MAC Protocol for Reliable Multicast over Multi-Hop Wireless Ad Hoc Networks

Sung Won Kim, Byung-Seo Kim, and Inkyu Lee

Abstract: **Multicast data communication is an efficient communication scheme, especially in multi-hop ad hoc networks where the media access control (MAC) layer is based on one-hop broadcast from one source to multiple receivers. Compared to unicast, multicast over a wireless channel should be able to deal with varying channel conditions of multiple users and user mobility to provide good quality to all users. IEEE 802.11 does not support reliable multicast owing to its inability to exchange request-to-send/clear-to-send and acknowledgement packets with multiple recipients. Thus, several MAC layer protocols have been proposed to provide reliable multicast. However, additional overhead is introduced, as a result, which degrades the system performance. In this paper, we propose an efficient wireless multicast MAC protocol with small control overhead required for reliable multicast in multi-hop wireless ad hoc networks. We present analytical formulations of the system throughput and delay associated with the overhead.**

Index Terms: **Multicast, media access control (MAC), wireless ad hoc, multi-hop.**

I. INTRODUCTION

Computing and communication anytime, anywhere is a global trend in today's wireless network technologies. Ubiquitous computing has been made possible by the advance of wireless communication technology and the availability of many lightweight, compact, and portable computing devices. Ad hoc networks support peer-to-peer communication between active nodes via multi-hop wireless links. In ad hoc networks, the network topology is changed by the mobility of the wireless nodes. The ad hoc networks are self-configurable and do not require any infrastructure for their operation. This enables many applications such as teleconferencing, disaster relief coordination, and battlefield operations over wireless networks. These group-oriented and mission-critical applications require accurate and timely data delivery [1].

Multicast is the transmission of data to a group of nodes identified by a single destination address. The two node types in multicast transmission are multicast source nodes and multicast member nodes. The source node mainly distributes multicast data to multiple member nodes that want to receive the multicast data and join the multicast group. Hereafter, we use the term member node to refer to a multicast member node.

Unlike multicast in wired networks, wireless multicast takes advantage of the broadcast-channel nature of wireless networks to efficiently and simultaneously disseminate common information to multiple location-independent receivers, such that wireless resource consumption is reduced. Thus, multicast constitutes a bandwidth-efficient technique for group communication. However, it introduces new challenges owing to the error-prone nature of wireless channels compared to wired networks. Undoubtedly, low loss and low latency are basic building blocks supporting multicast applications, especially in the face of frequent route outages and random packet dropping due to mobility, fading, external interference, etc. Multicast packets over wireless channels may be corrupted and lost for many reasons. First, channel fading, environmental interference, and mobility can produce random data loss. In the case of military or civil defense surveillance, adverse jamming may cause additional data loss. Another cause of data loss is packet collision.

To deal with data loss due to channel error, unicast transmission adopts the automatic repeat request (ARQ) method to carry out successful data transmission. Request-to-send (RTS)/clear-to-send (CTS) handshake standardized in IEEE 802.11 media access control (MAC) partially solves the problem of packet loss due to collision by letting other nodes delay their transmissions. Even though it cannot completely prevent collision due to hidden nodes, it has been considered as the best solution for the issue over ad hoc networks. While unicast provides solutions for packet losses, neither ARQ nor RTS/CTS handshaking is available for multicast in standards such as IEEE 802.11 and IEEE 802.15. The main reason for this is the overhead. Because all member nodes need to respond with an acknowledgement (ACK) packet or CTS to the multicast source, too much overhead is required. Consequently, this overhead degrades the network performance. The overhead over wireless multicast with ACK and CTS increases as the number of member nodes increases. Therefore, most standards do not adopt the overhead and the multicast data is unreliably transmitted. This is illustrated in standards for wireless communications, such as IEEE 802.11, IEEE 802.15, IEEE 802.16, 3rd generation partnership project (3GPP), and 3GPP2. ARQ, CTS, or retransmission for multicast is not available in any of these standards. Some studies have proposed packet-loss recovery schemes and methods to prevent hidden node problems and solve reliability issues in wireless multicast, particularly in distributed network environments such as ad hoc networks [2]–[7]. However, these error recovery schemes may introduce even more excessive overhead, causing congestion and possibly forcing the system to totally

Manuscript received August 4, 2010; approved for publication by Wha Sook Jeon, Division III Editor, January 20, 2011.

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0015236)(2010-0002483)(2010-0028002).

S. W. Kim is with the Department of Information and Communication Engineering, Yeungnam University, Gyeongsangbuk-do 712-749, Korea, email: swon@yu.ac.kr.

B. Kim is with the Department of Computer and Information Communications Engineering, Hongik University, ChungCheongNam-do 339-701, Korea, email: jsnbs@hongik.ac.kr.

I. Lee is with the School of Electrical Engineering, Korea University, Seoul 136-701, Korea, email: inkyu@korea.ac.kr.

1229-2370/12/$10.00 © 2012 KICS

collapse, unless the input rate is also controlled. A recently proposed method shown in [8] may solve the overhead issue in packet loss recovery, but not the hidden node issue over multihop networks.

The goal of our multicast design is to utilize the concept of orthogonal frequency-division multiple access (OFDMA) to reduce overhead. The method proposed in this paper modifies conventional CTS and ACK packets by adding one special orthogonal frequency-division multiplexing (OFDM) symbol. Each subcarrier in the OFDM symbol is assigned to each group member node. All member nodes simultaneously send their RTS or data-reception statuses using the pre-assigned subcarriers in the CTS or ACK packet on receiving the RTS or data packet. Because the subcarriers are orthogonal, the multicast source is able to receive all subcarriers and check if any node fails to receive the RTS or data packet. Therefore, it reduces the overhead required to acknowledge the packet-reception status of all member nodes to the multicast source and efficiently resolves the hidden node problem as well as the ARQ issue for wireless multicast. We present a comprehensive mathematical model for the proposed multicast design. The remainder of this paper is organized as follows. The next section reviews related work. In Section III, the proposed method is described. In Section IV, we analyze the throughput and delay of the proposed method. In Section V, we discuss the improvement achieved by the proposed method and provide some numerical results. Finally, this paper is concluded in Section VI.

II. RELATED WORK

IEEE 802.11 wireless local area networks (WLANs) [9] use multicast transmission. In contrast to unicast transmission, multicast transmission is unreliable, in the sense that multicast packets are transmitted from the access point (AP) without any ACK being returned from each receiver. Thus, the transmitted multicast packets may be lost owing to collisions or errors. IEEE 802.11 also suffers from the hidden node problem, because the RTS/CTS handshake is not adopted in multicast.

In IEEE 802.11-based ad hoc networks, multicast packets are broadcast to all the multicast members within one-hop distance in a single transmission. Packets suffer from increased instances of the hidden node problem owing to the properties of broadcast and multicast. The mobility of nodes makes things even more difficult. In unicast transmissions, MAC can detect the movement associated with the next hop by retrying several times: However, this is not possible in the case of multicast forwarding. The multicast-aware MAC protocol (MMP) [3] was proposed to address these issues. MMP uses the MAC header to support ACK-based data delivery. After sending the data packet, the transmitter waits for the ACK from each destination. ACKs from the destination nodes are sent in a strictly sequential order to prevent collisions between ACKs at the transmitter. Overhead increases as the number of nodes increases owing to the use of multiple ACKs, thus resulting in throughput degradation. MMP also suffers from the hidden node problem because of the lack of the RTS/CTS handshake.

Leader-based protocol (LBP) was proposed in [7]. This protocol works around the problem of collisions between multiple CTS/ACK packets by providing a means for only one (leader) of the multicast recipient nodes to respond with a CTS or an ACK. This protocol performs well in low mobility networks. However, as the mobility of the nodes increases, the performance is degraded. When a node cannot decode a MAC header, LBP does not perform accurately. A source node in LBP knows that any member node cannot receive a RTS packet when the leader's CTS packet collides with the member node's CTS packet. However, if the member node cannot decode the MAC header of the RTS packet owing to channel error or a hidden node, it cannot send a CTS packet to the source to create a collision. This gives false information to the source, and the source will send a multicast packet. The multicast packet might collide with a transmission from a member node that does not receive the RTS. This false information also appears for ACK packet transmission. That is, if a member node does not receive RTS as well as a data packet, it will not cause an intentional collision with the ACK packet from the leader. This false information prevents the source from retransmitting, so that the member node permanently loses an opportunity to receive the data packet. This could be a severe problem in the TCP/IP layer. Moreover, CTS transmission by only the leader partially solves the hidden node issue because nodes hearing the CTS from the leader can set their own network allocation vector (NAV). Nodes that cannot hear the CTS from the leader and are in radio range of the other member nodes may cause collisions.

The batched mode multicast MAC (BMMM) protocol in [4] and [5] focuses on the collision issue in wireless multicast. It requires RTS/CTS exchange between a sender and all member nodes to resolve the issue. In addition, after data transmission, it requires request-ACK (RAK)/ACK exchange between the sender and all member nodes. Therefore, BMMM suffers from more overhead than MMP. The protocol proposed in [10] uses a multi-tone scheme to avoid collision. This protocol uses two separate channels for data transmission and non-ACK (NACK) signaling. Even though this protocol uses two separate channels, a sender cannot collect indications of whether all the members receive the data packet correctly. Enhanced LBP (ELBP) [2] adopts LBP with extended control frame exchange: RTS-CTS-SEQ-DATA-NACK. The sequence (SEQ) message is used to clearly announce that the following data frame is a multicast frame. Unlike LBP, a node that fails to receive the data packet sends a NACK packet. However, this cannot provide reliability when the node fails to receive both a SEQ and data. For example, when a node is under a short deep fading channel, the node cannot send a NACK packet. Like LBP, ELBP also suffers from the hidden node issue. Beacon-driven LBP (BLBP) [11] is also an LBP, but adopts ELBP. Instead of using the SEQ frame in ELBP, BLBP uses a beacon frame to ensure all receivers know that an upcoming frame is a multicast frame. Hybrid LBP (HLBP) [12] is BLBP with packet-level forward error correction (FEC) to increase reliability. Although the level of reliability is increased using FEC, both BLBP and HLBP still have an issue when the beacon frame is not received by any receiver. This causes false information, as mentioned in the description of LBP, because the receivers that do not receive the beacon packet cannot send the NACK packet. In addition, like ELBP, HLBP, and BLBP create additional overhead, which includes the beacon frame;

this increases as the number of function increases. In [13], LBP was experimentally studied and an algorithm was proposed to select a leader. Recently, we proposed OFDMA-based ACK (OMACK) protocol [8]. OMACK adopts the OFDMA concept in the ACK frame format. Therefore, a reliable ARQ method is achieved without additional overhead. However, OMACK focuses on ARQ and one-hop wireless networks. It does not consider the hidden node issue over multi-hop ad hoc networks.

III. PROPOSED WIRELESS MULTICAST

A. Multi-Hop Network Environment

The network environment considered here is a multi-hop wireless ad hoc network. We consider certain multicast routing protocols from the literature [14]. Multicast routing paths (tree or mesh) are constructed using multicast routing protocol and multicast traffic is forwarded to the next hop. In one-hop transmission over routing paths, a node multicasts a multicast packet to one-hop member nodes; thus, it is termed a source within one-hop transmission. If the multicast packet needs to be forwarded to the next hop in the path, one of the members receiving the multicast packet becomes a source node within the next one-hop range and forwards the packet to the next one-hop member nodes. This forwarding sequence is defined by the multicast routing protocol. The transmission mechanism described in this paper is also applicable to one-hop communication over such a network environment, because layer-2 protocols deal with one-hop communications. Therefore, if a member node is two-hop away from source node A in terms of the multicast routing tree, the node is not a member of source node A within one hop. The node might be a member of source node B, which is a member of source node A. That is, when a member node is within one-hop range of a source, the node is a member of the source node according to a routing path. Thus, the proposed protocol provides reliable transmission for each one-hop communication in multi-hop multicast transmissions.

Two issues have to be resolved to achieve reliability of multicast transmissions. The first is the hidden node issue irrespective of whether the node is within one-hop range or two-hop range. Multi-hop networks have a worse transmission environment than one-hop networks owing to greater hidden node issues. Even though a node is more than two-hop away in a routing path, it can be a hidden node for communications two-hop away owing to the time-varying nature of the channel. The second issue is packet loss due to channel errors, even within one-hop communication range. Both issues cause packet losses and degrade reliable transmission. The proposed protocol also adopts RTS-CTS exchange to deal with such issues. The RTS-CTS transmission alleviates performance degradation due to unnecessary data transmission. If there are hidden nodes, the RTS-CTS exchange makes hidden nodes delay their transmission. In addition, if a member node receives an erroneous RTS packet, a source stops transmitting a multicast data, because CTS is not returned to the source.

B. Protocol Operation

Wireless multicast in layer-2 has been suffering from two issues: the hidden node issue and the overhead required for data acknowledgement. Even though much effort has been devoted to resolve these issues, as discussed in the previous section, they are infeasible to implement. Although OMACK [8] successfully resolves the overhead issue with acknowledgements, it still has the hidden node issue over multi-hop networks. As an extension of our previous work (OMACK), we aim to design a layer-2 protocol to resolve both the issues in wireless multicast, even over multi-hop wireless ad hoc networks.

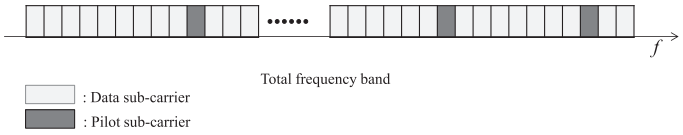

Fig. 1. An example of OFDMA sub-carrier allocation.

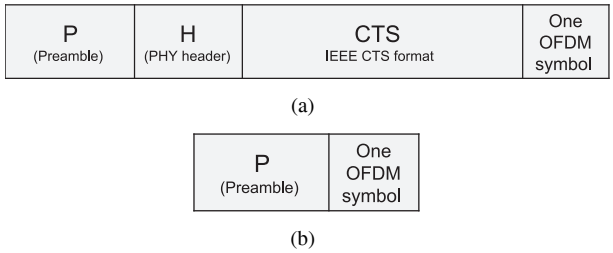

Fig. 2. (a) CTS and (b) ACK packet format.

The design of the proposed method is inspired by OFDMA, which utilizes the orthogonality of the sub-carriers in the OFDM symbols [15]–[17]. Fig. 1 shows an example of the OFDMA frequency band. The formats of the CTS and ACK packets in the IEEE 802.11 standard are modified for the proposed protocol. As shown in Fig. 2(a), the format of the CTS packet has one additional OFDM symbol at the end of the conventional IEEE 802.11-based CTS packet. The ACK packet is composed of a preamble and an OFDM symbol, as shown in Fig. 2(b). The OFDM symbols in the CTS and ACK packets include a cyclic prefix. These symbols are used to acknowledge successful receipt of the previous packet. Usage of the OFDM symbols is explained in detailed below.

Each member node has a unique pre-assigned sub-carrier location in an OFDM symbol. The process of assigning a unique sub-carrier location to a node is described in the next subsection. When a member node receives an RTS packet from the sender, it allocates one of two binary phase-shift keying (BPSK) symbols, -1 or 1, to its pre-assigned sub-carrier in the additional OFDM symbol of the new CTS packet, as shown in Fig. 2(a). The successful reception of the RTS packet is indicated by the BPSK symbol 1 on the sub-carrier. On the contrary, the BPSK symbol -1 indicates the failed reception of the RTS packet. If a member node cannot demodulate the MAC header of the RTS packet, it will not send a CTS packet.

The sub-carriers, with the exception of the sub-carrier assigned to the CTS transmitter, are not allocated a symbol. That is, the additional OFDM symbol of the new CTS packet carries one BPSK symbol on only one of the sub-carriers. The remaining parts of the CTS packets from all of the member nodes are identical, except for the additional OFDM symbol. The additional OFDM symbols are different for each node, because each

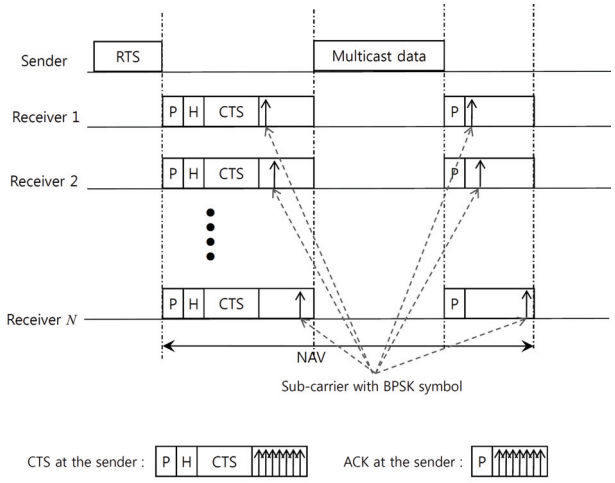

Fig. 3. Example of a data packet transmission cycle.

node allocates a BPSK symbol to its own sub-carrier, which is unique. It is assumed that all member nodes send their CTS packets simultaneously after the short interframe space (SIFS) idle period. Furthermore, CTS packets from all member nodes are modulated with the lowest data rate in the basic data rate set (6 Mbps). Because all of the CTS packets from member nodes are the same, the multicast sender receives many copies of a CTS packet; this increases the power of the received CTS packet at the source. That is, the sender receives the CTS packet more reliably. In addition, unlike the aforementioned LBP, all nodes around member nodes receive the CTS packet, so that the hidden node issue is prevented. On the other hand, the OFDM symbols at the end of the CTS packet are different. However, because the OFDM symbols have one BPSK symbol in a member node's unique sub-carrier, the OFDM symbols from member nodes are combined at the multicast sender and look like one OFDM symbol with as many BPSK symbols as the number of member nodes. This is a principle and characteristic of OFDMA. Thus, a receiver can distinguish data on each one of the sub-carriers even though all sub-carriers with data are transmitted simultaneously, because all sub-carriers are orthogonal to each other in the frequency domain. The BPSK symbol in the combined OFDM symbol indicates each member's ACK for the previously transmitted packet. Similar to the OFDM symbol in the new CTS packet, the OFDM symbol in the new ACK packet is used to acknowledge the reception of a data packet. The manner in which the OFDM symbol used in the ACK packet is the same as that in the CTS packet. When member nodes successfully receive a data packet, they allocate a BPSK symbol on their pre-assigned sub-carrier in the OFDM symbol and then send the OFDM symbol after attaching a preamble, as shown in Fig. 2(b).

Fig. 3 shows an example scenario of the proposed method. A sender multicasts an RTS packet to the member nodes that range from receiver 1 to receiver N. Each receiver responds with a CTS packet that has one BPSK symbol on its pre-assigned sub-carrier. When a node hears the CTS packet, it sets its NAV value using the duration subfield in the CTS packet. Thus, the proposed scheme also provides a means for contention-free transmission, similar to the scheme in the IEEE 802.11 standard, but reduces the overhead due to multiple CTS transmissions from member nodes.

Note that the additional OFDM symbol at the end of the CTS packet is illustrated on a frequency scale (that is, the arrow in the CTS packet represents the sub-carrier with a BPSK symbol), whereas the overall transmission sequence is illustrated on a time scale in Fig. 3. If any receiver does not receive the RTS packet, it will not send a CTS packet to the sender. After receiving the CTS packets, the sender checks the sub-carriers that are assigned to the member nodes. If any one of the member nodes' sub-carriers is not allocated with any symbol or is allocated with the BPSK symbol -1, the sender prepares to retransmit an RTS packet.

When all of the required sub-carriers in the OFDM symbol in the CTS packet have the BPSK symbol 1, the sender transmits a multicast data packet to the member nodes. An example of a received CTS packet at the multicast sender is shown at the bottom of Fig. 3, which represents the case where all the member nodes send their CTS packets. As seen, the simultaneously received OFDM symbols form one OFDM symbol with multiple sub-carriers owing to the orthogonality of sub-carriers. When a member node receives a multicast data packet from the sender, it allocates a symbol on the pre-assigned sub-carrier as an ACK for the data packet. The generation of ACK is the same as that of CTS. An example of ACK is shown in Fig. 3. As in the case of the CTS packet reception described above, the sender checks the BPSK symbols on all of the required sub-carriers in the OFDM symbol of the ACK packet, and decides whether to retransmit the data packet. In this paper, the retransmission policy adopted is that of unicast in the IEEE 802.11 standard. Fig. 4 shows the procedures performed by each member after it receives an RTS packet and a data packet from a sender.

Regarding backward compatibility, it is assumed that the source is able to recognize OFDMA-multicast-enabled nodes and legacy nodes through the process of association or multicast group join. The protocol-version subfield in the frame control field of the MAC header can be used to identify the OFDMA-multicast-enabled node. Therefore, if there is legacy node in a multicast group, the multicast traffic will be transmitted in a legacy format, which is a transmission without ACK as described in IEEE 802.11.

C. Sub-Carrier Assignment

The sub-carrier assignment is managed by the multicast leader (ML). Each multicast group has an ML. When a node wants to join a multicast group, it broadcasts a multicast join request (MJREQ) packet. When the ML receives the MJREQ, it assigns an empty sub-carrier to the requesting node. The maximum number of members for a multicast service is 52, which is the number of available sub-carriers in one OFDM symbol defined in the IEEE 802.11 standard. If the number of member nodes exceeds 52, more OFDM symbols might be attached at the end of the CTS and ACK packets shown in Fig. 2, and ML assigns not only the sub-carrier number but also the OFDM symbols number to the member nodes. If a member node is assigned the 10th sub-carrier with the second OFDM symbol, it sends two OFDM symbols followed by the CTS frame. However, the first symbol is blank and the 10th sub-carrier in the second symbol

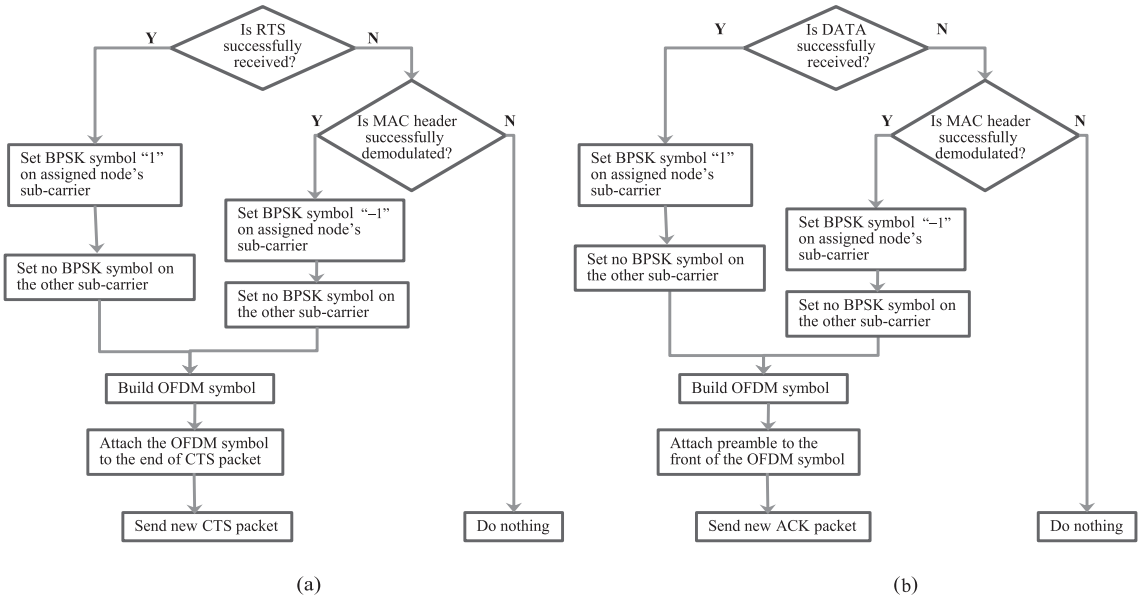

Fig. 4. Procedures after (a) receiving an RTS packet and (b) a data packet from a sender.

has a BPSK symbol. Then, the ML responds with a multicast join ACK (MJACK) packet that has the information of the allocated sub-carrier. The assigned sub-carrier has to be unique for each node within the same multicast group address.

If there is no ML, no MJACK will be sent. In that case, i.e., if there is no response within a certain time threshold, the requesting node becomes the new ML for that multicast group address.

When an ML wants to leave a multicast group, it unicasts a multicast leader request (MLREQ) packet to one of the multicast group members. If the node responds with a multicast leader ACK (MLACK), the responding node becomes the new ML. If there is no MLACK within a certain time threshold, the ML selects another node and transmits MLREQ packets until a new ML is selected.

D. Time and Frequency Offset

The time and frequency offset problems due to imperfect time synchronization and different propagation delays from all of the member nodes have been addressed in [15]–[20]. These problems may break the sub-carriers' orthogonality in an OFDM symbol and make it difficult to evaluate the channel condition.

Timing accuracy becomes a stringent requirement in applications where the cyclic prefix is made as short as possible to minimize the overhead. However, using a sufficiently long guard interval between adjacent OFDMA blocks (in the form of a cyclic prefix) provides intrinsic protection against timing errors at the expense of some reduction in data throughput due to the extra overhead [21].

A specific number of un-modulated subcarriers is typically inserted among subbands to provide adequately large guard intervals and mitigate frequency errors. If the frequency offsets are sufficiently smaller than the guard intervals, user's signals can easily be separated at the receiver by passing the received samples through a bank of digital band-pass filters, each one subband [21].

Timing and frequency correction is an active research area in OFDMA. Research in [15]–[17] shows that the problems are solved using a cyclic prefix that is longer than any of the delay spread profiles. In [18], a novel preamble structure was proposed to decouple multi-user synchronization and channel estimation. In [19] and [20], link protocols were proposed to synchronize OFDMA-based packets from multi-users over ad hoc networks.

In the WLAN environment, the guard interval is expected to be small enough to be ignored because of low mobility and small coverage area. In [22], it was proposed that the degradation due to residual frequency and timing errors was negligible at signal-to-noise (SNR) ratios of practical interest.

It is important to deal with the trade-off between the system performance, guard interval, and frequency offset. However, it is laborious and is beyond the scope of this paper. Hence, the time and frequency offset problems are not considered in this paper. However, the result of the timing and frequency synchronization errors is SNR degradation [23]. The effect of SNR degradation is discussed in our paper as a packet loss probability in the next section.

IV. PERFORMANCE ANALYSIS

A. System Model

As discussed in the previous section, two types of reliable multicast are proposed in the IEEE 802.11 MAC layer: The ACK-based multicast (ABM) and the LBP. We compare the performance of the proposed method with ABM and LBP. In ABM, multiple CTSs and ACKs are transmitted in a sequential order for a packet transmission. In LBP, CTS and ACK are transmitted only by a leader. Thus, LBP is not only weak against the hidden node problem but also causes decision error on the transmission statuses from all member nodes in certain cases. Moreover, the protocol overhead for selecting a leader increases as the mobility of nodes increases. However, the leader-selection overhead

of LBP is not dealt with in this paper. The superscripts PRO, ABM, and LBP are used for the proposed method, ABM, and LBP, respectively.

We adopt the analytical model used in [24]–[26]. We consider a system consisting of N nodes. Each node always has a packet available for transmission. In other words, we operate under saturation conditions in which the transmission queue of each node is always assumed to be nonempty. The average number of nodes within a node's transmission range is denoted by n. The average number of multicast group nodes within a node's transmission range is denoted by r.

The duration of backoff is determined by the contention window (W) size, which is initially set to $W_{\min}$. The W value is used to randomly select the number of slot times (σ) in the range of [0, $W-1$], which is used for the backoff duration. In the case of an unsuccessful transmission, the W value is updated to $2W$ as long as it does not exceed $W_{\max}$. Let us adopt the notation $W_i = 2W_{i-1}$, where $i \in \{1, \cdots, B\}$ is called the backoff stage and B is the maximum backoff stage such that $W_{\max} = 2^B W_{\min}$. After the maximum number of retries, a packet is dropped from the transmission buffer.

B. Transmission Probability and Failure Probability

A discrete and integer time scale is adopted: t and $t+1$ correspond to the beginnings of two consecutive changes in the backoff time counter. We refer to the time interval between t and $t+1$ as the "counter time slot." Note that the counter time slot is of variable time duration, whereas the slot time is of constant time duration. Because the decrement of the backoff time counter is stopped when the channel is sensed to be busy, the time interval between the beginnings of two consecutive backoff time counter instants may be much longer than the constant slot time duration.

Let us denote the event wherein a node transmits a packet into a counter time slot as X. We focus on the *transmission probability* $\tau = \Pr(X)$ that a node transmits a packet into a counter time slot. Let p_c be the probability that a transmitted packet sees a collision on the channel. Channel conditions such as shadowing and fading are assumed to generate a constant packet loss probability, p_e, for all of the wireless connections. When $p_e = 0$, channel conditions are idle. We assume that the control packets are received with $p_e = 0$ because they are transmitted with a low data rate and their packet size is small compared with that of the data packet. We assume that the events of p_c and those of p_e are mutually exclusive. Let p be the *failure probability* that a transmitter does not receive ACK for the transmitted data packet because of a collision or channel error. Let p_s be the *success probability* that a transmitter receives ACK for the transmitted data packet, that is, $p_s = 1 - p$. In LBP, a transmitter receives ACK from a leader and the failure probability is given as

$$p^{\mathrm{LBP}} = p_c^{\mathrm{LBP}} + p_e = 1 - p_s^{\mathrm{LBP}}. \tag{1}$$

The minimum value of p^{LBP} is p_e when p_c is equal to zero. In ABM, a transmitter confirms ACKs from all the member nodes and the failure probability is

$$p^{\mathrm{ABM}} = p_c^{\mathrm{ABM}} + 1 - (1-p_e)^r = 1 - p_s^{\mathrm{ABM}}. \tag{2}$$

The minimum value of p^{ABM} is $1-(1-p_e)^r$ when p_c is equal to zero.

In the proposed method, a transmitter in backoff stage $i+1$ confirms ACKs from the nodes that have not been confirmed from backoff stage 0 to i. In other words, the ACKs that are already received in the previous stages are not checked in the proposed method. Let r_i be the number of receivers that do not return ACK until backoff stage i is reached. Note that the initial number of receivers is $r_0 = r$. Let s_i be the number of receivers that returns ACK for the packet transmitted during backoff stage i. Thus,

$$r_{i+1} = r_i - s_i, \quad 0 \le s_i \le r_i. \tag{3}$$

The probability that s_i will be s in backoff stage i is given as

$$\Pr(s_i = s) = \binom{r_i}{s} (1-p^{\mathrm{PRO}})^s (p^{\mathrm{PRO}})^{r_i - s}. \tag{4}$$

The r_i is a binomial random variable, and its mean value is given as

$$\begin{aligned} E[r_0] &= r, \\ E[r_1] &= E[r_0]p^{\mathrm{PRO}} = rp^{\mathrm{PRO}}, \\ E[r_{i+1}] &= E[r_i](p^{\mathrm{PRO}}) = r(p^{\mathrm{PRO}})^i, \\ &\quad \text{for } i = 0, \cdots, B-1. \end{aligned} \tag{5}$$

The failure probability of the proposed method is given as

$$p^{\mathrm{PRO}} = p_c^{\mathrm{PRO}} + 1 - \sum_{i=0}^{B} (1-p_e)^{E[r_i]} P(b=i) \tag{6}$$

where $\Pr(b=i)$ is the probability that a node is found in the backoff stage i. The minimum value of p^{PRO} is $1 - \sum_{i=0}^{B}(1-p_e)^{E[r_i]}\Pr(b=i)$ when p_c is equal to zero.

From [26], p_c is assumed to be a constant value, independent of the number of retransmissions that have occurred. Thus, p_c can be expressed as

$$p_c^{\mathrm{LBP}} = p^{\mathrm{LBP}} - p_e, \tag{7}$$

$$p_c^{\mathrm{ABM}} = p^{\mathrm{ABM}} - 1 + (1-p_e)^r, \tag{8}$$

$$p_c^{\mathrm{PRO}} = p^{\mathrm{PRO}} - 1 + \sum_{i=0}^{B} (1-p_e)^{E[r_i]} \Pr(b=i). \tag{9}$$

In a steady state, each remaining node transmits a packet with probability τ. For each protocols, p_c is equal to

$$p_c = 1 - (1-\tau)^{n-1} \tag{10}$$

which represents the probability that at least one of the $n-1$ remaining nodes transmits.

The probability that a node is found in the backoff stage i is given as

$$\Pr(b=i) = \tau \frac{\Pr(b=i|X)}{\Pr(X|b=i)}, \; i \in (0, \cdots, B). \tag{11}$$

By summing all values of i, we get

$$\sum_{i=0}^{B} \Pr(b=i) = 1 = \tau \sum_{i=0}^{B} \frac{\Pr(b=i|X)}{\Pr(X|b=i)}. \tag{12}$$

From (12), τ can be expressed as

$$\tau = \frac{1}{\sum_{i=0}^{B} \frac{\Pr(b=i|X)}{\Pr(X|b=i)}}. \tag{13}$$

The transition probabilities of the backoff stage are given as

$$\begin{cases} \Pr(b(t+1) = i \mid b(t) = i-1) = p, \\ \qquad \text{for } i = 1, \cdots, B \\ \Pr(b(t+1) = 0 \mid b(t) = i) = 1-p, \\ \qquad \text{for } i = 0, \cdots, B-1 \\ \Pr(b(t+1) = 0 \mid b(t) = B) = 1. \end{cases} \tag{14}$$

It readily follows that the conditional backoff stage probability $\Pr(b = i|X)$ is a geometric distribution, i.e.,

$$\Pr(b = i|X) = \frac{(1-p)p^i}{1-p^{B+1}},\ i \in (0, \cdots, B). \tag{15}$$

From the independence among transmission cycle and renewal theory, we can obtain the conditional transmission probability $P(X|b = i)$ by dividing the average number of counter time slots required in a transmission cycle (exactly one time slot) by the average number of counter time slots required by the node during the complete cycle (backoff and transmission cycle in backoff stage i). Because a time slot corresponds to a backoff counter decrement,

$$\Pr(X|b = i) = \frac{1}{1 + E[c_i]},\ i \in (0, \cdots, B) \tag{16}$$

where $E[c_i]$ is the average value of the backoff counter extracted by a node entering stage i. $E[c_i]$ is equal to $W_i/2$ under the assumption of a uniform distribution in the range of (0, W_i). By substituting (15) and (16) into (13), we get

$$\tau = \frac{1}{1 + \frac{1-p}{1-p^{B+1}} \sum_{i=0}^{B} p^i E[c_i]}. \tag{17}$$

From (11), (15), and (16), the probability $\Pr(b = i)$ can be expressed as

$$\Pr(b = i) = \tau \frac{(1-p)p^i}{1-p^{B+1}}(1 + E[c_i]). \tag{18}$$

Equations (7)–(10), (17), and (18) represent a nonlinear system in terms of the two unknowns τ and p, which can be solved using numerical techniques.

C. Packet Drop Probability

In this paper, packet drop probability is used to determine the degree of transmission reliability of each system. When all member nodes receive a multicast data packet, the transmission of the data is considered to be reliable. Therefore, if any one of the member nodes misses a current data packet and the next data packet is transmitted, the current packet is considered as a dropped one.

In the proposed method and ABM, a data packet is dropped because of retry limit exhaustion. In LBP, we consider that a data packet is also dropped when one of the receivers does not receive the packet even though a leader receives it. This is because although a leader returns an ACK packet, one of the receivers may fail to receive the packet. As mentioned in Section II, LBP does not retransmit a data packet once a source receives CTS and ACK from a leader even though members do not receive the data packet. That is, the members that do not receive data packet permanently lose the opportunity to receive the data packet. From this perspective, if any member node does not receive a data packet but a leader successfully sends CTS and ACK, we consider this case as a packet drop, which means a loss of reliability. Thus, in LBP, packet is dropped owing to either retry limit exhaustion or any reception failure at the non-leader nodes. Let p_d represent the probability that a data packet is dropped. Since this probability depends on backoff stage i, we obtain

$$p_d = \sum_{i=0}^{B} \Pr(\text{drop}|b = i) P(b = i). \tag{19}$$

In LBP, there are two reasons for packet drop in stage i. The first reason is that a packet in backoff stage i reaches stage B (i.e., it collides $B - i$ times) and also collides during the last transmission attempt. This probability is equal to p^{B+1-i}. The second reason of packet drop is that a leader successfully receives a packet while one of the other receivers fails to receive the packet. The probability of the second reason in stage i is equal to $p_s(1 - p_s^{r-1})$. The probability of the second reason in stage $i + 1$ is equal to $p_s(1 - p_s^{r-1})p$, where p is the probability of the failure in stage i, p_s is the success probability of the leader node in stage $i + 1$ and $1 - p_s^{r-1}$ is the failure probability of any of the other nodes. Similarly, the probability of the second reason in stage j is equal to $p_s(1 - p_s^{r-1})p^{j-i}$, where $i \le j \le B$. Hence, $\Pr(\text{drop}|b = i)$ of LBP is given as

$$\begin{aligned} \Pr(\text{drop}|b = i) &= p^{B+1-i} + p_s(1 - p_s^{r-1}) \\ &\quad + p_s(1 - p_s^{r-1})p + \cdots + p_s(1 - p_s^{r-1})p^{B-i} \\ &= p^{B+1-i} + p_s(1 - p_s^{r-1}) \sum_{j=i}^{B} p^{j-i} \\ &= p^{B+1-i} + p_s(1 - p_s^{r-1}) \frac{1 - p^{B-i+1}}{1-p} \\ &= p^{B+1-i} + (1 - p_s^{r-1})(1 - p^{B-i+1}) \end{aligned} \tag{20}$$

where the superscript LBP is omitted for the sake of simplicity.

As mentioned earlier, in the proposed method and ABM, a packet is dropped because of retry limit exhaustion. The backoff stage is updated if any of the receivers does not return ACK. Hence, $\Pr(\text{drop}|b = i)$ of the proposed method and ABM are given as

$$\Pr^{\text{PRO}}(\text{drop}|b = i) = (p^{\text{PRO}})^{B+1-i}, \tag{21}$$

$$\Pr^{\text{ABM}}(\text{drop}|b = i) = (p^{\text{ABM}})^{B+1-i}. \tag{22}$$

From (19)–(22), we can obtain the packet drop probabilities of LBP, ABM, and the proposed method.

D. State Probability and Counter Time Slot

Let T_{RTS}, T_{CTS}, T_{DAT}, T_{ACK}, T_{SIFS}, and T_{DIFS} be the transmission durations of an RTS packet, a CTS packet, a data packet,

an ACK packet, SIFS, and DIFS, respectively. Let $T_{\rm tx}$ be the time duration of a data packet transmission cycle. $T_{\rm tx}$ is the entire time duration required for a data packet transmission including overhead. The value of $T_{\rm tx}$ for the proposed method and LBP is given as

$$T_{\rm tx}^{\rm PRO} = T_{\rm tx}^{\rm LBP} = T_{\rm RTS} + T_{\rm CTS} + T_{\rm DAT} + T_{\rm ACK} + 3T_{\rm SIFS} + T_{\rm DIFS}. \quad (23)$$

Because ABM requires multiple CTSs and ACKs, T_{tx} for ABM is given as

$$T_{\rm tx}^{\rm ABM} = T_{\rm RTS} + r(T_{\rm CTS} + T_{\rm ACK} + 2T_{\rm SIFS}) + T_{\rm DAT} + T_{\rm SIFS} + T_{\rm DIFS}. \quad (24)$$

Note that $T_{\rm tx}$ can also be the amount of time wasted if the data packet is lost. Let $T_{\rm col}$ be the wasted time if the RTS packet collides. For the proposed method and LBP, it is given as

$$T_{\rm col}^{\rm PRO} = T_{\rm col}^{\rm LBP} = T_{\rm RTS} + T_{\rm CTS} + T_{\rm SIFS} + T_{\rm DIFS}. \quad (25)$$

For ABM, it is given as

$$T_{\rm col}^{\rm ABM} = T_{\rm RTS} + r(T_{\rm CTS} + T_{\rm SIFS}) + T_{\rm DIFS}. \quad (26)$$

Let α and β be the tagged source and one of the destination nodes, respectively. For each possible state j of α, we find the state probability P_j and counter time slot T_j to estimate the system throughput in the next subsection.

The probability that α is idle in a counter time slot is $1-\tau$. Under such a condition, the probability that all other nodes within the transmission range of α are idle is $(1-\tau)^{n-1}$. Since α and all other nodes within α's transmission range are idle in this state, α will remain in the idle state for σ. Let this case be state 1. Then, the state probability and the counter time slot of state 1 are given as

$$P_1 = (1-\tau)^n, \quad (27)$$
$$T_1 = \sigma.$$

Let us consider state 2 where α is idle and only one node in the transmission range of α transmits. Note that packet collision may occur in this case because there may exist a hidden node of the transmitting node, which is out of the transmission range of α. The probability that α is idle in a counter time slot is $1-\tau$. Under this condition, the probability that at least one of the nodes within the transmission range of α transmits a packet is $1-(1-\tau)^{n-1}$. Under the condition that at least one node transmits, the probability $P_{\alpha 1}$ that only one node transmits a packet is given as

$$P_{\alpha 1} = \frac{(n-1)\tau(1-\tau)^{n-2}}{1-(1-\tau)^{n-1}}. \quad (28)$$

Then, the state probability of State 2 is given as

$$P_2 = (1-\tau)[1-(1-\tau)^{n-1}]P_{\alpha 1} = (n-1)\tau(1-\tau)^{n-1}. \quad (29)$$

The counter time slot for RTS packet loss is $T_{\rm col}$ and that for data packet loss is $T_{\rm tx}$. Let w be the ratio between the number of lost RTS packets and the sum of the lost RTS and data packets. Then, the counter time slot for state 2 is given as

$$T_2 = (1-p)T_{\rm tx} + p[wT_{\rm col} + (1-w)T_{\rm tx}]. \quad (30)$$

Let us consider state 3 where α is idle and more than one node in the transmission range of α transmit. The probability of state 3 is

$$P_3 = (1-\tau)[1-(1-\tau)^{n-1}](1-P_{\alpha 1}). \quad (31)$$

Because there is more than one concurrent transmission in the same transmission range, the counter time slot of state 3 is given as

$$T_3 = wT_{\rm col} + (1-w)T_{\rm tx}. \quad (32)$$

From state 1 to state 3, α is idle during the counter time slot.

Let us consider state 4 where α transmits and at least one node in the transmission range of β transmits. The probability that α transmits a packet in a tagged counter time slot is τ. Under this condition, the probability that at least one node in the transmission range of β transmits a packet is $1-(1-\tau)^{n-1}$. Thus, the state probability is given as

$$P_4 = \tau[1-(1-\tau)^{n-1}]. \quad (33)$$

In this state, the packet is lost and the counter time slot is given as

$$T_4 = wT_{\rm col} + (1-w)T_{\rm tx}. \quad (34)$$

Let us consider state 5 where α transmits and all other nodes in the transmission range of β are idle. The conditional probability that all other nodes in the transmission range of β are idle is $(1-\tau)^{n-1}$. The state probability is given as

$$P_5 = \tau(1-\tau)^{n-1}. \quad (35)$$

In this state, the packet can be transmitted successfully and the counter time slot is

$$T_5 = T_{\rm tx}. \quad (36)$$

E. Throughput and Delay

From the analytical results given in the previous subsection, the average counter time slot, $T_{\rm CT}$, is given as

$$T_{\rm CT} = \sum_{j=1}^{5} P_j T_j. \quad (37)$$

Let $P_{\rm tr}$ be the probability that there is at least one transmission in the considered counter time slot. Because n nodes contend on the channel and each node transmits with probability τ,

$$P_{\rm tr} = 1-(1-\tau)^n. \quad (38)$$

The probability $P_{\rm su}$ that a data packet is successfully transmitted is given by the probability that exactly one node transmits on the

channel without packet error, assuming that at least one node transmits, i.e.,

$$P_{\rm su} = \frac{n\tau(1-p_e)(1-\tau)^{n-1}}{P_{\rm tr}}. \tag{39}$$

The normalized throughput S within a transmission range can be expressed as

$$\begin{aligned} S &= \frac{E[\text{time of a successful data transmission}]}{E[\text{time of a counter time slot}]} \\ &= \frac{P_{\rm tr}P_{\rm su}T_{\rm DAT}}{T_{\rm CT}}. \end{aligned} \tag{40}$$

The throughput in (40) represents the system utilization required for successful transmission in a point-to-point communication. In multicast, we have to consider the successful transmission for point-to-multipoint communication. However, in LBP, the packet whose ACK is received from a leader while none of the other nodes receives the packet, is included in the throughput. Thus, we define a goodput G as the system utilization required for successful transmission when packets are received by all the receivers. The goodput excludes the packet drop from the throughput and is given as

$$G = S(1-p_d) = \frac{P_{\rm tr}P_{\rm su}(1-p_d)T_{\rm DAT}}{T_{\rm CT}}. \tag{41}$$

Let M be the number of counter time slots required for the multicast receivers to successfully receive the multicast packet. Because the average number of counter time slots in backoff stage i before the transmission is $E[c_i]$, the average value of M is given as

$$E[M] = \sum_{i=0}^{B}(1+E[c_i])\Pr(b=i). \tag{42}$$

From (11), (15), and (16), it can be rewritten as

$$E[M] = \sum_{i=0}^{B}\tau(1+E[c_i])^2\frac{(1-p)p^i}{1-p^{B+1}}. \tag{43}$$

Packet delay is defined as the time period from the start of a data packet becoming a head-of-line (HOL) in the queue to the end of the data packet's removal from the queue [6]. The packet's removal is caused by either retry limit exhaustion or its successful reception by all the receivers in the proposed method and ABM or by a leader in LBP. The sender must process every ACK received for the packet. If the sender does not receive ACKs from all of the intended receivers of the packet, the packet must be re-multicasted, the backoff stage must be updated, and the backoff timer must be restarted. Let us denote packet delay by D. If the sender contends the channel for M counter time slots before the packet's removal from the queue, the average packet delay is

$$E[D] = E[M]T_{\rm CT}. \tag{44}$$

Table 1. Parameter values.

Parameter	Value
B	6
$W_{\min}$	16
$W_{\max}$	1024
SIFS time	16 μs
DIFS time	34 μs
Slot time	9 μs
MAC header	272 bits
PHY header	46 bits
Preamble	16 μs
ACK time	44 μs
RTS time	52 μs
CTS time	44 μs
Packet payload	8192 bits
Channel bit rate	54 Mbps
p_e	0.05
r	6

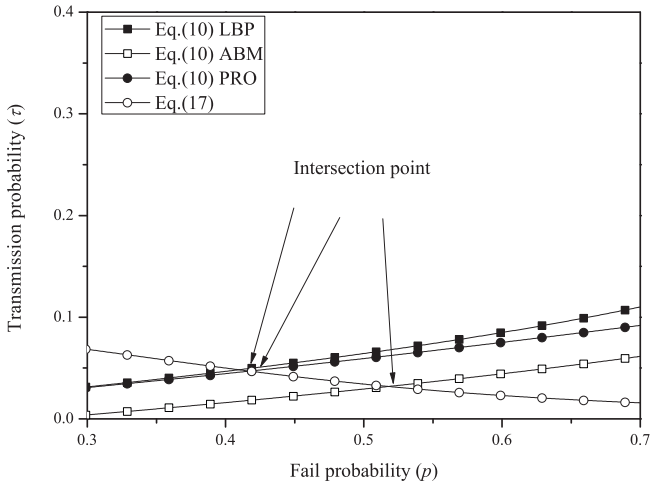

Fig. 5. Transmission probability (τ) and failure probability (p).

V. NUMERICAL RESULTS

Unless otherwise specified, the values shown in the following figures are obtained using the system parameters listed in Table 1 and are based on the OFDM physical layer used in the IEEE 802.11a standard [27].

Figs. 5 and 6 show an example of finding the failure probability (p) and the transmission probability (τ). For the sake of simplicity, we denote the proposed method as PRO. In these figures, (10) and (17) are used to find p and τ by numerical methods. In Fig. 5, the intersection points between the results of (10) and (17) are the values of p and τ obtained for each different multicast protocol in which the number of nodes in the transmission range n is set to 10. The transmission and fail probabilities of PRO are between those of LBP and ABM. While LBP checks the ACK only from a leader, ABM and the proposed method check all the ACKs from the receiver nodes. Thus, the transmission probability of LBP is higher than that of ABM and

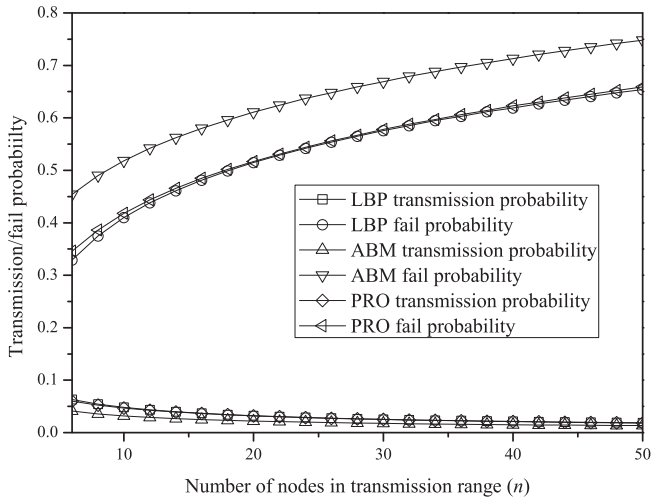

Fig. 6. Transmission probability (τ) and failure probability (p) as a function of the number of nodes.

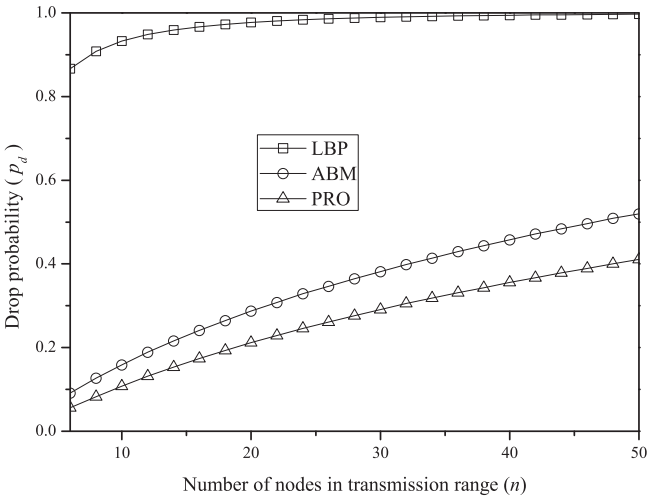

Fig. 7. Packet drop probability (p_d) as a function of the number of nodes.

the proposed method. The transmission probability of the proposed method is higher than that of ABM, because the proposed method does not check the ACKs that are confirmed in the previous backoff stage.

Fig. 6 shows all the intersection points for each value of n. p increases as the number of nodes increases, because the number of collisions increases as the number of nodes increases. On the contrary, τ decreases as the number of nodes increases. Because the number of collisions increases, nodes experience longer backoff durations, which results in a reduction of transmission probability. The failure probability of LBP is less than that of ABM and PRO. This is because transmissions in ABM and PRO succeed if ACKs from all the receivers are received correctly. Thus, the failure probability in ABM and PRO is the actual failure probability in multicast transmission. From these confirmations from all nodes, ABM and PRO can achieve reliable multicast. On the contrary, the transmission of LBP succeeds only if a leader returns ACK even if other nodes fail to return ACK. Hence, in LBP, failures during multicast packet transmission cannot be checked by the transmitter. The packets received by a leader but not received by any of the other nodes are dropped.

The packet drop probability is shown in Fig. 7. In PRO and ABM, packets are dropped because of retry limit exhaustion. In LBP, in addition to retry limit exhaustion, packets are also dropped when one of the receivers does not receive the packet even though a leader receives it. Thus, the drop probability of LBP is higher than that of ABM and PRO. In the current backoff stage, PRO is only concerned with the ACKs from the members that did not send ACKs in the previous backoff stage, and hence, the drop probability of PRO is lower than that of ABM, which is concerned with all the ACKs in every stage. The drop probability increases as the number of nodes increases because the failure probability increases as shown in Fig. 6. Because of the high drop probability, LBP does not provide reliable multicast communication. The proposed method shows the lowest drop probability, which means the highest reliability in multicast communication.

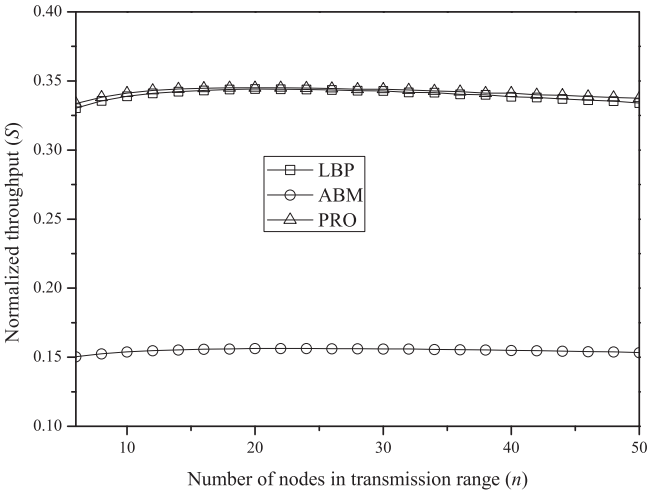

Fig. 8. Normalized throughput (S) as a function of the number of nodes.

Fig. 8 shows the system throughput mainly considering the transmission overheads. The throughput includes packet transmission whose ACKs are returned from some of the receivers rather than all of the receivers. The throughput of ABM is less than that of the other protocols because it has higher overhead due to multiple ACK packets in every transmission. LBP and PRO have similar overheads in terms of ACK. They require only one ACK for every transmission. Thus, LBP and PRO show similar throughput. Note that a portion of the throughput is not acknowledged by the receivers in LBP. ABM is inefficient in multicast communication because of the low throughput.

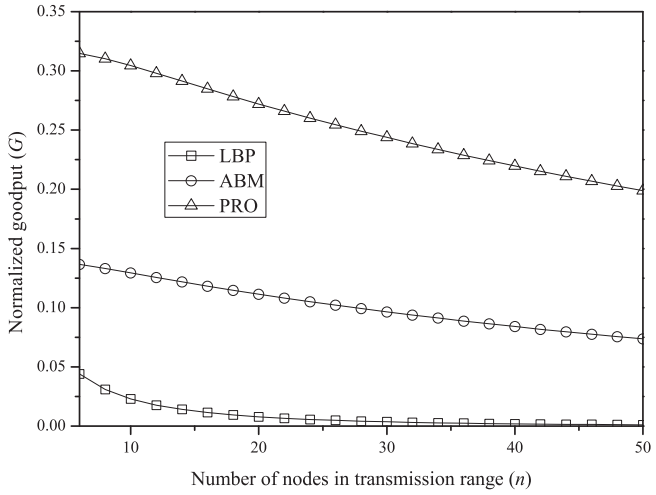

Fig. 9. Normalized goodput (G) as a function of the number of nodes.

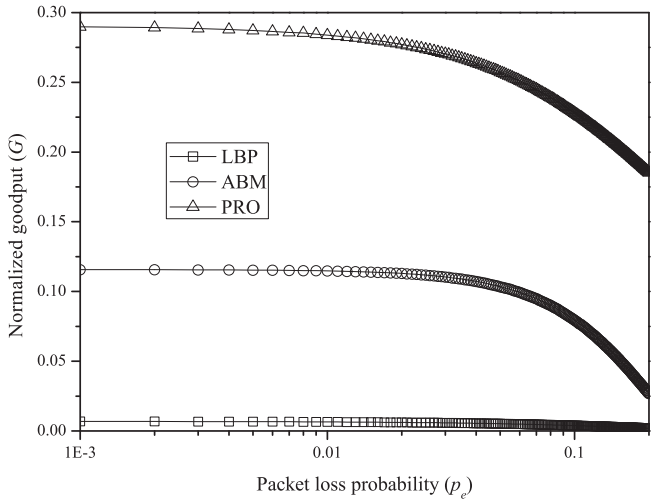

Fig. 10. Normalized goodput (G) as a function of packet loss probability.

The goodput is shown in Fig. 9. The goodput decreases as the number of nodes increases, because the probabilities of packet collision and packet error increase. The goodput of LBP is very low despite the high throughput. Because LBP only checks the ACK from a leader, most packet transmissions are not completely confirmed by other receivers. The highest goodput of the proposed method provides reliable transmission and efficient channel utilization in multicast communication.

The effect of packet loss probability on the goodput is shown in Fig. 10, in which the number of nodes in the transmission range n is set to 25. The packet loss probability depends on the time and frequency offset and the channel conditions such as shadowing and fading. The goodput decreases as the packet loss probability increases because of the increased packet loss. The proposed method achieves the highest goodput in the practical operational range. The goodput of ABM is better than that of LBP because of the same reason as seen in Fig. 9.

VI. CONCLUSION

Reliable multicast requires a certain level of overhead to guarantee successful packet transmission. We proposed a reliable multicast MAC protocol for wireless ad hoc networks. The MAC layer uses an OFDMA-based acknowledgement for RTS and data packets for the protocol design. Thus, the overhead required for reliable multicast is reduced. This reduction in the overhead enhances system goodput and reliability. The improvement in system performance is demonstrated by extensive analytical modelling and numerical results. The proposed method achieves better goodput performance in reliable multicast as compared to previous methods. The proposed method also reduces the packet drop probability in multi-hop wireless ad hoc networks. Reliable multicast services can be provided in multi-hop wireless ad hoc networks using the proposed protocol.

REFERENCES

[1] J.-S. Park, M. Gerla, D. S. Lun, Y. Yi, and M. Medard, "Codecast: A network-coding-based ad hoc multicast protocol," *IEEE Wireless Commun. Mag.*, vol. 13, no. 5, pp. 76–81, Oct. 2006.

[2] C.-W. Bao and W. Liao, "Performance analysis of reliable MAC-layer multicast for IEEE 802.11 wireless LANs," in *Proc. IEEE ICC*, May 2005, pp. 1378–1382.

[3] H. Gossain, N. Nandiraju, K. Anand, and D. P. Agrawal, "Supporting MAC layer multicast in IEEE 802.11 based MANETs: Issues and solutions," in *Proc. IEEE LCN*, Nov. 2004, pp. 172–179.

[4] M.-T. Sun, L. Huang, A. Arora, and T.-H. Lai, "Reliable MAC layer multicast in IEEE 802.11 wireless networks," *Wireless Commun. Mobile Comput.*, vol. 3, no. 4, pp. 439–453, June 2003.

[5] ——, "Reliable MAC layer multicast in IEEE 802.11 wireless networks," in *Proc. IEEE ICPP*, Aug. 2002, pp. 527–536.

[6] D. Towsley, J. Kurose, and S. Pingali, "A comparison of sender-initiated and receiver-initiated reliable multicast protocols," *IEEE J. Sel. Areas Commun.*, vol. 15, no. 3, pp. 398–406, Apr. 1997.

[7] J. Kuri and S. K. Kasera, "Reliable multicast in multi-access wireless LANs," *ACM Wireless Netw.*, vol. 7, no. 4, pp. 359–369, Aug. 2001.

[8] B.-S. Kim, S. W. Kim, and R. L. Ekl, "OFDMA-based reliable multicasting MAC protocol for WLANs," *IEEE Trans. Veh. Technol.*, pp. 3136–3145, Sept. 2008.

[9] IEEE Std 802.11: 1999(E), "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," Aug. 1999.

[10] S. Gupta, V. Shankar, and S. Lalwani, "Reliable multicast MAC protocol for wireless LANs," in *Proc. IEEE ICC*, vol. 1, May 2003, pp. 93–97.

[11] Z. Li and T. Herfet, "BLBP: A beacon-driven leader based protocol for MAC layer multicast error control in wireless LANs," in *Proc. WiCOM*, Oct. 2008, pp. 1–4.

[12] ——, "MAC layer multicast error control for IPTV in wireless LANs," *IEEE Trans. Broadcast.*, vol. 55, no. 2, pp. 353–362, June 2009.

[13] D. Duiovne and T. Turletti, "Multicast in 802.11 WLANs: An experimental study," in *Proc. ACM MSWiM*, Terromolinos, Spain, Oct. 2006, pp. 130–138.

[14] H. Karl and A. Willig, *Protocols and architectures for wireless sensor networks*. Wiley, 2005.

[15] Z. Cao, U. Tureli, and Y.-D. Yao, "Deterministic multiuser carrier-frequency offset estimation for interleaved OFDMA uplink," *IEEE Trans. Commun.*, vol. 52, no. 9, pp. 1585–1594, Sept. 2004.

[16] S. Kaiser and W. A. Krzymien, "Performance effects of the uplink asynchronism in a spread spectrum multicarrier multiple access system," *European Trans. Commun.*, vol. 10, no. 4, pp. 399–406, 1999.

[17] S. Kapoor, D. J. Marchok, and Y. F. Huang, "Adaptive interference suppression in multiuser wireless OFDM system using antenna arrays," *IEEE Trans. Signal Process.*, vol. 47, pp. 3381–3391, Dec. 1999.

[18] X. Fu and H. Minn, "TDMA-type preamble for low complexity multi-user synchronization in OFDMA uplink," in *Proc. IEEE VTC Fall*, vol. 2, Sept. 2005, pp. 1093–1097.
[19] V. P. G. Jimenez and A. G. Armada, "Multi-user synchronisation in ad hoc OFDM-based wireless personal area networks," *Wireless Personal Commun.*, vol. 40, no. 3, pp. 387–399, Feb. 2007.
[20] H. Aiache *et al.*, "WIDENS: Advanced wireless ad-hoc networks for public safety," in *Proc. IST Mobile & Wireless Commun. Summit*, June 2005.
[21] M. Morelli, C.-C. J. Kuo, and M.-O. Pun, "Synchronization techniques for orthogonal frequency division multiple access (OFDMA): A tutorial review," *Proc. IEEE*, vol. 95, no. 7, pp. 1394–1427, July 2007.
[22] M. Morelli, "Timing and frequency synchronization for the uplink of an OFDMA system," *IEEE Trans. Commun.*, vol. 52, no. 2, pp. 296–306, Feb. 2004.
[23] M. Konstantinos, A. Adamis, and P. Constaninou, "SNR degradation due to timing and frequency synchronization errors for OFDMA systems with subband carrier allocation," in *Proc. European Wireless Conf.*, Prague, Czech Republic, June 2008, pp. 1–6.
[24] S. W. Kim, B. Kim, and Y. Fang, "Downlink and uplink resource allocation in IEEE 802.11 wireless LANs," *IEEE Trans. Veh. Technol.*, vol. 54, no. 1, pp. 320–327, Jan. 2005.
[25] T.-C. Hou, L.-F. Tsao, and H.-C. Liu, "Analyzing the throughput of IEEE 802.11 DCF scheme with hidden nodes," in *Proc. IEEE VTC*, Oct. 2003, pp. 2870–2874.
[26] G. Bianchi and I. Tinnirello, "Remarks on IEEE 802.11 DCF performance analysis," *IEEE Commun. Lett.*, vol. 9, no. 8, pp. 765–767, Aug. 2005.
[27] IEEE Std 802.11a-1999, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher-speed physical layer in the 5 GHz band", Sept. 1999.

Sung Won Kim received the B.S. and M.S. degrees from the Department of Control and Instrumentation Engineering, Seoul National University, Korea, in 1990 and 1992, respectively, the Ph.D. degree from the School of Electrical Engineering and Computer Sciences, Seoul National University, Korea, in August 2002. From January 1992 to August 2001, he was a Researcher at the Research and Development Center of LG Electronics, Korea. From August 2001 to August 2003, he was a Researcher at the Research and Development Center of AL Tech, Korea. From August 2003 to February 2005, he was a Postdoctoral Researcher in the Department of Electrical and Computer Engineering, University of Florida, Gainesville, USA. In March 2005, he joined the Department of Information and Communication Engineering, Yeungnam University, Gyeongsangbuk-do, Korea, where he is currently an Associate Professor. His research interests include resource management, wireless networks, mobile networks, performance evaluation, and embedded system.

Byung-Seo Kim received his B.S. degree in Electrical Engineering from In-Ha University, In-Chon, Korea in 1998 and his M.S. and Ph.D. degrees in Electrical and Computer Engineering from the University of Florida in 2001 and 2004, respectively. His Ph.D. study was supervised by Dr. Fang. Between 1997 and 1999, he worked for Motorola Korea Ltd., PaJu, Korea as a Computer Integrated Manufacturing (CIM) Engineer in Advanced Technology Research and Development (ATR&D). From January 2005 to August 2007, he worked for Motorola Inc., Schaumburg Illinois, as a Senior Software Engineer in Networks and Enterprises. His research focuses in Motorola Inc. were designing protocol and network architecture of wireless mission critical communications. Since September 2007, he has been an Assistant Professor at the Department of Computer and Information Communication Engineering in HongIk University, Korea. His research interests include the design and development of efficient link-adaptable MAC protocols, cross layer architectures, multi-MAC structures, and resource allocation algorithms for wireless networks.

Inkyu Lee received the B.S. degree (Hon.) in Control and Instrumentation Engineering from Seoul National University, Seoul, Korea, in 1990, and the M.S. and Ph.D. degrees in Electrical Engineering from Stanford University, Stanford, CA, in 1992 and 1995, respectively. From 1995 to 2001, he was a Member of Technical Staff at Bell Laboratories, Lucent Technologies, where he conducted research on high-speed wireless system designs. He later worked for Agere Systems (formerly Microelectronics Group of Lucent Technologies), Murray Hill, NJ, as a Distinguished Member of Technical Staff from 2001 to 2002. In September 2002, he joined the faculty of Korea University, Seoul, Korea, where he is currently a Professor in the School of Electrical Engineering. During 2009, he visited University of Southern California, LA, USA, as a Visiting Professor. He has published around 70 journal papers in IEEE, and has 30 U.S. patents granted or pending. His research interests include digital communications and signal processing techniques applied for next generation wireless systems. He currently serves as an Associate Editor for IEEE Transactions on Communications and the IEEE Transactions on Wireless Communications. Also, he has been a Chief Guest Editor for the IEEE Journal on Selected Areas in Communicatins (Special Issue on 4G Wireless Systems). He received the IT Young Engineer Award as the IEEE/IEEK joint award in 2006, and received the Best Paper Award at APCC in 2006 and IEEE VTC in 2009. Also he was a recipient of the Hae-Dong Best Research Award of the Korea Information and Communications Society (KICS) in 2011.