IA-MAC: Interference Aware MAC for WLANs

Daniela Maniezzo, Matteo Cesana, Mario Gerla
Computer Science Department,
University of California, Los Angeles, CA 90095-1596, U.S.A.
dmaniezzo@ieee.org; {cesana, gerla}@cs.ucla.edu

UCLA-CSD Technical Report Number 020037

December 11, 2002

Abstract

Among the numerous standards for wireless communications, the IEEE 802.11 Wireless Local Area Network is the one with the highest utilization at the moment. The 802.11 has been devised explicitly for low mobility, single access point scenario, so its effectiveness can be limited when it is utilized both in ad hoc mode and with multiple access points. Many research has been done and is still ongoing aiming to face well known problems typical of these scenarios like the exposed/hidden terminal cases. In this technical report we propose a novel MAC layer for Wireless LAN which is able to extend the capabilities of the basic IEEE 802.11 DCF (Distributed Coordination Function) to environments with high interference, both in ad hoc and in infrastructured mode.

1 Introduction

Wireless Networking is one of the fastest growing areas both in scientific research and in industry. In wireless communications the physical media is subject to errors and temporary failures which are not encountered in the wired world. Furthermore, media is shared and resource are often scarce. In this scenario the employed access control schemes get an enormous importance and together with routing level is a key point for achieving QoS.

Among the numerous standards for wireless communications, the IEEE 802.11 Wireless Local Area Network is the one with the highest utilization at the moment. In 1997, the IEEE adopted the first standard for WLANs and revised it in 1999. The actual standard, implemented in many wireless card, is the 1999 version. IEEE defines a MAC (Medium Access Control) sublayer, MAC management protocols and services, and three physical (PHY) layers respectively based on IR, FHSS at 2.4 GHz and DSSS at 2.4 GHz.

The goal of the standard is to deliver within mobile users services previously found only in wired networks, with high throughput, highly reliable data delivery and continuous network connection.

The 802.11 MAC DCF (Distributed Coordination Function) is the standard for both infrastructure and ad hoc wireless LAN (Local Area Network) [1, 2]. For unicast data packet transfer, IEEE 802.11 defines two access methods. The first one is based on a two-way handshake procedure (DATA/ACK), the second one adopts a four-way handshake procedure, where the DATA/ACK phase is preceded by a channel probing phase called RTS/CTS (Request To Send/ Clear To Send).

Both of the access methods use a multiple access scheme based on carrier sensing with collision avoidance (CSMA/CA). Basically, each node senses the channel before transmitting the first frame of the handshake; if the channel is sensed idle for a certain period of time called DIFS (Distributed Inter Frame Space), the node starts transmitting the first frame of the handshake immediately. Otherwise the nodes waits for the channel to be idle for DIFS and draws a random additional backoff time to avoid possible collisions when the channel gets free (Collision Avoidance).

Even if 802.11 is the official standard for Wireless LAN's both in infrastructure and in ad hoc mode, originally it was devised only for a single Access Point scenario where all the nodes were within the transmitting range of one another. For this reason, many problems arise when we use 802.11 both in a pure ad hoc mode and in a infrastructured cellular-like scenario where we have different APs and mobile nodes moving around [3].

IEEE 802.11 also employs a mechanism called virtual carrier sensing. Each transmitted frame brings the information about the duration of the ongoing communication. Every other node overhearing that frame is prevented from accessing the media for all the duration of the ongoing communications by setting its NAV (Network Allocation Vector).

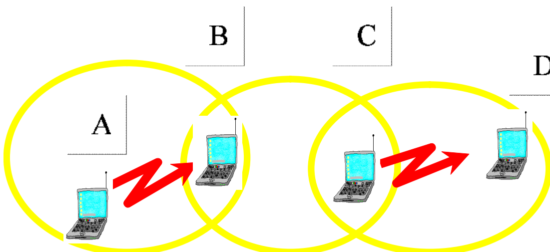

Figure 1: Hidden Terminal Example

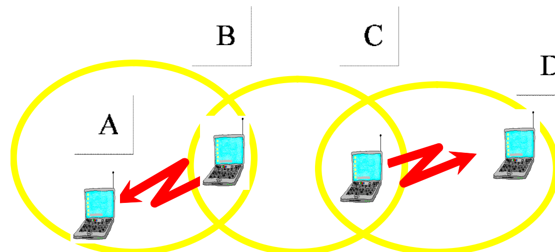

Figure 2: Exposed Terminal Example

Well known problems in these environments are the hidden and the exposed terminal [4]. Figure 1 reports a typical hidden terminal situation where there's an ongoing communication between A and B. If C does not have any information about the communication between A and B, it can start transmitting to D causing a collision in B. In order to get rid of the hidden terminal problem, the standard has introduced the four way handshake procedure based on RTS and CTS. In the case of the figure, C overhears the CTS B sends to A and refrains from transmitting and colliding.

In Figure 2 the exposed terminal problem is described. A node is exposed when is within the sensing range of the sender but out the interfering range of the receiver. In the case of the figure, supposing on ongoing communication between B-A, every communication involving C is not feasible, since C is in the zone cleared by the RTS sent by B, even if C could transmit to D without causing any collision.

The exposed terminal problem is still unsolved and can deeply affect the performances of multi hop ad hoc networks based on IEEE 802.11 [5].

Different solutions have been proposed to face such problem. Most of them are based on a wise sharing of the common resource between different communications based on the management of the numerous timers the IEEE 802.11 MAC level has [6, 7].

In this technical report we propose a novel MAC layer for Wireless LAN which is able to extend the capabilities of the basic IEEE 802.11 to environments with high interference, both in ad hoc and in infrastructured mode [8, 9].

2 Interference Aware MAC Basics

The basic idea is to propose minimal modifications to the IEEE 802.11 MAC DCF in order to make feasible multiple parallel communications in an interference scenario. The 4 way handshake working mode is considered, where all the transmissions happen with a fixed power level.

First step, we propose to deactivate the physical Carrier Sensing by setting an high value of capture power. In this way, each node would recognize the channel as busy only if highly overloaded. Second, we propose to modify the CTS packet including an information on the Signal to Interference Ratio (SIR) measured by the CTS sender. All the mobile nodes receiving a RTS should include in their CTS the explicit information of the experimented SIR which is simply the ratio of the power received on the RTS and the perceived interference level. All the other mobile nodes in the communication range, aiming to start their own transmissions, overhear the CTS and decide whether to start transmitting or refraining on the basis of the SIR information coded in the CTS. More in details, they refrain from transmitting if they estimate that the SIR at the receiver of the ongoing communication would fall beyond a certain threshold.

Let's refer again to figure 2 to explain the proposed algorithm with an example. Let P_{RTS} be the power received by B on the RTS sent by A, and let I_r be the interference level perceived by B. B inserts in its CTS the information of the Signal to Noise Ratio it experiences $SIR_B = \frac{P_{RTS}}{I_r}$ and of the power received by A, P_{RTS}. C overhears the CTS sent by B and estimates the SIR B would get if it started transmitting according to the formula:

$$SIR_{ext} = \frac{P_{RTS} SIR_B}{P_{RTS} + P_{CTS} SIR_B}$$

where P_{CTS} is the power C receives on the CTS sent by B. If SIR_{ext} is below a certain threshold (3,6 dB), C refrains from transmitting and set its NAV otherwise sends its own RTS.

IA-MAC can be useful both in ad hoc mode and in infrastructured one. In the former case, as we argued above, it can be a partial solution to the exposed terminal problem, granting a good gain with respect to the basic MAC mechanism. As far as concerned the latter case, let's consider a scenario where different 802.11 Access Points cover different adjacent areas. In this situation many communication from and towards an Access Points can be blocked by the interference generated by ongoing communications in adjacent cells, limiting the throughput. IA-MAC can easily deal with this situations.

The impact of the proposed modifications on the actual deployed IEEE 802.11 standard seems to be minimal. As a matter of fact The modification to the standard needed are minimal. Three bits of the CTS (8 levels) packet should be used to transfer the information about the perceived SIR. We suggest the use of three bits of the Duration Field (DF) of the CTS packet. Furthermore, with few modifications, the proposed algorithm can be applied also to scenarios where the transmitted power is not uniform between different communications.

3 Simulation Results

We used Qualnet [10] to evaluate the performance of the IA-MAC. In deatils, we introduced the proposed modifications in the Qualnet implementation of the IEEE 802.11 DCF. Figure 3 and 4 report preliminary results obtained in the simulation scenario described in table 1.

Parameter	Value
Number of nodes	50
Testbed Area	1000mX1000m
SNR Threshold	6dB
Transmission Power	15 dB
Fading Model	Rice
Traffic Model	CBR
Inter-arrival Time	exponential
Duration Time	exponential
Simulation Time	200s

Table 1: Simulation parameters.

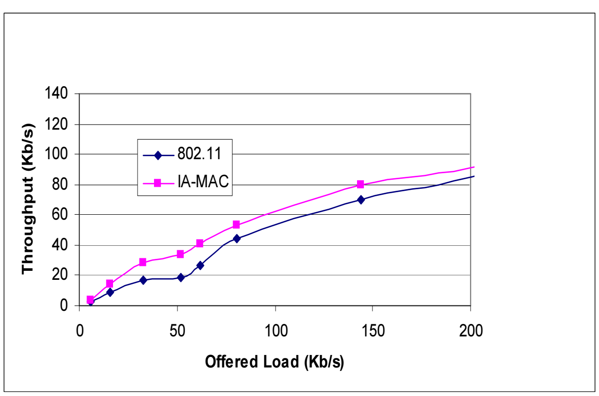

Figure 3: Throughput versus offered load.

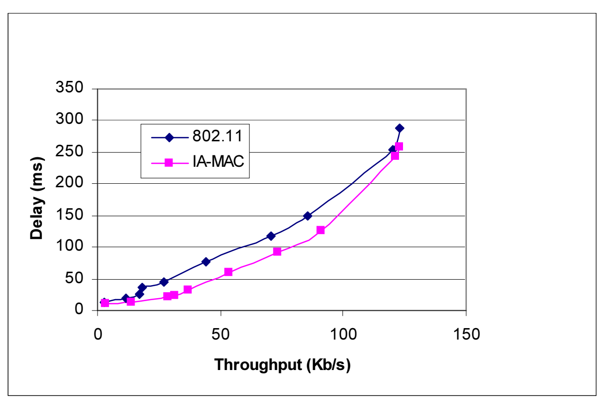

Figure 4: Average delay versus achieved throughput.

In particular, figure 3 gives the curves of throughput as a function of the offered load both for the basic 802.11 DCF and for the proposed IA-MAC. The proposed scheme achieves higher throughput with respect to the basic one at low loads. As the network gets congested the two schemes perform similarly.

Figure 4 reports the average packet delivery delay versus the achieved throughput. Two results come from this figure: firstly the IA-MAC can reach a given value of throughput granting lower delays, second given a certain target delay the IA-MAC can achieve an higher throughput value with respect to the IEEE 802.11 DCF.

4 Conclusions and Research in Progress

In this technical report we presented a novel MAC layer for wireless LANs named IA-MAC, Interference Aware MAC. IA-MAC permits parallel 802.11 communications and solves partially the problem of the exposed terminal in the ad hoc mode. The preliminary results we obtained show that IA-MAC grants a good gain in term of throughput with respect to the basic IEEE 802.11 in a medium-low network load situation and definitely grant lower packet delivery delays.

Further experiments have been planned to test the performance of the IA-MAC in different topological scenario, both in ad hoc mode and in infrastructure mode. We expect the proposed MAC to show very useful in a multiple Access Point scenario, where different Access Points cover overlapping cells in a cellular-like topology.

References

[1] IEEE Standard 802.11, *Wireless LAN media access control (MAC) ans physical layer (PHY) specifications*, 1999.

[2] http://grouper.ieee.org/groups/802/11/

[3] Haitao Wu, Shiduan Cheng, Yong Peng, Keping Long, Jian Ma, *Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?*, IEEE Communication Magazine, June 2001.

[4] Haitao Wu, Shiduan Cheng, Yong Peng, Keping Long, Jian Ma, *IEEE 802.11 distributed coordination function (DCF): analysis and enhancement*, ICC 2002.

[5] C.C. Chow, V.C.M. Leung, *Performance of IEEE 802.11 medium access control protocol over a wireless local area network with distributed radio bridges*, WCNC 1999.

[6] V. Bharghavan, *MACAW: a Media Access Protocol for Wireless LAN's*, SIGCOMM, 1994.

[7] F. Talucci, M. Gerla, L. Fratta, *MACA-BI (MACA By Invitation)-a receiver oriented access protocol for wireless multihop networks*, PIMRC 1997.

[8] K.K. Leung, B. McNair, L.J. Cimini, J.H. Winters, *Outdoor IEEE 802.11 cellular networks: MAC protocol design and performance*, ICC 2002.

[9] P. Gupta, P.R. Kumar, *The capacity of wireless networks*, IEEE Transactions on Information Theory, Volume: 46 Issue: 2 , March 2000 Page(s): 388 -404.

[10] http://www.qualnet.com/