Interference Avoidance in Wireless Multihop Networks

Cheng Tien Ee
Department of Computer Science
University of California, Berkeley

Scott Shenker
Department of Computer Science
University of California, Berkeley
International Computer Science Institute

Brent Chun Wei Hong
Intel Research, Berkeley

***Abstract*— In recent years there has been an increase in the types of devices that access unlicensed parts of the radio spectrum. Deployment of wireless multihop networks that use the same parts of the spectrum thus needs to account for possible external interference. Since cooperation in terms of shared medium access cannot be guaranteed, the only alternative would be to communicate on an alternate frequency. Interference can also be caused by nodes in the same network: upstream and downstream nodes of a flow can interfere with one another, a problem commonly encountered in multihop networks. We propose a medium access control scheme that uses a base channel to dynamically allocate channels on a per hop and burst of traffic basis, and that locally blacklists channels that were known to be of poor quality. An advantage of this scheme would be the statistical sharing of the total available bandwidth across all channels amongst multiple networks and types of devices. This results in bursts of traffic being better accomodated compared with static allocation of channels to each network.**

Key words: dynamic channel allocation, multihop, interference avoidance

I. Introduction

Unlicensed portions of the radio spectrum have served as a communication medium for multiple types of devices, the common ones being 802.11a/b/g, cordless phones, Bluetooth, and sensor networks. Other types of devices have been using the same parts of the spectrum for other purposes, for instance microwaves at 2.45 GHz are used to heat food, and radar in the 5.8 GHz range detect the presence of aircrafts. While there is ongoing effort to standardize the co-existence of wireless devices [2], this does not include all possible devices that can access the spectrum. Cooperation between all devices thus cannot be guaranteed, and in the presense of severe interference, the only alternative would be to switch to an alternate frequency.

The issue of external interference is not new. Bluetooth [3] utilizes fine-grained frequency hopping across 79 channels to combat the negative effects. However, packet loss can still be severely high enough to necessitate the removal of poor channels[1] from the hopping sequence. This is implemented in Bluetooth v1.2 in the form of adaptive frequency hopping. In Europe, Digital Enhanced Cordless Telecommunications (DECT) [4] is used by cordless phones in the 1.9 GHz range. DECT implements Dynamic Channel Selection and Allocation (DCS/DCA) at call connection and during the call itself to improve the quality of speech. DCS/DCA is used to ensure that calls in the same locality and time do not interfere.

A different source of interference comes from within the network itself. Multiple nodes within range of one another can attempt to transmit simultaneously, resulting in collisions. For an intermediate node acting as a router, a received packet is likely to be forwarded immediately, resulting in possible interference with further incoming packets. This has the effect of increased packet loss, as well as increasing backoffs that in turn reduces throughput.

We propose a MAC layer solution, Blackbird, that addresses these two issues. Blackbird uses dynamic, per hop, per burst of traffic channel allocation to reduce interference between upstream and downstream nodes. Also, local blacklisting of channels is carried out to avoid interfering with external devices. Whilst the main ideas behind these mechanisms have individually been investigated on before, their combined effect, especially in a multihop network encountering external interference, has not. In the following sections we briefly describe these two primary mechanisms, as well secondary ones that support them.

II. Packet Transfer

The general notion of Dynamic Channel Selection (DCS) has been around for some time [4]–[7]. Our work differs in the following areas:

- We assume that each node has only one radio that is capable of receiving or transmitting only on a particular channel at any one time.
- We consider extended periods of channel reservation, rather than for single packets. This reduces the communication overhead, as well as provide a means of determining whether a channel should be blacklisted (Section III).
- Retransmissions of packets are performed both on the current data channel, as well as on alternate channels. The latter is important for improved link-level reliability.

The primary data structure involved is the neighbor table, an entry of which is given in Table I. The table is updated whenever an RTS or CTS is eavesdropped upon, and during the course of packet transfer to the receiver.

[1] defined to be channels with high bit error rates

TABLE I

NEIGHBOR TABLE ENTRY

Entry	Purpose
addr	MAC address of neighbor
pktsToSend	total number of packets to send to this neighbor
pktsToSendBurst	current number of packets remaining in this burst
channelsInUse	channels currently in use by neighbor
waitTime	time to wait before neighbor returns to base channel
pBuffer[MAC_Q_SIZE]	queue of pointers to packets due for this neighbor
pHead, pTail	pointers to head and tail of circular queue of packet pointers
dsn	last sequence number assigned to packet due for this neighbor

We now provide a description of the packet transfer process. Assume that sender S has X packets due for receiver R. S

- checks its neighbor table and finds that R is currently idle.
- compiles a subset of the list of all free channels not in use by its neighbors, not blacklisted, and carrier-sensed to be free,
- subsequently sends an RTS to R, containing the number of packets to send, as well as the subset of free channels.

On receiving the RTS, S then

- performs flow control by checking if the total number of packets due is more than the amount of buffer available,
- finds a free channel using information from its neighbor table, as well as fast probing (i.e. carrier-sensing) of potential channels,
- responds to R with a CTS containing the channel to communicate on, as well as the number of packets to send.

The exchange of control packets takes place on the base channel, using CSMA with exponential backoff as per 802.11b [1]. Since transfer on the data channel is not expected to encounter other traffic, the maximum backoff involved is minimal and constant. After X packet transmission time has elapsed, both R and S timeout and return to the base channel.

III. CHANNEL BLACKLISTING

Blacklisting of channels is carried out to avoid future usage of a channel known to drop a significant fraction of packets. Although there are multiple ways of determining the quality of a channel, in this work we use fraction of packets sent successfully in the past as the metric. Since channels under heavy usage at one point in time may become free later, the duration of the blacklist must be bounded. A simple way of determining the bound would be to use a monotonically increasing function of the packet loss fraction.

IV. SUPPORTING MECHANISMS

We now briefly describe two supporting mechanisms, network-wide base channel determination, and neighbor support.

A. Base Channel Determination

Since the bulk of data packets transfered is on alternate channels, the base channel is not likely to be heavily loaded, and can thus operate on one with lower bandwidth. However, if the base channel is continuously jammed at a portion of the network, the nodes will need to collectively switch to a different base channel. To achieve this, we assign a preference to the channels, for instance we might prefer lower numbered channels than higher ones. In deployments, the order can be specified by some characteristic unique to a particular network, e.g. base station address. Each node periodically scans through the channels in the preferential order, exchanging a global blacklist and the current base channel with any node on the same channel. To reduce flapping between different channels, nodes do not switch to a more preferred and available channel unless the current one is blacklisted. The base channel is thus the most preferred one, that is not blacklisted, and that is less preferred than the current one.

B. Neighbor Support

Since a potential receiver R may be communicating on a different channel and not hear an incoming RTS of a potential sender S, R's neighbors can assist in informing S by responding on R's behalf. This response will inform S of the time needed before R is available to communicate. To suppress duplicate CTS, R's neighbors can backoff for random periods of time, and keep quiet upon hearing another's CTS.

V. CURRENT AND FUTURE WORK

Blackbird is currently being implemented on MicaZ sensor motes, extending the 802.15.4 standard. It is anticipated that the basic ideas behind Blackbird can be applied to any multi-hop networks capable of channel switching. In the near future performance evaluation, using metrics such as packet loss, throughput and latency, will be carried out. Also of importance is the comparison between static allocation of channels to each co-located network and the dynamic scheme proposed in our work.

REFERENCES

[1] ANSI/IEEE, "802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[2] IEEE 802.19 Coexistence Technical Advisory Group (TAG), http://grouper.ieee.org/groups/802/19/

[3] Bluetooth, http://www.bluetooth.org/

[4] Digital Enhanced Cordless Telecommunications (DECT), http://www.dect.org

[5] N. Jain and S.R. Das, *A Multichannel MAC Protocol with Receiver-Based Channel Selection for Multihop Wireless Networks*, In Proceedings of the 9th Int. Conf. on Computer Communications and Networks (IC3N), Phoenix, Oct 2001.

[6] J. So and N. H. Vaidya, *A multi-channel mac protocol for ad hoc wireless networks*, Technical report, Dept. of Comp. Science, Univ. of Illinois at Urbana-Chamapign, 6, 2003.

[7] S.-L. Wu, C.-Y Lin, Y.-C. Tseng and J.-P. Sheu, *A New Multi-Channel MAC Protocol with On-Demand Channel Assignment for Multi-Hop Mobile Ad Hoc Networks*, Int'l Symp. on Parallel Architectures, Algorithms and Networks (I-SPAN), 2000, pp. 232-237.