbps. Adaptive RD protocol allows increasing number of supported VoIP client by approximately 75% from 17 to 30 and also improving QoS metric values. The another observation is that the more the system is congested, the more throughput RD provides.

Results given heavy background TCP traffic of 10Mbps are shown in Figure-6. Heavy TCP traffic does not have any affect on the packet-loss performance of RD protocol, whereas it terribly increases the asymmetric quality of up and down flows in case no RD protocol is turned on in stations. This asymmetry is even worse for the too-late packets metric. On the other hand, up and down flows has almost same too-late packets performance with adaptive RD protocol.

The mean total packet-loss metric and the total throughput is illustrated in Figure-7 in case 10 Mbps TCP traffic is used. The system with the adaptive RD protocol now tolerates 22 VoIP clients while it allows only 11 VoIP clients without RD protocol. RD protocol provides 100% increase for VoIP applications. The total throughput shows very interesting result. In case no RD is used, after 20 clients, the system goes into congestion and the TCP traffic starts to go down. That is why there is a break for the results in which no RD protocol is used. Moreover, the TCP traffic does not reduce its traffic rate from TCP layer even until 40 VoIP clients are served in the system. In other words, the congestion for TCP traffic reaches much earlier for no RD protocol used than for RD protocol used.

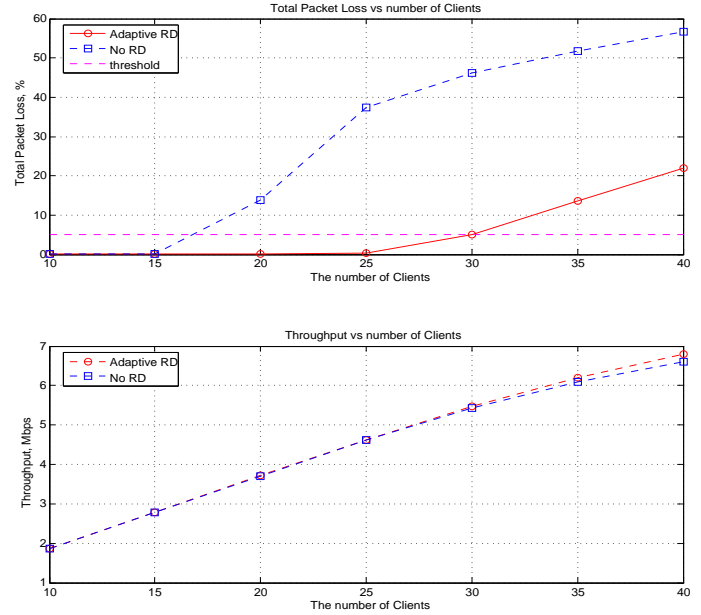


Fig. 5. (a) The mean total packet loss for VoIP flows in percentage (b) The throughput for all flows in Mbps versus the number of clients

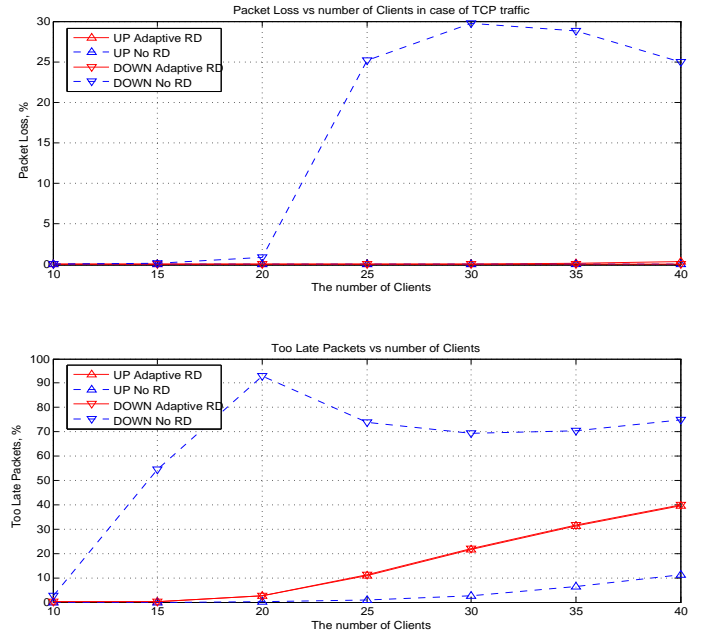


Fig. 6. Average QoS performance metrics of up and down VoIP flows in percentage versus the number of VoIP client stations in case 10 Mbps TCP traffic is used (a) for packet-loss (b) for too-late packets

VI. Related Work

Liu et al [6] provides a simple analytic model for computing the capacity of an infrastructure IEEE 802.11 WLAN enhanced with the support of the bidirectional MAC frame aggregation. However, it does not give any detail how to succeed the bidirectional frame aggregation. The simulation scenarios are performed for the validation purposes. There is no simulation for any QoS applications.

Xiao et al [7] proves that a theoretical throughput upper

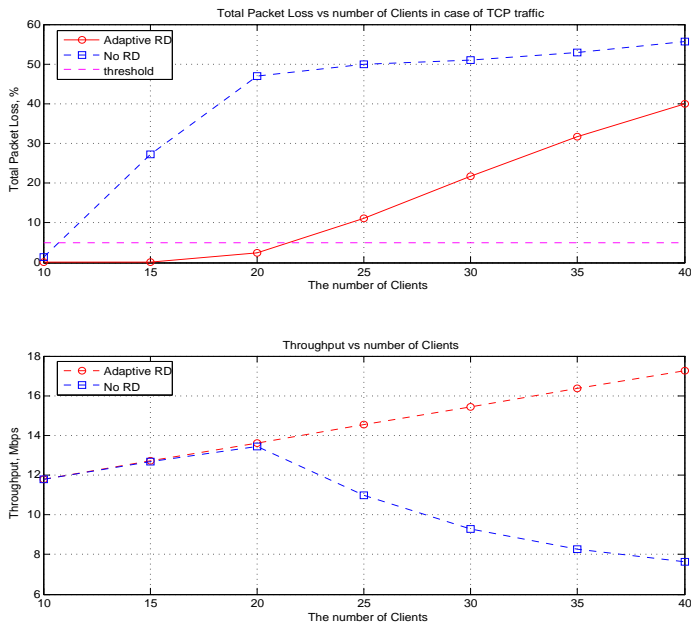


Fig. 7. in case 10 Mbps TCP traffic as a background traffic (a) The mean total packet loss for VoIP flows in percentage (b) The throughput for all flows in Mbps versus the number of clients

limit and a theoretical delay lower limit exist for IEEE 802.11 protocols. They show that by simply increasing the data rate without reducing overhead, the enhanced throughput is limited and bounded, even when the data rate becomes infinitely high. In order to reduce overhead, they proposed and studied a burst transmission and acknowledgement mechanism. They do not use any bidirectional frame aggregation mechanism to further reduce the overhead.

VII. Conclusions

We have presented and studied the RD protocol in order to provide the bidirectional MAC frame aggregation. RD protocol enhances the performance of IEEE 802.11e EDCA. In particular, it fits well to TCP by allowing a TCP link to piggyback TCP ack collection onto TCP data transmission. Also, RD protocol specifically suits the QoS applications having the bidirectional flows even if it is not TCP traffic. Furthermore, RD protocol adapts to the traffic conditions by measuring the remaining reverse size for each asynchronous data service. The extensive simulation results show that RD protocol greatly improves not only the capacity of the infrastructure 802.11 WLAN but also the quality of VoIP clients with or without the background traffic.

References

- [1] IEEE Standards Board, *Ieee standard 802.11 - wireless lan medium access control (mac) and physical layer (phy) specifications*, IEEE, 345 East 47th Street, New York, NY 10017-2394, USA, June 1997.
- [2] IEEE, *Ieee standard 802.11a - wireless lan medium access control (mac) and physical layer (phy) specifications: High-speed physical layer in the 5 ghz band*, September 1999.
- [3] IEEE, *Ieee standard 802.11b - wireless lan medium access control (mac) and physical layer (phy) specifications high-speed physical layer extension in the 2.4 ghz band*, September 1999.

- [4] IEEE, *Ieee standard 802.11g - wireless lan medium access control (mac) and physical layer (phy) specifications: Further higher-speed physical layer in the 2.4 ghz band*, April 2003.
- [5] IEEE, *Ieee standard 802.11e/d13.0 - wireless lan medium access control (mac) and physical layer (phy) specifications: Medium access control (mac) enhancements for quality of service (qos)*, January 2005.
- [6] Changwen Liu and Adrian P. Stephens, *An analytic model for infrastructure wlan capacity with bidirectional frame aggregation*, WCNC, 2005, pp. pp. 113–119.
- [7] Y. Xiao and J. Rosdahl, *Performance analysis and enhancement for the current and future ieee 802.11 mac protocols*, ACM SIGMOBILE Mobile Computing and Communications Review (MC2R), special issue on Wireless Home Networks vol. 7 (2003), no. 2, pp. 6–19.