A Reliable PLCP-based Multicast Protocol for IEEE 802.11 WLAN

Yousri Daldoul, Djamal-Eddine Meddour, Toufik Ahmed

A Reliable PLCP-based Multicast Protocol for IEEE 802.11 WLAN

Yousri Daldoul[1, 2], Djamal-Eddine Meddour[1], Toufik Ahmed[2]
[1]France Telecom - Orange Labs, France
[2]LaBRI, University of Bordeaux 1, France
{yousri.daldoul, djamal.meddour}@orange-ftgroup.com, tad@labri.fr

***Abstract*- In current IEEE 802.11 WLAN, the unicast provides a reliable way of communication thanks to the use of acknowledgement feedbacks. As to the multicast, it suffers from unreliability and inefficiency. Recently many protocols have been designed for 802.11 such as Leader Based Protocol (LBP), to provide a reliable multicast transport. Yet no optimal solution has been proposed. In this paper we present Reliable PLCP-based Multicast Protocol (RPMP), a new reliable multicast protocol as an extension to the 802.11g and 802.11a. RPMP achieves reliability through the use of Negative Acknowledgements (NAK). We reduce the transmission overhead of our protocol, compared to other NAK-based proposals, by adding one additional OFDM symbol in the Physical Layer Convergence Procedure (PLCP) header of the multicast frame instead of using additional control frames. Further we show, based on our simulation results that the delivery ratio of RPMP remains at 100% in a lossy channel when it falls down to 50% with the standard. We also show that the efficiency of RPMP is much more enhanced than that of LBP.**

Keywords- IEEE 802.11 WLAN; reliable multicast; NAK feedback

I. INTRODUCTION

The failure of data transmission on the wireless channel can be caused by several reasons: 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 performs the transmission retry when necessary. The increased CW allows minimizing 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 to generate the backoff time. Although most of the multicast traffic is loss tolerant traffic and is more sensitive to real time constraints than reliability constraints (video conference, real time streaming video, etc…), investigating the multicast reliability over 802.11 remains important for many reasons. The first reason is related to the multirate aspect of the PHY layer. The 802.11 standard uses the lowest but the most robust data rate of the PHY layer to transmit multicast frames, thus maximizing the delivery ratio of the MAC layer. This approach reduces significantly the performance of the standard, and makes it inappropriate for several applications requiring important bitrates even if these bitrates are included in the range supported by the 802.11. A multicast protocol with ACK policy allows the development of an efficient dynamic rate-switching algorithm like [3,7,12], and a reliable use of high data rates. The second reason is related to the recovery performance. In our study, we show that using a recovery policy can provide a delivery ratio of 100% when the loss ratio of a transmission, with no feedback policy, reaches 50%. This leads us to the third reason being the uncontrolled loss ratio due to a variable link quality between the sender and the receivers: using a non reliable multicast transport can cause a serious loss ratio which makes the traffic content unusable, even for a loss-tolerating traffic. The fourth reason is to guarantee a multiuser network with an equitable and fair access to the medium between unicast and multicast traffics. A reliable multicast protocol using ACK feedbacks achieves this fairness by enabling the multicast source to perform binary exponential backoff for multicast frame losses. The impact of the multicast traffic on the unicast one is explained in more details in [11]. The last reason concerns the impact of reliability on real time traffic. An efficient MAC recovery policy does not require much time, compared to the real time constraints, and consequently improving the traffic reliability for real time applications leads to an enhanced Quality of Service (QoS) with a reduced cost.

In this paper we propose a new reliable multicast protocol for the 802.11 called Reliable PLCP-based Multicast Protocol (RPMP), and we evaluate its performance through simulation. The novelty of RPMP is threefold. First, we redefine the utilization of the Negative Acknowledgement (NAK) feedback policy in order to allow the use of NAK with individual data frames. Second, we reduce the transmission overhead and we increase the protocol efficiency by inserting one additional OFDM symbol in the Physical Layer Convergence Procedure (PLCP) header of the multicast frame instead of using additional control frames (RTS/CTS, CTS-To-Self). This new symbol carries the information required by the receiver to build a NAK. Third, we use a complementary sequence number to protect the multicast against unnecessary retransmissions.

978-1-4577-1261-6/11/$26.00 ©2011 IEEE

The remainder of this paper is organized as follows: In section II we introduce related work of some proposed multicast protocols we have studied, highlighting their problems and drawbacks. Our RPMP protocol is described in section III. We devote section IV to show the performance of our protocol through simulation results. Finally, in section V, we conclude and we provide an overview of our future work.

II. Related Works

Many protocols were designed to address the unreliability of the multicast in the 802.11 WLAN [2-10]. They can be classified into two categories: ACK based [2,8-10] and Negative Acknowledgement (NAK) based [3-7] protocols. The ACK based protocols use a similar concept to the unicast ACK, and they require each multicast member to send an explicit ACK. These proposals face several of the following performance-related issues: an increased transmission overhead, a reduced efficiency, synchronization concerns, a prolonged channel holding, real-time constraints, etc.

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. The transmission process is illustrated in Fig. 1:

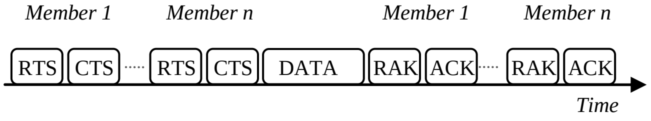

Fig. 1. BMMM Acknowledgement policy

BMMM is considered as a reliable protocol but it requires an important transmission 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) [8], defines a new format for RTS/CTS and extends their use to gather feedbacks from each member with a more reduced overhead than in BMMM. But it remains inefficient. Its concept, based on the 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. Even if this draft defines a reliable multicast transport, it requires ACK synchronization between all multicast members. Another drawback consists in the lack of efficiency caused by the important transmission overhead. As in BMMM, the increasing number of multicast members in 802.11aa leads to a potential monopolization of the channel, and results in affecting the time sensitive applications.

In the NAK-based protocol, the receiver will reply with a NAK only if the frame is received with errors. In some proposals, the implementation of the protocol is joined 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 enough 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 [5]. 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.

The Leader Based Protocol (LBP) [4] is the first proposal to use NAK feedbacks. It has been extensively studied in [3,6-8]. As it is illustrated from its name, LBP selects a leader for each multicast group. This protocol has attracted a great attention thanks to its efficiency and reliability. However, it suffers from many drawbacks. First, the leader selection is done randomly, and 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 mechanism against redundant transmission, which may lead to unnecessary retransmissions.

In [7], authors provide a new version of the LBP protocol called the Leader-based Multicast with Auto Rate Fallback protocol (LM-ARF). This protocol combines the use of NAK feedbacks with 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.

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

Table 1. Protocols comparison and evaluation

The NAK principle is very interesting since it increases the reliability and the efficiency of the protocol: the reliability is improved thanks to the use of a feedback and a MAC-layer recovery mechanism, and the efficiency is enhanced as only one ACK/NAK frame delay is extended to the multicast frame transmission delay. Therefore the transmission overhead is limited.

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 including the MAC Protocol Data Unit (MPDU), to eliminate the use of control frames, and we insert a new OFDM symbol in the PLCP header of the multicast frame instead. The new symbol, illustrated in bold in Fig. 2, is used to carry in a reliable way, the information required to build feedbacks.

RPMP is designed to operate in an infrastructure and in an Ad-hoc mode. In the remainder of this paper, we focus on the infrastructure 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.

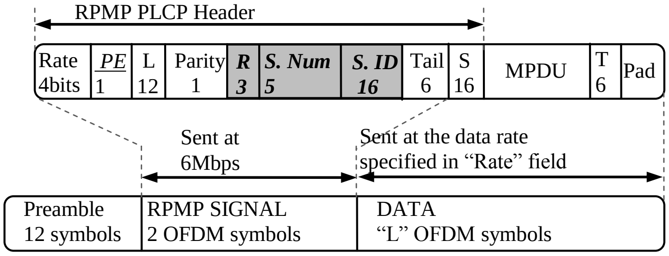

Fig. 2. PPDU frame format in RPMP

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 who has received correctly the frame during the first transmission, fails to receive it during the retry phase and causes consequently 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 a 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.

A STA sends a NAK if it receives a faulty frame with a Session ID identifying a session that the STA has joined and with a Sequence Number different then the last recorded one. Otherwise, only the leader sends an ACK.

The AP maintains a table called Master Allocated IDs Table (MAIDT) for all the allocated IDs. This table, illustrated in Table 2, 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 remove the latter from the MAIDT table. A LID is liberated at the end of the multicast session.

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)	1244215242
00:20:A6:61:1F:2B	01:00:5E:00:00:F3	30FA (LID)	-

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

Each STA maintains a table of all discovered IDs: STA Discovered IDs Table (SDIDT). This table, illustrated in Table 3, 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 large enough to delete a FID.

Allocator address	Multicast address	Session ID	Recept. time
00:20:A6:61:1F:2B	01:00:5E:00:00:01	755E (AID-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)	1244215242
00:20:A6:61:1F:2B	01:00:5E:00:00:F3	30FA (AID-JID)	-

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

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 SN_S1 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 all of 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 from 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 (which may be due to a collision with other NAKs or because no ACK has been generated) or receives a NAK instead. The sequence number of a frame remains unchanged for all the transmission retries.

In Fig. 3, 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 Fig, 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 retry 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.

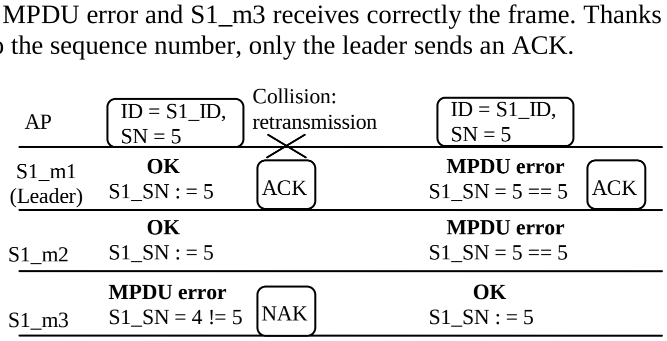

Fig. 3. RPMP transmission procedure

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. If a member detects that an ID is becoming used by other multicast sources, 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 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. 4 and Fig. 5 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.

Overhead ratio = [Multicast frame overhead Time +required acknowledgement Time] / Transmission Time (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. 4.

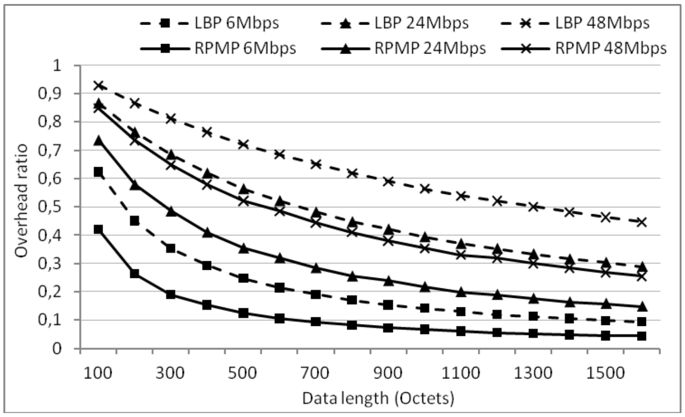

Fig. 4. RPMP vs. LBP: Overhead ratio versus Data length

In Fig. 5 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).

Overhead ratio = [Multicast frame overhead Time +N × (SIFS + ACK Time)] / Transmission Time (2)

Where N is the Multicast members Number

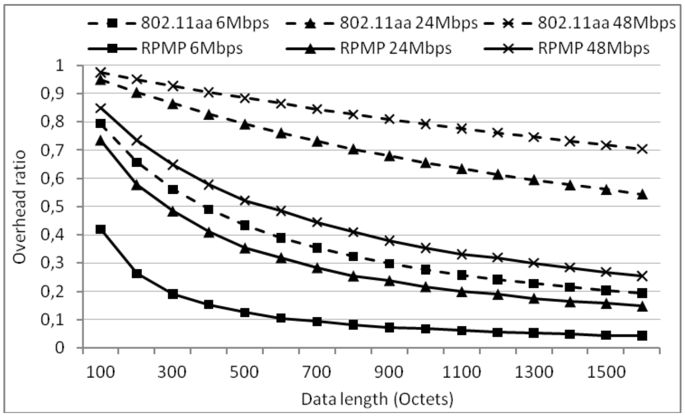

Fig. 5. RPMP vs. 802.11aa: Overhead ratio versus Data length

In the rest of this section we provide simulation results to compare the performance of our protocol with that of LBP and the standard multicast procedure. We obtained our results using the OMNet++ simulator [13] in conjunction with the INET framework. Our simulation scenario consists of an AP and 8 multicast members situated at the same distance "R" from the AP, as it is illustrated in Fig. 6. 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 PLCP errors on the reliability of RPMP in the obtained results. The AP starts only one multicast session and no traffic other than the multicast one is transmitted on the medium. All transmitted frames have 1532 bytes' data length.

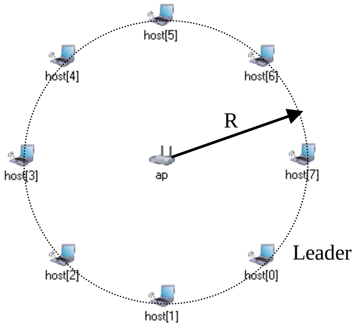

Fig. 6. Simulation scenario

More details about the simulation scenario are listed in Table 4.

Parameter	Values
Simulator	OMNet++ with INET framework
Number of multicast members	8
MAC frame length	1532 bytes
MAC protocol	IEEE 802.11g
PHY Layer	OFDM
Data rates	6, 24 and 48 Mbps
Retry limit	7
Transmission Power	100mW
Path loss (alpha)	2.6
Channel model	Rayleigh

Table 4. Simulation parameters

Fig. 7 and 8 represent the protocol throughput versus the distance R and SNR respectively. These figures show that RPMP has a higher throughput than LBP. The enhanced throughput of RPMP is justified by the fact that our protocol uses only one additional OFDM symbol, where LBP uses RTS/CTS control frames with each multicast frame.

The use of protection against unnecessary retransmissions allows RPMP to behave better than LBP when the Bit Error Rate (BER) increases. Based on Fig. 4 we conclude that the throughput difference between RPMP and LBP is more significant for shorter data lengths.

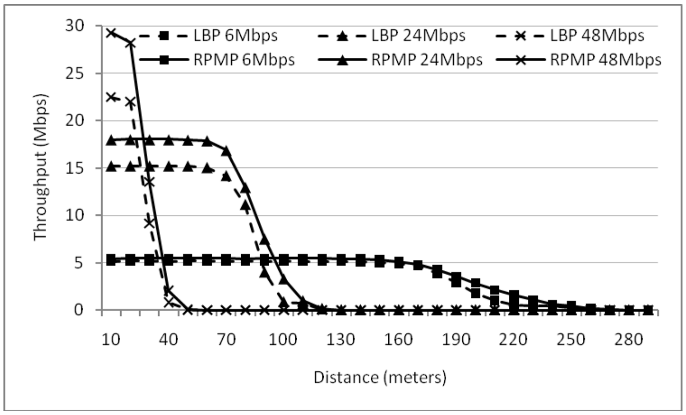

Fig. 7. Throughput versus Distance

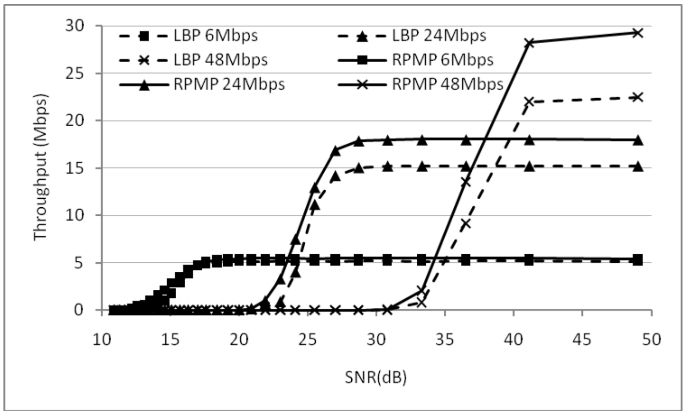

Fig. 8. Throughput versus SNR

In Fig. 9, we show that the delivery ratio of the legacy multicast is reduced, compared to that of RPMP. Since the 802.11 multicast procedure does not use feedbacks, the sender can not update its transmission data rate based on the link quality and the rate performance. However, the use of NAKs allows RPMP to run any dynamic rate switching algorithm to take advantage of the multirate capability of the PHY layer.

We show also the reliability of both RPMP and LBP. As it is shown, both protocols are reliable and are able to provide a delivery ratio up to 100% when the delivery ratio of the 802.11 falls to 50%. Even if the delivery ratio of LBP is the same as RPMP, our protocol remains more efficient. RPMP is also easier to implement because it does not need to manage RTS information for the next frame to come, as is the case in LBP.

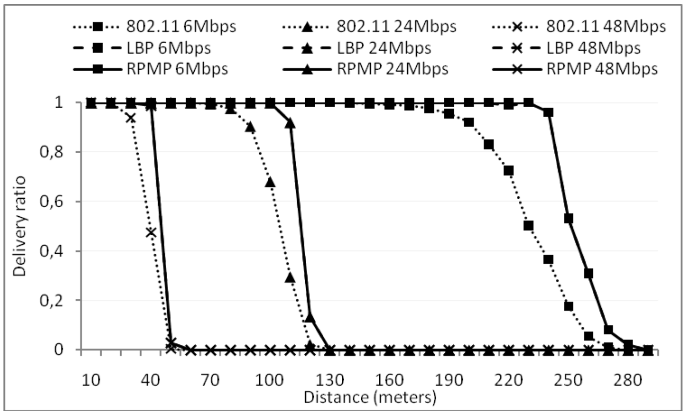

Fig. 9. Delivery ratio versus Distance

V. Conclusion

In this paper we presented RPMP, a reliable and efficient multicast protocol designed for the 802.11 WLAN. This protocol is based on a leader selection and NAK frames. In our simulation results, we proved that RPMP behaves better than the well-established LBP protocol since RPMP eliminates RTS/CTS frames and uses only one additional OFDM symbol in the PLCP header of the multicast frame instead. RPMP integrates a protection mechanism to prevent unnecessary retransmissions and consequently increases the protocol efficiency. This mechanism is neither available in LBP nor in other NAK based protocols. In this paper we presented the multicast transmission procedure, but the leader selection procedure has not been introduced yet and will be studied in our future works.

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] 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.

[4] J. Kuri and S. K. Kasera, "*Reliable multicast in Multi-Access Wireless LANs*," ACM/Kluwer Wireless Networks Journal, 2001.

[5] J. Miroll, Z. Li and Th. Herfet, "Wireless Feedback Cancellation for Leader-Based MAC Layer Multicast Protocols," IEEE ICSE, 2010.

[6] A. Basalamah , H. Sugimoto and T. Sato, "*Rate adaptive reliable multicast MAC protocol for WLANs*," IEEE VTC, 2006.

[7] S. Choi, N. Choi, Y. Seok, T. Kwon, Y. Choi, "*Leader-based Rate Adaptive Multicasting for Wireless LANs*", IEEE GLOBECOM, 2007.

[8] Xiaoli Wang, Lan Wang, "*Reliable Multicast Mechanism in WLAN with Extended Implicit MAC Acknowledgment*", IEEE VTC, 2008.

[9] M.T. Sum, L.Huang, "*Reliable MAC layer multicast in IEEE 802.11 wireless networks*," ICPP, 2002.

[10] N. Choi, Y. Seok, T. Kwon, Y. Choi, "*Transparent Unicast Translation to Improve Quality of Multicast over Wireless LAN*,“ IEEE CCNC, 2010.

[11] N. Choi, J. Ryu, Y. Seok, Y. Choi, T. Kwon. "*Unicast-Friendly Multicast in IEEE 802.11 Wireless LANs*," IEEE CCNC, 2006.

[12] J. Bicket. *Bit-rate Selection in Wireless Networks*. MIT Master's Thesis, 2005.

[13] http://www.omnetpp.org/