University of Würzburg
Institute of Computer Science
Research Report Series

Performance Comparison of Handover Mechanisms in Wireless LAN Networks

Rastin Pries and Klaus Heck

Report No. 339 September 2004

University of Würzburg
Department of Computer Science
Am Hubland, D-97074 Würzburg, Germany
[pries,heck]@informatik.uni-wuerzburg.de

Performance Comparison of Handover Mechanisms in Wireless LAN Networks

Rastin Pries and Klaus Heck
University of Würzburg
Department of Computer Science
Am Hubland, D-97074 Würzburg, Germany
[pries,heck]@informatik.uni-wuerzburg.de

Abstract

The upcoming discussion about integrating the Wireless LAN standard into future mobile networks of the 4th Generation (4G) does not only strengthen the importance of the IEEE 802.11 standard family, but necessitates the support of Quality-of-Service (QoS) even when the user moves between different Access Points. In this paper, we study different Wireless LAN handover mechanisms and their ability to support QoS traffic. Therefore, we implemented the handover mechanisms and additional proposals in a simulation environment and analyzed their ability to support a specific QoS level.

1 Introduction

Wireless Local Area Networks (WLAN) based on the IEEE 802.11 standard [1] have seen an immense growth in recent years. Public access to WLAN systems has become increasingly available in areas like convention centers, airports, shopping malls, and restaurants. So far, the coverage of the networks has been limited to these hot spot areas in contrast to existing mobile networks such as GSM and GPRS. These cellular networks provide almost a complete coverage of the country, but only low data rates are supported. Developments like the Universal Mobile Telecommunication System (UMTS) aim at overcoming this drawback and provide higher data rates for applications such as gaming, video streaming, and music downloads. Due to the immense costs of the introduction of third generation mobile networks, the comparatively "cheap" WLAN has evolved to a contender to the mobile industry and needs to be taken seriously.

Originally, Wireless LAN was designed for indoor solutions where a wired LAN cannot be supported. In a home network or a small office, a single Access Point (AP) is often sufficient. When considering larger networks with many APs where the client can cross the coverage areas of several APs, the system should ensure that the connection is maintained. A *handover* is the process, where the client leaves the coverage area of one AP and enters another. Data loss and delays should be kept minimal to ensure seamless handover. In contrast to existing mobile networks, the WLAN handover is mobile initiated, i.e. the client decides according to the signal strength, if it has to perform a handover.

If the Wireless LAN standard is integrated into future mobile networks of the 4th Generation (4G), the handover times will have to be minimized to ensure a specific Quality of Service (QoS) level. In this paper, we want to show that it is possible to support QoS traffic in a Wireless LAN network even if the stations have to perform a handover. Therefore, we implemented five different handover mechanisms in the OPNET modeler, a simulation environment. All handover mechanisms will be analyzed with regard to the delay and we will see that at least two mechanisms are fast enough to provide QoS traffic.

The paper is organized as follows. In Section 2, one WLAN Medium Access Control (MAC) mechanism is introduced and Section 3 describes the handover mechanisms for Wireless LAN networks. This is followed by Section 4 which deals with the simulation model. After the description of the simulation scenario, the performance of the different handover mechanisms is evaluated in Section 5. Finally, Section 6 concludes this paper.

2 WLAN Specifications

The IEEE 802.11 standard specifies the Medium Access Control (MAC) layer and the Physical (PHY) layer to provide a Wireless LAN that enables station mobility transparent to higher protocol layers. The standard supports the following three different topologies.

- Independent Basic Service Set (IBSS) networks
- Infrastructure Basic Service Set (BSS) networks
- Extended Service Set (ESS) networks

The IBSS networks are often referred to as ad-hoc networks, where all stations are communicating directly with each other and must be in direct communication range. IBSS networks are composed of a small number of stations for a specific purpose and for a short period of time, for example a single meeting in a conference room.

In contrast, a BSS network is divided by the use of an Access Point (AP). The AP is used for the whole communication in the network, including the communication between mobile stations in the same area. The stations transmit each frame to the Access Point, who forwards them within the same area or to the backbone network. An Extended Service Set network combines different BSS networks. In such an ESS network, the Access Points act as bridges between the wireless link and any other layer 2 connection, for example an Ethernet backbone. Figure 1 illustrates a network with two BSS forming an ESS.

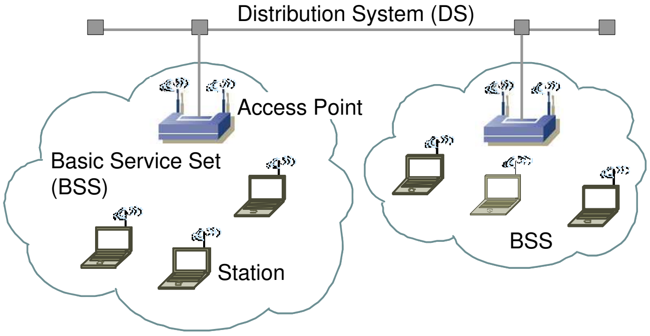

Figure 1: Two different Basic Service Sets (BSS) forming an ESS

For our simulations, we chose one ESS with a variable number of BSSs. To offer a continuous coverage area in one ESS, the different BSSs have to overlap and the interference between the Access Points have to be minimized. To reduce the interference, the Access Points have to be configured to use different channels on the 2.4 GHz band. The German regulatory domain allows 13 channels. Due to the fact that these channels overlap, the Access Points have to be separated by a minimum of five channels. If adjacent channels are selected, there would be a great deal of overlap in the center lobes and high levels of interference. Therefore, the Access Points in our simulations are configured to use channel one, six, and eleven as seen in Figure 2.

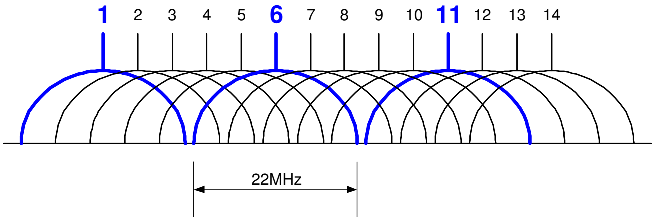

Figure 2: Overlapping frequencies

To move from one BSS to another, the stations have to accomplish a layer 2 handover and if moving from one ESS to another, a layer 3 handover is needed which can be accomplished with Mobile IP. Analyzing the layer 2 handover mechanisms in one ESS between the different Basic Service Sets is the goal of this paper.

2.1 Medium Access Control (MAC) Layer

The Distributed Coordination Function (DCF) is the primary access mode using the CSMA-CA protocol for sharing the wireless medium as shown in Figure 3.

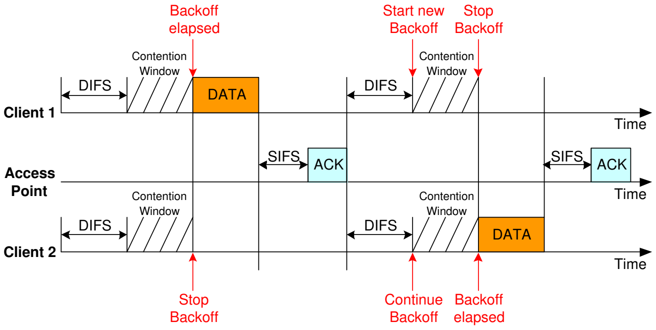

Figure 3: Carrier Sense Multiple Access with Collision Avoidance

Stations that want to transmit a packet have to compete with each other for access and all stations have equal rights. However, Wireless LAN stations cannot detect a collision on the medium. Therefore, an acknowledgment scheme has to be performed. If no Acknowledgment is received by the sending station it will simply retransmit the packet. In order to reduce the collision probability on the wireless medium, the stations sense the medium for a period of time (DIFS) and perform a backoff before transmitting a packet.

3 Handover Mechanisms

The basic parameter for a roaming station is the *Signal-to-Noise Ratio* (SNR). As soon as the SNR drops below a specific threshold, called *Cell Search Threshold*, the station starts the handover process. During this process, the station searches for new Access Points and if the difference between the SNR of the old AP and one possible new AP has passed a threshold known as *Delta SNR*, see Figure 4, the station initiates the actual handover.

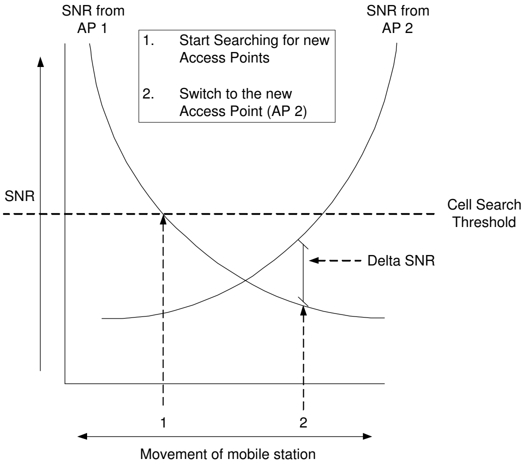
SNR from AP 1
SNR from AP 2
1. Start Searching for new Access Points
2. Switch to the new Access Point (AP 2)
SNR
Cell Search Threshold
Delta SNR
1
2
Movement of mobile station

Figure 4: Handover decision

These two thresholds depend on the Access Point density. The AP density can be set by the user to low, medium, or high. Table 1 shows the Cell Search Threshold and the Delta SNR for these densities. The Wireless LAN handover itself consists of three individual steps: *scanning*, *authentication*, and *association*. During the scanning process, the station searches for new Access Points to associate to. The authentication procedure is needed to exchange information about the station and data encryption. Finally, the station has to associate with the Access Point.

Table 1: IEEE thresholds

Threshold	AP Density		
	Low	Medium	High
Cell Search [dB]	10	23	30
Delta SNR [dB]	6	7	8

3.1 Scanning

To determine which network to join, a station must first scan for available networks. The IEEE 802.11 standard defines two scanning mechanisms, *active* and *passive scanning*.

A station using *passive scanning* switches to the first channel allowed by the regulatory domain and waits for *Beacon* frames. If the station receives a Beacon frame, it measures the Signal-to-Noise Ratio and stores additional Access Point information. After a specific time, the station switches to the next channel until every channel is scanned. Scanning every channel results in a lot of overhead, because the station receives Beacon frames from a number of Access Points from overlapping channels. Therefore, most stations scan only the non-overlapping channels, for example channel one, six, and eleven. This *fast passive scanning* mode reduces the period of time used for scanning compared to the normal passive scanning, but is more fault-prone. An Access Point might not be detected due to a Beacon delay or a low SNR.

The second main type of scanning is called *active scanning*. Here, the station takes a more assertive role. Rather than listening for networks to announce themselves, the station attempts to find the network by transmitting *Probe* frames. The station moves to the first channel and waits for the Probe Delay Timer to expire. If an incoming frame is detected, the channel is in use and will be probed. The timer prevents an empty channel from blocking the entire procedure. Afterwards, the station gains access to the channel using the Distributed Coordination Function. It transmits a broadcast *Probe Request* frame, starts a timer called *Min Channel Time* and processes all incoming *Probe Response* frames. If the medium is not busy during Min Channel Time, the station scans the next channel. If the channel gets busy, the Min Channel Time is canceled and the station waits for Probe Response frames until the maximum time, *Max Channel Time*, has expired as seen in Figure 5. Each Access Point receiving the Probe Request frame has to respond with a Probe Response frame.

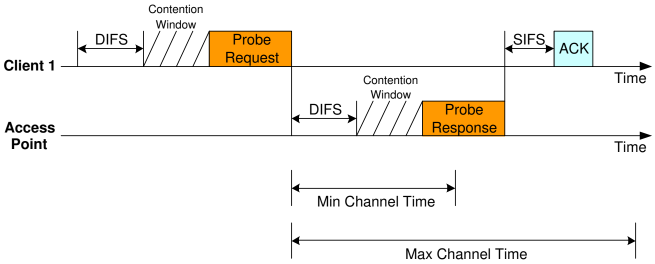

Figure 5: Active scanning procedure

The purpose of this scanning procedure is to find every Basic Service Set that the station can join. To be able to process all Access Points in a specific area, the Max Channel Time has to be adjusted in areas with a large number of Access Points. One way to adjust the Max Channel Time is described in Section 5. Like in passive scanning, the station may be configured to scan all channels, *normal active scanning*, or scan only the non-overlapping channels, *fast active scanning*.

Finally, there is one additional active scanning mechanism, *scanning with neighborhood detection*, which is not included in the IEEE 802.11 standard. Different proposals [2], [3], and [4] try to reduce the channel scanning time. Therefore, the moving station has to know the MAC address and current channel of the Access Point to be scanned in advance. This information is placed in all Beacon and Probe Response frames, see [3]. The maximum number of Access Point information within a single Beacon and Probe Response frame is set to twelve to reduce the overhead. An administrator can set the information about all other Access Points in the network or the Access Point list can be created with the movement ratio which is described in [4]. If a station uses neighborhood scanning, it picks up an Access Point from the list and transmits the Probe Request frame directly to this Access Point.

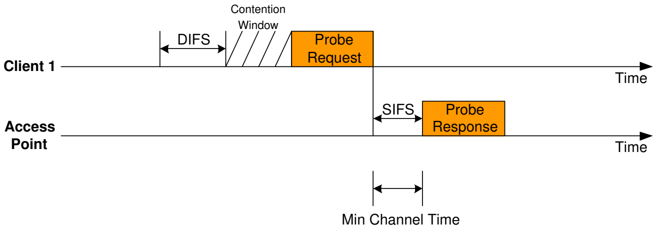

Figure 6: Scanning using neighborhood detection

Kawahara [2] describes three different types of neighborhood scanning, but only the one in Figure 6 is used for the simulation. The other two types acknowledge the Probe Request and transmit the Probe Response frame after the transmission of other frames which increases the scanning delay. When using type one, the Access Point responds directly to the request, if the address of the Probe Request frame matches. The reply is transmitted after a Short Interframe Space (SIFS) like an Acknowledgment during a normal data transmission. If the Access Point does not reply after Min Channel Time, the station picks the next Access Point from the list and transmits another Probe Request frame. This reduces the scanning time compared to other active scanning mechanisms, because the station does not have to scan three or all channels and wait for the Max Channel Time to expire.

3.2 Authentication

Subsequent to the scanning procedure, the station tries to authenticate with the Access Point with the best SNR or, if neighborhood scanning is used, with the Access Point which first replies to the Probe Request. A station has to authenticate before joining a network, but the standard does not describe that the station can authenticate only for one Access Point. The station might authenticate during the first association procedure with all Access Points in the network, see [4]. If the station leaves the coverage area of the Access Point, it does not have to authenticate with the new AP of the same network provider before reassociating with this AP. This form of pre-authentication is used for the simulation, because we can ignore the whole authentication process during a layer 2 handover.

3.3 Association

To gain full access to the network, the station has to associate with an Access Point or reassociate with a new Access Point. Because we are simulating handovers where the station has already associated with an Access Point in a specific Extended Service Set, only the reassociation procedure is taken into account.

If a station moves from the coverage area of one Access Point to a new one, the reassociation procedure is used to inform the whole network of its new location. First of all, the station transmits a *Reassociation Request* frame to the Access Point with which the station wants to connect, as seen in Figure 7.

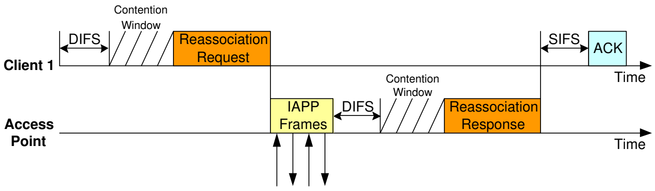

Figure 7: Reassociation procedure

The Reassociation Request contains the MAC address of the previous Access Point. The new AP has to verify that the station was connected to the previous AP by using the *Inter Access Point Protocol* (IAPP) over the wired backbone network.

The IAPP is a part of the IEEE 802.11 family specified as IEEE 802.11f [5]. It defines messages and data to be exchanged between Access Points to support roaming. The IAPP protocol uses TCP for Access Point communication and UDP for Remote Authentication Dialing User Service (RADIUS).

After the Access Point has received the Reassociation Request from the station, it transmits a Move Request frame over the wired network to the previous AP. The previous Access Point disassociates the station, or, if the station is not found, denies the request. If the station has been associated with the previous Access Point and the Access Point has acknowledged the Move Request, the new Access Point transmits a Layer 2 Update frame to inform every other Access Point, switch, and router of the station's new location. Afterwards, the previous Access Point forwards the packets destined for the station over the wired network to the new Access Point. The new Access Point transmits a Reassociation Response to the station using the normal DCF as seen in Figure 7. Finally, the station acknowledges the Reassociation Response frame and the handover is completed.

4 Simulation Overview

We implemented a simulation of the Wireless LAN IEEE 802.11b [6] standard using the OPNET simulator. The IEEE 802.11b standard is a part of the IEEE 802.11 family allowing data rates of up to 11 Mbps. Our implementation accounts for the MAC and the PHY layer, all handover mechanisms, and the IAPP layer which is placed above the TCP/UDP layer at the Access Points.

In order to evaluate which handover process is responsible for the most delay, a scenario with no background traffic is created, see Figure 8. The Access Points, AP1 uses channel 1 and AP2 uses channel 6, are connected via a 100 Mbps Ethernet link to a switch which is attached to a router. The Access Points are placed at a distance of 70 meters and the wireless source client moves with 5 kmph between the Access Points. The source client itself communicates with a destination workstation in the backbone network. The source client performs a handover after it has moved about 50 meters away from Access Point 1 (AP1). The total handover time is measured and split in scanning and reassociation timings.

To get to know which effect background traffic has on the total handover performance, different clients are placed in the WLAN cells for the next scenario, as shown in Figure 9. The Access Points are configured to use only non-overlapping channels. AP1 uses channel 1, AP2 channel 6, and AP3 channel 11. The circles around the Access Points mark their coverage areas. One client using a voice application moves between the different Wireless LAN cells. Other, fixed clients are placed in the Wireless LAN cells to produce background traffic with voice and FTP applications.

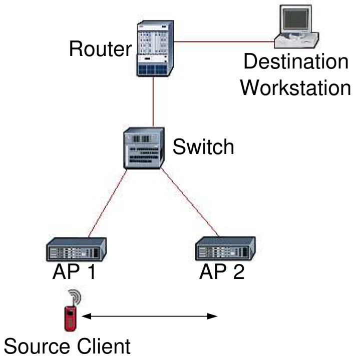

Figure 8: Simulation scenario

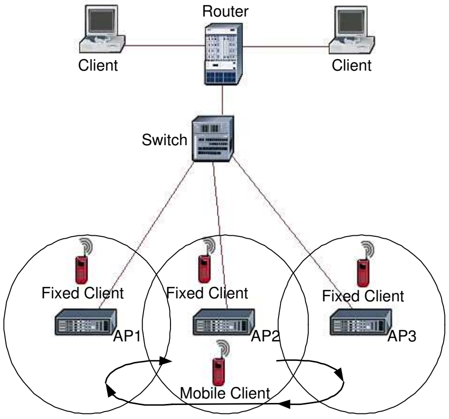

Figure 9: Simulation scenario with background traffic

4.1 Traffic Model

The most common best-effort application is the World Wide Web. However, the simulation of WWW users demands very long simulation runs in order to account for the high variability of traffic. Therefore, FTP traffic is considered as a worst-case scenario for Web traffic. An FTP client placed in a WLAN cell is assumed to perform FTP downloads from an FTP Server in the backbone network.

Additionally to the FTP traffic, some simulations are configured to use voice traffic. The most important voice codecs are G.711 (64 kbps), G.729 (8 kbps), and G.723.1 (5.3 or 6.3 kbps). Earlier studies regarding the suitability of voice codecs in Wireless LAN environments have shown that the G.723.1 [7] voice codec with 5.3 kbps and a frame size of 30 ms provides the best performance. It is possible to support up to 18 voice clients in one cell with the necessary Quality of Service (QoS) level from the ITU-T [8].

5 Results

The results section is divided into three different parts. In the first part, we analyze the WLAN handover and show which part of the handover process is responsible for the most delay. The next part focuses on the handover performance using a voice application and in the last part the voice application is simulated together with FTP traffic.

5.1 Handover with no background traffic

First, we analyze the handover with the five different scanning mechanisms described in Section 3. The simulation is set up like shown in Figure 8 with the Access Points transmitting a Beacon frame every 100 ms. The source client moves between AP1 and AP2 and uses the normal Distributed Coordination Function while communicating with a workstation in the backbone network. The station starts the scanning process when the Signal-to-Noise Ratio (SNR) drops below 10 dB. Figure 10 shows the ratio between the scanning and the reassociation process for the five different scanning mechanisms. For all mechanisms, the reassociation process takes the same amount of time, but the scanning time varies.

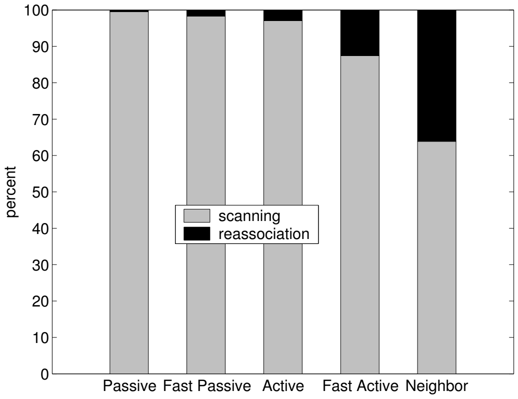

Figure 10: Scanning versus reassociation time

If the normal passive scanning is used, which means that the station scans each of the thirteen channels for 100 ms, the total scanning procedure takes 1.3 s or 99.8 % of the total handover time. The scanning time can be reduced if neighborhood scanning is used, but still takes about 63 % of the total handover time. The neighborhood scanning is the fastest method, because only two Access Points are placed in the network and therefore, the source client has to scan only the AP with which it is not actually connected to. Since the reassociation time always takes the same amount of time, the different scanning mechanisms have to be analyzed and optimized to reduce the whole handover time.

First of all, we analyze the scanning delay for the two passive scanning mechanisms. The passive scanning delay depends on the inter-arrival time of the Beacon frames. Most Access Point vendors set this value to 100 ms, but the IEEE 802.11 standard does not specify this value. Therefore, we set up the Beacon inter-arrival time between 4 ms and 100 ms and simulate the maximum throughput on the wireless link. To get the maximum throughput, a station acts as a saturated UDP source, such that it utilizes the whole bandwidth that remains. Figure 11 shows the maximum throughput on the left Y-axis and the total handover delay on the right Y-axis using the fast passive scanning mechanism.

For a Beacon inter-arrival time between 4 ms and 50 ms, the maximum throughput increases from 4.4 Mbps to more than 5.5 Mbps. If we choose a Beacon interval greater than 50 ms, the maximum throughput does not further increase, thus the Beacon inter-arrival time should be set to 50 ms to get a maximum throughput about 5.5 Mbps on the wireless link. This reduces the complete handover time to 652.65 ms for the normal passive scanning and to 152.65 ms for fast passive scanning.

The scanning time with active scanning depends on the Min Channel Time and the Max Channel Time. Therefore, we simulate the time an Access Points needs to reply to a Probe Request frame. The number of Access Points is varied from one to ten Access Points within the reach of the station. Figure 12 shows the Probe Response delay.

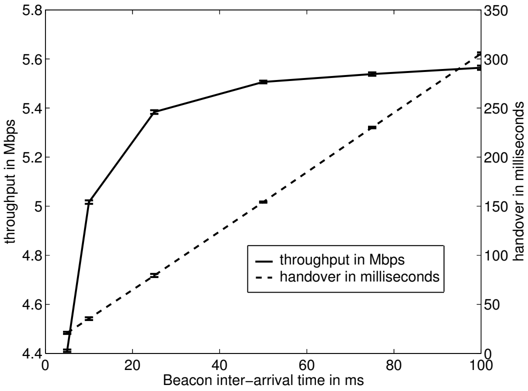

Figure 11: Fast passive scanning with different Beacon inter-arrivals

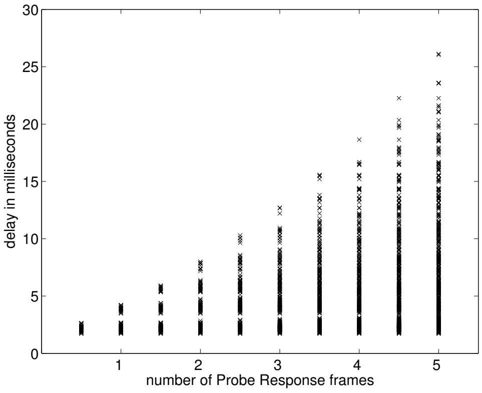

Figure 12: Probe Response frame delay

The probe-wait time tends to be within one millisecond and seven milliseconds for three or less Probe Response messages. For four to eight response messages the responses take to up to 17 ms. Otherwise, it tends to be within an interval from four milliseconds to 27 ms. This shows that the MaxChannelTime should be set according to the number of Access Points within the reach of the station. The start of a Probe Response frame is always received within 0.8 ms and so the Min Channel Time is set to this value for the following simulations. The IEEE standard created a value for the number of Access Points, called AP density which is normally used for handover decisions. Table 2 shows our settings of the Max Channel Time according to the AP density.

When using neighborhood detection, the scanning process does not only depend on the Min Channel Time, but also on the number of Access Points on the list, transmitted with every Beacon and Probe Response frame. If the number of Access Points in an ESS is increased and not all Access Points are within the reach of the station, the station has to scan for more Access Points to find one with an acceptable SNR. Figure 13 shows the handover delay for different numbers

Table 2: MaxChannelTime based on the AP density

Number of Responses	AP Density	Max Channel Time
1-3	low	7 ms
4-7	medium	17 ms
8-10	high	27 ms

of APs in the network. The total handover increases from 4 ms for two Access Points to about 23 ms for twelve Access Points. If there are more than twelve APs in the network, the APs have to decide which APs they have to put on the list and transmit with the Beacon and Probe Response frames.

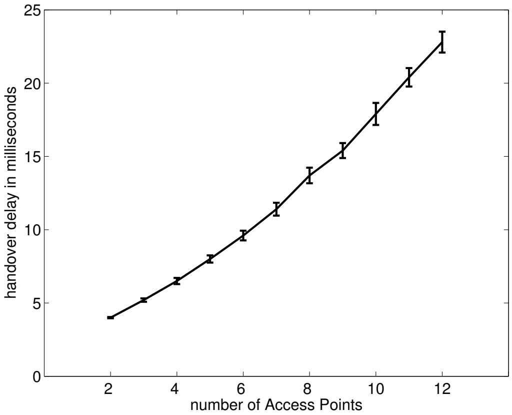

Figure 13: Handover time with different number of AP's using neighborhood scanning

The simulations with no background traffic have shown that the scanning mechanisms are responsible for the most handover delay. Therefore, we analyzed the different scanning mechanisms and adjusted the parameters. In the next part, we analyze the handover performance with a voice application to show if it is possible to support QoS even if a handover has to be performed.

5.2 Handover with voice traffic

For the voice scenarios, we use the G.723.1 standard as already described above. In contrast to the last simulation scenario, we use three Access Points like shown in Figure 9, which increases the handover time for the active scanning and neighborhood scanning mechanisms. The Beacon inter-arrival time is set to 50 ms according to the results in the previous part. When we are using normal passive scanning, the handover takes at least 652.65 ms, which does not suffice the ITU-T guidelines for QoS during a voice conference. Therefore, normal passive scanning is not taken into account for the following simulation runs.

The remaining four scanning mechanisms are simulated with a different number of fixed voice clients in each wireless cell. The number of fixed voice clients is increased from 0 to 17. Figure 14 illustrates the results for this simulation scenario.

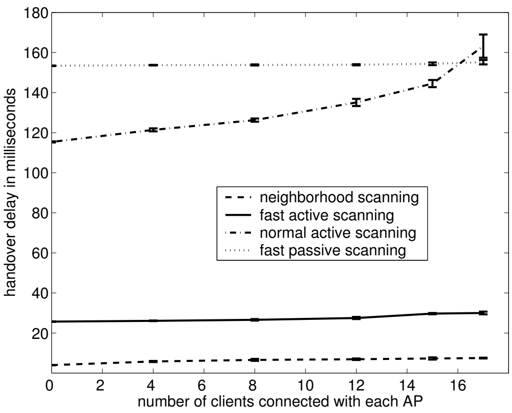

Figure 14: Handover time / number of clients

The x-axis shows the number of voice clients in each Basic Service Set and the y-axis illustrates the complete handover time. For fast active, neighborhood, and fast passive scanning, the time needed to complete a handover does not raise much with an increasing number of voice clients in one wireless cell. If we take for example the fast active scanning mechanism, the time to accomplish a handover increases from 26 ms with no other clients in the network to 30 ms with 17 fixed voice clients. The neighborhood scanning mechanism provides the fastest handover, but only three Access Points are placed in the network and therefore, the scanning time is reduced to about five milliseconds.

When using normal active scanning, the time increases from 117 ms to 166 ms if 17 voice clients are placed in each cell and is even worse than fast passive scanning. The handover delay itself with the active and fast passive scanning mechanisms is still conform with the ITU-T guidelines, but if we take the coding delay and the delay on the wired network into account, an adequate echo control has to be assumed.

5.3 Handover with traffic mix

The last part has shown that the fast passive scanning mechanism provides faster handover than normal active scanning, if the number of fixed voice clients connected to one Access Point is large enough. The next simulations analyze the handover performance with one FTP client at each Access Point and one moving voice client. The FTP clients try to use the full WLAN capacity and the voice client performs 500 handovers for each scanning mechanism. Figure 15 shows the cumulative handover PDF for the different scanning scenarios. The figure illustrates that only 40 % of the normal active scanning handovers are faster than the fast passive scanning handovers, but 60 % take more time. This approves the result from the voice scenario where the fast passive scanning mechanism is always faster in wireless cells with high loads.

Thus, we use only three Access Points, neighborhood scanning provides the fastest handover. Almost every handover has finished after 15 ms and when using fast active scanning, the handover takes at least 26 ms. Compared to the fast passive scanning, the fast active scanning mechanism is more than three times faster.

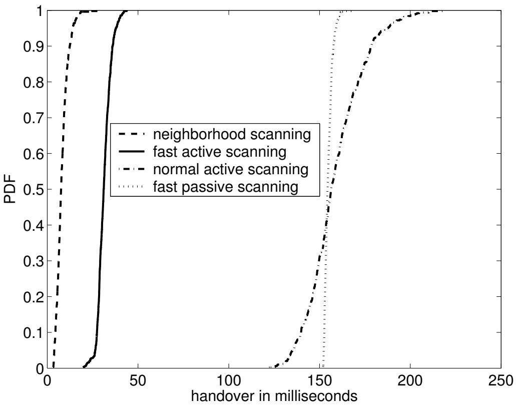

Figure 15: Cumulative probability distribution function of handover times using DCF

6 Conclusion

In this paper, we investigated the handover mechanisms described in the IEEE 802.11 standard and additional subsequently published proposals. Only two of the three parts of the handover were analyzed, since we assumed a form of pre-authentication for the simulations. We showed that the scanning process dominated the handover time and thus, concentrated on analyzing the different scanning mechanisms.

The handover performance was analyzed in relation to three different traffic types (no background traffic, voice traffic, and a traffic mix with FTP data sources). We have shown that a 50 ms Beacon inter-arrival time does not decrease the maximum throughput, but highly improves the handover performance for the passive scanning mechanisms. However, the normal passive scanning still does not suffice the QoS requirements.

For the active scanning mechanisms, we have shown a way to adapt the Max Channel Time according to the Access Point density.

Finally, we can conclude that neighborhood scanning provides the fastest handover in all scenarios even with a large number of Access Points, but this scanning mechanism is not yet included in the IEEE 802.11 standard and fast active scanning is completely sufficient for providing QoS in public hot spots. If no Access Point is found during fast active scanning, the station might switch to fast passive scanning.

Our studies proof that QoS support in Wireless LAN environments is possible even if the station has to perform a handover. Further studies have to take a closer look at prioritizing multimedia traffic and analyze the system performance in case of overlapping and co-located cells.

References

[1] IEEE, "IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification," 1999. ISO/IEC 8802-11:1999.

[2] T. K. M. Ryong Jeong, F. Watanabe and Z. Zhong, “Proposed Text for Fast Active Scan,” 2003.

[3] S. Black and H. Sinivaara, “A revised proposal for the distribution of neighborhood BSS information,” 2003.

[4] S. Pack and Y. Choi, “Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model,” 2002.

[5] IEEE, “Recommended Practice for Multi-Vendor of Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation,” 2003. IEEE 802.11f-2003.

[6] IEEE, “IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band,” 1999. IEEE 802.11b-1999.

[7] ITU-T, “Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s,” 1996. ITU-T Study Group 15.

[8] P. Coverdale, “Multimedia QoS requirements from a user perspective,” 2001. ITU-T Study Group 12.