Performance Study of Access Control in Wireless LANs - IEEE 802.11 DFWMAC and ETSI RES 10 HIPERLAN

Jost Weinmiller, Morten Schläger, Andreas Festag, Adam Wolisz*
Technical University Berlin, Sekr. FT5-2, Einsteinufer 25, 10587 Berlin, Germany
**also with STEP GMD-Fokus*
[jost, morten, festag, wolisz]@ee.tu-berlin.de

Abstract

[1] *Currently two projects are on their way to standardize physical layer and medium access control for wireless LANs - IEEE 802.11 and ETSI RES10 Hiperlan. This paper presents an introduction to both projects focussing on the applied access schemes. Fyrther we will present our simulation results, analyzing the performance of both access protocols depending on the number of stations and on the packet size, evaluating them regarding their capability to support QoS parameters, regarding the impact of hidden terminals and their range extension strategy.*

1 Introduction

Wireless LANs (WLANs) are expected to be a major growth factor for the network industry in the upcoming years. They will be used as an extension of the wired network with a wireless last link to attach the large number of mobile terminals. Currently only proprietary solutions are available mostly operating in the license-free 900 MHz or 2.4GHz frequency bands. In order to enable multivendor interoperability and thus avoiding limitations of mobility due to technical boundaries, standardization is on its way in two working groups specifying physical layer (PHY) and media access control (MAC) for wireless LANs. The IEEE 802.11[1] working group has delivered its IEEE standard for approval later in 1996, the ETSI RES 10 Hiperlan[2] specification is expected to be finished some months later.

Our focus in this paper will be on the performance of the access control protocols that the two working groups agreed upon, with respect to their particular system environments, as they have been defined in both projects. Based on a simulative study we will analyze the performance characteristics and discuss problems of the two access schemes. We will start by describing the environment, in which wireless LANs are expected to operate and elaborate the problems for access protocol design that arise from this setup. Further we will present the simulative analysis and discussion of both systems regarding several key criteria like influence of number of active stations, support for quality of service parameters, vulnerability to hidden terminals and strategy to extend the connectivity area. The paper is finished by conclusive remarks.

[1]This Work has been supported by a grant from the DFG (Deutsche Forschungs Gemeinschaft) within the Priority Program Mobile Communications

2 Issues in Designing WLANs and Wireless Access Schemes

Both the working groups IEEE 802.11 and ETSI RES 10 have targeted their work to the physical layer and the medium access control sublayer for wireless LANs, in order to remain within the IEEE 802 LAN framework. The two projects address wireless LANs operating at 2.4GHz (IEEE) and 5.2GHz (ETSI), respectively. The protocols are developed for a number of slowly moving stations (Hiperlan limits the station speed to <10m/s), usually indoor, with communication either among each other without any supporting infrastructure (ad-hoc mode) or with support of an infrastructure and its services over a central station (infrastructure mode). The communication is packet oriented, the generated traffic may or may not require the support of quality of the service (QoS) guarantees by the WLAN. The QoS-parameters considered are bandwidth reservation and transmission delay constraints, e.g. for time bounded voice- or video traffic. In order to implement the different traffic classes, user priorities are needed, that have to be mapped onto MAC-layer priorities. Furthermore both projects have suggested some concept to provide connectivity beyond radio range of a single station (Hiperlan defines a radio range of ~50m). In order to protect the limited power of the battery driven mobile hosts as far as possible, power saving functionality is a necessary feature of a WLAN concept, however it is not the primary area of interest of this paper and only touched where necessary.

Several key problems arise with the different nature of the wireless medium: One of the main media-dependent differences between future WLANs and the well known wired LANs is the inability to listen while sending since (usually) just one antenna is available for both sending and receiving. This makes collision detection more difficult, as the commonly applied collision detection algorithms rely on continuous monitoring of the medium. When switching between the two circuits responsible for either task, the interface will not be able for either sending or receiving for a certain time causing a limited "mute-deaf-time". This so called Rx/Tx-turnaround-time has significant influence on the design of the MAC layer, since most access control schemes rely on either sending or receiving of signals, which cannot be exchanged in WLANs faster than Rx/Tx-turnaround. Another problem concerning collision detection in WLANs is caused by the "hidden terminal problem". A station, that may not be within receiving range of a sending station and thus senses the medium idle may however well be within sending range of the receiver of that ongoing communication and may thus cause a collision of two signals there, if it starts transmitting itself. Since this collision may not be detected at the sender (it is sending and thus not listening) any reliable collision detection functionality at the sending side is impossible (section 5.5 discusses this problem in further detail). Opposed to this is the "exposed terminal scenario", where a station may sense the medium busy, since it is within range of a sender and thus it refrains from sending. However the target for its transmission may be well outside the range of the other sending station and would normally be able to receive and understand the nearer signal. This scenario does not cause serious performance degradation and is therefore tolerated. Other relevant different characteristics of wireless communications compared to their wired counterparts are different received signal power from individual stations and higher error rates compared to wired medium, partially caused by interference among co-located WLANs, self interference, self collision or up-down collision.

MAC protocols can be roughly categorized into fixed assignment (e.g. TDMA, CDMA, FDMA), random assignment (e.g. ALOHA, CSMA/CD, CSMA/CA) and demand assignment protocols (e.g. Token Ring, PRMA, DAMA). Fixed assignment protocols lack the flexibility in allocating resources and allowing frequent configuration changes. This makes them seem unsuitable for wireless packet data networks. Demand assignment schemes attempt to combine the flexibility of random assignment and the deterministic behavior of fixed assignment. Due to the particularities of the wireless media however (e.g. lacking isolation of the media, non-directed transmission, no fixed location of terminals) special effort is needed to be able to implement some of the needed logical topologies. Token based schemes for example rely on the knowledge about the network configuration, in a way that each station needs to know what stations are currently its neighbors. This however is constantly changing in wireless networks or maybe not even unambiguous. This kind of flexibility is inherently present in random access systems which is why both the WLAN-standards in question have decided on a random access scheme that shows stochastic bandwidth allocation behavior. Random access allows unconstrained, unrestricted motion of the mobile host into, within and out of a radio cell, however the price for this is non-deterministic behavior that causes problems in supporting QoS guarantees. In order to better meet those requirements, one of the two projects (IEEE 802.11) has integrated a centralized mode that offers a demand assignment scheme.

3 Simulation Goals and Simulation Environment

With the above discussed issues for WLAN MAC protocol design in mind we have identified several key issues in evaluating the performance of the protocols. First we evaluated the performance in general scenarios, that were targeted by both projects. We evaluated the applicability in ad-hoc networks with respect to the number of active stations and the offered load. We put our next focus on the capabilities to support QoS parameters. Further we looked at two issues of special importance in WLANs: the dependency on the size of the data units and at the hidden terminal vulnerability. Finally we discuss the solutions, that have been suggested for range-extension.

For our simulations we used PTOLEMY [3], an object oriented simulation tool, developed at the University of California Berkeley which proved suitable for our intentions due to its ability for concurrent process oriented simulations. We simulated a WLAN that uses either IEEE 802.11 DFWMAC or ETSI Hiperlan EY-NPMA as the access scheme. In our channel model for the wireless channel we can set attenuation as a function of distance and the attenuation coefficient, propagation delay, Poisson distributed packet loss, carrier sense threshold and the size of the picocell.

The distribution of the packet sizes is taken form a trace file, that contains the arrival times and corresponding packetsizes of an ethernet and that has been recorded over 24 hours at Bellcore Morristown Research Institute[4]. This setup is similar to the one described in [5]. The preference of using trace files for the packet size comes from the fact, that local and wide area traffic has been found not to be Poisson distributed but rather selfsimilar[6],[7]. The packet interarrival times however are exponentially distributed in order to be able to define different load conditions, since the trace file only represents one particular load condition. The

average packet size of the tracefile is 432byte, before MAC header and physical header are added. Figure 1 shows the packet size distribution of our trace file with its (ethernet-type) bimodal mixture of 64 byte and 1500 byte packets.

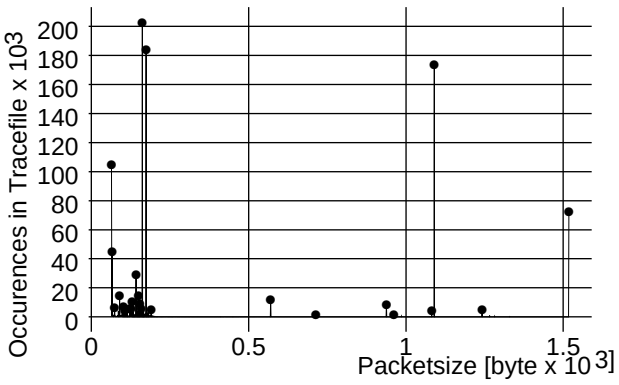

Figure 1: Packet Size Distribution of Tracefile

The "Load" in our figures represents "offered load". However since we have implemented our packet sources with a limited queue we get a finite delay even under very high load. Our model also contains a time-bounded packet sources in order to simulate traffic with QoS requirements, that are generating traffic at a given constant rate or at a random constant rate.

If not stated otherwise no hidden terminals were simulated. For 802.11 we chose to use the parameter set for the frequency hopping spread spectrum physical layer (SIFS=28usec, DIFS=128usec, backoff slottime=50usec, physical preamble=122bit) at the optional 2Mb/s transmission rate.[2] In our Hiperlan model we considered the protocol overhead introduced by the channel access sublayer and the physical layer overhead.

4 Overview over the Draft Standards

Since the new draft standards are not widely known yet we will start with a brief overview over both the standards in question mostly focussing on the elements that are relevant for the understanding of the MAC protocol.

4.1 IEEE 802.11

The 802.11 draft standards consist of three main parts, the physical layer specification, the medium access control specification, and the power saving functionality that operates on both layers. An 802.11 WLAN may be operated in two working modes - ad-hoc mode where just peer-to-peer communication between mobiles takes place and infrastructure mode where a supportive infrastructure may be accessed over a base station. In infrastructure mode either a contention service with stochastic bandwidth sharing is accessible to the mobiles by using the distributed coordination function (DCF), or a contention free service with possible support for limited delay guarantees may be used by using the point coordination function (PCF). Both coordination modes coexist simultaneously within a (time-multiplex-) superframe structure.

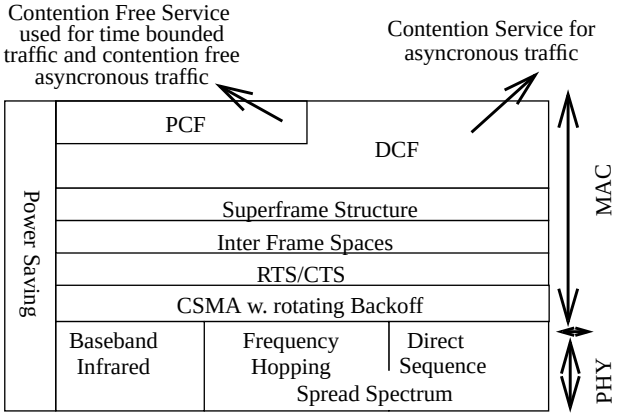

Figure 2: System Architecture IEEE 802.11

The two coordination modes use two different access schemes - a polling based reservation scheme for the point coordination and a CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) algorithm with rotating backoff [3] for the distributed medium sharing. Optionally the basic access scheme can be extended with the RTS/CTS mechanism to increase robustness against hidden terminals. Figure 2 shows the elements in 802.11 and the services offered as well as their relation towards each other. They will be described below.

The Physical Layers

The IEEE 802.11 draft standard specifies three different physical layers, each applying to a different kind of transmission technology. One layer applies baseband-infrared transmission (IR), the two others apply radio based direct-sequence spread-spectrum (DSSS) and frequency-hopping spread-spectrum (FHSS) technology. All 802.11 compliant devices using any of the three technologies are required to operate at 1 Mb/s data rate, optionally 2 Mb/s may be supported. The

[2] Looking at the simulations in figures 3 and 4 one can assume, that the results for the other physical layers will not differ qualitatively and will only slightly differ quantitatively

[3] after a station lost a competition for access it freezes its backoff counter and only has to wait the reduced backoff time in the following cycle, in order to get an increased possibility of gaining access

maximal size of a MSDU is 2312 octets (MAC payload without the MAC header and the physical preamble). Each physical layer adds a physical preamble of different length to each packet. Infrared adds 92-112 timeslots of 250ns + 32 bit, direct sequence 192 bit [4]. and frequency hopping 122 bit. A couple of physical-layer-dependent parameters have relevant influence on the design of the MAC protocol. First to mention is the Rx/Tx turnaround time, that varies from 0 usec for infrared, 10 usec for direct sequence to 19usec for frequency hopping. Since this time length not only influences the interframe spaces but also the length of the backoff slots in the contention window (see 4.1), it causes significantly different performance of the MAC protocol on top of the 3 physical layers. Each slot in the backoff window therefore has the length of 6usec(IR), 20usec(DS) and 50usec(FH). It becomes obvious, that the resulting performance will be highly dependent on the type of applied physical media.

This can be seen in Figure 3 where we show the simulated throughput and in Figure 4 showing the simulated mean access delay, in a general configuration setup (8 stations, no hidden terminals, trace file based packet size distribution, Poisson distributed packet arrival times) for the 3 different physical layers.

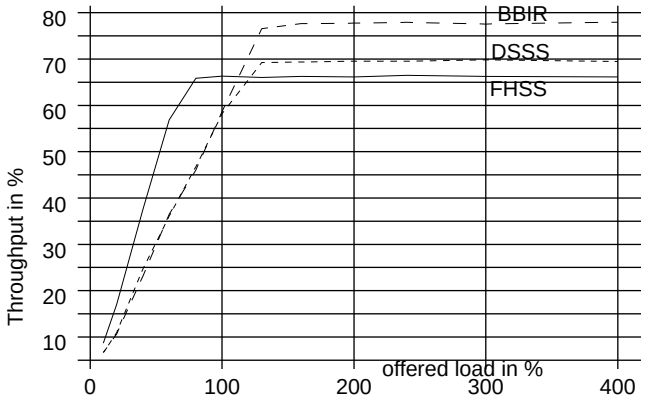

Figure 3: Throughput for different Physical Layers IEEE 802.11

The larger time constants for frequency hopping result in a smaller throughput and a larger access delay, whereas the opposite is true for infrared. The advantage of infrared compared to the two other schemes however has to be seen in the context of disadvantageous characteristics for infrared transmission. The limitation of this technology to only indoor use with just 10-20m radius without propagation through walls and almost no propagation through windows severely limits the number of suitable installation environments.

[4]This physical preamble may not be transmitted at 2Mb/s, if direct sequence is applied,- only the MPDU may use the faster rate

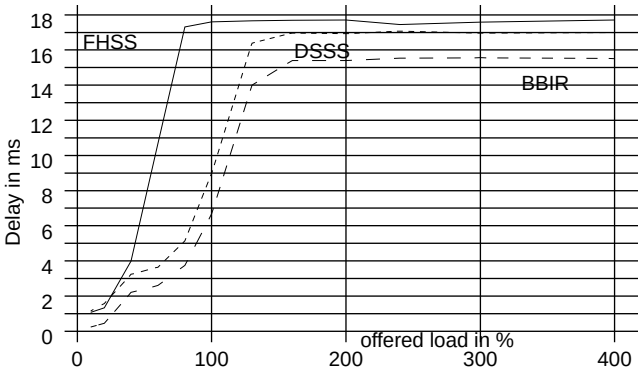

Figure 4: Mean access delay for different Physical Layers IEEE 802.11

Inter Frame Spaces

In order to separate the different types of packets, different levels of access priority are implemented by defining 3 interframe spaces (IFS) of different length. They define the minimal time, that a station has to let pass after the end of a packet, before it may start transmitting a certain type of packet itself. After SIFS (Short IFS), the shortest interframe space, only acknowledgments, CTS- (see section 5.5) and DATA-frames in response to a poll by the PCF may be sent. After PIFS (PCF-IFS), any frames from the contention free period may be sent in PCF-mode, after DIFS (DCF-IFS), the longest of the 3 IFS, all frames in DCF-mode may be sent asynchronously. This use of IFS allows the most important frames to be sent without any additional delay and without having to compete for access with lower priority frames. It allows the prioritized access to the medium for point coordination mode over the contention mode frames in distributed coordination mode.

802.11 Access Scheme

As explained before two access schemes are used in IEEE 802.11, one for point coordination and one for distributed coordination. In DCF, access is organized by applying a CSMA/CA scheme called DFWMAC (Distributed Foundation Wireless MAC). The access control scheme is shown in Figure 5. A station that intends to transmit and senses the channel busy will wait for the end of the ongoing transmission, then wait for a time period of DIFS length, and then randomly selects a time slot within the backoff window. If no other station started transmitting before this slot is reached (i.e. another station that selected an earlier slot) it starts its own transmission. Collisions can now only occur in the case that two stations selected the same slot. If another station selected an earlier slot, the station freezes its backoff counter, waits for the end of this transmission and now only waits for the slots remaining from the previous competition.

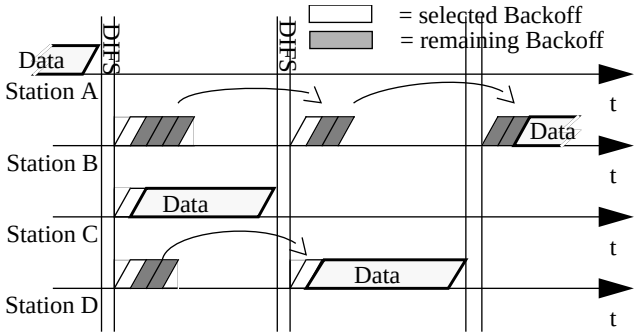

Figure 5: Backoff procedure in DFWMAC IEEE 802.11

This basic access mechanism can optionally be extended by the RTS/CTS (Ready To Send / Clear To Send) message exchange in order to guarantee undisturbed transmission even if hidden terminals are present (See section 5.5 for a description of the RTS/CTS mechanism). To justify the additional overhead the usage of the RTS/CTS message exchange in DFWMAC has been made dependent of the size of the payload of the packet to be transmitted.

Point Coordination and Power Saving

The service offered by DCF is a contention service, that is used for asynchronous traffic. This service does not guarantee any boundaries for access delay or available bandwidth. In order to also offer contention free service for time bounded traffic or contention free asynchronous traffic the point coordinated mode PCF may also be used on top of DCF. In point coordinated mode both services are available, - the two coordination modes share the bandwidth available in a superframe structure (see Figure 6). After the PCF-part in the superframe, the PCF passes control to the DCF and regains control of the bandwidth once the DCF-part is over. The PCF part itself is offering both a time bounded service based on a requested rate and a contention free service for asynchronous data.

In PCF mode the central coordination station polls stations, that are on its polling list and allows them undisturbed, contention free access to the medium. To get on the polling list, either once or repeatedly, the stations have to apply during DCF period at the point coordinator.

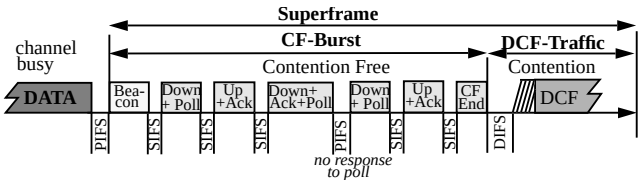

Figure 6: PCF and DCF integration IEEE 802.11

To enable power saving functionality two states are defined: *awake and doze*. If a station is in doze-state, it may turn off its power for most of the time. It polls the base station at predefined times to check for waiting packets. To enter doze-state a station has to notify the base station first. We have examined the power saving functionality, its dependancies and effect on the overall performance in a not yet published technical report.

4.2 ETSI RES 10 Hiperlan

The Hiperlan project has defined a system architecture as shown in Figure 7. On top of the physical layer specification a separate sublayer has been integrated, containing the channel access mechanism. This mechanism is used by the different functional entities, offering different MAC-services.

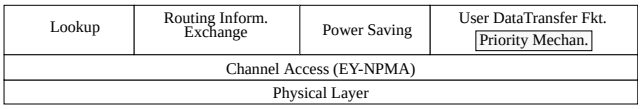

Figure 7: System Architecture Hiperlan

In order to be able to support forwarding of packets to stations outside of radio range of the sender with the help of supporting stations (forwarder), a routing information exchange functionality is present. A lookup functionality is added to enable collocated operation of distinct WLANs. Optional encryption/decryption may be used, however the mechanisms applied are not specified. 2 MAC-user priority classes are supported, that are mapped onto 5 channel priorities.

ETSI RES10 - Physical Layer

The physical layer allows a Hiperlan to select one of five independent channels within the allocated bandwidth. While channel 1 to 3 are license-free in any country, channel 4 and 5 are not globally available. The channel transmits data at two different datarates - a low datarate (1,4706Mb/s), that is used to transmit acknowledgment packets and the packet header, and a high datarate (23,5294 Mb/s) to transmit the data packet itself. The physical layer adds to the MPDU the low rate header, 450 high rate bits for synchronization and training sequence, n*496 high-rate bits payload coded with BCH(31,26) and a variable number of bits for padding. The selection of a new channel and the changing of the carrier must not take more than 1ms. The Rx/Tx Turnaround time is limited to <5usec.

Priority classes

Although the Hiperlan draft standard does not define different priority classes for the various traffic classes like multimedia or file transfer it supports time

bounded delivery of packets. This task is performed by assigning channel access priorities dynamically to the packets. The channel access priority depends on the normalized residual MSDU lifetime (NRMT) and the assigned user priority. The MAC-User has to assign a lifetime and a user priority to every data packet. The NRMT is the ratio of residual lifetime and the distance between source and destination in hops. Thus the priority of each packet increases while its lifetime expires. In each access cycle only packets with the same access priority compete for the channel since the access mechanism guarantees hierarchical independence of performance between packets with different channel access priorities.

NRMT ms	High User Prio	Low User Prio
> 80	4 (lowest)	4 (lowest)
40<X<80	3	4
20<X<40	2	3
10<X<20	1	2
<10	0(highest)	1

Hiperlan Access Mechanism - EY-NPMA

In Hiperlan a station seeking access listens to the channel for a certain time period (channel free condition, 1700 high-rate bit duration). If it doesn't catch any ongoing transmission it is allowed to start tranmitting without any further processing. This reduces protocol overhead under low load condition, however with load higher than 30% the condition criteria is hardly ever fulfilled. If another transmission is heard the full MAC protocol path has to be taken. EY - NPMA (Elimination Yield - Non-preemptive Priority Multiple Access) has been chosen to be the MAC protocol for Hiperlan. It offers a mechanism, that requires a minimal number of Rx/Tx-turnarounds, while still resulting in a single winning station with high probability (97.8% [9]). Features of this access scheme are:

- No preemption by frames with higher priority after the priority resolution possible
- Hierarchical independence of performance
- Fair contention resolution of frames with the same priority

The access mechanism is split into 3 phases (see Figure 8): *Priority Resolution*, *Elimination* and *Yield phase*. In the first phase, a station seeking access to the media listens to the medium until the priority slots of the higher priorities have passed idle. If the channel was idle for p-1 priority slots only the stations with the same highest priority survive.

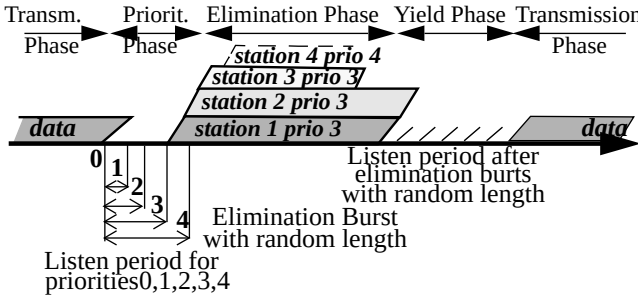

Figure 8: EY-NPMA Access Scheme Hiperlan

In the second phase every surviving station transmits a burst with a random length, bounded and defined by a certain discrete probability distribution. After this the station listens to the channel for an Elimination Survival Verification Period (ESVP). If another station sends a burst of longer duration, i.e. the station notices a signal after it stopped transmitting itself, the station withdraws from transmission. At least one station survives after this phase. The duration of this listening period (yield phase) once again has random length. If a station hears another station starting its transmission before its own yield phase is over, it stands back from transmission - If not it transmits immediately the data frame after the yield period.

Power Saving

The Hiperlan draft standard supports power saving in two ways. First of all the low rate header of each packet allows the receiver to determine whether it is the destination for the packet or not before it has to turn on the power consuming equalizer. Second, a node can save power by receiving packets only at prearranged moments instead of continuously. Hiperlan power conservation is achieved by an implicit bilateral agreement between a node conserving power (p-saver) and a node deferring transmissions (p-supporter). This agreement is defined by the declaration and transmission of active wake patterns.

Hiperlan Identifier and LookUp

Each Hiperlan assigns itself a certain identifier to distinguish itself from other Hiperlans. The look-up functionality is used to explore the communication environment. A new Hiperlan can be created by choosing an identifier which is not in current use in the communication environment. An already existing Hiperlan can be joined by just using its identifier, it is left by refraining from using its identifier, it is destroyed when no more HM-entity uses its identifier.

5 Simulation Results

5.1 Ad-Hoc Networks

Our first simulations intend to show the performance, that can be expected from both protocols with respect to the number of stations, that are active in a picocell. Figure 9 shows the network throughput with increasing load for different numbers of sender in an ad-hoc network.

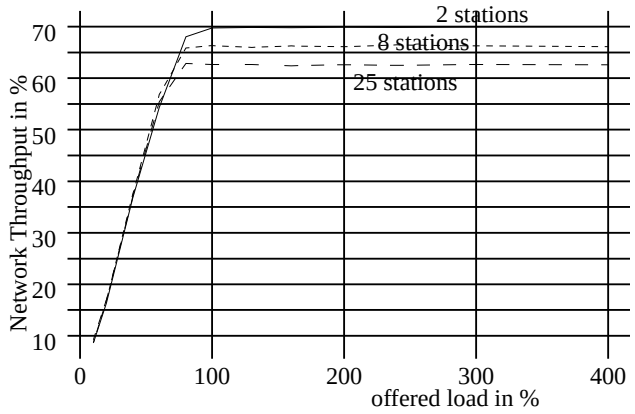

Figure 9: Throughput for 2, 8, 25 stations IEEE 802.11

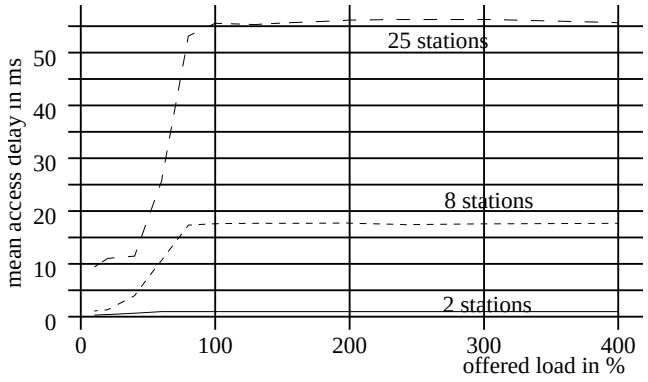

Figure 10: Delay for 2, 8, 25 stations IEEE 802.11

One can see, that the overall network throughput decreases with increasing number of sending stations. The achievable throughput per station is reduced even more since the smaller overall available throughput has to be shared among more stations.

Parallel to the decreasing throughput one can see quite obviously an increase in the mean access delay, as shown in Figure 10. We observe the same effect, when we simulate an increasing number of stations in Hiperlan - the overall network throughput decreases with more stations being active (Figure 11).

However, compared to 802.11 the higher datarate in Hiperlan results in a larger available bandwidth for each station. E.g. if 8 stations are active, each station in 802.11 gets 8,25% of 2Mb/s equalling 165 Kb/s,

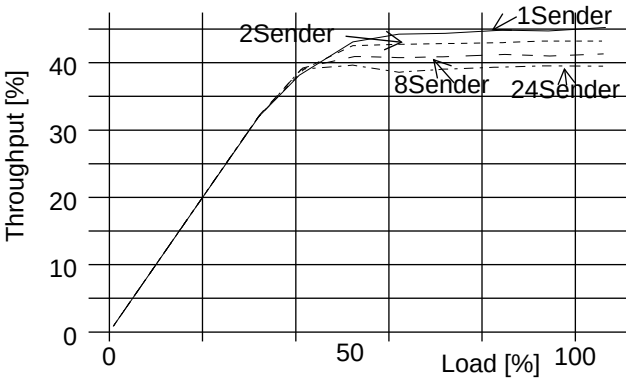

Figure 11: Throughput for 1, 2, 8, 24 stations Hiperlan

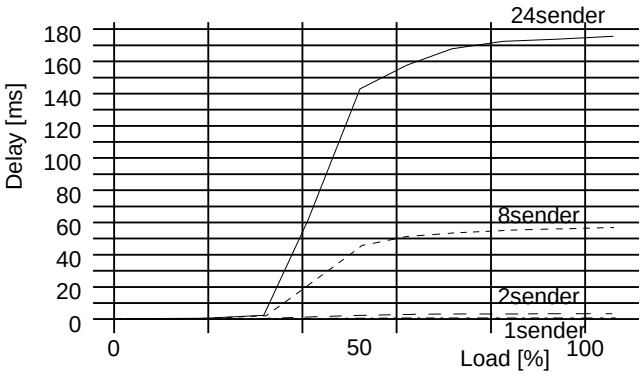

Figure 12: Delay for 1, 2, 8, 24 stations Hiperlan

each station in Hiperlan gets 5,25% of 23,5294Mb/s equalling 1,2Mb/s per station. The much higher delay values for Hiperlan compared to IEEE 802.11 (180 ms for 24 stations compared to 50 ms) is a result of the special backoff strategy in IEEE 802.11. It gives longer waiting stations an increasing chance to win the access competition. In these particular Hiperlan simulation we set the maximum life time of the packets to 1000 ms because we wanted to evaluate the access scheme for non time-constrained traffic without an upper bound for the lifetime at all. This however results in the fact that *all packets are assigned the* same MAC-priority up to an age of 920 ms (1000 ms - 80 ms), before they reach a higher priority class in the access competition.

It has to be noted, that both protocols offer a constant stable service even under high load and with many stations.

5.2 Infrastructure Networks

Only IEEE 802.11 offers a special access scheme for a point coordinated infrastructure mode. In order to evaluate the benefit of such a scheme we simulated a cell with 8 stations and compared the resulting throughput if either only distributed mode or only point co-

ordinated mode is applied (no time-bounded packet sources, only the contention free asynchronous service is used).

Figure 13 shows, that due to assured collision avoidance and reduced access overhead higher throughput is reached with PCF, even though the improvements are not very impressive (66% to 70%).

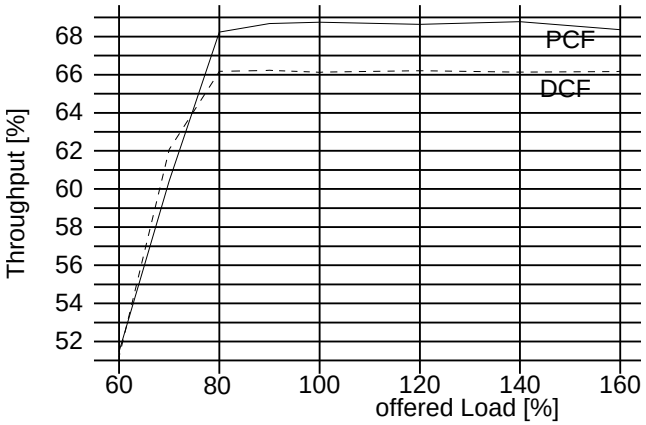

Figure 13: Throughput PCF vs. DCF IEEE 802.11

However, we have left out the additional overhead of managing the access tables in PCF, managing the application to contention free service and other functionality needed to adaptive operate in point coordination mode, since this has not been specified in the draft standard. This would cause performance degradation to a yet unknown degree.

5.3 Quality of Service in WLANs

We have already described in section 2 the potential QoS characteristics, that may be demanded by applications making use of the network. We are now looking at the capabilities of the two WLANs to support QoS guarantees:

Although Hiperlan claims to support time bounded services it does not provide any services that guarantee Quality of Service requirements. The idea behind the concept chosen for Hiperlan is that the LAN should transmit a time bounded packet first before a packet which is not time constraint and should transmit a packet with a short deadline before a packet with a longer deadline. To realize this concept the channel access mechanism provides non pre-emptive priorities. Any node automatically defers before any other node about to transmit a packet with higher priority. Therefore the Hiperlan allows to distinguish between traffic classes but it does not support the allocation of a fixed portion of bandwidth nor any other QoS parameters. Thus, Hiperlan is still just a best effort network, not suitable to extend QoS-guaranteeing networks. We simulated a network with 6 sender, that attempt to transmit time bounded traffic at a fixed rate of 100.000 byte/s. They send with high user priority whereas the parallel increased background traffic is transmitted with low user priority. The effect of both traffic classes against each other is shown in Figure 14. The throughput and delay of the time bounded traffic remains unaffected from the increasing background traffic due to its higher priority. This good behavior for the traffic classes against each other however can be damaged simply if too many stations are attempting to send with high user priority. There is no mechanism to protect the QoS from competition with too many equally prioritized stations.

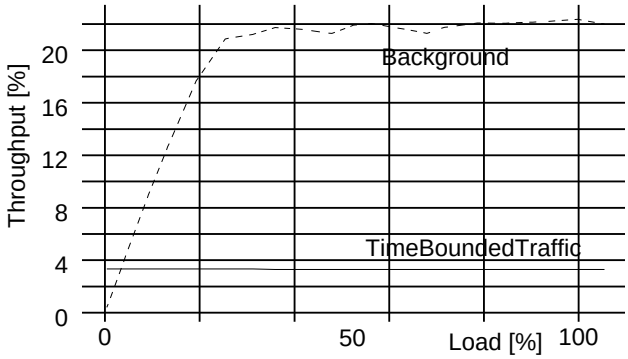

Figure 14: Throughput with Time Bounded Traffic Hiperlan

An interesting aspect can be seen in Figure 15 showing the corresponding delay: Hiperlan does not deliver any packets that have been aged beyond a certain limit. Those old packets are dropped to protect the network resources from transmitting unnecessary information. Under high load one can assume that many packets that did not reach the destination on time are dropped. Since in our simulation we only count packets that actually have reached their final destination all those dropped packets are not reflected in our delay curve. The delay value is mostly limited by the maximal life time as we have set it in our simulations (here 100 ms for time bounded traffic, 1000 ms for bacground traffic). 802.11 does not impose such a maximum life time for packets. Packets, that may not be useful anymore at the destination still count for "successful transmission".

The IEEE 802.11 draft standard offers support for time bounded services by integrating the before mentioned point coordinated mode in which a centralized controller gains control over the networks resources and as such is able to guarantee a fixed portion of these resources to stations requesting it. We ran several simulations regarding the performance of this centralized mode, for brevity reasons we will only describe the results we found. Unlike in Hiperlan any background traffic does not have any influence on the throughput time bounded traffic due to the guaranteed reserved

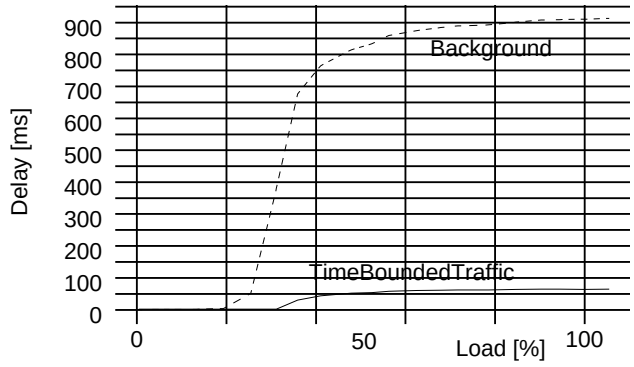

Figure 15: Delay with Time Bounded Traffic Hiperlan

bandwidth. However once more time bounded bandwidth is requested than is available, all bandwidth requests may end up unsatisfied. This depends on the strategy that is applied to satisfy requests: reduce the available bandwidth for everyone or refuse new additions to the polling list. This has not been specified by 802.11. Other unspecified issues in applying the concept of centralized polling are e.g. what strategy is used to register inside the WLAN for the services guaranteed, how the WLAN QoS is mapped to the QoS on other links of the end-to-end-connection, how to adapt to QoS-destroying configurations like hidden terminals or large fluctuations of stations in one cell etc. Another uncertainty comes with the proportion of each part within the superframe (Figure 6). We found, that if the length of the DCF part is large compared to the PCF part the advantage of the PCF does not become apparent. However if the PCF part is large compared to the DCF part, all traffic flowing across the access point (i.e. all traffic going into or coming from the attached infrastructure) has an unfair advantage to gain access compared to direct traffic between mobile hosts, reducing the availabe bandwidth for the intracellular traffic.

5.4 Dependency on Packet Size

For several reasons the dependency of the throughput on the packet size is of high interest for the evaluation of a network: First it cannot be predicted, what average packet size will be transmitted over the network, since this is highly dependent on the application, that generates the data. NFS-traffic as an example has significantly different traffic characteristics compared to WWW-related traffic or file transfer. Any future application might change the dominant traffic characteristics on a LAN, which might not perform well in the changed environment.

Second, the dependency on the packet size is important with respect to interconnection of the WLANs with other networks. The potential interconnection partners for a WLAN have significantly different maximum sizes for the transmission units (over 8000 byte for FDDI, 1500 byte for Ethernet, only 53 byte for ATM). If those packets cannot be transmitted equally efficient over the interconnected network they have to be bundled or fragmented which increases the processing overhead and complexity in the interconnecting units.

Finally, if the wireless channel is error prone with changing characteristics, it would make sense to adapt the packet size to the current state of the channel since the shorter packet has a higher chance to get through successfully without errors over a bad link.

We looked at the performance of both protocols with respect to the fixed packet size. Only for these simulations we used fixed packet sizes. As one can easily see in Figures 16 and 18, performance of both schemes severely degrades when the packet size decreases. The cost of accessing the medium in these random access scheme is independent of the size of the payload, therefore the relative overhead increases with smaller payloads. The corresponding delay figures (Figure 17 and Figure 19) show in both cases an increase for the access delay of larger packets with increasing load.

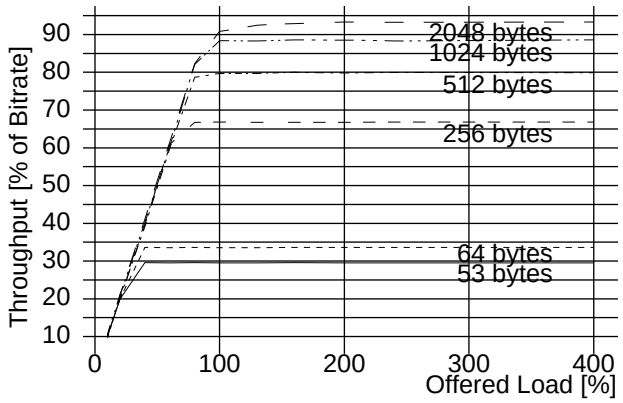

Figure 16: Throughput with different Packetsizes IEEE 802.11

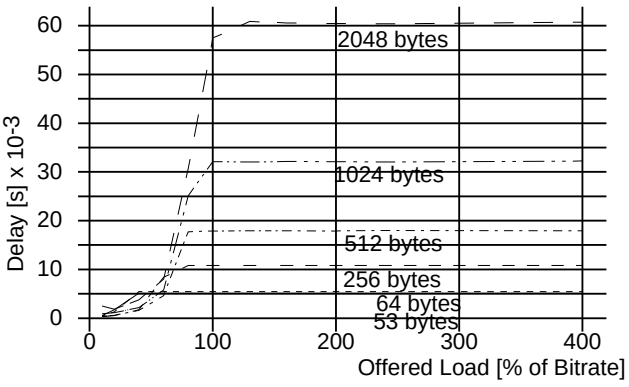

Figure 17: Delay with different Packetsizes IEEE 802.11

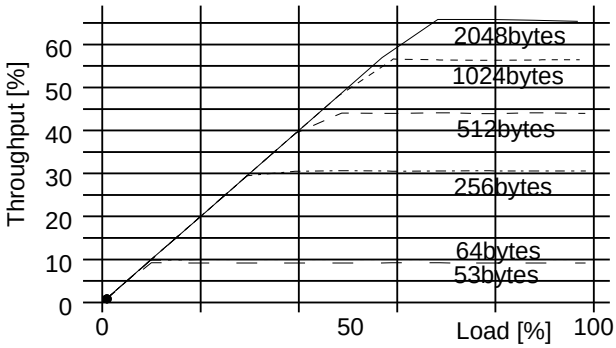

Figure 18: Throughput with different Packetsizes Hiperlan

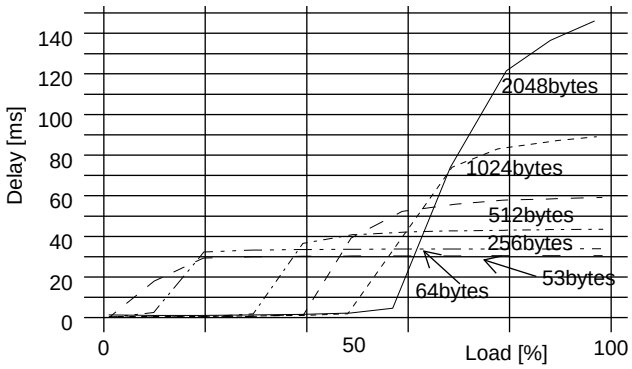

Figure 19: Delay with different Packetsizes Hiperlan

Especially when one considers to interconnect ATM with WLANs, one has to recognize that both standards perform equally poor, if the small 53 byte ATM cells are transmitted. Since packets larger than 2500 byte are ruled out in the standards for the WLANs, fragmentation cannot be prevented, if the interconnected network delivers larger packets.

5.5 Hidden Terminal Vulnerability

As elaborated earlier the "hidden terminal scenario" requires special attention on the MAC design in a wireless environment. This scenario and the problem it causes is explained in Figure 20: If station B is sending to station C the medium appears busy only for the stations located within the range of the sending station B - other stations cannot sense a signal and consider the medium idle. Therefore, station D might start a transmission since it does not notice B's ongoing transmission. However, since the receiving station C is within range of B *and* D and thus receives two signals at once it will not receive any undisturbed signal (whether destined for it or not). However, this collision cannot be detected at the sending station B unless it notices the lacking acknowledgment from station C after a certain time-out.

Both protocols are equally vulnerable to this sce-

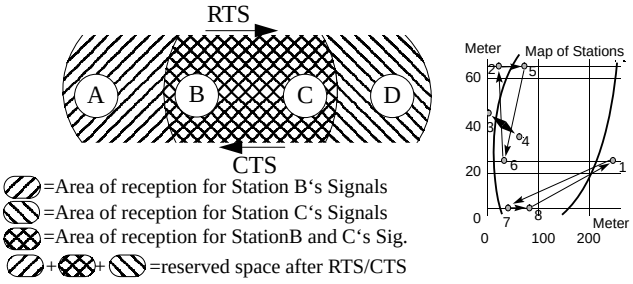

Figure 20: Hidden Terminal Scenario and simulated station topology

nario. Figure 21 and Figure 22 show the decrease of throughput for 802.11 and Hiperlan respectively, if hidden terminals are present.

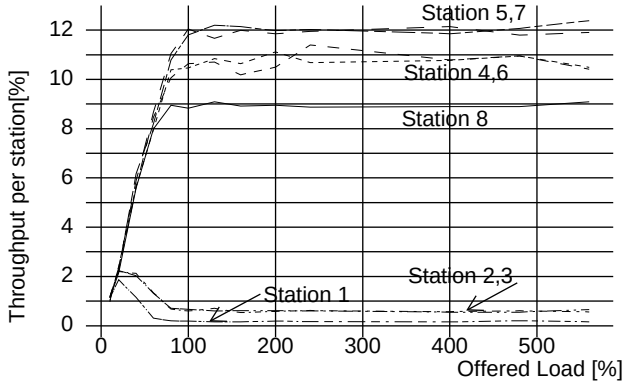

Figure 21: Throughput Hidden Terminal Setup IEEE 802.11

In both WLANs we observe different behavior depending on the position of the sender and the receiver. Our simulation setup (Figure 20) contains a cluster of 5 stations, that each could receive the signals of all 8 stations present and one station (number 1) being hidden to the remaining two stations (2 and 3). Our simulations for 802.11 (Figure 21) show that stations that send towards hidden stations (4, 6, 8) and the hidden stations themselves (1 and 2,3) achieve significantly lower throughput than the other stations (5,7). The first group (4, 6, 8) gets packets through successfully, however many acknowledgment packets are destroyed by traffic from the hidden stations. The breakdown of inbound data traffic in the case of higher load stems from the fact that the mutually hidden stations become synchronized by an earlier data exchange in the area between them. As a result, they start their backoff counters at the same time but they are unable to detect the begin of transmission of the other station.

A similar negative influence occurs in Hiperlan-networks (Figure 22). The simulation shows the decrease of the overall throughput in that scenario. With increasing load the damage done by the hidden termi-

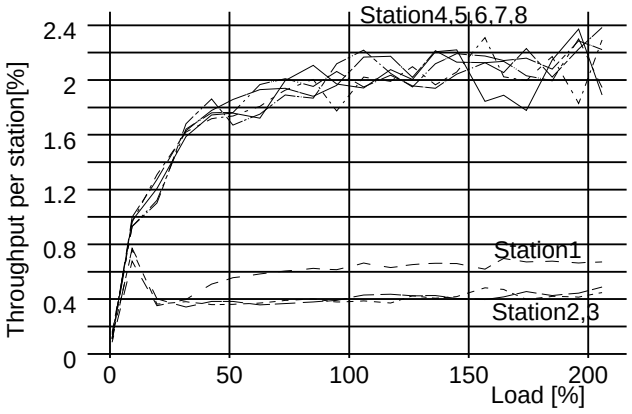

Figure 22: Throughput Hidden Terminal Scenario Hiperlan

nals to the overall load increases. Even the peak achievable throughput at 40% load is significantly lower than the throughput without hidden terminals. The Hiperlan draft standard does not yet attack this problem.

The IEEE 802.11 group realized the necessity to address this problem and integrated the RTS/CTS mechanism, developed in [10] and analyzed in [11] to solve it: Each station competes for access as described in section 4.1. When the RTS/CTS mechanism is applied, the winning station does not send data packets right away but sends a RTS[5] packet to the receiving station, that responds with a CTS[6] packet (see Figure 20). If a station captures a RTS packet from another station and it is not the destination of the RTS packet it reads the intended transmission duration from the RTS packet and stays silent for that time. The same happens if only a CTS packet is received i.e. by a station outside of the transmission range of the sender but within the range of the receiver. This guarantees that all stations within range of either sender or receiver have knowledge of the transmission as well as of its duration.

The effects of the RTS/CTS mechanism are as follows

- It increases bandwidth efficiency by its reduced collision probability since the ongoing transmission has been made known everywhere within the range of it
- It increases bandwidth efficiency since, if collisions occur, they do not occur with the long data packets but with the relative small control packets
- It decreases bandwidth efficiency since it transmits two additional packets without any payload
- It decreases bandwidth efficiency since it reserves geographical space for its transmission where or when it might actually not need it.

[5]Ready To Send
[6]Clear To Send

We simulated the same setup as in Figure 20, however with the RTS/CTS mechanism. As can be seen in Figure 23, the RTS/CTS message exchange does not completely solve the hidden terminal problem, even though significant improvements can be achieved. Still the stations that are hidden to other stations hardly get any packets through due to the above mentioned synchronization effect. Station 1 still hardly gets any packets through, but its throughput is improved compared to the figure without RTS/CTS. The same goes for stations 2 and 3 - all of the hidden stations benefit from the captured CTS packets. The non-hidden terminals all achieve the same (high) throughput due to the fact that outbound traffic is protected by the RTS packets

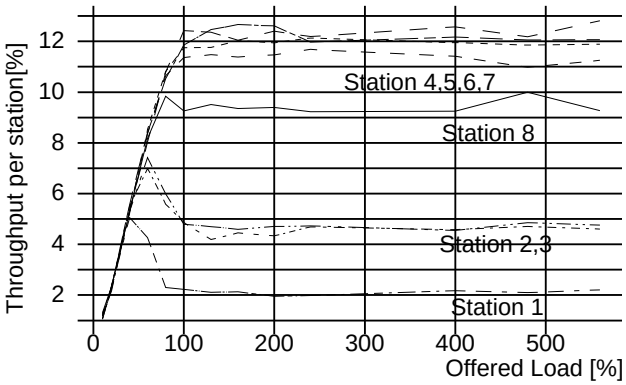

Figure 23: Throughput hidden terminal scenario RTS/CTS ON IEEE 802.11

5.6 Range Extension

A single wireless picocell is too small compared to the wired subnets commonly used, to justify ‚full subnet-status'. Therefore both draft standards have proposed strategies to extend the range of a picocell in order to reach the characteristics of a typical LAN with respect to number of supported stations and geographical coverage.

Such a range extension concept has to meet a couple of requirements: Looking from outside onto the extended LAN one should see exactly the same behavior as is expected from other widely used LANs. This means, that all added functionality has to be transparent to upper layers. As far as possible a user should not experience any disruptions while moving within the boundaries of the extended LAN. The added organizational overhead (registration, routing table setup and update and others) should be kept as small as possible. Broadcast and multicast functionality should be implemented.

Distribution System

The 802.11 project decided on an architectural concept to extend a LAN beyond a single cells range by using a separate infrastructure to interconnect the base stations in the picocells, as shown in Figure 24.

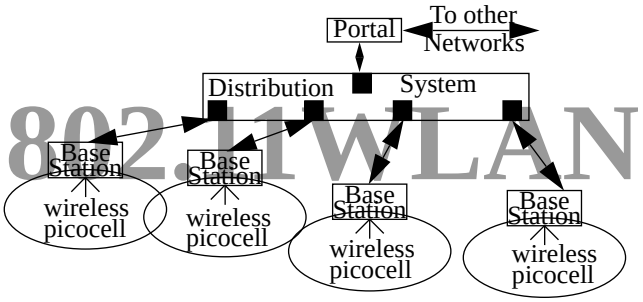

Figure 24: Distribution System

Access to or from other networks has to be realized with the help of a special device called portal, that passes the packets over the DS on to the base stations, even if only one picocell is used to form a WLAN. However, a single WLAN formed by several picocells and a DS, but without a portal is allowed as well. The media used for this distribution system (DS) as well as all its algorithms and specific details are kept unspecified in the draft standard. Just the services that have to be offered by a DS have been defined. Therefore we cannot give any graphs on the influence of such an architecture on the performance of the overall system yet. We will however sketch the issues arising with the design of a DS.

A DS has to offer solutions for two general tasks. The first task is transparent mobility support - creating the knowledge about the *current* location of the mobile hosts withing the group of cells. This splits up in the subtasks of administration of ‚routing tables' and the handover management. The second task is the transport of packets to the different picocells. This involves intercellular as well as incoming and outgoing external traffic. To do so an addressing concept is needed on top of the general MAC or IP addressing scheme, since these two addresses do not indicate the position of the end host in a group of picocells.

To avoid a new addressing scheme (like the Hiperlan-ID in the ETSI project) 802.11 carries 4 address fields in every packet (instead of the commonly applied 2 address fields "sender" and "receiver") with different meaning of the fields depending on the direction of the packet. Depending on the values in the "To DS" and "From DS" fields the addresses used in the packet have the following meaning:

To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

The 5 different address types are BSSID (Basic Service Set ID = MAC Address of BS serving the picocell), Destination Address (DA = final recipient), Source Address (SA = originator of frame), Receiver Address (RA = next station to receive frame = NOT final recipient), and Transmitter Address (TA = last intermediate station to transmit frame = NOT originator).

This addressing scheme asks for a "single-hop-source-routing" scheme, since the base stations and the portal have to have exact knowledge of the locations of the mobile hosts in the LAN in order to generate the addresses correctly and have to decide about the path at the source. To gain the information necessary on the topology registration of the mobile hosts or a search algorithm is implicit required. Alternatively a multicast/broadcast scheme may be applied, that offers the data at several points to the mobile host.

This leads to a set of possible solutions, that can be classified as shown in Figure 25. Either solution will offer different service characteristics

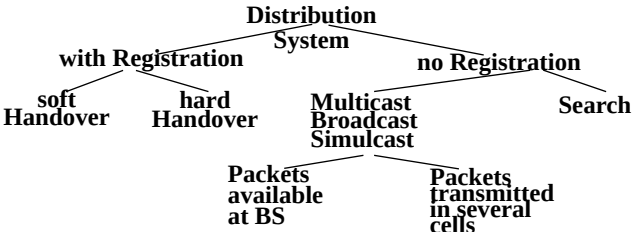

Figure 25: Classification of possible DS Solutions

Forwarding

The Hiperlan concept does not apply any fixed infrastructure to extend the radio range but relies on forwarding of packets between the wireless hosts. A Hiperlan distinguishes between two types of nodes - forwarders and non-forwarders. Non-forwarders only know their direct neighbors (stations within radio range) while forwarders know the network topology. The topology information is retrieved and maintained by continuously transmitting and receiving special control PDUs and ageing. If a non-forwarder wants to transmit a packet to a node not within radio range it either addresses the next forwarder or broadcasts it to all neighbor stations. Every packet is relayed from forwarder to forwarder until it reaches its final destination either by unicast relaying or broadcast relaying or until its lifetime is expired.

Forwarding introduces some new problems. First of

all control information have to be exchanged between the mobile nodes in order to update the topology periodically - for an effective routing decision, the forwarder has to have a consistent image of the topology at the very moment. Since common routing algorithms are not designed for the continuously changing network topology new algorithms have to be designed [12]. Second, some packets have to travel via more than one wireless link to their destination. As wireless links are known as error-prone this increases the risk of errors.

From the internetworking point of view in order to support mobility one has the major advantage that no re-routing of the End-to-End-connection is needed. The relaying of cells to the destination is done invisibly within the wireless LAN. Also problems like continuous service and hitless switching are inherent features of this approach as long as the dynamic forwarding algorithm works appropriately.

In order to investigate the influence of introducing forwarding we have investigated a scenario as depicted in Figure 26. We examine traffic from a single terminal which is outside radio range of a second cluster. Please note that we have chosen such artificially terminal configuration in order to stress the problems one has to be aware of in the case of forwarding. The simulation results showed that an isolated station almost has no chance to send into a cluster of communicating stations due to the hidden terminal effect. In fact starting with fairly low overall load the throughput from the hidden station into the cluster decreases rapidly with increasing overall load.

The reverse case - traffic to a single terminal outside a cluster - causes similar unsatisfying results. We observed that the isolated station was able to receive packets from the cluster even under high overall offered load. But we also observed that the achieved throughput per station is lower than in the case of a fully meshed network with the same overall offered load. A more detailed discussion of the simulation results can be found in [13].

The simulation model we used for the investigation above makes the assumption that the carrier sense detection range is of the same size as the communication size. Since the bad performance results of the isolated station are mainly due to the hidden terminal problem the emerging standards have a larger carrier sense detection range than communication range. The effects of this slightly different situation will have to be investigated in a further step.

Comparing the Approaches

Looking at the two approaches ‚distribution system' and ‚forwarding', one can say that both may be able to fulfill the task of extending connectivity beyond the radio range, but have different degrees of reliability. The

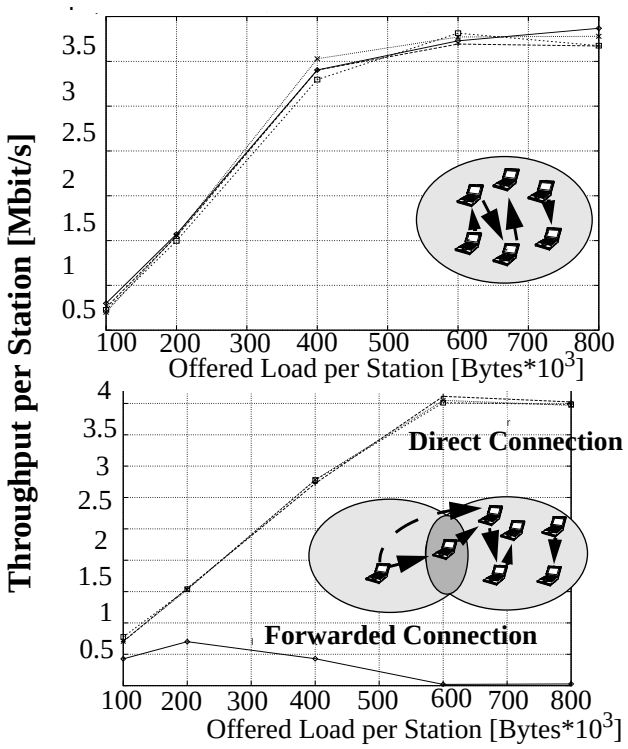

Figure 26: Throughput fully meshed or with Forwarding Hiperlan

forwarding concept relies on the presence of forwarding stations - mobile hosts that are willing to donate energy and processing power to the benefit of other stations. Therefore in an environment, where these resources are scarce it might be hard to find such a ‚volunteer'. The advantage of forwarding however is the instantaneous possibility of using the mechanism without any additional installation of infrastructure. In cases of very low load the implicit hidden terminal scenarion will not be a big obstacle for succeeful communication beyond radio range. The distribution system requires the installation and maintanance of a supporting infrastructure, before it is usable. The supporting hardware will also have to be considered for the cost-per-interface calculation. Once this installation is done, the system will reliably offer its services, it will easily integrate common LAN services like printer or file server and thus will easily fit into the well known LAN environments.

6 Final Remarks

In this paper we have presented our simulations on the two draft standards currently in development - IEEE 802.11 and ETSI RES10 Hiperlan. We have been concentrating on the performance of the access protocols, simulating general application scenarios and looking at special issues relevant for WLANs. We evaluated the performance for different numbers of stations and under

different load conditions.

According to our simulations both protocols perform satisfyingly in general configurations, however the much larger delay values in Hiperlan if no maximum lifetime is used are remarkable. Performance under overload condition remains stable. Both WLANs are able to separate traffic with requirements for time bounded delivery from asyncronous traffic, but only 802.11 will be tunable to protect time bounded traffic rate from too many high-priority sources. Hiperlan is able to support time bounded traffic in ad-hoc networks whereas 802.11 requires point coordination mode. Both access schemes perform equally bad with small packets. The hidden terminal scenario is still a problem in both protocols, which is also the reason for the failing of the forwarding mechanism in Hiperlan under high load. Solving these problems will be an area for future research.

References

[1] The editors of IEEE 802.11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Draft Standard IEEE 802.11, P802.11/D5.0*; Jul 1996

[2] ETSI Secretariat, *Hiperlan Functional Specification, Draft prETS 300 652*, Jul 1995

[3] Regents of the University of California*PTOLEMY*, ftp://ptolemy.eecs.berkeley.edu, http://ptolemy.eecs.berkeley.edu, news:comp.soft-sys.ptolemy

[4] TraceFile pOct.TL and TraceFile OctExt.TL, no longer available

[5] W. Diepstraten, *Wireless Network Performance Modelling Approach*, IEEE 802.11 working group paper 11/92-26, Feb 1992

[6] J. Fowler, W. Leland, *Local Area Traffic Characteristics with Implications for Broadband Network Congestion Management*, IEEE Journal on Selected Areas in Communications 9, 1139-1149, 1991

[7] Will Leland et al. *On the Self-Similar Nature of Ethernet Traffic (Extended Version)*, IEEE Transactions on Networking, Vol. 2, Nr. 1, Feb 1994

[8] W. Diepstraten, *A Wireless MAC Protocol Comparison*, IEEE 802.11 working group paper 802.11/92-51, May 1992

[9] H-Y. Lach *EY-NPMA*, ETSI Res 10 working group paper 94/CAM/1, Sep 1994

[10] P. Karn, *MACA - A new Channel Access Method for Packet Radio*, ARRL/CRRL Amateur Radio 9th Computer Networking Conference, Sept. 22 1990

[11] V. Bharghavan, A. Demers, S. Shenker, L Zhang, *MACAW: A Media Access Protocol for Wireless LAN's*, SIGCOM 1994

[12] D. Johnson, *Routing in Ad Hoc Networks, Proceedings of the Workshop on Mobile Computing Systems and Applications*, pp. 158-163, IEEE Computer Society, Santa Cruz, CA, Dec 1994

[13] A. Wolisz, J. Weinmiller, M. Schlaeger, H. Woesner, *Wireless Access to High Speed Networks*, October 1995 in: High-Speed Networking for Multimedia Applications, W. Effelsberg, O. Spaniol, A. Danthine, D. Ferrari (eds.), Kluwer Academic Publishers, Boston/Dordrecht/London, 1996

[14] A. Wolisz, R. Popescu-Zeletin, *Modelling end-to-end protocols over interconnected heterogeneous networks*, Computer communications, vol 15 no 1, Jan/Feb 1992