A NOVEL PRIORITY BASED CHANNEL ACCESS METHOD IN 802.11S WIRELESS NETWORK

P.S. Patheja*

Akhilesh A. Waoo**

Ankita Gupta***

ABSTRACT

IEEE 802.11s defines a new mesh data frame format and an extensibility framework for routing. The present 802.11 interconnections rely on wired networks to carry out bridging functions. For a number of reasons, this dependency on wired infrastructure must be eliminated .WMNs rely on the IP layer to enable multihop communication and do not provide an inherently wireless solution. Since wireless links are less reliable than wired links, a multihop routing protocol operating in a wireless environment must take this into account. It defines the Hybrid Wireless Mesh Protocol (HWMP) based on Ad hoc On-demand Distance Vector Routing (AODV) using MAC addresses for layer 2 routing and Radio-Aware routing metric.802.11s differentiate four traffic categories with different priority in medium access and they allow for limited support of QoS. EDCA uses priority for traffic that do not support MCCA. To overcome the problem of MCCA channel access method we propose a novel access method that support both relative proportional throughput allocation and absolute priority in 802.11 wireless network. It is built on the idea of the Idle sense method that provide the optimal throughput and fairness.

Keywords: *Ad-hoc network, Routing Protocol: AODV, HWMP.*

*Assistant Professor, BIST, Bhopal.

**Assistant Professor, BIST, Bhopal.

***BIST, Bhopal.

I. INTRODUCTION

Being an extension of IEEE 802.11 specification, IEEE 802.11s [7] inherits the mandatory channel access method, EDCA, for operation in multi hop scenarios. Many papers, e.g. [8]–[9], show that the performance of EDCA degrades dramatically in multi hop networks because of the hidden stations (STAs) effect. One may say that IEEE 802.11 introduces the RTS/CTS mechanism to avoid this effect. Un-fortunately, this mechanism works effectively in infrastructure mode only as all STAs hear CTS frames transmitted by the AP and collisions of data frames are completely avoided. In multi hop networks, due to their nature, there is no guarantee that all STAs hear CTS frames, so the RTS/CTS exchange is not enough to protect transmission [5]. In 2006, a novel channel access method, called MCCA (in early IEEE 802.11s drafts, the method was called Mesh Deterministic Access (MDA), specifically designed for operation in multi hop networks was introduced. MCCA allows mesh STAs to reserve time intervals, called MCCAOPs, for data transmissions in a periodic manner. The transmitting and receiving STAs advertise each MCCAOP reservation to their neighbors which then re-broadcast the advertisement to ensure that all STAs in the two-hop neighborhood of the transmitting and receiving STAs become aware of this reservation. During an MCCAOP, the transmitting STA obtains access to the channel with the highest priority, while other STAs which track this reservation defer from starting their transmissions to escape interference. The MCCA looks like a solution for Quality of Service (QoS) provisioning, especially for periodic multimedia traffic, because it gives an opportunity of controlled access to the channel with virtually no interference from neighboring STAs. Multimedia traffic, such as a VoIP or Video traffic, usually requires low and stable end-to-end delay and low packet loss probability. As reservations provide some control on the delay, the packet loss probability is the most critical factor. In this paper, we show that transmissions in MCCAOPs are not fully protected from interference and therefore packet loss ratio requirements may not be met. We reveal the reasons of packet losses, additional to random noise and interference from MCCA-incapable STAs, and propose solutions which guarantee reliable transmission in MCCAOPs and accomplishment of QoS requirements.

II. MCCA DESCRIPTION

MCCA is an channel access method that allows STAs to access the channel in predefined time intervals, called MCCAOPs, with lower contention than it would otherwise be possible. To set up a reservation, which may be for either individually or group addressed transmissions, a STA, called MCCAOP owner, transmits an MCCAOP setup request specifying parameters of the planning reservation. The receiver(s), called MCCAOP responder(s), checks the re-quested reservation for any conflict with reservations it is involved in and reservations of neighboring STAs it is aware of, and transmits a response with accept or reject code. To reduce the probability of reservation conflicts a STA advertises its own reservations and reservations of neighboring STAs it is aware of. For this purpose, the STA periodically generates and transmits via beacons or management frames (a) an MCCAOP Advertisement Overview Information Element (IE) and (b) a set of MCCAOP Advertisement IEs which contain all reservations *tracked* by this STA. To set up a reservation, which may be for either individually or group addressed transmissions, a STA, called MCCAOP owner, transmits an MCCAOP setup request specifying parameters of the planning reservation. There receiver (s), called MCCAOP responder(s), checks the requested reservation for any conflict with reservations it is involved in and reservations of neighboring STAs it is aware of, and transmits a response with accept or reject code.

III. HYBRID WIRELESS MESH PROTOCOL

The key functionality of IEEE 82.11s is the wireless multi-hop routing and forwarding, which sets up transmission paths. Effective routings can provide reliable transmission paths and adapt to topology changes flexibly, so the nodes which are not within each other's communication range can also communicate with each other. The Hybrid Wireless Mesh Protocol (HWMP) is the default routing protocol for IEEE 802.11s WLAN mesh networking and it has both reactive components and proactive components. HWMP uses a common set of protocol primitives, generation and processing rules inspired by Ad hoc On-demand Distance Vector (AODV) protocol[8]. There are four message frames used in HWMP, namely path request (PREQ), path reply (PREP), path error (PERR)and root announcement (RANN). HWMP uses destination sequence numbers in order to detect outdated or stale routing information. Newly received routing information with as maller sequence number than the sequence number of the corresponding information already known to the mesh point will be discarded, because it is outdated. This avoids the creation of routing loops and problems known from classical distance vector protocols, such as "counting to infinity". .

Reactive Routing

The foundation of HWMP is an adaption of the reactive Ad hoc On-demand Distance Vector routing protocol(AODV) called Radio-Metric AODV (RM-AODV)[9].While AODV works on layer 3 with IP addresses and uses the hop count as routing metric, RM-AODV works on layer2 with MAC addresses and uses a radio-aware routing metric for the path selection. In

RM-AODV, it is assumed that each node has some mechanism to determine the metric cost of the link to each of its neighbors. In order to propagate the metric information between nodes, a metric field is used in the RREQ and RREP messages. If a source MP needs to find a route using the on demand routing mode, it broadcasts a RREQ with the destination MP specified in the destination list and the metric field initialized to 0. When a MP receives a RREQ, it creates a route to the source or updates its current route if the RREQ contains a greater sequence number, or the sequence number is the same as the current route and the RREQ offers a better metric than the current route. If a new route is created or an existing route modified, the RREQ is also forwarded (rebroadcast).Each MP may receive multiple copies of the same RREQ that originated in the source, each RREQ traversing a unique path from the source to the MP. Whenever a MP forwards a RREQ, the metric field in the RREQ will be updated to reflect the cumulative metric of the route to the RREQ’s source. After creating or updating a route to the source, the destination MP sends a unicast RREP back to the source. Intermediate MPs create a route to the destination on receiving the RREP, and also forward the RREP toward the source. When the source receives the RREP, it creates a route to the destination. If the destination receives further RREQs with a better metric, then the destination updates its route to the source to the new route and also sends a fresh RREP to the source along the updated route. Thus a bidirectional, best metric end-to-end route is established between the source and destination.

Proactive Routing

There are two mechanisms for proactively disseminating grouting information for reaching the root MP. The first method uses a proactive Route Request (RREQ) message and is intended to create routes between the root and all MP sin the network proactively. The second method uses a root Announcement (RANN) message and is intended to distribute route information for reaching the root but the actual routes to the root can be built on-demand.

1) Proactive PREQ Mechanism*:* The RREQ tree building process begins with a proactive Route Request message sent by the root MP, with the destination address set to all ones (broadcast address). The RREQ contains the distance metric (set to 0 by the root) and a sequence root, with increasing sequence numbers. Any MP hearing a proactive RREQ creates or updates its forwarding information to the root MP, updates the metric and hop count of the RREQ, records the metric and hop count to the root, and then transmits the updated RREQ. Each MP may receive multiple copies of a proactive RREQ, each traversing a unique path from the root to the MP. A MP updates its current route to the root if and only if the RREQ contains a greater sequence number, or the sequence number is the same as the current route and the RREQ offers a better metric than the current route to the root. If the proactive RREQ is sent with the "Proactive RREP" bit set to 0, the recipient MP may send a gratuitous RREP if required (for example, if the MP has data to send to the root and requires establishing bidirectional route with the root). Ift he RREQ is sent with a **"**Proactive RREP**"** bit set to 1, the recipient MP shall send a gratuitous RREP. The gratuitous RREP establishes the route from the root to the MP. When the route from an MP to a root changes, and the root RREQ was sent with a "Proactive RREP" bit set to 1, it shall send a gratuitous RREP to the root containing the addresses of the MPs which have established a route to the root through the current MP.

2) Proactive RANN Mechnism*:* The root periodically floods a RANN message into the network. The information contained in the RANN is used to disseminate route metrics to the root. Upon reception of a RANN, each MP that has to create or refresh a route to the root will send a unicast RREQ to the root via the MP from which it received the RANN. The unicast RREQ will follow the same process in rules defined in the on demand mode. The root sends a RREP in response to each RREQ. The unicast RREQ creates the reverse route from the root to the originating MP, while the RREP creates the forward route from the MP to the root. When the route from an MP to a root changes, it may send a RREP with the addresses of the MPs which have established a route to the root through the current MP.

The forced proactive mode

The proactive path reply flag is set—requires any mesh station, which receives a path request with the broadcast dress as target address, to send a PREP message to the originating root mesh STA in order to establish a bidirectional path proactively. This mode allows for bidirectional communication between a root mesh STA and any other mesh STA without falling back to reactive path establishment. However, the network overhead for sending the path replies may be significant. The RANN mechanism uses special broadcast root announcement (RANN) messages that distribute information on suitable next hops towards the root mesh STA periodically. The RANN messages, however, do not establish any paths. The actual path selection is done with unicast, single-hop path requests/path replies based on this next hop information. In this paper, the focus is on the proactive PREQ mechanisms. The RANN mechanism has not been considered due to its peculiarity. Network with the target being the broadcast address. This creates paths from all mesh stations towards the root mesh STA. The Proactive Path Reply flag, contained in such a proactive PREQ, determines whether a PREP message has to be generated or not in response to the proactive PREQ. In case the proactive path reply flag is not set, this mode is called simple proactive mode. This mode is expected to be very lean with respect to path selection overhead. However, there are only unidirectional paths from all mesh stations to the root mesh STA proactively available. If bidirectional data communication is required, the mesh STA sends a proactive PREP to the root mesh STA before it starts sending data frame sand after receiving a proactive path request as long as the data communication is ongoing. If the root mesh STA needs a bidirectional path to a mesh STA, a reactive path discovery is initiated by the root mesh STA. The forced proactive mode—the proactive path reply flag is set— requires any mesh station, which receives a path request with the broadcast address as target address, to send a PREP message to the originating root mesh STA in order to establish a bidirectional path proactively. This mode allows for bidirectional communication between a root mesh STA and any other mesh STA without falling back to reactive path establishment. However, the network overhead for sending the path replies may be significant. The RANN mechanism uses special broadcast root announcement (RANN) messages that distribution information on suitable next hops towards the root mesh STA periodically. The RANN messages, however, do not establish any paths. The actual path selection is done with unicast, single-hop path requests/path replies based on this next hop information. In this paper, the focus is on the proactive PREQ mechanisms. The RANN mechanism has not been considered due to its peculiarity.

802.11 DCF

802.11 DCF uses the Carrier Sense Multiple Access

Collision Avoidance (CSMA/CA) principle: before initiating a transmission, a station senses the state of the channel. If the medium is sensed busy, the station waits until the channel is free during a *Distributed Inter frame Space*(DIFS) interval, afterwards, it waits for an additional random contention time. The station chooses a back off time that is an integer number of time slots distributed uniformly in the contention window $[0,CW-1]$; if another transmission occurs during this procedure, the residual back off is kept for the next contention period. The value of *CW* is set to *CW* min for the first transmission attempt and it is increased in integer powers of 2 at each failed transmission (collision or frame loss) up to *CW* max (*exponential back off mechanism*).

Idle Sense

Idle Sense optimizes 802.11 DCF for high throughput and fairness: contending stations do not perform the exponential back off algorithm after collisions or failed transmissions, rather they make their contention windows dynamically converge in a fully distributed way to similar values solely by tracking the number of idle slots between consecutive transmissions. The method works as follows: each station measures *ni*, the number of consecutive idle slots between two transmission attempts. Every *max Trans* transmissions, estimates *ni*, the average of observed values of *ni*. Then, it uses *ni* to adjust its contention window to the target value i computed numerically for a given variant of IEEE802.11 PHY and MAC parameters—its value is 5.68 for IEEE802.11b and 3.91 for IEEE 802.11g [7]. When stations adjust their *CW* so that *ni* converges to *ni* target, their throughput is optimal.

The *Idle Sense* adaptation algorithm makes *ni* converge to $n_t\ t^{arget}$ by applying AIMD (*Additive Increase Multiplicative Decrease*) [9] [9] to contention window *CW* as follows:

- If $n_i \geq n_t{}^{target}$,$CW \leftarrow \alpha . CW$
- If $n_i < n_t t^{arget}$, $CW \leftarrow CW + \varepsilon$

where ε and α are some adaptation parameters. If a station observes too many idle slots compared to the target, it needs to increase *CW* additively, which in turn will decrease n_i, whereas if it observes too few idle slots, it needs to decrease *CW* in a multiplicative way, which in turn will increase n_i. We use the following values of the adaptation parameters, because they yield the best balance between accuracy and convergence for any number of contending wireless stations [6]:

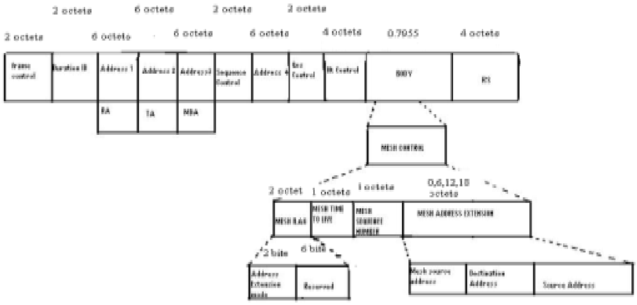
- $1/\alpha = 1.0666$
- $E = 6.0$

802.11e EDCA

IEEE 802.11e EDCA extends DCF for channel access differentiation. It offers eight traffic priorities mapped into four default access categories (AC): voice (AC VO), video(AC VI), best-effort (AC BE), and background (AC BK).AC VO has the highest priority. For each access category, an Enhanced Distributed Channel Access Function (EDCAF) contends separately for the channel. The method inherits the principles of the contention phase from DCF, but EDCAF defines its own parameter set for each access category: AIFS durations (Arbitration Inter-Frame Spaces), the minimum $CW_{\min}$ and maximum $CW_{\max}$ contention windows, and TXOP transmission opportunity limit. Like in DCF, the EDCA function of AC*j* resets the value of *CWj* to CW^{j}_{min} after a successful transmission, while after a collision or frame loss, it increases this value exponentially up to $CW_{\max}$. EDCA makes DIFS periods dependent on an access category: AIFS of a given AC is the interval during which the channel has to be idle before initiating a transmission. To support priorities between access categories, AIFS for a higher priority AC is shorter or equal to AIFS of a lower priority

AC.TXOP is another parameter of each access category: a station that wins contention can exclusively use the channel during the TXOP period so t may transmit one or more data frames separated by SIFS intervals. EDCA suffers from several performance problems [3]–[4]. In particular, it does not perform well when the number of competing stations increases, because the collision rate also increases so that the total network throughput drops. Figure 1presents an example of such a bad performance—we can observe a significant decrease in the aggregate throughput per class in a simulation of proportional differentiation with three classes (minimum and maximum contention window are $CW_1 \in [16, 48]$ for class 1, $CW_2 \in [31, 93]$ for class 2, and $CW_3 \in [61, 183]$ for class 3).

One may think that 802.11e EDCA can provide an absolute differentiation in addition to the relative one. However, it is not the case: assigning a short AIFS to the absolute priority class and a long AIFS to the lower priority one does not result in absolute differentiation, because AIFS is followed by the contention back off that still gives the lower priority class some transmission opportunity. Using short AIFS may only work, if the absolute priority class benefits from a very small $CW_{\min}$, but in this case, collision rate increases significantly for a larger number of absolute priority stations, which leads to a sharp drop in the aggregated throughput.



Frame formate of 802.11

AODV routing protocol

The AODV (Ad-hoc On demand Distance Vector) is an on-demand reactive protocol that uses the distant vector routing algorithm. In AODV, the source node and the intermediate nodes store the next-hop information corresponding to each o_w for data packet transmission. This protocol uses the messages RREQ (Route Request), RREP(Route Replies) and RERR (Route Errors).In AODV, nodes discover routes in request-response cycles. A node requests a route to a destination by broadcasting an RREQ message to all its neighbors. When a node receives an RREQ message but does not have a route to the requested destination, it broadcasts again the RREQ message. Also, it remembers a reverse-route to there questing node which can be used to forward subsequent responses to this RREQ. This process repeats until the RREQ reaches a node that has a valid route to the destination. This node (which can be the destination itself) responds with an RREP message. This RREP is unicast along the reverse-routes of the intermediate nodes until it reaches the original requesting node. Thus, at the end of this request-response cycle a bidirectional route is established between the requesting node and the destination. When a node loses connectivity to its next hop, the node invalidates its route by sending an RERR to all nodes that potentially received its RREP. The major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number (DSN) to determine an up-to-date path to the destination. A node updates its path information only if the DSN of the current61packet received is greater than the last DSN stored at the node. A RREQ carries the source identifier (SrcID), the destination identifier (DestID), the source sequence number (SSN), the DSN, the broadcast identifier (Bcast ID), and the time to live (TTL)_field. DSN indicates the freshness of the route that is accepted by the source. When an intermediate node receives a RREQ, it either forwards it or prepares a RREP if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RREQ. If a RREQ is received multiple times, which is indicated by the Broadcast ID- Scr ID pair, the duplicate copies are discarded. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send RREP packets to the source. Every intermediate node, while forwarding a RREQ, enters the previous node address and its Broad cast ID. A timer is used to delete this entry in case a RREP is not received before the timer expires. This helps in storing an active path at the intermediate node as AODV does not employ source routing of data packets. When a node receives a RREP, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination. All nodes active in the network transmit periodically hello messages (considered as special RREP messages). If one node does not receive a hello from the neighbors it means that the connection has been lost and they modify their routing table deleting that path. It also sends a RRER to the other neighbor nodes that used that path.

CONCLUSION AND RELATED WORK

We propose a novel access method that supports both relative proportional throughput allocation and absolute priorities in 802.11 wireless networks. The method is efficient, scalable, and fair. It builds on the idea of the Idle Sense method that provides the optimal throughput and fairness for 802.11 WLANs [1]: each station adjusts its contention window based on the observed average number of idle slots. We achieve absolute priority differentiation by setting the target value for the number of idle slots to a small value, so that the absolute priority class gains all the available throughput. The method also supports relative proportional throughput allocation in which several classes share the available throughput according to desired ratios.

We propose a novel access method that support both relative proportional throughput allocation and absolute priorities in 802.11 wireless network .The method is efficient, scalable, and fair. It build on idea of the idle scene method that provide the optimal throughput and fairness for WLAN each station adjust its contention window based on the observed average number of idle slots .We achieve absolute priority differentiation by setting the target value for the number of idle slots to a small value ,so that the absolute priority class gains all the available throughput. It has all desirable properties: high aggregate throughput even for a large number of contending stations, fair allocation to all stations in the same class, fast adaptation to changing conditions, and support for absolute priorities in addition to relative proportional allocation. We build upon the idea of the *Idle Sense* method that provides the optimal throughput and fairness for 802.11 WLANs [10]. The method proposed in this paper achieves absolute priority differentiation by setting the target value for the number of idle slots to a small value, so that the absolute priority class gains all the available throughput. The proposed method also supports relative proportional throughput allocation in which several classes share the available throughput according to desired ratios. We define how stations need to adjust their contention windows to achieve relative differentiation. We keep the definition of traffic classes compatible with the IEEE 802.11e standard.

Previous mesh network , its problems , Internetworking using a Mesh Access Point or a Portal is not implemented neither, but this functionality is not needed to evaluate the performance in the creation of mesh networks. The security, power safe mode and although multi-radio operation is supported, no channel assignment protocol is proposed. We propose a novel access method that supports *idle sense adaptation algorithm* give both relative proportional throughput allocation and absolute priorities in 802.11 wireless networks. The method is efficient, scalable, and fair.

REFERENCES

[1] "IEEE Draft Standard for Information Technology-telecommunications and in-

formation exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 10: Mesh Networking," IEEE P802.11s/D10.0, March 2011, pp. 1 –379, 29 2011.

[2] J. Yan, S. Zhang, Y. Sun, and H. Feng, "Performance Analysis of the IEEE802.11s Common Channel Framework," in Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on, pp. 1–4, oct. 2008.

[3] W. Pattara-Atikom, P. Krishnamurthy, and S. Baner jee , "Distributed Mechanisms for Quality of Service in Wireless LANs." IEEE Wireless Communications Magazine, June 2003.

[4] W. Pattara-Atikom, S. Banerjee, and P. Krishnamurthy, "A- DRAFT: an adaptive QoS mechanism to support absolute and relative throughput in802.11 wireless LANs." in *Proc. MSWiM'04*. ACM, 2004, pp. 117–126.HWMP.

[5] Perkins, C.E., Belding-Royer, E. M., and Das, S. R. Ad hoc On-Demand Distance Vector (AODV) Routing. IETF Experimental RFC3561, July 2003.

[6] M. Chen. OPNET Network Simulation [M]. Beijing: Tsinghua University Press April, 2004.

[7] M. Heusse, F. Rousseau, R. Guillier, and A. Duda, "Idle Sense: An Optimal Access Method for High Throughput and Fairness in Rate Diverse Wireless LANs," in *Proc. of ACM SIGCOMM 2005*, vol. 35,no. 4, August 2005, pp. 121–132.

[8] IEEE, "IEEE 802.11e: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) specifications: MAC Enhancements for Quality of Service (QoS)," January 2005.

[10] Aoki, H. et al. 802.11 TGs Simple Efficient Extensible Mesh (SEE Mesh) Proposal. IEEE P802.11 Wireless LANs, Document IEEE802.11-05/0562r0, June 2005.