N° d'ordre: 4926

THÈSE

Présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET D'INFORMATIQUE

Par **Yousri Daldoul**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : INFORMATIQUE

Transport Multicast fiable de la vidéo sur le réseau WiFi

Reliable Multicast transport of the video over the WiFi network

Soutenue le : 29 Novembre 2013

Devant la commission d'examen composée de :

M. AHMED Toufik	Professeur, ENSEIRB-MATMECA – IPB	Directeur de thèse
M. CHAUMETTE Serge	Professeur, Université Bordeaux 1	Président du jury
M. GAYRAUD Thierry	Professeur, Université Paul Sabatier	Rapporteur
M. MEDDOUR Djamal-Eddine	Responsable R&D, Orange Labs	Examinateur
M. SENOUCI Sidi Mohamed	Professeur, Université de Bourgogne	Rapporteur

Abstract

The multicast transport is an efficient solution to deliver the same content to many receivers at the same time. This mode is mainly used to deliver real-time video streams. However, the conventional multicast transmissions of IEEE 802.11 do not use any feedback policy. Therefore missing packets are definitely lost. This limits the reliability of the multicast transport and impacts the quality of the video applications. To resolve this issue, the IEEE 802.11v/aa amendments have been defined recently. The former proposes the Direct Multicast Service (DMS). On the other hand, 802.11aa introduces Groupcast with Retries (GCR) service. GCR defines two retry policies: Block Ack (BACK) and Unsolicited Retry (UR).

In this thesis we evaluate and compare the performance of 802.11v/aa. Our simulation results show that all the defined policies incur an important overhead. Besides, DMS has a very limited scalability, and GCR-BACK is not appropriate for large multicast groups. We show that both DMS and GCR-BACK incur important transmission latencies when the number of the multicast receivers increases. Furthermore, we investigate the loss factors in wireless networks. We show that the device unavailability may be the principal cause of the important packet losses and their bursty nature. Particularly, our results show that the CPU overload may incur a loss rate of 100%, and that the delivery ratio may be limited to 35% when the device is in the power save mode.

To avoid the collisions and to enhance the reliability of the multicast transmissions, we define the Busy Symbol (BS) mechanism. Our results show that BS prevents all the collisions and ensures a very high delivery ratio for the multicast packets. To further enhance the reliability of this traffic, we define the Block Negative Acknowledgement (BNAK) retry policy. Using our protocol, the AP transmits a block of multicast packets followed by a Block NAK Request (BNR). Upon reception of a BNR, a multicast member generates a Block NAK Response (BNAK) only if it missed some packets. A BNAK is transmitted after channel contention in order to avoid any eventual collision with other feedbacks, and is acknowledged. Under the assumption that 1) the receiver is located within the coverage area of the used data rate, 2) the collisions are avoided and 3) the terminal has the required configuration, few feedbacks are generated and the bandwidth is saved. Our results show that BNAK has a very high scalability and incurs very low delays. Furthermore, we define a rate adaptation scheme for BNAK. We show that the appropriate rate is selected on the expense of a very limited overhead of less than 1%. Besides, the conception of our protocol is defined to support the scalable video streaming. This capability intends to resolve the bandwidth fluctuation issue and to consider the device heterogeneity of the group members.

Keywords: IEEE 802.11 multicast transport; 802.11aa evaluation; 802.11v evaluation; Loss diagnosis; Device unavailability; Busy Symbol; BS; Reliable multicast protocol; Block Negative Acknowledgement; BNAK; Rate adaptation; Assisted Rate Adaptation; ARA

Résumé

Le transport multicast est une solution efficace pour envoyer le même contenu à plusieurs récepteurs en même temps. Ce mode est principalement utilisé pour fournir des flux multimédia en temps réel. Cependant, le multicast classique de l'IEEE 802.11 n'utilise aucun mécanisme d'acquittement. Ainsi, l'échec de réception implique la perte définitive du paquet. Cela limite la fiabilité du transport multicast et impact la qualité des applications vidéo. Pour résoudre ce problème, 802.11v et 802.11aa sont définis récemment. Le premier amendement propose Direct Multicast Service (DMS). D'autre part, le 802.11aa introduit GroupCast with Retries (GCR). GCR définit deux nouvelles politiques de retransmission : Block Ack (BACK) et Unsolicited Retry (UR).

Dans cette thèse, nous évaluons et comparons les performances de 802.11v/aa. Nos résultats montrent que tous les nouveaux protocoles multicast génèrent un overhead de transmission important. En outre, DMS a une scalabilité très limitée, et GCR-BACK n'est pas approprié pour des grands groupes multicast. D'autre part, nous montrons que DMS et GCR-BACK génèrent des latences de transmission importantes lorsque le nombre de récepteurs augmente. Par ailleurs, nous étudions les facteurs de pertes dans les réseaux sans fil. Nous montrons que l'indisponibilité du récepteur peut être la cause principale des pertes importantes et de leur nature en rafales. En particulier, nos résultats montrent que la surcharge du processeur peut provoquer un taux de perte de 100%, et que le pourcentage de livraison peut être limité à 35% lorsque la carte 802.11 est en mode d'économie d'énergie.

Pour éviter les collisions et améliorer la fiabilité du transport multicast, nous définissons le mécanisme Busy Symbol (BS). Nos résultats montrent que BS évite les collisions et assure un taux de succès de transmission très important. Afin d'améliorer davantage la fiabilité du trafic multicast, nous définissons un nouveau protocole multicast, appelé Block Negative Acknowledgement (BNAK). Ce protocole opère comme suit. L'AP envoi un bloc de paquets suivi par un Block NAK Request (BNR). Le BNR permet aux membres de détecter les données manquantes et d'envoyer une demande de retransmission, c.à.d. un Block NAK Response (BNAK). Un BNAK est transmis en utilisant la procédure classique d'accès au canal afin d'éviter toute collision avec d'autres paquets. En plus, cette demande est acquittée. Sous l'hypothèse que 1) le récepteur est situé dans la zone de couverture du débit de transmission utilisé, 2) les collisions sont évitées et 3) le terminal a la bonne configuration, très peu de demandes de retransmission sont envoyées, et la bande passante est préservée. Nos résultats montrent que BNAK a une très grande scalabilité et génère des délais très limités. En outre, nous définissons un algorithme d'adaptation de débit pour BNAK. Nous montrons que le bon débit de transmission est sélectionné moyennant un overhead très réduit de moins de 1%. En plus, la conception de notre protocole supporte la diffusion scalable de la vidéo. Cette caractéristique vise à résoudre la problématique de la fluctuation de la bande passante, et à prendre en considération l'hétérogénéité des récepteurs dans un réseau sans fil.

Mots-clès : transport multicast sur le réseau IEEE 802.11 ; évaluation du 802.11v ; évaluation du 802.11aa ; diagnostique des pertes ; non-disponibilité du récepteur ; Busy Symbol ; BS ; transport multicast fiable ; Block Negative Acknowledgement ; BNAK ; adaptation du débit ; ARA

Résumé (long)

De nos jours, les applications multimédia sont largement déployées sur Internet et sur des réseaux locaux et privés. Elles sont utilisées pour fournir de nombreux services, tels que l'apprentissage, la publicité, la vidéo surveillance, la vidéo conférence, etc. Le transport multicast est un mode principal de la diffusion d'un contenu vidéo. Il permet d'offrir le même contenu à plusieurs récepteurs en même temps, et permet à une seule source de servir des millions de clients partout dans le monde en utilisant une bande passante limitée. Ainsi, le multicast est une solution intéressante pour de nombreuses applications, telles que l'IPTV. Cependant, un trafic multicast est livré sur UDP pour deux raisons principales. 1) L'utilisation d'une politique d'acquittement, similaire à celle utilisée par TCP, amène à l'implosion des acquittements et limite l'évolutivité de transport multicast. 2) Les paquets retransmis peuvent arriver avec des retards importants en fonction de la distance entre le serveur et le client. Par conséquent, ils peuvent être rejetés par le récepteur lui-même. Par ailleurs, un contenu vidéo est tolérant aux pertes ; si un paquet est perdu, une fluctuation temporelle de la qualité est aperçue, mais la diffusion ne s'arrête pas. Par conséquent, la fiabilité et la qualité d'un flux multicast dépendent principalement de la fiabilité du chemin parcourus. Dans les réseaux filaires, le taux de perte est très limitée parce que les collisions sont détectables et sont évitées. En outre, les paquets sont toujours reçus avec une puissance de signal appropriée. Par conséquent, le transport de multicast sur ces réseaux a une haute fiabilité et offre une bonne qualité pour les services multimédia.

D'autre part, les réseaux IEEE 802.11 sont déployés partout et assurent un transport unicast fiable. En outre, ils offrent une communication à haut débit. Cette capacité permet au WLAN de supporter les flux haut débit tels que le trafic multimédia. En plus, le standard définit des services différenciés afin de garantir une faible latence pour les applications sensibles au délai. Dans un réseau sans fil, un paquet peut être perdu pour plusieurs raisons : affaiblissement du signal, collisions, interférences, etc. Par conséquent, le 802.11 définit une politique d'acquittement pour les transmissions unicast afin de détecter et de retransmettre les paquets manquants. En outre, le standard définit plusieurs débits de données avec différents degrés de robustesse contre l'atténuation du signal. Par conséquent, les nœuds communiquant profitent des accusés de réception pour estimer la qualité de la liaison radio et pour sélectionner le débit de données le plus approprié. Cela garantit une utilisation optimale de la bande passante. Toutefois, la procédure de transmission classique du multicast n'utilise aucun mécanisme d'acquittement. Par conséquent, les paquets manquants sont définitivement perdus. Le flux multicast est livré par défaut au débit le plus faible. C'est parce que l'emetteur n'a aucune idée de la qualité de la liaison descendante vers les membres du groupe multicast. Le débit le plus bas est le plus robuste et a la plus grande zone de couverture. Par conséquent, il permet aux paquets multicast d'atteindre tous les récepteurs dans la zone de couverture de l'émetteur. Cependant, l'utilisation de ce débit de transmission limite le débit du réseau de manière significative, augmente la probabilité de congestion et peut conduire à une suppression fréquente des paquets.

Afin d’améliorer la fiabilité des transmissions multicast sur les réseaux sans fil, les amendements 802.11v/aa sont définis récemment. Le premier introduit Direct Multicast Service (DMS) tandis que le second présente le service Groupcast with Retries (GCR). DMS convertit un trafic multicast en plusieurs flux unicast. Par conséquent, DMS tire profit de la fiabilité du transport unicast au détriment de la bande passante. En outre, les retards de livraison de DMS augmentent avec l'augmentation du nombre de récepteurs multicast. D'autre part, GCR définit deux politiques de retransmission: Block Ack (BACK) et Unsolicited Retry (UR). La première politique nécessite la mise en place d'un accord GCR-BACK avec les membres du groupe, puis la transmission des paquets en bloc suivie par des échanges multiples de Block Ack Request (BAR) / BACK entre le point d'accès (AP) et les récepteurs multicast. Ces acquittements ont besoin d'un temps de transmission supplémentaire qui dépend de la taille du groupe. Cela limite l'évolutivité et le débit de GCR-BACK, et provoque des retards de retransmission. En outre, GCR-UR nécessite la transmission des paquets multicast plusieurs fois afin d'augmenter la probabilité de la réussite des transmissions. Cette politique conserve la scalabilité puisque l’en-tête du protocole ne dépend pas de la taille du groupe. Cependant, la redondance de transmission limite l'efficacité de GCR-UR significativement. Nous notons que peu de travaux ont étudié et comparé la performance de 802.11v/aa, mais aucun d'eux n'a été en mesure de fournir une évaluation complète de tous les paramètres pertinents (càd débit, délai et scalabilité).

En plus de 802.11v/aa, de nombreuses autres propositions sont définis afin d'améliorer la fiabilité du transport multicast. La plupart d'entre eux peuvent être classés en trois catégories: ACK, ACK négatif (NAK) et pseudo-broadcast. Le principe de la première catégorie est héritée de la politique d’acquittement de l’unicast, et nécessite que chaque récepteur multicast envoi un acquittement. Cependant, les protocoles appartenant à cette catégorie provoquent une surcharge importante qui dépend de la taille du groupe. Cela limite l'évolutivité de ces propositions de manière significative.

Les protocoles basés sur les NAK reposent sur le choix d'un chef de groupe qui doit acquitter chaque paquet. D'autre part, les autres membres sont autorisés à envoyer un NAK au cas d’échec de réception. Ce NAK a l'intention de prévenir la bonne réception de l'accusé de réception envoyé par le chef du groupe. Une fois que l’ACK est manquant, l’émetteur retransmet le paquet multicast perdu. Le principe du NAK nécessite un seul temps d’acquittement, que ce soit pour envoyer un ACK ou un NAK. Cela limite la surcharge de transmission et conserve l'évolutivité du protocole. Mais ce concept n'est pas conforme avec la norme 802.11 qui repose sur la prévention des collisions. Par ailleurs, le principe du NAK ne fournit pas une solution efficace car il a été prouvé que la transmission simultanée de deux paquets ne conduit pas nécessairement à la perte des deux. Par conséquent, l'accusé de réception du chef peut être reçu même si un NAK est transmis. Une autre limite de ces protocoles est que chaque paquet doit être acquitté séparément des autres. Par conséquent, ces protocoles ne peuvent ni être utilisés avec le transfert en bloc ni avec l'agrégation des paquets de la norme 802.11n. En outre, ils sont vulnérables à la question de la non-disponibilité du récepteur: si un paquet est perdu à cause de cette non-disponibilité, le récepteur ne peut pas envoyer un NAK et le paquet est définitivement perdu.

L'idée principale des protocoles de type pseudo-broadcast est de choisir un membre pour envoyer les acquittements après la bonne réception de chaque paquet multicast. Toutefois, les autres membres ne peuvent envoyer aucune notification. Ainsi, ces protocoles sont évolutives et conformes à la norme, mais ils ne sont pas totalement fiables. En outre, ils ne permettent pas au point d'accès de sélectionner le débit de transmission le plus approprié, car l'émetteur est conscient uniquement de la qualité du lien radio avec le chef du groupe multicast. Cela conduit l'AP à sélectionner le débit de transmission le plus bas qui réduit le débit du réseau.

Ainsi aucune des solutions existantes n'est capable de 1) résoudre le problème de manque de fiabilité, 2) maintenir l'évolutivité et 3) maintenir la conformité à la norme 802.11 en même temps.

Une alternative efficace pour améliorer la fiabilité du flux multicast sur les réseaux 802.11 est de prévenir les pertes de paquets. Par conséquent, il est nécessaire d'identifier les facteurs de perte et de définir les actions de prévention nécessaires. De nombreux travaux ont évalué les problèmes de transmission sur les réseaux sans fil. Ils ont classé les causes des pertes dans les catégories suivantes: affaiblissement du signale, collisions, interférences, effet multi-trajet et le débordement de la file d'attente. Plusieurs diagnostics ont remarqué que le taux de livraison des paquets peut parfois être très faible, et que les récepteurs peuvent subir des pertes en rafale. D'autres recherches, cependant, ont montré que les récepteurs avec le même état de réception peuvent rencontrer des taux de perte complètement éloignés. Mais aucune de ces études n'a identifiée les facteurs de perte en rafale et du taux de perte extrêmement élevé qui peut être rencontré par un équipement avec un bon état de réception.

Dans cette thèse, nous introduisons les nouvelles fonctionnalités de 802.11v/aa. On définit ensuite un modèle analytique pour déterminer le débit sous différentes valeurs de: taille du groupe, taille du bloc, longueur du paquet, fréquence de transmission et taux de perte. De plus, nous évaluons la performance de DMS, GCR-BACK et GCR-UR en utilisant NS-3. Nous comparons les résultats d'analyse avec les résultats de simulation, et nous montrons que notre modèle a une très bonne précision. Les résultats obtenus démontrent que DMS a l'évolutivité la plus faible et entraîne des retards importants. En outre, nous montrons que GCR-BACK n'est pas approprié pour les grands groupes multicast. Egalement, les retards de retransmission de ce protocole augmentent de façon significative avec l'augmentation de la taille du groupe multicast. Nous démontrons que GCR-UR conserve l'évolutivité du transport multicast, mais nécessite une surcharge importante et réduit le débit du réseau de manière significative.

Par ailleurs, nous étudions les facteurs de perte dans le réseau local sans fil. Le principal objectif du diagnostic de perte est de trouver la réponse à la question suivante: pourquoi les récepteurs au même endroit et dans les mêmes conditions de réception peuvent rencontrer des taux de perte différents et des pertes en rafale? Il est à noter que si les pertes en rafales sont dues au canal sans fil, même le mode unicast devient non fiable. C'est parce qu'un paquet et ses retransmissions peuvent être perdues au sein du même block. Cela jette un doute sur la fiabilité du transport unicast de 802.11. Ainsi nous réalisons un diagnostic de l'équipement de communication afin de fournir une réponse aux taux de pertes injustifiés, et parfois excessive, et de prouver que les pertes en rafale ne sont pas liés au support sans fil. Par conséquent, nous identifions la problématique de la non-disponibilité de l'appareil et nous montrons que le récepteur lui-même peut être responsable du taux de perte élevé. En particulier, nous montrons que la surcharge du processeur peut conduire à un taux de perte de 100%, et que le rapport de livraison peut tomber à 35% lorsque le récepteur est en mode d'économie d'énergie. Nos résultats montrent qu'un récepteur avec une configuration appropriée peut subir un taux de perte très faible de moins de 0,05% en l'absence de collisions.

Pour protéger les paquets multicast contre les collisions, nous définissons une nouvelle procédure de transmission basée sur la transmission d'un signal OFDM court, appelé Busy Symbol (BS), avant d'envoyer le paquet lui-même. Le principe de BS est d'occuper brièvement le canal, de sorte que les stations rivales, qui sont à l'écoute du canal, différent leurs transmissions. Par conséquent, si aucun émetteur n'a commencé la transmission simultanément avec le BS, ce symbole va permettre de libérer le canal de tout accès pendant une période de temps au moins égale à DIFS après la fin de la transmission du BS. Ce délai permet à l'AP de transmettre le paquet multicast sans collision.

Après la fin de la transmission du BS, l'AP écoute le canal. Si le support de transmission est déterminé comme étant inactif pendant une durée égale à SlotTime moins la durée du BS, alors le point d'accès commence à transmettre le paquet multicast. Dans le cas contraire, le point d'accès commence à recevoir le paquet entrant (le paquet qui provoquerait une collision si aucun mécanisme de protection n'a été utilisé) et diffère la transmission multicast. Lors de la prochaine tentative de transmission du paquet multicast, l'AP augmente sa Contention Window (CW) et génère un nouveau Backoff time. L'augmentation de la CW a pour but de réduire la probabilité de collision lors de la prochaine tentative d'accès, et de garantir un partage équitable du canal entre les trafics unicast et multicast.

Nous notons qu'un paquet OFDM est une séquence de symboles OFDM séparées par des intervalles de garde. Par conséquent, l'ajout d'un nouveau symbole OFDM (c'est à dire la BS), séparées par un intervalle plus long à partir du premier symbole du paquet (c'est à dire SlotTime moins la durée du BS), est facile à implémenter. En outre, le BS est un symbole OFDM standard. Par conséquent, tout récepteur est capable de le détecter. Si un récepteur manque le BS, cela signifie que ce récepteur n'est pas à l'écoute du canal et n'a aucune transmission à réaliser. Dans ce cas, ce récepteur ne causera pas de collision au paquet multicast. Notre mécanisme de protection est conforme à toutes les couches physiques de 802.11 et assure donc la protection des paquets multicast envoyés avec tous les débits de transmission disponibles.

Nous évaluons notre procédure de transmission en utilisant Network Simulator 3, et nous montrons que le mécanisme proposé assure une protection parfaite contre les collisions. En outre, nous démontrons que le BS représente une surcharge très limitée. De plus, ce mécanisme est facile à installer et ne nécessite aucune modification, sauf au niveau de l'AP.

Même si le flux multicast est protégé contre les collisions, une politique de notification est toujours nécessaire. En effet, BS ne permet pas à lui seul le point d'accès de déterminer le débit de transmission approprié. Par conséquent, nous définissons un nouveau protocole multicast appelé Block Negative Acknowledgement (BNAK). Notre protocole repose sur le principe que le taux de perte dans les réseaux sans fil est très limité sous les hypothèses suivantes: 1) les récepteurs sont situés dans la zone de couverture de l'émetteur, 2) les paquets sont envoyés en utilisant un débit de transmission approprié, 3) les collisions sont évitées, et 4) l'appareil a la configuration appropriée. Par conséquent, il est plus approprié pour l'AP de demander des réponses à des membres qui ont subi des pertes, au lieu de demander l'acquittement de tous les récepteurs. En utilisant BNAK, les paquets sont transmis en bloc suivi par un Block NAK Request (BNR). Seuls les utilisateurs ayant des pertes sont invités à envoyer une demande de retransmission. Par conséquent, si tous les paquets sont transmis correctement, aucun BNAK n'est envoyé et la bande passante est économisée. Si une perte se produit, seuls les récepteurs concernés sont autorisés à envoyer une notification. Afin de garantir une livraison fiable des acquittements, ces paquets sont transmis après un temps de Backoff et sont confirmés par l'AP.

En plus de la procédure de transmission de BNAK, nous définissons une nouvelle fonctionnalité de gestion des membres du groupe qui considère que seulement l'AP doit recueillir des informations sur les membres du groupe. Par conséquent, un membre multicast n'a pas besoin d'effectuer l'analyse syntaxique (snooping) de tous les paquets au niveau de la couche MAC. Cela minimise les besoins du client et simplifie le déploiement de notre protocole. Quand un client se joint à un service multicast, l'AP est responsable de notifier la couche MAC du membre. Ainsi, le client tire profit de la fiabilité de BNAK. De même, lorsque le client quitte le groupe, le point d'accès envoie un message à la couche MAC du membre afin de retirer cette station du groupe.

Nous évaluons notre protocole BNAK analytiquement et par simulation. Les résultats montrent que le modèle analytique a une précision élevée et offre une très bonne estimation du débit en fonction des paramètres suivants: taille du paquet, taille du groupe, taille du bloc, débit de transmission et taux de perte. En outre, les résultats de simulation prouvent que notre protocole est fiable et efficace, et surpasse 802.11v/aa significativement. Egalement, nous montrons que l'évolutivité de BNAK est presque illimitée. En outre, notre protocole est conforme à tous les amendements du 802.11, et nécessite des mises à jour logicielles seulement afin de fonctionner avec les équipements actuels.

En outre, nous définissons un nouvel algorithme d'adaptation de débit pour BNAK. Nous montrons que la sélection du débit de transmission approprié nécessite un surcoût très limité de moins de 1%. Aussi, nous introduisons la capacité de diffusion d'une vidéo en couches et nous montrons que notre protocole est approprié pour traiter avec les deux caractéristiques suivantes du WLAN: fluctuation de la bande passante et hétérogénéité des récepteurs. Durant les périodes de congestions, le point d'accès est autorisé à sélectionner un débit de transmission plus élevé pour le flux de la couche d'amélioration afin d'éviter le débordement de la file d'attente. Cependant, indépendamment de la charge du réseau, les couches de base et d'amélioration sont livrées de manière fiable aux membres éligibles.

Le reste de cette thèse est organisé comme suit. Dans chapitre 1, nous introduisons le contexte, les enjeux et les contributions. Chapitre 2 présente l'état de l'art. Au début de ce chapitre, nous présentons les protocoles de streaming et les techniques principales d'adaptation du débit de la vidéo. Ensuite, nous donnons un aperçu des réseaux 802.11 et nous présentons les caractéristiques les plus pertinentes des couches PHY et MAC. En outre, nous présentons des protocoles multicast de l'état de l'art, et nous mettons en évidence leurs limites.

Nous consacrons chapitre 3 à l'évaluation de la performance des amendments 802.11v/aa. Ainsi, nous présentons les fonctionnalités les plus pertinentes et nous décrivons plus en détail le mode de fonctionnement de DMS, GCR-BACK et GCR-UR. Ensuite, nous comparons le débit, la fiabilité, l'évolutivité et les délais de transmission de ces protocoles.

Nous étudions les facteurs de perte dans le chapitre 4. Par conséquent, nous donnons des mesures empiriques de l'impact du mode d'économie d'énergie et du débordement du CPU sur le taux de perte des paquets multicast. En outre, nous évaluons par des simulations l'impact des collisions et de l'affaiblissement du signal sur la fiabilité de la procédure classique de transmission multicast. En plus, nous introduisons le mécanisme BS et nous fournissons des résultats de simulation de la performance et de l'efficacité de ce dispositif de protection.

Dans chapitre 5, nous présentons BNAK et la fonction de détection de l'appartenance au groupe. Nous présentons les différentes politiques de retransmission de notre protocole et nous décrivons le mode de fonctionnement plus en détails. Egalement, nous illustrons le format de paquets BNR et BNAK. Ensuite, nous présentons notre modèle analytique et nous fournissons les analyses et les résultats de simulation.

Chapitre 6 présente le schéma d'adaptation de débit et la capacité de diffusion d'une video en couches de BNAK. En outre, nous présentons les résultats de simulation de la performance de notre protocole.

Dans chapitre 7, nous concluons cette thèse et nous fournissons quelques perspectives pour des travaux futurs dans le cadre de ce domaine de recherche.

Table of Contents

List of Figures

List of Tables

Publications

Yousri Daldoul, Toufik Ahmed, Djamal-Eddine Meddour, “*An Analytical Comparison of the Block NAK Protocol and the IEEE 802.11aa Feedback Policy for a Reliable Multicast Transport in the WLAN*,” in the 18th IEEE Symposium on Computers and Communications (ISCC) 2013. 7–10 July 2013, Split, Croatia.

Yousri Daldoul, Djamal-Eddine Meddour, Toufik Ahmed, “*A Collision Prevention Mechanism for the Multicast Transport in IEEE 802.11 Networks*,” in the 18th IEEE Symposium on Computers and Communications (ISCC) 2013. 7–10 July 2013, Split, Croatia.

Yousri Daldoul, Djamal-Eddine Meddour, Toufik Ahmed, “*A Study of the DMS Service Scalability for the Multicast Delivery over the IEEE 802.11 Networks*,” in Nouvelles Technologies de la Répartition/ Colloque francophone sur l’ingénierie des protocols (NOTERE/CFIP) 2012. 29–31 October 2012, Anglet, France.

Yousri Daldoul, Djamal-Eddine Meddour, Toufik Ahmed, “*A New Design of the IEEE 802.11 MAC Layer to Enhance the Scalability of the DMS Service*,” in the 37th IEEE Conference on Local Computer Networks (LCN) 2012. 22–25 October 2012, Clearwater, Florida, USA.

Yousri Daldoul, Djamal-Eddine Meddour, Toufik Ahmed, “*An LTE-based Hybrid Architecture to support a Reliable IEEE 802.11n Multicast Transport*,” in the 9th IEEE Consumer Communications and Networking Conference (CCNC) 2012. 14–17 January 2012, Las Vegas, Nevada, USA.

Yousri Daldoul, Toufik Ahmed, Djamal-Eddine Meddour, “*IEEE 802.11n aggregation performance study for the multicast*,” in the 4th IFIP Wireless Days (WD) 2011. 10–12 October 2011, Niagara Falls, Canada.

Yousri Daldoul, Djamal-Eddine Meddour, Toufik Ahmed, “*The Impact of the Reliability on the Fairness Between the Unicast and the Multicast in Highly Loaded WLANs*,” in the 36th IEEE Conference on Local Computer Networks (LCN) 2011. 4–7 October 2011, Bonn, Germany.

Yousri Daldoul, Djamal-Eddine Meddour, Toufik Ahmed, “*A Reliable PLCP-based Multicast Protocol for IEEE 802.11 WLAN*,” in the 3rd IEEE Global Information Infrastructure Symposium (GIIS) 2011. 4–6 August 2011, Da Nang, Vietnam.

Chapter 1

1 Introduction

Nowadays, the multimedia applications are widely deployed over the Internet and over local and private networks. They are used to provide many services, such as learning, advertisement, video surveillance, conference, etc. The multicast transport is a principal mode for the video streaming. It delivers the same content to many receivers simultaneously, and allows one single source to serve millions of clients around the world. Thus, the multicast streaming is an attractive solution for many applications, such as IPTV. However, multicast traffic is delivered over UDP for two main reasons. 1) The use of an acknowledgement policy, similar to that used by TCP, leads to the feedback implosion issue and limits the scalability of the multicast transport. 2) Retransmitted packets may arrive with important delays depending on the distance between the server and the client. Therefore, they may be dropped by the receiver itself. Besides, a video content is loss-tolerant; if a packet is lost, a temporal video fluctuation may be experienced but the streaming does not interrupt. Hence, the reliability and the quality of a multicast stream depend mainly on the reliability of the delivery path. In wired networks, the loss rate is very limited because the collisions are detectable and are avoided. Besides, the packets are always received with the appropriate signal strength. Hence, the multicast transport over these networks has a high reliability and offers a good quality for the multimedia services.

On the other hand, the IEEE 802.11 networks are deployed everywhere and ensure a reliable unicast transport. Furthermore, they offer a high throughput communication. This capability allows the WLAN to support high throughput streams such as multimedia traffic. Moreover, the standard defines differentiated services in order to guarantee a low latency for time sensitive applications. In a wireless network, a packet may be lost due to many factors: path-loss, collisions, interference, etc. Therefore, the standard defines a feedback policy for the unicast transmissions in order to detect and to retransmit the missing packets. Furthermore, the 802.11 standard defines several data rates with different robustness degrees against the signal attenuation. Therefore, the communicating nodes take advantage of the acknowledgements to estimate the link quality and to select the most suitable data rate. This ensures an optimized use of the bandwidth. However, the legacy multicast transmission procedure does not use any feedback policy. Therefore, missing packets are definitely lost. The multicast stream is by default delivered at the lowest data rate. This is because the sender has no idea about the quality of the downlink to the multicast members. The lowest rate is the most robust one and has the largest coverage area. Therefore, it allows the multicast packets to reach all the receivers within the coverage area of the sender. However, the use of this rate limits the network throughput significantly, increases the congestion probability and may lead to frequent packet drops.

To enhance the reliability of the multicast transmissions over the wireless networks, the 802.11v/aa amendments are defined recently. The former introduces Direct Multicast Service (DMS) while the latter presents the Groupcast with Retries (GCR) service. DMS converts the multicast traffic into multiple unicast streams. Therefore, DMS takes advantage of the reliability of the unicast transport on the expense of the bandwidth. Besides, the delivery delays of DMS increase with the increasing number of the multicast receivers. On the other hand, GCR defines two retransmission policies: Block Ack (BACK) and Unsolicited Retry (UR). The first policy requires the establishment of a GCR-BACK agreement with the group members, and then transmits the packets in block followed by multiple Block Ack Request (BAR)/ BACK exchanges between the Access Point (AP) and the multicast receivers. These feedbacks require an additional transmission time which depends on the group size. This limits the scalability and the throughput of GCR-BACK, and impacts the retransmission delays. Furthermore, GCR-UR requires the transmission of the multicast packets several times in order to increase the probability of the successful delivery. This policy retains the scalability since the overhead does not depend on the group size. However, the transmission redundancy limits the efficiency of GCR-UR significantly. We note that few works have studied and compared the performance of 802.11v/aa, but none of them has been able to provide a complete evaluation of all the relevant parameters (i.e. throughput, delays and scalability). In addition to 802.11v/aa, many other proposals are defined to enhance the reliability of the conventional multicast procedure. But none of them is able to 1) resolve the unreliability issue, 2) maintain the scalability and 3) retain the compliancy with the 802.11 standard at the same time.

An efficient alternative to improve the reliability of the multicast stream over 802.11 networks is to prevent the packet losses. Therefore, it is necessary to identify the loss factors and to define the required prevention actions. Many works have evaluated the transmission failures over the wireless networks. They have classified the causes into the following categories: path-loss, collisions, interference, multi-path effect and queue overflow. Several diagnoses have noticed that the packet delivery ratio may sometimes be very low, and that the receivers may experience bursty losses. Other researches, however, have shown that devices with the same channel condition may experience completely different loss rates. But none of these works has identified the loss factors of the bursty losses and of the extremely high loss rate which may be experienced by a receiver with a good channel condition.

In this thesis we introduce the new functionalities of 802.11v/aa. Then we define an analytical model to determine the throughput under different values of: group size, block size, packet length, transmission rate and loss rate. Moreover, we evaluate the performance of DMS, GCR-BACK and GCR-UR using NS-3. We compare the analytical and the simulations results, and we show that our model has a very good accuracy. The obtained results demonstrate that DMS has the lowest scalability and incurs important delays. Besides, we prove that GCR-BACK is not appropriate for large multicast groups. Moreover, the retransmission delays of this policy increase significantly with the increasing size of the multicast group.

We demonstrate that GCR-UR retains the scalability of the multicast transport, but requires an important overhead and reduces the network throughput significantly.

Furthermore, we investigate the loss factors in the WLAN. Therefore we indentify the device unavailability issue and we show that the device itself may be responsible for the high loss rate. Particularly, we show that the CPU overflow may lead to a loss rate of 100%, and that the delivery ratio may fall to 35% when the receiver is in the power save mode. Our results show that a receiver with an appropriate configuration may experience a very limited loss rate of less than 0.05% in the absence of the collisions. To improve the reliability of the multicast transmissions, we define a collision prevention mechanism called the Busy Symbol (BS). The principle of BS is to send a short symbol in order to briefly occupy the medium. Hence, the contending nodes defer their channel access upon the reception of this radio signal. Following the BS transmission, the AP senses the channel again. If the medium is busy, the AP defers the channel access in order to avoid the collision. Otherwise, the multicast transmission starts. We evaluate this procedure and we show that our mechanism ensures a perfect protection against the collisions. Besides, we demonstrate that the BS incurs a very limited overhead. Moreover, this mechanism is easy to implement and does not require any modification except at the AP.

Even though the multicast stream is protected against the collisions, a feedback policy is still required. This is because the BS alone does not allow the AP to determine the appropriate data rate. Therefore we define a new multicast protocol called Block Negative Acknowledgement (BNAK). Our protocol relies on the principle that the loss rate in the wireless networks is very limited under the following assumptions: 1) the receivers are located within the coverage area of the sender, 2) the packets are sent at the appropriate data rate, 3) the collisions are avoided, and 4) the device has the appropriate configuration. Therefore, it is more appropriate for the AP to request feedbacks from the multicast members experiencing losses, than requesting repeatedly acknowledgements for packets which are delivered correctly almost all the time. Using the BNAK policy, packets are transmitted in block followed by a Block NAK Request (BNR). Only users encountering losses are invited to send a feedback. Therefore if all the packets are transmitted correctly, no BNAK is transmitted and the bandwidth is saved. If a failure occurs, only the impacted receivers are allowed to send a feedback. In order to ensure a reliable delivery of the feedbacks, these packets are transmitted after channel contention and are acknowledged by the AP. Our results prove that our protocol is reliable and efficient, and outperforms 802.11v/aa significantly. Besides, we show that the scalability of BNAK is almost unlimited. Moreover, our protocol is compliant with old and recent amendments, and requires software updates only to be implemented within current devices.

Furthermore, we define a new rate adaptation scheme for BNAK. We show that the selection of the appropriate transmission rate requires a very limited overhead of less that 1%. Besides, we introduce the scalable video streaming capability of BNAK and we show that our protocol is appropriate in dealing with the two following characteristics of the WLAN: bandwidth fluctuation and receiver heterogeneity. During the congestion periods, the AP is allowed to select a higher transmission rate for the enhancement stream in order to avoid the queue overflow. However, regardless of the network load, both the base and the enhancement layers are delivered reliably using BNAK to the eligible members.

This thesis is carried out as part of collaboration between Orange Labs and Laboratoire Bordelais de Recherche en Informatique (LaBRI), University of Bordeaux 1. Particularly, it was conducted in the premises of Orange Labs R&D, Lannion, France, in the team Backhauling Architecture and Traffic for Seamless network (BATS). The main objective of this team is to develop mobile networks at low cost for developing countries. The work of this thesis is part of two collaborative projects, internal to the company: QuETZAL and CapRadio. The purpose of these projects is to improve the quality, the performance and the capacity of wireless and wired communication networks.

The remainder of this thesis is organized as follows. In chapter 2, we introduce the background and the related work. At the beginning of this chapter, we present the streaming protocols and the principal video bit-rate adaptation techniques. Then we provide an overview of the 802.11 networks and we introduce the most relevant characteristics of the PHY and the MAC layers. Moreover, we present related multicast protocols and we highlight their limitations.

We dedicate chapter 3 to the performance evaluation of 802.11v/aa amendments. Thus, we present the most relevant functionalities and we describe in more details the operating mode of DMS, GCR-BACK and GCR-UR. Then we compare the throughput, the reliability, the scalability and the transmission delays of these retry policies.

We investigate the loss factors in chapter 4. Therefore we provide empirical measurements of the impact of the power save mode and the CPU overflow on the loss rate of the multicast packets. Besides, we evaluate the impact of the collisions and of the path loss on the reliability of the legacy multicast procedure through simulations. Furthermore, we introduce the BS mechanism and we provide simulation results of the performance and the efficiency of this protection feature.

In chapter 5, we introduce BNAK and the group membership detection function. We present the different retry policies of our protocol and we describe the operating mode in more details. Besides, we illustrate the frame format of BNR and BNAK packets. Then, we introduce our analytical model and we provide the analytical and the simulation results.

Chapter 6 presents the rate adaptation scheme and the scalable streaming capability of BNAK. Besides, we show the simulation results of the performance of our scheme.

In chapter 7, we conclude this thesis and we provide several perspectives for future works within the topic of this research field.

Chapter 2

2 Background and State of the Art

2.1 Introduction

Although the delivery of many videos is achieved using the unicast mode, many other multimedia applications require the use of the multicast transport in order to deliver the same content to many receivers simultaneously. Thus, video multicasting ensures the service scalability. However, this transport mode usually relies on UDP and does not allow the retransmission of missing packets. Hence, the reliability of the multicast application depends on the reliability of the used networks. While a video multicast service is able to ensure a very good quality over wired networks, the reliability of the multicast transport over wireless networks is very limited due to the high collision rate and the path loss issue.

The IEEE 802.11 standard defines high throughput wireless networks (WLAN). These networks are widely deployed thanks to their affordable cost and easy use. Even though the loss rate in a shared wireless network may be important, the IEEE 802.11 defines a reliable unicast transport thanks to the use of the appropriate feedback policies. Hence, a missing unicast packet is retransmitted. However, the multicast transport does not use any acknowledgement policy. Hence missing packets are definitely lost. Although the multimedia services are loss-tolerant, a high loss rate reduces the video quality considerably and may corrupt the video content.

In this chapter we present the requirements of the video streaming applications, and we show the principal bit-rate adaptation techniques. Besides, we introduce the multicast transport over the IP networks. Therefore we present the routing procedure and the group management protocol. Moreover, we introduce the address mapping function which enables forwarding the multicast traffic over Ethernet. Then, we provide an overview of the principal characteristics of the IEEE 802.11 standard. Particularly, we focus on the capabilities of the physical (PHY) layer, and on the operating mode of the MAC layer. Furthermore, we introduce the weakness of the conventional multicast procedure, and we present the most relevant proposals to enhance the video multicasting quality over a WLAN.

The remainder of this chapter is organized like the following. In Section 2.2, we introduce the principal requirements of the video multicasting over IP networks. We dedicate Section 2.3 to presenting the characteristics of the PHY and the MAC layers of the IEEE 802.11. Section 2.4 summarizes the most relevant proposals which deal with the unreliability issue of the legacy multicast transport. Finally, we conclude this chapter in Section 2.5.

2.2 Video Multicasting over IP Networks

2.2.1 Video Delivery

2.2.1.1 Delivery Methods

The multimedia content is delivered using different methods over the communication networks. The basic way to receive a video stream is to download it as a file. When a video file is downloaded over IP networks, it is likely sent over a TCP-based protocol such as FTP or HTTP. BitTorrent [4] is another widely used protocol to share and to download various kinds of files, including the video files. This protocol is used in peer to peer networks. It makes many small data requests over different TCP connections with different peers. The video streaming is another method to send a video content over the Internet. By definition, streaming is the process of playing a file while it is being downloaded. This method does not require a storage space since the content is visualized without the need to be saved. The principal protocol for video streaming is Real-time Transport Protocol (RTP) [5] which relies on UDP connections. Video streaming systems can be classified into two categories: Video on Demand (VoD), and Live streaming. On demand streaming applications deliver pre-recorded videos to users having requested the stream. Besides, they allow the user to control the video progress and to perform operations such as Play, Resume and Stop. On the other hand, the live streaming is used to deliver a recently captured video content to a group of users. Besides, the server does not retransmit any previous sequence. This kind of applications is mainly used for IPTV, video surveillance, video conferencing and interactive video calls.

2.2.1.2 Transport Modes

There are three different modes for data sending: unicast, multicast and broadcast. The unicast is the principal mode of the IP networks and allows a point to point communication. It is used to send packets from one source to one destination identified by a unique address. Therefore the unicast packets are routed in the IP network till reaching the receiver. Several routing protocols are used to establish the logical path between the sender and the receiver such as Border Gateway Protocol (BGP) [6] and Open Shortest Path First (OSPF) [7]. The use of the unicast allows the implementation of a reliable transport by enabling feedback policies such as those used by TCP. However, a loss-tolerant unicast flow is usually delivered over UDP. The unicast is used by many video applications like file download and on demand streaming. The principal issue of this transport mode is its limited scalability. This is because the network load depends on the number of the established unicast sessions. Thus, the server can deliver a limited number of unicast streams simultaneously. This mode is also used by layer 2 to forward the packets over Ethernet. Thus, the destination is identified by a MAC address. Besides, it is necessary to map the IP address to the MAC one. This mapping is performed by Address Resolution Protocol (ARP) [8].

The multicast transport is used to deliver one stream to many receivers at the same time. It ensures the service scalability, and allows many applications, such as IPTV, to serve millions of users around the world simultaneously. The destination address of a multicast traffic is a multicast address. This address identifies the group and is designed to enable the delivery of the traffic to a group of interested hosts. Furthermore, routers in the delivery path of the multicast traffic should implement a multicast routing protocol such as Protocol-Independent Multicast (PIM) [9,10]. Such a protocol is required in order to construct the multicast delivery trees and to forward the multicast packets to the appropriate sub-networks. Moreover, each router needs to implement a group membership protocol like Internet Group Management Protocol (IGMP) [11] in order to detect the group members on its directly attached sub-networks.

On the other hand, the multicast packets are usually delivered using UDP. This means that these packets are not guaranteed to reach the group members. Thus, the reliability of the multicast transport depends on the reliability of the used network. For this reason, this mode is mainly used to deliver loss-tolerant traffic such as video streams. Besides, there is no need for any address resolution protocol to forward IP packets over Ethernet, but a simple mapping of an IP address to a MAC address is enough.

The broadcast mode is used to deliver messages to all the receivers within a network. Broadcasting over large networks has a high cost on the bandwidth, particularly when this mode is used to deliver high throughput traffic like the videos. For this reason, the broadcast is mainly used to send control packets within one single sub-network. By default, broadcast packets do not leave their local networks. Broadcast services such as IPTV are delivered using the multicast mode in order not to flood all the networks.

2.2.1.3 Constraints

The IP networks are used to deliver many kinds of traffic to many users around the world. For this reason, the network load may vary over the time. This variation may be more important for multi-rate networks such as Wi-Fi. Besides, the video stream has a variable bit rate, and for several instants, the bit rate may exceed the average one significantly. This issue concerns the video streaming applications which require a real-time delivery. Thus, the bandwidth should be enough during all the streaming duration in order to avoid the packet drops and the temporal service interruptions.

The transmission latency is another parameter to evaluate the user satisfaction. This is because a video is viewed in real-time, and packets arriving after their processing time are rejected. However, the delay constraint depends on the kind of application. Hence, video conferencing and video calls are subject to severe delay constraints in order to ensure an interactive communication between the participating parties. According to ITU, a delay of less than 200ms offers a very good quality while a delay of up to 280ms is still suitable for an interactive service [12]. However, IPTV and VoD are less sensitive to the delays and may allow a shifting of few seconds between the reception and the processing instants. This shifting is performed using the buffering policy, and allows the video application to process packets arriving with relatively important delays whenever these delays do not exceed the shifting duration.

2.2.1.4 Transport Protocols

The main protocols used for video streaming are Real-time Transport Protocol (RTP) [5] and Real Time Streaming Protocol (RTSP) [13]. RTP is used to send the data packets at the progress rate of the stream.

Hence, for a video of 25 frames per second (fps), one image is packetized and transmitted every 40ms. The RTP client receives theses packets, reassembles the images and forwards them to the video decoder. If a packet is missing or does not arrive within a specific delay limit, the entire image is rejected. RTP relies on UDP and does not retransmit any missing packet. Besides, it is used to deliver unicast and multicast streams. It is widely deployed to deliver a real-time service. The delay limit of a packet depends on the delay constraints of the application, and is implementation dependent.

RTSP is used to control the session. When RTSP is used to stream a VoD, it permits the client to control the video progress using functions like Play, Stop and Resume. This protocol is also considered to stream a live video content or to deliver the IPTV. In this case, only a subset of RTSP functions may be available such as: Play and Stop. RTSP cooperates with other protocols such as RTP to deliver the stream, and Session Description Protocol (SDP) [14] to negotiate the session parameters (e.g. the supported codecs, the video duration, the available languages, the screen resolutions, etc.). Although the data packets are transmitted using another protocol, RTSP may use recovery policies in order to retransmit missing packets [15].

2.2.2 Multicast Transport

2.2.2.1 Multicast Address Mapping

In current networks, the packets are forwarded using 2 addresses: IP and MAC addresses. IP multicast addresses belong to class D, and are assigned from the following range: 224.0.0.0 to 239.255.255.255. Therefore, they are encoded as follows: "0xE + multicast group identifier (28 bits)". Similarly, the following range of MAC addresses is allocated to the MAC multicast addresses: 01:00:5e:00:00:00 to 01:00:5e:7f:ff:ff. The mapping of an IP address to a MAC address is necessary in order to forward IP packets over Ethernet. This mapping is performed as follows: the lower order 23 bits of a MAC address should correspond to the IP multicast group identifier. This means that the lower order 23 bits of the MAC address should correspond to the lower order 23 bits of the IP address. Since the higher order 5 bits of the IP group identifier are ignored, it is clear that this mapping does not ensure a unique MAC address for the IP addresses. Precisely, up to 32 different multicast sessions may be delivered over Ethernet using the same MAC address.

2.2.2.2 Group Membership Management

The management of the multicast group members is achieved using Internet Group Management Protocol (IGMP) [11]. This protocol involves two devices: the client and the router. The client (i.e. the multicast member) sends messages to the router in order to join or to leave a multicast session. The member also responds to the queries of the router. On the other hand, the multicast router processes the Join/Leave messages and decides if a multicast traffic should be delivered on a given network interface or not. The router sends queries periodically to the group members to determine if the traffic is still requested. These queries are useful to recover from a disconnection failure. The multicast router is the end point of the IGMP requests, i.e. the router does not send IGMP messages to its upstream neighbors. Therefore, the router builds the routing paths using other protocols such as Protocol Independent Multicast (PIM) [9,10], Distance Vector Multicast Routing Protocol (DVMRP) [16] and Multicast extension to Open Shortest Path First (MOSPF) [17].

IGMP provides four basic functions for IP networks:

- JOIN: the host sends a Join message to the router to join the multicast group.
- LEAVE: when the client leaves the group, it sends a Leave message to the router.
- QUERY: the IGMP Query is a broadcast message sent periodically to all the connected terminals. It allows the router to determine if there is any client in the group. This message is useful to detect the LEAVE failure. For example, a set-top box may be unplugged, and a computer may crash, so they do not leave the group using the LEAVE message.
- MEMBERSHIP REPORT: the client builds a report following the reception of an IGMP query. This report tells the router about the groups to which the host belongs.

2.2.2.3 Multicast Routing

Multicasting on a local sub-network does neither need a multicast capable router nor a routing protocol. On such a network, the source sends the multicast packets which are received by the group members. But when the multicast source is beyond the network segment, the members should be attached to a multicast capable router which is attached to other multicast capable routers. These routers must support a multicast routing protocol. This protocol is responsible for the construction of logical distribution trees and for the forwarding of the multicast traffic through the established paths. The most relevant routing protocols are Distance Vector Multicast Routing Protocol (DVMRP) [16], Multicast OSPF (MOSPF) [17] and Protocol-Independent Multicast (PIM). PIM has two modes of operation: PIM Dense Mode (PIM-DM) [9], and PIM Sparse Mode (PIM-SM) [10]. We limit our presentation to PIM for two reasons: 1) PIM is appropriate for both dense and sparse network environments, and 2) is currently the most widely used multicast routing protocol [18-21].

PIM does not build its own routing table, but it uses the unicast one to perform the forwarding function. At the same time, PIM is independent of the used unicast routing protocol. This means that PIM may operate using any unicast routing table regardless of the used protocol for managing this table. PIM-DM is defined for networks where many of the available routers are connected to multicast receivers. The number of members per router does not matter since the multicast tree is built regardless of this number. The dense mode is expected to be deployed in LANs with many members, such as a campus network.

PIM-DM expects that most of the connected hosts (e.g. PCs, smartphones, set-top boxes, etc.) are interested in receiving the multicast traffic. Therefore the protocol initially forwards the traffic from the multicast source to all the routers in the network. Routers with no group members send Prune messages to be removed from the multicast tree. These messages are also used to filter the traffic and to receive only the required sessions among those available. PIM-DM is typically used in the backbone to deliver IPTV services [18].

The sparse mode is optimized for environments where group members are distributed across many regions and over a large network like the Internet. In a PIM-SM network, the sources send their multicast traffic to Rendezvous Points (RPs). This traffic is in turn forwarded to the group members on the delivery tree. This tree is built based on explicit Join/Leave messages transmitted hop-by-hop from the local router (the router with directly attached members) to the RP. The Join message is sent periodically in order to maintain the delivery path. PIM-SM allows the receivers either to continue receiving the traffic through the RP or to receive it over a source-routed shortest path tree that the receiver subsequently creates. We depict an example of PIM-SM network in Fig. 1.

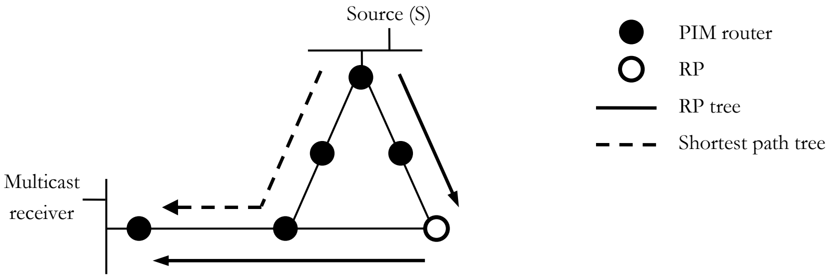


Figure 1. Network components and path creation using PIM

The location of the RP affects both the multicast service delay and the network load. Since the multicast transport is mainly used to reduce the backbone traffic, it is advantageous to locate the RP near the source compared to any other location in the backbone middle [15]. Besides, the RP is recommended to support the deployment redundancy in order to improve the stability of the multicast service in case of a RP failure.

2.2.2.4 Multicast Snooping

IGMP is a protocol of layer 3 and is not designed to operate in environments where there are network equipments between the IGMP router and the IGMP clients. However, in a typical deployment of a multicast service, intermediate devices such as switches and DSLAMs may exist as it is illustrated in Fig. 2. If these devices are not aware of the IGMP messages, then by default they will forward the multicast traffic on all ports. Thus, this traffic may be delivered to sub-networks with no group members and may cause an excessive use of the bandwidth on these network segments. To mitigate this issue, the snooping technique is defined and is implemented in many devices, enabling them to forward the multicast traffic on the right ports. IGMP snooping [22] allows a network device located between the router and the clients to inspect incoming IGMP messages and to take the required actions. The device builds a table to track which multicast sessions are being forwarded to which ports.

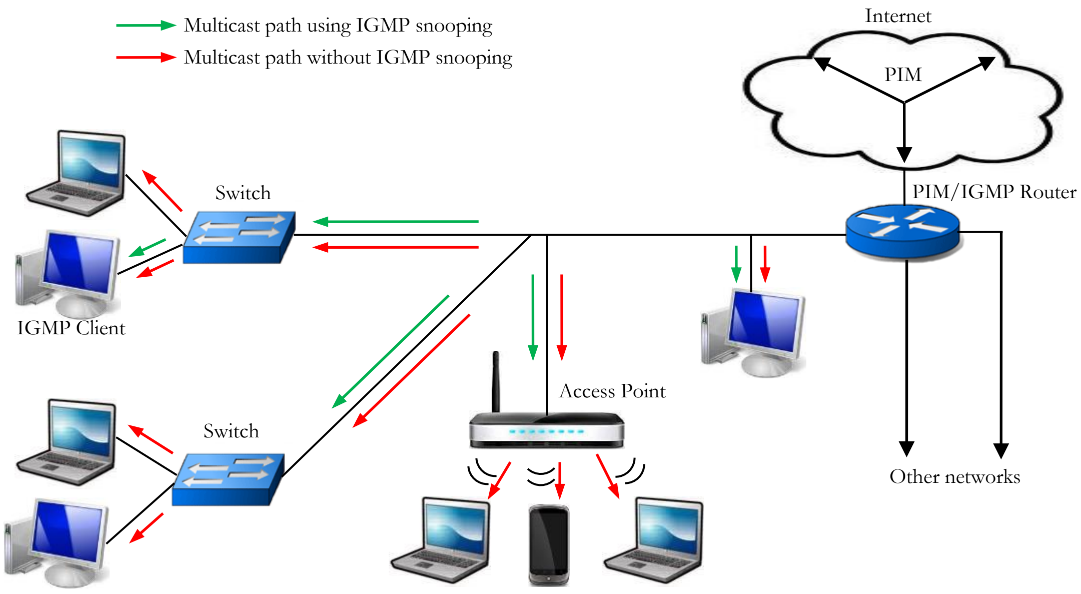


Figure 2. Local deployment of a multicast service with and without IGMP snooping

2.2.3 Video Adaptation

2.2.3.1 Motivation

In heterogeneous environments, the members of the same multicast group may have different quality requirements due to the bandwidth limitations or due to the technical characteristics of the used devices. Thus, two motivations involve the need to adapt the video bit rate: 1) to deal with the available network resources, and 2) to satisfy the device heterogeneity.

The video stream is known to have a variable bitrate. This is because the content of the video sequences varies over time and may include additional objects and details resulting in larger frames and instantaneously higher throughput. Besides, the principal video compression standards [23-26] encode the videos into two types of images: reference and dependent. The reference images are intra-coded only and therefore do not depend on any other video frame. The dependent images are intra-coded and inter-coded with regard to other frames in order to improve the compression efficiency. Thus, the reference images are larger than the dependent ones. As such, the instantaneous video bitrate depends on both the instantaneous content and on the image type.

On the other hand, the communication networks are shared between many flows and many users. Hence, the available bandwidth varies over the time; during some periods of the day the network is congested while it is free during other periods. During the congestion instants several packets are rejected. These drops occur when the load of the transmission queue exceeds a specific limit, or when the buffering delay reaches the packet lifetime limit. TCP flows are able to reduce their throughput in order to adapt to the new network load. However, UDP traffic does not use feedbacks and does not detect rejected packets. This leads to the following two issues: 1) UDP throughput does not adapt to the available bandwidth, and

2) rejected packets are not retransmitted. Thus the quality of a video streaming service depends significantly on the network load and on the available bandwidth.

Since video streaming is a real-time service, the receivers need to visualize the video continuously and without interruptions. Therefore the video bitrate should be adapted in order to fit with the network load and to avoid the packet rejections. The main techniques used to adapt the video bitrate are: simulcast, transcoding and layered video encoding. These techniques are also suitable to deal with the device heterogeneity of a multicast group. They allow the user to select the appropriate quality.

2.2.3.2 Simulcast

Simulcast [27-29] is among the principal techniques defined to deliver a multimedia service with different qualities to multicast receivers. This proposal is used to address both the bandwidth availability and the device heterogeneity. The main idea of simulcast is to deliver the same video content with different qualities (e.g. different resolutions), and therefore with different bitrates. Thus, users with low throughput connections, subscribe to a low quality session, regardless of their device characteristics. However, if the bandwidth is available, the multicast receiver subscribes to the session which fits with the device capabilities. Simulcasting a video content increases the load over parts of the network used to deliver all the video qualities. Besides, when receivers with different requirements are connected to the same access network (e.g. Wi-Fi), the simulcast increases the network load on the entire delivery path from the source to the receivers.

2.2.3.3 Transcoding

The principle of this solution is to re-encode an initial video stream into a different quality in order to fit with the available network resources or with the terminal characteristics [30-32]. When the transcoding is applied to a VoD, the server itself re-encodes the video. However, if the video is delivered using the multicast transport, intermediate nodes in the network, such as servers or smart routers, are responsible for the video transcoding. Therefore, the transcoding technique is not optimized for multicast services since it requires dedicated network components. Besides, it increases the processing load of the VoD server and limits the number of streamed videos.

2.2.3.4 Layered Video

The main characteristic of a layered video is that it is encoded into one base layer and one or several enhancement layers. Thus, decoding the base layer alone ensures the base video quality, while decoding the enhancement layers progressively improves the output quality. However, the enhancement layers are useless if they are not decoded with the base one. This concept ensures that the stream bitrate depends on the number of the transmitted layers and therefore is able to resolve the issue of the network congestion. Besides, a video with enhancement layers improving the resolution is accurate for the issue of the device heterogeneity. Scalable Video Coding (SVC) [26] is the principal layered video encoder. It is extensively studied to deal with the bandwidth variation and the device heterogeneity [33-36].

2.2.3.5 Scalable Video Coding (SVC)

SVC is defined by H.264 [26] and inherits the temporal scalability of Advanced Video Coding (AVC). SVC also defines two additional types of scalability: spatial and quality. The temporal scalability allows the decoding of a video with a variable number of frames per second. Hence the temporal scalability allows the adaptation of the bitrate by varying the frame rate. This scalability is not efficient since it relies on the suppression of several dependent images while keeping the reference ones. However, it is known that the reference images are the largest parts of the video and are significantly larger than the dependent frames. Thus, the removal of the dependent images does not reduce the stream bitrate significantly. Besides, reducing the number of frames per second damages the video fluidity and limits the client satisfaction.

The quality scalability allows a video stream to encapsulate more than one visual quality. This scalability relies on the encoding of each image using a high compression level leading to the suppression of some details from the base layer, while adding these details into the enhancement layers. Thus, the quality scalability is efficient in reducing the stream bitrate without impacting the frame rate. Although this scalability is able to mitigate the bandwidth fluctuation, it does not satisfy the device heterogeneity and the need for different resolutions.

The spatial scalability allows every image to be encoded into different resolutions. Thus, each image is encoded into a low resolution while the additional information to obtain the full resolution is encapsulated into the enhancement layers. Therefore, the spatial scalability does not impact the display rate of the video. Besides, it is efficient to reduce the stream bitrate and to address the bandwidth fluctuation; when the enhancement layers are rejected, the decoder enlarges the image of the base layer. Also, the spatial scalability satisfies the resolution requirements of the heterogeneous devices without the need for the transcoding process.

Similar to H.264/AVC videos, any SVC stream includes the temporal scalability. However, the spatial and the quality scalabilities may or may not be available, and their respective numbers are configurable. Thus, a SVC video may have 0 or many layers of each of these two scalabilities.

2.3 IEEE 802.11 Networks

2.3.1 Standard Presentation

IEEE 802.11 standard defines the MAC and the physical (PHY) layers of a Wireless Local Area Network (WLAN). Since the first release of 1997, several amendments have been proposed in order to increase the data rate and the coverage area of the PHY layer, and to enhance the efficiency of the MAC layer. Therefore, 802.11 networks are now able to provide very high transmission rates of up to 600Mbps while the maximum data rate of the initial release do not exceed 2Mbps. Besides, the communication may be established over important ranges of more than 200 meters. On the other hand, the MAC layer is able to provide different levels of priority. This allows the network to deliver time sensitive flows with very low latencies. Furthermore, the MAC layer offers a reliable and secured communication mode, and defines efficient power save mechanisms. It also supports different network configurations such as infrastructure and Ad hoc modes. Among the most relevant amendments we can find:

- 802.11e (2005): Defines different priority levels to improve the quality of time sensitive flows.
- 802.11w (2009): Protects the management packets.
- 802.11u (2011): Enables the interworking with other technologies such as 3G. Hence it allows mobile networks to off-load to 802.11 WLANs.
- 802.11n (2011): Improves the network throughput.
- 802.11s (2011): Defines the architecture of a Mesh network.
- 802.11aa (2012): Enhances the quality of audio and video streaming applications, and particularly defines retransmission policies for the multicast transport.

In addition to the already approved amendments, many other enhancements are in progress such as:

- 802.11ac: Specifies the enhancements to the 802.11 MAC and PHY to support very high throughput (> 6 Gbps) in the 5 GHz bands.
- 802.11af: Defines the required modifications to allow WLANs to coexist in the TV White Space.
- 802.11ad: Defines transmission rates of up to 7Mbps in the 60 GHz band.

2.3.2 Network Modes

2.3.2.1 Infrastructure Mode

An infrastructure network is built using a central node called the Access Point (AP). A station should associate with the AP in order to become a member of the network. The AP and the associated stations build the Basic Service Set (BSS). This set of nodes is identified using the BSSID which is the MAC address of the AP. In a BSS, the stations should communicate with the AP only. If an associated node wants to communicate with another station in the same BSS, it should address the data to the AP which forwards the message to the destination. This procedure is performed even if the two stations are in direct visibility. Recently, the 802.11n has defined the Direct-link setup (DLS) which allows two stations of the same WLAN to communicate directly. The DLS is established by the AP based on the request of the associated stations.

An AP accesses to the Distributed System (DS) in order to interconnect the WLAN with external networks. The DS needs an additional component, called the portal, to allow the infrastructure network to communicate with non-802.11 LANs such as the traditional wired LAN.

It is possible to connect several BSSs together in order to obtain an Extended Service Set (ESS). The ESS increases the coverage area of the WLAN and enhances the throughput. It is identified with a string of 32 characters, called ESSID. This identifier is often abbreviated to SSID. Stations within an ESS may communicate and may move from one BSS to another within the same ESS transparently. The handover within an ESS is performed based on the connection characteristics, i.e. the reception signal strength and the network load.

2.3.2.2 Ad hoc Mode

The 802.11 defines the Independent BSS (IBSS) as the most basic type of WLAN. An IBSS may be built using two stations only. It allows a simple communication since there is no infrastructure equipment, and is therefore called Ad hoc network. The members of an IBSS are able to communicate directly. Thus, an Ad hoc network is mainly established for short durations in order to exchange files.

2.3.2.3 Mesh Mode

The IEEE 802.11 mesh facility provides the required MAC functionalities to support mesh topologies. A mesh BSS (MBSS) is a WLAN consisting of autonomous nodes. A station that belongs to a MBSS is called mesh station. Within a MBSS, all the stations establish connections with their neighbors to exchange packets. The multi-hop capability allows nodes of the MBSS which are not in direct communication to exchange messages with each other. We distinguish three kinds of nodes: source, sink and traffic propagator. Therefore, some mesh stations may only forward the traffic of other nodes. Only mesh stations may perform the mesh functionalities such as the formation of the MBSS, path selection and forwarding, etc. Accordingly, mesh stations are not members of an infrastructure BSS or an IBSS, and do not communicate with non-mesh stations directly. However, a MBSS may access to the DS in order to interconnect with external networks. This access is established using the mesh gate. This latter component is equivalent to the AP in an infrastructure BSS since it allows the mesh stations to communicate with devices other than the members of the MBSS. The DS still needs a portal in order to allow the MBSS to interconnect with non-802.11 LANs.

2.3.3 The IEEE 802.11 Physical Layer

2.3.3.1 Physical Layers and Supported Data Rates

The standard defines several physical (PHY) layers with a multi-rate capability. The Infra Red (IR), the Frequency-Hopping Spread Spectrum (FHSS) and the Direct Sequence Spread Spectrum (DSSS) layers are defined by the first release of IEEE 802.11 standard. They provide a transmission rate of 1 and 2 Mbps, and operate at the 2.4 GHz spectrum. The 802.11b amendment specifies a High Rate extension of DSSS (HR DSSS) which supports 5.5 and 11Mbps in addition to 1 and 2Mbps. Besides, the amendment defines a smaller packet header to improve the throughput. The Orthogonal Frequency Division Multiplexing (OFDM) layer is first defined by 802.11a then by 802.11g. The major difference between these two amendments is that the former operates at 5GHz while the latter coexists with the earlier 802.11 devices at the 2.4GHz band. Thus 802.11g uses some different parameters in order to operate properly with older terminals. The OFDM layer increases significantly the transmission rate of 802.11 networks and defines data rates of up to 54Mbps. This layer is also used by 802.11n in order to support very high transmission rates up to 600Mbps. We summarize the different physical layers and the supported data rates in Table 1.

Table 1. Data rate capabilities of the different PHY layers

Standard	Band	PHY layer	Data rates
IEEE 802.11 1997	2.4 GHz	IR, FHSS, DSSS	1, 2 Mbps
802.11b	2.4 GHz	HR/DSSS	1, 2, 5.5, 11 Mbps
802.11a	5 GHz	OFDM	up to 54 Mbps
802.11g	2.4 GHz	OFDM	up to 54 Mbps
802.11n	2.4, 5 GHz	OFDM	up to 600 Mbps (see Table 2)

802.11n increases the data rate of the primary OFDM layer by considering the following additions: make use of 4 more subcarriers previously not used, a larger bandwidth of 40 MHz, a spatial multiplexing capability which allows the simultaneous transmission of up to 4 symbols, a shorter Guard Interval (GI) and an additional coding rate of 5/6. A mapping between 802.11a data rates and those defined by 802.11n is illustrated in Table 2.

Table 2. PHY data rates of 802.11a/n

802.11a 20 MHz	802.11n															
	1 Spatial Stream (SS)				2 SS				3 SS				4 SS			
	20 MHz		40 MHz		20 MHz		40 MHz		20 MHz		40 MHz		20 MHz		40 MHz	
	GI 0.8μs	GI 0.4μs	GI 0.8μs	GI 0.4μs	GI 0.8μs	GI 0.4μs	GI 0.8μs	GI 0.4μs	GI 0.8μs	GI 0.4μs	GI 0.8μs	GI 0.4μs	GI 0.8μs	GI 0.4μs	GI 0.8μs	GI 0.4μs
6	6.5	7.2	13.5	15	13	14.4	27	30	19.5	21.7	40.5	45	26	28.9	54	60
9*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
12	13	14.4	27	30	26	28.9	54	60	39	43.3	81	90	52	57.8	108	120
18*	19.5	21.7	40.5	45	39	43.3	81	90	58.5	65	121.5	135	78	86.7	162	180
24	26	28.9	54	60	52	57.8	108	120	78	86.7	162	180	104	115.6	216	240
36*	39	43.3	81	90	78	86.7	162	180	117	130	243	270	156	173.3	324	360
48*	52	57.8	108	120	104	115.6	216	240	156	173.3	324	360	208	231.1	432	480
54*	58.5	65	121.5	135	117	130	243	270	175.5	195	364.5	405	234	260.0	486	540
-	65	72.2	135	150	130	144.4	270	300	195	216.7	405	450	260	288.9	540	600
Mandatory except *		Optional														

2.3.3.2 Communication Channels

IEEE 802.11 uses two different unlicensed radio bands: 2.4 GHz called Industrial, Scientific and Medical (ISM), and 5GHz called Unlicensed National Information Infrastructure (UNII). The ISM radio band is divided into several channels separated by 5MHz. This interval is explained by the fact that the standard supports communication at a bandwidth of 5MHz. In this case, the different wireless channels do not overlap. However, when the network operates at a larger bandwidth such as 10, 20 or 40 MHz, a variable number of channels overlap. Therefore, it is necessary that the frequencies attributed to neighbor networks are far enough in order to avoid the interference. We note that neighbor WLANs may operate on overlapping channels. In this case, terminals from different cells will share the same resources (i.e. transmission time) and the same collision domain. On the other hand, simultaneous transmissions over non-overlapping channels may occur without collisions. Hence, a good planning of the different frequencies minimizes the interference, reduces the collisions and increases the network throughput.

The number of channels depends on the country. Besides, the number of non-overlapping frequencies depends on the bandwidth. Hence, the 2.4GHz band offers 3 non-overlapping channels of 20MHz, but only 2 channels of 40 MHz spacing. The 5GHz band has a larger spectrum than the ISM band and offers 24 separated communication channels of 20MHz and 9 channels of 40MHz. Therefore, it is possible to build in the same area an important number of WLANs which do not interfere with each other.

2.3.4 The IEEE 802.11 MAC Layer

2.3.4.1 Transport Modes

IEEE 802.11 defines three transport modes: unicast, multicast and broadcast. Both the multicast and the broadcast modes do not use any feedback policy, and they deliver the packets only once. Therefore, any missing multicast packet is definitely lost. Besides, only the AP is allowed to use the multicast transport within an infrastructure network. If an associated station is the source of a multicast traffic, then it should send this stream in unicast to the AP which forwards the packets using the multicast mode.

On the other hand, the unicast mode offers a reliable communication over the wireless medium using two feedback policies: ACK and Block Ack (BACK). It is worth noting that if the packet loss rate of the network is very important, even the unicast transport becomes unreliable. This is because the packets are dropped once the retry limit is reached. Therefore, it is necessary to avoid the interferences and to select the appropriate transmission data rate. The former requirement may be achieved thanks to a good planning of the radio channels. This limits the interferences with the neighbor networks, and reduces the collisions. The data rate adaptation is beyond the scope of 802.11. Therefore, several adaptation schemes are proposed and implemented. The transmission rate of the multicast mode is not easy to adapt since it is not possible to detect the packet losses. Therefore, the lowest data rate is selected by default in order to increase the probability of the transmission success. We highlight the fact that there is no restriction, other than the reception capability of the receivers, to use high data rates to send multicast packets. Therefore, adapting this rate is required in order to increase the network throughput.

2.3.4.2 Channel Access

The principal channel access method is the Distributed Coordination Function (DCF). This function allows different devices to share the medium using CSMA/CA and a random backoff time. A station desiring to send a packet should sense the medium to determine if another transmission is in progress. In case the medium is busy, the station defers until the end of the current transmission. Then it should wait an additional delay called interframe space (IFS). If the station receives correctly the last transmission, the IFS corresponds to DCF IFS (DIFS). Otherwise, the additional delay is Extended IFS (EIFS). After DIFS/EIFS, and if the medium is still idle, the station contends using the randomly generated backoff time (BT), or the remaining of the BT if it has already been generated. If the medium remains idle till the expiry of the waiting time, the transmission starts. Otherwise, the station defers again and tries transmitting later using the remaining value of the BT.

The BT is a random number of SlotTimes. This number is generated from a Contention Window (CW). The initial value of CW is CWmin. Then this window is exponentially increased up to CWmax following the transmission failure of a unicast packet, i.e. no ACK is received. The CW is initiated to CWmin in any of the following two cases: 1) successful delivery or 2) packet dropped. The increased CW minimizes the 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]. Multicast packets, however, are always transmitted using the smallest CW. Thus, they are more vulnerable to the collisions than the unicast traffic. But they have more priority to gain the channel. This leads to the unfair sharing of the medium between unicast and multicast flows [37]. The values of CWmin and CWmax depend on the used physical layer. We depict these values in Table 3 for the case of OFDM since this is the used layer in high throughput networks (i.e. 802.11a/g/n).

Table 3. Contention windows min and max for the OFDM physical layer (802.11a/g/n)

CWmin	CWmax
15	1023

Upon the successful reception of a unicast packet, the receiver waits a Short IFS (SIFS), and then sends an ACK. On the other hand, the sender retransmits the packet in case the ACK is missing. However, this retransmission is subject to a retry limit and to the packet lifetime limit. The retry limit is implementation dependent. As an example, the driver Ath9k [38] defines a transmission limit of four. Thus, a packet is dropped if it is not acknowledged following any of the four first transmissions. The lifetime limit may be set to infinity. In this case, the packet is retransmitted only subject to the retry limit. On the other hand, the multicast packets are sent only once. Besides, their transmission may be subject to the lifetime limit.

The relationship between the different IFS is as follows:

- DIFS = SIFS + 2 SlotTimes;

- EIFS = DIFS + SIFS + ACKTxTime, where ACKTxTime is the required time to transmit an ACK at the lowest data rate.

IEEE 802.11e defines an enhanced access mechanism called Enhanced Distributed Channel Access (EDCA). This mechanism defines four access categories (AC): Voice (VO), Video (VI), Best Effort (BE) and Background (BK). When a new packet arrives from the upper layers, it is classified based on its User Priority (UP) and buffered into one of the four queues according to the mapping scheme illustrated in Table 4. The MAC layer determines the UP of a packet according to several rules such as the packet origin (coming from a wireless or a wired network) and the protocol type (IP or not). For the case of an IP packet coming from the Ethernet, the UP is determined by examining the DiffServ Code Point (DSCP) from the Differentiated Services (DS) field [39,40] in the IP header.

Table 4. UP to AC mapping

User Priority (UP)	Access Category (AC)
1 (Lowest priority)	BK
2	BK
0	BE
3	BE
4	VI
5	VI
6	VO
7 (Highest priority)	VO

Each category is allowed to access the channel using different Arbitration IFS (AIFS) and CW intervals. AIFS is a function of the AC and is used instead of DIFS. In case of an internal collision between the different queues, the channel access is granted to the AC with the highest priority. By defining smaller CW for high priority AC, packets belonging to these categories experience reduced delays compared to low priority traffic. However, there is no fair sharing of the medium between flows with different priority degrees. We illustrate the different values of CWmin, CWmax and AIFS in Table 5. The value of aCWmin is either 15 or 31 for the OFDM layer.

Table 5. Channel access parameters for the OFDM physical layer under EDCA operation

Access category	CWmin	CWmax	AIFS
BK	aCWmin	1023	SIFS + 7 SlotTimes
BE	aCWmin	1023	SIFS + 3 SlotTimes
VI	(aCWmin + 1)/2 -1	aCWmin	SIFS + 2 SlotTimes
VO	(aCWmin + 1)/4 -1	(aCWmin + 1)/2 -1	SIFS + 2 SlotTimes

In addition to DCF and EDCA, the standard defines a polling function called Point Coordination Function (PCF). PCF defines two access periods: Contention Period (CP) and Contention Free Period (CFP). These periods alternate and share the channel access time. During the CFP, a station is allowed to send only upon the reception of a poll packet. Besides, the data exchange between the AP and another station may take a long duration. This is because the AP polls each station till the transmission end of all the buffered packets. Therefore, the packets of other nodes may experience important latencies. For this reason the polling procedure is not appropriate for time sensitive flows.

2.3.4.3 Block Transfer

The block transfer improves the channel efficiency by aggregating several acknowledgements into one packet. Two types of Block Ack (BACK) are defined: immediate and delayed. Delayed BACK primarily intends to allow former devices to use this mechanism with minimal updates. However, immediate BACK is the principal feedback policy. In the remainder we only refer to the immediate BACK policy. The block transfer allows the transmission of several packets separated with SIFS during one or many transmission opportunities (TXOP). The packets within a TXOP may be separated by a shorter interval called Reduced IFS (RIFS). This interval is recently defined by 802.11n. Furthermore, a TXOP is granted following channel contention. The duration of a TXOP depends on the AC. The different values are illustrated in Table 6. When the TXOP is nil, only one data packet may be transmitted. Thus each packet of the block is delivered after channel contention.

Table 6. TXOP limit for OFDM physical layers (802.11a/g/n)

Access category	TXOP limit
BK	0
BE	0
VI	3.008ms
VO	1.504ms

To use BACK mechanism, a BACK agreement should be established between the sender and the receiver. Then, a block of packets is delivered and is followed by a Block Ack Request (BAR)/ BACK exchange. The BACK packet may notify the reception status of up to 64 MPDUs. Upon the reception of the feedback, the sender retransmits missing packets. Unlike the normal ACK, the retransmission of a packet is only subject to the lifetime limit. When BACK is used, missing packets are not detected immediately following the transmission end. Therefore, the CW is not updated and CWmin of the corresponding access category is always used to generate the Backoff Time. Even though a BACK agreement is established, it is possible to use the normal ACK if few packets are available for transmission. An example of the block transfer is depicted in Fig. 3.

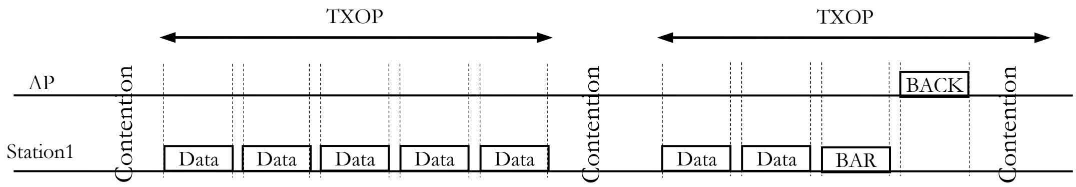


Figure 3. Block transfer using the BACK mechanism

2.3.4.4 Packet Aggregation

The packet aggregation is defined by the 802.11n amendment in order to improve the transport efficiency. Two aggregation schemes are available: Aggregated MSDU (A-MSDU) and Aggregated MPDU (A-MPDU). The first one allows the aggregation of several MSDU into one single MPDU. The A-MSDU aggregation reduces the transmission overhead since only one MAC header is generated for all the aggregated MSDUs. Besides, the entire A-MSDU is validated using one single CRC. However, this scheme becomes inefficient in noisy channels; if only one MSDU is corrupted, the entire A-MSDU is rejected and all the aggregated MSDUs are lost. It is worth noting that an A-MSDU is acknowledged using a simple ACK. The maximum length of an A-MSDU is limited to 7955 bytes when only one MPDU is encapsulated within the PHY packet (i.e. PPDU).

The A-MPDU scheme allows the aggregation of several MPDUs into the same PPDU. In an A-MPDU each MPDU is encapsulated with its MAC header and CRC. Hence, a corrupted MPDU is separately detected and does not affect the entire A-MPDU. However, the A-MPDU aggregation requires more overhead than an A-MSDU. This overhead reduces the transport efficiency particularly when small MSDUs are aggregated [41]. The maximum supported length for an A-MPDU is 65535 bytes. However, the maximum length of the effectively transmitted A-MPDUs depends on the device capability. This capability is announced at the association time. The acknowledgement of an A-MPDU is achieved using BACK. For this reason no more than 64 MPDUs can be aggregated within an A-MPDU.

The two-level aggregation scheme [42] allows the aggregation of one or many A-MSDUs within an A-MPDU. In this case, the maximum length of an A-MSDU is 3839 bytes. The size limit of the A-MPDU remains the same.

2.3.4.5 RTS/CTS Handshaking

The RTS/CTS exchange is used to protect the unicast packets against the collisions and against the hidden terminal issue. In the case of a WLAN with a high collision rate, it is more appropriate to miss a small control packet rather than the data one. Therefore the unicast packet is transmitted following the successful reception of the CTS. If this control packet is missing, the main transmission is deferred.

In the infrastructure network, a station may be hidden to other stations due to the path loss. This may occur particularly when the connected terminals use different transmission powers (We highlight the fact that the transmission power is configurable and may be reduced in order to limit the energy consumption). Hence, the carrier sensing area of one node may be smaller than the communication range of another. In this case the latter node may start sending while the transmission of the former terminal is already in progress. This is called a staggered collision [43]. We depict a scenario of the hidden terminal issue in Fig. 4. In this figure, S2 can not sense the transmissions of S1 and both of them are able to communicate with the AP. The RTS/CTS exchange is a possible solution for this issue in an infrastructure network. It allows any associated station to send an RTS to the AP before sending the unicast packet. The reduced size of this control packet increases the probability of the transmission to occur without staggered collision. Following the CTS reply, all the stations within the BSS become aware of the unicast transmission and defer any channel contention till the end of the reserved time.

The multicast transmissions do not need RTS/CTS for the protection against the hidden terminal issue. This is because the AP is the central node in the infrastructure network and is heard by all the associated devices. However, RTS/CTS may be used for collision prevention purposes. In this case, the AP exchanges RTS/CTS with any group member and then sends the multicast packet. CTS-to-Self is another alternative for RTS/CTS and requires less overhead. It is also appropriate for the multicast transmission since the AP does not need to select any particular receiver. This protection works as follows. Before sending the multicast packet, the AP sends CTS then senses the channel. If the medium is idle, the AP starts the transmission of the data packet after SIFS (or RIFS) following the transmission end of the CTS. Otherwise, the AP defers the multicast transmission. Therefore, it is possible to send the CTS at a high data rate in order to reduce its transmission duration and to enhance the overall throughput. We highlight the fact that the CTS-to-Self does not require to be received correctly when it is used to protect the multicast packets against the collisions. This is because any contending station will defer its transmission at least for a period of DIFS (following the successful reception of CTS) or EIFS (following the CTS reception failure). Thus the multicast packet is delivered without collision.

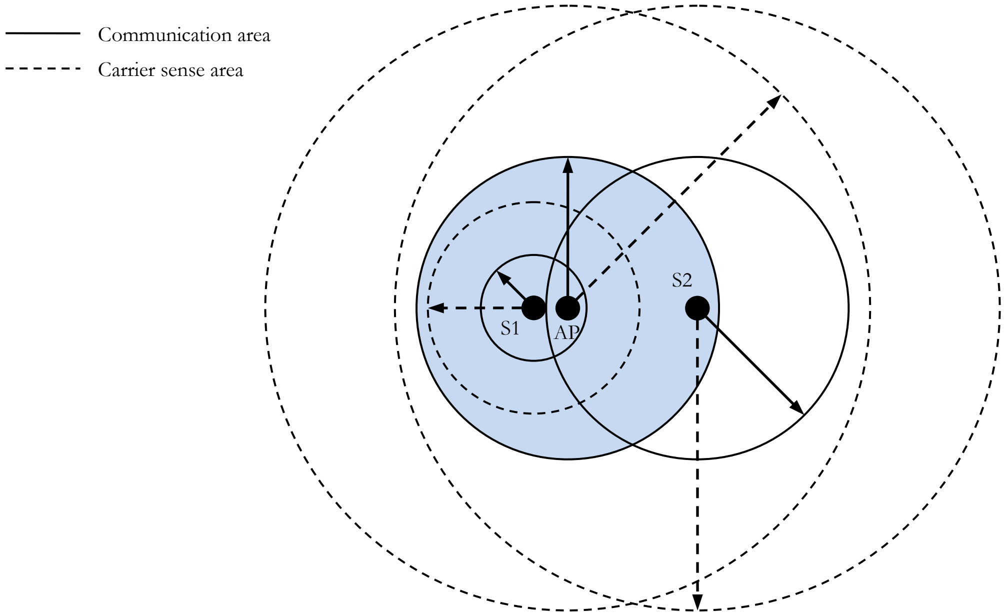


Figure 4. Hidden terminal scenario in an infrastructure network

2.4 Enhancing the Quality of Video Multicasting over IEEE 802.11

Many multicast protocols were designed in order to improve the reliability of the multicast transmissions and to enhance the video quality over the IEEE 802.11 networks [44-79]. Most of these proposals may be classified into 3 categories: 1) Acknowledgement (ACK) based [44-52], 2) Negative Acknowledgement (NAK) based [53-66], and 3) Pseudo broadcast [67-70].

2.4.1 Acknowledgement based Multicast Protocols

2.4.1.1 Broadcast Medium Window (BMW)

The principle of BMW [44] is to reliably transmit each multicast packet to each neighbor in a round robin fashion. Therefore, the multicast sender maintains a list of all the neighbor nodes in the network. When a packet is available for transmission, the sender selects the next neighbor in the list and contends for the channel. Before sending the data packet, the multicast source exchanges RTS/CTS packets with the selected receiver. These control packets are exchanged not only for the protection purpose but also for advertising the available packets and notifying the reception status. Thus, RTS indicates the sequence numbers of the available packets while the receiver fills the CTS with the list of missing packets. If all the previous packets are received correctly, the sender transmits the new packet only and waits for the ACK.

Otherwise, the multicast source transmits the missing packets one by one without additional channel contention. Each packet is preceded by RTS/CTS and followed by ACK.

BMW transmits the multicast packets reliably to all the neighbors, regardless of their being members of the multicast group or not. This issue limits the protocol efficiency significantly and impacts both the throughput and the delivery delays. Besides, any rate adaptation scheme for BMW may continuously select the lowest data rate in order to satisfy the farthest neighbor even if this node is not member of the multicast group. Another weakness of BMW is that this protocol retransmits all the missing packets in one single block. If an important number of packets are missing, the channel will be held for an important duration. Thus, BMW may potentially impact the quality of any time sensitive application sharing the medium. Furthermore, the retransmission delay of BMW is a function of the number of the available neighbors. This is because a receiver should wait for one round in order to request a missing packet.

2.4.1.2 Batch Mode Multicast MAC (BMMM)

BMMM [45] is another ACK-based multicast protocol which requires the acknowledgement of all the multicast members. This protocol does not modify the frame format of the standard control packets but defines a new control packet called Request for Ack (RAK). This packet allows the multicast sender to recover the feedbacks of all the group members. However, BMMM does not define a negative feedback; if a member receives the data packet correctly, it replies to the RAK with an ACK. Otherwise, it does not reply. The transmission procedure requires the use of the RTS/CTS protection. Following the channel contention, the multicast source exchanges RTS/CTS with all the group members. Then it sends the multicast packet. RAK is addressed individually to each member after the data transmission. Every member replies to the RAK with an ACK if the multicast packet is received correctly. The transmission procedure of BMMM is illustrated in Fig. 5.

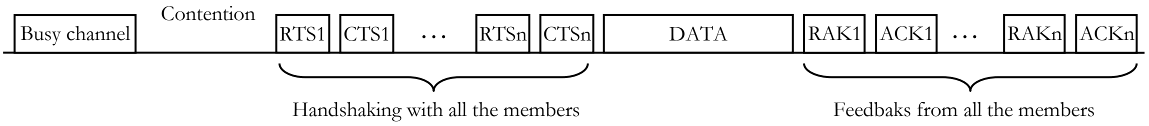


Figure 5. Frame exchange using BMMM

We note that BMMM has a very weak design since the RAK does neither indicate the sequence number of the packet that should be acknowledged, nor the multicast address. This means that a member should acknowledge the last received multicast packet upon the reception of a RAK. Thus, following the reception of the first multicast packet and regardless of its multicast address, any member will always send an ACK upon the reception of a RAK. Hence, if a multicast packet other than the first one is lost, it will not be detected. It is therefore necessary to add the multicast group address and the packet sequence number into the RAK in order to ensure the reliability of BMMM. Besides, it is important to define a negative acknowledgement. This feedback allows a member to reply to a RAK if the data packet is lost.

Another weakness of BMMM is its limited efficiency (i.e. throughput). This is because BMMM requires the exchange of several control packets with all the group members. The number of these packets depends on the group size. Thus the protocol has a limited scalability. Besides, the multicast delivery to large groups requires an important transmission slot. This impacts the quality of time sensitive applications sharing the channel.

The group membership management is beyond the scope of BMMM. This protocol considers that the MAC layer is already aware of the different members. Besides, BMMM does not define any procedure to deal with the disconnection failure of a member. In this case, BMMM experiences the following issue: the multicast source keeps sending the RTS to all the recorded members. When it transmits the RTS to the disconnected member, it does not receive any answer. After 7 retries of RTS (i.e. the default retry limit of 802.11), the sender deletes the data packet and tries the next buffered one, always using the RTS/CTS exchange. The disconnected member does not reply and the new packet is removed too before being transmitted. The same transmission procedure occurs again and again and all the multicast packets are rejected before being transmitted. Thus, the multicast service is cut for all the other group members each time a multicast receiver encounters a disconnection failure. Therefore, BMMM needs an effective policy to detect the disconnection of any member immediately.

2.4.1.3 Transparent Multicast/Unicast Translation

The authors of [46] propose a transparent multicast/unicast translation method which converts multicast packets into multiple unicast flows at the MAC layer. This method requires the implementation of the Multicast/Unicast Translator (MUT). This entity may be either a logical or a physical component located between the multicast router and the AP. The MUT transparently duplicates each multicast packet and sets the destination address of each copy to the address of a group member. Therefore, the multicast traffic is delivered reliably using the unicast. The proposed network architecture is illustrated in Fig. 6. The main advantage of this solution is its reliability. Besides, the MUT may be a software component within the AP. In this case there is no need for any additional equipment.

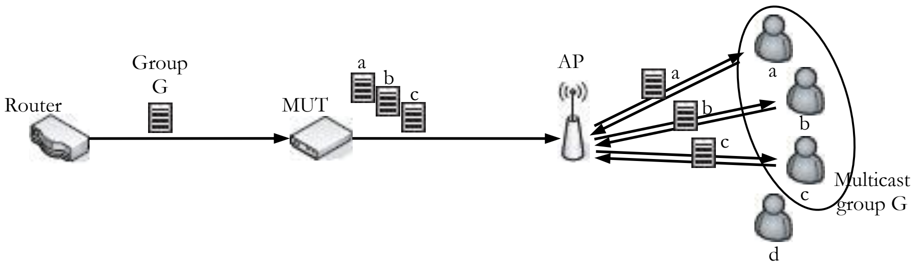


Figure 6. Network architecture of the transparent multicast/unicast translation method

This method delivers the multicast traffic reliably on the expense of the bandwidth. Besides, the average transmission time of each multicast packet is a function of the multicast group size. Therefore, this method has a very limited scalability. On the other hand, the translation method does not define a group membership management function, and suggests snooping the IGMP Join/Leave messages to learn about the available members. As we previously explained, the snooping technique is not efficient against the disconnection failure. If this failure occurs, the MUT can not detect it by snooping the messages. Thus MUT keeps copying the packets to the disconnected member. This significantly impacts the throughput since the other members will be served after reaching the retry limit of the packets addressed to the disconnected device. We note that the translation procedure does not propose any solution to deal with the disconnection failure.

2.4.1.4 Reliable Access Multicast Protocol (RAMP)

RAMP [47] allows each receiver to acknowledge sequentially. This protocol defines new control packets instead of modifying the standard ones: Multicast RTS (MRTS), Multicast CTS (MCTS) and Multicast ACK (MACK). Besides, RAMP encapsulates the multicast traffic into a new data packet type called Multicast DATA (MDATA). Unlike the standard RTS, MRTS has a variable number of destination addresses instead of a single one. These addresses identify the receivers in the acknowledgement order. The MRTS/MCTS exchange is used in two cases: 1) to deliver the first packet of a multicast flow and 2) to retransmit a packet. The other multicast packets are transmitted without handshaking in order to reduce the control overhead. The transmission procedures, with and without MRTS/MCTS, are illustrated in Fig. 7(a) and (b), respectively. The MRTS/MCTS exchange allows the sender to determine the available members since only these receivers reply with MCTS. If a receiver is no longer available, it does not reply. Thus, its disconnection is detected. Therefore RAMP resolves the issue of the disconnection failure. Following the handshaking, the source sends MDATA. This packet lists the receivers which should acknowledge and the reply order. Once the active members are determined, the sender disables MRTS/MCTS and sends the next packets without handshaking. If the feedback of at least one member is missing, the multicast source exchanges MRTS/MCTS before retransmitting the multicast packet. This is because the feedback failure may be caused by the departure of a group member.

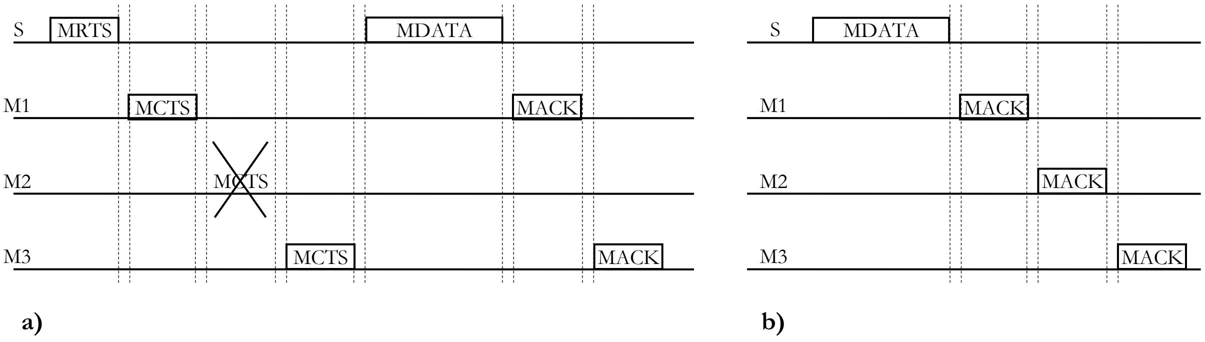


Figure 7. RAMP transmission procedures: a) transmission of the first packet and packet retransmissions, and b) packets (except the first one) transmitted for the first time

We note that the right functioning of RAMP requires the ability of all the group members to receive one another's MCTS/MACK correctly. This is because the 802.11 standard requires that a station should defer any transmission for a delay of EIFS (i.e. SIFS + DIFS + ACKTxTime) following the reception failure of a packet. Therefore, if member 2 (M2) in Fig. 7(b) fails to receive correctly the MACK of M1, then M2 should defer any transmission for the aforementioned duration. Thus, M2 does not acknowledge. As a result, the multicast source considers that the multicast transmission failed and retransmits the packet using more overhead (i.e. MRTS/MCTS). We note that the multicast receivers are not always able to hear their respective transmissions since they may be located at the opposite sides from the sender. Therefore RAMP may fail frequently in real networks.

It is worth noting that the use of MRTS/MCTS may be more frequent than expected. This is because the loss rate caused by the collisions may be very important (e.g. loss rate > 40%). The excessive use of control packets and the individual acknowledgement of each receiver increase significantly the incurred overhead and reduce the efficiency of RAMP. Besides, this overhead is a function of the group size. Hence, RAMP has a limited scalability.

2.4.2 Negative Acknowledgement based Multicast Protocols

2.4.2.1 Leader Based Protocol (LBP)

The main characteristic of LBP [53] is that this protocol dedicates one single acknowledgement slot time for all the members, regardless of the multicast group size. In this way, the protocol ensures the scalability of the multicast service. The operation of LBP relies on the selection of one member as the group leader. The leader is the only allowed node to acknowledge the successful reception of all the packets. In addition, all the multicast receivers are allowed to send a NAK upon the reception failure. If the data packet is correctly received by all the members, only the leader's ACK is transmitted. Otherwise, at least one NAK is sent. The transmitted NAKs aim at damaging the leader's ACK, if any. Once the ACK is missing, the sender retransmits the data packet. The transmission procedure of LBP requires the use of the RTS/CTS handshaking. The RTS notifies the receivers about the multicast packet and its duration. Therefore the RTS allows the members to build a NAK and to transmit it at the appropriate instant if the data packet is lost. We note that the RTS is necessary to build a NAK. This is because the errors may be every where in an erroneous packet, including in the MAC header. Therefore, the corrupted packet alone is not enough to build an appropriate feedback. The transmission procedure of LBP is illustrated in Fig. 8.

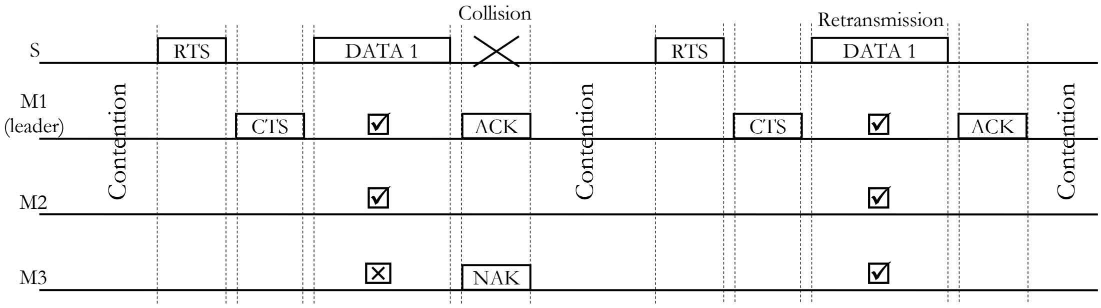


Figure 8. LBP transmission procedure

LBP does not define any specific procedure to select the leader. Hence, the first member joining the group is designated as the leader by default. This selection policy limits the reliability of LBP particularly if the leader is not the farthest member from the multicast source. In this scenario, the reception signal strength of the ACK is likely to be higher than that of several other NAKs. Therefore the ACK may be received correctly even if several NAKs are simultaneously transmitted [57]. In this case the multicast packet is not retransmitted. Moreover, the NAK principle of LBP can be used to notify the reception status of a single packet at a time. Therefore, it is neither appropriate for the block transfer nor for the packet aggregation of 802.11n. Besides, LBP does not consider the sequence numbers to build the negative feedbacks. Thus, some useless retransmissions may occur, wasting the bandwidth. The need for RTS/CTS is another weakness of LBP since this exchange incurs an important overhead and limits the protocol efficiency. However, the major weakness of LBP is that this protocol is not compliant with the collision avoidance principle of 802.11.

2.4.2.2 Reliable and Efficient Multicast Protocol (REMP)

REMP [54] is defined to enhance both the reliability and the efficiency of the multicast transport of the 802.11 standard. This protocol adapts the NAK principle with the packet aggregation feature of 802.11n. REMP defines additional control packets called Multicast Feedback Request (MFR) and Multicast Channel Acknowledgment (MCA). These packets are periodically exchanged between the AP and the group members in order to measure the reception signal strength of each receiver, and to select the group leader with the weakest SNR. Besides, the protocol defines the Multicast Transmission Announcement (MTA) and the Multicast Block Ack (MBA). The former is transmitted before each A-MPDU, and announces the multicast transmission in addition to the designated leader. Upon the reception of the A-MPDU, the leader replies with MBA. The other receivers do nothing if they obtain all the aggregated MPDUs correctly. Otherwise, a member sends a NAK in order to damage the MBA, if any. The NAK transmission causes the AP to request an individual feedback from each member. We note that the transmission procedure of REMP implies three possible cases:

1) The channel remains idle following the A-MPDU transmission. This case occurs if the designated leader fails to receive the MTA. Therefore, the AP retransmits the entire A-MPDU, preceded by a MTA.

2) The AP receives the leader's MBA correctly. Hence it concludes the transmission success toward all the group members.

3) The AP fails to receive the MBA but senses the channel to be busy following the A-MPDU transmission. This case occurs if a NAK is transmitted simultaneously with the leader's feedback. Since the AP is unable to determine the missing MPDUs, it switches to the individual feedback procedure. Therefore the multicast source sends a MFR and each member sequentially replies with a MBA. These feedbacks allow the AP to retransmit the appropriate packets and to update the group leader. This scenario is depicted in Fig. 9.

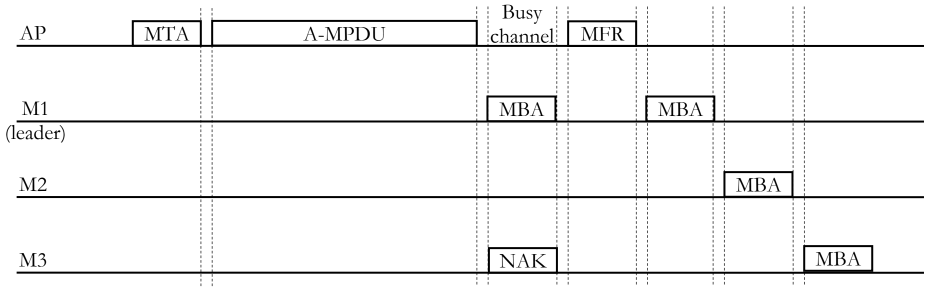


Figure 9. REMP transmission procedure: case of simultaneous transmission of MBA and NAK

Although REMP relies on both NAK and ACK principles, we classify it as a NAK-based protocol since it switches to the individual feedback following the NAK step. It is worth noting that REMP defines an accurate leader selection procedure which allows the member with the worst channel condition to be the group leader. Therefore, any NAK is likely to prevent the successful transmission of the leader's MBA. Although the first feedback step is NAK-based and does not incur an important overhead, we believe that REMP does not scale well for large multicast groups. This is because sending an important number of aggregated packets and increasing the group size, lead to an increased probability to have at least one NAK transmission for each A-MPDU. Therefore the proposed scheme is expected to request frequently individual feedbacks following the NAK step. This increases the transmission overhead and reduces the protocol throughput significantly. Besides, the success of the leader selection and of the individual feedback recovery is subject to the condition that each member is able to receive the acknowledgements of the other members correctly. Otherwise, the sequential reply may be cut frequently as previously explained. Recall that the major issue of REMP is that the colliding NAK policy is not compliant with the collision avoidance principle of the IEEE 802.11.

2.4.2.3 802.11MX

802.11MX is proposed in [55] as an extension to IEEE 802.11. We highlight that this proposal is not defined by any 802.11 working group and is not an approved extension. It defines a new NAK-based transmission procedure. However, the protocol makes use of tones instead of packets in order to reply. The transmission procedure of 802.11MX is as follows. After the channel contention, the multicast sender transmits a RTS then senses the medium. This packet announces the multicast transmission and allows the receivers to reply at the appropriate moment with a NAK tone if necessary. Besides, if the group member is not ready to receive the multicast packet, it sends a tone following the RTS. If the AP senses the medium to be busy following the RTS, it cancels the data transmission. Otherwise, the AP sends the multicast packet then senses the medium. Only members missing the packet are allowed to send a NAK tone. This tone allows the AP to detect the transmission failure and to retransmit the packet. We note that this protocol does not require a leader. Besides, the disconnection failure of any member does not interrupt the multicast service. The transmission procedure of 802.11MX is illustrated in Fig. 10.

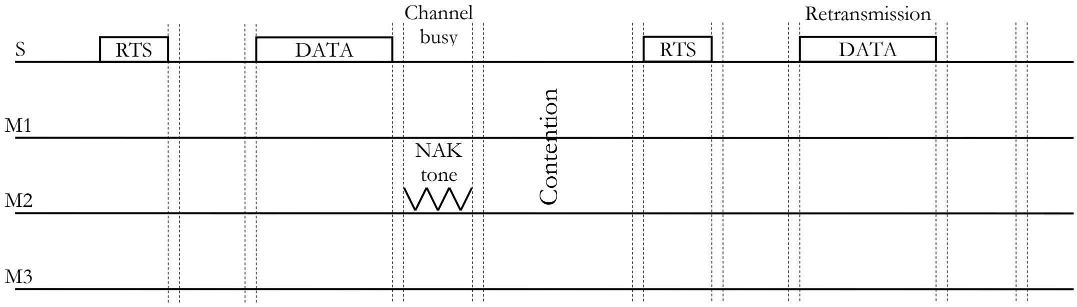


Figure 10. 802.11MX transmission procedure

802.11MX inherits many of the weaknesses of NAK protocols. First, it is not appropriate for block transfer and for the aggregation feature of 802.11n. Second, it does not record the sequence number. Hence useless transmissions may occur. Third, it is not compliant with the 802.11 standard, and requires hardware updates in order to be supported by the existing terminals. Besides, it does not ensure a perfect reliability of the multicast transport; if the RTS is lost, it becomes impossible to detect the transmission failure of the multicast packet. Furthermore, if the missing packet is not immediately notified using the NAK tone, there is no way to request it later.

2.4.2.4 Pragmatic General Multicast (PGM)

PGM [66] aims at providing a reliable multicast transport over the entire delivery path between the sender and the receivers. This protocol belongs to the transport layer and is considered as a scalable alternative to TCP for the multicast transport. Therefore, it runs transparently over any access technology, including 802.11 WLANs. We note that [66] does not provide default values for the different parameters of PGM. Therefore we present the protocol based on the considered values in [80]. The PGM source sends sequenced multicast data packets, called Original Data (ODATA). The receivers build and transmit NAKs upon the detection of a gap in the sequence numbers. The NAK is transmitted following a random backoff time. We note that this backoff procedure is different from that of 802.11. The PGM backoff time is randomly chosen from a period of 50ms. Following the NAK transmission, the receiver and any Network Element (NE) expect a NAK Confirmation (NCF) from the upstream NE. If the NCF is missing within a delay of 0.5 second, the NAK is retransmitted. But if the confirmation is still absent within a total delay of 2 seconds, the NAK is deleted. We note that a NAK/NCF exchange is required for each missing multicast packet. This is because PGM is expected to recover from the limited loss rate of the wired networks. Hence if a gap of 10 exists between the last recorded sequence number and that of the recently received ODATA, 10 NAKs and 10 NCF are exchanged. On the other hand, the PGM router replies with a NCF to each received NAK, but forwards to the upstream node only one copy of all the NAKs corresponding to the same ODATA. The multicast sender first replies with a NCF upon the reception of a NAK, and then retransmits the multicast packet, called the Repair Data (RDATA). We illustrate the transmission procedure of PGM in Fig. 11.

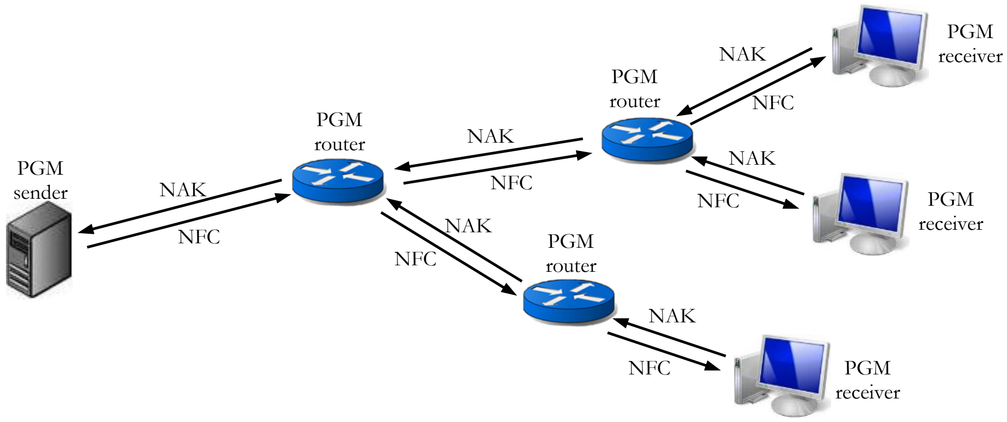


Figure 11. PGM NAK/NFC dialog

Similarly to TCP, PGM requires the server itself to retransmit the missing data. Besides, PGM incurs higher recovery latency than TCP. This is because the NAK is subject to a backoff time. Therefore, PGM is not appropriate for time sensitive applications. Besides, its performance is very limited over 802.11 networks. This is because the multicast transport of the MAC layer is not reliable, and the loss rate over the wireless channel may be very important (e.g. more than 40%) due to the collisions and to the path loss. Therefore, PGM receivers may generate an important number of NAKs. These feedbacks contend for the channel at the MAC layer and further increase the collisions and the loss rates. Besides, they incur an important overhead and limit the network throughput. As this overhead is a function of the group size, we believe that the scalability of PGM is expected to be very limited over 802.11 networks. We highlight that the loss recovery using PGM increases the load of the entire multicast path and not only the wireless hop. Furthermore, the 802.11 standard defines multiple data rates with different ranges. The selection of the appropriate one requires the loss detection at the MAC layer itself. Thus PGM does not allow the data rate adaptation in the wireless networks. In order to allow PGM to operate efficiently over the WLAN, it is necessary to implement a reliable and scalable multicast protocol at the MAC layer. Such a protocol limits the retransmission delays and is suitable for both time sensitive and delay tolerant multicast services.

2.4.3 Pseudo-broadcast based Multicast Protocols

2.4.3.1 Pseudo-broadcast for Multi-room IPTV Distribution

In [67] the authors try to enhance the quality of IPTV channels over 802.11 networks while retaining the scalability of the multicast transport. Therefore they propose a simple pseudo-broadcast scheme which converts a multicast TV stream into a unicast flow and delivers it to one selected group member. The other members, however, are configured in the promiscuous mode in order to forward the unicast packets to their upper layer. When only one member is in the network, it is designed as the unicast destination. But if more than one receiver is available, then the AP should select one target for the multicast session. The proposed selection procedure aims at designating the member with the worst link quality as the unicast receiver. Therefore, the AP polls the group members periodically in order to recover their loss statistics during each period. These reports allow the multicast source to select a receiver. The initial polling period is 100ms and is exponentially increased up to 3200ms if the medium state is stable and the designated receiver has not changed.

This solution is quite compliant with the 802.11 standard and requires few software updates in order to be used. Furthermore, it incurs a limited overhead and scales for large groups. Although this scheme slightly improves the reliability of the multicast transmissions over the wireless medium, it does not resolve the unreliability issue efficiently. This is because the packet losses are not always correlated between the different receivers. Thus, the designated station may receive a given packet correctly while one or many other members miss it. Besides, only the member experiencing the highest loss rate is selected. The others, however, should deal with their losses.

2.4.3.2 Leader-Based Multicast Service (LBMS)

LBMS [68] is another pseudo-broadcast protocol. It does not specify how the leader is selected, but the authors suggest that the member experiencing the highest loss rate is designated as the group leader. Once the leader is selected, the AP sends a LBMS report to notify the designated station. This leader is then responsible for acknowledging each successfully received multicast packet. Therefore, LBMS requires neither converting a multicast stream into unicast nor configuring the receivers into the promiscuous mode. This protocol does not require an important overhead. Therefore it is scalable. However, as the authors acknowledge, LBMS is not fully reliable but is a semi-reliable protocol. Thus, it does not ensure the quality of the multicast service.

2.4.3.4 Semi-Reliable Multicasting (SRM)

Similarly to LBMS, SRM [69] does not convert multicast traffic into unicast and selects a leader to acknowledge each multicast packet. However, the main novelty in SRM is that the leader is selected in a round robin fashion. The authors choose this procedure because they believe that it is impossible to select the station with the worst SINR link for every transmission. In their opinion it is difficult to keep track of time-varying SINRs of all the multicast receivers in real-time.

SRM inserts the identifier of the designated leader in the header of each multicast packet. This identifier allows the appropriate receiver to reply with an ACK upon the reception success, and is dynamically modified in order to involve all the group members. Hence, each member is responsible for replying to a given number of packets. This number is variable and depends on the loss statistics. Its initial value is 4, and is increased by 5 following every transmission failure. Besides, a receiver is designated leader for up to 50 packets before moving to the next receiver in the group. The authors motivate this variable value by the need to allow a station with a bad channel condition to serve as a leader for a longer duration.

Like the aforementioned pseudo-broadcast protocols, SRM is not fully reliable and may reduce the quality of video streaming applications considerably. Furthermore, SRM can not determine the link quality of all the group members at the same time. Therefore it can not adapt the transmission rate properly.

2.4.3.2 DirCast

In [70], authors design the DirCast system to enhance the QoS of multicast services over the IEEE 802.11 networks. DirCast selects one member called "target client" for each multicast group, then sends multicast packets in unicast to the selected client. The other clients receive the packets by monitoring the channel in the promiscuous mode. Since transmission failures may occur while listening in the promiscuous mode, DirCast sends extra Forward Error Correction (FEC) packets. These packets allow the non-target members to recover any packet they miss. However, the transmission of the additional packets increases the overhead and may incur congestion losses. Furthermore, only clients in the promiscuous mode may participate in the multicast sessions. However, the use of this mode increases the kernel processing load and reduces the system performance.

2.4.4 Other Protocols

2.4.4.1 SoftCast

SoftCast, a cross-layer design for mobile multicast video, is presented in [71]. SoftCast compresses the video pixels to bit sequences as a video codec would do, then maps these bits to complex samples in order to protect them from channel errors and packet losses, as a PHY layer would do. However, the SoftCast encoder uses only linear real codes for both compression and channel coding in order to ensure that the final coded samples are linearly related to the original pixels. Therefore, increasing the channel noise progressively perturbs the transmitted bits in proportion to their importance to the original video; a high-quality channel perturbs only the least significant bits while bad channel conditions still preserve the most significant bits. Thus, each receiver decodes the received signal into a video whose quality is proportional to the quality of its specific instantaneous channel.

The design of SoftCast relies on the following 3 assumptions. 1) The bit errors are caused only by the channel noise. 2) All received packets are processed and forwarded to the upper layer even if they contain errors. 3) Neither feedback nor bit rate adaptation is used. However, the first assumption is not compliant with a typical 802.11 network where errors and losses are frequently caused by interferences and collisions. In this case, the received bits are correlated with the collision source content and not with the original video pixel. In SoftCast, all received packets are processed even if they contain errors. However, an error may occur in the MAC header, preventing the MAC layer from forwarding the packet to the appropriate application. Moreover, SoftCast can not use any encryption algorithm to protect the data because this will remove the wanted linearity between the transmitted signal and the original video pixel.

2.4.4.2 Medusa

Medusa [72] is designed to allow the packet retransmission based on the encapsulated content priority. Yet the retry policy is implemented and managed by a third party server called *the medusa proxy*. This proxy is installed between the video server and the AP. The proposed retry policy operates based on "reception reports" periodically generated by each client and emitted to the proxy through the AP. Such a design incurs important delays for packet loss recovery since the proxy should wait for the following report of each client to decide whether a particular packet should be retransmitted or not. Besides, the 802.11 MAC layer can not detect the transmission failures. Therefore, it can not adapt the transmission rate, and the lowest one is selected by default. This impacts the throughput of Medusa significantly.

2.4.4.3 QoS-Directed Error Control scheme (QDEC)

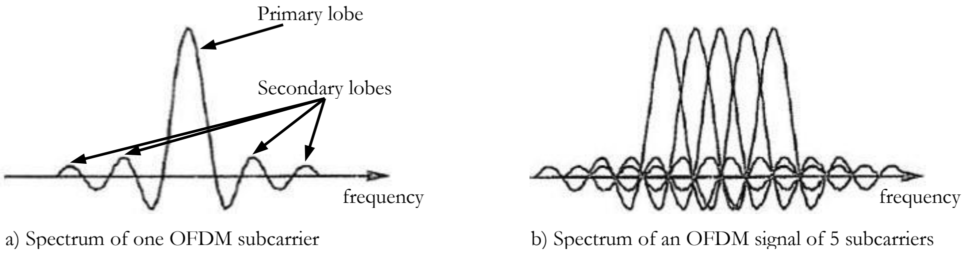
Many researches focus on the use of Forward Error Correction (FEC) in order to enhance the reliability of the multicast transport [73-76]. An *(n,k)* FEC scheme encodes *k* source data packets into *n* packets, where $n > k$. The reception and the decoding of any *k* among the *n* transmitted packets, allow the receiver to construct the original data. The QDEC scheme [73] is defined for video multicasting in wireless networks. It classifies the video frames into *essential* and *optional* images, and transmits the former category with error control while the optional images are delivered using the legacy multicast. QDEC defines three error control algorithms to deal with the loss of packets belonging to the essential images: FEC_only, FEC_Retrans and Retrans_only. The first one is used to recover from a limited packet loss rate. When this rate increases, FEC alone is no longer efficient. Thus the second algorithm is used. FEC_Retrans combines the FEC and the transmission of redundant packets. The redundant transmissions reduce the loss rate and allow the FEC scheme to operate properly. Finally, Retrans_only works in the worst condition. In this case the losses exceed the capacity of any FEC that the sender and the receivers can afford.

FEC schemes require a high processing capability of both the sender and the receivers. Therefore, they increase the power consumption and reduce the processor availability. However this availability is responsible for processing the incoming packets. Thus, a processor with a limited availability may ignore many arriving packets [112], and the impact is similar to packet losses. We note that QDEC does not define any feedback policy. Such a policy is necessary for the sender to select the most appropriate data rate. Therefore, the right functioning of QDEC requires the transmission of the multicast packets at the lowest data rate. In this case, the protocol suffers from a very limited efficiency even when the channel condition is good and convenient for high transmission rates.

2.4.4.4 OFDMA-based Multicast ACK (OMACK)

In [77] the authors propose a new multicast protocol for the OFDM physical layer. OMACK attributes one subcarrier to each multicast member. Upon the successful reception of a multicast packet, a member sends a BPSK symbol with a value of 1 over the assigned subcarrier. The authors expect that their protocol allows the multicast sender to detect any missing feedback and to retransmit a lost packet if necessary.

This solution is not realistic for wireless networks for the following reason. An OFDM subcarrier has one strong side lobe in addition to several secondary lobes. The value of a secondary lobe is very weak compared to the principal lobes of all the subcarriers received from the same member. Fig. 12 depicts an example of an OFDM subcarrier and an OFDM signal of 5 subcarriers. However, the secondary lobe of a subcarrier may be very important compared to the primary lobe of another subcarrier received from a different member. This is because 802.11 devices are able to communicate with a reception signal strength of -75dBm (Cisco recommendation) and higher. Thus the primary lobe of a subcarrier received at -45dBm is about 1000 times stronger than the primary lobe of another subcarrier received at -75dBm. In this case, the secondary lobes of the first subcarrier hide the main lobe of the second one. This prevents the sender from extracting the different feedbacks. Thus OMACK can not exist in real wireless networks.



a) Spectrum of one OFDM subcarrier

b) Spectrum of an OFDM signal of 5 subcarriers

Figure 12. OFDM Subcarriers

2.5 Conclusion

In this chapter we present the requirements for delivering video streams over IP networks. Particularly, we focus on the case of video multicasting. Then we introduce IEEE 802.11 as the widely used access technology. We present the principal network modes (i.e. Infrastructure, Ad hoc and Mesh). Then we list the different supported data rates of the PHY layer, and we show that the use of non-overlapping channels is necessary to avoid the interference between co-located WLANs and to enhance the network throughput. On the other hand, we introduce the principal operating modes of the MAC layer and particularly: the different priority levels, the unicast feedback policies and the roles of RTS/CTS handshaking. We highlight that the multicast transport of the MAC layer does not use any retransmission mechanism and is therefore unreliable. We describe the different solutions which enhance the quality of video multicasting over 802.11 networks. We classify most of these proposals into three principal categories: ACK-based, NAK-based and pseudo-broadcast protocols. We show that none of these solutions is able to define a reliable, efficient, standard-compliant and low-latency multicast protocol. Therefore, it is necessary to define a new feedback policy which satisfies the requirements of video streaming applications and retains the transport scalability.

Chapter 3

3 Evaluation of IEEE 802.11v/aa

3.1 Introduction

The multicast transport is becoming popular nowadays due to the increasing deployment of the multimedia services over the IP networks. On the other hand, the IEEE 802.11 standard defines the principal wireless access network. However, the legacy multicast transport of this standard does not ensure any reliability for the delivered traffic. Therefore, the multicast packets may experience a very important loss rate which degrades the quality of the offered services significantly.

Recently, two amendments to the standard have been defined: 802.11aa and 802.11v. The first one introduces the Groupcast with Retries (GCR) service which proposes two retransmission policies: Block Ack (GCR-BACK) and Unsolicited retry (GCR-UR). On the other hand, 802.11v defines the Directed Multicast Service (DMS). In this Chapter we introduce these new protocols and we compare their performance. Particularly we evaluate their throughput and scalability as a function of the multicast group size. Besides, we measure their reliability. We compare these new proposals using analytical and simulation results. We demonstrate that DMS has the lowest scalability while GCR-BACK is not appropriate for large multicast groups. We show that GCR-UR is the most appropriate for large groups. However, increasing the number of the transmission retries reduces significantly the achieved throughput of the unsolicited retry policy.

The remainder of this chapter is organized as follows. In Section 3.2 we introduce the most relevant works having studied the 802.11v/aa amendments. We investigate the novelties of 802.11v and of 802.11aa in Sections 3.3 and 3.4, respectively. We dedicate Section 3.5 to present our analytical model. We present the analytical and the simulation results in Section 3.6. Finally, we conclude this chapter in Section 3.7.

3.2 Related Work

IEEE 802.11aa/v have recently been approved, but not implemented within real equipments and in network simulators yet. Therefore few works have evaluated and compared the new multicast protocols. In [81], the authors provide a general presentation of GCR and DMS. Besides, they introduce the new buffering architecture of 802.11aa. However, they do not evaluate any of the following parameters: throughput, scalability, delays and loss rate. In other words, the paper only provides a global overview of the aforementioned amendments without being able to evaluate and to compare any of the key parameters of the new retry policies.

In [82], the authors evaluate and compare the new amendments using OPNET simulator [85]. They compare the scalability, delays, efficiency and reliability of the legacy multicast, DMS, GCR-BACK and GCR-UR. However we notice the following two major limitations. First, the authors consider a partial evaluation of GCR-BACK. Thus, they consider that only one member is allowed to send a feedback. This simple scenario requires few modifications to the unicast BACK mechanism already implemented within the network simulator. However, it can not evaluate the scalability of GCR-BACK since it does not allow the evaluation of the impact of the multicast group size on the network throughput and on the delivery delays. Besides, this scenario is not accurate in measuring the reliability of GCR-BACK. This is because the obtained loss statistics are mainly caused by the absence of feedbacks from the other members. Therefore, they do not illustrate the protocol reliability. The second limitation of this work is that there is no analytical validation of the obtained results. We believe that an analytical model is required, not only to validate the simulation results but also to provide an easy performance estimation for any particular network configuration, such as the expected throughput for a given group size and a specific transmission rate. This is because simulation results can not cover all the use cases while an analytical model can.

In [83], the authors introduce the operating mode of 802.11aa/v. They evaluate the reliability and the overhead of the different multicast protocols as a function of the packet error rate (PER). Their results show that none of the different proposals is reliable. This is because the authors consider all the loss factors together, including the queue drops. However, this factor depicts the networks congestion and is not related to the multicast protocol. Thus, these results are not accurate in evaluating the reliability of the different protocols. Besides, the authors do not evaluate the throughput; they only measure the overhead ratio. Moreover, they do not evaluate the delays and they do not show the impact of the group size on the protocol scalability. Furthermore, the authors do not provide any analytical model to determine the throughput under various network configurations. Therefore, it is not possible to deduce the efficiency of transmission rates other than the used one (i.e. 54Mbps).

In [84] the authors evaluate the impact of the collisions on the throughput of 802.11aa/v. But they do not evaluate the maximum throughput of the different multicast protocols when the medium is not shared with other flows. Besides, they do not consider any protection mechanism against the simultaneous access to the medium, unlike what is required by 802.11aa. Such a protection would enhance the reliability and the throughput of GCR-UR and GCR-BACK significantly. Hence, it is necessary to revise the proposed analytical model in order to consider a collision prevention feature. According to the obtained results, none of the protocols is reliable. This is because the authors consider a particular scenario of a highly loaded network in addition to a high throughput video. Therefore, an important number of packets are rejected due to the queue overflow. Thus, we believe that the major limitation of this work is that it does not show when the aforementioned protocols are reliable and when they are not. Furthermore, they do not evaluate the incurred transmission delays and they limit their evaluations to a group of 16 members only. We believe that this is a very limited size, particularly with the increasing need for off-loading mobile networks to 802.11 WLANs, and with the intention of many 802.11 working groups to exceed the transmission rate of 1Gbps. Thus, it is expected to have large multicast groups within the same WLAN.

We note that none of all the aforementioned studies has introduced any of the following new features: GCR Service Period (GCR-SP) and GCR-Active (GCR-A) defined by 802.11aa, and Flexible Multicast Service (FMS) introduced by 802.11v. These new mechanisms tackle the power management when a multicast traffic is being delivered. Furthermore, a data rate selection procedure is added for the first time into IEEE 802.11. This procedure in defined by 802.11v for the multicast transmissions. However, this news is still unknown to the research community. Therefore we hope to introduce it and to highlight its weaknesses.

3.3 Overview of IEEE 802.11v

3.3.1 Directed Multicast Service (DMS)

The IEEE 802.11v amendment [2] defines the Directed Multicast Service (DMS) in order to resolve the unreliability issue of the multicast transport. This service allows the members to receive the multicast traffic as individually addressed packets (i.e. using the unicast transport). Therefore, DMS guarantees the same unicast reliability degree to the multicast transport at the expense of the bandwidth. Hence, it can be used to stream a standard traffic to a limited group size, but does not scale well for high throughput streams like HDTV. Moreover, DMS does not allow the use of the block transfer. We note that 802.11v defines the required procedures to establish DMS sessions but does not define any functionality to manage the multicast groups and to detect their members. According to the amendment, the method an AP uses to determine the multicast group members is outside the scope of IEEE 802.11, but is typically performed by snooping IP packets.

3.3.2 Data Rate Adaptation

802.11v defines a rate adaptation procedure for the multicast transmissions. The data rate is selected according to the following steps. In the beginning, the AP sends a Multicast diagnostic request in a Radio Measurement Request frame indicating the measurement duration. This packet includes the address of one or many multicast sessions to be considered. Besides, it is transmitted in multicast if all the associated stations support the diagnosis capability. Otherwise, the packet is individually addressed to the compliant nodes. This request can be ignored by receivers which did not join any of the mentioned sessions. On the other hand, the group members start counting the number of received packets from the specified sessions, and record the maximum observed data rate to receive these packets. These values (i.e. the number of the received packets and the maximum used data rate per joined multicast address) are then returned to the AP in a Radio Measurement Report.

Triggered reports are also defined and allow the AP to gather statistics from the group members without having to send diagnostic requests periodically. These reports are transmitted subject to the following two conditions: 1) the multicast trigger condition occurs, and 2) the specified delay between two successive reports, called re-activation delay, expires. The trigger condition occurs when no multicast packet is received within a specific time period. But this period may be unspecified. In this case the trigger condition is always true, and the reports are sent every re-activation period. This period should be greater or equal to a minimum threshold in order to limit the number of generated reports. These reports indicate the number of received packets and the highest data rate per joined session, since the previous diagnostic request. Therefore, it is necessary that the AP sends a new request each time the data rate is modified. This allows the members to report the recently observed highest data rate.

We notice many performance issues for this procedure. First, the diagnostic request may be lost when it is transmitted in multicast. Therefore, some solicited reports may be missing and this may reduce the accuracy of the selected data rate. Besides, probing high transmission rates may cause the loss of all the delivered packets during the measurement periods. Therefore the quality of the multicast services may be disrupted frequently. Moreover, this selection procedure is not appropriate for large multicast groups since an important collision rate may occur between the different reports themselves and between these reports and any other traffic (particularly multicast packets). This reduces the network throughput and further increases the loss rate of the multicast traffic.

3.3.3 Flexible Multicast Service (FMS)

The Flexible Multicast Service (FMS) intends to reduce the power consumption of the multicast receivers. It allows a group member in the power save mode to request an alternate Delivery Traffic Indication Map (DTIM) interval for the multicast traffic. FMS defines 8 alternate intervals from 1 to 8. The first one corresponds to 2 DTIM intervals and each successive interval is one DTIM interval larger. The multicast packets are buffered then sent in one block following the selected alternate interval. Recall that a DTIM is a variable number of Beacon intervals and that the legacy PS mode delivers multicast packets in one block each DTIM. Therefore, FMS allows the AP to schedule the transmission of the multicast packets at longer intervals. This allows the stations to spend more time in the doze state, and allows a significant energy saving compared to the legacy procedure.

We note that FMS is accurate for low bit rate and delay-tolerant multicast streams. This is because packets may be buffered for more than one second at the AP. During this time, a limited number of packets may be stored without queue overflow. Similar to the legacy PS procedure, FMS is not appropriate for high throughput applications such as video services. Moreover, many packets may arrive and cause the queue overflow. Since FMS delivers the multicast traffic in one single burst, the channel may be used for very long transmission durations. This may be an impediment for time-sensitive flows sharing the medium.

Furthermore, FMS enables the group members to request a specific data rate. Therefore, the AP selects any transmission rate equal or lower than the lowest rate value provided by the associated members.

3.4 Overview of IEEE 802.11aa

3.4.1 Stream Classification

The 802.11aa amendment [3] defines MAC enhancements for robust audio and video streaming. Hence, it defines additional transmit queues called Alternate VO (A_VO) and Alternate VI (A_VI). Incoming packets from the upper layer are mapped similarly to 802.11e except that flows with UP of 7 and 4 are buffered in A_VO and A_VI respectively. These new queues are optional and may be disabled. In this case only the four principal queues (i.e. VO, VI, BE and BK) are used. We note that the standard does not define new EDCA functions for A_VO and A_VI. Therefore they share the same access functions as VO and VI as illustrated in Fig. 13. Packets are selected from the primary and alternate queues in such a way that packets with higher UP are selected with higher priority. However, 802.11aa does not define a specific scheduling function, but requires that the default algorithm selects the transmission queue according to the selection procedure of IEEE 802.1Q [86]. Therefore, the packets are selected by default based on the strict priority algorithm. This algorithm selects packets from the highest priority queue (i.e. in our case A_VO and VI) whenever this queue is not empty. Otherwise, the other queue is processed.

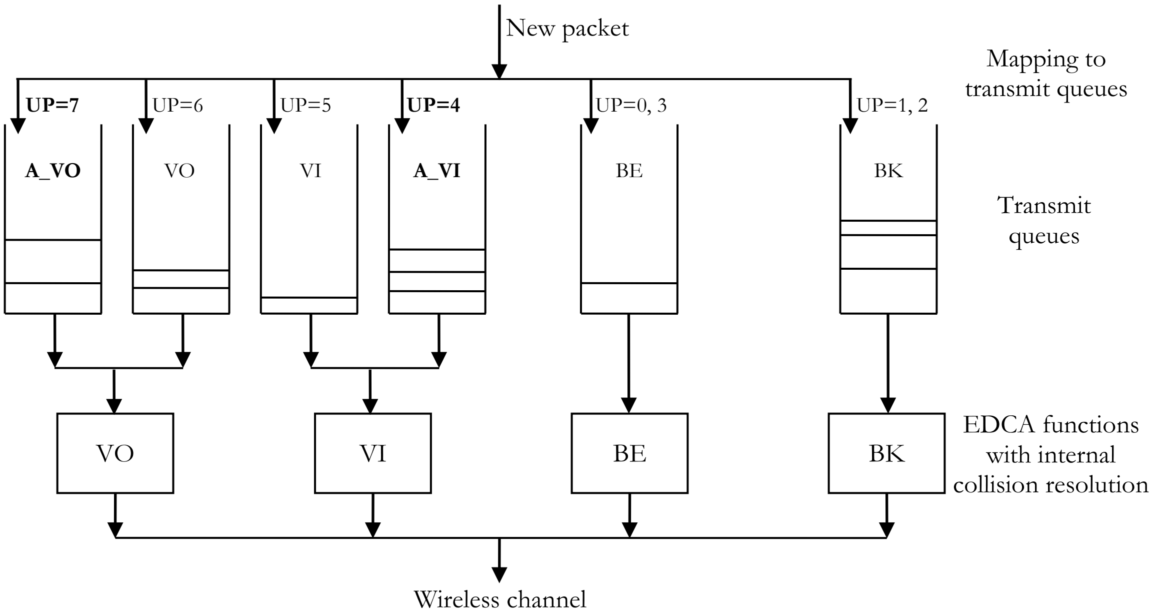


Figure 13. Primary and alternate transmission queues of 802.11aa

As we observe, one alternate queue (i.e. A_VO) has more priority than a primary queue (i.e. VO). Then another primary queue (i.e. VI) has more priority than a second alternate queue (i.e. A_VI). Hence, a primary queue does not always stand for a queue with the highest priority. We believe that this is confusing and is not justified. The main reason to have two different queues for voice and video streams is to give more priority for time sensitive applications. Therefore, flows with strict delay requirements (i.e. less than 200ms), such as VoIP, are delivered first, while delay-tolerant streams (i.e. about 1 second), such as IPTV, still have a high transmission priority compared to other flows.

Although the new queues are defined for both unicast and multicast flows, the principal novelty of 802.11aa is the conception of new retransmission policies and delivery methods for the multicast mode.

3.4.2 Group Membership Management

IEEE 802.11aa proposes one simple method to discover the members of the different multicast sessions. This method relies on the awareness of the receiver itself about the groups to which this receiver belongs. Thus, the AP sends a packet, called Group Membership Request, individually to every associated station in order to request the addresses of the joined sessions. Each receiver replies to this request using a Group Membership Response packet which contains the list of all the joined groups. Every time this list changes, the station sends an unsolicited Group Membership Response with the updated list to the AP. This allows the multicast source to be aware of the different members of the available multicast sessions. It is worth noting that the standard does not define any mechanism allowing the immediate detection of the unexpected departure of a group member. Therefore, if a disconnection failure occurs, the multicast source can not take the required actions in time.

In addition to the aforementioned procedure, the amendment allows the use of any other group membership detection method such as IGMP snooping. But the definition of such a procedure is beyond the scope of the current standard.

3.4.3 Groupcast with Retries (GCR)

Groupcast with Retries (GCR) service is defined to improve the reliability of the multicast transmissions. GCR defines two additional retransmission policies for the multicast flows: GCR Unsolicited Retry (GCR-UR) and GCR Block Ack (GCR-BACK). These policies allow the retransmission of multicast packets in order to reduce the loss rate. Besides, GCR defines two new delivery methods: GCR Service Period (GCR-SP) and GCR Active (GCR-A). These methods define the way the multicast packets should be transmitted under different power states, and particularly when the members are in the power save mode.

3.4.3.1 GCR Service Period (GCR-SP)

Unlike FMS, the GCR-SP method transmits the multicast packets at intervals, called service intervals, which may be smaller than the beacon interval. The AP informs the group members about the SP intervals, then sends the packets assigned to this group at the SP periods. We note that the SP duration is not limited and may reach an important number of TXOPs. Moreover, two or many SP may be linked. During all this time, only the multicast stream is delivered. Therefore GCR-SP should not be used with a high throughput service in order to allow a fair sharing of the channel with other flows.

3.4.3.2 GCR Active (GCR-A)

The second delivery method of GCR is GCR-A. It allows the AP to send multicast packets at any time, regardless of the power state of the group members. When this method is used, multicast members which are in the power save mode should enter the awake state in order to be ready to receive any multicast packet. These receivers should remain awake indefinitely until the delivery method is modified or the GCR agreement is canceled (e.g. the receiver leaves the group or the multicast session is over). Therefore, this is the most appropriate method to deliver high throughput streams without impacting time sensitive flows sharing the same network.

3.4.3.3 GCR Unsolicited Retry (GCR-UR)

When the GCR-Unsolicited-Retry policy is used, the multicast source defines a retry limit, say "*N*", and transmits each multicast packet "*N*" times without waiting for any feedback after each transmission. The retry limit is not defined by the standard and is implementation dependent. Besides, GCR-UR allows the transmission of multicast packets in blocks separated by SIFS. However, a packet and its retransmission should not occur in the same block. On the other hand, the standard requires the use of a collision protection mechanism such as RTS/CTS or CTS-to-Self, in order to reduce the collision probability. The retransmission of the same packet several times, allows the sender to increase the probability of the successful delivery. The main advantage of this policy is its scalability. Therefore, it is appropriate for large multicast groups. However, its reliability depends on the retry limit and on the accuracy of the selected transmission rate. We note that 802.11aa does not define any rate adaptation scheme for GCR-UR.

The main issue of GCR-UR is that this policy does not allow the detection of packet losses. Thus, the multicast sender is not able to adapt the transmission rate when the losses are caused by the signal attenuation. Therefore the right functioning of GCR-UR relies on the use of the lowest transmission rate. In this way, the multicast packets are reliably delivered to any member in the network even those located at the limit of the coverage area. However, the use of the lowest rate causes a significant limitation of the overall network throughput. On the other hand, if a high transmission rate is used instead of the lowest one, all the members located beyond the coverage area of the used data rate (but are still connected at a lower transmission rate) can not receive the multicast packets. We note that GCR-UP may use the rate selection procedure of 802.11v. However, the limited scalability of this procedure limits that of the multicast protocol.

We highlight that the transmission of every packet several times increases the protocol reliability but reduces the network throughput significantly. Thus, losses over the wireless channel may be avoided, but rejections due to the queue overflow may occur more frequently. This may limit the reliability of the multicast traffic even though the loss rate over the wireless link is low.

3.4.3.4 GCR Block Ack (GCR-BACK)

The GCR-Block-Ack feedback policy is similar to the basic block transfer of the unicast. It allows the AP to establish a Block Ack agreement with one or many of the group members at the beginning of the multicast session. Then the sender transmits a block of multicast packets followed by multiple exchanges of Block Ack Requests (BAR) and BACKs. A member is allowed to reply only upon the reception of an explicit request. The received feedbacks allow the AP to detect any transmission failure. Furthermore, missing packets are retransmitted until their lifetime limit is reached. Therefore, the GCR-BACK guarantees the same reliability degree of the unicast transport. New agreements may be established and existing ones may be deleted during the streaming duration. If all the agreements are deleted, the AP switches to another delivery policy such as the legacy multicast or GCR-UR till all the members leave the group.

Similar to GCR-UR, the GCR-BACK policy requires the use of a protection mechanism (like RTS/CTS with one member, CTS-to-Self) to avoid the collisions. CTS, data packets, BARs and BACKs within a block transfer are separated by a SIFS period. If the medium remains idle within a period of PIFS (i.e. SIFS plus one SlotTime) after the transmission end of a BAR, the AP concludes the reception failure of the last BAR and sends it again immediately. The AP retransmits a BAR in this way until it detects a transmission before the PIFS expiry or the lifetime of all the multicast packets expires. If the AP detects the BACK transmission but does not receive it correctly, then the AP retransmits the BAR following channel contention. Besides, packets transmitted within a block are subject to the TXOP duration. Therefore, if this duration is not enough to gather all the feedbacks, the AP should interrupt the block and contends for the channel again in order to request the remaining BACKs during a new TXOP. The GCR-BACK procedure using the CTS-to-Self protection, is illustrated in Fig. 14. We note that GCR-BACK can also be used to deliver aggregated packets, i.e. A-MPDU and A-MSDU.

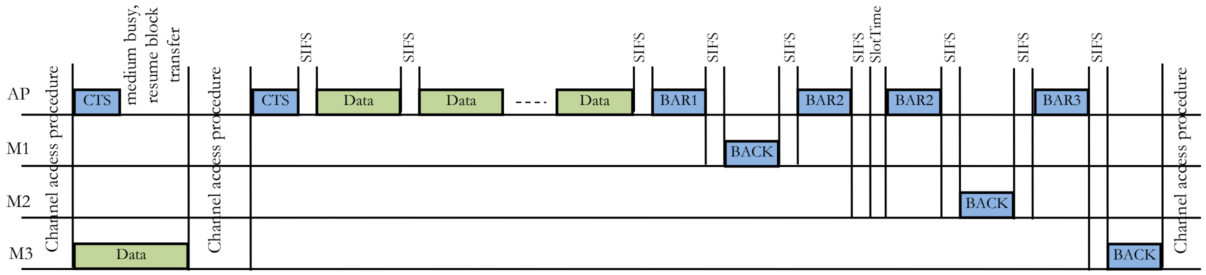


Figure 14. Typical frame exchange scenario with GCR-Block-Ack policy

The GCR-BACK policy allows the AP to adapt the transmission rate according to the loss statistics. Hence, it enables the selection of the most appropriate data rate. If a member in the group does not establish a BACK agreement with the AP, this member does not receive any BAR and is not allowed to send any feedback. In this case, the selected rate may be inappropriate for this receiver. Therefore, the AP needs the feedbacks of all the members in order to deliver the multicast stream reliably using the most appropriate data rate. However, this policy requires an important number of feedbacks. This number depends on the multicast group size. Thus GCR-BACK has a limited scalability and is not appropriate for large groups.

3.5 Model Description

In this section we define an analytical model to evaluate the throughput and the scalability of DMS, GCR-UR and GCR-BACK. We consider multicast UDP/IP packets with the maximum transmission unit size of 1500 octets. Thus the MAC packet length is 1538 Bytes. We consider that ACKs, BNRs and BNAKs are transmitted at the lowest data rate of 6Mbps and that they are always delivered successfully. This is a valid assumption since these packets have a small size and use the most robust rate.

Let G be the multicast group size. Each member in the group experiences a PER of p_i for i=1..G. We consider that losses are not correlated between different receivers. We fix the transmission limit to 7 for DMS. However, for GCR-BACK we set the limit to 100. We choose this value because the retransmission of a packet is subject to lifetime limit. Thus we fix a transmission limit by excess. We note that the probability to reach high retransmission stages is negligible when the PER is limited. Let N be the block size and Nr(k) be the number of packets transmitted for the kth time within a block. Nr(1) is the number of packets transmitted for the first time. Every block is composed of $\sum_{k=1}^{100} Nr(k)$ packets. Nr(k), k=1..100, depends on the PER of the network.

Table 7 presents the used variables and their values at different transmission rates. We consider that the CTS-to-Self is always delivered at the highest data rate of 54Mbps in order to have the shortest length. Thus, it allows the efficient detection of simultaneous transmissions (as depicted in Fig. 14).

Table 7. Parameters description and value

Variables	Values
Network	IEEE 802.11a
T_{PPDU_Data}: PHY packet duration, 1538 B.	252 µs (at 54 Mbps)
T_{PPDU_BAR}: PHY BAR duration, 30 B.	64 µs (at 6 Mbps)
T_{PPDU_BACK}: PHY BACK duration, 38 B.	76 µs (at 6 Mbps)
PROTECTION_DURATION, CTS	40 µs (at 54Mbps + SIFS)
SlotTime	9 µs
SIFS	16 µs
DIFS (SIFS + 2 SlotTime)	34 µs
CWmin: Contention Window min	15

We define X as the number of transmission attempts. The probability for a given member M_i, for i=1..G, to receive correctly a packet in any of the k first transmissions is given in Equation (1).

$$P^i(X \leq k) = 1 - p_i^k \quad (1)$$

We derive the probability to serve all the G receivers in any of the k first transmissions in Equation (2).

$$P^G(X \leq k) = \prod_{i=1}^{G}(1 - p_i^k) \quad (2)$$

We obtain Nr(1) and Nr(k), k=2..100, in Equations (3) and (4) respectively.

$$Nr(1) = N - \sum_{k=2}^{100} Nr(k) \quad (3)$$

$$Nr(k) = N(1).(1 - P^G(X \leq k - 1)), k = 2..100 \quad (4)$$

We resolve Equations (3) and (4) and we obtain Nr(k), for k=1..100, in Equation (5). It is obvious that the probability to receive a packet correctly in $X = 0$ attempts is nil, hence $P(X=0) = P^G(X=0) = 0$.

$$Nr(k) = \frac{N.\left(1-P^G(X\leq k-1)\right)}{\sum_{k0=1}^{100}\left(1-P^G(X\leq k0-1)\right)}, k = 1..100 \quad (5)$$

We express the average packet transmission time using GCR-BACK, in Equation (6). This time takes into account the minimum waiting time between two successive transmission opportunities, i.e. one DIFS, and the average backoff time. Besides, we consider the duration of any protection mechanism against the collisions. Thus, for the case of CTS-to-Self transmitted at 54Mbps, the protection duration is 40µs. It corresponds to the required time to send CTS plus one SIFS time period. Besides, the average time to send a block depends on the block size. We note that the packets within a block are separated by SIFS. Following the transmission end of the data packets, the AP exchanges BAR/BACKs with every group member. Then we divide the total time by the number of packets transmitted for the first time within a block. This allows us to obtain the average time to send one multicast packet. It is worth noting that retransmitted packets are considered as overhead and they increase the average time per packet.

$$T_{BACK}(N,G) = \Big(DIFS + \frac{CWmin}{2} \times SlotTime + PROTECTION\_DURATION + (T_{PPDU\_Data} + SIFS) \times N - SIFS + G \times (SIFS + T_{PPDU\_BAR} + SIFS + T_{PPDU\_BACK})\Big) / Nr(1) \quad (6)$$

The average packet transmission time using GCR-Unsolicited-Retry does not depend on the group size. Instead, this time depends on how many times every packet is transmitted. We define *U* as the transmission number, and we derive the average transmission time of GCR-UR in Equation (7). Similarly to GCR-BACK, we consider the waiting time, the average backoff time and the duration of the used protection mechanism. Then we add the transmission duration of the multicast packets. We multiply this duration by the retry count and we divide by the number of data packets within a block to obtain the average transmission time per packet.

$$T_{UR}(N,U) = \Big(DIFS + \frac{CWmin}{2} \times SlotTime + PROTECTION\_DURATION + (T_{PPDU\_Data} + SIFS) \times N - SIFS\Big) \times U/N \quad (7)$$

Besides, we measure the PER of GCR-UR as experienced by member M_i, for i=1..G, in Equation (8).

$$P_{UR}^i(U) = p_i^U \quad (8)$$

The average transmission time of DMS is a function of the group size. We express this average time in Equation (9). This time depends on the group size. On the other hand, the average backoff time of DMS depends on the retry count. Besides, we do not use any protection mechanism as this is not required by 802.11v.

$$T_{DMS}(G) = \sum_{i=1}^{G}\Big[\sum_{k=1}^{7}\Big(\Big(DIFS + \frac{CW(k)}{2} \times SlotTime + T_{PPDU\_Data} + SIFS + T_{PPDU\_ACK}\Big).\Big(1 - P^i(X \leq k-1)\Big)\Big)\Big] \quad (9)$$

, where *CW(k)* is the Contention Window of the k^{th} transmission. Equations (10), (11) and (12) illustrate the packet transmission rate of GCR-Block-Ack, GCR-UR and DMS, respectively.

$$Throughput_{BACK} = 1/T_{BACK}(N, G) \tag{10}$$

$$Throughput_{UR} = 1/T_{UR}(N, U) \tag{11}$$

$$Throughput_{DMS} = 1/T_{DMS}(G) \tag{12}$$

3.6 Performance Evaluation

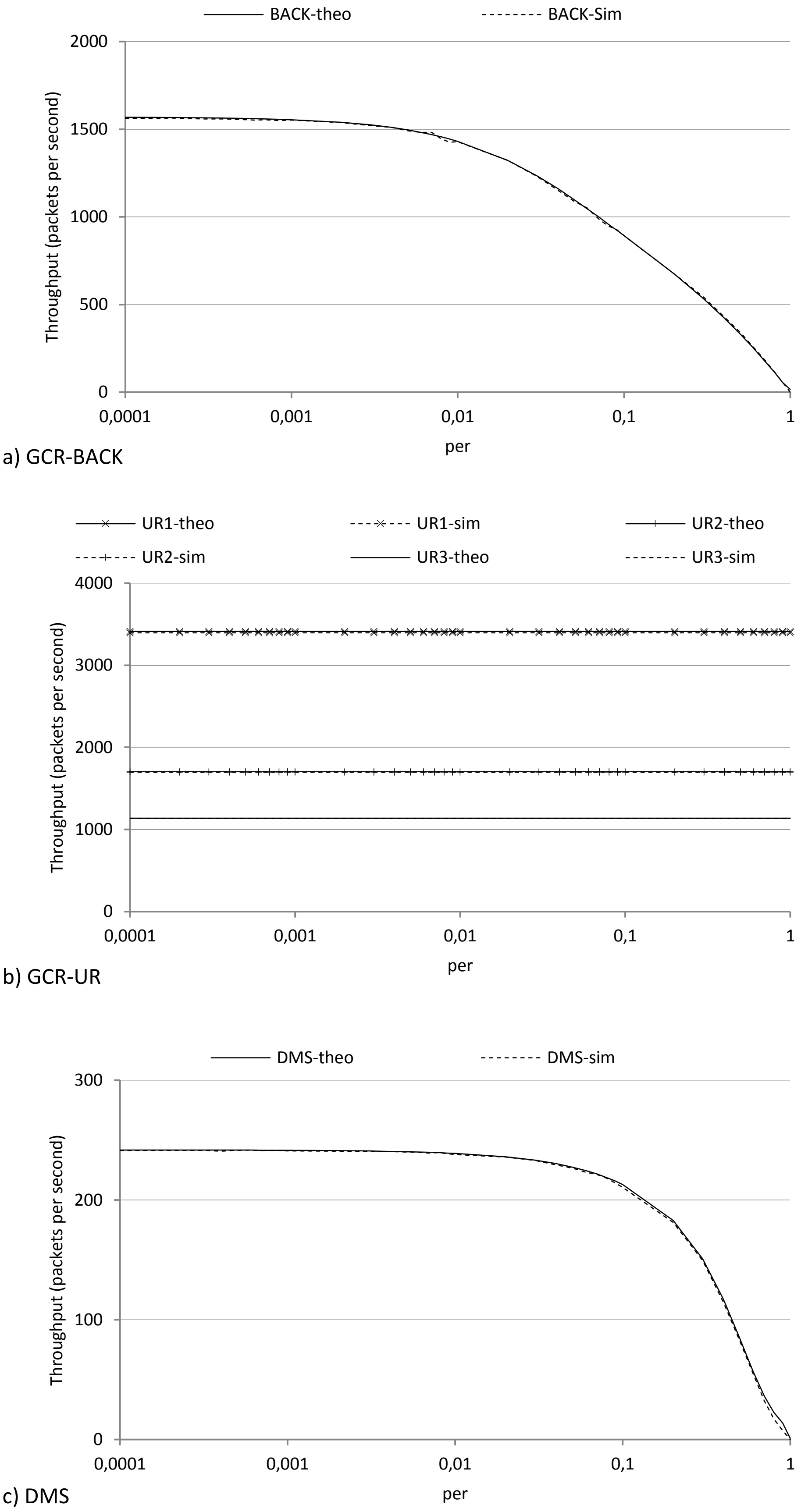
We use NS-3 [87] to evaluate DMS, GCR-UR and GCR-BACK, and to validate our analytical model. We build an IEEE 802.11a infrastructure network and we consider the simulator configuration of Table 8. In the remainder of this chapter we consider multicast packets of 1538 Bytes (including the MAC header) transmitted at the highest rate of 54Mbps. Besides, the CTS-to-Self is continuously sent at 54Mbps while the other control packets (i.e. ACK, BAR, BACK) are always delivered at the lowest rate of 6 Mbps.

Table 8. Simulator configuration

Parameters	Values
Simulator version	Ns-3.13
Transmission power	40mW (16.02dBm)
Transmission gain	1dB
Reception gain	1dB
Reception noise figure	7dB
Propagation loss model	Log distance
- Path loss exponent	3
- Reference distance	1m
- Reference loss (at 1 meter)	46.677dB
Propagation delay model	Constant speed propagation
- Speed	3.10^8 m/s
Error rate model	Nist
Energy detection threshold	-96dBm
Network	IEEE 802.11a
- Beacon interval	1 second
- Packet lifetime limit	60ms
- Queue size	20 packets
- CWmin	15
- CWmax	31

3.6.1 Model Validation

To validate our analytical model we consider that all the group members have the same PER. We compare the analytical and the simulation results of GCR-BACK, GCR-UR and DMS in Fig. 15(a), (b) and (c) respectively. We consider a multicast group of 10 members for all the protocols. In Fig. 15(b) we illustrate the obtained results using three different transmission limits: 1) GCR-UR1 transmits each packet one single time, 2) GCR-UR2 sends each packet 2 times, and 3) GCR-UR3 allows each packet to be delivered 3 times. We observe a very good accuracy of our model for all the protocols and regardless of the loss rate.



a) GCR-BACK

b) GCR-UR

c) DMS

Figure 15. Model validation: throughput estimation of a) GCR-BACK, b) GCR-UR and c) DMS, for a group of 10 members and a data rate of 54Mbps

Furthermore, we validate the accuracy of our mathematical estimation of the reliability of GCR-UR. Therefore we compare the simulation and the analytical results for three different transmission limits: UR1, UR2 and UR3. We depict the obtained results in Fig. 16. We conclude that our analytical model is accurate in estimating the delivery ratio of GCR-UR as a function of the packet error rate. We highlight that these results do not depend on the group size since GCR-UR does not require any feedback from the multicast receivers.

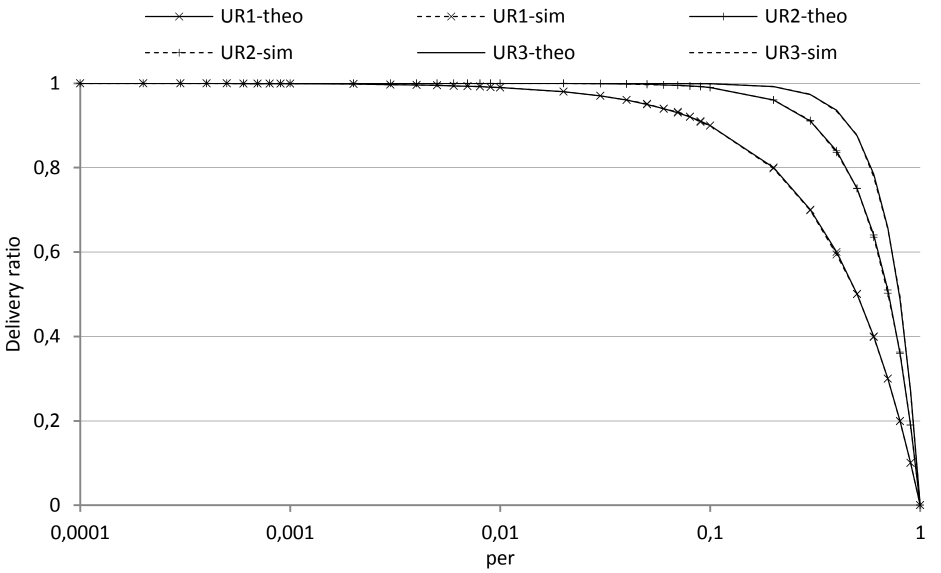


Figure 16. Model validation: packet delivery ratio of GCR-UR

As we show, our analytical model is able to determine the throughput of DMS, GCR-UR and GCR-BACK as a function of the loss rate, with a very high accuracy. Besides, our model takes into account any value of group size, block size, transmission rate and packet length. Therefore, it is useful to determine the expected throughput under various network configurations. The second utility of our model is to validate our simulation results. Therefore, we can confirm that our simulation results are also trustworthy.

3.6.2 Simulation Results

In the remainder, we compare DMS, GCR-UR, GCR-BACK and the legacy multicast procedure using simulation. In Fig. 17, we measure the throughput of the different protocols for a variable group size. We set all the receivers at a distance of 10 meters from the AP. This distance is suitable for the used data rate of 54Mbps. Therefore, the incurred loss rate due to the signal attenuation is very limited and is almost nil. Besides, GCR-UR and GCR-BACK use CTS-to-Self. We set the block size limit to 5. Thus, GCR-UR and GCR-BACK may send up to 5 packets within a block.

We note that the main difference between GCR-UR1 and the legacy multicast procedure is that the former policy uses a protection feature against the collisions, and is allowed to deliver more than one packet within a transmission opportunity. Therefore GCR-UR1 has an enhanced throughput and is less vulnerable to the collisions compared to the legacy procedure.

We notice that GCR-UR with one single transmission per packet (i.e. UR1) has the highest efficiency and delivers more than 3300 packets per second (pps), regardless of the group size. Besides, GCR-UR1 outperforms the legacy multicast. Furthermore, we notice that increasing the number of transmissions per packet reduces significantly the achieved throughput of the unsolicited retry policy; we observe that the efficiency of GCR-UR2 is less than 50% of that of GCR-UR1. Moreover, GCR-UR3 achieves only 1125 pps. This is about 30% of the throughput of GCR-UR1. However, the major advantage of the unsolicited retry policy is that this protocol is scalable and the achieved throughput does not depend on the group size. Thus, under the assumption that the appropriate data rate is carefully selected using a scalable rate adaptation algorithm, in this case GCR-UR becomes suitable for large multicast groups.

We observe in Fig. 17 that the throughput of GCR-BACK decreases with the increase of the group size. Therefore the protocol is able to deliver about 3000 pps when there is one single member in the group. This throughput decreases by 50% when there are 10 members, and falls to less than 270pps for a group of 100 receivers. Therefore, this policy is appropriate for groups with a few members but is not efficient with large groups.

As expected, DMS has the lowest scalability. The efficiency of this protocol falls significantly when a second member joins the group. Moreover, the highest throughput is limited to 236 pps when 10 members are present and is limited to 23 pps when 100 receivers join the group. Therefore, DMS is appropriate for small groups of two or three members.

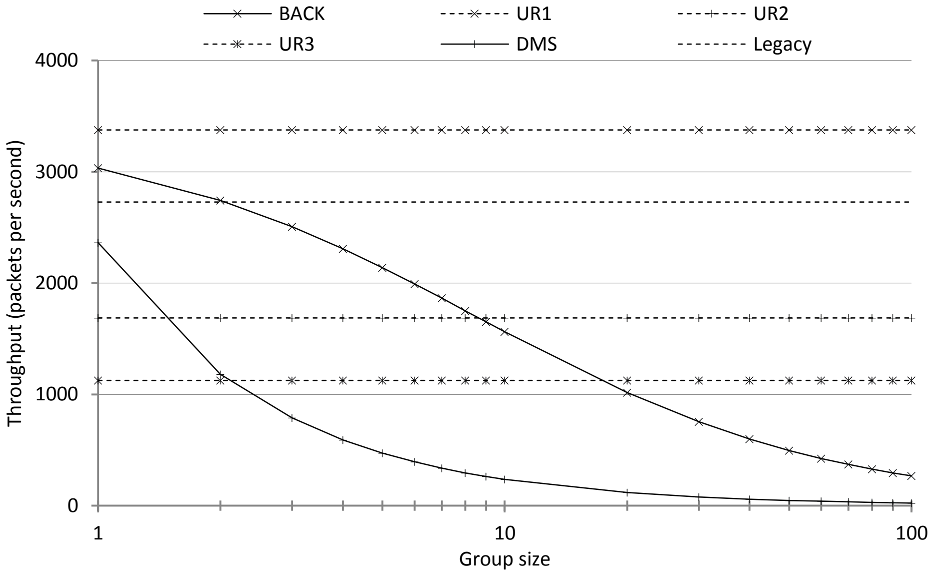


Figure 17. Throughput vs. group size

We conclude that DMS has the lowest scalability while the throughput of GCR-BACK is significantly impacted by the group size. Furthermore, the efficiency of GCR-UR decreases significantly by increasing the number of transmissions per packet. However, the scalability of this policy does not depend on the group size. But, to maintain this scalability, the protocol needs a scalable data rate selection procedure which is currently missing from the standard.

Now, we evaluate the impact of the distance on the throughput. We note that the distance is the principal parameter to determine the signal attenuation and to vary the bit error rate. Furthermore, we measure the packet delivery ratio in order to evaluate the reliability of the different protocols. We build a group of 10 members and we set them all at the same distance from the AP. We vary this distance and we measure the throughput and the reliability in Fig. 18 and 19, respectively. These results are obtained in the absence of collisions. Thus the AP is the only sender. This scenario allows us to compute the highest throughput.

In Fig 18 we observe that the throughput of GCR-BACK and of DMS depends on the packet error rate. Thus, the loss rate experienced by one single member is able to reduce the throughput of the entire multicast session. On the other hand, the throughput of GCR-UR and of the legacy multicast procedure does not depend on the loss rate. According to Fig. 19, we notice that the reliability of all the protocols depends on the distance. Thus, when the loss rate increases significantly, none of the protocols is reliable. However, we notice that GCR-UR1 and the legacy multicast have the lowest reliability when the receiver is located at a distance of 24 to 29 meters from the sender. This reliability improves slightly for UR2 and UR3. The reliability of DMS is better than that of GCR-UR at these locations. This is because DMS is allowed to retransmit a packet up to 7 times according to our configuration. On the other hand, GCR-BACK provides the highest delivery ratio. This is because this protocol is allowed to retransmit a packet till the expiry of its lifetime limit. In our configuration we set this limit to 60ms. Thus, a packet may be transmitted even more than 100 times.

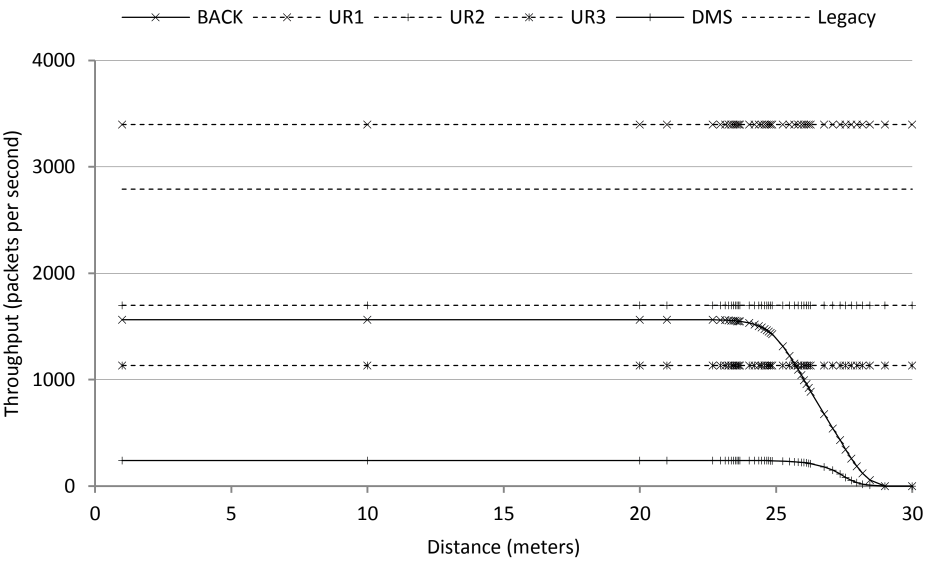


Figure 18. Throughput in the absence of collisions for a group of 10 members

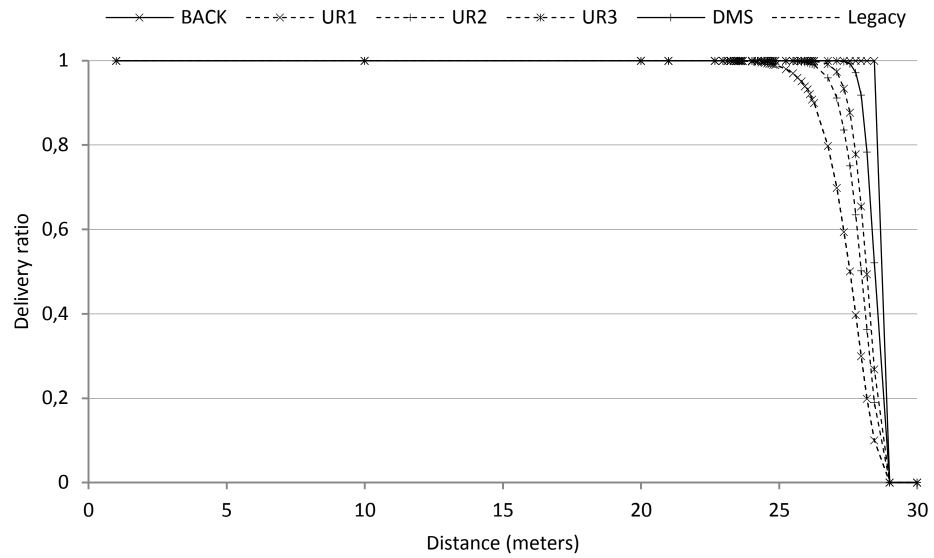


Figure 19. Delivery ratio in the absence of collisions for a group of 10 members

We evaluate the throughput and the reliability of the different protocols in Fig. 20 and 21 respectively, in the presence of collisions. Therefore, we configure a station to send unicast packets to the AP and to be in the saturation condition (i.e. the transmission queue of this station is never empty). The main goal of this configuration is to evaluate the impact of the collisions on the loss rate of the multicast packets.

In Fig. 20 we observe that the throughput of the different protocols decreases compared to the first scenario of Fig. 18. This is explained by the fact that the remaining time to send multicast packets decreases since the medium is shared with another traffic. However we notice that the throughput of the legacy multicast and of DMS is more impacted than that of the other protocols. This is because these two protocols do not take advantage of the block transfer.

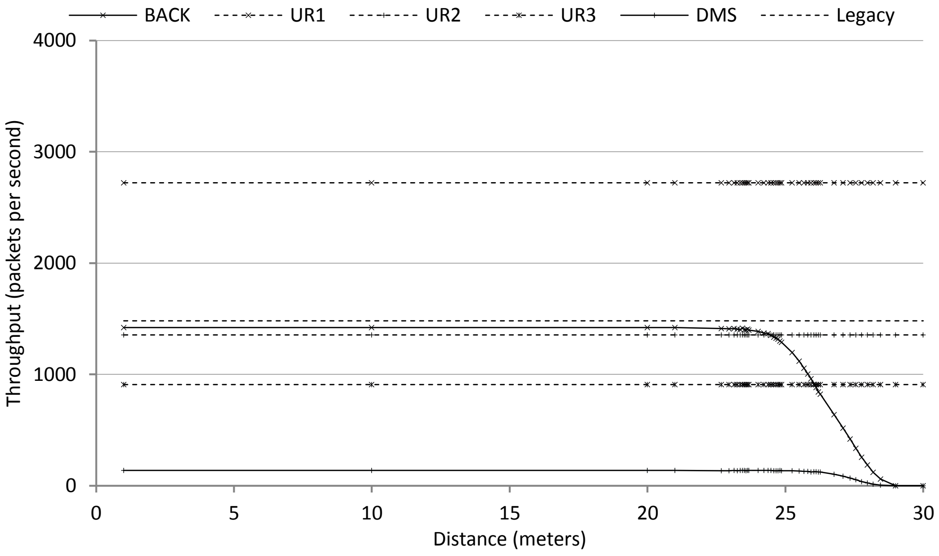


Figure 20. Throughput in the presence of collisions for a group of 10 members

In Fig. 21, we observe that the legacy multicast experiences an important loss rate even when the receiver is located near to the sender. This is caused by the collisions. On the other hand, we notice that the loss rate of GCR-UR is not impacted by the unicast traffic. This is because this protocol uses a protection mechanism to avoid the collisions.

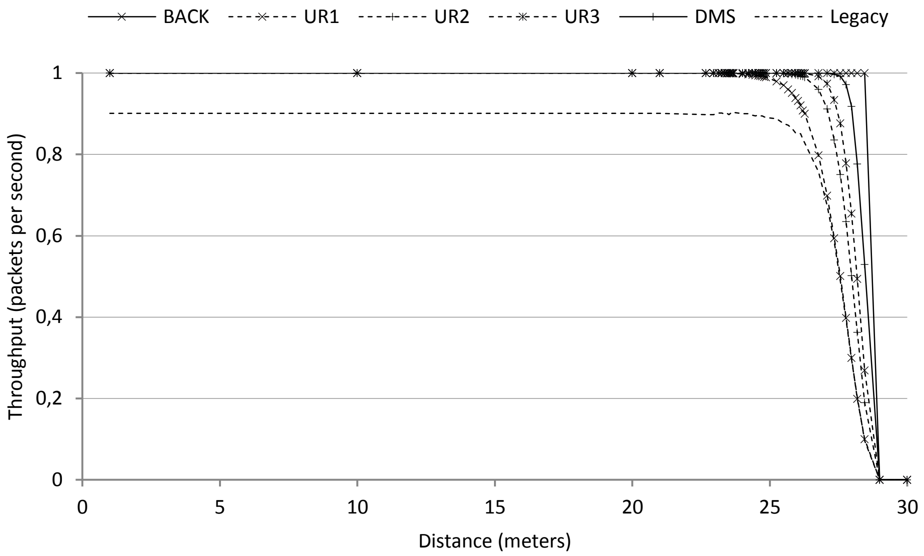


Figure 21. Delivery ratio in the presence of collisions for a group of 10 members

In the remainder of this section we evaluate the transmission delays as a function of the distance (i.e. bit error rate), the throughput and the group size. We consider that only the multicast packets are transmitted and that the channel is not shared with any other traffic. In the first scenario we build a group of 10 members located at the same distance from the AP. We vary this distance progressively till reaching a loss rate of 100%. We send a multicast traffic with a rate of 1pps. The main advantage to use a very low throughput is to avoid the buffering delays. Thus, the transmission of each multicast packet starts immediately upon the arrival of that packet to the MAC layer, and the obtained results are limited to the delays incurred by the multicast protocol. We illustrate the obtained results in Fig. 22.

For the case of DMS, we measure the average transmission delays as experienced by the first and last (i.e. the 10th) members. For the other protocols, all the members experience the same average delays. We notice that the delays experienced by member 10 using DMS (i.e. DMS10) are significantly more important than the average delays of the first member (i.e. DMS1). These delays increase at important distances due to the need to retransmit the missing packets. Furthermore, we observe that the delays of GCR-BACK increase with the increase of the loss rate. But the delays of the unsolicited retry policy are the lowest since a packet is retransmitted up to 3 times.

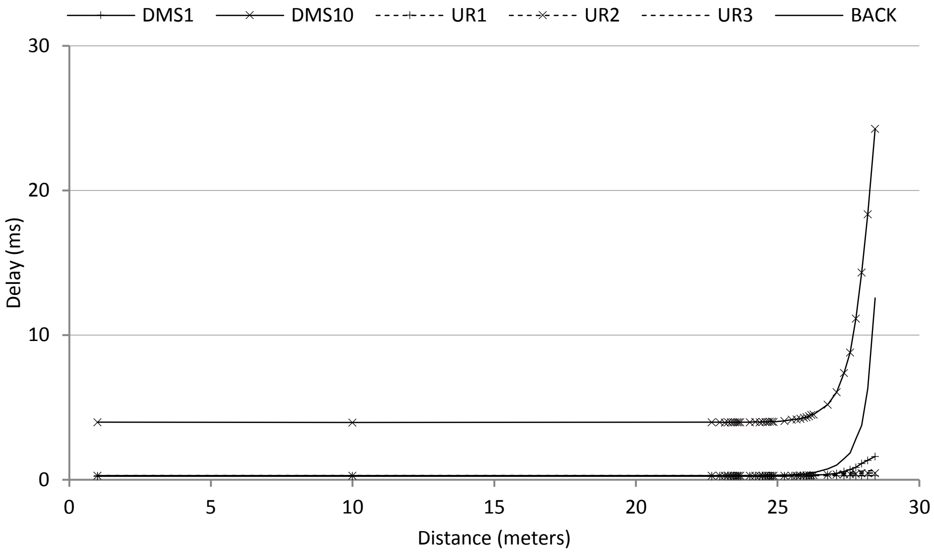


Figure 22. Delivery delays as a function of the distance for a group of 10 members

In Fig. 23 we depict the transmission delays under variable network load, and we consider a constant bit rate multicast traffic. We obtain these results when all the group members are located at a distance of 10 meters from the sender. We observe that the transmission delays increase significantly when the throughput exceeds the maximum capacity of the used protocol. This is because the buffering delays will be added. Besides, a packet is rejected when it exceeds the lifetime limit. Therefore, the highest delays are limited to this limit which is 60ms (as depicted in Table 8). Similar to the previous scenario, we observe that member DMS1 experiences lower delays than DMS10 when the throughput is up to 200pps. For the case of GCR-BACK, we notice that the delays are very limited when the packet rate is lower than 500pps. This is because a packet is immediately transmitted when it arrives to the MAC layer. Then the delays increase slightly for data rates from 500pps to 1500pps. This is because a packet may arrive while the protocol is in the feedback phase, i.e. the AP is exchanging BAR/BACK with the members. In this case the new packets wait the end of the exchange and the channel contention before being transmitted. When the throughput exceeds 1600pps, the delays of GCR-BACK increase significantly due to the buffering delays. This is because the highest supported throughput without queue overflow is limited to 1564pps, according to Fig. 17. However, we notice that the highest delays of GCR-BACK are much lower than the lifetime limit of 60ms. This is because these delays depend on the queue size; the packets are rejected if they arrive when the queue is full. But when a packet is in the queue, it should wait the transmission end of the older packets. In our case, the queue size is 20. In a saturated network, the delays of GCR-BACK are bounded by the maximum delay to send 20 packets, whenever this delay is lower than 60ms. We observe the same curve behavior for GCR-UR1, UR2 and UR3. However, GCR-UR3 reaches the saturation condition first. Besides, the maximum delays of UR3 are higher than those of UR1 in a saturated network. This is because the average service time for a packet under UR3 is more important than that required by UR1 and UR2.

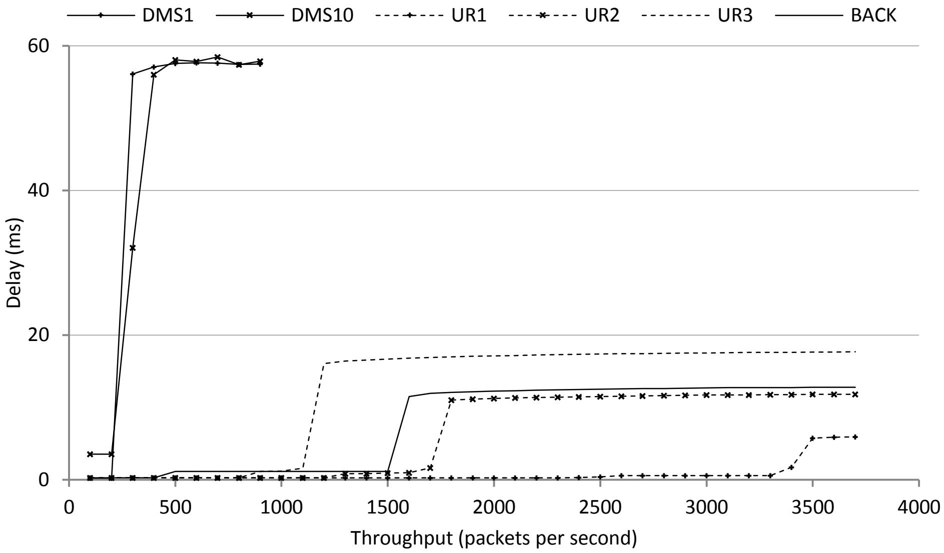


Figure 23. Delivery delays as a function of the throughput for a group of 10 members

In Fig 24, we measure the average delays for variable group sizes. We use a very low throughput of 1pps and we set all the members at a distance of 10 meters from the AP. We observe that all the protocols, except DMS, incur very limited delays. It is worth noting that the curve of GCR-BACK does not illustrate the required time to send the feedbacks. This is because all the packets are delivered correctly at the first transmission attempt. Therefore, the feedback duration is not added to the transmission latency because the feedback step occurs following the packet transmission. For the case of DMS however, the incurred delays depend on the receiver rank. Thus, the first member experiences very low delays, while the last receiver (i.e. DMSLast) encounters the worst latencies. These delays increase linearly with the group size.

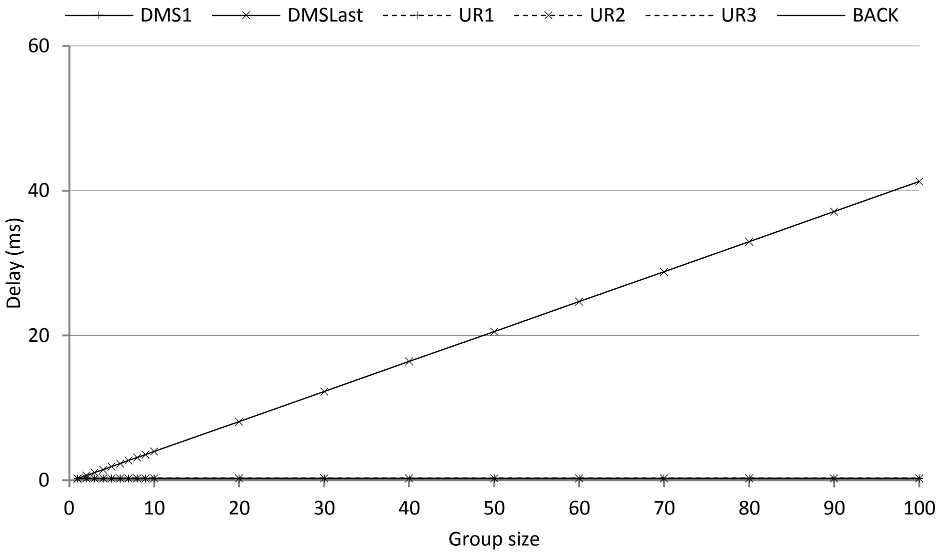


Figure 24. Delivery delays as a function of the group size

3.7 Conclusion

In this chapter we present the most relevant novelties of 802.11v and 802.11aa. Therefore, we introduce DMS, FMS and the data rate selection procedure of 802.11v. Moreover, we present the GCR service of 802.11aa. Particularly we describe GCR-SP, GCR-A, GCR-UR, GCR-BACK. We argue that FMS ensures very low power consumption but incurs important buffering delays and is not appropriate for high throughput and time-sensitive multicast flows. Moreover, we explain how GCR-SP is appropriate for low throughput applications. We conclude that GCR-A is the most appropriate method to deliver high bit rate flows to receivers in the power save mode. Furthermore, we define an analytical model to determine the throughput of DMS, GCR-UR and GCR-BACK for different values of group size, block size, transmission rate, packet error rate and packet size. This model is also able to determine the delivery ratio of GCR-UR. We validate our model using simulation results and we show its accuracy. On the other hand, we evaluate the scalability of the different protocols and we show that DMS has the lowest efficiency. We demonstrate that GCR-BACK is not appropriate for large group members. Moreover, we show that the throughput of GCR-UR does not depend on the group size but is significantly impacted by the increasing number of transmissions per packet. Also, we measure the incurred delays and we show that they increase significantly in a saturated network. However, we show that the delays experienced by the last DMS member increase linearly with the group size increase.

Chapter 4

4 Loss Diagnosis and Collision Prevention

4.1. Introduction

Packet Losses in a WLAN may occur due to many factors. These losses reduce the network throughput, impact the reliability of the wireless link, and increase the transmission delays. This is because missing packets are considered as wasted transmission time, and retry-based protocols require additional delays to send a data again. Besides, the losses reduce the delivery ratio of multicast and even unicast transmissions. Therefore, it is necessary to identify these factors and to define the required actions in order to avoid the transmission failures. This enhances the reliability and the latency of the multicast transport, and improves the network throughput.

We dedicate this chapter to determine the causes of the transmission failures in wireless networks, and we evaluate their impact on the loss rate. Particularly, we focus on the case of the multicast transport. Hence we briefly introduce the two principal loss factors: collisions and path loss. Then we present a new factor called the device unavailability. We show that the device may be unable to process any packet when 1) it is sleeping according to the power save mode, 2) the Control Processing Unit (CPU) is overloaded with many tasks exceeding the processing capability of the terminal, and 3) internal system failures occur at the network chipset. Thus, we show that the device itself is responsible for missing several multicast packets and that the loss rate due to device unavailability may reach 100%. We highlight that this factor is widely ignored, particularly in the field of wireless communication. Furthermore, we provide the required recommendations to avoid these losses and to enhance the reliability of the multicast transmissions. Hence, we define the Busy Symbol (BS) as an effective protection mechanism for the multicast packets against the collisions. We show that BS is able to avoid all the collisions and to ensure a very high delivery ratio for the multicast stream. We note that this mechanism is easy to implement and does not require any modification except at the AP. Therefore, BS is compliant with current receivers.

The remainder of this chapter is organized as follows. In Section 4.2 we introduce the related work concerning the loss diagnosis and the collision prevention. We dedicate Section 4.3 to evaluate the impact of the path loss, the collisions and the device unavailability on the loss rate experienced by the multicast transmissions. In Section 4.4 we introduce the Busy Symbol and we demonstrate using simulation, that this mechanism ensures a perfect protection for the multicast packets against the collisions. We conclude this chapter in Section 4.5.

4.2 Related Work

4.2.1 Loss Diagnosis

There is an intensive work to identify the different kinds of packet losses in the wireless networks [88-106]. The main objective of these researches is to provide an overview of the different loss factors in order to understand the variation of the available bandwidth. The second motivation is to define enhanced rate adaptation algorithms which are aware about the loss source. This awareness allows the algorithm to decrease the transmission rate when necessary in order to keep a reliable communication link with the receiver.

Most data rate adaptation algorithms [119-135] consider that the losses in a WLAN occur either due to the radio signal deterioration or due to the collisions. Therefore the typical action associated to a reduced SNR is to decrease the transmission rate since a lower rate is always more robust. But if the algorithm decides that the transmission failure is caused by simultaneous channel access, it does not reduce the data rate and let the MAC layer increase the contention window in order to reduce the collision probability at the following transmission attempt.

In [88] the authors evaluate the impact of the multipath and the interferences on the loss rate of the multicast packets. Therefore they build two networks operating at neighbor channels (channels 10 and 11) in the same room. They show that the loss rate varies between 2% and 7% in the presence of interferences from channel 10. Then they disable the interfering network and they evaluate the multipath impact on the packet losses. Thus, they consider the scenario of a moving person in order to create reflections. They show that the average loss rate is about 0.3% when a human is moving. Then they show that the average rate falls to 0.1% in a static environment. The authors confirm that this variation is related to the multipath effect. However, we think that this very limited variation is not enough to make such a conclusion. This is because the measurements are done using commercial devices which are not perfect and may incur their own losses as we will show later. According to our results, losses related to the device performance may vary within an interval of 5%. Thus, the interval of 0.2% may be random.

In [89] the authors study the correlation of packet losses as experienced by the receivers of multicast/broadcast streams. This is called the spatial loss correlation. They show that closely located receivers loose the same packets almost all the time when the received signal is strong enough. This correlation decreases and the losses become independent when the radio signal deteriorates. In [128], the authors evaluate the loss rate as a function of the signal fluctuation. Then they define a new model which estimates the bit error rate of the wireless link based on the notion of the effective SNR. Another experimental study is introduced in [90]. It measures the loss rate of the multicast transport, and evaluates the unfair sharing of the medium between unicast and multicast flows. In this study, the authors classify the losses into three categories: collisions, queue overflow and others. Hence they do not investigate the causes of the transmission failures for the case of the third category. In [91] the authors collect loss traces from a real 802.11b network. They study their spatial correlation. Besides, they evaluate the burstiness nature of the missing packets. This is called the temporal loss correlation. They show that the loss rate varies between 4% and 30% from one receiver to another. In their testbed, the station with the highest loss rate (i.e. 30%) is the nearest one to the AP. Therefore we notice that the device with the best link quality may experience the highest loss rate. The same observation is found in [92], and the authors confirm that identical devices perform quite differently in term of packet error rate. This conclusion is obtained using a multicast group of 9 collocated mobile phones and an IEEE 802.11b network. The authors show that the loss rate varies between 4% and 94% from one receiver to another.

A series of hypotheses for the causes of the transmission failures is explored in [93]. The authors show that the loss rate depends on the signal attenuation and the interferences. Besides, they investigate the losses caused by the multipath effect; they show that the loss rate increases when the delay between the direct and the reflected signals is higher than several hundreds of nanosecond. Besides, they find that some nodes among the 38 deployed stations experience important and frequent bursty losses. Moreover, these bursts and their frequency do neither depend on the transmission rate nor on the distance between the sender and the receiver. But, the authors do not provide any clarification for this loss pattern. In [94] the authors show that a missing burst can be as long as several hundred packets, but the size of loss free bursts may exceed 10000 packets. Many other works find that the losses may occur frequently in bursts [95-97]. But they do not provide any certain explanation for this pattern which does not necessary affect all the receivers. The authors in [96] suspect that the synchronization failures are a cause of these losses. We do not share this opinion. This is because 802.11 defines a communication system which is able to ensure a very high success rate for data symbols that the receiver ignores before their successful reception. Besides, the synchronization symbols are a priori known information and are transmitted using a dedicated modulation scheme which is more robust than those used to carry the data. Thus we expect that the success rate of the reception synchronization is significantly much higher than that of the data symbols. We note that all the simulators consider that the synchronization success rate is always 100%.

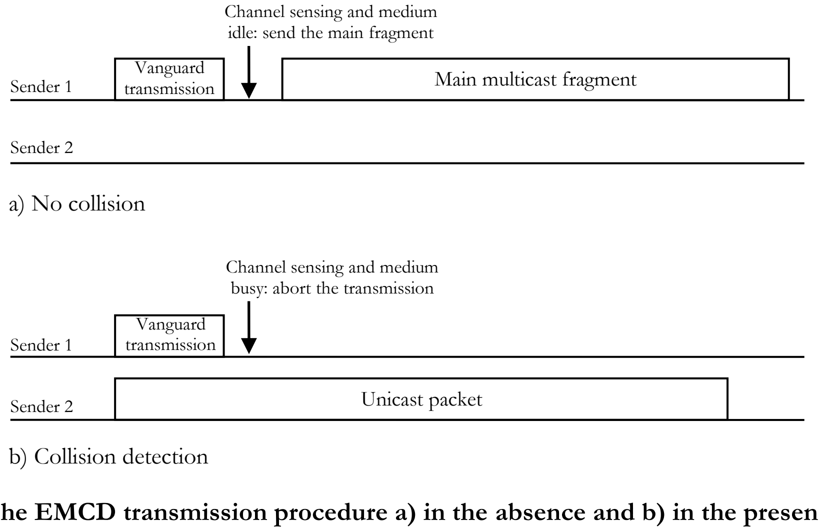
Based on our conviction that the transmission failures should occur individually and randomly (except when the lost rate is very high or the connection is definitely lost), and because we notice that the loss rate depends sometimes on the device itself, we conclude that the device performance may be the main responsible of the unexplained and important losses, and their burstiness nature. It is worth noting that if the losses are bursty due to the wireless channel, even the unicast mode becomes unreliable. This is because a packet and its retransmissions may be lost within a burst. This casts doubt on the reliability of the 802.11 unicast transport. Hence we derive a diagnosis of the communication device in order to provide an answer to the unexplained, and sometimes excessive, reception failures, and to prove that the bursty losses are not related to the wireless link. We find that an important loss rate may occur due to the receiver unavailability and particularly due to the power save mode and to the CPU overload. We conclude that the terminal unavailability is the cause of the important and bursty losses.

4.2.2 Collision Prevention

The collisions are another issue of the wireless network. They occur when two contending nodes start transmitting at the same time. Therefore, each transmission behaves like interference to the other one, and both of them reduce the reception Signal to Noise and Interference Ratio (SNIR) of each other. This leads to frequent reception failures. When a unicast packet is lost, the sender increases the contention window size in order to reduce the collision probability at the following transmission attempt. However, multicast packets do not use any feedback and are always delivered using the lowest contention window size. Hence, the conventional multicast transport is vulnerable to the collisions. It is necessary, therefore, to protect the multicast packets against the collisions in order to enhance the delivery ratio of these flows.

In [107] the authors propose the transmission of the multicast packets, one PIFS period after the acknowledgement of the unicast packet. This is an efficient way to protect the multicast packets against the collisions, but still has one major weakness: the number of multicast transmissions depends on the number of transmitted unicast packets. Therefore, if the unicast packet rate is less than that of the multicast one, multicast packets should be buffered even if the bandwidth is available, and may be rejected because of the queue overflow.

The Early Multicast Collision Detection (EMCD) transmission procedure is proposed in [108]. It allows the multicast sender to detect the collision during the transmission of the multicast packet. The principle of EMCD is to perform a second channel sensing during the packet transmission. This protocol operates in three phases. At the beginning, the algorithm sends a small portion of the packet, called the vanguard transmission. Then it senses the channel again to determine if a simultaneous transmission is in progress. If the channel is sensed idle, in this case the second fragment is transmitted. Otherwise, the sender concludes that a collision occurred, and aborts the transmission of the multicast packet. This packet will be retransmitted later after a new channel contention. We illustrate the transmission procedure of EMCD in Fig. 25.



a) No collision

b) Collision detection

Figure 25. The EMCD transmission procedure a) in the absence and b) in the presence of collision

This solution is efficient to detect the collisions and to enhance the reliability of the multicast transport. However, it requires the fragmentation of a packet into two parts. Each of them is transmitted with PHY preamble and header, and a MAC header. This requires additional overhead and reduces the protocol efficiency. We note that 802.11n defines longer PHY preamble and header, and very high data rates. Thus, these preamble and header have a significant duration compared to the data part. As an example, the required time to send a 1500 byte-length packet at 600 Mbps using the standard transmission procedure, is like follows: 56μs for the PHY overhead and 21.6μs for the data part (including the MAC header) = 77.6μs. On the other hand, the transmission duration of this packet using EMCD is like follows: 56μs (first PHY overhead) + 3.6μs (data part of the first fragment) + 11μs (intermediate channel sensing) + 56μs (second PHY overhead) + 18μs (data part of the main fragment) = 144.6μs. Hence, EMCD doubles the required time to send the packet. As we observe, this collision detection procedure introduces an important overhead for the high throughput networks. Therefore it is not an optimized solution for these networks.

4.3 Loss Diagnosis

4.3.1 Losses due to Week Signal to Noise Ratio

The path loss is the main factor to limit the coverage area of a WLAN. It causes the strength of the radio signal to fall progressively till the data distortion. The 802.11 standard defines several transmission rates with different robustness degrees against the signal attenuation. The rate of 54Mbps provides a high transmission rate but has the most limited coverage area. The rate of 6Mbps provides the lowest data rate, but has the largest communication range and defines the coverage area of the wireless network. The Signal to Noise plus Interference Ratio (SNIR) is an accurate indicator to determine the bit error rate of each transmission rate. It depicts the signal strength while taking into account the channel noise in addition to any existing interference. In the absence of interference, we obtain the following equality: SNIR = SNR. We evaluate the packet loss rate due to SNIR using NS-3 [87]. We consider the simulator configuration of Table 8. We build an IEEE 802.11a network of one AP and one multicast receiver. The packets are delivered using the legacy multicast transport and do not use any feedback policy. We send these packets in an unshared network, i.e. the AP is the only sender. We consider this scenario in order to avoid the collisions. Thus the losses are caused by the signal attenuation. The multicast receiver moves away from the AP with a step of one meter. We record the Packet Delivery Ratio (PDR) at various transmission rates and at different distances from the AP. We transmit multicast packets of 1500 Bytes. Fig. 26 depicts the obtained results. This figure shows that the multicast packets are reliably delivered at each data rate whenever the receiver is at the appropriate location. Then the loss rate increases significantly till loosing the connectivity definitively.

We illustrate the PDR for packets transmitted at the lowest rate of 6 Mbps in Fig. 27. We consider three packet lengths of 1500, 500 and 38 Bytes. These results show that short packets may be transmitted successfully at longer distances. We illustrate the variation of the SNIR in Fig. 28. We observe that the loss rate of 1500 byte-length packets transmitted at 6 Mbps increases significantly for SNIR values lower than 11dB. Then the connection is completely lost for SNIR lower than 9dB.

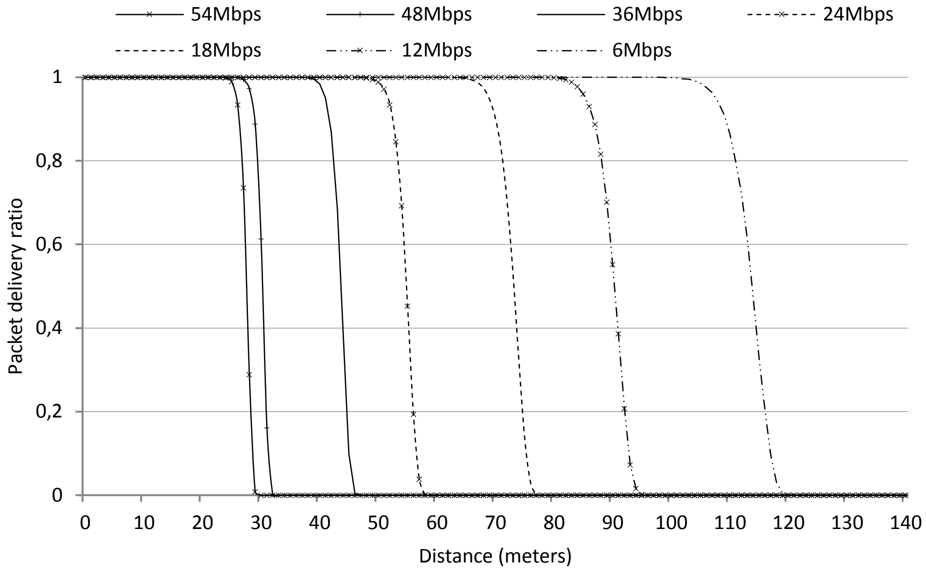


Figure 26. Packet delivery ratio at various transmission data rate

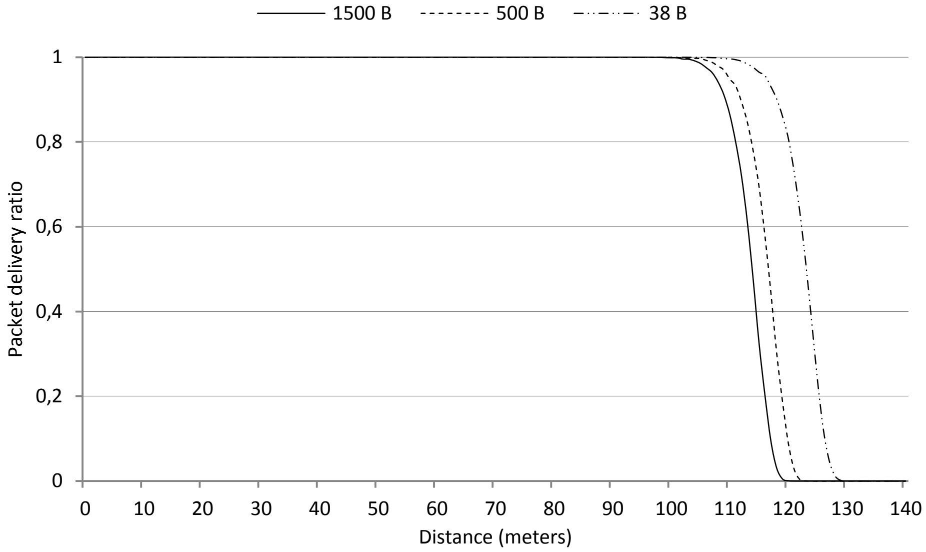


Figure 27. Packet delivery ratio for different packet lengths

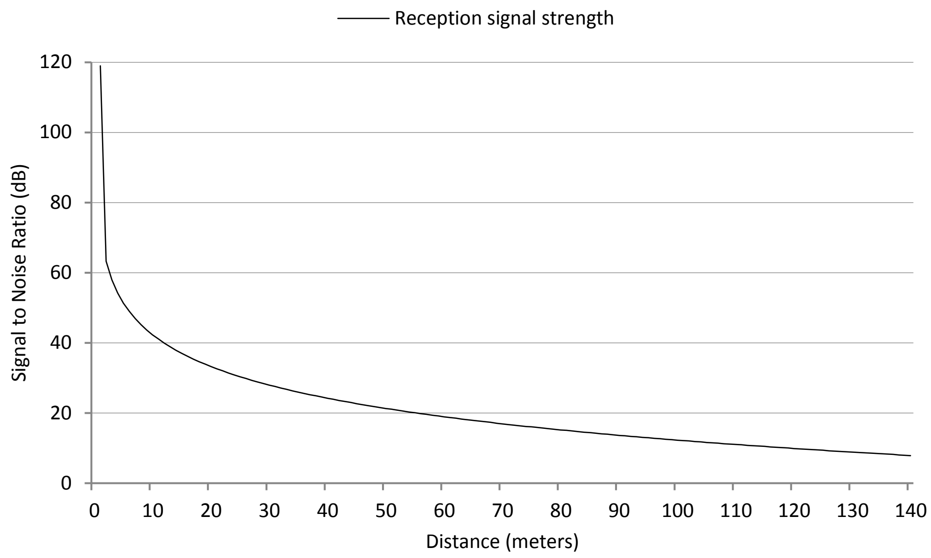


Figure 28. Reception SNIR at different distances from the AP

4.3.2 Losses due to Collisions

The collisions are a principal cause of packet losses in 802.11 networks. They occur when two or many nodes access the medium at the same time. The contention procedure is efficient to limit the simultaneous transmissions but is not collision free. While the unicast transport deploys several feedback policies to recover from packet losses, the conventional transmission procedure of the multicast mode is primitive and does not allow detecting and retransmitting missing packets. Therefore, missing packets are definitely lost. Hence, the collisions are an important factor which impacts and reduces the reliability of the multicast in the IEEE 802.11 networks.

The collision rate in wireless networks depends on the number of the contending devices and the Contention Window (CW) size. It does neither depend on the packet length nor the transmission data rate. The size of the CW depends on the retry count. The first transmission of each packet uses the smallest window. Following a transmission failure, the sender increases the window in order to reduce the collision probability at the next delivery attempt. Since the legacy multicast does not use any feedback policy, each packet is transmitted only once using the smallest size of CW. Hence the multicast is vulnerable to the collision issue.

We evaluate the loss rate caused by the collisions using NS3. We build an IEEE 802.11a network of one AP and 25 associated stations. We set the nodes within a distance of 10 meters around the AP in order to ensure a good link quality. Hence, packet losses are only caused by collisions. In all the tests, the AP delivers a multicast traffic. In each test we run a new unicast session on a new station among the associated stations. This allows us to increase the collision rate of the WLAN progressively. We consider the case of a highly loaded network, i.e. the transmission queue of every node, including the AP, is never empty. We illustrate the loss rate caused by the collisions in Fig. 29.

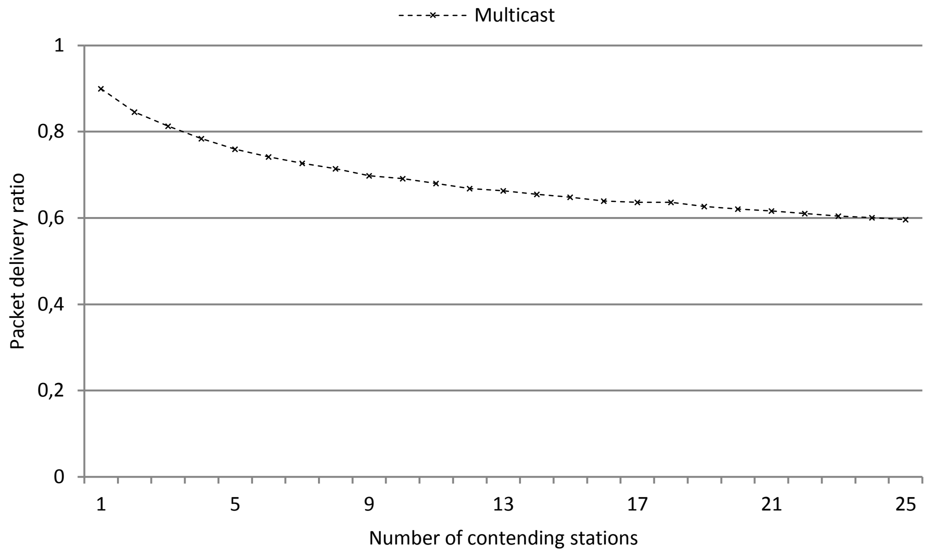


Figure 29. Packet delivery ratio in the presence of collisions

These results show that even if one station is sharing the channel with the AP, the collision rate of the multicast traffic is about 10%. We believe that this scenario is frequent in real networks and may occur if one user starts uploading a large file while the multicast service is running. Furthermore, we observe that the collisions may incur a packet loss rate higher than 40%.

4.3.3 Losses due to Device Unavailability

4.3.3.1 Device in the Power Saving Mode

The standard defines the Power Save (PS) mode in order to reduce the energy consumption of the connected devices. In a BSS, the AP sends a Beacon frame periodically. This control packet contains the Traffic Indication Map (TIM) which identifies the STAs for which traffic is pending and buffered at the AP. It also notifies the presence of multicast/broadcast packets. Two different TIM types are defined: TIM and Delivery TIM (DTIM). Every specific period of *DTIMPeriod*, a TIM of type DTIM is transmitted within the Beacon frame rather than an ordinary TIM.

If any STA in the BSS is in PS mode, the AP should buffer all multicast and broadcast packets, and deliver them immediately following the next Beacon including a DTIM. The More Data field shall be set in the headers of all packets except the last one to indicate the presence of further buffered broadcast/multicast packets. These packets should be sent before transmitting any unicast traffic.

A STA that stays awake to receive broadcast/multicast traffic should remain awake 1) until the More Data field of the broadcast/multicast packets indicates there is no further buffered broadcast/multicast traffic, or 2) until a TIM is received indicating there are no more buffered broadcast/multicast packets.

The current power management of the standard allows the implementation of several standard-compliant energy saving levels. Hence, depending on the power management requirements of a STA, this latter may choose to wake up every TIM, DTIM or otherwise. A STA may have its *ReceiveDTIMs* variable set to "False". This means that the STA is not required to wake up every DTIM. This configuration may be selected to further reduce the power consumption, but leads to frequent multicast packet losses.

Fig. 30 illustrates the AP and STA activity under the assumption that a DTIM is transmitted once every 3 TIMs. The first line represents the AP activity. The AP schedules Beacon frames for transmission every Beacon interval. The second and third lines depict the activity of two STAs operating with different power management requirements. In this example, the second STA has *ReceiveDTIMs* set to "False" and does not wake up at every DTIM. Thus, STA2 may miss several multicast packets.

The first STA, powers up its receiver and receives a TIM in the first Beacon frame; that TIM indicates the presence of a buffered packet for that STA. STA1 then generates a PS-Poll frame, which elicits the transmission of the buffered packet from the AP.

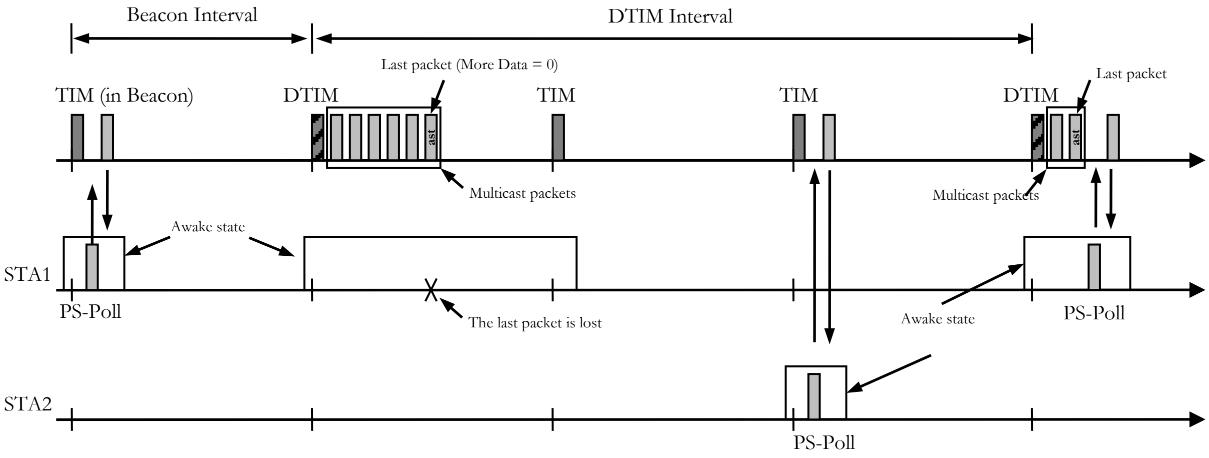


Figure 30. Infrastructure power management operation

The Second Beacon contains a DTIM. Hence the AP sends all the buffered multicast packets. STA1 remains awake to receive these packets. However, in our example, STA1 misses the last packet. Hence it remains awake until the third Beacon which indicates that there are no more multicast/broadcast packets.

STA2 wakes up before the fourth Beacon in order to receive it correctly. As the TIM indicates buffered packets for STA2, this latter sends a PS-Poll to the AP which sends the buffered packet. At the fifth Beacon interval, the AP sends a Beacon including a DTIM field. This field indicates the availability of multicast packets in addition to unicast packets for STA1. After receiving the last multicast packet, STA1 sends a PS-Poll to the AP which sends the buffered unicast packet.

Since the default Beacon interval is 100ms, if the *DTIMPeriod* value is set to 3, multicast services may experience latency in the order of 300ms. This delay may impact considerably the experienced quality of real-time multicast services. Moreover, since multicast packets are transmitted immediately following a

DTIM and before transmitting any unicast packet, high throughput multicast services impact considerably the latency experienced by other time sensitive unicast traffic. This impact has been tackled and evaluated in [109]. Besides, several STAs may be required to awake in order to receive multicast traffic (*ReceiveDTIMs = False*), even if they are not concerned by this data. Therefore, the multicast transmissions lead to a useless increase in the power consumption [110].

Furthermore, the PS operating mode may increase the loss rate of the multicast packets; these packets are transmitted without the request of the STAs which may be sleeping and may therefore miss all the transmissions. Also, the PS mode may impact the throughput of the multicast services; by limiting the multicast transmissions to specific time intervals, the available bandwidth for the multicast traffic will be reduced. We highlight that this impact may be experienced even if all the STAs in the PS mode are not members of the multicast group and are not interested in the multicast traffic. This is because the AP is not aware about the group memberships.

In the remainder of this section we evaluate the impact of the PS mode on the reliability and the throughput of the multicast transport. We achieve our tests in a closed area without or with a very limited interference with other systems and networks. We consider a WLAN composed of one Access Point (AP) and two stations: STA1 and STA2. We illustrate the network and the devices characteristics in Table 9. All the three laptops are powerful Dell computers and use recent 802.11n chipsets. We install the AP and the two STAs close to each other in order to avoid failures caused by the path loss.

Table 9. Configuration parameters

Parameters	Values
Network	802.11a
Beacon interval	100ms
DTIMPeriod (resp. DTIM interval)	1 (resp. 100ms)
CWmin	31
Atheros chipsets (AP, STA2)	Atheros AR9300-XB112
Intel card (STA1)	Intel® WiFi Link 5100 AGN
Computer AP, STA2	Dell Latitude D420
Computer STA1	Dell Latitude E6400
Driver AP, STA2	Ath9k (Atheros)
Driver STA1	NETw5 (Intel)

In our evaluations we notice that the default socket configuration does not block forwarding multicast packets when any of the associated STAs is in the PS mode. In fact these packets are stored in a special queue (PS queue) at the MAC layer, and are transmitted after the DTIM. The MAC layer notifies the socket only about the state of the main queue. Therefore, when this queue is full, the socket resumes sending in order to avoid the packet rejections. However, the PS queue may experience frequent packet drops due to the queue overflow. In order to provide accurate results of the losses caused by the PS mode, we consider only the effectively transmitted multicast packets. Hence we collect statistics directly from the transmitter module of the AP driver.

The two chipsets provide different power management levels. The Intel card may operate at 6 different levels of power savings numbered 0 through 5 [111]. Level 0 disables the PS mode (i.e. the device is fully powered) and level 5 provides the greatest amount of savings. The Atheros chipset provides only two levels: ON (device in PS mode) and OFF (no PS). We measure the packet delivery ratio for a video of 25 frames per second (fps) and an average bitrate of 1360 Kbps. The multicast application is running on the AP and delivers this video using RTP. Hence, one image is packetized and forwarded to the MAC every 40 ms.

Fig. 31 illustrates the reception ratio of STA1 for the different power levels. For each level, we transmit the same video 10 times. In each of these trials we illustrate the packet delivery ratio. Our results show that the loss rate depends on the power level; for levels 5 and 4 the delivery ratio varies between 33% and 63%. This ratio increases at levels 3, 2 and 1 and reaches 90%. The loss ratio becomes less important at level 0 where the delivery ratio is about 98%.

We evaluate the reception performance of STA2 for the 2 supported levels: power management ON and OFF. We compare the delivery ratio of STA1 and STA2 in Fig. 32. During the 10 first trials, we set STA1 at level 2 and STA2 at level ON. We switch to levels 0 and OFF for the 10 last trials. We observe that the Atheros chipset outperforms the Intel one. Moreover, we notice that the delivery ratio in a collision free medium is higher than 99% for STA2 when it is fully powered.

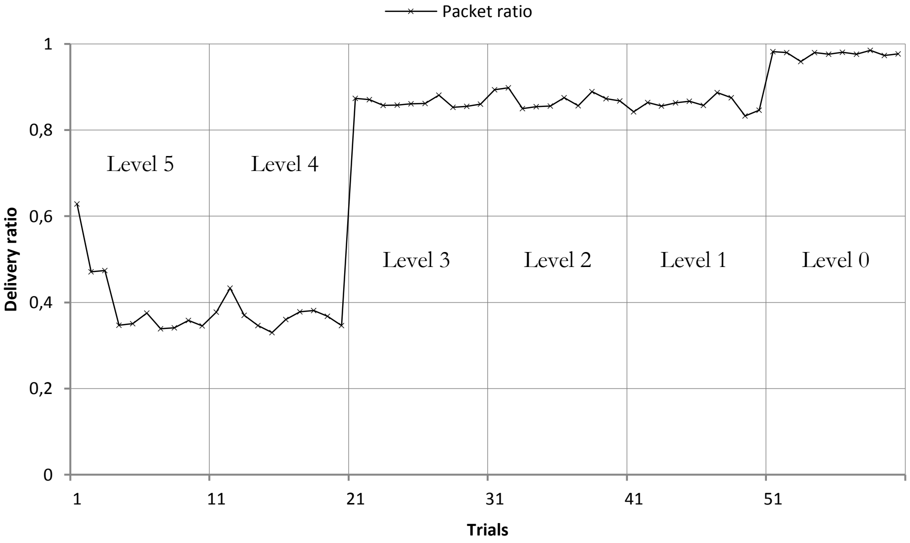


Figure 31. Impact of PS mode on the packet delivery ratio - STA1

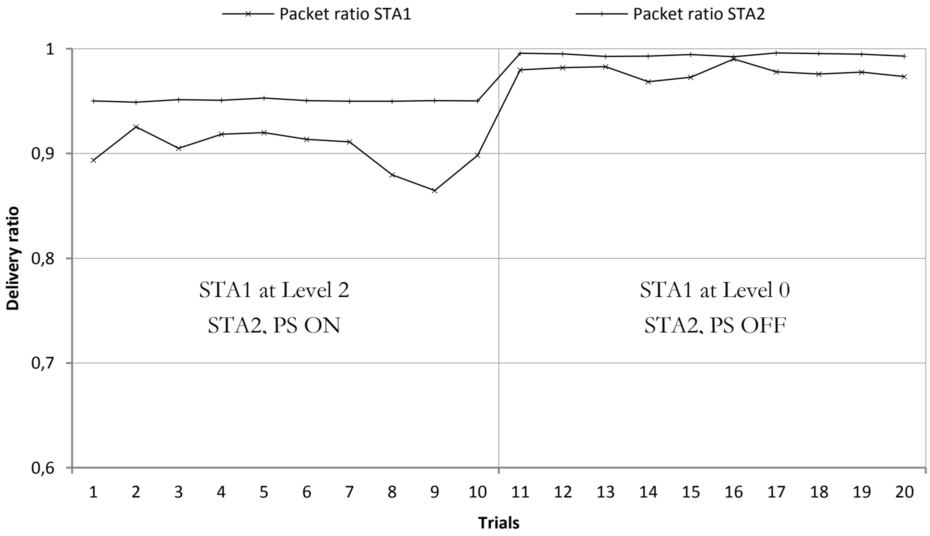


Figure 32. Impact of PS mode on the packet delivery ratio - STA1 vs. STA2

In the remainder of this section we evaluate the impact of the PS mode on the throughput of the multicast services in a real network. We consider a Constant Bit Rate (CBR) stream and measure the number of transmitted multicast packets for the following transmission data rates: 6, 12, 24 and 54 Mbps. We increase the packet length progressively, and we compare the average transmitted packets per second during the PS operation and in a fully powered (FP) network. We compare the FP rate with the theoretical one. We illustrate the obtained results in Fig. 33.

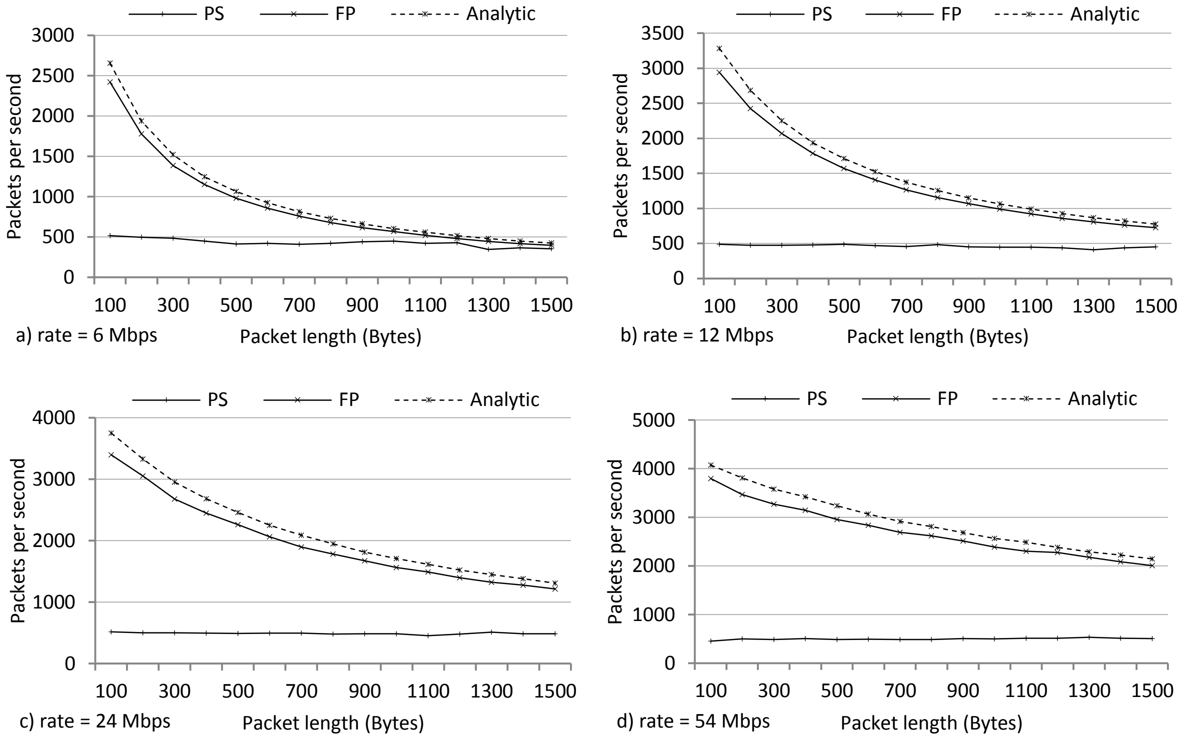


Figure 33. Multicast packets transmission rate for PHY rates of 6, 12, 24 and 54 Mbps

In Fig. 33(a), all packets are transmitted at 6 Mbps. We observe that the transmission rate under PS operation is about 500 packets per second (pps) and is bounded by the rate of the fully powered network. Also we notice that the theoretical results are higher than those of the test bed. We believe that this is related to the device performance. As we will show in the next section, the device may be unavailable during some instants, and unable to transmit. Hence the bandwidth is not totally used.

We observe the same curves' behavior in Fig. 33(b), (c) and (d). We notice that the multicast throughput under the PS operation is about 500 pps regardless of the packet length and of the used PHY data rate. On the other hand, the theoretical throughput slightly exceeds the throughput of the fully powered network.

The main solution to avoid the high loss rate cause by the Power Save mode is to disable it. It may be disabled temporarily during the streaming period using GCR-A. We note that a device is made in order to communicate. The primary goal of designing the PS mode is to reduce the power consumption of devices which are idle almost all the time. However, multimedia services deliver a high throughput traffic which requires that the device is continuously in communication.

Furthermore, it is necessary to distinguish between multicast members which should be fully powered, and non-members which may be allowed to stay in the PS mode. Therefore, a reliable and energy-efficient multicast protocol should be aware about every group member. This awareness allows a receiver to switch back to the PS mode once it is not member any more of the multicast service. The design and the requirements of our group membership management functionality are described in details in chapter 5.

4.3.3.3 Unavailable CPU

Communication terminals, such as computers and smartphones, are composed from a main processor, called Central Processing Unit (CPU). The CPU is typically connected to several other devices including network chipsets, screen, hard disk, storage devices, CD reader, sound card and keyboard. The CPU is the host of the operating system which manages all the plugged devices. On the other hand, the latter components are equipped with less sophisticated but dedicated processors, typically called microprocessors or microcontrollers.

The hardware interrupts are a principal method to ensure the communication between the main processor and the associated devices, including the 802.11 chipsets. Therefore, when a new packet arrives from the wireless medium, the microcontroller puts the data in a shared buffer and triggers an interrupt. Under the assumption that the CPU is available, the packet is processed and forwarded to the appropriate applications. The way an interrupt is handled depends on the operating system and may evolve from one release to another. Table 10 illustrates some potential sources of interrupts according to [112].

Note that a processor may handle one hardware interrupt at a time. If a new interrupt occurs from another interface while the processor is still handling a hardware interrupt, in this case the second one is lost. If the interrupt arrival rate exceeds the processing capacity, several tasks will be ignored. For the case of 802.11 chipsets, several packets (including those received correctly) will be dropped. The impact of these drops is similar to packet losses from the application point of view. Besides, they reduce the reliability of both the unicast and the multicast transmissions. We note that the impact of the interrupts on the CPU depends on the amount of work required to process an interrupt. For example an interrupt coming from the keyboard to tell that a key is pressed requires much less processing time than the required time to process a large packet coming from the network device with many parameters such as the reception power, the data rate, the sender, the receiver, etc.

Table 10. Potential sources of excessive interrupts for embedded processors

Source	Interruption rate (per second)
serial port @115 kbps	11 500
10 Mbps Ethernet	14 880
CAN bus	15 000
I2C bus	50 000
USB	90 000
100 Mbps Ethernet	148 800
Gigabit Ethernet	1 488 000

In the remainder of this section we measure the impact of the packet arrival rate on the packet loss rate as experienced by the multicast application. We build an IEEE 802.11a network on a free channel in order to avoid the collisions and the interference. We use AP and STA1 of Table 9 as the sender and the receiver, respectively. We configure the sender to use CWmin = CWmax = 0. Therefore packets are separated with DIFS time period. Moreover, all multicast packets have 100 Byte-length (including the MAC header) and are delivered at 54Mbps. This scenario intends to deliver packets with a very high rate and to incur an important interrupt rate at the receiver. The two terminals are separated with less than 0.1 meter in order to ensure good reception signal and to avoid losses caused by the signal attenuation. Therefore, any packet loss is caused by the device performance (i.e. CPU unavailability of chipset failures). We increase the packet transmission rate progressively and we record the delivery ratio. For each rate, we perform between 10 and 20 measurements. In each measurement we send 100000 packets at a constant rate. We make only 10 measurements for the low packet rates because the delivery ratio looks to be stable. Then we increase the measurement number starting from the rate of 9000 packets per second. We depict the obtained results in Fig. 34. We note that the maximum achieved rate is limited to 12500 pps. Thus the results illustrated for throughputs of 13000 and 14000 pps are obtained for an effective packet transmission rate of 12500pps.

Fig. 34 shows the maximum, the minimum and the average delivery ratios using the results of the different measurements. We observe that the average ratio is about 98% for relatively low rates of 1000 and 2000 pps. For these rates, the inter-arrival periods are the longest. Then the average delivery ratio increases and varies between 99.1% and 99.8% for rates from 3000 to 8000 pps. This let us deduce one or both of the following two assumptions: 1) the CPU attributes more attention to devices triggering frequent interrupts, or 2) the network device is more ready to receive when the packet arrival rate increases. We highlight that it is not possible to determine which of these assumptions is true due to the limited control on the chipset. Further, we notice that the delivery ratios vary between 99.9% and 74.1%, and the averages are 95.8% and 89.1% for packet rates of 9000 and 10000 pps, respectively. Then we observe a very high loss rate which may reach 100% starting from 11000pps. At this level, the average delivery ratio is limited to 56%, although the loss rate is sometimes very low (less than 0.3%). We note that the case of 0% delivery ratio illustrates one of the measurements where the application did not receive any packet among the 100000 transmitted ones. During this test, the computer hangs and does not respond to any event till the end of the multicast session. Then, it returns to ordinary operations without needing a reboot. For all the other tests, the computer responds to any request but a slight slow is observed when we move the mouse. This is observed when the packet rate increases (starting from 11000pps).

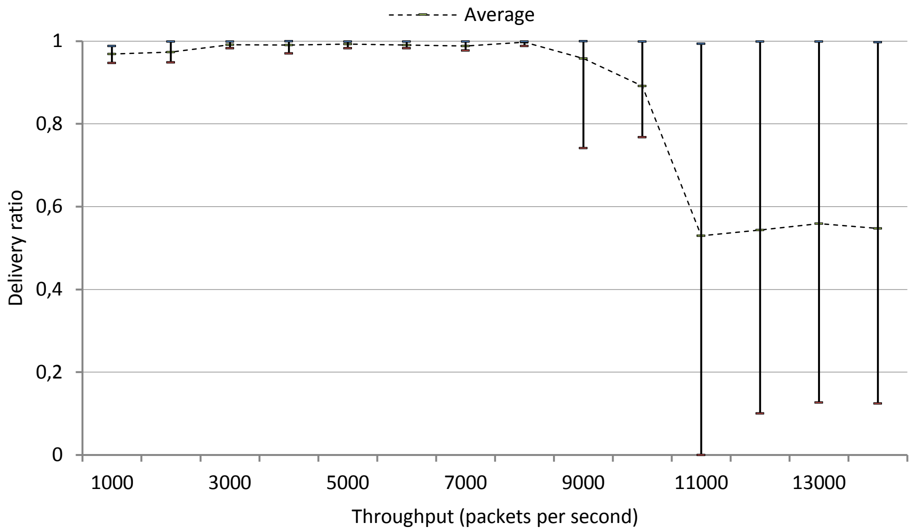


Figure 34. Impact of the packet transmission rate on the delivery ratio of multicast packets

As we aforementioned, the highest achieved rate is 12500 pps. However, the effectively expected rate is 14285 pps. Thus the achieved throughput is bounded by the CPU capability of the sender. To confirm this finding, we consider a second scenario of larger packets of 1500 byte-length transmitted at 54 Mbps and 6 Mbps, and then we compare the expected and the achieved throughputs. These results are illustrated in Table 11. They show that the gap between the two throughputs is lower when the packet transmission rate is reduced. Therefore they confirm that this rate is impacted by the CPU capability.

Table 11. Impact of the CPU performance on the packet transmission rate and the delivery ratio in a highly loaded network (i.e. the transmission queue of the sender is never empty)

Mode	Packet length	PHY rate	Highest theoretical rate	Highest achieved rate	Gap	Delivery ratio
Multicast	100 Bytes	54Mbps	14285pps	12500pps	12.50%	12.45 – 99.73%
	1500 Bytes	54Mbps	3597pps	3333pps	7.34%	99.88%
	1500 Bytes	6Mbps	486pps	471pps	3.09%	99.69%
Unicast	100 Bytes	Ath9k rate adaptation	-	-	-	11.2 – 99.99%

Moreover, we observe that the delivery ratios using 6Mbps and 54Mbps are almost the same although these data rates have different robustness degrees against the bit errors. This confirms that the losses are not caused by the signal distortion but they are due to the receiver unavailability. Furthermore, we notice that even the reliability of the unicast transport is considerably impacted by the CPU unavailability. However, the delivery ratio of the unicast outperforms that of the multicast when the packet transmission rate is low. This is because losses occur individually and the packets are received correctly at a retransmission attempt. But when the packet rate increases, losses occur in bursts with important sizes. Therefore a unicast packet and its retransmissions are all lost. This leads to packet rejections. To deal with these losses, one of the following or both of them should be considered. 1) The actual rate adaptation algorithms should take into account the fact that a packet may be lost due to CPU overload. 2) The CPU processing capability should be enough to process any arriving packet.

To obtain these results we use a powerful computer with two processors and no active acquisition device other than the 802.11 chipset (the keyboard is kept idle while the mouse is softly used). Hence, a less sophisticated receiver with one single processor (such as a smartphone or a tablet) may experience important losses starting from lower packet reception rates. Therefore, the use of a terminal with an appropriate configuration is the first requirement in order to take advantage of a multicast session with a high quality, but also to take a full advantage of the very high throughput capability of future networks.

It is worth noting that any coming packet (including that arriving with PHY or MAC errors and that addressed to another receiver) generates an interrupt and increases the processor load. Furthermore, disabling the promiscuous mode does not resolve the issue. This is because this mode is implemented by the device driver, and filters the packets already processed by the CPU. Therefore it is necessary to implement an alternative promiscuous mode at the network chipset itself in order to get ride of useless interrupts. This is required particularly with the imminent arrival of very high throughput networks which may send a huge number of packets to different receivers, and may disturb uninvolved stations with limited processing capabilities.

4.3.3.4 System Failures

Like any other electronic device, 802.11 terminals may experience internal system failures and may require a reboot. We highlight that this reboot is limited to the chipset (more precisely to the micro-controller) and does not concern the host terminal (e.g. the PC or the smartphone). Besides, the reboot is performed by a component of the chipset, conventionally called watchdog, and therefore does not require a human intervention. The aforementioned failures reduce the reception availability of the device and lead to packet losses. However, the high technological evolution enhances the devices performance significantly. Therefore the system failures may incur a very limited loss rate, typically less than 0.1% [113]. We are not able to determine the exact value of this rate for the case of the 802.11 chipset because it is not possible to separate the system failures from the losses caused by the CPU unavailability. But we agree that this rate is much lower than 0.1%. This is because during our empirical measurements, the device was able to receive more than 99.957% of the multicast packets. If we consider that the system failures occur with a constant rate, in this case this rate is less than 0.05%.

4.4 The Busy Symbol Mechanism

4.4.1 Transmission Procedure

To protect multicast packets against collisions we define a new transmission procedure based on the transmission of a short signal, called the Busy Symbol (BS), before sending the multicast packet itself. The principle of the BS is to briefly occupy the channel, so that the contending stations, which are sensing the channel, defer their transmissions. Therefore, if no station has started transmission along with the BS, this symbol will create a contention free medium for a period of time at least equal to DIFS after the BS transmission end. This delay allows the AP to transmit the multicast packet without collision.

There are no special duration constraints for the BS. However, the multicast packet should not be transmitted later than a PIFS (i.e. SIFS + SlotTime) after the transmission end of the BS in order to avoid the collisions. In this paper we consider that the BS is a short OFDM symbol of 0.8μs for two main reasons. 1) First, to save the available bandwidth and 2) second, to allow the AP to switch quickly to sense the channel in order to be able to receive correctly, if possible, any transmitted packet, in case another station started transmitting simultaneously with the BS. Furthermore, we consider that the sum of the BS duration and the sensing time is equal to one Slot Time. This delay is enough to detect any transmission which has started simultaneously with the BS [1].

After the BS transmission end, the AP starts sensing the channel. If the medium is determined to be idle for the duration of one slot time minus the BS duration, then the AP starts transmitting the multicast packet. Otherwise, the AP starts receiving the incoming packet (the packet that would cause a collision if no protection mechanism was used) and defers the multicast transmission. At the next transmission attempt of the multicast packet, the AP increases its CW and generates a new BT as a unicast sender does after a transmission failure. Increasing the CW intends to reduce the probability of a simultaneous channel access at the following attempt, and to guarantee a fair sharing of the medium between unicast and multicast traffics.

Our protection mechanism is compliant with all the 802.11 Physical layers (PHY) and ensures therefore the protection of multicast packets transmitted using all the available PHY data rates. We highlight that the use of the lowest PHY data rate to transmit multicast packets is the default configuration of the AP. However, there is no restriction, other than the reception capability of the multicast members, to use high data rates to transmit group addressed packets. In the remainder of this paper, we study the OFDM PHY layer as an example since it is the used layer within high throughput 802.11n devices. IEEE 802.11 OFDM symbols are classified into 4 categories:

- Short symbols. The duration of a short OFDM symbol is 0.8µs. 10 short training symbols are transmitted at the beginning of each OFDM PHY packet and allow the synchronization between the sender and the receiver.
- Long symbols. The duration of a long symbol is 3.2µs. 2 long training symbols are transmitted after the short symbols. Long and short symbols are separated by a Guard Interval (GI) of 1.6µs.
- SIGNAL. This is an OFDM symbol of 3.2µs and is situated one GI (of 0.8µs) after the 2 long symbols. SIGNAL carries the PLCP header and is always coded using the 6Mbps data rate. It indicates the length of the current packet and the used modulation of the following DATA symbols.
- DATA symbols. This is a variable number of OFDM symbols of 3.2µs separated with a GI of 0.8µs. The symbols' number is indicated in the PLCP header. The DATA part can contain up to 65535 symbols.

The PHY packet format is illustrated in Fig. 35.

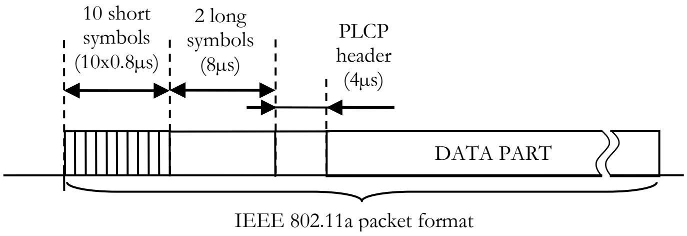


Figure 35. IEEE 802.11a (OFDM) PHY packet format

We illustrate, in Fig. 36 and 37, two examples of transmission attempts of a multicast packet using the BS mechanism. In Fig. 36, the AP and one station (STA1) are contending for the channel. In this example the AP has a BT set to 3 while the contending station has a BT equal to 4. Therefore the AP transmits first. Hence it sends the BS which defers any transmission of STA1 for a period of time corresponding to a DIFS and the rest of the decremented BT (in this case a slot time, corresponding to the initial 4 slot times minus the 3 slot times already elapsed) after the reception end of the BS. This delay allows the AP to send its multicast packet without collisions. Fig. 37 illustrates an example where both the AP and the station use a BT = 3. Hence they both start transmitting at the same time. After the transmission end of the BS, the AP senses the channel again and therefore detects the transmission of STA1. The transmission of the BS does not necessarily destroy the station's packet since an OFDM packet has 7 short symbols for detection purpose. The preserved symbols may allow the AP to synchronize with the unicast packet successfully and to receive it correctly.

When the BS mechanism is used to transmit a block of group-addressed packets, only the first one is protected. The others, however, are transmitted successively and are separated by a SIFS period, as specified by the standard.

The BS mechanism should be used by one device only within a WLAN in order to provide the highest performance. If our protection mechanism is used by several neighbor nodes, they may send their BS simultaneously then sense the channel at the same time. In this case, the nodes may miss the BS of each other since they were transmitting their own BS. Therefore they consider that the medium is free and start transmitting their packets. Hence a collision occurs. To avoid this scenario, our mechanism is designed to be used by the AP to transmit multicast packets, since the AP is the only allowed node to use the multicast mode within an infrastructure BSS.

We note that an OFDM packet is a sequence of OFDM symbols separated by Guard Intervals. Therefore, adding a new OFDM symbol (i.e. the BS) separated by a longer interval from the first symbol of the packet (i.e. one Slot time minus 0.8µs), is easy to implement. Moreover, the BS is a standard short OFDM symbol. Therefore any receiver is able to detect it. If a receiver misses the BS, this means that this receiver is not sensing the medium and is not contending for the channel. In this case this receiver will not cause any collision to the multicast packet.

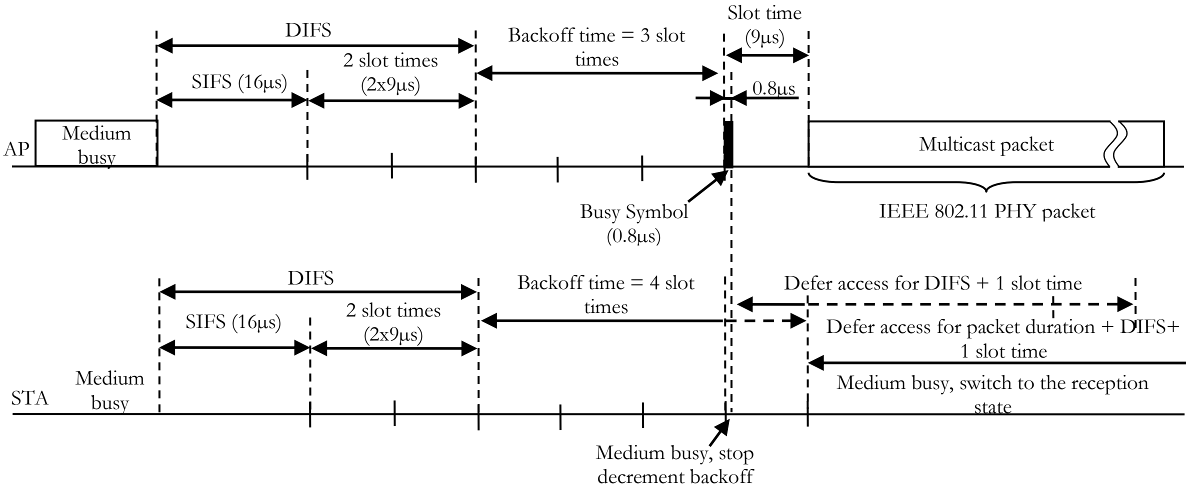

DIFS
Backoff time = 3 slot times
Slot time (9µs)
SIFS (16µs)
2 slot times (2x9µs)
0.8µs
AP
Medium busy
Multicast packet
Busy Symbol (0.8µs)
IEEE 802.11 PHY packet
DIFS
Backoff time = 4 slot times
Defer access for DIFS + 1 slot time
SIFS (16µs)
2 slot times (2x9µs)
Defer access for packet duration + DIFS+ 1 slot time
Medium busy
STA
Medium busy, switch to the reception state
Medium busy, stop decrement backoff

Figure 36. Example 1: contention with one station and transmission of the multicast packet

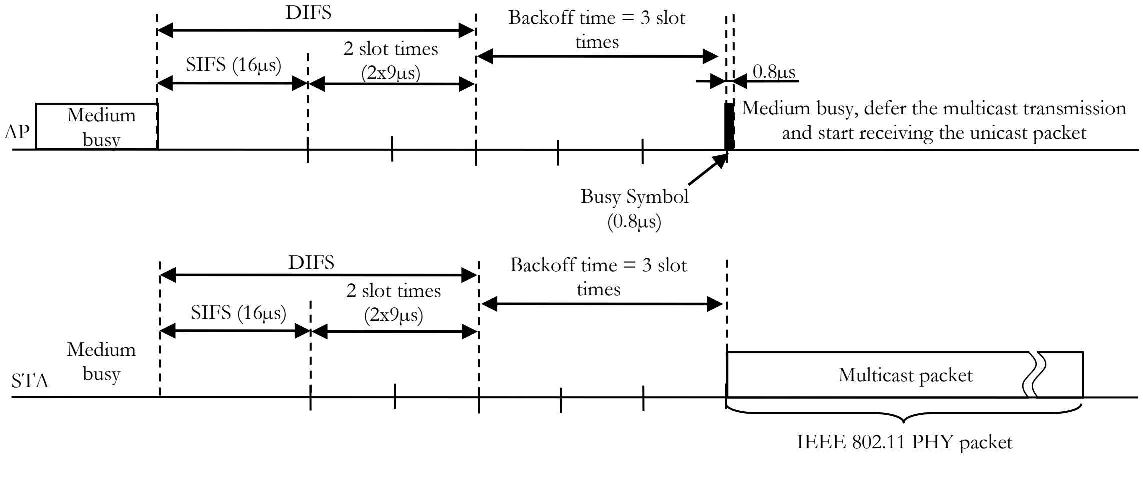


Figure 37. Example 2: contention with one station and transmission of the unicast packet

4.4.2 Performance Evaluation

In this section we evaluate the additional overhead incurred by the use of the BS mechanism. This overhead is equal to one *Slot Time* since one additional *Slot Time* is required to utilize our protection mechanism. We compute the transmission overhead ratio ($T_{overhead}$) using Equation (1):

$$T_{overhead} = \frac{Slot\ time}{Slot\ time + packet\ transmission\ duration} \qquad (1)$$

We show the obtained results in Fig. 38 for 3 different PHY data rates of 6, 54 and 300Mbps. We use the aggregation feature of the IEEE 802.11n (A-MPDU) and we draw the overhead ratio for different numbers of aggregated packets. Each packet has a data length of 1500 octets. We observe that the highest transmission overhead is incurred when transmitting only one packet at 300Mbps. This highest ratio remains inferior to 6% and decreases significantly when increasing the number of aggregated packets. We notice that the incurred overhead is less than 1% for an A-MPDU of more than 20 aggregated packets for all the 3 used data rates.

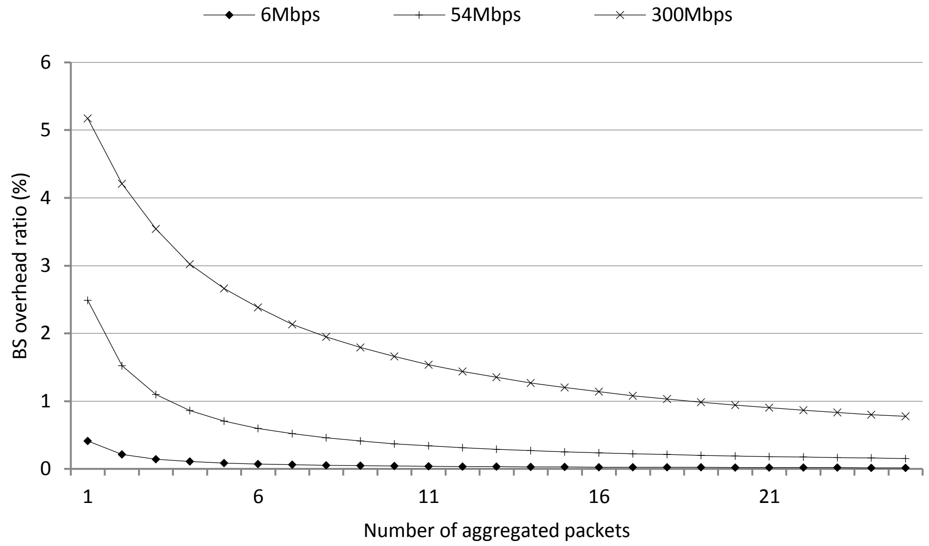


Figure 38. Theoretical overhead ratio using the BS

We use NS-3 to evaluate our proposal. We build an IEEE 802.11 network and we set the stations randomly at a distance of 10 meters around the AP in order to ensure a good reception signal. Therefore packet losses are only caused by collisions.

We measure the maximum throughput of the AP in an unshared WLAN. We compare the efficiency of the multicast, the multicast + BS, the unicast and the unicast + RTS/CTS. All packets are delivered using UDP and have 1500 Bytes length. Moreover the transmission queue of the AP is never empty (i.e. the AP is in the saturated condition). We illustrate the obtained results in Fig. 39. Hence, we demonstrate that the efficiency of the protected multicast is close to that of the legacy multicast.

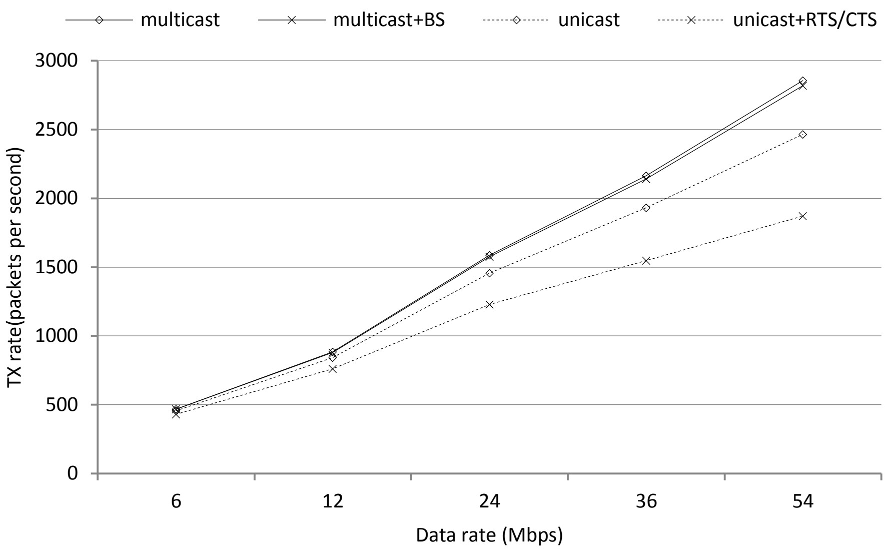


Figure 39. Transport efficiency vs. Data rate

We evaluate the fair sharing of the channel in Fig. 40. We consider the case of a highly loaded network. We build a WLAN of one AP and 25 associated stations. In all the tests, the AP delivers a multicast traffic. In each test we run a new unicast session on a new station among the associated stations, in order to increase the collision rate of the network. We show that the numbers of transmitted (TX) and delivered (RX) multicast packets are similar to those of the delivered unicast packets. On the other hand, the unicast transport may encounter several collisions (between other unicast packets). Since missing packets are retransmitted, the number of transmitted packets is higher than that of the delivered packets. Furthermore, our results show that the protected multicast transport avoids the collisions perfectly, allowing the delivery of all the transmitted multicast packets.

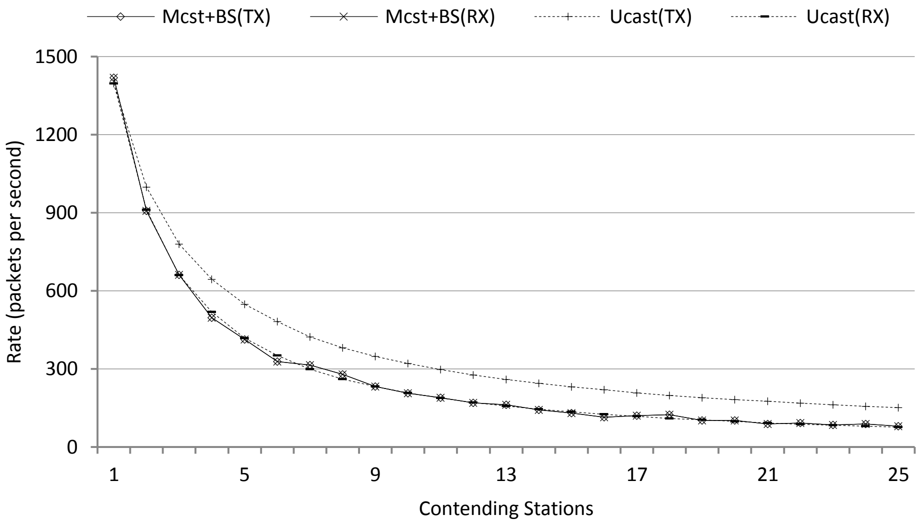


Figure 40. Medium sharing using the BS

We compare the delivery rate of the protected and the legacy multicast transports in Fig. 41. These measurements show that the BS mechanism provides a perfect protection against the collisions, allowing the successful delivery of all the transmitted packets. However, the reliability of the legacy mode is very limited and decreases significantly with the increasing number of contending stations.

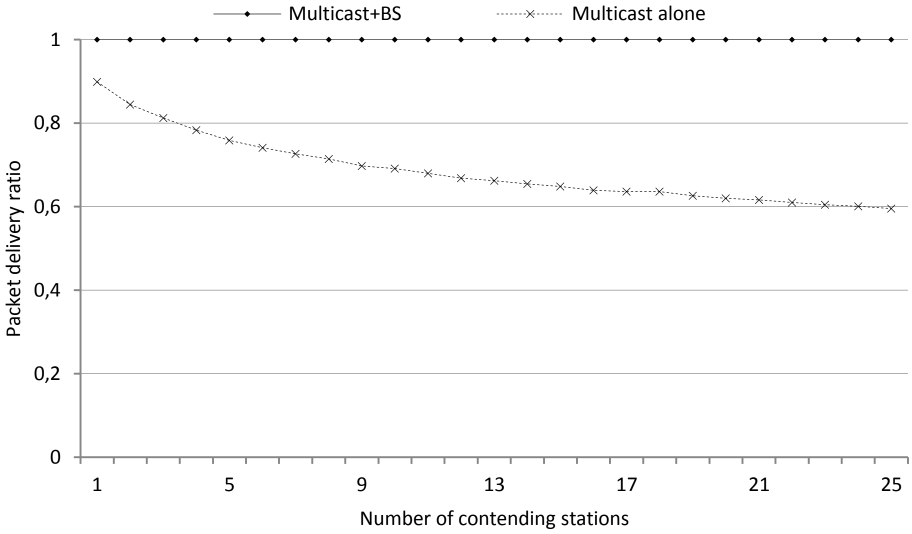


Figure 41. Packet delivery ratio in an ideal medium

We evaluate the impact of the legacy and the protected multicast transports on the collision rate of the unicast flows. Thus we build a BSS of one AP and 5 associated stations. All the stations are in the saturation condition and transmit unicast packets to the AP. During the first 10 seconds, the AP does not send any data, and then it sends bulks of multicast data. Fig 42 illustrates the impact of the legacy multicast on the unicast collision rate and shows that this rate increases when the AP starts delivering the multicast flow. Besides, we observe that the multicast suffers from a high collision rate.

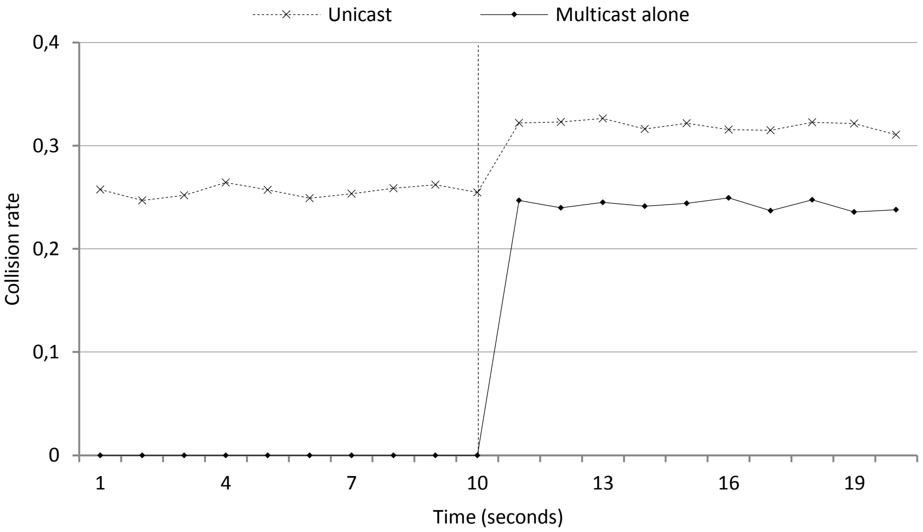


Figure 42. Impact of multicast on the collision rate of unicast flow

In Fig 43, we evaluate the behavior of the collision curve of the unicast mode before and after the beginning of the multicast session. This curve shows that, if we consider that the BS does not destroy the unicast packet, the collision rate of the unicast is not impacted by the protected multicast transport. However, with or without this consideration, our results show that the BS mechanism is able to avoid the collisions perfectly.

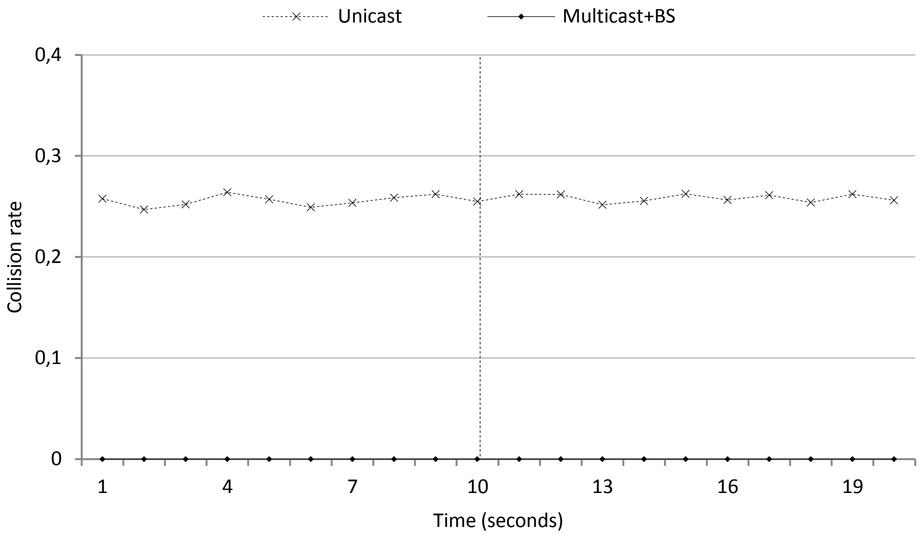


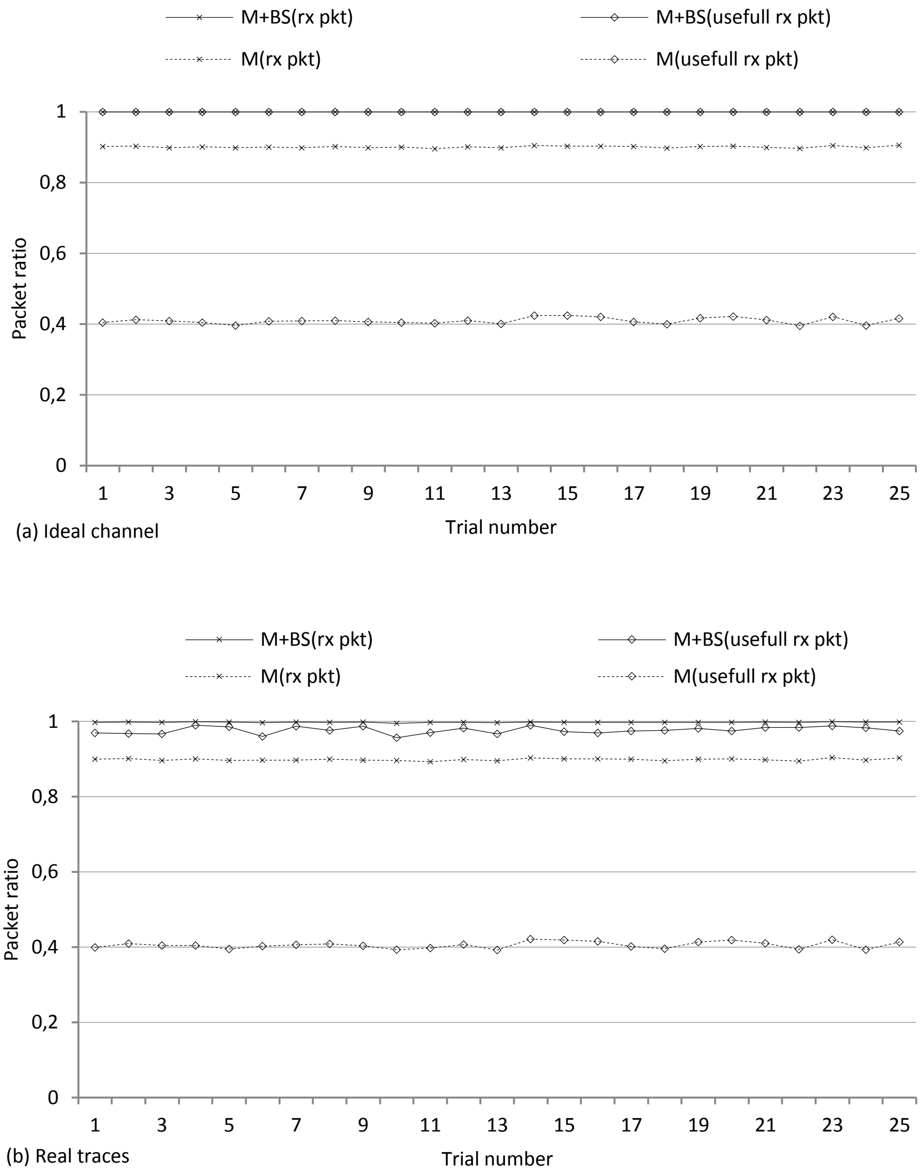
Figure 43. Impact of the BS on the collision rate

It is worth noting that the multicast transport is mainly used to deliver video services. Therefore we evaluate the impact of the multicast transport, with and without protection, on the delivery ratio of a variable bit rate (VBR) video stream. The video has an average rate of 1360 Kbps, 25 frames per second (fps) and duration of 60 seconds. The AP delivers the multicast stream using Real-time Transport Protocol (RTP). Hence one image is packetized and forwarded to the MAC layer every 40 ms. We consider that the medium is shared between the AP and one station transmitting unicast packets and being in the saturation condition. We believe that this scenario is frequent in real networks and may occur if one user starts uploading a large file or sharing such a file with another user in the WLAN.

In Fig. 44(a) we consider that the transmission failures are caused only by the collisions. However in Fig. 44(b), we use loss traces gathered from a real network in order to obtain performances similar to a real test bed. The AP transmits the same video several times.

We measure the average delivered packets (rx) and useful delivered packets (useful rx). We consider that a packet is useful if it belongs to a video image which can be decoded because all of its constituent packets were received correctly. This is the reception policy of the live555 [114] module which forwards only the entirely received images to the decoder module. An image with missing portions is rejected and its received packets are useless.

We observe that in the ideal channel, the protected multicast is reliable and delivers all the packets. On the other hand, the legacy multicast is able to deliver almost 90% of the packets. However, less than 60% of the video packets are useful. Using traces of real network losses, the performance of the legacy and the protected multicast transports is slightly decreased. But the reliability of the protected multicast remains acceptable for a loss tolerant traffic which is the case of the video streams.



(a) Ideal channel

(b) Real traces

Figure 44. Video delivery ratio using the legacy and the protected multicast transport

We evaluate the video image delivery ratio in an increasingly shared WLAN, using loss traces gathered from a real network. All the contending stations are in the saturation condition. We compare the reliability of the legacy and the protected multicast. The obtained results are illustrated in Fig. 45. While the reliability of the legacy multicast is always limited, that of the protected multicast depends on the retry limit. Hence if the AP has no retry limit (nrl), it tries indefinitely till transmitting the multicast packet. However, if the AP uses the default retry limit, it may delete several packets after reaching the transmission attempt limit. Fig. 45 shows that the protected multicast with no retry limit has a high reliability which does not depend on the collision rate. However, the protected multicast with the default retry limit still has a high reliability in a network of a limited number of active users.

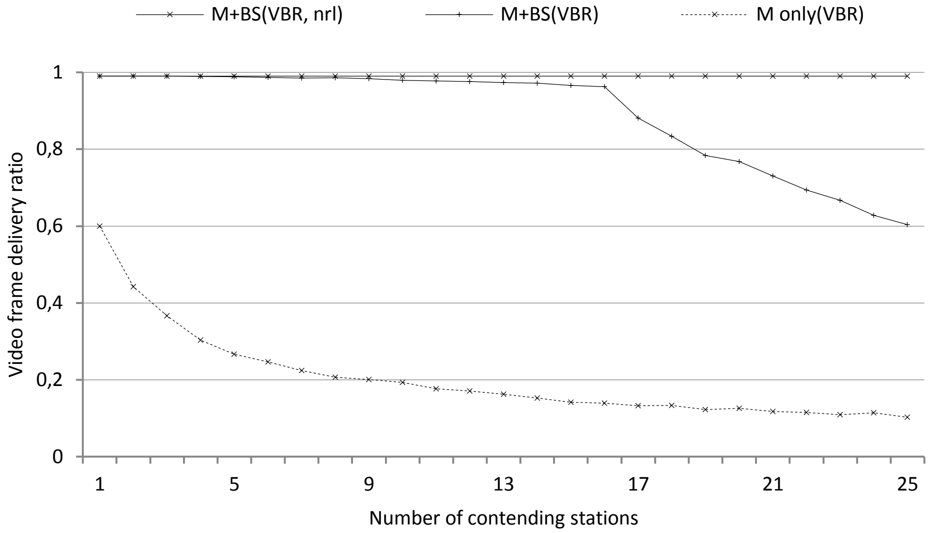


Figure 45. Video frame delivery ratio using real loss traces

4.5 Conclusion

In this Chapter we show that the path loss and the collisions are the principal factors of packet losses in wireless networks. Besides, we introduce the device unavailability phenomena and we demonstrate that the device itself may increase considerably the loss rate of the multicast traffic in the following 2 cases: 1) the device is sleeping according to the power save mode, and 2) the CPU is overloaded and is unable to process all the arriving packets. Thus we identify the causes of the bursty losses and of the unexplained excessive losses which may occur even in good reception conditions.

Furthermore, we define and introduce the Busy Symbol and we prove that this mechanism is able to protect the multicast packets against all the collisions. Thus, BS improves the reliability of the multicast transmissions considerably. Moreover, we demonstrate that almost all the loss factors may be avoided and that the multicast transmission failures become very limited in a typical network under the following assumptions: 1) the receiver is within the range of the sender, 2) packets are transmitted using the appropriate PHY data rate, 3) collisions are avoided, and 4) the availability of the receiver is maximized.

Chapter 5

5 The Block Negative Acknowledgement (BNAK) Protocol

5.1 Introduction

The main advantage of the multicast transport is its high scalability. However, the conventional multicast protocol of 802.11 is not reliable due to the absence of any feedback policy. Thus, missing packets are definitely lost. In particular, the multicast transmissions are vulnerable to the collisions and to the device unavailability. Besides, multicast packets are by default delivered at the lowest data rate to reach the entire coverage area of the wireless network. This selected rate wastes the bandwidth and reduces the network throughput. The selection of a higher transmission rate is not obvious since the AP is not aware about the reception capabilities of the group members. To resolve both of the unreliability issue and the reduced efficiency problem, it is necessary to define a feedback policy for the multicast transport.

The IEEE 802.11v and 802.11aa are two recent amendments which enhance the reliability of the multicast transmissions. The former defines Directed Multicast Service (DMS) while the latter introduces the Groupcast with Retries (GCR) service. DMS converts a multicast stream into multiple unicast sessions. It resolves the unreliability issue on the expense of the bandwidth. Therefore, DMS has a very limited scalability. On the other hand, GCR defines the Block Ack (BACK) policy which allows the AP to recover the feedback of each member using the individual Block Ack Request (BAR)/BACK exchange. Similar to DMS, GCR-BACK is a reliable multicast protocol. But it incurs an overhead which depends on the group size. Thus, the scalability of GCR-BACK is also limited.

In this chapter we introduce a new multicast protocol called Block Negative Acknowledgement (BNAK). The main objective of BNAK is to define a reliable and a scalable multicast transport in 802.11 networks while retaining the compatibility with the former and the newer amendments of the 802.11 standard. The principle of our protocol relies on the fact that losses in WLANs become very limited if the appropriate actions are taken. Thus, BNAK requests negative acknowledgement from members experiencing packet losses. Under the assumption that the loss rate of the network is reduced, a very limited number of feedbacks are transmitted and the bandwidth is saved. These feedbacks are also useful to select the most appropriate transmission rate.

The remainder of this chapter is organized as follows. In Section 5.2 we provide an overview of the principle categories of multicast protocols, and we highlight their major limitations. We dedicate Section 5.3 to introduce a new functionality in managing the group members, and to present BNAK. We define an analytical model of our protocol in Section 5.4. Then we present simulation results in Section 5.5. Finally, in Section 5.6, we conclude this chapter.

5.2 Related Work

Many protocols are defined in order to improve the performance of the multicast transport over 802.11 networks [44-79]. Most of them can be classified into three categories: ACK-based, Negative ACK (NAK) based and pseudo-broadcast protocols. The principle of the first category is inherited from the unicast feedback policy, and requires each multicast receiver to send a feedback. However, ACK-based protocols incur an important overhead which depends on the group size. This limits the scalability of these proposals significantly.

The NAK-based protocols rely on the selection of a group leader to acknowledge each packet. On the other hand, the other members are allowed to send a NAK following a reception failure. This NAK intends to prevent the successful reception of the ACK which may be transmitted to the multicast source. Once the ACK is missing, the sender retransmits the multicast packet. The NAK principle requires one single feedback slot to send ACK/NAK. This limits the transmission overhead and retains the scalability of the protocol. But this concept is not compliant with the 802.11 standard which relies on the collision prevention. Besides, The NAK principle does not provide an efficient solution as it has been proven that the simultaneous transmission of two packets does not necessarily lead to the loss of both of them [57]. Hence, the ACK may be received even if a NAK is transmitted. Another limit of these protocols is that they can acknowledge only one packet at a time. Therefore they can neither be used with the block transmissions nor with the aggregation delivery of the 802.11n. Moreover, they are vulnerable to the device unavailability issue: if a packet is lost due to this issue, the receiver can not send a NAK and the packet is definitely lost.

The main idea of Pseudo-broadcast protocols is to select one member to send a feedback following the successful reception of each multicast packet. The other members, however, do not send any notification. Thus, these protocols are scalable and compliant with the standard but they are not fully reliable. Besides, they do not allow the AP to select the appropriate data rate since the sender is aware about only one down link. This leads the AP to select the lowest transmission rate which reduces the network throughput.

Furthermore, all the proposed protocols require a group membership detection function in order to identify the multicast members. The definition of such a function is beyond the scope of the standard, but a detection function typically relies on the snooping of IP packets. This design is pretty enough to identify new joining members but is not optimized. This is because an IP packet is processed twice, once at the

MAC layer and once by the network layer. Besides, the MAC layer needs additional snooping and management functionalities which are already available at the upper layer.

5.3 Protocol Presentation

5.3.1 Group Membership Management

In our conception of BNAK, we consider that only the AP is required to gather information about the group members. Therefore a multicast member does not need to perform any snooping at the MAC layer. This minimizes the client requirements and simplifies the deployment of our protocol. When a client joins a multicast service, the AP is responsible for notifying the member's MAC layer. So the client takes advantage of the reliability of the BNAK. Similarly, when the client leaves the group, the AP sends a message to the client's MAC layer in order to remove this station from the multicast group.

Most AP equipments integrate both the AP and the router functionalities within the same terminal. Therefore membership information is available at the Network layer of the same device. In order to ensure the awareness of the MAC layer about the group membership, we propose the exchange of internal messages (packets or signals), called membership notifications, between the Network and the MAC layers of the AP equipment. These messages are transmitted from the router level to the 802.11 MAC layer, whenever a new event occurs.

Two possible events may occur: 1) a new member joins the group and 2) a member leaves. As the notification messages are internal to the same device, they do not need any bandwidth resources and they are transmitted reliably to the MAC layer. Hence the AP does not need to acknowledge them. We highlight that this group management procedure eliminates the need for snooping IP packets at the MAC layer, and therefore reduces the device processing load compared to a snooping-based approach. The group membership management function may be achieved in a constructor dependent fashion when the AP equipment is entirely built by the same manufacturer. But in most cases, the chipset driver and the network stack are implemented by different parties. In this case it is necessary to standardize the notification interface between the network and the MAC layers. The signal-based notification method is the most appropriate one and is commonly used to configure the MAC layer and to set the different parameters such as: CWmin, CWmax, Retry limit, packet lifetime limit, beacon interval, etc. However, this method depends on the operating system (Windows, Linux, Android, embedded systems, etc.). On the other hand, the approach based on the internal packet exchange is another alternative which runs transparently to the underlying system architecture. In this chapter we provide a simple, yet accurate example of the notification function using the packet exchange method. This method may be easily converted later to the signal-based approach.

The MAC layer of the AP saves a table of the different available multicast sessions. This table contains the multicast MAC address and the Session Identifier (SID) pairs. The MAC address per multicast session should be unique. We note that two different sessions may have the same MAC address in the following two cases: 1) two servers use the same multicast IP address, or 2) the mapping of two IP addresses leads to the same MAC address. Therefore, it is necessary that the mapping function of the upper layer attributes a unique MAC address for each multicast session. Besides, to each address corresponds a unique Session Identifier (SID). This identifier is generated by the MAC layer and is encoded on 15 bits. Thus the AP may deliver up to 32768 sessions simultaneously. We use a SID as the session identifier instead of the MAC address in order to reduce the size of the control and management packets and to maximize the efficiency of our protocol. This is because a MAC address requires 6 Bytes compared to only 2 Bytes needed to send an identifier. However, it is possible to replace the SID with the MAC address. This does not disturb the right operation of BNAK but slightly reduces the achieved throughput.

When the Network layer of the AP receives an IGMP/MLD join or leave request, it sends a notification packet to the MAC layer. Similar to the Address Resolution Protocol [8], the notification packet uses a simple message format and is encapsulated in an Ethernet frame. To identify this packet, we use a specific EtherType of 0xF000. This value is not attributed and will not cause any processing confusion. However we neither add padding nor CRC to the packet since it does not leave the machine. Besides, we recommend the use of the MAC address of the AP as the source and the destination addresses of the Ethernet frame. This allows the MAC layers, which do not support BNAK, to delete the packet or to send it back to the Kernel. The format of the notification Ethernet packet is illustrated in Fig. 46.

6 Bytes	6 Bytes	2 Bytes	6 Bytes	6 Bytes	1 Byte
MAC Destination	MAC Source	EtherType = 0xf000	Member MAC Address	Multicast MAC Address	Event

Figure 46. Ethernet notification packet of type 0xf000

The MAC address of the member allows the AP to determine the receiver. The *Event* field carries the value 1 when the member joins the group. However, the value 0 notifies the member departure. The AP maintains a table per multicast session. This table contains the addresses of all the group members. The AP updates this table by adding or removing an address each time a new event occurs. When the last member leaves the group, the AP deletes the table and releases the attributed SID.

Furthermore, the AP notifies the appropriate receiver following any join or leave event. We note that BNAK does not need a specific membership detection function. But it requires the awareness of AP of the group members. This awareness may be achieved using the proposed message notification method or any other solution, including the snooping technique. On the other hand, BNAK defines a management packet, called *Membership Notification*, to inform the associated stations about their membership. This packet is illustrated in Fig. 47.

The four first fields and the last field of the notification packet are standard elements. The *Multicast Address* field is used to identify the concerned session. The *SID* field carries the identifier of this session. The *Starting Sequence Number* field indicates the sequence from which the receiver is allowed to request packets. This field is required when a member joins a group in the middle of the session. Therefore it does not request packets which were transmitted and still buffered for older members. The membership status is 1 if the receiver joins the group and 0 if it leaves the session.

2 Bytes	2B	6B	6B	6B	2B	2B	1B	1B		2B	4B
Frame control	Duration/ ID	Address 1 (RA)	Address 2 (TA)	Multicast Address	SID	Starting Seq. Num.	Membership Status	Rsvd 4bits	Lowest Rate	PER Limit	FCS

Figure 47. Membership notification packet format

The *Lowest Rate* field indicates the minimum transmission rate that the AP can afford for the multicast session. The default PHY layer is OFDM since it is the used one within high throughput networks. Thus, the *Lowest Rate* field is encoded on 4 bits according to Table 18.6 of [1]. However, any other PHY layer may be used and signaled by allocating the reserved bits preceding the *Lowest Rate* field. The *PER Limit* field contains the value of the Packet Error Rate that the AP tolerates. This value is set on a basis of 10000, e.g. PER=100 indicates a PER of 1%. The value of the *PER Limit* field varies between 1 and 10000. It allows a member to determine the coverage area of the multicast service. This coverage is infinite when PER=10000. The nil value as well as values higher than 10000, are reserved.

A notification packet is acknowledged and, therefore, is transmitted reliably to the receiver. Fig. 48 illustrates an example of membership management using BNAK and a layer 3 management protocol.

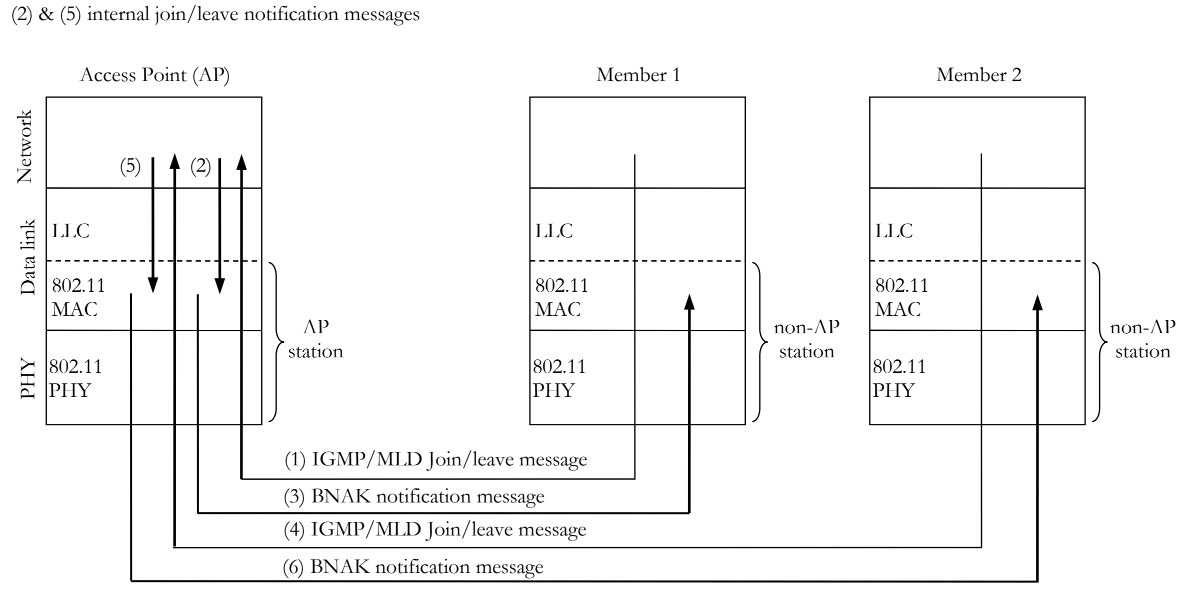

(2) & (5) internal join/leave notification messages
Access Point (AP)
Member 1
Member 2
Network
Data link
PHY
(5)
(2)
LLC
802.11 MAC
802.11 PHY
AP station
LLC
802.11 MAC
802.11 PHY
non-AP station
LLC
802.11 MAC
802.11 PHY
non-AP station
(1) IGMP/MLD Join/leave message
(3) BNAK notification message
(4) IGMP/MLD Join/leave message
(6) BNAK notification message

Figure 48. Group membership management example using BNAK and IGMP/MLD with internal notification messages at the Access Point equipment

5.3.2 Transmission Procedure

The IEEE 802.11 defines robust modulation schemes, an efficient signal processing and powerful error correction codes. Thus errors are mainly due to collisions, inappropriate transmission data rate or device unavailability. Therefore, packet losses become very limited in a typical network under the following assumptions: 1) collisions are avoided, 2) the receiver is within the range of the sender, 3) packets are transmitted using the appropriate PHY data rate, and 4) the terminal availability is maximized. In order to ensure this limited PER it is essential to use a certified terminal with a suitable configuration, to select the appropriate data rate and to protect multicast packets against collisions. This protection may be guaranteed using standard features like CTS-to-Self or channel access during Contention Free periods. To further protect multicast packets against collisions, we propose the Busy Symbol mechanism.

The design of the Block Negative Acknowledgment (BNAK) policy relies on the principle that the PER of the wireless network is very limited. In this case it is more appropriate for the AP to request negative feedbacks from the multicast members experiencing losses, than requesting repeatedly BACKs for packets which are delivered correctly almost all the time. Using the BNAK policy, packets are transmitted in block followed by a Block NAK Request (BNR). Only users encountering losses are invited to send a feedback. Therefore if all packets are transmitted correctly, no BNAK is transmitted and the bandwidth is saved. If a failure occurs, only the impacted receivers are allowed to send a feedback. In order to avoid eventual collisions between multiple BNAKs, these packets are transmitted after channel contention and are acknowledged by the AP. Therefore a BNAK is retransmitted if it is lost. Once the BNR is transmitted, the AP should contend for the channel before transmitting any other packet. It is therefore possible that the AP gains the channel and transmits a new block before receiving the BNAKs, if any. We depict an example of the BNAK procedure in Fig. 49.

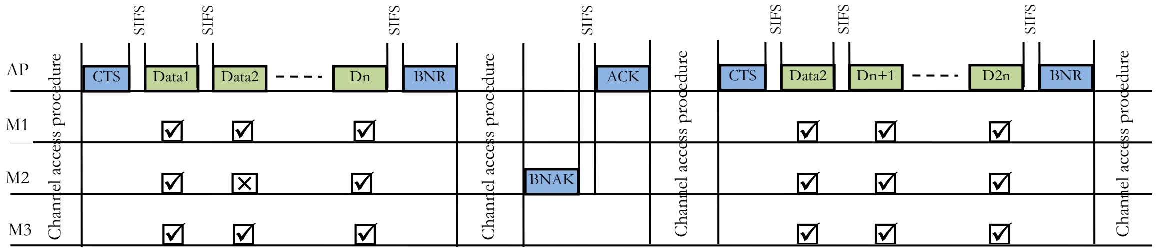
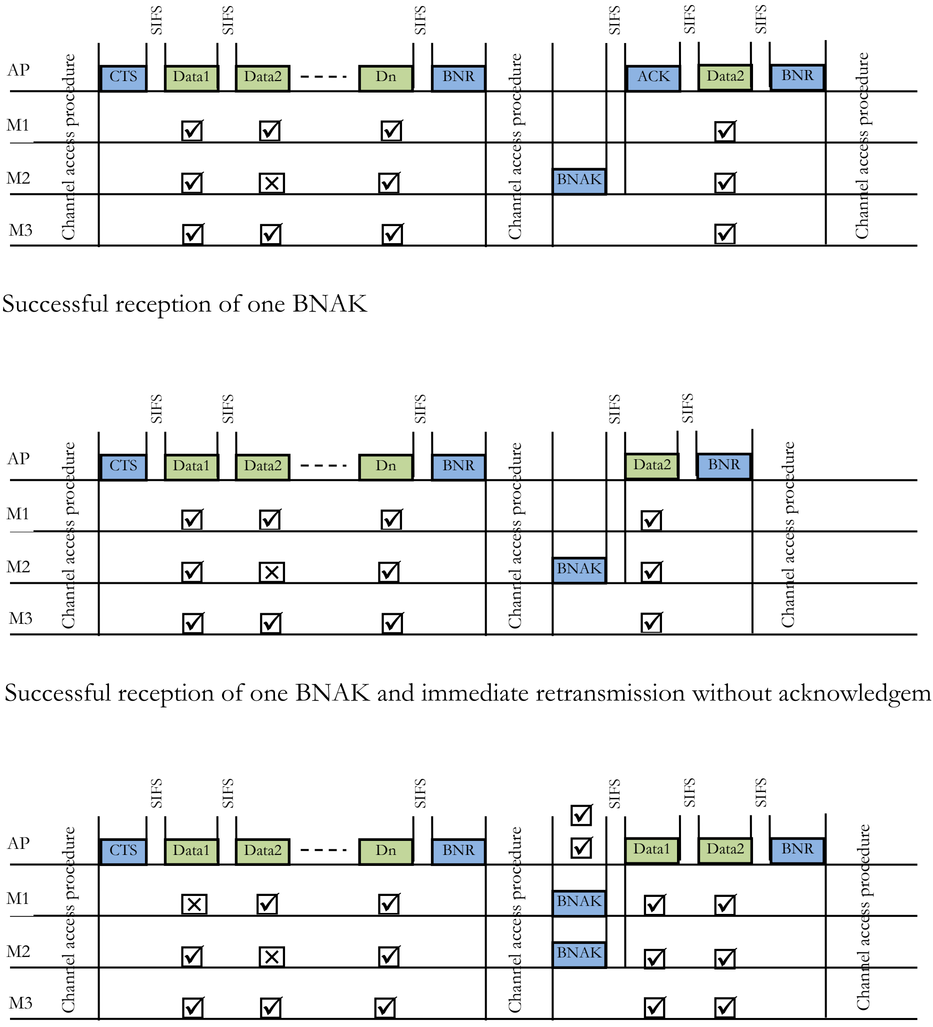


Figure 49. Packet exchange using the BNAK policy and the CTS-to-Self protection mechanism

In addition to the main transmission procedure of BNAK, we define the immediate retry mode. This policy reduces the retransmission latency. It allows the AP to send missing packets immediately after acknowledging the BNAK. Besides, the immediate retry policy is more robust against high loss rates. Under this scenario, several receivers may lose the same packet and may contend for the channel to send a BNAK. Upon the reception of the first feedback, the AP retransmits the requested packet. Once the missing packet is received, the other members cancel their contention. However, the immediate retry is used only to send missing packets. It should not be used to send new data. New packets should be sent after channel contention. The immediate retry mechanism of BNAK is illustrated in Fig. 50. Optionally, the AP may send missing packets without acknowledging the BNAK. This reduces the overhead.

It is worth noting that recent physical layers may receive simultaneous transmissions correctly under certain conditions. This new capability is called Successive Interference Cancellation (SIC) [115-117]. When the AP receives several BNAKs simultaneously, it does not send multiple ACKs. Instead, it sends the requested packets. This scenario is depicted in Fig. 50(c). We highlight that a member should cancel its BNAK transmission if it receives the missing packets before the successful delivery of the feedback.



a) Successful reception of one BNAK

b) Successful reception of one BNAK and immediate retransmission without acknowledgement

c) Successful reception of multiple BNAKs

Figure 50. Packet exchange using the immediate retry mechanism of the BNAK policy

The reliability of our protocol is based on the successful reception of the BNR. But this packet may be lost. To avoid the loss of the BNR, we transmit it using a robust data rate (or even the most robust, but the lowest rate). Even though this packet is lost (this should be very exceptional), a multicast member builds its BNAK, if any, using the following BNR. We note that the loss of a BNR does not affect the reliability of our protocol if the multicast packets are received correctly.

It is worth noting that the use of a low data rate to send BNRs does not require much more transmission time compared to a high PHY data rate. This is because an important part of the transmission time of the packet is used by the SIFS plus the required time to transmit the PHY preamble and header. Table 12 illustrates the required time to transmit a BNR and another 1500 byte-length packet at different data rates. As successive packets are separated by one SIFS period, we add this delay to both packets.

We notice that the BNR transmission duration at 6Mbps requires less than twice the duration at 54Mbps, instead of 9 times as would be expected. We observe that transmitting the BNR at 12 Mbps may even require less time than using the data rate of 130 Mbps. This is because the IEEE 802.11n defines longer PHY preambles and headers.

Table 12. PHY packet transmission duration (plus one SIFS)

Rates (Mbps)	BNR (21Bytes)	Data packet (1500B)
6	68 μs	2040 μs
12	52 μs	1040 μs
24	44 μs	540 μs
48	40 μs	288 μs
54	40 μs	260 μs
130	48 μs ; 56 μs	140 μs ; 148 μs

When a packet is lost, the receiver builds a BNAK immediately following the reception of the BNR. Therefore, the required delays to retransmit missing packets vary from several hundreds of microseconds to few milliseconds. For the extremely rare cases where both the data packet and the BNR are lost, the incurred retransmission latency remains very limited and appropriate for multimedia applications. This is because a video streaming service generates a real-time flow at the image display rate. For a video of 25 frames per second, the typical delay between two successive BNRs is about 40ms. Thus, some exceptional retransmissions are subject to this delay. Such latency is very limited and is perfectly supported by all the video players which mostly tolerate delays starting from 1 second. However, our protocol is also very appropriate for applications with strict delay requirements. This is because the packets experiencing latencies higher than 20ms are very rare, and their rejection does not affect the user satisfaction.

It is worth noting that the BNAK policy may also be used to deliver individual packets. Moreover, our proposal works properly with the packet aggregation feature of 802.11n, i.e. A-MPDU. To enhance the efficiency of our protocol, a BNR may be used to request feedbacks of all the available multicast sessions. The packet format of BNR and BNAK is illustrated in Fig. 51.

Both BNR and BNAK have several standard MAC fields which are the 3 first fields and the last field for BNR, and the 4 first fields and the last field for BNAK. The Session Identifier (SID) field is present in both BNR and BNAK. This field contains the *Is last SID* bit and the SID. If the *Is last SID* bit is set, the current session is the last one in the packet. Otherwise, one or many other sessions follow till the *Is last SID* bit is set. The SID is used to identify the multicast session. This identifier is encoded on 15 bits. Thus the AP may attribute up to 32768 different SID. Following the SID field, both BNR and BNAK contain 4 reserved bits and the *Number Sub-Session* field. We define the latter field to support streams with different layers. In this chapter we consider multicast traffic with one single layer. Thus the value of the *Number Sub-Session* field is set to 0. The utility of this field is explained in chapter 6.

The BNR contains the first and the last sequence numbers of the multicast packets which belong to a given session and are available at the AP. If the first sequence is equal to the last sequence, this means that only one packet (having a sequence number equal to that of the first sequence field) may be requested and retransmitted. Since the sequence number of a packet is modulo 4096, we limit the maximum number of packets which may be signaled using the BNR to 2040. However, the effective limit is implementation dependent. In our evaluation of the BNAK protocol we consider a limit of 255 packets.

We define the *Rate* field to support quality differentiation of layered streams. This field indicates the used PHY data rate to deliver the multicast packets. The default PHY layer is the OFDM one. Thus the *Rate* field is encoded on 4 bits according to Table 18.6 of [1]. However any other PHY layer may be used and signaled by allocating the reserved bits preceding the *Rate* field.

The BNAK includes the sequence of the first missing packet. The *Bitmap length* field indicates the length of the *bitmap* field. If only one packet is lost, no bitmap is inserted and the *Sequence first loss* field is used to identify the missing packet. Otherwise a bitmap of up to 255 bytes is included and is used to indicate the reception status of up to 2040 packets. This bitmap is filled similarly to the bitmap of the standard BACK feedback.

All reserved bits in BNR and BNAK are set to 0.

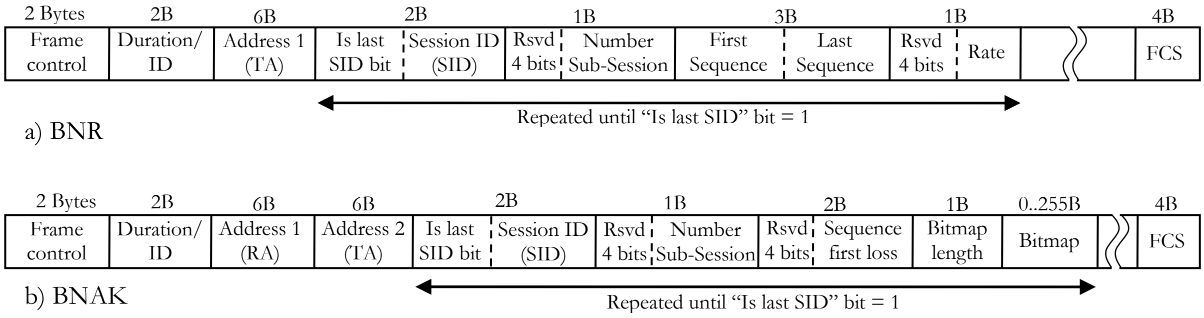


Figure 51. BNR and BNAK packet format

5.3.3 Protection against Useless Transmissions

It is necessary to define robust actions in order to avoid useless BNAK transmissions. Also the member should not send a BNAK which requests missing packets in addition to packets being received correctly. Therefore we define the following 3 different statuses of a packet:

- **OK**: the packet is correctly received and does not need any retransmission;

- **Missing**: the packet is lost and either 1) the receiver sent a BNAK successfully and is waiting for the retransmission of the missing packet or 2) the receiver is waiting a BNR in order to build a BNAK;

- **Pending**: the member generated a BNAK to request the retransmission of this packet. However, the BNAK is still buffered or being delivered, but the delivery has not finished yet (i.e. ACK not received yet).

When the packet status is *Pending*, the member should not build a new BNAK to request the pending packet, unless the status of at least one other packet is *Missing*. In this case, upon the reception of a BNR, the member should 1) delete the pending BNAK, 2) modify the status of *Pending* packets to *Missing*, 3) build a new BNAK and 4) set the status of all missing packets to *Pending*. Upon the final transmission success or failure of the BNAK (failure due to reaching the retry limit), the status of all pending packets is set back to *Missing*.

A member may receive correctly a packet having the status *Pending* (the packet is retransmitted based on the feedback of another member which experienced the same failure and gained access to the channel first). In this case this receiver 1) sets the status of the corresponding packet to *OK*, 2) deletes the buffered BNAK (since it is not adequate any more), 3) sets any pending packet to *Missing* and 4) waits for the reception of a new BNR in order to build a new BNAK, if still required.

It is possible that the AP receives BNAKs requesting the retransmission of more packets than what the AP is allowed to send within a block. In this case the AP retransmits as many packets as possible within a TXOP, and builds a BNR which has in the *Last Sequence* field the sequence number of the packet preceding the first missing packet which will be retransmitted in the next block. Therefore, the AP avoids any BNAK which may request a packet that the AP is willing to retransmit. As an example, suppose that the AP is allowed to send one single packet per block, but receives a BNAK requesting packets 1 and 4. Then the AP retransmits packet 1 followed by a BNR having 3 in the *Last Sequence* field and contends again for the channel to send the second missing packet. Hence the AP avoids BNAKs requesting packet 4 before the retransmission of this packet.

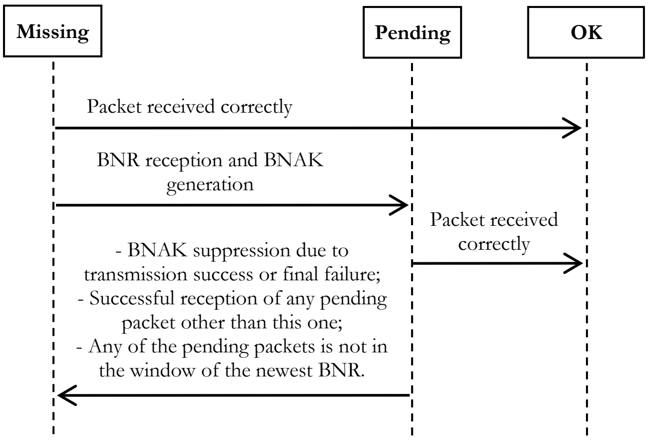

Missing
Pending
OK
Packet received correctly
BNR reception and BNAK generation
Packet received correctly
- BNAK suppression due to transmission success or final failure;
- Successful reception of any pending packet other than this one;
- Any of the pending packets is not in the window of the newest BNR.

Figure 52. Packet status sequence diagram

On the other hand, if a member receives a BNR and finds that the sequence number of at least one pending packet is no longer in the BNR window, in this case this member should delete the pending BNAK and build a new BNAK, if still required, based on the new BNR.

We highlight that all 802.11 devices deliver a copy of all transmitted packets to their drivers and notify about the transmission success or failure. This notification allows a member to update the status of *Pending* packets following the transmission of a BNAK. Fig. 52 depicts the sequence diagram of different status.

We consider the special scenario illustrated in Fig. 53 in order to clearly introduce the required actions for a robust protection against useless BNAK transmissions and useless data retransmissions. We intentionally omit the collision protection feature in this figure for a better quality of the presentation.

At t=t_1, members M1 and M2 receive packets 1 and 3 successfully. However they fail to receive the same packet having the sequence number 2. Therefore they record the following information:

M1(t_1): 1 -> OK; 2 -> Missing; 3 -> OK.

M2(t_1): 1 -> OK; 2 -> Missing; 3 -> OK.

At t=t_2, M1 and M2 receive a BNR. Thus each of them builds a BNAK to request packet 2. Once the BNAK is buffered, the two members record the following information:

M1(t_2): 1 -> OK; 2 -> Pending; 3 -> OK.

M2(t_2): 1 -> OK; 2 -> Pending; 3 -> OK.

Hence, M1 and M2 will not generate a new BNAK upon the reception of a new BNR. At t=t_3, M1 sends a BNAK but the AP misses the feedback (for example, due to a collision). Since this is not the last transmission attempt of BNAK, M1 does not change the status of packet 2. At t=t_4, M1 receives correctly packets 4 and 5 while M2 misses a new packet. Hence their respective records become as follows:

M1(t_4): 1 -> OK; 2 -> Pending; 3 -> OK; 4 -> OK; 5 -> OK.

M2(t_4): 1 -> OK; 2 -> Pending; 3 -> OK; 4 -> OK.; 5 -> Missing.

Therefore, when M1 receives a new BNR at t=t_5, it does not perform any action. Note that if there are only two statuses: *OK* and *Missing*, in this case M1 builds a new BNAK at t=t_5 to request packet number 2, even though a BNAK is already in the queue. Therefore, the status *Pending* is necessary in order to avoid useless transmissions. On the other hand, M2 deletes its pending BNAK which does not include the new missing packet. Then M2 sets the status of packet 2 to *Missing*, generates a new BNAK for packets 2 and 5, and sets the status of these two packets to *Pending*. Thus we obtain the following records.

M1(t_5): 1 -> OK; 2 -> Pending; 3 -> OK; 4 -> OK; 5 -> OK.

M2(t_5): 1 -> OK; 2 -> Pending; 3 -> OK; 4 -> OK.; 5 -> Pending.

At t=t$_6$, M2 concludes the success of the BNAK transmission. Thus it sets the status of packets 2 and 5 to *Missing*. The records of M1 remain unchanged. At t=t$_7$, M1 and M2 receive packet 2 successfully. Thus their records become as follows:

M1(t$_7$): 1 -> OK; 2 -> OK; 3 -> OK; 4 -> OK; 5 -> OK.

M2(t$_7$): 1 -> OK; 2 -> OK; 3 -> OK; 4 -> OK.; 5 -> Missing.

Therefore M1 deletes its buffered BNAK which perished due to the successful reception of the pending packet. At t=t$_8$, M2 receives packet 5 correctly and sets its status to *OK*. Thus at t=t$_9$, when M1 and M2 receive a BNR, they do not build any BNAK since they have received all the multicast packets correctly.

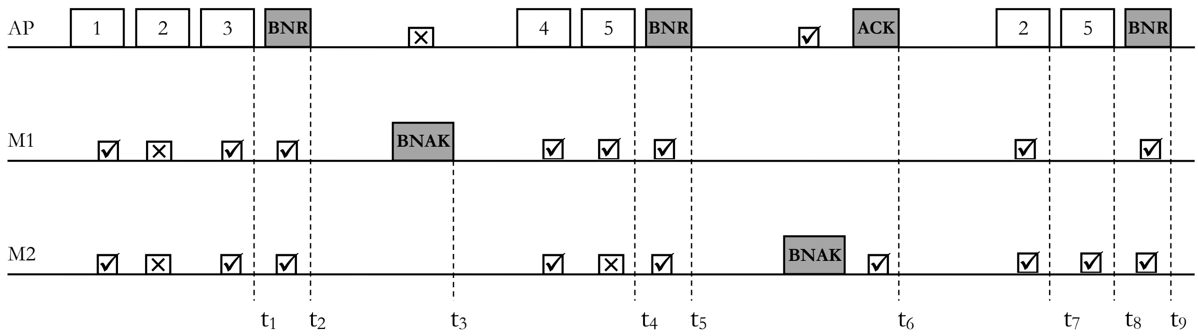


Figure 53. Operating mode of the BNAK protocol

5.3.4 Member Retirement and Reactivation

Although BNAK can be used to share any type of files, our protocol is mainly designed to deliver multimedia services reliably over wireless networks. In the remainder of this thesis, we consider only the case of real-time video streams. The data rate adaptation is another requirement to deal with the multi-rate capability of 802.11 WLANs. However, when an adaptation algorithm is used together with BNAK, the AP may select the lowest rate in order to establish a reliable communication with the farthest group member. This reduces the overall network throughput significantly and increases the congestion probability. We note that the application-level bit rate of multicast flows is not adjustable. Thus the AP may drop many packets during the congestion periods. These packets will not be retransmitted and will be lost definitely. When the network is saturated, portions of most video images are likely to be rejected. This leads either to a significant distortion of the video quality or to the total service interruption. Besides, the quality deterioration will be experienced by all the group members even those supporting high transmission rates. Therefore, the other alternative to the dynamic rate adaptation approach is to select a transmission rate statically. This solution ensures the use of a transmission rate which satisfies the throughput requirements of the video streaming application. Moreover, it prevents farther members from disturbing the multicast session. In this chapter we consider the static selection of the transmission rate. We devote the next chapter to the study of a rate adaptation scheme.

For a given multicast session, the AP notifies the group members about the lowest allowed PHY data rate. This notification is achieved using the BNAK Notification Message, whenever a new member joins the session. Several methods may be considered to configure the lowest rate per multicast address. The easiest one is to set one single rate to all the sessions. This is the default configuration of current AP where the lowest supported data rate is used. Another method is to offer a configuration tool (e.g. a local web interface) to the network administrator to set the lowest allowed rate per session. However, we recommend the updating of IGMP/MLD in order to include the bandwidth requirements of the multicast service. This information is then communicated to the MAC layer of the AP using internal messages, as previously described. Based on the required application bitrate, the AP selects a transmission rate which avoids the congestion and ensures the real-time streaming. We note that the way the transmission rate per multicast address is configured is beyond the scope of this work.

When the multicast packets are delivered using a transmission rate higher than the lowest one supported by the physical layer, in this case a member may miss all the transmitted packets if it is located out of the coverage area of the used rate but within the range of the AP. However, this member remains able to detect these losses. This is because the BNR is sent at the lowest PHY rate, and is received correctly regardless of the location of the associated station. Thus, it is necessary to prevent this receiver to send BNAKs in order not to disturb the streaming session. We highlight that it is useless to retransmit the missing packets because the member is already beyond the coverage area of the multicast session. Therefore, a receiver should retire temporarily till it comes back to the streaming area. We note that the retirement and the reactivation decisions are achieved internally by the member and without the need for any request or packet exchange with the AP.

5.3.4.1 Member Retirement

A member should retire if the SNR corresponds to a loss rate exceeding *PER Limit* at *Lowest Rate*. These two values are communicated to the members using the BNAK Membership Notification packet each time a new receiver joins the session. We note that a member may join the group while it is located out of the coverage area of the multicast service. In this case this member retires immediately upon the reception of the membership notification. Following the reception of a BNR, a retired member should set all missing packets as received correctly. Thus, it does not request them when reactivating.

5.3.4.2 Member Reactivation

When a member retires, it should wait till its connection link improves before reactivating. This improvement is based on the SNR increase. The reception signal strength is time-averaged based on recent packets received correctly from the AP, and particularly following the successful reception of BNR, multicast packets and beacons. The SNR is then mapped to bit error rate. Since the PER depends on both the bit error rate and the packet length, we measure the packet loss rate on the basis of 1538 byte-length packets. This size corresponds to the maximum size of Ethernet frames in addition to the MAC header and is the typical size of packets belonging to a video stream. We note that SNR is easily mapped to PER

[126-131]. However, this mapping may vary slightly from one chipset to another. This is because some high quality devices have enhanced sensitivity compared to other receivers. Therefore we recommend the implementation of a vendor-specific mapping function. We highlight that the manufacturers usually provide data sheets of their products including the bit error rate as a function of the SNR (e.g. Fig 14 and 15 of [118]). These documents can also be used to define an accurate mapping function. Another alternative is to use a self-learning algorithm at the receiver [131] to find the PER based on the SNR.

We define *PER Low* as the indicator of the eligibility of a retired member to reactivate. This value is lower than *PER Limit*. A member reactivates when the PER is lower than *PER Low*. We use different PER values to retire and to reactivate in order to avoid frequent retirement and reactivation when the receiver is at the edge of the multicast service area. To determine the relationship between *PER Limit* and *PER Low*, we illustrate the PER at different distances using different data rates in Fig. 54. These results are obtained using NS-3 according to the simulator configuration of Table 8. We observe that these curves are almost linear. Hence a ratio of 100 (i.e. *PER Low* = *PER Limit*/100) implies a reactivation sub-area of about 90% of the entire multicast area, regardless of the transmission rate and *PER Limit*. Unlike *PER Limit*, the value of *PER Low* is not defined by the AP and is configured by the receiver itself. In the remainder of this paper, we measure the PER using the Nist-Error-Rate model of NS-3.

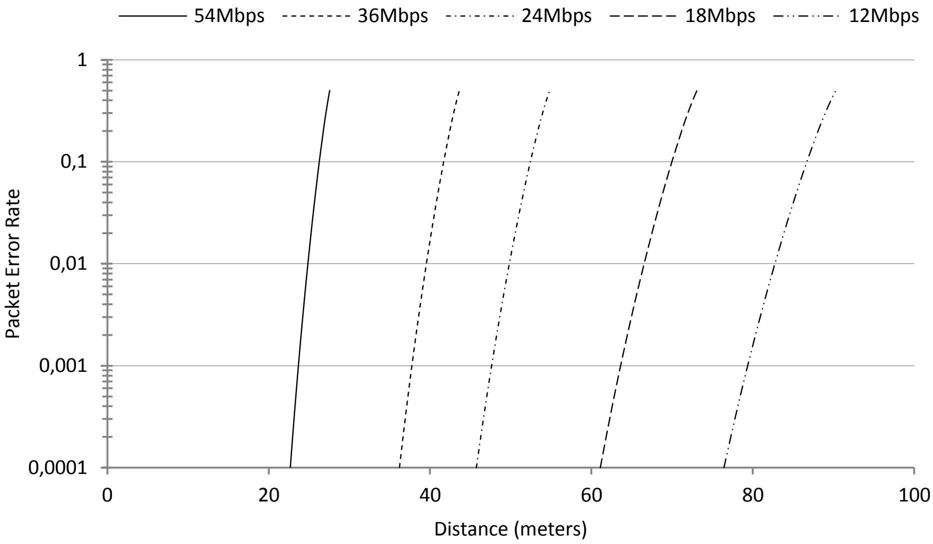
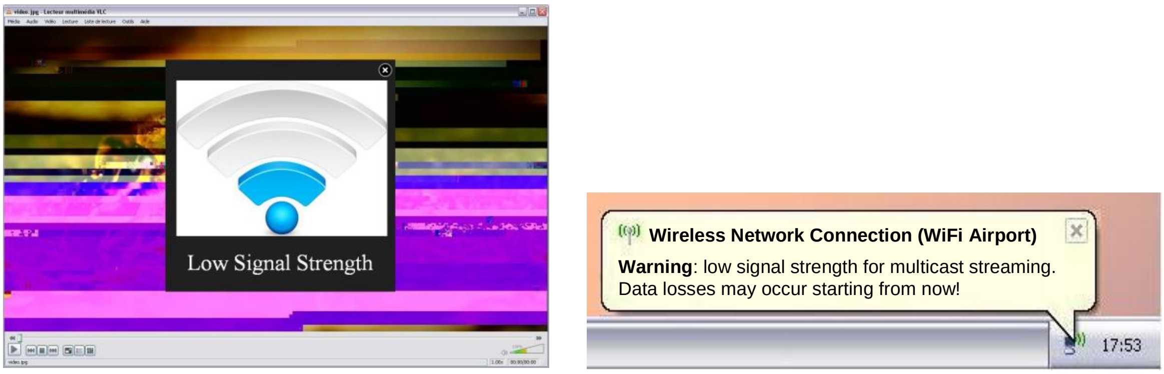


Figure 54. Packet Error Rate as a function of distance for 1538 byte-length packets; use of the Nist-Error-Rate model

During the retirement period, the receiver remains member of the group but stops sending BNAKs. This is because the loss rate exceeds the allowed limit. However, the viewer may ignore the reason of the video quality deterioration or the total streaming interruption. Therefore we recommend that the MAC layer sends a notification to the video player or to the operating system in order to report a temporal disruption due to weak signal strength. An alert message is then displayed at the front of the user's screen. Examples of retirement notifications are illustrated in Fig. 55. This motivates the client to move toward the AP, and enables a quick reactivation of the MAC layer.



Low Signal Strength

Wireless Network Connection (WiFi Airport)

Warning: low signal strength for multicast streaming.
Data losses may occur starting from now!

a) Alert message from the application

b) Alert message from the operating system

Figure 55. High level notification about the MAC layer retirement

5.4 Model Description

In this section we define an analytical model to evaluate the efficiency, i.e. throughput, and the scalability of BNAK. We consider multicast UDP/IP packets with the maximum transmission unit (i.e. 1500 octets). Thus the MAC packet length is 1538 Bytes. We consider that BNRs are always transmitted successfully. The key approximation of our model is that BNAKs do not collide and are always transmitted correctly to the AP. This is a valid approximation when the PER is limited since BNAKs are supposed to be non-frequent and the channel contention is very limited. Therefore our model provides a high accuracy when the PER is limited.

Let G be the multicast group size. Each member in the group experiences a PER of p_i for i=1..G. We consider that losses are not correlated between different receivers. We fix the transmission limit of a packet to 100. We choose this value because the retransmission of a packet is subject to lifetime limit. Thus we fix a transmission limit by excess. We note that the probability to reach high transmission stages is negligible when the PER is limited. Let N be the block size and Nr(k) be the number of packets transmitted for the kth time within a block. Nr(1) is the number of packets transmitted for the first time. Every block is composed of $\sum_{k=1}^{100} Nr(k)$ packets. Nr(k), k=1..100, depends on the PER of the network.

Table 13 presents the used variables and their values at different transmission data rates. We consider that BNR, BNAK and ACK are always transmitted at 6 Mbps. On the other hand, the CTS-to-Self is always delivered at the highest data rate of 54Mbps in order to have the shortest length. Thus it allows the efficient detection of simultaneous transmissions.

We define X as the number of transmission attempts. The probability for a given member M_i, i=1..G, to receive correctly a packet in any of the k first transmissions is given in Equation (1):

$$P^i(X \leq k) = 1 - p_i^k \qquad (1)$$

Table 13. Parameters description and value

Variables	Values
Network	IEEE 802.11a
T_{PPDU_Data}: PHY packet duration, 1538 B.	252 µs (at 54 Mbps)
T_{PPDU_BNR}: PHY BNR duration, 20 Bytes	52 µs (at 6 Mbps)
T_{PPDU_BNAK}: PHY BNAK duration, 27 B.	60 µs (at 6 Mbps)
T_{PPDU_ACK}: PHY ACK duration, 14 B.	44 µs (at 6 Mbps)
PROTECTION_DURATION, CTS	40 µs (at 54Mb + SIFS)
PROTECTION_DURATION, BS	16 µs (SIFS)
SlotTime	9 µs
SIFS	16 µs
DIFS (SIFS + 2 SlotTime)	34 µs
CWmin: Contention Window min	15

Then we derive the probability to serve all the *G* receivers in any of the *k* first transmissions in Equation (2):

$$P^G(X \le k) = \prod_{i=1}^{G}(1 - p_i^k) \qquad (2)$$

We obtain Nr(1) and Nr(k), k=2..100, in Equations (3) and (4) respectively.

$$Nr(1) = N - \sum_{k=2}^{100} Nr(k) \qquad (3)$$

$$Nr(k) = N(1).(1 - P^G(X \le k-1)), k = 2..100 \qquad (4)$$

We resolve Equations (3) and (4) and we obtain Nr(k), for k=1..100, in Equation (5). It is obvious that the probability to receive a packet correctly in *X = 0* attempt is nil, hence *P(X=0) =* P^G*(X=0) = 0.*

$$Nr(k) = \frac{N.\left(1-P^G(X \le k-1)\right)}{\sum_{k0=1}^{100}\left(1-P^G(X \le k0-1)\right)}, k = 1..100 \qquad (5)$$

In Equation (6) we derive the probability to deliver correctly a block to a given member M_i, i=1..G. This equation allows us to compute the probability of a BNAK generation.

$$P^i(N) = \prod_{k=1}^{100}(1 - p_i^k)^{Nr(k)} \qquad (6)$$

We compute the average deferral time as follows. Suppose nodes n1, n2 and n3 contend for the channel. Using our no-collision approximation, the 3 nodes generate different Backoff Times (BT). For example: 2 for n1, 5 for n2 and 7 for n3. Thus n1 transmits first, after DIFS+2×SlotTimes at the end of the current transmission. Then n2 transmits, DIFS+3×SlotTimes after the transmission end of n1. Finally n3 transmits, DIFS+2×SlotTimes after the transmission end of n2. Thus the total deferral time in this example is 3×DIFS + 7×SlotTimes, and the maximum deferral time which may occur is 3×DIFS + CWmin×SlotTime. As we suppose that BNAKs are not frequent, we consider that the average Backoff Time is BT=CWmin/2. Therefore, the average deferral time for G_0+1 contending nodes, is: DIFS + CWmin/2 × SlotTime + G_0 × DIFS. In Equation (7) we obtain the average packet transmission time using the BNAK policy.

$$T_{BNAK}(N,G) = \left(DIFS + \frac{CWmin}{2} \times SlotTime + PROTECTION\_DURATION + (T_{PPDU\_Data} + SIFS) \times N + T_{PPDU\_BNR} + \left[\sum_{i=1}^{G} (1 - P^i(N))\right] \times (DIFS + T_{PPDU\_BNAK} + SIFS + T_{PPDU\_ACK}) \right) / Nr(1)$$

(7)

Equation (8) illustrates the packet transmission rate of BNAK.

$$Throughput_{BNAK} = 1/T_{BNAK}(N,G) \qquad (8)$$

5.5 Simulation Results

We use NS-3 to validate our analytical model and to evaluate our protocol. We build an IEEE 802.11a infrastructure network and we consider the simulator configuration of Table 8. In the remainder of this chapter we consider multicast packets of 1538 Bytes (including the MAC header) transmitted at the highest rate of 54Mbps. Besides, the CTS-to-Self is continuously sent at 54Mbps while the other control packets (i.e. BNR, BNAK, ACK, BAR, BACK) are always delivered at the lowest rate of 6 Mbps.

5.5.1 Model Validation

To validate our analytical model we consider that all the group members have the same PER. We compare the analytical and simulation results of BNAK in Fig. 56. We consider groups of 1, 10 and 100 members. We notice that there is a good accuracy between the simulator and the mathematical model for limited values of PER. As expected, we observe a small gap between the analytical and the simulation results when both the loss rate and the group size increase. Particularly we find that the analytical results exceed the simulation ones when the group size is 100 and the packet error rate varies between 0.1% and 3%. This gap is caused by the collisions between the BNAKs. However, the simulation throughput becomes higher when the packet error rate is between 20% and 50%. This is because a few BNAKs are enough to request the retransmission of all the missing packets. Therefore several feedbacks are canceled under the simulator. However, the analytical model does not consider these suppressions. This explains the reversed gap at high error rates.

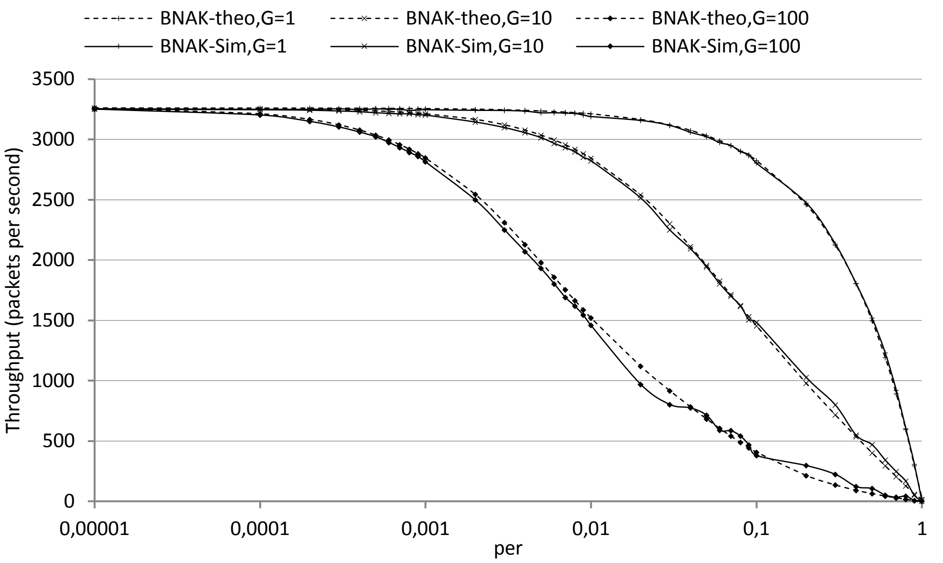


Figure 56. BNAK model validation: blocks of 5 packets and transmission rate of 54Mbps

Then we validate our model for different block sizes. We consider a multicast group of 10 members and two different PER values of 0.01% and 1%. We compare the analytical and the simulation throughput. Fig. 57 illustrates the obtained results. We observe that our model has a high accuracy for all the considered block sizes. Therefore it can be used to determine the throughput based on the block size.

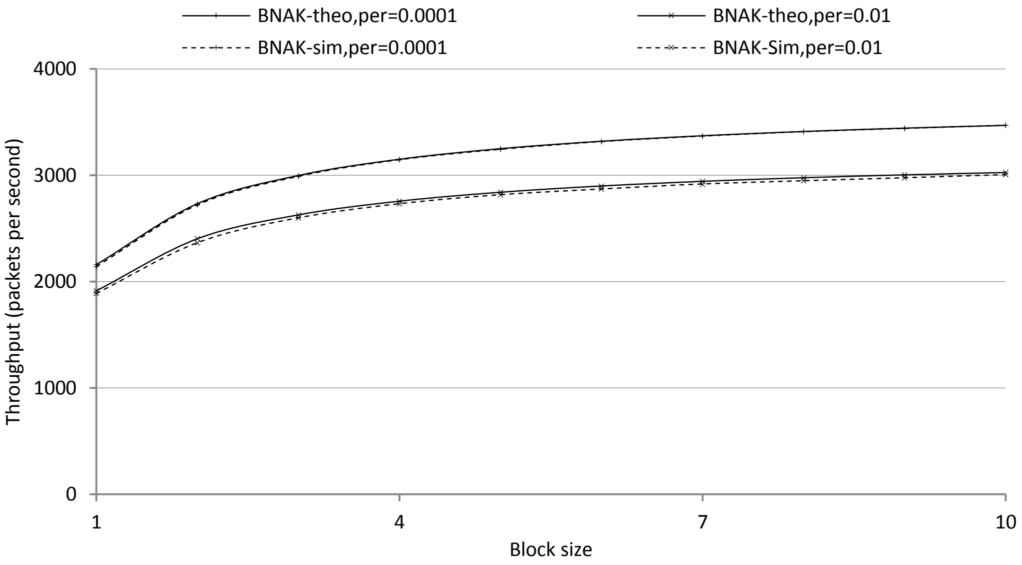


Figure 57. BNAK model validation: variable block size, G=10 and a transmission rate of 54 Mbps

5.5.2 Performance Evaluation

We evaluate the scalability of BNAK and we compare our protocol with GCR-BACK, GCR-UR2 (i.e. each packet is transmitted twice) and the legacy multicast procedure. We set all the group members at a distance of 10 meters from the AP and we transmit the flow at 54Mbps. We consider that no traffic other than the multicast stream is transmitted. Besides, we consider that the AP is in the saturation condition. We illustrate the obtained results in Fig. 58 for variable sizes of multicast groups. These results show that the scalability of BNAK is unlimited when the receivers are located at an appropriate distance from the sender. We observe that the throughput of GCR-BACK decreases significantly when the group size increases. Particularly when 100 members are in the group, we notice that GCR-BACK delivers only 268 pps while our protocol achieves more than 3250 pps. Besides, these results demonstrate that the redundant retransmissions limit the efficiency of the Unsolicited Retry policy significantly. Hence, the throughput of GCR-UR2 is less than 50% of that of BNAK. Moreover, we find that our protocol outperforms the legacy transmission procedure. This is because BNAK takes advantage of the high efficiency of the block transfer, while the conventional multicast delivers each packet following channel contention and waiting periods.

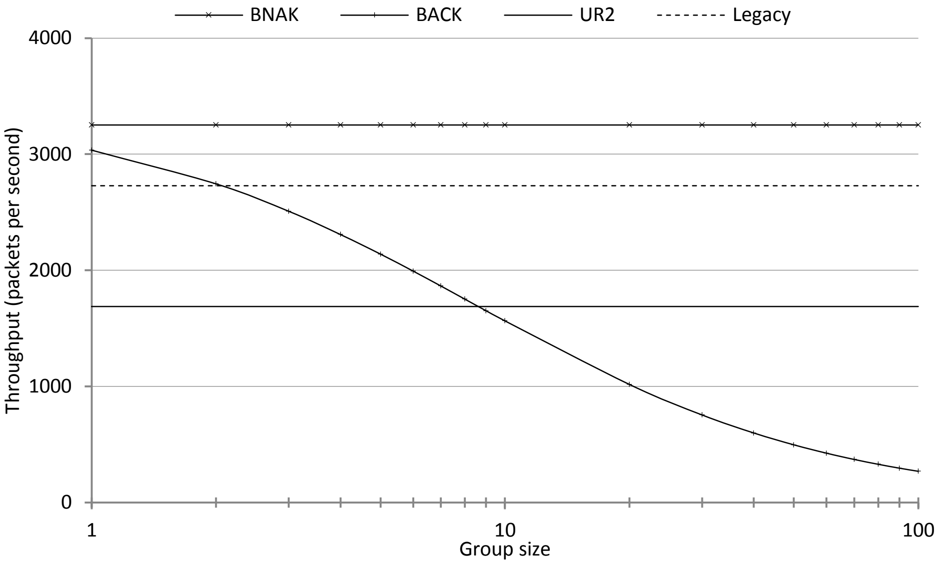


Figure 58. Throughput vs. group size: block size limit of 5 packets

We consider two group sizes of 10 and 100 members and we evaluate the throughput and the reliability of these protocols under a variable loss rate. We consider that all the members are located at the same distance from the AP in order to ensure the same PER for all the receivers. We consider the saturation condition in order to measure the highest throughput. Thus the transmission queue of the AP is never empty. We consider blocks of 5 packets.

In Fig. 59 and 60 we consider the case of an unshared network. Hence the AP is the only sender and the medium is entirely used by the multicast traffic. Therefore, the reliability of the legacy multicast is not reduced by the collisions. In Fig. 59(a) and 60(a) we consider a group of 10 members. We observe that BNAK outperforms 802.11aa significantly and provides more than twice the throughput of BACK when the loss rate is limited. Moreover BNAK outperforms the legacy multicast at distances below 25 meters. When the loss rate increases, we observe that the legacy multicast provides higher throughput on the expense of limited delivery ratio.

Fig. 59(b) and 60(b) illustrates the throughput and the reliability, respectively, for a group of 100 members. We observe that the throughput and the reliability of the legacy multicast do not depend on the group size. At the same time we notice that the throughput of BNAK is not impacted by the group size when the loss rate of the network is limited. Moreover we observe that BNAK delivers about 12 times the throughput of GCR-BACK at reasonable distances from the AP.

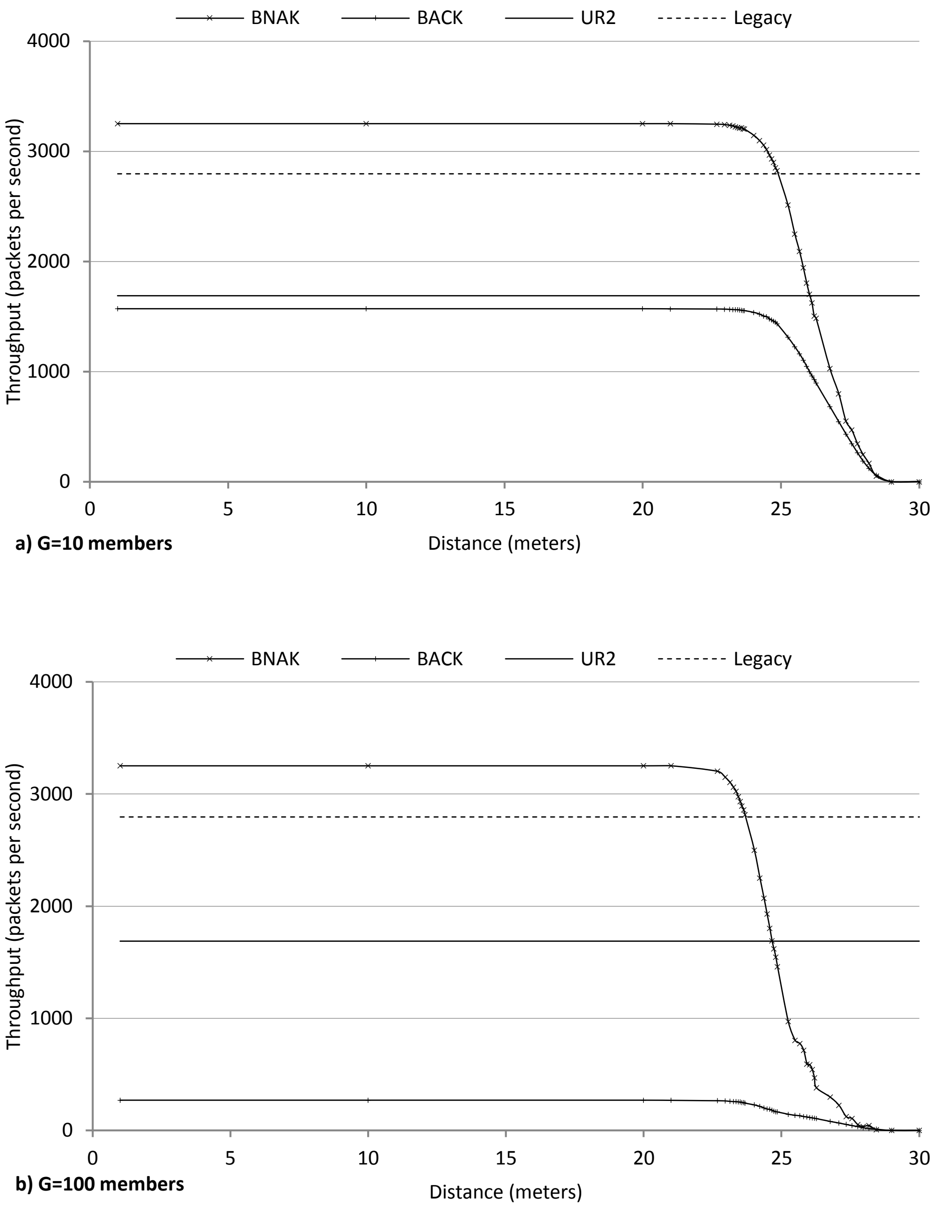


Figure 59. Throughput evaluation in an unshared network (only the multicast traffic is transmitted), using a block size of 5 packets and a transmission data rate of 54 Mbps

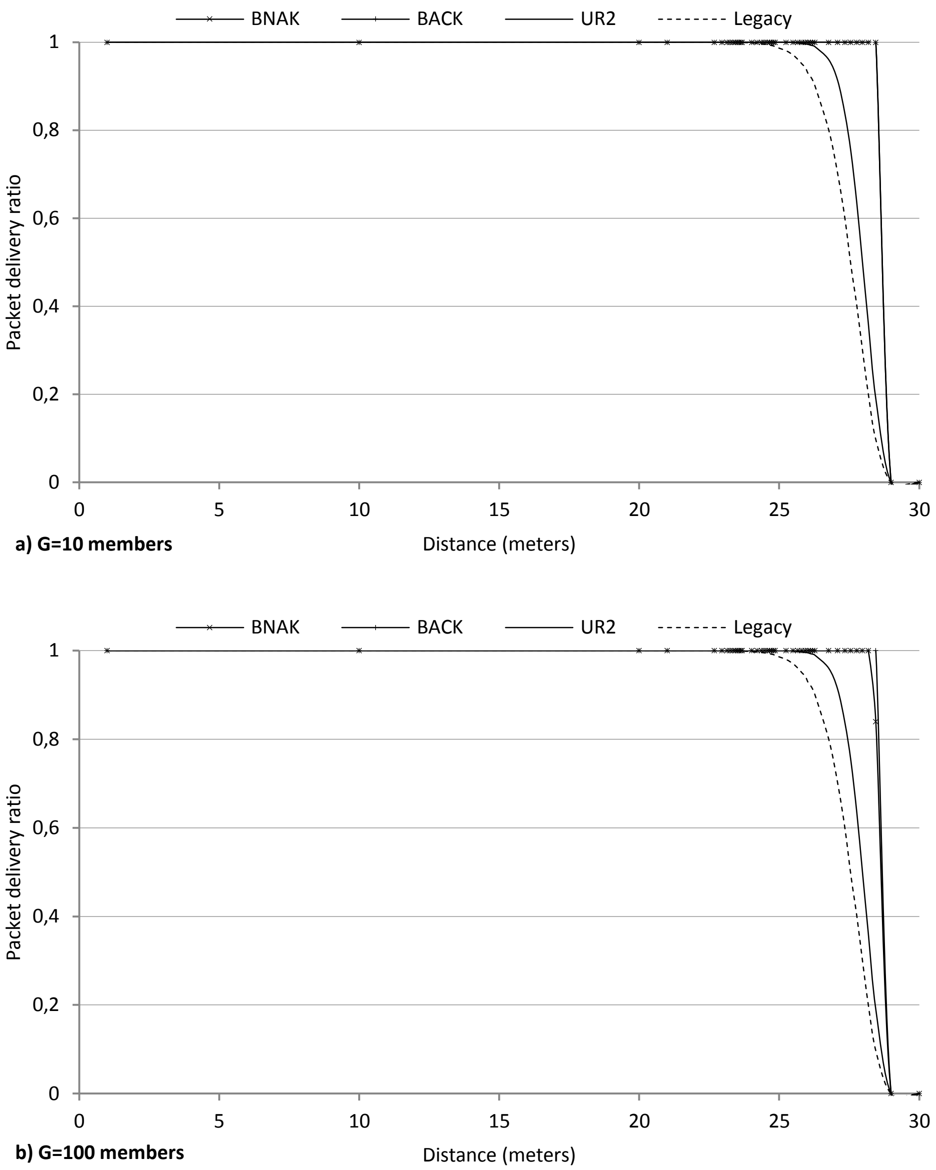


Figure 60. Reliability evaluation in an unshared network, using a block size of 5 packets and a transmission data rate of 54 Mbps

In Fig. 61 and 62 we consider a medium shared between the multicast traffic of the AP and a unicast flow generated by an associated station. The unicast traffic is transmitted at 54Mbps using the basic feedback policy (i.e. individual transmission and acknowledgement). The unicast sender is in the saturation condition and its transmission queue is never empty. This scenario may occur in a WLAN when a client uploads a large data file while a multicast session is running. We notice that the throughput of all the protocols decrease. This is expected since the channel is shared between the multicast and the unicast flows. Besides, the reliability of BNAK, GCR-BACK and GCR-UR is maintained. However, we observe that the reliability of the legacy multicast is impacted by the collisions and that the delivery ratio of the standard procedure is about 90% when the receivers are at reasonable distances from the sender.

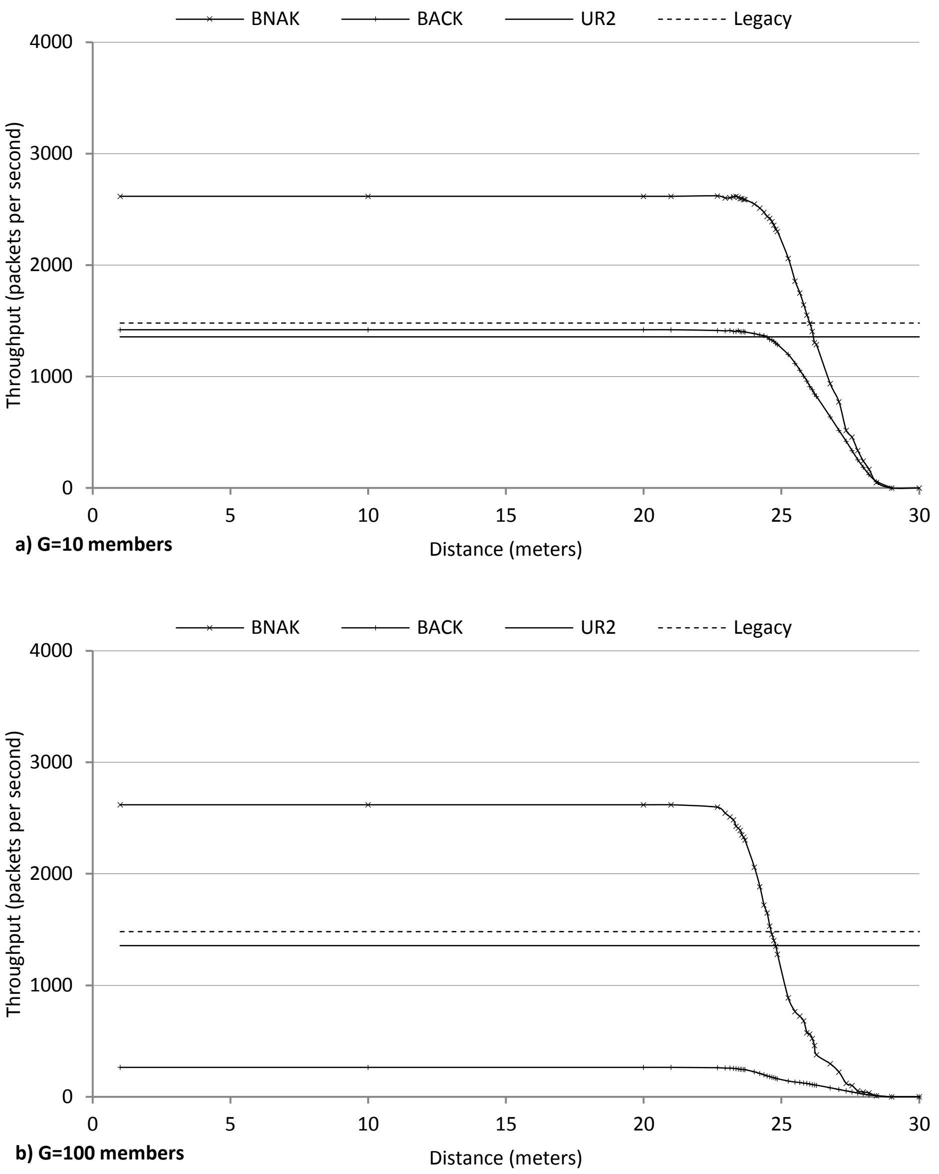


Figure 61. Throughput evaluation in the presence of contention between the multicast traffic and one unicast flow, using a block size of 5 packets and a transmission data rate of 54 Mbps

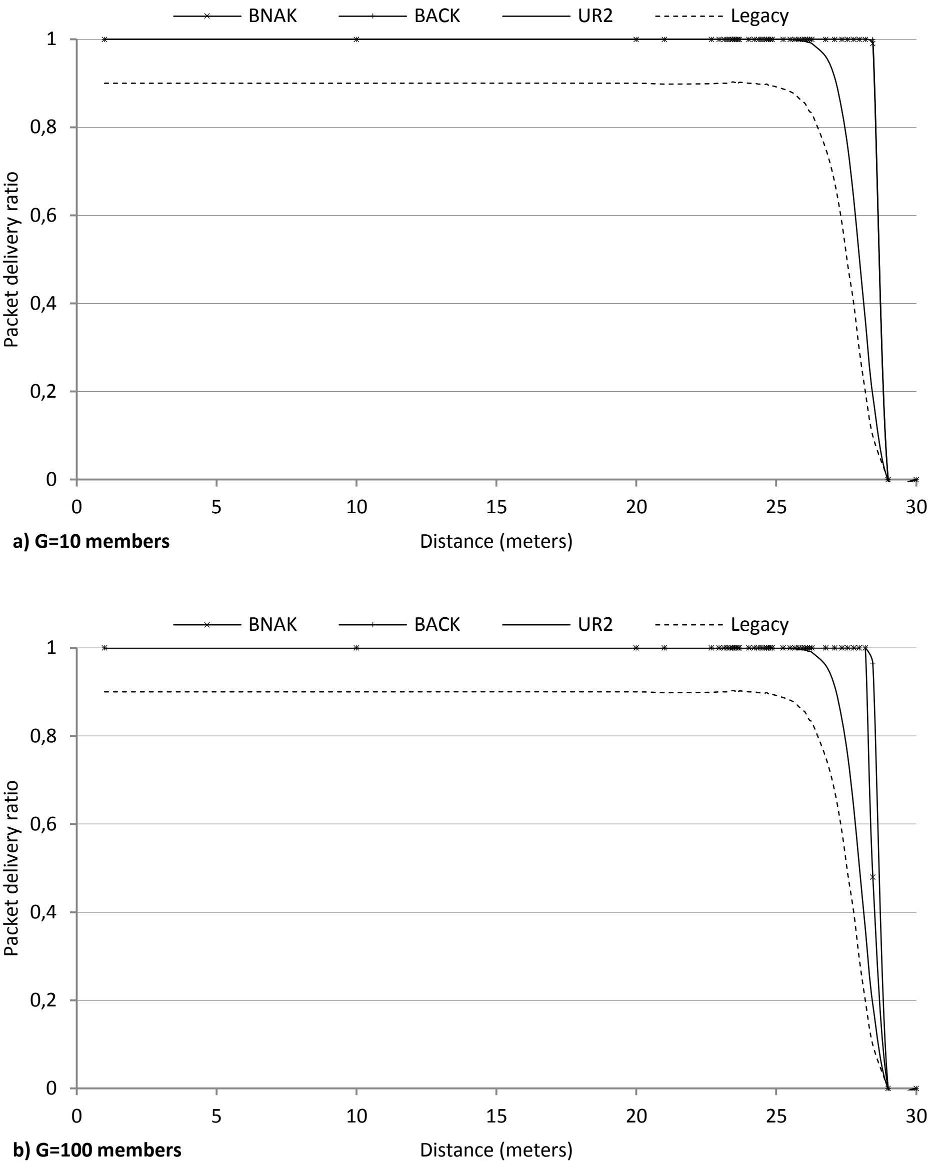


Figure 62. Reliability evaluation in the presence of contention, using a block size of 5 packets and a transmission data rate of 54 Mbps

We vary the block size and measure the throughput of BNAK and GCR-BACK. We consider groups of 10 and 100 members. We install the multicast receivers at the same distance of 10 meters from the AP in order to obtain the same loss rate. Fig. 63 depicts the obtained results. We observe that BNAK has a high efficiency even if it is used to deliver one single packet per transmission opportunity. Thus our protocol is also appropriate for low throughput streams such as voice and audio. On the other hand we observe that the throughput of 802.11aa for groups of 10 members is 472 pps when multicast packets are acknowledged individually. However, the worst performance of GCR-BACK is illustrated for a group of 100 receivers and a block of one packet. In this case, the highest achieved throughput is limited to 58 pps. This is less than 3% of the capability of our protocol. We conclude that the recent standard is not appropriate for large groups even for delivering low throughput flows.

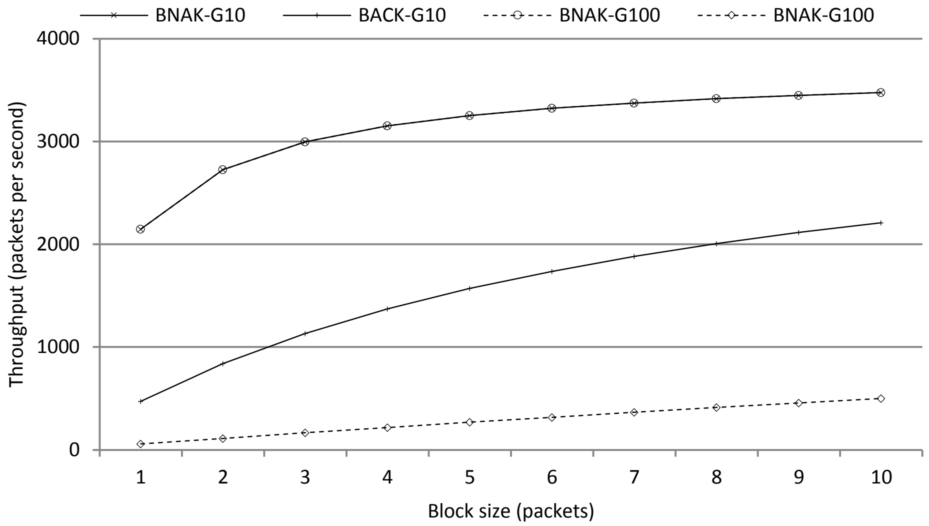


Figure 63. Throughput versus block size

We evaluate the impact of one moving receiver on the throughput of BNAK and GCR-BACK. Therefore, we vary the distance of one member from 1 to 40 meters, and we set the other receivers at a distance of 10 meters from the AP. We consider two different configurations of BNAK: 1) no member retirement (i.e. *PER Limit* = 100%) and 2) retirement for PER exceeding 5%. In the former case the receiver replies to BNR whenever it has missing packets and regardless of the packet error rate. Therefore the throughput of the entire group is impacted by the loss rate experienced by one single receiver and particularly when this receiver leaves the coverage area of the multicast service. In the latter configuration, the moving member retires when the SNR corresponds to a PER higher than 5%. We illustrate the obtained results for groups of 10 and 100 members in Fig. 64 and 65 respectively. When the moving member retires, the BNAK throughput is again maximized regardless of the group size. On the other hand, we observe that the throughput of GCR-BACK depends on the group size, regardless of the channel quality. Besides, this throughput is impacted by the loss rate of the moving station.

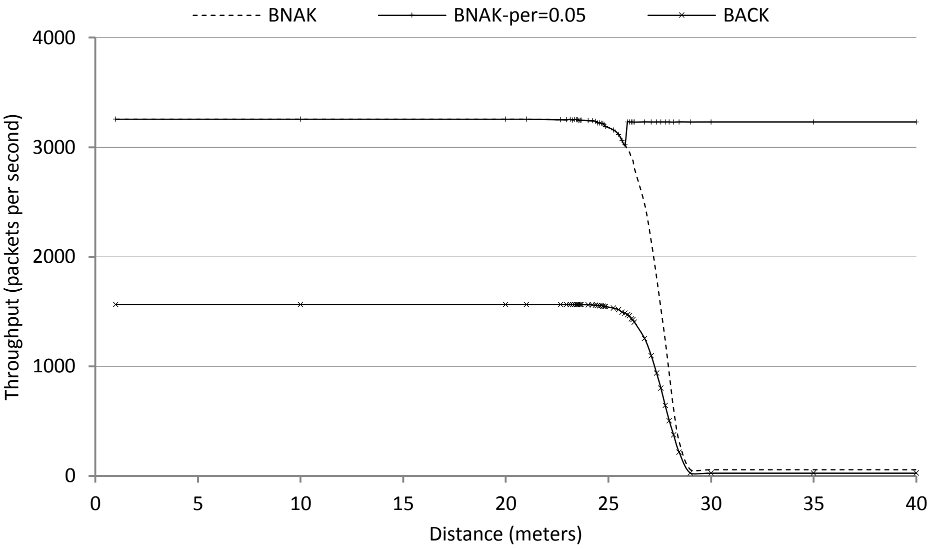


Figure 64. Impact of one moving member on the throughput of the entire group, G=10 members

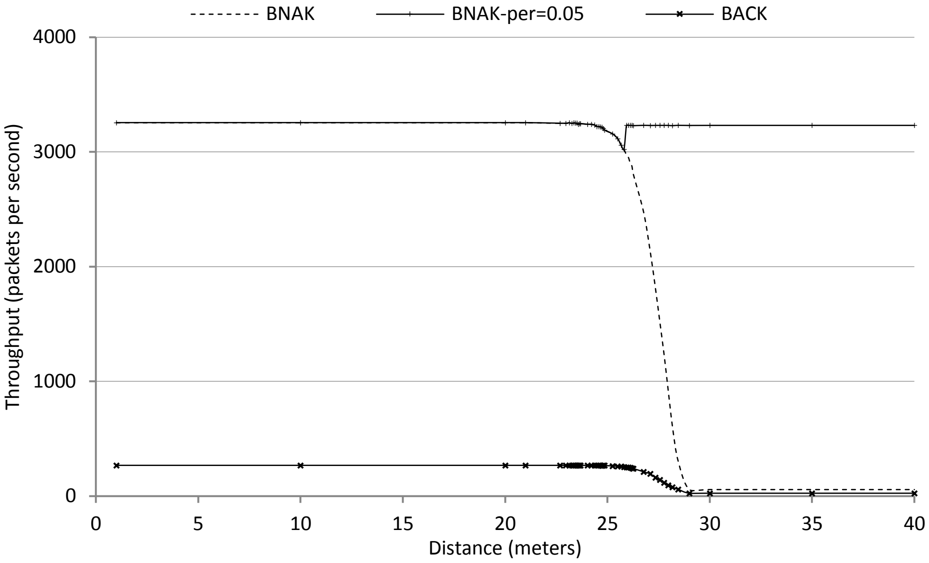


Figure 65. Impact of one moving member on the throughput of the entire group, G=100 members

We evaluate the delays as a function of the throughput. The multicast sender generates packets at equal intervals and at a constant rate. We increase this rate progressively. All the group members are located within a distance of 10 meters from the AP. We depict the obtained results for groups of 10 and 100 members in Fig. 66 and 67, respectively. As expected we observe that the incurred delays using BNAK do not depend on the group size since the experienced packet error rate is very low. Moreover, we notice that these delays increase when we exceed the capacity of our protocol which is 3251 pps. When the AP is in the saturation condition, the delivery latency is also impacted by the buffering delays and is bounded by the packet lifetime limit. We observe that the maximum delay of BNAK in the saturation condition is limited to 6.7ms. This value depends on the queue size and the average service time. In our configuration of Table 8 we consider a maximum size of 20 packets. Thus, packets are dropped if they arrive while the queue is full. However, when a new packet is buffered, it should wait for the transmission of the first 19 packets.

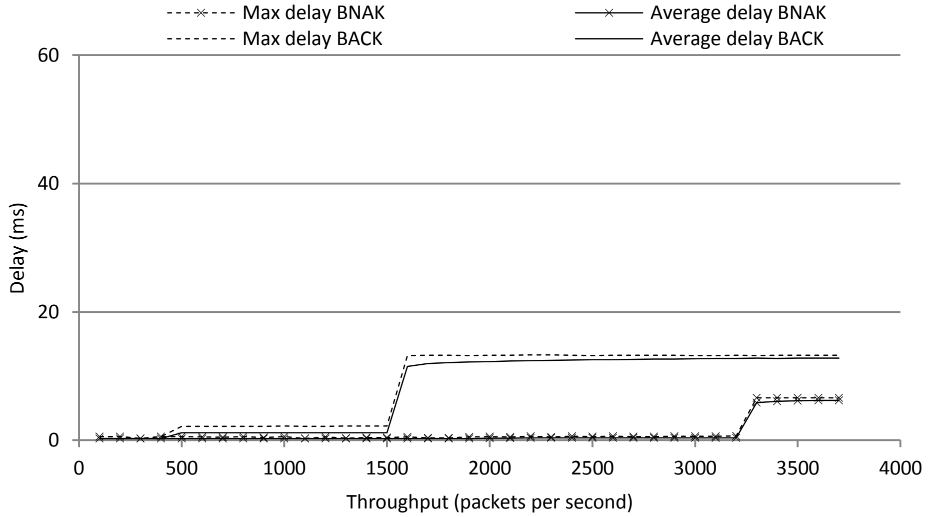


Figure 66. Buffering and transmission delays vs. throughput, G=10 members

On the other hand, the delays of 802.11aa BACK depend on the group size. According to Fig. 66, we notice that the delays of GCR-BACK increase slightly between 500pps and 1500pps. This is because a packet may arrive while BAR/BACK exchanges are in progress. In this case the new packet remains in the queue till the end of the feedback recovery phase before it is transmitted. Then, the delays increase again in the saturation condition. These delays are higher than those of our protocol because the average service time of GCR-BACK exceeds that of BNAK.

Fig. 67 shows that the standard protocol incurs important delays even before the saturation condition. This is because the feedback recovery phase becomes long for 100 members. Starting from 300pps, the maximum delays of GCR-BACK are close to the lifetime limit. This is because the average service time of this protocol increases significantly. However, we notice a slight decrease of the average delays. We explain this as follows: when the throughput increases, more packets are rejected due to the lifetime limit. Many of them are dropped while BARs/BACKs are being exchanged. Therefore, the AP cancels several recovery phases since the multicast packets are not available any more. This reduces the average transmission delays slightly.

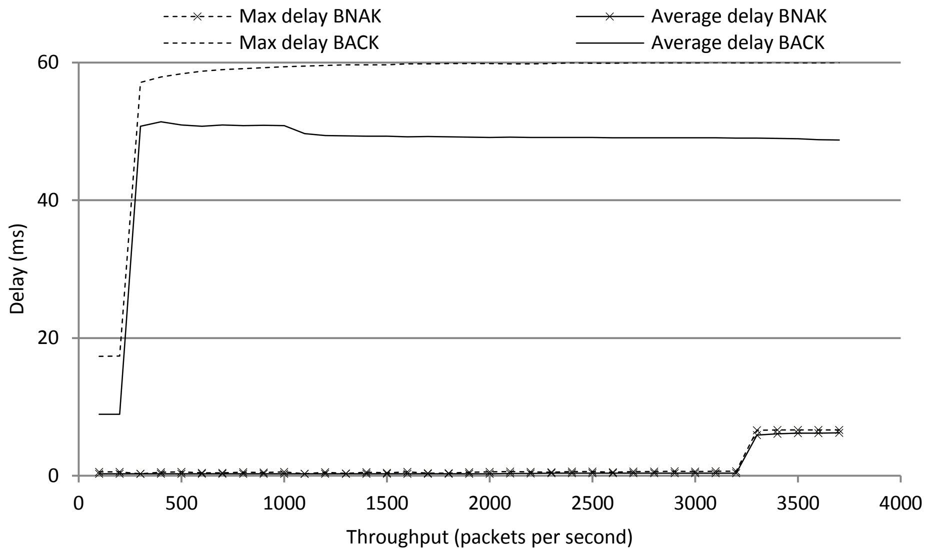


Figure 67. Buffering and transmission delays vs. throughput, G=100 members

Furthermore we evaluate the delays as a function of the distance. We set all the members at the same distance from the AP. This scenario allows the illustration of the loss rate impact on the protocol latency. We consider a multicast traffic with a very low throughput of only 1 packet per second. Thus we avoid any delays related to the transmission queue. We consider groups of 10 and 100 members in Fig. 68 and 69, respectively. We observe that the incurred delays of BNAK are very low whenever the PER is limited, and then they increase reasonably. In Fig. 68, we observe that the delays of GCR-BACK are very limited when the loss rate is almost nil. This is because all the packets are delivered correctly at the first time and do not suffer from the long feedback step. But when the loss rate rises, missing packets have to wait the feedback recovery end before being retransmitted. The same curve behavior is obtained in Fig. 69. But we notice that delivery latency is very important for GCR-BACK due to the long feedback recovery step. On the other hand, our protocol has a reduced latency since a BNAK packet is generated immediately following the loss detection.

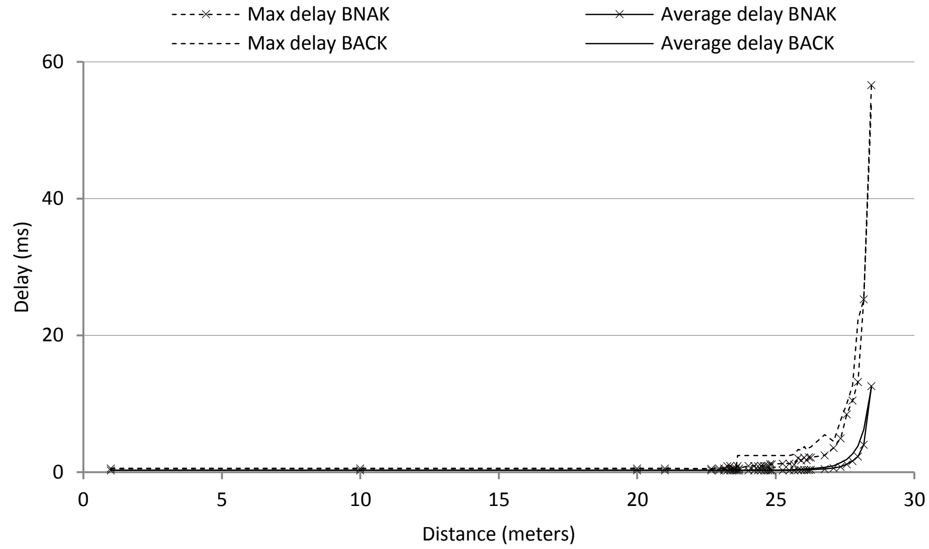


Figure 68. Buffering and transmission delays vs. distance, G=10 members

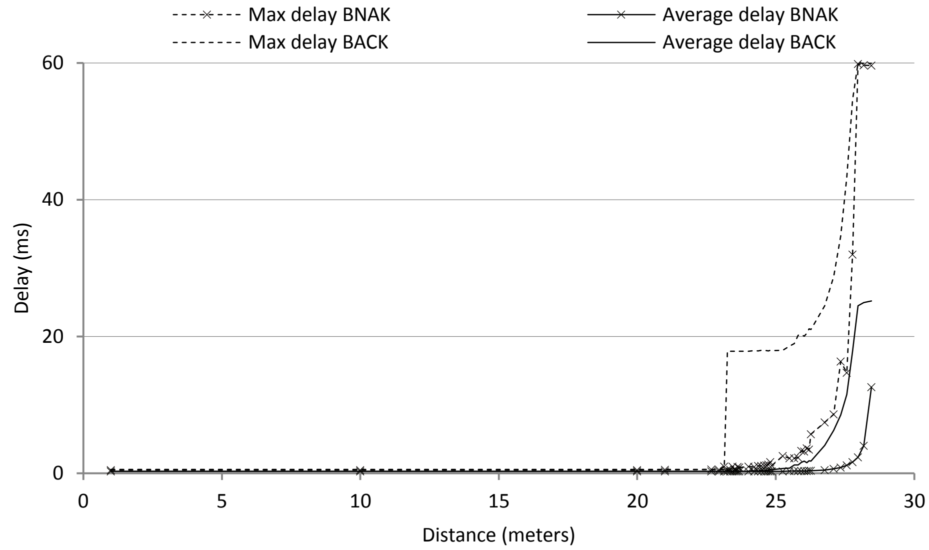


Figure 69. Buffering and transmission delays vs. distance, G=100 members

5.6 Conclusion

In this chapter we introduce a new multicast protocol for 802.11 networks. Besides, we define a membership detection function for the MAC layer. This function runs at the AP and does not need any updates at the receivers. In addition to the principal transmission mode of BNAK, we present the immediate retry policy. Then we introduce the packet format and the operating mode of our protocol.

Furthermore, we tackle the retirement and the reactivation decisions of a moving member based on the reception SNR. We illustrate some notification messages in order to motivate the viewer to move toward the AP. Moreover, we introduce an analytical model to measure the throughput of BNAK under various configurations and particularly for variable values of group size, block size and packet error rate. We validate this model using simulation results. Thus we show that our model is very accurate in measuring the expected throughput. Besides, the simulation results show that BNAK is perfectly reliable, and outperforms 802.11aa significantly. Hence, the throughput of our protocol may exceed 10 times that of GCR-BACK.

We conclude that BNAK is a reliable and efficient multicast protocol. Besides, it incurs very limited transmission delays. Furthermore, we demonstrate that the scalability of our protocol is almost unlimited when the loss rate is very low. Therefore, our protocol is appropriate for large multicast groups. We note that our protocol is easy to implement within current devices. It requires software updates only and does not need any hardware modifications. Besides, it is appropriate for individual and block transfer, and supports the packet aggregation feature of 802.11n perfectly.

We note that BNAK is designed to recover from a limited packet error rate of multicast flows. Although almost all multicast services are loss-tolerant, the impact of a PER of 1% on a video is disastrous. This is because an image is composed of several packets, and missing one single packet leads to the rejection of the entire image. Moreover images are inter-dependent. Hence, for a PER of 1%, each missing packet degrades the video quality for a while, till the loss of the next packet which takes over, and so on. Even though the packet error rate is nil, a feedback policy is a must. This is because the transmission rate is reliable whenever the receivers are located at the appropriate distance. When a group member moves away from the sender, the loss rate may increase significantly. A feedback policy allows the AP to detect the transmission failures and to update the data rate in order to maintain a reliable communication link. The rate adaptation will be studied in the next chapter.

Chapter 6

6 BNAK Data Rate Adaptation

6.1 Introduction

The 802.11 standard defines many transmission rates with different ranges. This characteristic requires the selection of the most appropriate rate in order to maximize the network throughput. Several adaptation algorithms are defined for the unicast traffic. Most of them select the transmission rate of a packet according to the transmission status of the previous one. BNAK uses a new transmission procedure which is different from that of the unicast mode. This procedure recovers delayed feedbacks from the group members exhibiting packet losses. Therefore, the AP can not always deduce whether or not a packet is successfully delivered before starting the next transmission. Besides, there is no similarity between our protocol and any other multicast proposal. Therefore BNAK can not take advantage of any available rate selection scheme. This increases the need for defining a new rate adaptation algorithm which fits well with the specific characteristics of our protocol.

In this Chapter, we define a rate adaptation scheme for BNAK and we evaluate its performance using simulation results. This algorithm runs on the AP and requires the collaboration of the receivers in order to select the most appropriate data rate. For comparison purpose, we define a second scheme which does not require the members' assistance. We show that both schemes are appropriate for BNAK and that they maximize the delivery throughput of the principal and the immediate retry policies. However, we consider that the first scheme is the official one for our protocol.

The remainder of this chapter is organized as follows. In Section 6.2 we introduce the most relevant rate adaptation schemes for the unicast and the multicast transmissions. We present two new schemes for BNAK in Section 6.3. We introduce the scalable video streaming capability in Section 6.4. We dedicate Section 6.5 to show simulation results and to compare the two algorithms. Finally we conclude this chapter in Section 6.6.

6.2 Related Work

The IEEE 802.11 standard defines many transmission data rates. However the rate selection procedure is out of the scope of the standard. Therefore many adaptation algorithms are proposed to maximize the throughput of the wireless network [62-65,119-136]. Most of them are defined for the unicast transmissions, and can be classified into three principal categories: 1) probing based [119-125], 2) receiver driven [125-130] and 3) channel aware schemes [131-135]. The first category relies on the periodic test of a transmission rate higher than the currently used one. The higher rate is then selected if it achieves the required performance. Otherwise the sender switches back to the previous rate. This concept does not require any modification of the standard transmission procedure. Besides, the adaptation algorithm is only implemented by the sender and does not need any support from the receiver. The second category requires the collaboration of the receiver in order to select the most appropriate rate. Hence, when the destination notices an enhancement of the SNR, it notifies the source which selects a higher rate. Therefore, a receiver driven scheme requires additional extensions to the conventional transmission procedure in order to forward the explicit rate increase request. Besides, such a scheme should be supported by the two communicating parties. The last category relies on the principle of passively measuring the communication link quality. This is achieved by measuring the signal strength of packets coming from the potential destinations, and particularly the signal strength of the feedbacks. Based on this information, the sender deduces the SNR at the receiver and selects the most appropriate PHY data rate.

Automatic Rate Fallback (ARF) [119] is among the first designed rate adaptation schemes. It probes a higher transmission rate when any of the following two cases occurs: 1) a fixed number, typically 10, of transmissions succeed at the current rate, or 2) no failure occurs within a predefined period, say 100ms. If the probing transmission succeeds, the sender increases the transmission rate. Otherwise, it keeps the current one. On the other hand, ARF decreases the data rate following two successive transmission failures. The major advantage of this scheme is its implementation simplicity. But it has the following issues. First, this scheme is defined for the normal Ack policy and is not compliant with the block transfer. Second, the data rate increase process is relatively slow. For example, the sender should transmit about 70 packets before selecting the rate of 54Mbps starting from 6Mbps. Third, the algorithm can not differentiate between losses caused by the signal deterioration and those caused by collisions. Therefore, ARF is not optimized in the presence of a high collision rate.

Collision awareness is considered as an essential requirement for effective rate selection. Therefore, several proposals define collision-aware adaptation schemes. One of them is Robust Rate Adaptation Algorithm (RRAA) [120]. This scheme retransmits a lost packet using RTS/CTS before reducing the data rate. If the retransmission fails again, the sender concludes that the loss is caused by a weak SNR and selects a lower rate. To select a higher rate, RRAA probes more than one transmission at a higher rate. If the loss rate over the previous short-term time window exceeds a given threshold, the algorithm reduces the rate. Otherwise, a higher rate is selected. History Aware RRAA (HA-RRAA) [121] is an enhanced version of RRAA. This new algorithm aims at reducing the cost of the RTS/CTS exchange by integrating several statistics of the previous transmission status (i.e. success or failure) to decide whether it is more appropriate to use the RTS/CTS protection. The results show that HA-RRAA outperforms RRAA.

The Rate-Adaptive Framing (RAF) algorithm [126] controls the transmission rate and the frame size according to the preferences of the receiver. Therefore, the receiver continuously measures the link quality based on the signal strength and the interference history. Then it deduces the preferable rate based on the reception SNR, and determines the optimal packet size according to the observed set of idle intervals. These two values are inserted into each feedback and are sent back to the sender which applies them on the next transmission. This concept requires the modification of the ACK packet format. We note that these feedbacks are built by the chipset. Therefore, the implementation of RAF requires hardware updates. This reduces the attractiveness of RAF.

In SoftRate [127], the receiver calculates the bit error rate (BER) for each received packet, and reports this information to the sender in a feedback. This feedback is sent even when the data packet is received with errors. Following a successful packet reception, the receiver inserts the BER within the ACK. However, in case of a reception failure, a new control packet is used to report the BER and is sent at the ACK slot time. To correctly determine the identities of both the sender and the receiver of a faulty frame, SoftRate protects the MAC header using a separate CRC. The BER allows the sender to adjust the transmission rate. However, if no feedback is received, the sender automatically decreases the rate. Therefore the feedbacks are always sent at the lowest rate in order not to be lost. We notice that SoftRate requires fundamental modifications to the standard. These requirements are serious obstacles to the deployment of this proposal in real networks. Besides, SoftRate is vulnerable to the collisions. In case of a collision, the MAC header is likely to be lost, too. This prevents the feedback transmission and causes the sender to select a lower rate for the next transmission.

CHARM [131] is a channel-aware adaptation scheme. It does not require any information from the receiver other than the conventional ACK. The RSSI of this packet allows the sender to estimate the channel quality and to predict the SNR at the receiver. The predicted SNR is compared with the recorded SNR thresholds and is used to select an optimal rate. Due to the link asymmetry in wireless networks, the sender adjusts the SNR thresholds slowly based on the success and the failure of past transmissions. This allows CHARM to perform the rate adaptation process without modifying the standard transmission procedure. The authors show that their proposal outperforms probe-based schemes.

The rate adaptation for the multicast transmissions does not gain enough popularity for two major reasons: 1) the legacy multicast is unreliable and motivates the definition of a reliable transmission procedure instead of a rate adaptation scheme, and 2) GCR-UR and GCR-BACK are still new practices. Therefore, few adaptation schemes are proposed, and most of them are defined for non-standard multicast protocols. The principal way to track the quality of the downlink to the multicast members has recently been defined by 802.11v. It allows the receiver to send a notification to the AP, periodically, in order to report the reception statistics and the highest observed data rate within measurement periods. This feedback is useful for the rate selection. But the amendment does not define any particular rate adaptation algorithm.

SNR-based Auto Rate for Multicast (SARM) [136] is defined for the legacy multicast protocol. In the initialization phase, the multicast members measure the SNR of the Beacon frame and report this information to the AP after channel contention. After this phase, the AP broadcasts the lowest SNR and the MAC address of the receiver having reported this SNR, within the following Beacons. Hence, only the selected receiver and those having lower signal strength are allowed to report their measurements. The lowest reported SNR allows the AP to send the multicast stream at the appropriate rate. This solution has good performance and high scalability, but is not optimized for BNAK. This is because the reports are sent at fixed periods which may be very long. Thus, in case of signal deterioration the receiver should wait for the next period to send the new measurements. Besides, the feedbacks of BNAK are enough and allow the rate adaptation without any dependency on the Beacons.

6.3 Rate Adaptation for BNAK

The conception of BNAK has two major differences compared to the unicast mode. 1) The decision of the success or failure of a transmission can not be made immediately after the transmission of a packet. 2) The packets are delivered to a group of users. Therefore the data rate should be increased when all the group members are eligible to a higher rate, but should be decreased when at least one member is not able to receive correctly at the current rate.

6.3.1 Assisted Rate Adaptation (ARA)

We define the Assisted Rate Adaptation (ARA) scheme as the main algorithm for BNAK. The ARA relies on the collaboration of the members to indicate the most appropriate data rate when a rate decrease is required. Therefore the AP selects quickly the appropriate rate and avoids the progressive rate decrease following the reactivation of a retired member. In order to better explain the particularity of the reactivated member scenario, a typical network is illustrated in Fig. 70. In this figure, 5 stations are members of the multicast group. The lowest allowed rate is set to 12 Mbps. Therefore a member retires when it leaves the area of 12 Mbps. Thus member M5 is retired and the service is delivered reliably to members 1 to 4. Since these members are in the coverage area of 54 Mbps, the rate adaptation scheme progressively increases the transmission rate upon the retirement of M5 till selecting 54Mbps. But when M5 is back to the coverage area of the multicast service (i.e. in the area of 12 Mbps), the data rate should fall down directly to 12 Mbps. This is possible when the receiver is allowed to indicate its preferable rate. If this information is missing, the AP needs to probe all the rates between 54Mbps and 12Mbps to find the suitable one. This wastes the bandwidth and incurs additional delays.

ARA has two states: Delivery and Probing. During the delivery state, the AP sends multicast packets at one rate and reports this rate in all BNRs. Therefore the AP does not probe any higher rate. However the AP may decrease the transmission rate upon the request of a member. The delivery state has a fixed duration called Delivery Time Period (DTP) and a timer called Delivery Timer (DT). The timer is initiated when the sender enters the delivery state. If DT expires without receiving any rate decrease request, the AP switches to the probing state. Otherwise, DT is initiated again and a new delivery period should elapse before trying higher rates.

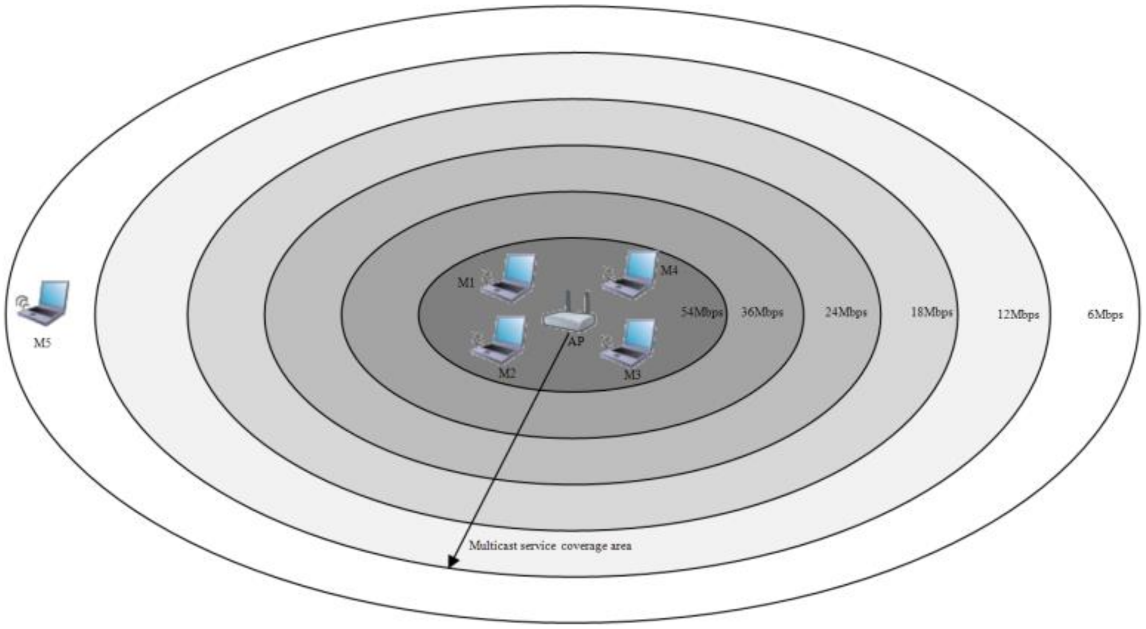


Figure 70. Data rates range and the multicast service area

During the probing state, the AP does not increase the data rate of the multicast packets but announces a higher rate in the BNRs. This announcement allows the members to know the data rate which will be used in advance. Thus a multicast receiver may request a rate decrease before the effective use of the higher rate. The probing state has a fixed duration called Probing Time Period (PTP) and a timer called Probing Timer (PT). The timer starts after the expiry of the delivery state and following the transmission of the first BNR announcing the higher rate. If no rate decrease request is received during PTP, the AP selects the advertised rate for the next multicast transmissions, and starts a new probing period. Thus PT is initiated again following the transmission of the first BNR. Otherwise, the adaptation scheme switches to the delivery state immediately following the reception of the BNAK and sends the multicast packets at the requested rate.

An example of the transmission procedure and the announced rates is illustrated in Fig. 71. For more clarity, we omit the collision protection mechanism. We consider that r_0 to r_5 are the set of available data rates, where r_0 and r_5 are the lowest and the highest rates respectively. Besides, we suppose that the lowest rate for the multicast packets is r_1. In this example we observe that the algorithm enters the probing state following the transmission of the first BNR. Therefore, the data is sent at r_3 while BNR indicates r_4. The first PTP elapses without receiving any rate decrease request. Thus the AP selects r_4 for the multicast transmissions and announces r_5 during the second PTP. Then a rate decrease request arrives and the algorithm enters the delivery state. During this state, the data is sent at r_4 which is the announced rate in BNR. Before the expiry of the first DTP, a member reactivates and requests r_1. This rate is selected and the AP enters a new delivery period.

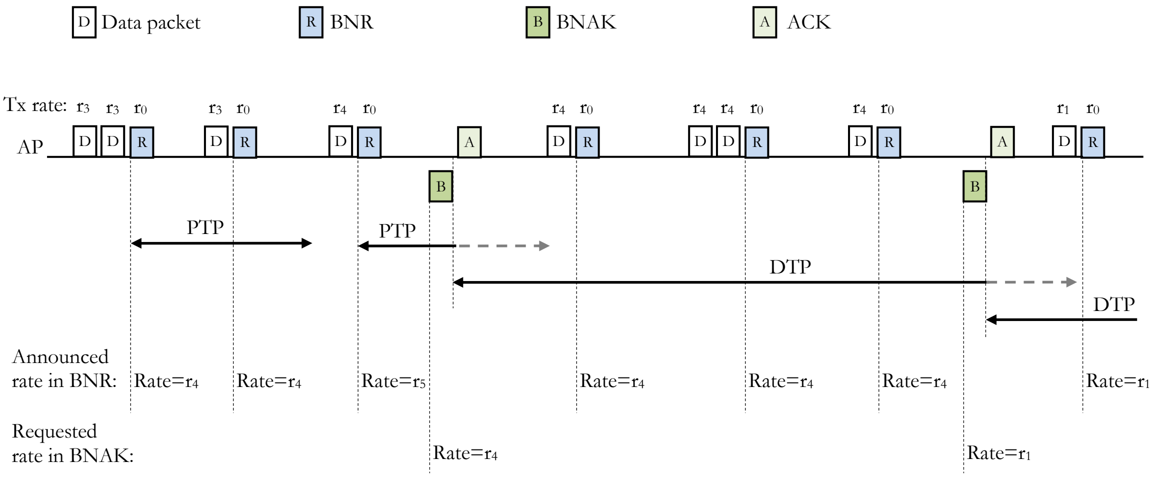

D Data packet
R BNR
B BNAK
A ACK
Tx rate: r_3 r_3 r_0 r_3 r_0 r_4 r_0 r_4 r_0 r_4 r_4 r_0 r_4 r_0 r_1 r_0
AP
D D R D R D R A D R D D R D R A D R
B
B
PTP
PTP
DTP
DTP
Announced rate in BNR: Rate=r_4 Rate=r_4 Rate=r_5 Rate=r_4 Rate=r_4 Rate=r_4 Rate=r_1
Requested rate in BNAK: Rate=r_4 Rate=r_1

Figure 71. Transmission procedure using BNAK-ARA

Fig. 72 depicts the two states of our adaptation scheme and the different conditions to switch from one state to another, or to initiate the timer. During the initiation phase, the AP is in the probing state and uses the lowest allowed rate for the multicast transmissions. Each time the PT expires, the sender remains in the same state and initiates the timer following a BNR. A probing state is followed by another probing state in order to ensure a quick rate increase process till finding the appropriate rate. When a rate decrease request arrives, the AP enters the delivery state and initiates DT. This timer is initiated each time a lower rate is selected. But if it expires, the AP enters the probing state.

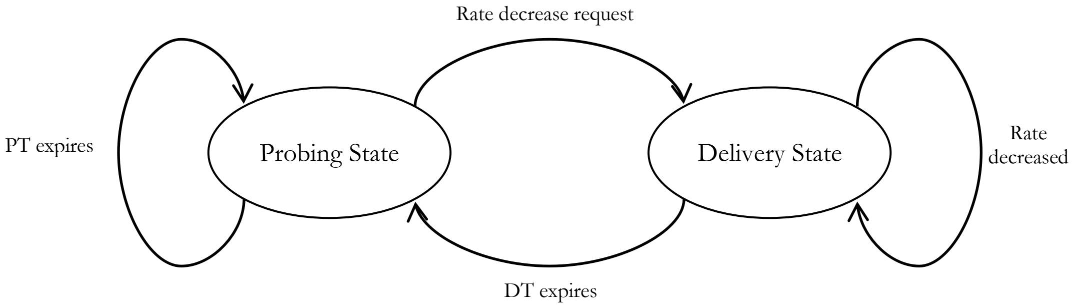


Figure 72. ARA state machine

A member decides whether to request a rate decrease based on the time-averaged SNR and the rate announced in the BNR. Therefore if the receiver concludes that the announced rate incurs a loss rate higher than *PER Limit*, this member requests a rate decrease. Similar to the Activation/retirement process, the member estimates the PER for packets having 1538 byte-length. The rate decrease request is achieved using a BNAK packet.

Since a BNAK is used to request a rate decrease, we define the *Rate* field following the *Bitmap*. This field is present when the *Rate Element Present* (*REP*) bit is set. The *REP* is one of the previously reserved bits. Besides, a BNAK may be sent only to request a rate decrease. In this case the *Sequence First Loss* field is not valid. To notify this, we define another bit among the reserved ones. It is called *No Loss* (*NL*) bit. The value of 0 indicates the presence of losses, while NL=1 means that the *Sequence First Loss* field is not valid. In this case the Bitmap length is nil. The updated segment of BNAK is illustrated in Fig. 73.

2Bytes				1B	0..255B	0/1B	
Rsvd 2 bits	REP bit	NL bit	Sequence first loss	Bitmap length	Bitmap	Rsvd 4 bits	Rate

Figure 73. BNAK format with rate decrease request

6.3.2 Probing-based Rate Adaptation (PRA)

For comparison purposes we define a second rate scheme called Probing-based Rate Adaptation (PRA). This algorithm does not need the receivers to request the rate. Instead, it measures the loss statistics to make the decisions. Besides, it uses the same states, periods and timers of the first adaptation scheme, i.e. probing and delivery states, PTP, DTP, PT and DT. However, to increase the rate, the AP sends one single packet at a higher rate periodically. If no BNAK is received to request the probing packet within PTP, then the rate is increased and another higher rate is tried. Otherwise, the AP enters the delivery state and DT is initiated. This timer is initiated each time a BNAK is received. But if DT expires without the reception of any feedback, the AP enters the probing state. Similarly to ARF [119], the rate is decreased following two successive transmission failures. Since the feedbacks arrive with variable delays, the AP maintains a list of the past transmissions. Once two successive transmissions are lost, the rate is decreased.

6.4 Scalable Video Streaming using BNAK

The conception of BNAK is defined to support scalable video streaming. This scalability intends to resolve two different issues in the wireless networks. This first issue is the bandwidth variation; even if the AP defines an appropriate rate limit for the multicast traffic, this rate may be unable to avoid the congestion when new flows share the medium with the multicast session. To prevent the packet drop in the saturation condition, BNAK allows the AP to increase the data rate of the enhancement layer while the rate of the base layer is adapted according to ARA. The second issue is the client preferences; in a multicast group, two different members may require different video resolutions due to the device heterogeneity. The base layer alone may satisfy the requirement of a customer having a smartphone with small screen size. Therefore, scalable video streaming [26,34] is an optimal solution to reduce the processing load of compact devices. BNAK may deliver up to 16 different layers. However, we present the case of a video of only two layers: base and enhancement. We consider that the preferable streaming solution is one base layer with full quality and full frame rate but with a reduced resolution. The enhancement layer increases the image dimension and offers the full video resolution. Therefore, the base layer offers the required quality for small terminals and allows large screen receivers to zoom the images during the bandwidth fluctuation in order to keep a real-time reception of a valid video content.

To differentiate the layers of the same multicast stream, the AP delivers the packets using different User Priorities (UP). It is worth noting that the current mapping of UP to Access Categories (AC) allows two different UP to be classified into one AC. We take advantage of this mapping to distinguish the layers. Furthermore, the AP uses one counter per multicast stream and per UP to generate the sequence numbers. However, one single SID is attributed to the different layers of the same session. Both BNR and BNAK process the two layers differently. The relevant segments of BNR and BNAK are illustrated in Fig. 74. The number of layers is indicated in *Number Sub-Session* field: 0 for one session, and 1 corresponds to one base layer and one enhancement layer. Besides, only the base layer is concerned by *Lowest Rate*. Therefore the member is eligible to this layer whenever the PER at *Lowest Rate* is lower than *PER Limit*. The enhancement layer, however, is subject to the rate at which this layer is transmitted. This rate is indicated in BNR and allows the members to determine if they are eligible to the enhancement stream or not. This eligibility is subject to the PER at the used rate. Hence, a member is eligible to the enhancement stream whenever the PER at the used rate to deliver this stream is lower than *PER Limit*. When a member retires from the enhancement layer, it should set all the packets within the BNR window of sub-session 2 as received correctly.

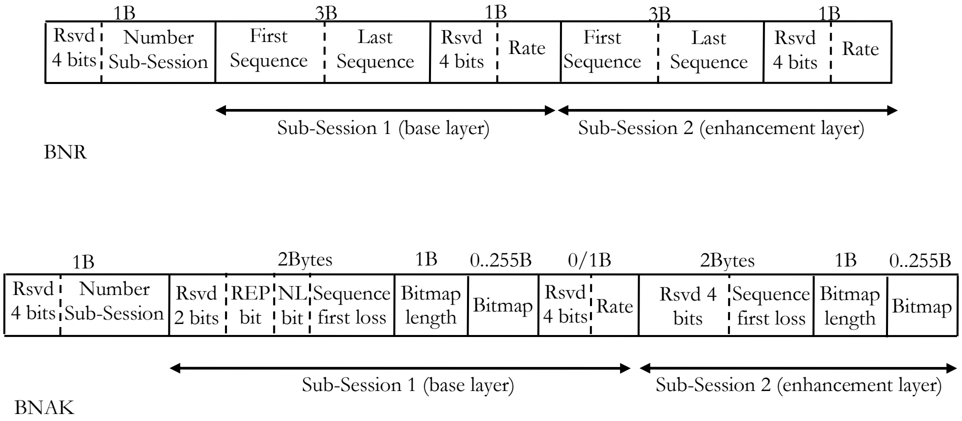


Figure 74. Packet format with one base layer and one enhancement layer

The used rate to send the enhancement layer is selected according to the network load in order to avoid the queue overflow. When the bandwidth is enough to deliver both layers without packet rejections, both layers are delivered at the same rate. Thus, the enhancement stream takes advantage of the rate adaptation of the base layer. During the congestion periods, the rate of sub-session 2 is increased. The AP may even reject all this flow to face the network condition. However, the transmission rate of the enhancement layer can not be lower than that of the base layer. We note that several works consider that the transmission rate of the enhancement layer is the upper rate of the used one to send the base layer [63-65]. According to the authors, this avoids the queue overflow and ensures a differentiated quality. Furthermore, these proposals deliver the enhancement stream using the legacy multicast. The main advantage of BNAK is that the enhancement layer is delivered reliably to the eligible receivers. Besides, this sub-stream may be sent at the rate of the base layer when the bandwidth is enough.

The rate selection of the enhancement layer is beyond the scope of this thesis.

6.5 Simulation Results

In this section we use NS-3 to determine the appropriate values of PTP and DTP. We consider the simulator configuration of Table 8. Besides, we consider that all the multicast packets have 1538 byte-length. This length includes the MAC header. We set *PER Limit* to 5%.

6.5.1 PTP and DTP Values Selection

We perform simulation tests in order to determine the appropriate value of PTP. This delay should be enough to allow a member's request to reach the AP before selecting a higher rate. We build a network of a variable number of multicast receivers which are all eligible to the data rate of 6 Mbps only. Therefore, we set the group members at a distance of 90 meters from the AP. Moreover, we set the lowest allowed rate of the multicast stream to 6Mbps. We consider this rate in order to measure the worst delays which may be required for a BNAK packet to reach the AP. On the other hand we consider 3 different values of the initial Contention Window (CWmin): 15, 31 and 63. These values are exclusively used by the multicast receivers to send a feedback. Moreover we evaluate the BNAK delivery delays for 3 different levels of network load. In all these scenarios, the AP delivers a low throughput multicast traffic. Thus the AP does not contend immediately following the transmission of a BNR to send new multicast packets. In the first scenario (Fig. 75) we consider a WLAN where the AP is the only active node. In the second scenario (Fig. 76) we increase the network load by adding a station which sends unicast packets of 1538 Bytes at 6Mbps and which is in the saturation condition, i.e., the transmission queue of this station is never empty and the station contends again for the channel after each transmission. In the third scenario (Fig. 77) we add a second station with the same configuration of the first unicast sender. We consider that the second and the third scenarios are the worst cases since a network is supposed not to be in the saturation condition in order to operate properly (i.e. operates without packet drop due to congestion). Therefore the two high load scenarios aim at depicting the worst delays in sending a rate decrease request to the AP.

We observe that the lowest delays are experienced in the first scenario since the network is not highly loaded. Therefore a BNAK requires less than 3 ms to reach the AP regardless of CWmin and of the number of multicast receivers which request the rate decrease. In Fig. 76 and 77 we notice that the maximum delays using CWmin=15 are less than 20 ms. However the average delays are less than 6 ms regardless of CWmin and the number of receivers. Therefore we use CWmin=15 and we consider a PTP=20ms for the remainder of this chapter.

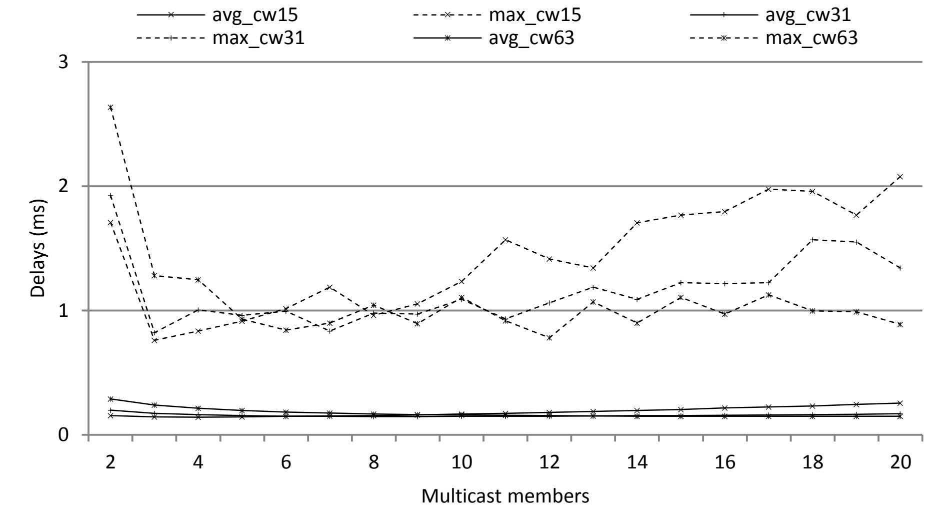


Figure 75. BNAK delivery delays in scenario 1: one multicast traffic

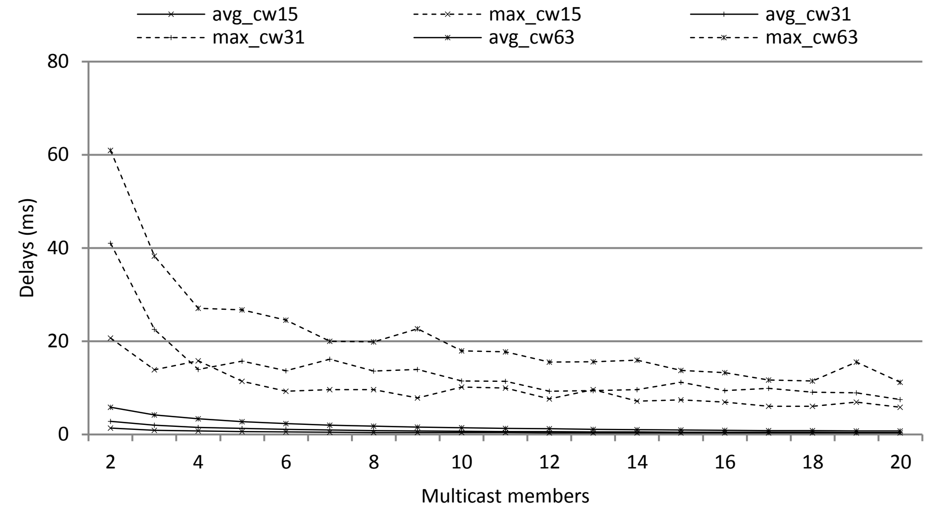


Figure 76. BNAK delivery delays in scenario 2: one multicast traffic and one unicast sender

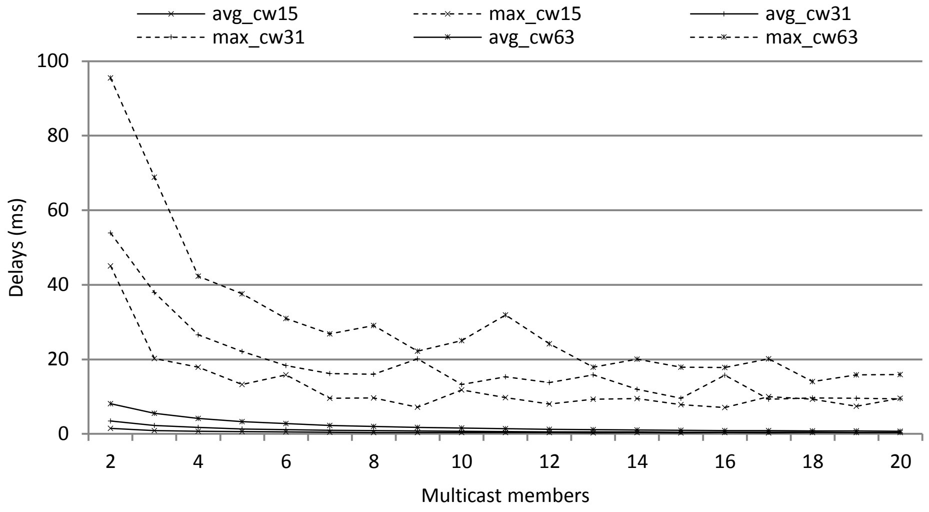


Figure 77. BNAK delivery delays in scenario 3: one multicast traffic and two unicast senders

The value of DTP has an impact on the throughput. This is because a very short value causes the AP to switch to the probing state frequently. Hence the number of BNAKs (which request a data rate decrease or request the retransmission of the probing packet) may reduce the network throughput. On the other hand, an important value of DTP reduces the frequency of the rate increase attempts. In order to define an appropriate value of DTP, we consider the case of multicast packets delivered at 12 Mbps. Therefore, we install all the receivers at a distance of 80 meters from the AP. We set the multicast sender in the saturation condition and we measure the achieved throughput for different values of DTP. Besides, we consider that the AP is the only sender in the WLAN. We vary the number of receivers which do not support any rate higher than 12 Mbps. Therefore these members will attempt to send a rate decrease request if the AP announces a rate higher than 12 Mbps or sends the probing packet at a rate higher than 12 Mbps. Fig. 78 illustrates the impact of the DTP on the throughput of BNAK protocol for two members. We consider the case of 10 and 20 members in Fig. 79 and 80 respectively. We obtain these results using the immediate retry policy. The dashed line illustrates the achieved throughput at the constant rate of 12 Mbps. We observe that the BNAK throughput using the rate adaptation schemes stabilizes starting from DTP=500ms for all the 3 scenarios. At this value, we observe that the throughput difference with and without rate adaptation is less than 8 packets for the case of Fig. 80. Therefore, the rate adaptation scheme of BNAK incurs a very limited overhead, of less than 1%. In the remainder of this chapter we use DTP=500ms.

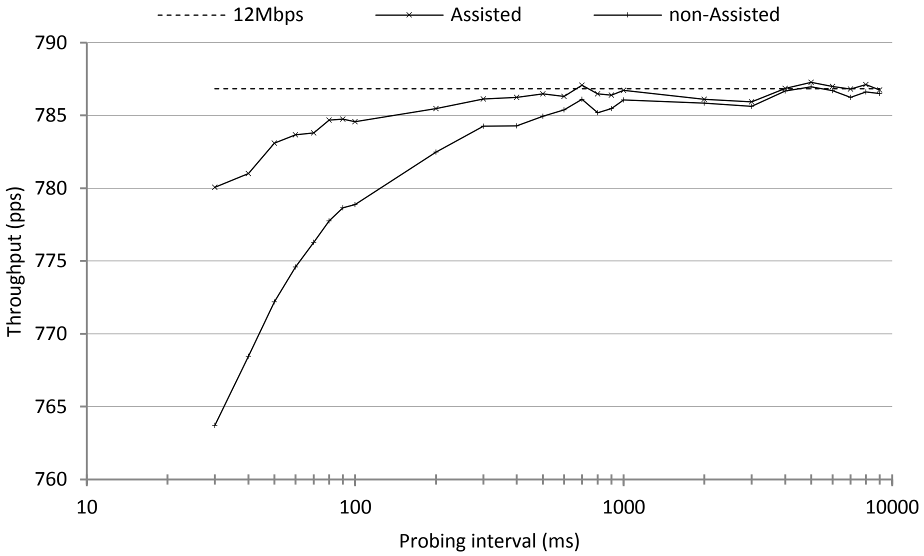


Figure 78. BNAK throughput for 2 members

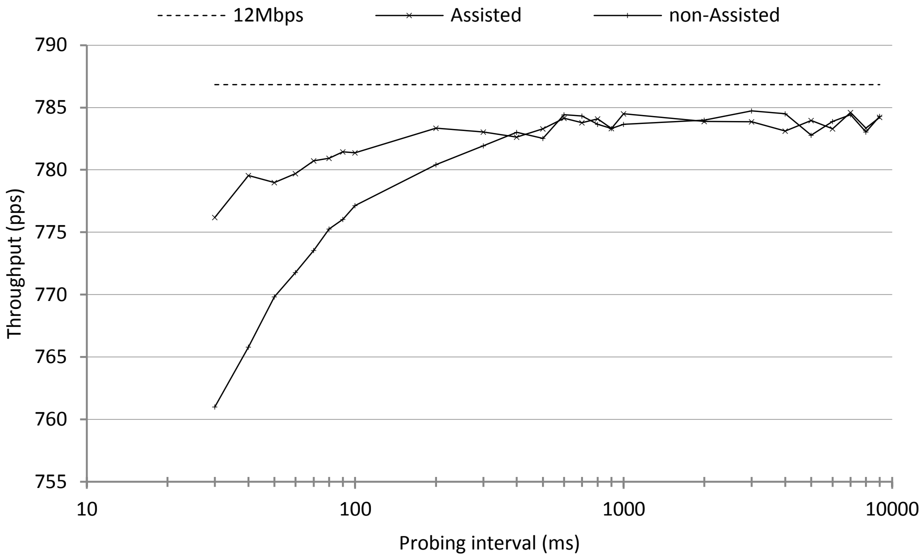


Figure 79. BNAK throughput for 10 members

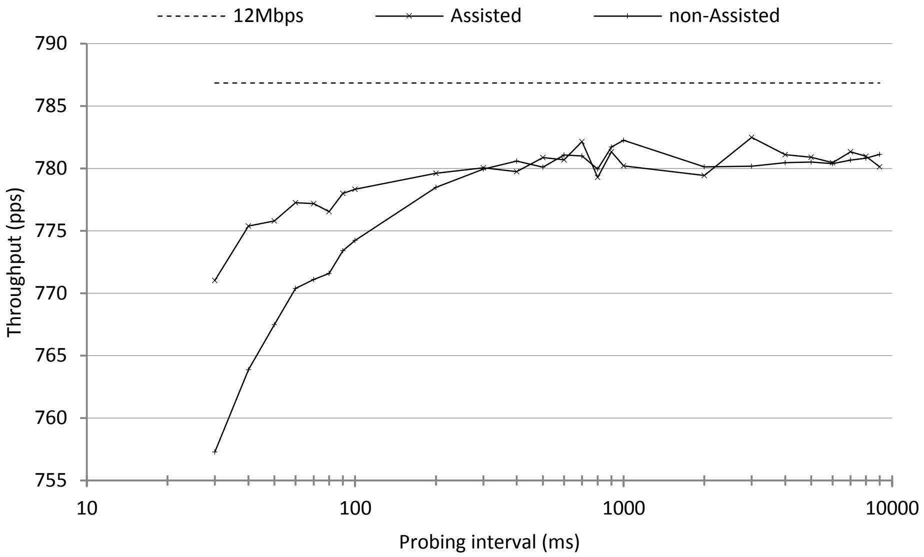


Figure 80. BNAK throughput for 20 members

6.5.2 Performance Evaluation

In the remainder, we compare the performance of ARA and PRA using the principal and the immediate retry policies of BNAK. We build a network with a variable number of multicast members distributed in the area which is situated between R and R/2 from the AP as illustrated in Fig. 81. R is the reference distance and is the location of the farthest member. This configuration intends to increase the probability of having more than 1 member at the reliability limit of a given data rate.

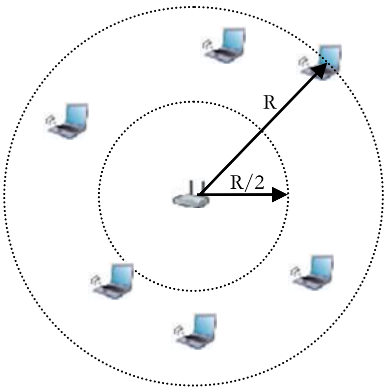


Figure 81. Network configuration

6.5.2.1 Performance Evaluation of the Immediate Retry BNAK with ARA and PRA

We illustrate the throughput of the immediate retry BNAK for groups of 2, 10 and 100 members in Fig. 82, 83 and 84 respectively. We vary the reference distance and we compare ARA and PRA. Besides, we depict the achieved throughput using static data rates. Fig. 82 illustrates the case of a multicast group of 2 members. Since the farthest member retires when it leaves the coverage area of the multicast service (i.e. the area covered by 12 Mbps), both adaptation schemes select a higher rate which fits with the second member. In Fig. 83 and 84 we notice that the throughput does not increase after the retirement of the first member. This is because other receivers are located in the coverage area of 12Mbps. Moreover we observe that the two algorithms achieve almost the same throughput for all the considered group sizes.

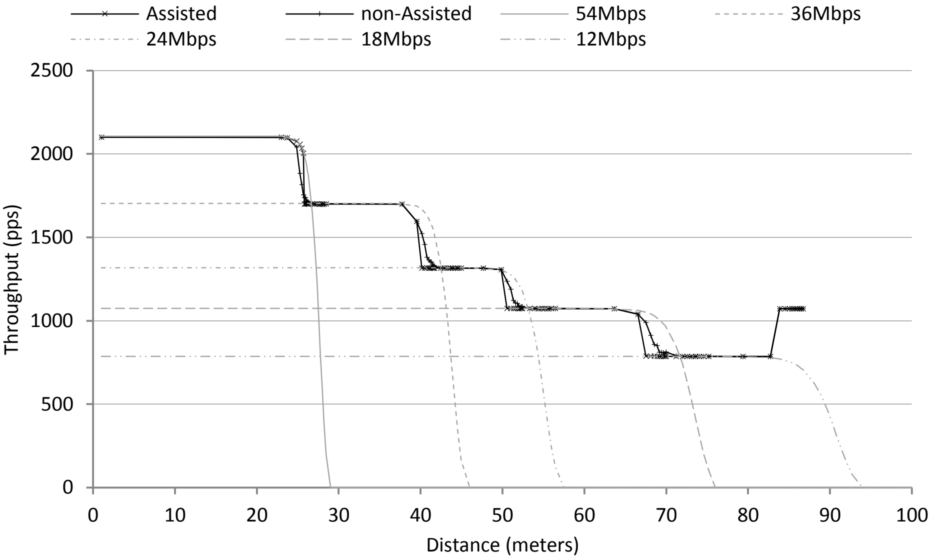


Figure 82. Immediate retry BNAK throughput for 2 members

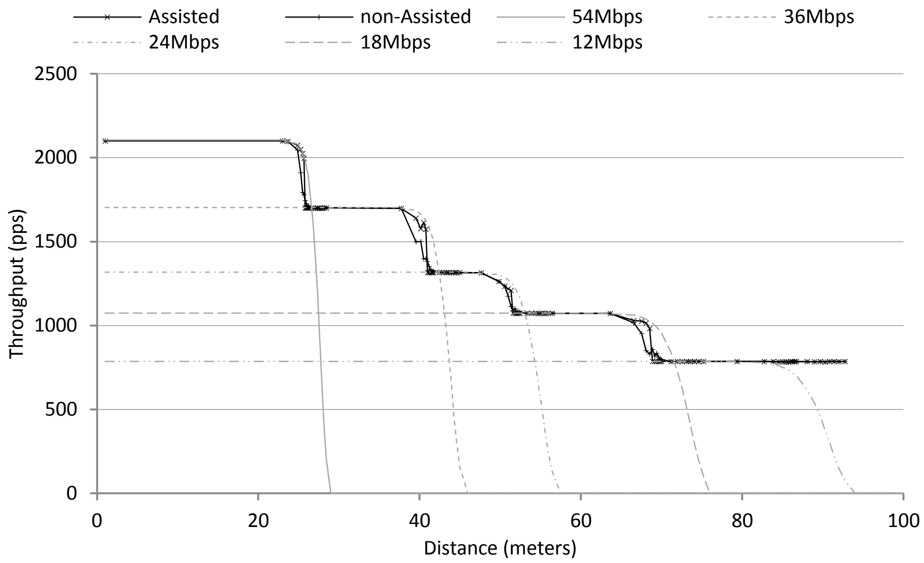


Figure 83. Immediate retry BNAK throughput for 10 members

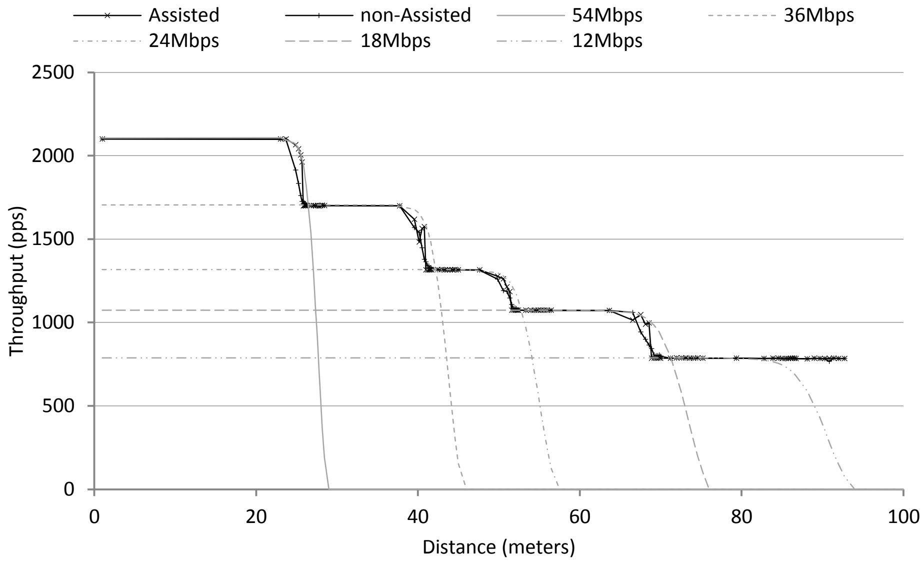


Figure 84. Immediate retry BNAK throughput for 100 members

6.5.2.2 Performance Evaluation of the Principal Retry Policy using ARA and PRA

We compare the throughput of ARA and PRA using the principal retry policy of BNAK. We consider multicast groups of 2, 10 and 100 members in Fig. 85, 86 and 87, respectively. Similar to the immediate retry policy, we observe that the rate adaptation of the principal retry policy does not require important overhead. As we notice, the achieved throughput using both schemes is similar to the highest throughput using constant rates.

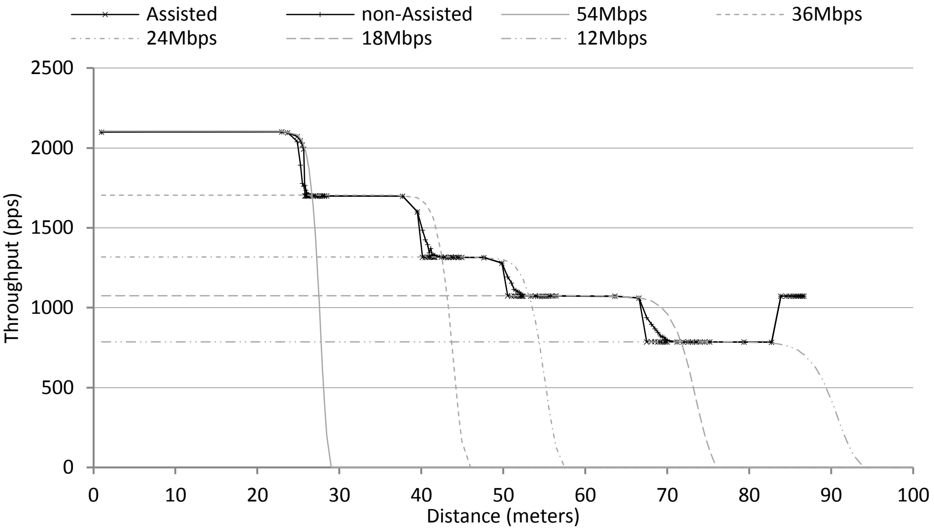


Figure 85. Basic BNAK throughput for 2 members

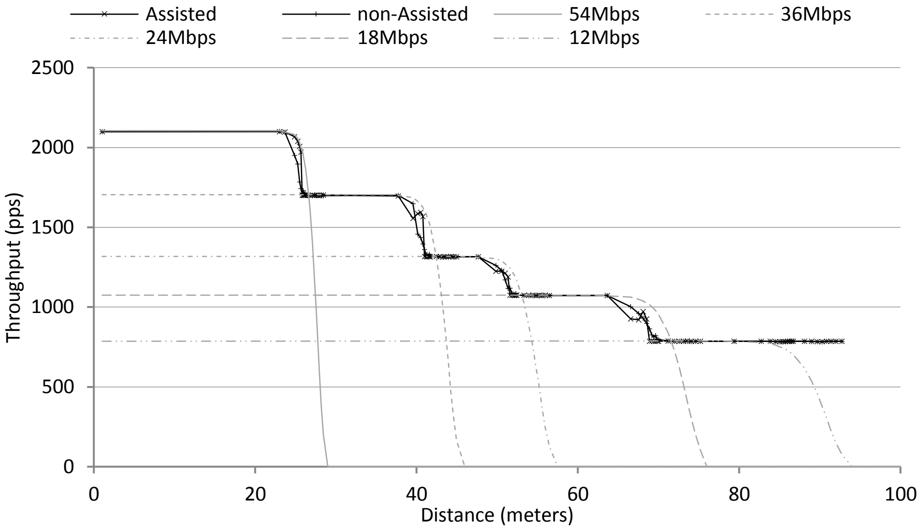


Figure 86. Basic BNAK throughput for 10 members

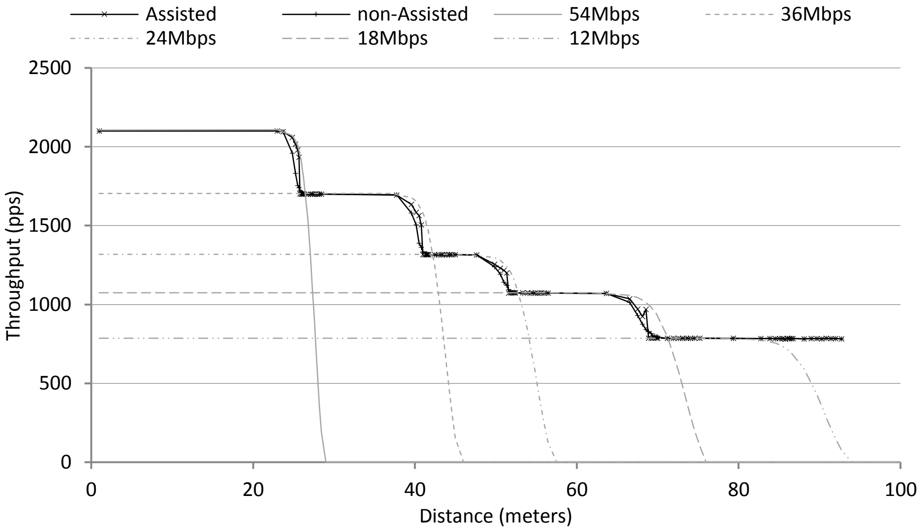


Figure 87. Basic BNAK throughput for 100 members

6.6 Conclusion

In this chapter we study the rate adaptation of BNAK. We introduce a rate selection scheme which relies on the receiver collaboration in order to select the most appropriate data rate. Our simulation results show that the rate adaptation of the principal and the immediate retry policies of BNAK incur very limited overhead even for large multicast groups. Besides, we introduce the scalable video streaming capability of BNAK. This feature allows the protocol to deliver the base and the enhancement layers reliably to the eligible receivers, and permits the AP to face the bandwidth fluctuation by increasing the transmission rate of the enhancement stream. In this chapter we recommend the adaptation of the enhancement layer according to the network load but we do not define a specific procedure. We dedicate the conception of such a procedure for our future work.

Chapter 7

7 Conclusion

This thesis tackles the multicast unreliability issue in wireless networks. Our principal contributions are fivefold. In the beginning we introduce the principal novelties of 802.11aa/v and we compare the different multicast retry policies of these two recent amendments. We show that DMS has a very limited scalability and is appropriate for a group of one or two receivers. Moreover, we demonstrate that GCR-BACK is reliable but incurs an overhead which depends on the group size. Therefore, it is not appropriate for large groups. We show that GCR-UR is scalable and does not depend on the group size. However, increasing the retry count leads to a significant limitation of the overall throughput.

The second contribution of this work is the investigation of the loss factors in WLANs. The major goal of the loss diagnosis is to find the answer to the following question: why receivers at the same location and in the same conditions may experience different error rates and bursty losses? At the start, we introduce the two fundamental causes of transmission failures: path loss and collisions. Then we present a new factor called the device unavailability which is widely ignored, particularly for the 802.11 networks. We measure the impact of this factor on the reliability of the multicast transmissions and we show that the loss rate may reach 100%. These results show that the loss rate in wireless networks may become very limited under the following four assumptions: 1) the receiver is located within the coverage area of the multicast sender, 2) the packets are delivered using the appropriate transmission rate, 3) the collisions are avoided, and 4) the receiver has the appropriate configuration.

To limit the losses and to enhance the reliability of the multicast transmissions, we introduce the Busy Symbol (BS) mechanism. We show that this third contribution ensures an efficient protection for the multicast packets against the collisions. Our simulation results demonstrate that BS avoids all the collisions, incurs a very limited overhead and allows a fair sharing of the bandwidth between unicast and multicast flows. Besides, we prove that this mechanism is easy to implement in real networks and does not need any modification except at the AP. Even though BS is efficient and practical, it is not enough for a reliable multicast transport. This is because BS does not allow the sender to select the most appropriate transmission rate, and does not allow the recovery of the few missing packets incurred by the system failures at the receiving chipset. Therefore, it remains necessary to define a scalable feedback policy.

The fourth contribution of this thesis is the definition of a new multicast protocol called Block Negative Acknowledgement (BNAK). We show that this protocol is reliable and retains the scalability of the multicast transport. Particularly, our simulation results demonstrate that the scalability of BNAK is almost unlimited when the receivers are located at the appropriate distance from the sender. Besides, we show that our protocol incurs very limited transmission delays. These results prove that BNAK outperforms all the proposals of 802.11aa/v significantly. However, the principal advantage of our protocol is its easy implementation and its compliance with old and recent amendments.

To deal with the multi-rate characteristic of 802.11 networks, we define a rate selection scheme for BNAK. We investigate this fifth contribution under a network simulator. The obtained results show that the rate adaptation under BNAK is achieved with very limited overhead. Besides, we show that the proposed scheme operates properly with the principal and the immediate retry policies. Similar to BNAK, the rate selection algorithm is easy to implement within current devices. This deployment requires software updates only, and does not need any hardware modification.

The conception of BNAK is defined to support scalable video streaming. This intends to resolve the issue of bandwidth fluctuation and to deal with the device heterogeneity in wireless networks. Several works [63-65] select one step higher rate for the enhancement stream. We consider that this solution is not optimized when the bandwidth is available and does not resolve the packet drops during the congestions. Therefore we recommend the adaptation of the rate of the enhancement layer according to the network load; when the bandwidth is available, the entire multicast stream is delivered at the same rate. But when the network load increases, the multicast sender increases the data rate of the enhancement stream to avoid the queue overflow. This allows the receivers with good channel conditions to keep receiving the full video quality reliably, and ensures a real-time streaming of a valid video content to remote members. In this thesis we do not define any particular adaptation scheme and we dedicate this task to future works.

One among the principal advantages of BNAK is that this protocol is easy to implement. Therefore, we hope to provide additional results arising from empirical measurements in the near future.

References

[1] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," IEEE std 802.11, 2012.

[2] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: IEEE 802.11 Wireless Network Management," IEEE std 802.11v, February 2011.

[3] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: MAC Enhancements for Robust Audio Video Streaming," IEEE std 802.11aa, May 2012.

[4] BitTorent. BitTorent Homepage: www.bittorrent.com

[5] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," Request for Comments: 3550, July 2003.

[6] Y. Rekhter, T. Li, S. Hares, "A Border Gateway Protocol 4 (BGP-4)," Request for Comments: 4271, January 2006.

[7] J. Moy, "OSPF Version 2," Request for Comments: 2328, April 1998.

[8] D. C. Plummer, "An Ethernet Address Resolution Protocol," Request For Comments: 826, November 1982.

[9] A. Adams, J. Nicholas, W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)," Request for Comments: 3973, January 2005.

[10] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)," Request for Comments: 4601, August 2006.

[11] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, "Internet Group Management Protocol, Version 3," Request for Comments: 3376, October 2002.

[12] "One-way transmission time," ITU-T Recommendation G.114, May 2003.

[13] H. Schulzrinne, A. Rao, R. Lanphier, "Real Time Streaming Protocol (RTSP)," Request for Comments: 2326, April 1998.

[14] M. Handley, V. Jacobson, C. Perkins, "SDP: Session Description Protocol," Request for Comments: 4566, July 2006.

[15] IPTV Focus Group Proceedings, 2008.

[16] D. Waitzman, C. Partridge, S. Deering, "Distance Vector Multicast Routing Protocol," Request For Comments: 1075, November 1988.

[17] J. Moy, "Multicast Extensions to OSPF," Request for Comments: 1584, March 1994.

[18] Daniel Minoli, "IP Multicast with Applications to IPTV and Mobile DVB-H," John Wiley & Sons Ltd, April 2008.

[19] Hua Wang, Xiangxu Meng, Min Zhang, Yanlong Li "Tabu search algorithm for RP selection in PIM-SM multicast routing," in Computer Communications, Volume 33, Issue 1, Pages 35–42, January 2010.

[20] Eun-Mi Lee, Yong-Tae Han, Hong-Shik Park, "Rendezvous Point Relocation for IPTV Services with PIM-SM," in the 14th Asia-Pacific Conference on Communications (APCC) 2008. 14-16 October 2008, Tokyo, Japan.

[21] Ritesh Mukherjee, J. William Atwood, "Rendezvous Point Relocation in Protocol Independent Multicast-Sparse Mode", in the 10th International Conference on Telecommunications (ICT) 2003. 23 February-1 March 2003, Papeete, Tahiti, French Polynesia.

[22] M. Christensen, K. Kimball, F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches," Request for Comments: 4541, May 2006.

[23] "Video Coding for Low Bitrate Communication," DRAFT ITU-T Recommendation H.263, May, 1996.

[24] "Part 14: MP4 file format," ISO/IEC 14496-14, November 2003.

[25] Joint Video Team (JVT) of ISO/IEC MPEG & ITU-T VCEG, "Draft ITU-T Recommendation and Final Draft International Standard of Joint Video Specification (ITU-T Rec. H.264 | ISO/IEC 14496-10 AVC," 8th Meeting, 23-27 May 2003, Geneva, Switzerland.

[26] Joint Video Team (JVT) of ISO/IEC MPEG & ITU-T VCEG, "Joint Draft ITU-T Rec. H.264 | ISO/IEC 14496-10 / Amd.3 Scalable video coding," 24th Meeting, 29 June – 5 July 2007, Geneva, Switzerland.

[27] Christos Bouras, Apostolos Gkamas, Georgios Kioumourtzis, "Adaptive Smooth Simulcast Protocol (ASSP) for Video Applications: Description and Performance Evaluation," in Journal of Network and Systems Management, Volume 19, Issue 2, Pages 143-177, June 2011.

[28] Christos Bouras, Apostolos Gkamas, Georgios Kioumourtzis, "Performance Evaluation of Simulcast vs. Layered Multicasting over Best-effort Networks," in the 17th International Conference on Software, Telecommunications and Computer Networks (SoftCOM) 2009. 24-26 September 2009, Hvar, Croatia.

[29] Christos Bouras, Apostolos Gkamas, Georgios Kioumourtzis, "Adaptive Smooth Simulcast Protocol for Multimedia Transmission," in IEEE Symposium on Computers and Communications (ISCC) 2009. 5 – 8 July 2009, Sousse, Tunisia.

[30] YongQing Liang, Yap-Peng Tan, "A new content-based hybrid video transcoding method," in IEEE International Conference on Image Processing (ICIP) 2001. 7-10 October 2001, Thessaloniki, Greece.

[31] Zhenyun Zhuang, Chun Guo, "Building cloud-ready video transcoding system for Content Delivery Networks (CDNs)," in IEEE Global Communications Conference (GLOBECOM) 2012. 3-7 December 2012, Anaheim, California, USA.

[32] Koji Hashimoto, Yoshitaka Shibata, "Design and Implementation of Adaptive Streaming Modules for Multipoint Video Communication," in the 22nd International Conference on Advanced Information Networking and Applications - Workshops (AINAW) 2008. 25-28 March 2008, Okinawa, Japan.

[33] Jong-Seok Lee, Francesca De Simone, Touradj Ebrahimi, "Subjective quality assessment of scalable video coding: A survey," in the 3rd International Workshop on Quality of Multimedia Experience (QoMEX) 2011. 7-9 September 2011, Mechelen, Belgium.

[34] Heiko Schwarz, Detlev Marpe, Thomas Wiegand, "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard," in IEEE Transactions on Circuits and Systems for Video Technology, Volume 17, Issue 9, Pages 1103 – 1120, September 2007.

[35] Thomas Schierl, Thomas Stockhammer, Thomas Wiegand, "Mobile Video Transmission Using Scalable Video Coding," in IEEE Transactions on Circuits and Systems for Video Technology, Volume 17, Issue 9, Pages 1204 – 1217, September 2007.

[36] Yen-Ting Chen, Hung-Yi Teng, Ren-Hung Hwang, Jeng-Farn Lee, "Optimal Bandwidth Adaptation for Layered Video Multicasting in IEEE 802.11 WLANs," in the 12th International Conference on ITS Telecommunications (ITST) 2012. 5-8 November 2012, Taipei, Taiwan.

[37] Nakjung Choi, Jiho Ryu, Yongho Seok, Yanghee Choi, Taekyoung Kwon, "Unicast-Friendly Multicast in IEEE 802.11 Wireless LANs," in the 3rd IEEE Consumer Communications and Networking Conference (CCNC) 2006. 8-10 January 2006, Las Vegas, Nevada, USA.

[38] Ath9k. http://wireless.kernel.org/en/users/Drivers/ath9k

[39] K. Nichols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," Request for Comments: 2474, December 1998.

[40] D. Grossman, "New Terminology and Clarifications for Diffserv," Request for Comments: 3260, April 2002.

[41] Anwar Saif, Mohamed Othman, Shamala Subramaniam, NorAsilaWati AbdulHamid, "Impact of aggregation headers on aggregating small MSDUs in 802.11n WLANs," in International Conference on Computer Applications and Industrial Electronics (ICCAIE) 2010. 5-8 December 2010, Kuala Lumpur, Malaysia.

[42] Dionysios Skordoulis, Qiang Ni, Hsiao-Hwa Chen, Adrian P. Stephens, Changwen Liu, Abbas Jamalipour, "IEEE 802.11n MAC Frame Aggregation Mechanisms for Next-Generation High-Throughput WLANs," in IEEE Wireless Communications, Volume 15, Issue 1, February 2008.

[43] Michael N. Krishnan, Sofie Pollin, Avideh Zakhor, "Local Estimation of Probabilities of Direct and Staggered Collisions in 802.11 WLANs," in IEEE Global Telecommunications Conference, (GLOBECOM) 2009. 30 November – 4 December 2009, Honolulu, Hawaii.

[44] Ken Tang, Mario Gerla, "MAC reliable broadcast in ad hoc networks," in IEEE Military Communications Conference (MILCOM) 2001. 28 – 31 October 2001, McLean, Virginia USA.

[45] Min-Te Sun, Lifei Huang, Anish Arora, Ten-Hwang Lai, "Reliable MAC Layer Multicast in IEEE 802.11Wireless Networks," in International Conference on Parallel Processing (ICPP) 2002. 18-21 August 2002, Vancouver, British Columbia, Canada.

[46] Yuki Tanigawa, Kenta Yasukawa, Katsunori Yamaoka, "Transparent Unicast Translation to Improve Quality of Multicast over Wireless LAN," in the 7th IEEE Consumer Communications and Networking Conference (CCNC) 2010. 9-12 January 2010, Las Vegas, Nevada, USA.

[47] Claudia Campolo, Antonella Molinaro, Claudio Casetti, Carla-Fabiana Chiasserini, "An 802.11-based MAC Protocol for Reliable Multicast in Multihop Networks," in 69th IEEE Vehicular Technology Conference (VTC) Spring 2009. 26-29 April 2009, Barcelona, Spain.

[48] Varun Srinivas, Lu Ruan, "An Efficient Reliable Multicast Protocol for 802.11-based Wireless LANs," in IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM) 2009. 15-19 June 2009, Kos, Greece.

[49] Xiaoli Wang, Lan Wang, Yingjie Wang, Yongsheng Zhang, "A Reliable and Efficient MAC Layer Multicast Protocol in Wireless LANs," in 69th IEEE Vehicular Technology Conference (VTC) Spring 2009. 26-29 April 2009, Barcelona, Spain.

[50] Jiawei Xie, Amitabha Das, Sukumar Nandi, Anil K. Gupta, "Improving the Reliability of IEEE 802.11 Broadcast Scheme for Multicasting in Mobile Ad hoc Networks," in IEEE Wireless Communications and Networking Conference (WCNC) 2005. 13-17 March 2005, New Orleans, Louisiana, USA.

[51] Xiaoli Wang, Lan Wang, Yingjie Wang, Daqing Gu, "Reliable Multicast Mechanism in WLAN with Extended Implicit MAC Acknowledgment," in 67th IEEE Vehicular Technology Conference (VTC) Spring 2008. 11-14 May 2008, Marina Bay, Singapore.

[52] Hrishikesh Gossain, Nagesh Nandiraju, Kumar Anand, Dharma P. Agrawal, "Supporting MAC Layer Multicast in IEEE 802.11 based MANETs: Issues and Solutions," in the 29th IEEE International Conference on Local Computer Networks (LCN) 2004. 16–18 November 2004, Tampa, Florida, USA.

[53] Joy Kuri, Sneha Kumar Kasera, "Reliable Multicast in Multi-access Wireless LANs," in IEEE INFOCOM 1999. 21-25 March 1999. New York, USA.

[54] Wan-Seon Lim, Dong-Wook Kim, Young-Joo Suh, "Design of Efficient Multicast Protocol for IEEE 802.11n WLANs and Cross-Layer Optimization for Scalable Video Streaming," in IEEE Transactions on Mobile Computing, Volume 11, Issue 5, Pages 780 – 792, May 2012.

[55] S. K. S. Gupta, V. Shankar, S. Lalwani, "Reliable Multicast MAC Protocol for Wireless LANs," in IEEE International Conference on Communications (ICC) 2003. 11-15 May 2003, Anchorage, Alaska, USA.

[56] M. Angeles Santos, Jose Villalon, Luis Orozco Barbosa, Fernando Ramirez Mireles, "A new ARQ mechanism for multicast traffic over IEEE 802.11 WLANs," in 4th Joint IFIP Wireless and Mobile Networking Conference (WMNC) 2011. 26-28 October 2011, Toulouse, France.

[57] Jochen Miroll, Zhao Li, Thorsten Herfet, "Wireless Feedback Cancellation for Leader-Based MAC Layer Multicast Protocols," in the 14th IEEE International Symposium on Consumer Electronics (ISCE) 2010. 7-10 June 2010, Braunschweig, Germany.

[58] Zhao Li, Thorsten Herfet, "MAC Layer Multicast Error Control for IPTV in Wireless LANs," in IEEE Transactions on Broadcasting, Volume 55, Issue 2, Pages 353 – 362, June 2009.

[59] Zhao Li, Thorsten Herfet, "Beacon-driven Leader Based Protocol over a GE Channel for MAC Layer Multicast Error Control," in International Journal of Communications, Network and System Sciences (IJCNS), Volume 1 No. 2, Pages 144-153, May 2008.

[60] Zhao Li, Thorsten Herfet, "HLBP: A Hybrid Leader Based Protocol for MAC Layer Multicast Error Control in Wireless LANs," in IEEE Global Telecommunications Conference (GLOBECOM) 2008. 30 November – 4 December 2008, New Orleans, Louisiana, USA.

[61] Anas Basalamah, Hiroki Sugimoto, Takuro Sato, "Rate Adaptive Reliable Multicast MAC Protocol for WLANs," in 63rd IEEE Vehicular Technology Conference (VTC) Spring 2006. 7-10 May 2006, Melbourne, Australia.

[62] Sungjoon Choi, Nakjung Choi, Yongho Seok, Taekyoung Kwon, Yanghee Choi, "Leader-based Rate Adaptive Multicasting for Wireless LANs," in IEEE Global Telecommunications Conference (GLOBECOM) 2007. 26-30 November 2007, Washington, USA.

[63] M. Angeles Santos, Jose Villalon, Luis Orozco-Barbosa, "A Novel QoE-Aware Multicast Mechanism for Video Communications over IEEE 802.11 WLANs," in IEEE Journal on Selected Areas in Communications, Volume 30, Issue 7, Pages 1205 – 1214, August 2012.

[64] Jose Villalon, Pedro Cuenca, Luis Orozco-Barbosa, Yongho Seok, Thierry Turletti, "Cross-Layer Architecture for Adaptive Video Multicast Streaming Over Multirate Wireless LANs," in IEEE Journal on Selected Areas in Communications, Volume 25, Issue 4, Pages 699 – 711, May 2007.

[65] Jose Villalon, Pedro Cuenca, Luis Orozco-Barbosa, Yongho Seok, Thierry Turletti, "ARSM: a cross-layer auto rate selection multicast mechanism for multi-rate wireless LANs," in IET Communications, Volume 1, Issue 5, Pages 893 – 902, October, 2007.

[66] T. Speakman, J. Crowcroft, J. Gemmell, D. Farinacci, S. Lin, D. Leshchiner, M. Luby, T. Montgomery, L. Rizzo, A. Tweedly, N. Bhaskar, R. Edmonstone, R. Sumanasekera, L. Vicisano, "PGM Reliable Transport Protocol Specification," Request for Comments: 3208, December 2001.

[67] Yongtae Park, Chiho Jo, Sangki Yun, Hyogon Kim, "Multi-Room IPTV Delivery through Pseudo-Broadcast over IEEE 802.11 Links," in 71st IEEE Vehicular Technology Conference (VTC) Spring 2010. 16-19 May 2010, Taipei, Taiwan.

[68] Nakjung Choi, Yongho Seok, Taekyoung Kwon, Yanghee Choi, "Leader-Based Multicast Service in IEEE 802.11v Networks," in the 7th IEEE Consumer Communications and Networking Conference (CCNC) 2010. 9-12 January 2010, Las Vegas, Nevada, USA.

[69] Nakjung Choi, Yongho Seok, Taekyoung Kwon, Yanghee Choi, "Multicasting multimedia streams in IEEE 802.11 networks: a focus on reliability and rate adaptation," in Wireless Networks, Volume 17, Issue 1, Pages 119-131, January 2011.

[70] Ranveer Chandra, Sandeep Karanth, Thomas Moscibroda, Vishnu Navda, Jitendra Padhye, Ramachandran Ramjee, Lenin Ravindranath "DirCast: A Practical and Efficient Wi-Fi Multicast System," in the 17th IEEE International Conference on Network Protocols (ICNP) 2009. 13-16 October 2009, Princeton, New Jersey, USA.

[71] Szymon Jakubczak, Dina Katabi, "A Cross-Layer Design for Scalable Mobile Video," in the 17th ACM International Conference on Mobile Computing and Networking (MobiCom) 2011. September 2011.

[72] Sayandeep Sen, Neel Kamal Madabhushi, Suman Banerjee, "Scalable WiFi Media Delivery through Adaptive Broadcasts," in the 7th USENIX Symposium on Networked Systems Design and Implementation (NSDI) 2010. 28-30 April 2010, San Jose, California, USA.

[73] Dongyan Xu, Baochun Li, Klara Nahrstedt, "QoS-Directed Error Control of Video Multicast in Wireless Networks," in the 8th International Conference on Computer Communications and Networks (ICCCN) 1999. 11-13 October 1999, Boston, Massachusetts, USA.

[74] Dong Nguyen, Tuan Tran, Thinh Nguyen, Bella Bose, "Wireless Broadcast Using Network Coding," in IEEE Transactions on Vehicular Technology, Volume 58, Issue 2, Pages 914 – 925, February 2009.

[75] Yoshihisa Kondo, Hiroyuki Yomo, Shinji Yamaguchi, Peter Davis, Ryu Miura, Sadao Obana "Reliable Wireless Broadcast with Random Network Coding for Real-time Applications," in IEEE Wireless Communications and Networking Conference (WCNC) 2009. 5-8 April 2009, Budapest, Hungary.

[76] Zhengye Liu, Zhenyu Wu, Pei Liu, Hang Liu, Yao Wang, "Layer Bargaining: Multicast Layered Video over Wireless Networks," in IEEE Journal on Selected Areas in Communications, Volume 28, Issue 3, Pages 445 – 455, April 2010.

[77] Byung-Seo Kim, Sung Won Kim, Randy L. Ekl, "OFDMA-Based Reliable Multicasting MAC Protocol for WLANs," in IEEE Transactions on Vehicular Technology, Volume 57, Issue 5, Pages 3136 – 3145, September 2008.

[78] Weisheng Si, Chengzhi Li, "RMAC: A Reliable Multicast MAC Protocol for Wireless Ad Hoc Networks," in the 33rd International Conference on Parallel Processing (ICPP) 2004. 15-18 August 2004, Montreal, Quebec, Canada.

[79] Yigal Bejerano, Jaime Ferragut, Katherine Guo, Varun Gupta, Craig Gutterman, Thyaga Nandagopal, Gil Zussman, "Scalable WiFi Multicast Services for Very Large Groups," in the 21t IEEE International Conference on Network Protocols (ICNP) 2013. 7-11 October 2013, Gottingen, Germany.

[80] Clarifications for RFC 3208, http://msdn.microsoft.com/en-us/library/cc219051.aspx

[81] Kostas Maraslis, Periklis Chatzimisios, Anthony Boucouvalas, "IEEE 802.11aa: Improvements on video transmission over Wireless LANs," in IEEE International Conference on Communications (ICC) 2012. 10-15 June 2012, Ottawa, Canada.

[82] M. Angeles Santos, Jose Villalon, Luis Orozco-Barbosa, "Evaluation of the IEEE 802.11aa group addressed service for robust audio-video streaming" in IEEE International Conference on Communications (ICC) 2012. 10-15 June 2012, Ottawa, Canada.

[83] Antonio de la Oliva, Pablo Serrano, Pablo Salvador, Albert Banchs, "Performance Evaluation of the IEEE 802.11aa Multicast Mechanisms for Video Streaming," in the 14th IEEE International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM) 2013. 4-7 June 2013, Madrid, Spain.

[84] Lucas Eznarriaga Barranco, "Performance Evaluation of IEEE 802.11aa MAC Enhancements for Robust Audio Video Streaming," University Carlos III of Madrid, Department of Telematics Engineering, Master of Science Thesis, 2011.

[85] OPNET. Home page, http://www.opnet.com/

[86] "Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks," IEEE Std 802.1Q, 2011.

[87] The NS-3 Simulator. Home page, http://www.nsnam.org/

[88] Shafqat Ur Rehman, Thierry Turletti, Walid Dabbous, "Multicast Video Streaming over WiFi Networks: Impact of Multipath Fading and Interference," in IEEE Symposium on Computers and Communications (ISCC) 2011. 28 June – 1 July 2011, Kerkyra, Greece.

[89] Zhe Wang, Mahbub Hassan, Tim Moors, "A Study of Spatial Packet Loss Correlation in 802.11 Wireless Networks," in the 35th IEEE Conference on Local Computer Networks (LCN) 2010. 10-14 October 2010, Denver, Colorado, USA.

[90] Diego Dujovne, Thierry Turletti, "Multicast in 802.11 WLANs: An Experimental Study," in the 9th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM) 2006. 2-6 October 2006, Malaga, Spain.

[91] Jerome Lacan, Tanguy Perennou, "Evaluation of Error Control Mechanisms for 802.11b Multicast Transmissions," in the 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt) 2006. 03-07 April 2006, Boston, Massachusetts, USA.

[92] Janus Heide, Morten V. Pedersen, Frank H.P. Fitzek, Tatiana K. Madsen, Torben Larsen, "Know Your Neighbour: Packet Loss Correlation in IEEE 802.11b/g Multicast," in the 4th International Mobile Multimedia Communications Conference (MobiMedia) 2008. 7 – 9 July 2008, Oulu, Finland.

[93] Daniel Aguayo, John Bicket, Sanjit Biswas, Glenn Judd, Robert Morris, "Link-level Measurements from an 802.11b Mesh Network," in the ACM SIGCOMM 2004. 30 August – 3 September 2004, Portland, Oregon, USA.

[94] Chiping Tang, Philip K. McKinley, "Modeling Multicast Packet Losses in Wireless LANs," in the 6th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM) 2003. 14 – 19 September 2003, San Diego, California, USA.

[95] Andreas Willig, Adam Wolisz, "Ring Stability of the PROFIBUS Token-Passing Protocol Over Error-Prone Links," in the IEEE Transactions on Industrial Electronics Volume 48, Issue 5, Pages 1025 – 1033, October 2001.

[96] Andreas Willig, Martin Kubisch, Christian Hoene, Adam Wolisz, "Measurements of a Wireless Link in an Industrial Environment Using an IEEE 802.11-Compliant Physical Layer," in the IEEE Transactions on Industrial Electronics, Volume 49, Issue 6, Pages 1265 – 1282, December 2002.

[97] Giao T. Nguyen, Randy H. Katz, Brian Noble, Mahadev Satyanarayanan, "A Trace Based Approach for Modeling Wireless Channel Behavior," in the Winter Simulation Conference 1996. 8 – 11 December 1996, Coronado, California, USA.

[98] Hamid R. Tafvizi, Zhe Wang, Mahbub Hassan, Salil S. Kanhere, "Multipath Fading Effect on Spatial Packet Loss Correlation in Wireless Networks," in IEEE Vehicular Technology Conference (VTC) Fall 2011. 5-8 September 2011, San Francisco, California, USA.

[99] Mingu Cho, Hakyung Jung, Shinhaeng Oh, Ted Taekyoung Kwon, Yanghee Choi, "Distinguishing Collisions from Low Signal Strength in Static 802.11n Wireless LANs," in the 7th ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT) 2011. 6 – 9 December 2011, Tokyo, Japan.

[100] Wang Hao, Jiang Hao, "A particle filter and joint likelihood ratio based error source diagnosing method for IEEE 802.11 networks," in Wireless Communications and Mobile Computing 2013. May 2013.

[101] Malik Ahmad Yar Khan, Darryl Veitch, "Peeling the 802.11 Onion: Separating Congestion from Physical PER," in the 3rd ACM International Workshop on Wireless Network Testbeds, Experimental evaluation and CHaracterization (WiNTECH) 2008. 19 September 2008, San Francisco, California, USA.

[102] Shinuk Woo, Hwangnam Kim, "Estimating Link Reliability in Wireless Networks: An Empirical Study and Interference Modeling," in IEEE INFOCOM 2010. 14-19 March 2010, San Diego, California, USA.

[103] Andreas Wapf, Michael R. Souryal, "Measuring Indoor Mobile Wireless Link Quality," in IEEE International Conference on Communications (ICC) 2009. 14-18 June 2009, Dresden, Germany.

[104] Michael R. Souryal, Luke Klein-Berndt, Leonard E. Miller, Nader Moayeri, "Link Assessment in an Indoor 802.11 Network," in IEEE Wireless Communications and Networking Conference (WCNC) 2006. 3-6 April 2006, Las Vegas, Nevada, USA.

[105] Shinuk Woo, Hwangnam Kim, "An Empirical Interference Modeling for Link Reliability Assessment in Wireless Networks," in IEEE/ACM Transactions on Networking Volume 21, Issue 1, Pages 272 – 285, February 2013.

[106] Muhammad Naveed Aman, Biplab Sikdar, "Distinguishing Between Channel Errors and Collisions in IEEE 802.11," in the 46th Conference on Information Sciences and Systems (CISS) 2012. 21-23 March 2012, Princeton, New Jersey, USA.

[107] M. Angeles Santos, Jose Villalon, Luis Orozco-Barbosa, "Multicast Collision Free (MCF) Mechanism over IEEE 802.11 WLANs," in IFIP Wireless and Mobile Networking Conference (WMNC) 2010. 13-15 October 2010, Budapest, Hungary.

[108] Thomas Nilsson, Greger Wikstrand, Jerry Eriksson, "A Collision Detection Method for Multicast Transmissions in CSMA/CA Networks," in Wireless Communications and Mobile Computing, Volume 7, Issue 6, pages 795–808, August 2007.

[109] Yeonchul Shin, Munhwan Choi, Jonghoe Koo, Young-Doo Kim, Jong-Tae Ihm, Sunghyun Choi, "Empirical Analysis of Video Multicast over WiFi," in the 3rd International Conference on Ubiquitous and Future Networks (ICUFN) 2011. 15-17 June 2011, Dalian, China.

[110] Yong He, Beijing, Ruixi Yuan, Xiaojun Ma, Jun Li, "The IEEE 802.11 Power Saving Mechanism: An Experimental Study," in the IEEE Wireless Communications and Networking Conference, (WCNC) 2008. March 31 - April 3 2008, Las Vegas, Nevada, USA.

[111] Intel website: http://www.intel.com/support/wireless/wlan/sb/CS-032513.htm

[112] John Regehr, Usit Duongsaa, "Preventing Interrupt Overload," in the ACM SIGPLAN/SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES) 2005. 15-17 June 2005, Chicago, Illinois, USA.

[113] Gary W. Scheer, David J. Dolezilek, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks,"" Western Power Delivery Automation Conference, Spokane, Washington, April 4– 6, 2000.

[114] The LiveMedia Framework, home page: http://www.live555.com/

[115] Souvik Sen, Naveen Santhapuri, Romit Roy Choudhury, Srihari Nelakuditi, “Successive Interference Cancellation: A Back-of-the-Envelope Perspective,” in Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks (Hotnets), 2010. 20–21 October 2010, Monterey, California, USA.

[116] Ece Gelal, Konstantinos Pelechrinis, Tae-Suk Kim, Ioannis Broustis, Srikanth V. Krishnamurthy, Bhaskar Rao, “Topology Control for Effective Interference Cancellation in Multi-User MIMO Networks,” in IEEE INFOCOM 2010. 14-19 March 2010, San Diego, California, USA.

[117] Md. Rakib Subaid, Md. Rakibul Hasan, Syed Ziauddin Ahmed, Md. Forkan Uddin, “Performance of successive interference cancellation technique in IEEE 802.11 based WLANs,” in the International Conference on Informatics, Electronics and Vision (ICIEV) 2013. 17-18 May 2013, Dhaka, Bangladesh.

[118] Intersil HFA3861B Direct Sequence Spread Spectrum (DSSS) baseband processor, Data Sheet February 2002.

[119] A. Kamerman, L. Monteban, “WaveLAN-II: A High-performance wireless LAN for the unlicensed band,” Bell Lab Technical Journal, summer 1997, Pages 118-133.

[120] Starsky H.Y. Wong, Hao Yang, Songwu Lu, Vaduvur Bharghavan, “Robust Rate Adaptation for 802.11 Wireless Networks,” in the 12th International Conference on Mobile Computing and Networking (MOBICOM) 2006. 23-29 September 2006, Los Angeles, California, USA.

[121] Ioannis Pefkianakis, Yun Hu, Songwu Lu, “History-Aware Rate Adaptation in 802.11 Wireless Networks,” in IEEE Symposium on Computers and Communications (ISCC) 2011. 28 June – 1 July 2011, Kerkyra, Greece.

[122] Prashanth A.K. Acharya, Ashish Sharma, Elizabeth M. Belding, Kevin C. Almeroth, Konstantina Papagiannaki, “Rate Adaptation in Congested Wireless Networks through Real-Time Measurements,” in the IEEE Transactions on Mobile Computing, Volume 9, Issue 11, Pages 1535 – 1550, November 2010.

[123] Minstrel, http://madwifi-project.org/browser/madwifi/trunk/ath_rate/minstrel/minstrel.txt

[124] Kaidi D. Huang, Ken R. Duffy, David Malone, “H-RCA: 802.11 Collision-Aware Rate Control,” in the IEEE/ACM Transactions on Networking, Volume 21, Issue 4, Pages 1021 – 1034, August 2013.

[125] Jongseok Kim, Seongkwan Kim, Sunghyun Choi, Daji Qiao, “CARA: Collision-Aware Rate Adaptation for IEEE 802.11 WLANs,” in the 25th IEEE INFOCOM 2006. 23 – 29 April 2009, Barcelona, Spain.

[126] Chun-cheng Chen, Haiyun Luo, Eunsoo Seo, Nitin H. Vaidya, Xudong Wang, “Rate-adaptive Framing for Interfered Wireless Networks,” in the 26th IEEE INFOCOM 2007. 6-12 May 2007, Anchorage, Alaska, USA.

[127] Mythili Vutukuru, Hari Balakrishnan, Kyle Jamieson, “Cross-Layer Wireless Bit Rate Adaptation,” in ACM SIGCOMM 2009. 17–21 August 2009, Barcelona, Spain.

[128] Daniel Halperin, Wenjun Hu, Anmol Shethy, David Wetherall, “Predictable 802.11 Packet Delivery from Wireless Channel Measurements,” in ACM SIGCOMM 2010. August 30–September 3, 2010, New Delhi, India.

[129] Shravan Rayanchu, Arunesh Mishra, Dheeraj Agrawal, Sharad Saha, Suman Banerjee, “Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal,” in the 27th IEEE INFOCOM 2008. 13-18 April 2008, Phoenix, Arizona, USA.

[130] S. Khan, S. A. Mahmud, H. Noureddine, H. S. Al-Raweshidy, “Rate-adaptation for multi-rate IEEE 802.11 WLANs using mutual feedback between transmitter and receiver,” in the 21st IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC) 2010. 26-30 September 2010, Instanbul, Turkey.

[131] Glenn Judd, Xiaohui Wang, Peter Steenkiste, “Efficient Channel-aware Rate Adaptation in Dynamic Environments,” in the 6th International Conference on Mobile Systems, Applications, and Services (MobiSys) 2008. 17–20 June 2008, Breckenridge, Colorado, USA.

[132] Saad Biaz, Shaoen Wu, “Loss Differentiated Rate Adaptation in Wireless Networks,” in the IEEE Wireless Communications and Networking Conference, (WCNC) 2008. March 31 - April 3 2008, Las Vegas, Nevada, USA.

[133] Qiuyan Xia, Mounir Hamdi, “Smart Sender: A Practical Rate Adaptation Algorithm for Multirate IEEE 802.11 WLANs,” in the IEEE Transactions on Wireless Communications, Volume 7, Issue 5, Pages 1764 – 1775, May 2008.

[134] Qiuyan Xia, Mounir Hamdi, Tsz Ho Chan, “Practical Rate Adaptation for IEEE 802.11 WLANs,” in the IEEE Global Telecommunications Conference (GLOBECOM) 2006. November 27 -December 1 2006, San Francisco, California, USA.

[135] Parag Kulkarni, Benjamin Motz, Tim Lewis, Sadia Quadri, “Inferring Loss Causes to Improve Link Rate Adaptation in Wireless Networks,” in the IEEE International Conference on Advanced Information Networking and Applications (AINA) 2011. 22-25 March 2011, Biopolis, Singapore.

[136] Youngsam Park, Yongho Seok, Nakjung Choi, Yanghee Choi, Jean-Marie Bonnin, “Rate-Adaptive Multimedia Multicasting over IEEE 802.11 Wireless LANs,” in the 3rd IEEE Consumer Communications and Networking Conference (CCNC) 2006. 8-10 January 2006, Las Vegas, Nevada, USA.