

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

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

Daqing Gu
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 data rate 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, a novel reverse direction (RD) protocol is proposed 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 data rate and higher throughput, i.e., upcoming IEEE 802.11n. Simulations with OPNET are performed and the comprehensive simulation results show that the novel RD protocol improves performance significantly.

I. Introduction

The rapid growth of wireless communication technologies has pushed the standardization of corresponding protocols. As new wireless applications emerge, higher Wireless LAN (WLAN) throughput is required. Key issues for next generation WLANs include cost and robust performance. In addition to different Physical (PHY) technology and wider bandwidth channels, new Medium Access Control (MAC) features maximizing throughput efficiency are required to reliably satisfy the demands of emerging applications.

A series of protocols for WLANs have been proposed and standardized under the IEEE 802.11 family. Among them, 802.11 was the first standard developed for medium access control layer (MAC) and physical layer (PHY) specification. The 802.11 working group (WG) has continued to issue extensions and amendments to the standard. The letters "a" through "n" have been officially designated to task groups (TGs) within the 802.11 WG. The state-of-art MAC solutions were not designed for the high-capacity physical layers. They fail to minimize overhead, thus limiting MAC throughput. As such, the IEEE 802.11n TG has been established to develop a new standard, IEEE 802.11n, intended to support MAC throughput of 100 Mbps using PHY-layer and MAC-layer enhancements.

The IEEE 802.11 MAC utilizes a contention-based channel access function called the Distributed Coordination Function

(DCF). There is an optional centrally controlled access function called the Point Coordination Function (PCF) [1]. The DCF exploits CSMA/CA with binary exponential backoff. To support MAC-level Quality of Service (QoS), the IEEE 802.11 WG is finalizing the standardization of IEEE 802.11e [6]. The upcoming IEEE 802.11e standard provides limited QoS support to the current 802.11a/b/g WLAN standards. However, improved MAC throughput is essential for broad support of real-time applications.

There are two major methods for improving the performance of a WLAN: One is to increase the raw bit rate at the physical (PHY) layer and the other one is to reduce MAC overhead. Physical layer rates have increased from 2 Mbps in IEEE 802.11 to 11 Mbps in 802.11b and 54 Mbps for 802.11a/g [1], [3], [4], [5]. However, data throughput at the MAC layer has not kept pace. For example, in order to support adaptive rate control and provide backward compatibility, the maximum possible throughput decreases in proportion to the increase in PHY-layer bit rate. Let t_d be then time to transmit a MAC-layer protocol data unit (MPDU) and t_{oh} the aggregate time required by the MAC-layer to acquire the channel (MAC overhead). If the raw bit rate at the physical (PHY) layer increases by a factor of k , then the time to transmit an MPDU will decrease to t_d/k , whereas the time required for MAC overhead remains fixed. Consequently, MAC-layer throughput increases, however at a decreasing rate with respect to the raw bit-rate. Assuming steady-state average values, then the original throughput will be bounded by: $t_d/(t_d + t_{oh})$. The new throughput will be bounded by: $t_d/(t_d + k \times t_{oh})$. Hence, it can be seen that the main challenge for high-performance WLAN design is the minimization of MAC protocol overhead.

This paper presents a novel solution for reducing MAC control overhead and idle periods to increase the capacity of high speed wireless LANs (WLANs). The Reverse Direction (RD) protocol represents an enhancement to existing IEEE 802.11 MAC protocol standards. Both the upcoming standard IEEE 802.11n and the RD protocol focus on MAC enhancement. RD protocol primarily targets overhead reduction at the MAC layer through two components. Most importantly is the support of fast bidirectional communication that avoids secondary handshaking, extra control frames and forced idle intervals. Secondly, RD protocol utilizes frame aggregation with more efficient mechanisms than existing standards.

The fundamental tenet of the RD protocol is based on the philosophy that channel acquisition is very costly. Moreover, the cost becomes proportionally greater as channel rates and load increase: both of which are desirable characteristics. RD reduces control overhead, idle intervals and collisions, thus improving turnaround times and ensuring contention protection within a Basic Service Sets (BSSs). Simulation results show that the RD protocol delivers higher data throughput at the MAC layer. It also supports more robust QoS control for multimedia applications than solutions without RD protocol.

Liu et al [7] 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 exchange. However, it does not give any detail how to succeed the bidirectional frame exchange. The simulation scenarios are performed for the validation purposes. There are no simulation results for QoS applications. Xiao et al [8] proves that a theoretical upper limit on throughput and a lower limit for delay exist for current IEEE 802.11 protocols. They show that by increasing the data rate without reducing MAC overhead bounds the potential increase in throughput. This result holds for infinitely high data rates. In order to reduce overhead they investigate a burst transmission/acknowledgement mechanism. They do not use any bidirectional frame aggregation mechanism to further reduce the overhead.

The remainder of this paper is organized as follows: An overview of IEEE 802.11/11e is presented in Section II. The limitations of current IEEE WLAN MACs are discussed in Section III. The design of RD protocol is described in Section IV, and performance is evaluated in Section V using discrete-event simulation. Finally, Section VI presents the conclusions and future work.

II. An Overview of IEEE 802.11/11e

The 802.11 MAC DCF is based on CSMA/CA in which stations with MPDUs ready to transmit first determine the state of medium as busy or idle. If a station senses the medium as busy it defers its transmission attempt by setting a backoff counter that only decrements after the medium is sensed idle for the DCF Interframe Space (DIFS). It continues to decrement as long as the medium remains idle, deferring its count-down during busy periods. The backoff counter is a uniformly distributed random number between 0 and contention window (CW). When the backoff counter reaches zero the station begins to transmit.

It is possible for multiple stations to begin transmissions at the same time, resulting in a collision. Collisions occur at the receiver, hence they must be inferred if a sender fails to receive a valid acknowledgement (ACK) from the receiver within a bounded time. All senders detecting a collision double their CWs (up to a maximum value, CW_{max}), and repeat the backoff algorithm. Reception of an ACK infers the channel access and MPDU transmission were successful, hence the station resets its contention window CW to CW_{min} and waits for its next MPDU.

The DCF cannot provide any QoS support. It was designed to provide fair and equal access to the transmission medium for all stations by operating with the same channel access para-

eters. IEEE 802.11e introduces a new channel access mechanism called Enhanced Distributed Channel Access (EDCA), which invokes a access category (AC) based priority system to provide better MAC service for QoS applications. EDCA manages priority access by assigning one of four ACs to each QoS station (QSTA): background, best-effort, video or voice [6]. Each AC is an enhanced variant of DCF that contends for transmission opportunity (TXOP),

using AC specified by the following channel access parameters:

- $CW_{min}[AC]$: The minimum CW value for a given AC. Smaller values of CW_{min} allows the backoff counter to decrement more rapidly (on average), thus providing higher access priority.
- $CW_{max}[AC]$: The maximum CW value for a given AC. Smaller values of CW_{max} bounds the maximum backoff counter value, thus generally reducing the backoff time. However, under congested conditions the likelihood of multiple collision may increase.
- $AIFS[AC]$: The Arbitration Interframe Space permits each AC to specify its own waiting time before backoff instead of DIFS. The $AIFS[AC]$ for a given AC should be equal to a short interframe space (SIFS) plus multiple time slots. In legacy systems $DIFS = SIFS + 2 * aSlotTime$. Consider the parameter $AIFSN[AC]$, which is typically set ≥ 2 , such that the shortest waiting time is DIFS. Finally, $AIFS[AC] = SIFS + AIFSN[AC] * aSlotTime$.
- $TXOP_{limit}[AC]$: TXOPs obtained via EDCA are referred as EDCA-TXOPs. During an EDCA-TXOP a station is allowed to transmit multiple data frames from the same AC with an SIFS gap between each MPDU in a data burst. The value of $TXOP_{limit}[AC]$ bounds the time allowed for multiple transmissions for each AC.
- "Virtual Collision": If the backoff counters for multiple ACs in the same station elapse at the same time, the event is treated 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 IEEE 802.11/11e MAC

The key factor that determines efficiency of WLAN is the asynchronous data service, as specified by [1] for the basic 802.11 MAC and shown in Figure 1. In this service, the local MAC sends an MPDU to a peer MAC entity on a best-effort connectionless basis. The local and peer MAC entities are called the initiator and the responder, respectively. The responder uses immediate positive acknowledgment (ACK), which is sent following a short inter-frame space (SIFS) after receiving a correct MSDU. If the initiator fails to receive its ACK it initiates backoff prior to retransmission. As shown in Figure 1 only one data packet is delivered during each channel access. Hence, the data service of the basic MAC becomes inefficient in its use of the acquired channel.

The IEEE 802.11e standard [6] improves MAC efficiency by permitting multiple MPDU transmissions separated by SIFS within a transfer opportunity (TXOP) during one channel

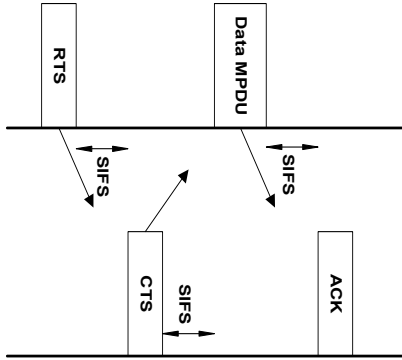


Fig. 1. Asynchronous data service for basic MAC

access from initiator to responder. This is illustrated in Figure 2, where the initiator or responder may be either a station (STA) or an access point (AP). The TXOP is an interval of time when an initiator station has the right to transmit MPDUs, and is defined by a starting time and a maximum duration. A Block Acknowledgement (BA) is used to cover all sent frames. The separation of MPDUs by SIFS decreases efficiency and could increase the probability of a collision. Moreover, the limitation of traffic flow to a single direction fails to leverage the important property that a responder frequently has return data to send, e.g. TCP and voice applications. The RD protocol improves MAC-layer efficiency by eliminating the inter-frame SIFS and enabling bi-directional data flow during a single TXOP without additional channel access overhead.

IV. Reverse Direction Protocol Design

An efficient reverse direction (RD) data exchange protocol is proposed to improve QoS support and overall efficiency of the emerging standard IEEE 802.11n for high rate physical layers. The RD protocol provides mechanisms that significantly reduce the MAC-overhead while retaining full compatibility with legacy systems. RD achieves these results by supporting "on-demand" bi-directional data flow using the existing two-way RTS/CTS handshake without any additional control frames. Furthermore, it reduces block transmission overhead by eliminating the interframe SIFS for transmission in both directions and relies on a single block acknowledgement frame. Finally, by engaging in bi-directional data flow that is under the complete control of the flow initiator it increases the robustness and processing efficiency of the protocol.

The RD protocol enables the node that accesses the channel using RTS/CTS (initiator) to allocate any remaining time in TXOP[AC] (grant) to its peer for reverse data flow upon request if the requested duration is less than the time remaining in TXOP[AC]. Reverse data flow is piggybacked with a block acknowledgement (BA). The initiator grants remaining TXOP when there is no more forward data to send. A grant only permits the responder to return data within the same AC

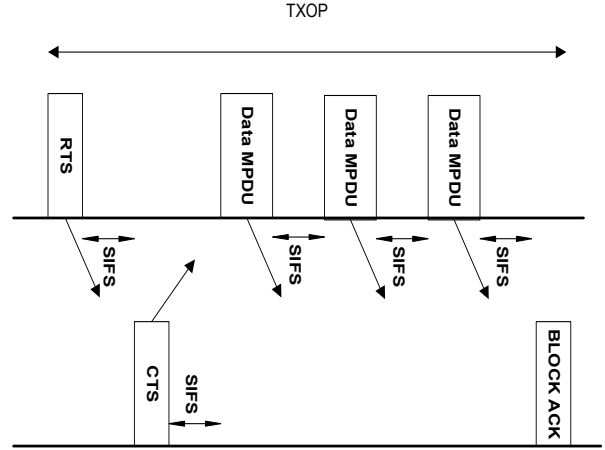


Fig. 2. Improved asynchronous data service in 802.11e

destined for the initiator, thus preserving EDCA semantics. A responder can request a grant inside the Network Allocation Vector (NAV) duration that must be less than TXOP[AC] duration. Thus, starvation is prevented using through NAV protection. Moreover, the initiator is responsible for channel ownership, the responder never owns it. This has the advantage of simplifying implementation and increases protocol robustness because the responder is not involved in timer management and scheduling.

Channel control is simplified and backward compatible because the responder is limited to a single PHY-layer PDU (PPDU), which consists of a block ACK (BA), one or more MPDUs and a block ACK request. Should an error occur leaving the initiator unable to correctly decode the signal field of the responder's transmission it reverts to the Clear Channel Assessment (CCA) mechanism at the Physical Layer to avoid collisions with other transmissions [3]. The initiator always retains the channel SIFS after the end of energy detection and the remaining TXOP[AC] protected with RTS/CTS becomes available for additional transmissions by the initiator.

RD protocol functionality can be summarized as follows: The initiator sends an RTS which includes the NAV duration of TXOP[AC]. Upon receiving the RTS the responder checks if it has any data of the same AC ready to send to the initiator. If it does then it must determine the duration needed for the reverse direction transmission. Under the unidirectional conditions the CTS is the duration value in the corresponding RTS minus the sum of CTS and SIFS. However, for reverse direction transmission the value in CTS is set equal to the the duration value in the corresponding RTS minus the actual reverse data duration. The initiator checks the duration in CTS. If the difference between the duration in RTS and CTS is not equal to CTS plus SIFS, then a grant is being requested. Assuming the duration is less than the remaining TXOP[AC] the initiator grants reverse time to the responder by piggybacking the grant of a data MPDU or Block ACK Request (BAR) MPDU. Fig. 3 illustrates this procedure.

In the RD protocol the NAV duration in a responder's CTS

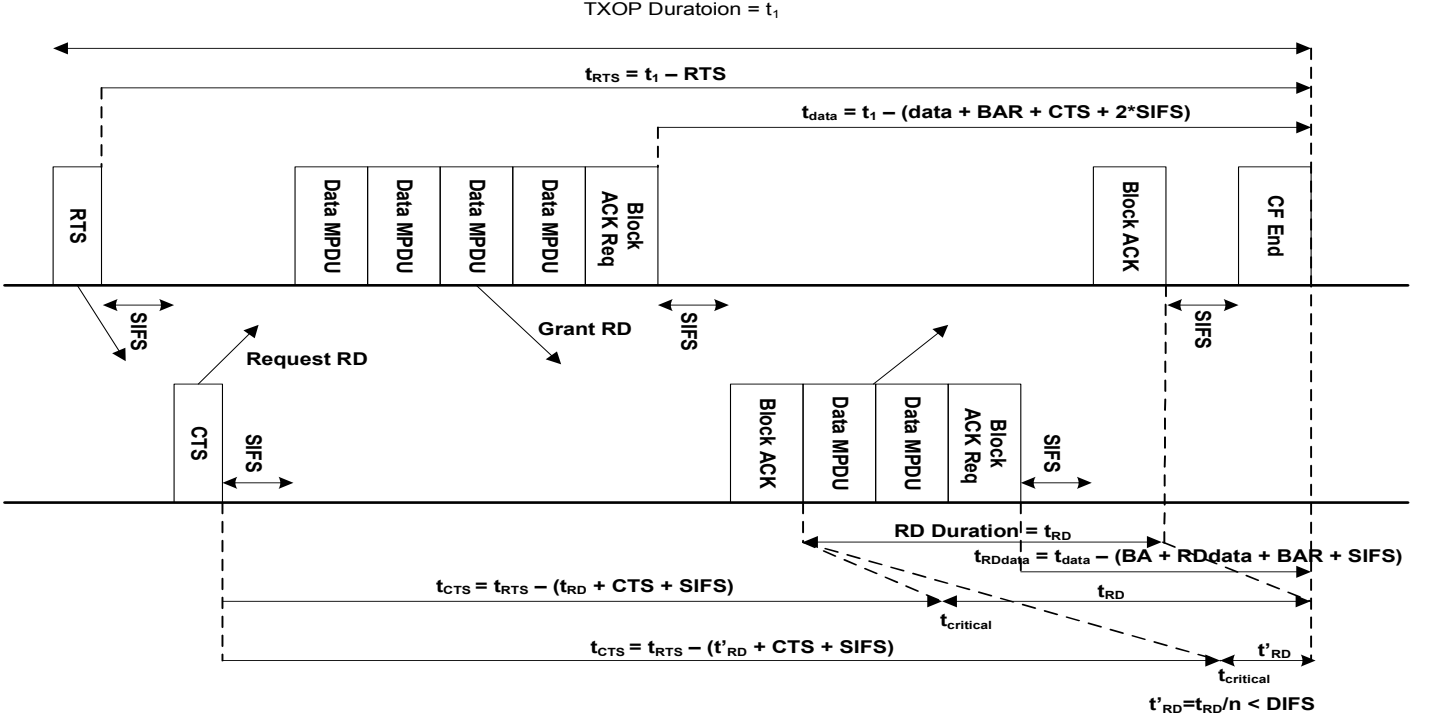


Fig. 3. Asynchronous data service in RD protocol

does not reflect the semantic NAV of the legacy standard. The CTS-NAV is modified according to the transmission time of reverse frames. Any STAs that have received the associated RTS do not alter their NAVs since the new NAV will have a smaller value [1]. This is a robust scheme within a single Basic Service Set (BSS). Overlapping BSSs (OBSSs) are not fully protected, hence it is better to have smaller unprotected area for OBSSs in case the frames following CTS is erroneous.

Hidden nodes are also potential problem areas. If the CTS reports a Duration change, the TXOP[AC] is not protected for those hidden nodes in an OBSS. This problem is addressed as follows: As shown in Fig. 3, the duration in CTS is always larger than the critical time. Hence, the responder transmits BA or RD data, which has updated the duration field, before the unprotected area starts. Therefore, the hidden nodes will set up their NAV upon receipt of the BA or RD data. If the requested duration is not less than remaining TXOP[AC], then initiator will reject it anyway. However, the possibility remains for an unprotected area if the next BA or data are received incorrectly by hidden nodes. Any problem associated with this outcome is eliminated as follows: the responder requests RD duration which is scaled down by "n". Both responder and initiator know what "n" is so the initiator computes the exact duration request by multiplying the difference by "n". This reduces the unprotected area in the event that a 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 RD data duration in CTS is decided upon receipt of RTS, which includes the address of initiator but not which AC the TXOP belongs to. Here it is assumed that each AC has

different TXOP duration ($TXOP_{limit}[AC]$). The responder infers the AC based on knowledge of the $TXOP_{limit}[AC]$ values. It selects waiting frames associated with the AC of the initiator from the corresponding queues and calculates the corresponding transmission times and finally adjusts the duration field in CTS according to the calculated transmission times. The number of frames is determined according to an adaptive scheme discussed in subsection IV-A. If granted, responder sends the corresponding frames to initiator.

If acceptance were based on a 1-way handshake versus the 2-way handshake, the responder would be required to prepare BA and determine the frames addressed to the initiator in SIFS. For high rate WLANs it is unlikely that a responder would consistently accomplish these tasks within the SIFS time budget. If the responder does not modify the duration in its CTS the initiator has no way know how much channel time is required for reverse data, hence the initiator will lose track of TXOP.

A. Achieving Adaptability in RD Protocol

On receiving an RTS the responder does not know how much of TXOP the initiator will use for the transmission of multiple data bursts and BA. If the duration of data transmission by initiator is too large, less time remains for reverse direction. For example, when the traffic load is heavy in a system, it will tend to transmit more frames in the TXOP time than under lighter load condition. This raises the question of how the responder knows the remaining time that will be available to exchange reverse direction data?

The only feasible distributed approach requires an adaptive scheme to estimate the available time. Each responder measures the remaining time for asynchronous data service per

802.11e Parameters	Values
Channel Transmission Rate	54Mbps/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

AC and destination and estimates a weighted time average for reverse direction transmission. To incorporate traffic dynamics, an exponential smoothing average is computed that weighs the most recent measurement with the average of all previous estimates

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

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. There is only one parameter α that needs to be defined. The value of α should reflect variance, however an adaptive scheme was not investigated in the present work. A fixed value of 0.5 was used in the simulation experiments, which reflects an equal weighting to history and the most recent observation.

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 a new QoS data subtype called QoS Data + Request-Accepted (RAD) can be defined. In the frame control field, if $b3b2$ is set to 10, it is QoS data and 1101 value of $b7b6b5b4$ is reserved and 1101 can be used for RAD. If BAR MPDU is to be used 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 [6]. 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

VoIP Traffic Parameters	Values
Packet Interarrival time	10ms
Voice packet length	80 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

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 the performance with and without RD protocol.

A. Simulation Parameters

The discrete-event simulation engine OPNET provides 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 [6]. System parameters were chosen to reflect typical installations of IEEE 802.11g. 10 simulation runs were 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. The raw packet lengths for voice were fixed at 80 bytes. However, Table II indicates the overhead required by the underlying protocol layers: RTP, UTP, IP and MAC; the aggregate frame lengths came to 178 bytes. Each VoIP session was held for 2 minutes, consisting of bidirectional traffic from the wireless clients to AP and vice versa. TCP Data traffic was generated by AP towards 10 stations which downloads local files from AP. AP sends fixed 1460 byte frames at a mean interarrival rate of 11.68 ms, causing 1 Mbps TCP traffic per client. The aggregate background data load 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 queuing delay at the source station and MAC delay incurred by the frame in service at the source station is considered. Studies have shown that for acceptable voice quality VoIP can tolerate 200 ms delays with as much as 5% packet loss [2]. 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

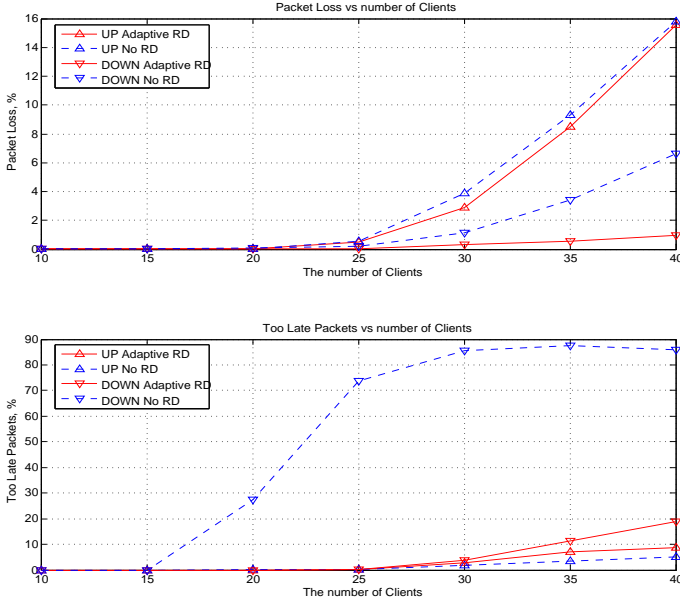


Fig. 4. Average QoS performance metrics of up and down VoIP flows in percentage versus the number of VoIP client stations (a) for packet-loss (b) for too-late packets

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

Extensive simulations are conducted 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 flows from AP is the number of stations in the system and the same as the number of up flows.

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.

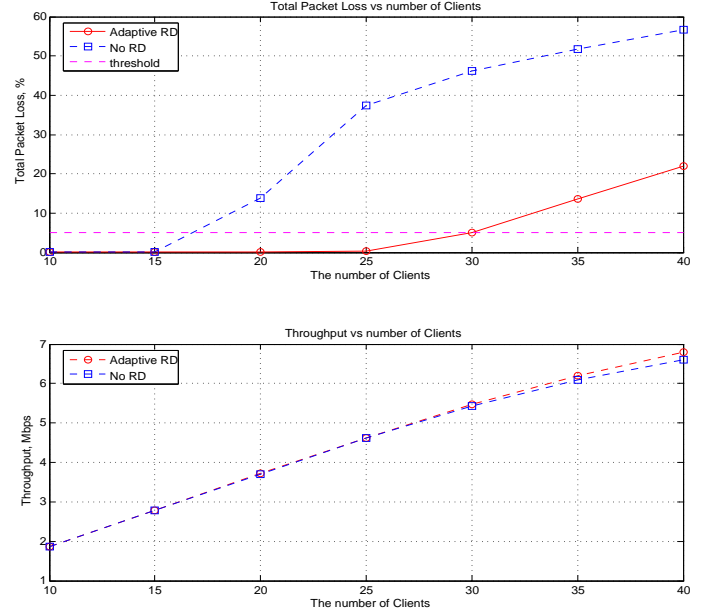


Fig. 5. (a) The mean total packet loss for VoIP flows in percentage (b) The throughput for all flows in Mbps versus the number of clients

With RD protocol this asymmetry greatly reduces, especially, 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 impact 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.

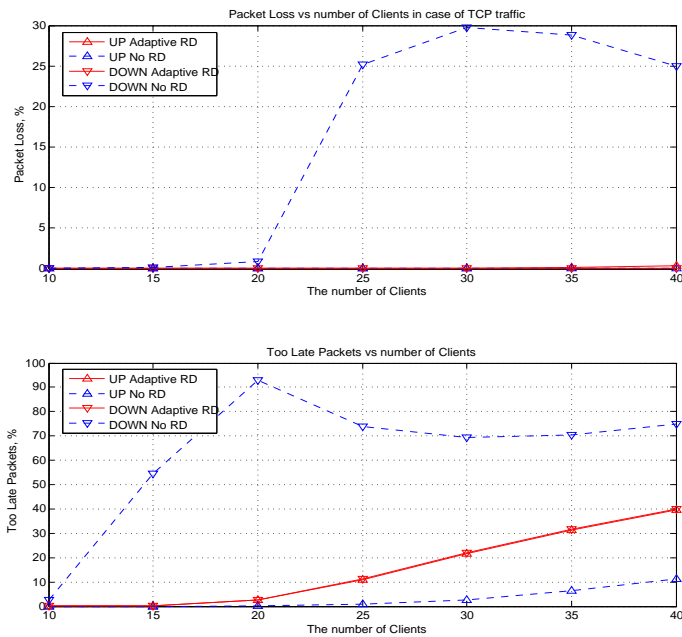


Fig. 6. Average QoS performance metrics of up and down VoIP flows in percentage versus the number of VoIP client stations in case 10 Mbps TCP traffic is used (a) for packet-loss (b) for too-late packets

VI. Conclusions

The RD protocol is presented and studied 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 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] ETSI, *General aspects of quality of service (qos),dtr/tiphon-05001 v1.2.5 technical report*, September 1998.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] Changwen Liu and Adrian P. Stephens, *An analytic model for infrastructure wlan capacity with bidirectional frame aggregation*, WCNC, 2005, pp. pp. 113–119.
- [8] Y. Xiao and J. Rosdahl, *Performance analysis and enhancement for the current and future ieee 802.11 mac protocols*, ACM SIGMOBILE

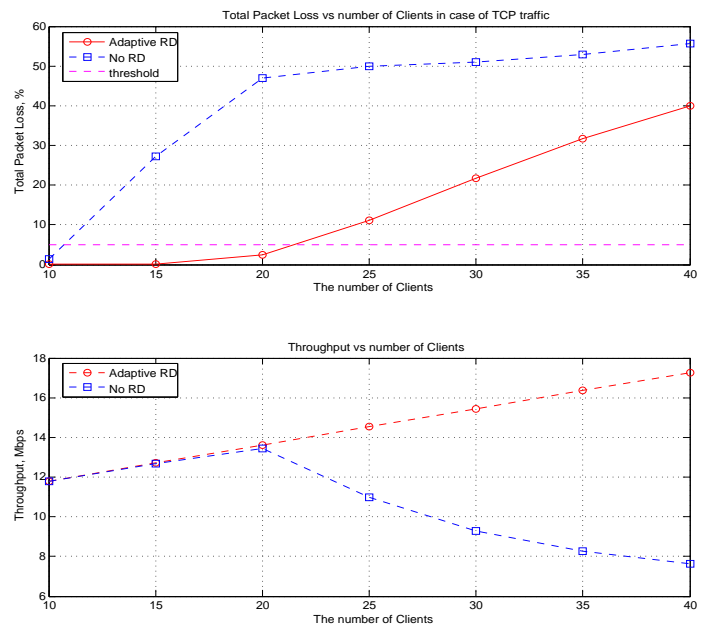


Fig. 7. in case 10 Mbps TCP traffic as a background traffic (a) The mean total packet loss for VoIP flows in percentage (b) The throughput for all flows in Mbps versus the number of clients

Mobile Computing and Communications Review (MC2R), special issue on Wireless Home Networks vol. 7 (2003), no. 2, pp. 6–19.