



HAL
open science

The Impact of the Reliability on the Fairness Between the Unicast and the Multicast in Highly Loaded WLANs

Yousri Daldoul, Djamal-Eddine Meddour, Toufik Ahmed

► **To cite this version:**

Yousri Daldoul, Djamal-Eddine Meddour, Toufik Ahmed. The Impact of the Reliability on the Fairness Between the Unicast and the Multicast in Highly Loaded WLANs. IEEE 36th Conference on Local Computer Networks (LCN 2011), Oct 2011, Germany. pp.835-840, 10.1109/LCN.2011.6115559 . hal-00657768

HAL Id: hal-00657768

<https://hal.science/hal-00657768>

Submitted on 9 Jan 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

The Impact of the Reliability on the Fairness Between the Unicast and the Multicast in Highly Loaded WLANs

Yousri Daldoul^{1,2}, Djamal-Eddine Meddour¹, Toufik Ahmed²

¹France Telecom - Orange Labs, France

²LaBRI, University of Bordeaux 1, France

{yousri.daldoul, djamal.meddour}@orange-ftgroup.com, tad@labri.fr

Abstract— One of the major issues experienced by the IEEE 802.11 standard is the fair sharing of the channel between unicast and multicast flows. This problem is obviously caused by the use of the smallest Contention Window size to transmit the multicast packets compared to an exponentially incremented size for every unicast packet transmission retry. This pattern is due mainly to the reliability degree difference between the unicast and the multicast traffic. Currently, the unicast uses feedbacks to provide reliability, whereas the multicast does not rely on such a mechanism and is therefore considered as unreliable.

In this paper we propose a reliable Multicast flow transport proposal called the Reliable PLCP-based Multicast Protocol (RPMP) and we study its impact on the fair channel sharing with unicast flows in high-load conditions. We show that RPMP solves the issues of the legacy multicast. (*Abstract*)

Keywords-IEEE 802.11 WLAN; reliable multicast; NAK feedback; fair chairing of the bandwidth

I. INTRODUCTION

The failure of data transmission on the wireless channel is caused by several elements: collision, interference, path loss, etc. In order to provide a reliable unicast transport, the IEEE 802.11 [1] defined an Acknowledgement (ACK) policy and a backoff time generated randomly from an exponentially increased Contention Window (CW). The use of ACK enables the sender to conclude the success or the failure of the transmission and to perform the transmission retry when necessary. The increased CW allows minimizing of collisions during contention between multiple stations (STAs) that have been deferring at the same time, and improves the stability of the unicast transmission under high-load conditions [1].

However, the 802.11 standard does not define any acknowledgement policy for the multicast and uses the lowest CW size (CW_{min}) to generate the backoff time. Such design has two main issues. 1) The multicast traffic has more priority to access the channel as its CW size is always set to CW_{min} causing unfair sharing with the unicast traffic; 2) The multicast traffic reliability is hugely reduced compared to the unicast one. These issues have a bigger impact in high-load conditions.

In [7], authors tackle the unfairness problem. Their proposed algorithm dynamically changes the CW size for multicast packets. Though this approach improves fairness, it does not offer any kind of reliability for the multicast traffic.

Many protocols were designed to deal with the unreliability of multicast traffic in IEEE 802.11 WLAN [2-6, 8-10]. They can be classified into two categories: ACK based [2, 8-10] and Negative Acknowledgement (NAK) based [3-6] protocols. The ACK based protocols use a similar concept to the unicast ACK, and they require each multicast member to send an ACK. These proposals face several of the following performance-related issues: an increased transmission overhead, a reduced efficiency, synchronization concerns, prolonged channel holding, real-time constraints, etc.

In the NAK-based protocol, the receiver will reply with a NAK only if the frame is received with errors. In some proposals [3, 5, 6], the NAK-based protocol is combined with the selection of a leader for the multicast group, where the leader is the only responder with an ACK in case of reception success. The implementation of a NAK-based protocol remains a challenging task as it requires, first, to eliminate cases where the leader's ACK signal strength may hide a multicast member's NAK, and second, to decide whether or not a NAK should be sent, since the received information within a faulty frame is not coherent and is not sufficient to build the appropriate feedback in a reliable way. The former constraint may be solved by selecting the leader member based on the lowest link quality criteria [4]. The latter is solved by using additional control frames (RTS/CTS, CTS-To-Self) to carry the trustworthy information which will be used to build a feedback. It is obvious that this solution increases the transmission overhead and consequently reduces the protocol efficiency. Another drawback is a duplicated control frames role which may cause processing confusion.

As the 802.11 standard defines the use of an increased CW to improve the stability of the unicast under high-load conditions [1], we study in this paper a wireless network with high traffic load in order to show the impact of the standard multicast procedure on the unicast. Then we present our Reliable PLCP-based Multicast Protocol (RPMP) and we evaluate it under high-load conditions by simulations. Our results show that RPMP resolves the unfairness problem and guarantees a high delivery ratio very suitable for multimedia traffic. We compare the RPMP overhead with the overhead incurred by the Leader Based Protocol (LBP) [3] and the 802.11aa [2] which are considered as the reference NAK-based protocol and the most recent ACK-based protocol respectively.

The remainder of this paper is organized as follows: In section II, we introduce related work of some proposed multicast protocols, highlighting their drawbacks. Our RPMP protocol is described in section III. Section IV shows the performance of our protocol through simulation results. Finally, we conclude the paper in section V.

II. RELATED WORK

The Batch Mode Multicast MAC protocol (BMMM) [9] defines a new control frame called RAK (Request for ACK). It first exchanges RTS/CTS frames with each multicast member, then it sends the multicast frame and finally it exchanges RAK/ACK frames again with each multicast member. BMMM is considered as a reliable protocol. The use of RAK allows the sender to perform the MAC-recovery process and to update the CW properly. Hence, BMMM eliminates the unfair sharing problem between the multicast and the unicast. However, it generates an important overhead. Besides, the growing number of multicast members increases the transmission time and causes a monopolization of the channel, which may affect the offered QoS of traffic sharing the same channel.

The “Extended Implicit MAC Acknowledgement” (EIA) [10], defines a new format for RTS/CTS and extends their use to gather feedback from each member with a more reduced overhead than in BMMM. But it remains inefficient. The design of EIA enables the MAC-recovery process, but the use of CTS to report the success or the failure of the previous transmission prevents the sender from updating its CW. The protocol concept, based on delayed ACK, is not suitable for a real time traffic transport.

The 802.11aa draft [2] is another research effort whose purpose is to enhance the QoS of the multimedia content over the 802.11 WLAN. This draft achieves the multicast reliability by asking every multicast member to acknowledge one after the other. The MAC-recovery is performed on the basis of a lack of one or more feedbacks. The MAC layer updates its CW properly and prevents the unfair sharing of the channel. Even if this draft defines a reliable multicast transport, it is clear that it requires ACK synchronization between all multicast members. Another drawback consists in the lack of efficiency caused by the important transmission overhead.

The Leader Based Protocol (LBP) [3] is the first proposal to use NAK feedbacks. It has been extensively studied in [5,6,10]. As its name indicates, LBP selects a leader for each multicast group. This protocol has attracted a great attention thanks to its efficiency and reliability compared to many other protocols. The use of the NAK feedback policy allows the sender to perform the MAC-recovery and to update the CW properly. Hence, LBP provides a fair sharing of the channel. However, it suffers from many drawbacks. First, the leader selection is done randomly, so the ACK signal may hide the NAK of other multicast members. Second, RTS/CTS frames are sent at the lowest data rate, and consequently increase the transmission overhead and reduce the protocol efficiency. And third, LBP

does not use any protection against redundancy, which may lead to unnecessary retransmissions.

In [6], authors provide a new version of the LBP protocol called the Leader-based Multicast with Auto Rate Fallback protocol (LM-ARF). This protocol uses CTS-To-Self instead of RTS/CTS in order to reduce the transmission overhead. The main advantage of this solution is the use of a dynamic rate switching algorithm. Authors show that the protocol is fair.

Table 1 summarizes the characteristics of the different studied multicast protocols.

Table 1. Protocols comparison and evaluation

Protocol	Feedback	Fair	Reliability	Efficiency
BMMM	ACK-based	Yes	Very high	Very low
EIA	ACK-based	No	Very high	Low
802.11aa	ACK-based	Yes	Very high	Low
LBP	NAK-based	Yes	High	High
LM-ARF	NAK-based	Yes	High	High

III. THE RELIABLE PLCP-BASED MULTICAST PROTOCOL

In RPMP, we use NAK feedbacks and we select a leader for each multicast group. We suppose that the leader is selected with the worst link quality to avoid cases where the ACK frame of the Leader can hide the NAK frame of another multicast member. The leader selection procedure is out of the scope of this paper and will be studied in future works.

In order to reduce the transmission overhead, compared to other NAK-based protocols, we take advantage of the existing separation between the PLCP header and the DATA part, to eliminate the use of control frames, and we insert a new OFDM symbol in the PLCP header of the multicast frame. The new symbol, illustrated in grey in Fig. 1, is used to carry the information required to build feedbacks in a reliable way.

RPMP is designed to operate in a BSS and in an Ad-hoc mode. In the remainder of this paper, we present and we evaluate our protocol in the BSS mode only. In this mode, the AP is the only multicast sender, and any multicast flow generated by a non-AP STA should be sent first in unicast to the AP which forwards that flow in multicast to the multicast group members.

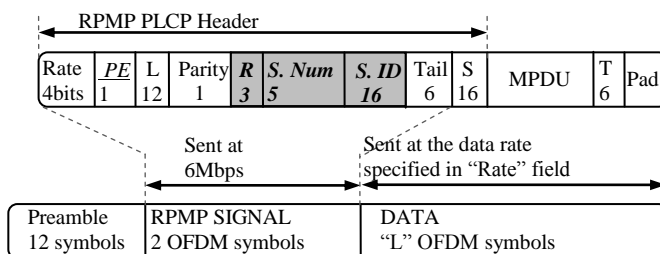


Fig. 1. PPDU frame format in RPMP

The reserved bit of the old SIGNAL becomes “PLCP Extension” (PE). This bit is used by STAs to distinguish between the RPMP PLCP header and the legacy PLCP header.

A PE set to “0” indicates a legacy PLCP and a PE set to “1” indicates a PLCP as defined by RPMP. Hence, the compatibility between standard STAs and STAs supporting RPMP is preserved.

When a frame is retransmitted, it is possible that a member which has received the frame correctly during the first transmission fails to receive it during the retry phase and consequently sends a NAK, causing a useless retransmission. Thus, we define the Sequence Number field to avoid transmission redundancy. The AP assigns a sequence number, to each multicast frame, from a modulo-32 counter, starting from 0 and incrementing by 1 for each new frame. A single counter is defined per multicast session.

The Session ID represents the multicast session to which the frame belongs. The Session IDs are attributed by the AP in a unique way for each multicast session and are managed by both the AP and each STA.

The R field is three reserved bits. As the PLCP header is protected with only one bit (the Parity bit), we recommend the use of the reserved bits as protection bits in order to increase the protection of the PLCP header against transmission errors.

The AP maintains a table called Master Allocated IDs Table (MAIDT) for all the allocated IDs. This table allows the AP to retrieve the session ID of a multicast address and to avoid allocating a used ID to a new session. Two kinds of IDs may figure in MAIDT; IDs allocated by the AP: Local IDs (LID), and IDs allocated by other APs running on overlapped BSSs: Foreign IDs (FID). LIDs are attributed for each new multicast session at the beginning of the session, while FIDs are collected using multicast members’ reports. The AP defines a lifetime long enough for a FID to be removed from the MAIDT table. A LID is liberated at the end of the multicast session.

Table 2. MAIDT of an AP with address 00:20:A6:61:1F:2B

Allocator address	Multicast address	Session ID	Recept. time
00:20:A6:61:1F:2B	01:00:5E:00:00:01	755E (LID)	-
00:20:A6:61:1F:2B	01:00:5E:00:00:0A	10E0 (LID)	-
00:20:92:27:8A:75	-	3F11 (FID)	124215242
00:20:A6:61:1F:2B	01:00:5E:00:00:F3	30FA (LID)	-

Each STA maintains a table of all discovered IDs: STA Discovered IDs Table (SDIDT). This table allows the STA to generate a NAK if needed, and to report the discovered IDs to its AP. We distinguish 3 ID types in SDIDT; (1) IDs allocated by the AP of the STA: Available IDs (AID), (2) IDs, among AIDs, identifying sessions that the STA has joined: Joined IDs (JID), (3) and FID. A STA adds a new entry in its SDIDT table on the reception of a correct multicast frame with a new ID. A STA defines a lifetime long enough to delete a FID.

Table 3. SDIDT of STA associated to AP with address 00:20:A6:61:1F:2B

Allocator address	Multicast address	Session ID	Recept. time
00:20:A6:61:1F:2B	01:00:5E:00:00:01	755E (JID)	-
00:20:A6:61:1F:2B	01:00:5E:00:00:0A	10E0 (AID)	-
00:20:92:27:8A:75	01:00:5E:00:02:F1	3F11 (FID)	124215242
00:20:A6:61:1F:2B	01:00:5E:00:00:F3	30FA (JID)	-

A multicast member should keep the sequence number of the most recently received frame from each joined multicast session in its cache. For example, for a multicast session S1, each member of this session maintains a value called S1_SN which records the sequence number of the most recently received frame from S1. This value will be used to avoid unnecessary retransmissions from S1.

Operating mode:

At the beginning of a new multicast session, the AP selects a leader and attributes a unique ID for this session. Once the ID is attributed, the AP adds the following entry in its MAIDT table : <AP address, multicast session address, ID>. When the MAC layer of the AP receives a multicast frame from the upper layer, it retrieves the ID corresponding to the AP address and the multicast address of the received frame from the MAIDT table. Then the MAC sends the frame, the retrieved ID and the sequence number to the PHY layer. Thus the latter builds the PLCP header and transmits the frame.

At the receiver side, 3 scenarios are possible:

- The multicast frame is received correctly: the receiver checks the entry corresponding to <AP address, multicast session address, ID> of the frame in its SDIDT table. If there is no entry for this triple, the receiver builds a new one. Each receiver updates the sequence number recorded in its cache to match with the sequence number of the received frame. Only the leader replies with an ACK.
- The frame is received with a correct PLCP header and a bad MPDU: the receiver retrieves the ID and the sequence number of the frame from the PLCP header, and extracts the entry corresponding to the received ID from its SDIDT table. If there is no entry for this ID or if the extracted entry does not correspond to a multicast session the receiver has joined, the receiver rejects the frame without performing any action. Otherwise, the receiver compares the sequence number of this frame with the recorded sequence number of the session. If these two values match, the receiver concludes that this frame has been previously received correctly, so only the leader sends an ACK. If not, the receiver sends a NAK.
- Both the PLCP and the MPDU are received with errors: the frame can not be decoded and will consequently be rejected. If this scenario is experienced by the leader, the sender will not receive an ACK and the retransmission will be performed.

The AP updates the CW and performs the frame retransmission if it does not receive an ACK or receives a NAK instead. In RPMP we keep the same CW increment process and retry limit value used with the unicast. The sequence number of a frame remains unchanged for all the transmission retries.

To attribute a unique ID for each new multicast session, the AP updates its MAIDT table at the beginning of each new multicast session by asking each member of the new session for its SDIDT table. During the session, if a member detects

that the ID is becoming used by another multicast source, it informs its AP to change the ID. So the AP asks each member for its SDIDT table again, updates its MAIDT table, attributes a new ID to the multicast session and switches to this ID.

In Fig. 2, the AP transmits frames from session S1 to 3 members. S1_m1 is the leader and S1_ID is the ID of S1. In this figure, the AP sends a frame with a sequence number equal to 5. S1_m1 and S1_m2 receive the frame correctly, so they update their cache with the sequence number of the frame. S1_m3, however, experiences a MPDU error. As the sequence number of the frame does not match with the previously recorded sequence number, S1_m3 sends a NAK. The collision between the leader's ACK and the NAK of S1_m3 prevents the AP from receiving an ACK, so the frame is retransmitted. In the retransmission phase, both S1_m1 and S1_m2 receive the frame with a MPDU error and S1_m3 receives correctly the frame. Thanks to the sequence number, only the leader sends an ACK.

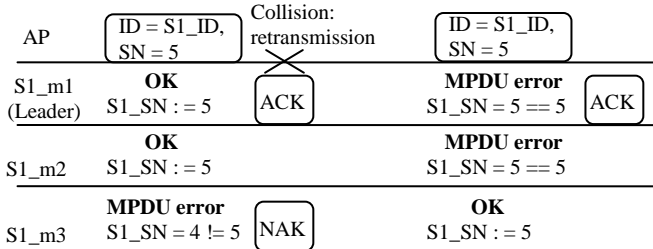


Fig. 2. RPMP transmission procedure

In RPMP, the reliability is achieved by enabling NAK feedbacks. And these frames are built based on the new OFDM symbol. Thus, the reliability of RPMP is based on the PLCP header, i.e. a NAK may be built only and only if the PLCP header has been received correctly. Even if RPMP does not provide a perfect reliability, its global reliability is high since, based on our observations, more than 99% of the transmission's errors are caused by MPDU's errors, and as such a limited transmission number of errors (less than 1%) may occur without recovery: the *PLCP errors phenomenon*. Since our main concern is to provide an optimal reliability with the lowest cost of bandwidth for multimedia traffics, RPMP remains very suitable for such loss-tolerant traffics.

IV. PROTOCOL EVALUATION

In Fig. 3 and Fig. 4 we evaluate the transmission overhead for a *per frame* transmission without taking account of the required time to contend for the channel. Hence, results are obtained according to Equation (1) for each of the evaluated protocols.

$$\text{Overhead ratio} = [\text{Multicast frame overhead Time} + \text{required acknowledgement Time}] / \text{Transmission Time} \quad (1)$$

The conception of RPMP gets rid of RTS/CTS frames. Thus only the multicast frame is transmitted, and this reduces the frame overhead considerably, compared to LBP, as depicted in Fig. 3.

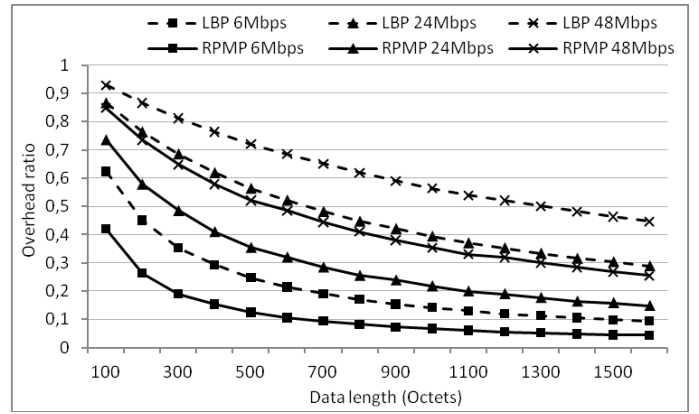


Fig. 3. RPMP vs. LBP: Overhead ratio versus Data length

In Fig. 4 we compare the overhead of RPMP with that of 802.11aa for a multicast group of 8 members. We show that 802.11aa requires an important overhead. This overhead increases with the growing number of the multicast members according to Equation (2).

$$\text{Overhead ratio} = [\text{Multicast frame overhead Time} + N \times (\text{SIFS} + \text{ACK Time})] / \text{Transmission Time} \quad (2)$$

Where N is the Multicast members Number

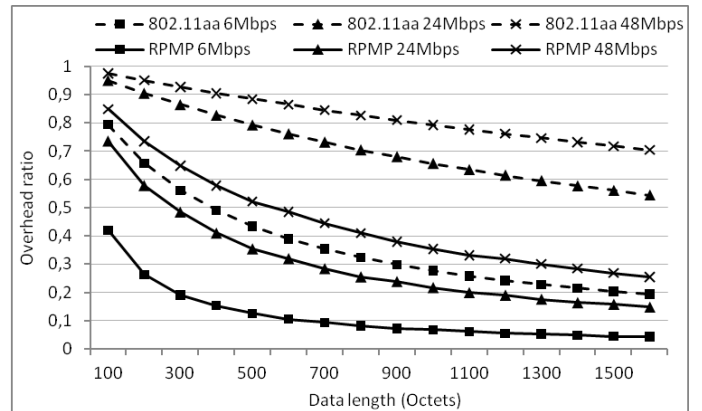


Fig. 4. RPMP vs. 802.11aa: Overhead ratio versus Data length

In the rest of this section we present simulation results to evaluate the channel sharing between the unicast and the RPMP multicast and we compare the delivery ratio of RPMP with that of the unreliable 802.11 multicast protocol in high-load condition. These results are obtained using the ns-3 simulator [11].

In our simulation scenario, we set up an infrastructure WLAN with one AP and 6 STAs situated at the same distance from the AP and distributed uniformly. We keep the position of the AP unchanged and we move periodically the position of all the STAs away from the AP keeping the same distance from the latter. This is considered as being the worst scenario, since the leader has the same reception signal strength as all the other members, maximizing the impact of the PLCP errors phenomenon on the reliability of RPMP in the obtained results. All transmitted frames have 1000 octets' data length.

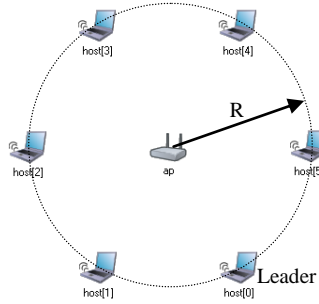


Fig. 5. Simulation scenario

The AP generates a single multicast flow. Each STA is at the same time a member of this multicast session and generates a single unicast flow. The transmission data queues of the AP (only multicast data) and of all the STAs (unicast data), are never empty (high-load condition). We use the 3 mandatory data rates of the 802.11a/g, (6, 12 and 24Mbps) and we run the AP with each of them in 3 simulations. In each simulation, we keep 2 STAs running with each mandatory data rate. We use different data rates for two reasons. First, to build a network similar to real networks where different data rates are deployed together, and second, to show that the number of channel access does not depend on the used rate, but depends on the CW instead.

In Fig. 6 and 7, the margin of the channel access number for the different unicast flows is grey-colored. Then we draw a curve for the multicast transmissions number per data rate, for the three mandatory data rates. In contrast to the legacy multicast, the use of RPMP allows the multicast access to the channel, to remain within the range of the unicast one. Hence, when we use RPMP we see that at distances below 50 meters, the margin of transmitted unicast frames is between 170 and 250 frames per second. So the average is 210 frames per second which is almost the average of transmitted multicast frames. When the legacy multicast is used, the average is reduced to 175 frames per second for the unicast flows. The average number of transmitted multicast frames depends on the used data rate and exceeds the unicast mean twice.

In Fig. 6, at distances below 50 meters, all data rates are efficient, so they share the medium equitably. As STAs are moving away from the AP, only STAs using robust data rates keep transmitting successfully at important distances and therefore keep sharing the channel. This explains the behavior of the grey zone as a function of distance. We see that when all the STAs leave the AP coverage area, the number of transmitted frames per second for the AP and for each STA, converges again to the same average value of 145 frames per second for all the data rates. The reason is that the AP and all the STAs increase their CW in the same way after each transmission failure.

In Fig. 7, however, when the STAs increase their CW, the AP keeps CW_{min} to transmit multicast flows. So the multicast frames dominate the channel when the STAs leave the AP coverage area.

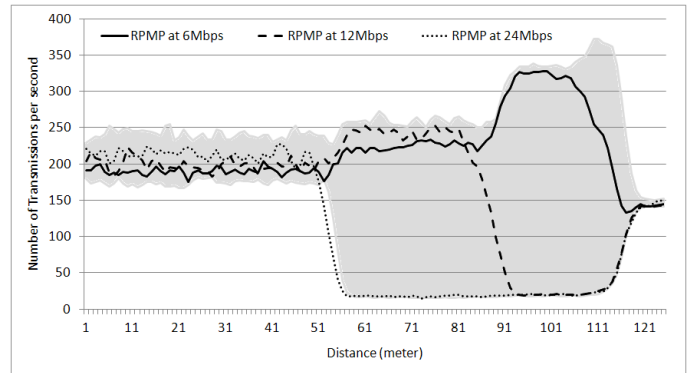


Fig. 6. RPMP multicast vs. unicast

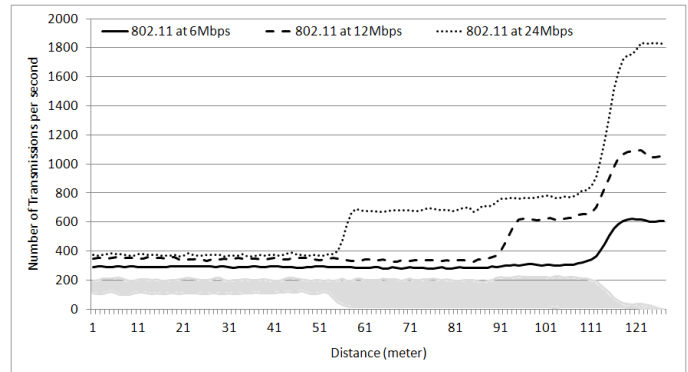


Fig. 7. Legacy multicast vs. unicast

In Fig. 8 we show that the delivery ratio of the legacy multicast is reduced, compared to that of RPMP. At distances below 50 meters, the legacy multicast encounters higher collision probability since all the unicast flows contend equally for the channel. As STAs are moving away from the AP, the unicast flows' contention is reduced, and this reduces collision probability and enhances the delivery ratio of the legacy multicast at higher distances in our scenario. We conclude that the delivery ratio of the standard multicast procedure decreases with the increasing number of contending STAs. However, the delivery ratio of RPMP depends only on the used data rate and the distance between the sender and the receivers.

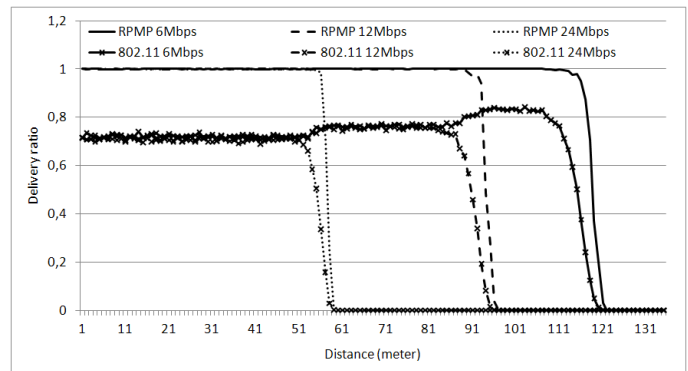


Fig. 8. Delivery ratio of RPMP vs legacy multicast with 5 contending unicast flows

V. CONCLUSION

In this paper, we present the unfair sharing problem of the channel between unicast and multicast flows and we present our reliable multicast proposal called RPMP as a solution for the fairness and for the multicast reliability. This work presents an evaluation of the performance of RPMP in a highly loaded WLAN. Simulation results show that RPMP is reliable and is efficient against unfair sharing of the channel between unicast and multicast flows, and remains very suitable for multimedia traffic.

REFERENCES

- [1] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE std 802.11, 2007.
- [2] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 4: MAC Enhancements for Robust Audio Video Streaming," IEEE P802.11aa/D1.01, June 2010.
- [3] J. Kuri and S. K. Kasera, "Reliable multicast in Multi-Access Wireless LANs," ACM/Kluwer Wireless Networks Journal, 2001.
- [4] J. Miroll, Z. Li and Th. Herfet, "Wireless Feedback Cancellation for Leader-Based MAC Layer Multicast Protocols," in IEEE ICSE, 2010.
- [5] N. Choi, Y. Seok, T. Kwon, Y. Choi, T. Kwon. "Multicasting multimedia streams in IEEE 802.11 networks: a focus on reliability and rate adaptation," Springer Science+Business Media, LLC 2010.
- [6] S. Choi, N. Choi, Y. Seok, T. Kwon, Y. Choi, "*Leader-based Rate Adaptive Multicasting for Wireless LANs*", IEEE GLOBECOM, 2007.
- [7] N. Choi, J. Ryu, Y. Seok, Y. Choi, T. Kwon. "Unicast-Friendly Multicast in IEEE 802.11 Wireless LANs," in Proc. IEEE CCNC, 2006.
- [8] N. Choi, Y. Seok, T. Kwon, Y. Choi, "Transparent Unicast Translation to Improve Quality of Multicast over Wireless LAN," in IEEE CCNC, 2010.
- [9] M.T. Sum, L.Huang, "*Reliable MAC layer multicast in IEEE 802.11 wireless networks*," ICPP, 2002.
- [10] Xiaoli Wang, Lan Wang, "*Reliable Multicast Mechanism in WLAN with Extended Implicit MAC Acknowledgment*", IEEE VTC, 2008.
- [11] The NS-3 Simulator, <http://www.nsnam.org/>